A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM

SURAPOL RUAYSUNGNOEN

A THEMATIC PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ENGINEERING (COMPUTER ENGINEERING)
FACULTY OF GRADUATE STUDIES
MAHIDOL UNIVERSITY
2015

Thematic Paper
entitled

A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM

……..

Mr. Surapol Ruaysungnoen
Candidate

……..

Asst. Prof. Suratose Tritilanunt,
Ph.D. (Information Technology)
Major advisor

……..

Asst. Prof. Konglit Hunchangsith,
Ph.D. (Information Technology)
Co- advisor

……..

Lect. Noppadol Wanichworanant,
Ph.D. (Electrical Engineering)
Co- advisor

……..

Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

……..

Assoc. Prof. Rangsipan Marukatat,
Ph.D. (Computer Science)
Program Director
Master of Engineering Program in
Computer Engineering
Faculty of Engineering
Mahidol University

Thematic Paper
entitled

A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM

was submitted to the Faculty of Graduate Studies, Mahidol University
for the degree of Master of Engineering
(Computer Engineering)
on
May 22, 2015

……..
Mr. Surapol Ruaysungnoen
Candidate

……..
Lect. Narit Hnoohom,
Ph.D. (Computer Engineering)
Chair

……..
Asst. Prof. Suratose Tritilanunt,
Ph.D. (Information Technology)
Member

……..
Asst. Prof. Konglit Hunchangsith,
Ph.D. (Information Technology)
Member

……..
Asst. Prof. Supakorn Kungpisdan,
Ph.D. (Computer Science and Software Engineering)
Member

……..
Lect. Noppadol Wanichworanant,
Ph.D. (Electrical Engineering)
Member

……..
Prof. Patcharee Lertrit,
M.D., Ph.D. (Biochemistry)
Dean
Faculty of Graduate Studies
Mahidol University

……..
Lect. Worawit Israngkul,
M.S. (Technical Management)
Dean
Faculty of Engineering
Mahidol University

ACKNOWLEDGEMENTS

First of all, I would like to express my sincere gratitude and appreciation to major advisor Asst. Prof. Suratose Tritilanunt , and co-advisor Lect. Noppadol Wanichworanant, Asst. Prof. Konglit Hunchangsith, for their valuable advice guidance, kindness support, good attention, encouragement and improving this research

My special thanks are sincerely to Lect. Narit Hnoohom, committee chair and Asst. Prof. Supakorn Kungpisdan, the external examiner of thesis defense for their kindness, attentiveness and time sacrifice for this research.

I am grateful to Executives, Chief of Information Security, System administrators, and all officials from hospitals case, which involved in this research for providing information, suggestion and nice cooperation.

I would like to thank all the lectures and staff of Computer Engineering Program, Faculty of Engineering, Mahidol University for their knowledge and kindness support.

Finally, I desire to express my deeply to my family and my friends for kindness support, encouragement, and understanding, these inspire me to success in my life.

Surapol Ruaysungnoen

A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM

SURAPOL RUAYSUNGNOEN 5537199 EGCO/M

M.Eng. (COMPUTER ENGINEERING)

THEMATIC PAPER ADVISORY: SURATOSE TRITILANUNT, Ph.D., NOPPADOL WANICHWORANANT, Ph.D., KONGLIT HUNCHANGSITH, Ph.D.

ABSTRACT

The purpose of this study is to propose a security risk analysis process for an IT security system at a hospital. The thesis uses computer security tools to support risk evaluation process. These tools were developed based on the study of standard and best practices of security risk assessment programs used in information system. Moreover, the security assessment was performed using a penetration testing technique that included key processes such as Risk Assessment and Vulnerability Verification along with others factors for supporting this researcher's risk analyzing process and computer security tool development.

The process of risk assessment proposed in this thesis was divided into 4 steps: (1) Planning, (2) Analyzing, (3) Developing, and (4) Utilizing. Results from the experiment showed by inputting the outcome from the vulnerability scan and adjusting the scale of business impact of sample hospitals, the tool was able to assess and rate the security risk which reflected the environment of the hospital's information system. Moreover, this tool was able to simulate some examples of exploitation in order to explore and show system flaws and then generate a report to be used as a reference.

KEY WORDS: SECURITY RISK ASSESSMENT / HOSPITAL SECURITY ASSESSMENT/ SECURITY ASSESSMENT TOOL

155 pages

ต้นแบบเครื่องมือสำหรับการประเมินความมั่นคงปลอดภัยและความเสี่ยงในระบบสารสนเทศโรงพยาบาล (A PROTOTYPE TOOL FOR SECURITY AND RISK ASSESSMENT IN HOSPITAL IT SYSTEM)

สุรพล รวยสูงเนิน 5537199 EGCO/M

วศ.ม.(วิศวกรรมคอมพิวเตอร์)

คณะกรรมการที่ปรึกษาสารนิพนธ์: สุรทศ ไตรติลานันท์, Ph.D.,นภดล วณิชวรนันท์, Ph.D., คงฤทธิ์ หันจางสิทธิ์, Ph.D.

บทคัดย่อ

สารนิพนธ์ฉบับนี้นำเสนอการวิเคราะห์ความเสี่ยงความมั่นคงสารสนเทศสำหรับระบบความมั่นคงปลอดภัยสารสนเทศโรงพยาบาล โดยการทดลองใช้ต้นแบบเครื่องมือช่วยสนับสนุนการประเมินระดับความมั่นคงสารสนเทศที่ถูกพัฒนาขึ้นจากการศึกษาวิเคราะห์แนวปฏิบัติและมาตรฐานที่เกี่ยวข้องกับการ ประเมินความเสี่ยงสารสนเทศ และการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินหาช่องโหว่ โดยเลือกขั้นตอนที่สำคัญและพัฒนาเป็นต้นแบบเครื่องมือเพื่อช่วยสนับสนุนขั้นตอนการประเมินจัดลำดับความสำคัญความเสี่ยง (Risk Assessment) และ การทดสอบยืนยันช่องโหว่ (Vulnerability Verification)

โดยงานวิจัยนี้ได้แบ่งขั้นตอนการดำเนินงานออกเป็น 4 ขั้นตอนคือ (1) การวางแผน (2) การวิเคราะห์ (3) การพัฒนาต้นแบบ และ (4) การทดลองนำไปใช้ จากการทดลองใช้ต้นแบบโดยนำเข้าข้อมูลผลลัพธ์ที่ได้จากการตรวจสอบหาช่องโหว่ (Vulnerability Scan) และปรับเพิ่มระดับผลกระทบทางธุรกิจ (Business Impact) ของโรงพยาบาลที่เป็นกรณีศึกษา พบว่าต้นแบบเครื่องมือสามารถช่วยประเมินจัดลำดับความเสี่ยงที่สะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศโรงพยาบาล และเครื่องมือสามารถจำลองตัวอย่างการทดสอบยืนยัน ค้นหาและแสดงช่องโหว่สาร สนเทศและสามารถสร้างรายงานเพื่อใช้เป็นแหล่งข้อมูลอ้างอิงได้

155 หน้า

CONTENTS

CONTENTS (cont.)

LIST OF TABLES

LIST OF TABLES (cont.)

LIST OF TABLES (cont.)

LIST OF FIGURES

LIST OF FIGURES (cont.)

LIST OF FIGURES (cont.)

LIST OF FIGURES (cont.)

CHAPTER I
INTRODUCTION

1.1 Background and Significance of the Problem

Whether the threats are external or internal, IT Security Threats involving medical information have become a serious modern issue. Of particular interest are the IT threats that cause system, device, hardware or software errors with viruses or professional hackers (Vulnerability). In the medical field, these errors dangerously affect not only patients' lives, but also the quality of services, diagnostic accuracy, patient confidentiality (Privacy) and negative impact on hospital service image as well as the main goals of HA quality assurance processes (Hospital Accreditation) [4]. These goals are as follows: 1) service quality development; 2) appropriate resource management; 3) risk management; 4) good governance and 5) patient rights, etc. A good information technology governance (IT Governance) framework can improve the quality of information technology or HITQIF (Hospital IT Quality Improvement Framework) [5]. Furthermore, the guidelines for the HA standards and international IT standards include SPA (Standards Practice Assessment), JCI (Join Commission International), CoBIT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library) and ISO/IEC 27002, etc. The above frameworks are related to IT Risk Management and Security Assessment.

Therefore, assessing the security of information technology (Security Assessment) is important for hospitals. However, hospitals' shortage of specialists, best practices and supporting tools, has prompted this research aimed at studying the process of Security Assessment. Moreover, best practice also develops support tools and models for Security Assessment and experimental approaches applied to hospitals as case studies in support of decision-making on the improvement of hospital information security systems.

1.2 Research Objectives

1) To conduct a comparative study of guidelines (framework) or system penetration testing standards and risk assessment for information technology to define the guidelines for hospital security assessment.

2) To analyze and select the most important steps in developing a model or function to support hospital security assessment.

3 To develop tools supporting hospital security assessment and experiments with a case study.

1.3 Scope of Work

1) Completion of a comparative study of guidelines (framework) for Information Risk Assessment Standards such as ISMS (Information Security Management System), NIST SP 800-30 (Risk Assessment Methodology Process), HIPPA Risk Assessment Process and OWASP (Risk Rating Methodology).

2) Completion of a comparative study on guidelines (framework) of System Security Testing Standards such as NIST SP800-115 (Technical Guide to Information Security Testing and Assessment), ISSAF (Information Systems Security Assessment Framework), OWASP (Web Application Penetration Testing), PTES (Penetration Testing Execution Standard) and SANS (Penetration Testing Methodology).

3) Analysis and selection of the most important step toward developing a model or function to support Information Security Assessment.

4) Development of supporting tools as a prototype for Information Security Assessment.

5) Experimentation with the prototyping tool to report the results of the Risk Assessment of Information Security Assessment to the hospital as a case study.

1.4 Results

1) Security Assessment Process.

2) Security and Risk Assessment Tool Prototyping.

3) Results of Information Risk Assessment for hospitals as a case study to support the decision of the Director of the hospital's Information Security Administrator.

CHAPTER II
LITERATURE REVIEW

This objectives of this research were to study the conceptual framework in Penetration Testing and IT Security Risk Assessment in technical terms for information systems at hospitals in Thailand. And this chapter addresses the advantages of the adapted research information for implementation. The study is divided into five sub-topics: 1) Health information technology; 2) Health information security; 3) Security risk assessment; 4) Penetration testing and 5) Vulnerability scoring system.

2.1 Health Information Technology

2.1.1 A compilation of Social Security Laws [1] describes "health information" as information related to histories of health care, diagnosis, treatment and any person's insurance payments for health services.

2.1.2 The HITECH Act (Health Information Technology for Economic and Clinical Health) Act [2] describes "health information technology" as hardware, software, integrated technologies, licenses, intellectual property, patches, packaged solutions, maintenance, access or exchange of health care information. The HIT includes systems such as electronic health records (EHRs), personal health records (PHRs), e-prescribing, health information exchange (HIE), analytics and decision support, patient support tools, and mobile health technologies, etc.

2.1.3 Electronic medical records (EMRs) [3] are digital files containing the medical records of healthcare organizations on the healthcare, diagnosis and treatment history of the patients in one practice.

2.1.4 An electronic health record (EHRs) [4, 5] is a secure, real-time, point -of-care, patient-centric information resource for clinicians. The EHR also supports the collection of data for uses other than clinical care such as billing, quality management and reporting.

2.1.5 The conceptual framework of Interoperable Electronic Health Record and E-Prescribing Systems Version 1.0 [6] describes "electronic health records" as a repository of maintained health care information providing services to the multiple users of records. And EHR should include information such as observations, laboratory results, x-rays, treatments, drugs, patient identification information and allergies as shown in Figure 2.1.

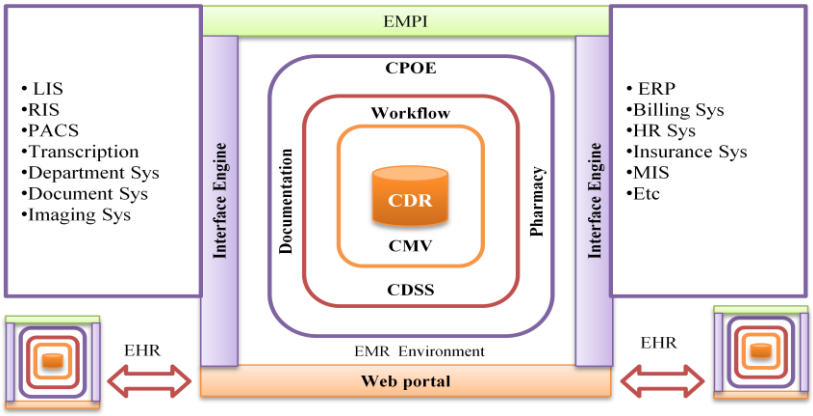


Figure 2.1 EHR Environments [6]

2.1.6 HIPAA Security and Privacy Rules [7] describes "protected health information" (PHI) as protected privacy health care information. The PHI should include information such as personal history, healthcare history, insurance history and other unique identification.

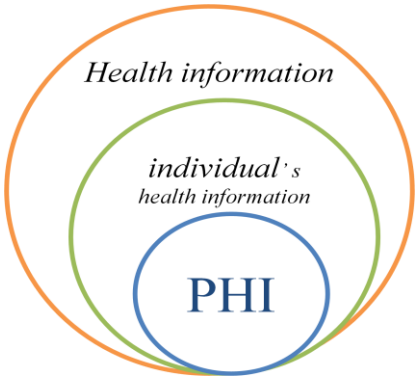


Figure 2.2 Health Information Relations

This research focuses on health information and critical health information systems, hospital information systems (HIS), laboratory information systems (LIS), radiology information systems (RIS), picture archiving and communication systems (PACS).

2.2 Health Information Security

2.2.1 Health Information Security Management Standards (ISO 27799) describe health information security goals [8] as control information confidentiality, availability and integrity. This paper should include authenticity, accountability and audit ability as shown in Figure 2.3.

Figure 2.3 Health Information Security Goals

2.2.2 Hospital IT Quality Improvement Framework (HITQIF) [9, 10] using and Integration Standard of COBIT (Control Objectives for Information and related Technology), ITIL (Information Technology Infrastructure Library), ISO/IEC 27002 (Information Security Standard), SPA (Standard Practice Assessment), and JCI (Joint Commission International) describe the definitions related to information security [4] as follows:

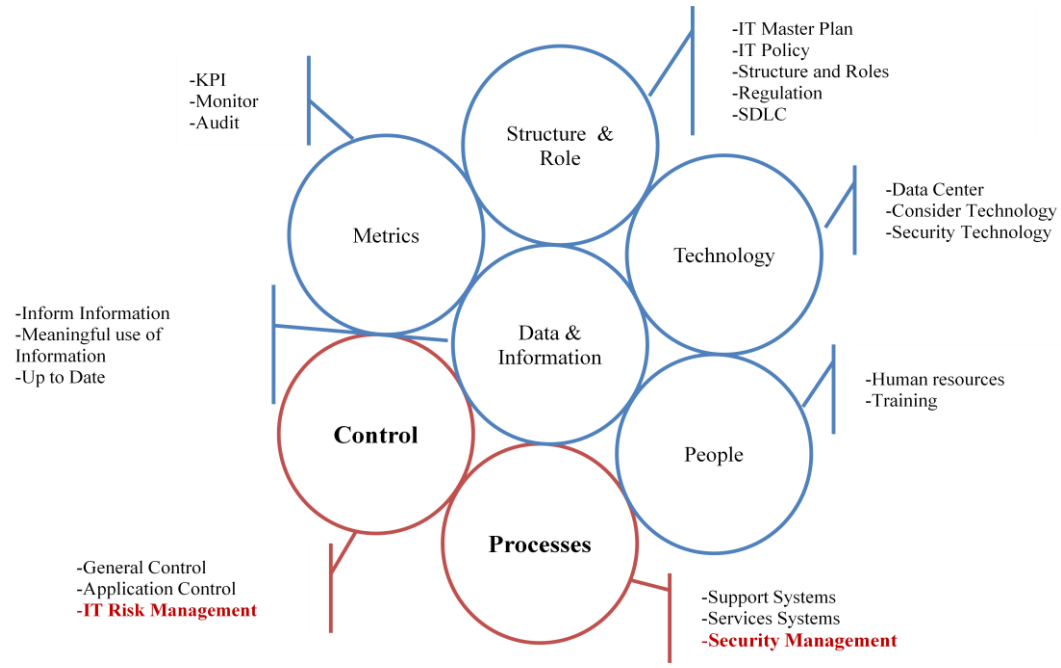


Figure 2.4 HITQIF Framework

1. Security Management is a process to ensure that systems protect all abuse or authorization such as physical security management, asset management, network and security management, etc.

2. IT risk management includes information technology risk management processes such as IT project failure, waste investment, security breaches, system crashes, etc.

2.2.3 ICT Readiness Assessment Model for Small and Medium Organizations in Thailand Public and Private Sectors: This paper presents an ICT readiness assessment model specifically designed to measure the readiness of ICT utilization and penetration levels [11] in small and medium-sized organizations in developing countries.

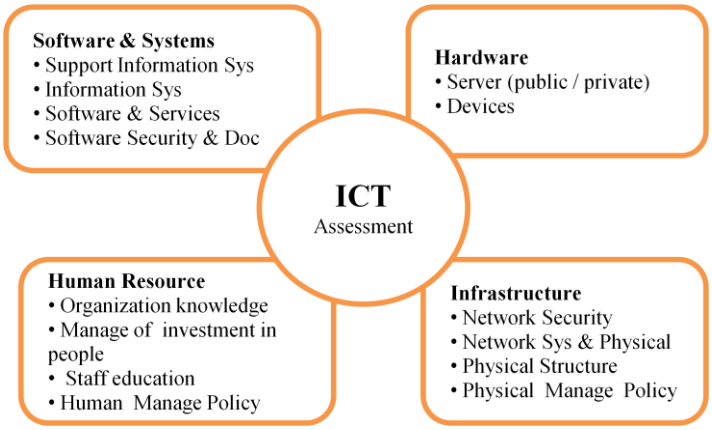


Figure 2.5 ICT Readiness Assessment Models

2.2.4 Risk Management for IT Disruptions in Health Care Settings: A Continuity of the Operations Planning Process [12] describes critical systems for business continuity by dividing into the following two types: 1) Common system communication and 2) Healthcare-specific functions as shown in Table 2.1.

Table 2.1 Critical Systems to business continuity

Type	Critical systems
1.Common system communication	Intranet and Internet
2.Healthcare-specific functions	Electronic Medical Records (EMR) system, Laboratory information system (LIS), Radiology information system (RIS), Picture archiving and communication system (PACS)

2.3 Security Risk Assessment

Security risk assessment is risk level evaluation process divided into the following four levels: critical, high, medium and low. The guidelines commonly used for the security risk assessment studies include the following: 1) Information Security Management System (ISMS); 2) National Institute of Standards and Technology (NIST): SP 800-30 Risk Management Guide for Information Technology Systems; 3) Open Web Application Security Project (OWASP): Risk Rating Methodology and 4) Health Insurance Portability and Accountability Act (HIPAA): Risk Assessment Processes.

2.3.1 For risk analysis and security management of IT information in hospitals [13], [14], this paper proposes techniques for applying the risk assessment framework of the information systems of hospitals in Thailand by using the framework proposed by the research. The hospital's IT administrators can manually collect and evaluate any IT system vulnerability and risks by themselves. The risk assessment framework consists of the following six steps: 1) information gathering; 2) current capacity to control vulnerability; 3) number of threat occurrences from the past; 4) evaluation of threat likelihood; 5) threat impact assessment and 6) risk evaluation and determination. This paper describes the method of attacks by dividing the aforementioned into the following ten types: 1) Code execution; 2) Buffer overflows; 3) Elevation of privilege; 4) Denial of service; 5) Man in the middle; 6) Cross site scripting; 7) Brute force; 8) Authentication bypass; 9) SQL Injection and 10) Information gathering as shown in Table 2.2.

Table 2.2 Method of Attack

Method of Attack	Descriptions
Code Execution	The attacker can send malicious commands through operating system's vulnerability ,so an attacker can tack control the server, including install, view or edit the information and create an account on the server.
Buffer overflows	The inputs or greater than the extent to which the program is backed up. As a result, the Server or system can be stopped.
Elevation of Privilege	Edit their information in order to obtain equivalent administrator right. As a result, an attacker can access the data within the system.
Denial of service (DoS)	To prevent or disrupt a system, the Server or system can be stopped.
Man in the middle	Eavesdrop or intercept information the conversation of sender and receiver.
Cross site scripting (XSS)	Bury script in web browser for intercept target's information
Brute force	Decrypt password for access to server or system.
Authentication bypass	Pass the system's vulnerability without having to go through identity verification.
SQL Injection	SQL Query String attack in showing needs information.
Information Gathering	Gather the required system information.

2.3.2 Information Security Management System (ISMS) proposes approaching risk assessment process by dividing into the following nine steps [15]: 1) Identify major assets; 2) Assess asset value in terms; 3) Identify threats; 4) Identify vulnerabilities; 5) Identify measures of risk; 6) Security requirements; 7) Security controls; 8) Minimize risks and 9) Risk acceptance as shown in Figure 2.6.

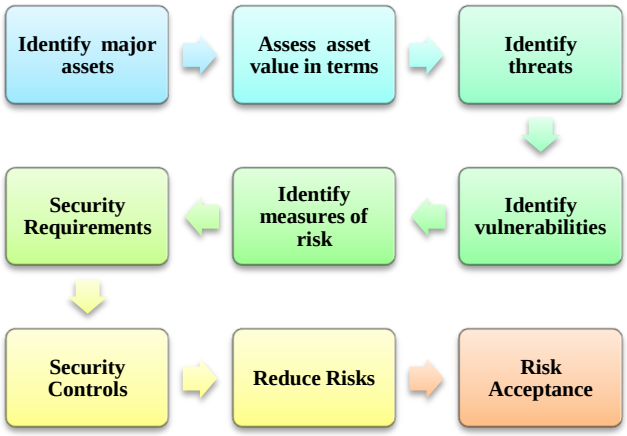


Figure 2.6 ISMS: Risk Assessment Process

2.3.3 National Institute of Standards and Technology (NIST) proposes approaching the risk assessment process in the SP800-30 document by dividing into the following nine steps [16]: 1) System characterization; 2) Threat identification; 3) Vulnerability identification; 4) Control analysis; 5) Likelihood determination; 6) Impact analysis; 7) Risk determination; 8) Control recommendations and 9) Results documentation as shown in Figure 2.7.

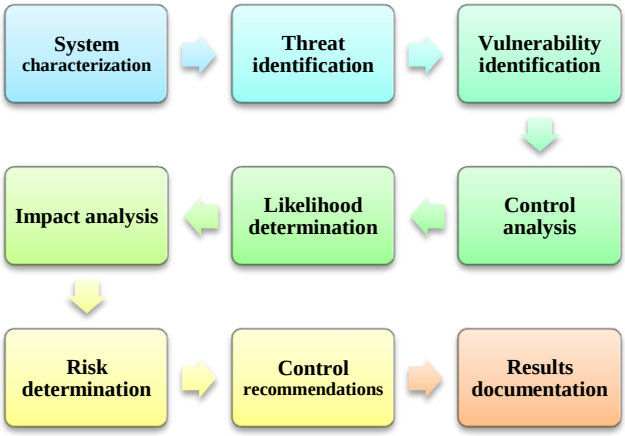


Figure 2.7 NIST SP 800-30: Risk Assessment Methodology Process

2.3.4 Open Web Application Security Project (OWASP) Testing Guide proposed approaching the risk rating process by dividing into the following six steps [17]: 1) Identifying risks; 2) Estimating likelihood; 3) Estimating impact; 4) Determining risk severity; 5) Deciding what to fix and 6) Customizing your risk rating model as shown in Figure 2.8.

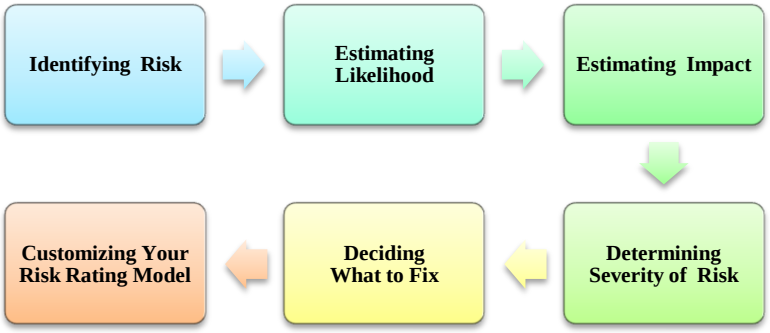


Figure 2.8 OWASP: Risk Rating Methodology

2.3.5 The Health Insurance Portability and Accountability Act (HIPAA) Security Management Process proposed approaching the risk assessment process by dividing into the following seven steps [18]: 1) Determining system characterization; 2) Stating the system mission; 3) Identifying any vulnerability or weakness in security procedures or safeguards; 4) Identifying impact; 5) Recommending security controls; 6) Determining residual risks and 7) Documenting all output as shown in Figure 2.9.

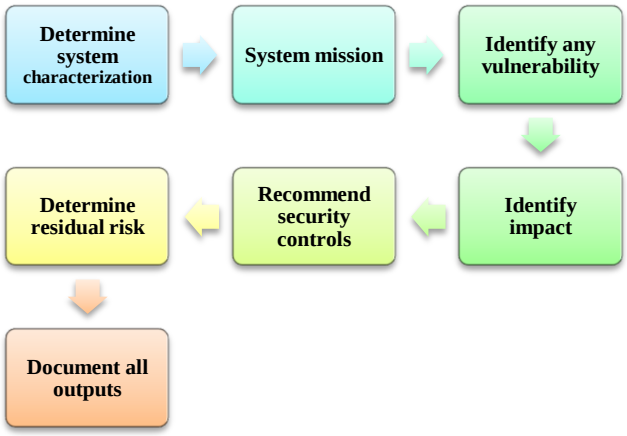


Figure 2.9 HIPPA Risk Assessment Processes

2.4 Penetration testing

Penetration testing is a method of security assessment for security vulnerability attack testing and assessment. Penetration testing is divided into the following two types [19]: 1) External testing and 2) Internal testing as shown in Table 2.3.

Table 2.3 Type of Penetration test

Type	Details
1. External testing	focused on the servers, infrastructure, and the underlying software to the target divided 2 methods as 1) Black box and 2) White box
2.Internal testing	considered to be a more versatile view of the security and performed from several network access points, including both logical and physical segments divide 5 methods as 1) Black box , 2) Gay box, 3) White box, 4) Announced test and 5) Unannounced test

Table 2.3 Type of Penetration test (Cont.)

Methods	Details
1.Black box	without having any prior knowledge the target. To simulate real-world attacks and minimize false positives
2.Gay box	limited knowledge about infrastructure, a defense mechanism, and communication channels of the target on which test is to be conducted.
3.White box	full knowledge of infrastructure, a defense mechanism, and communication channels of the target on which test is being conducted.
4.Announced test	An attempt to gain access or compromise systems on the client network with the full cooperation and knowledge of the IT staff.
5.Unannounced test	An attempt to gain access or compromise systems on network with the awareness of only the upper levels of management.

The study guidelines commonly used for security assessment include the following: 1) National Institute of Standards and Technology (NIST): SP800-115; 2) Information Systems Security Assessment Framework (ISSAF) draft 0.2.1B; 3) Open Web Application Security Project (OWASP): OWASP Testing Framework; 4) Penetration Testing Execution Standard (PTES) and 5) Sys-Admin Audit Networking and Security (SANS).

2.4.1 The National Institute of Standards and Technology (NIST) [20] proposed approaching the penetration testing process by dividing into the following four steps: 1) Planning; 2) Discovery; 3) Attack and 4) Report as shown in Figure 2.10.

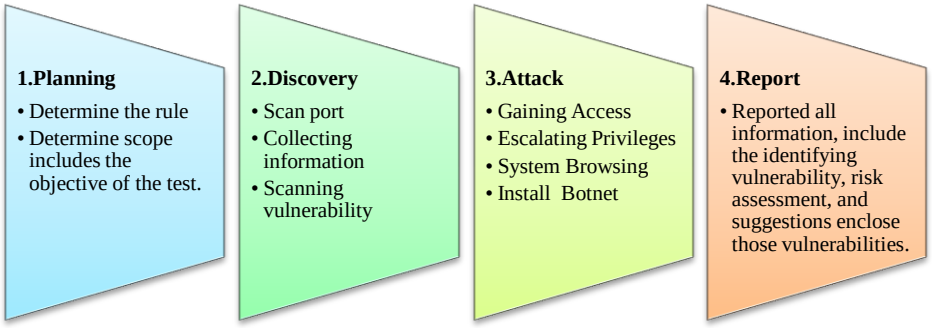


Figure 2.10 Phases Penetration Testing Methodology

2.4.2 The *Open Information Systems Security Group* (OISSG) [21] proposed approaching the security assessment process by dividing into the following three steps: 1) Planning and Preparation; 2) Assessment and 3) Report, Clean up and Destroy Artifacts as shown in Figure 2.11

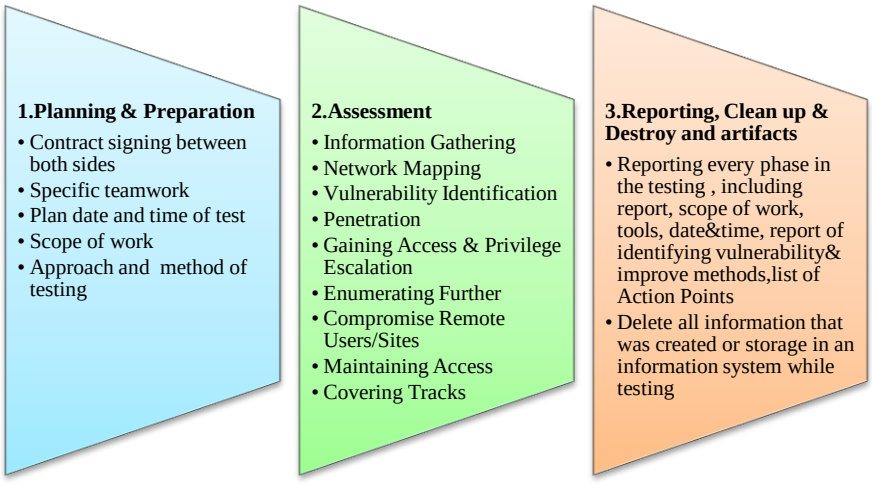


Figure 2.11 Approach & Methodology

2.4.3 The Open Web Application Security Project (OWASP) [17] proposed approaching the web application penetration process by dividing the following two modes: 1) Passive mode and 2) Active mode as shown in Figure 2.12.

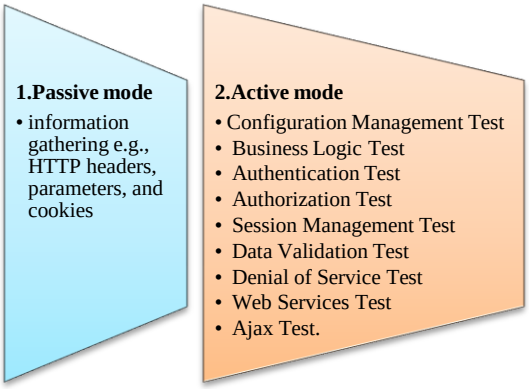


Figure 2.12 OWASP Testing Framework

2.4.4 The Penetration Testing Execution Standard (PTES) [22] proposed approaching the penetration test process by dividing into the following five steps: 1) Intelligence Gathering; 2) Vulnerability Analysis; 3) Exploitation; 4) Post Exploitation and 5) Reporting as shown in Figure 2.13.

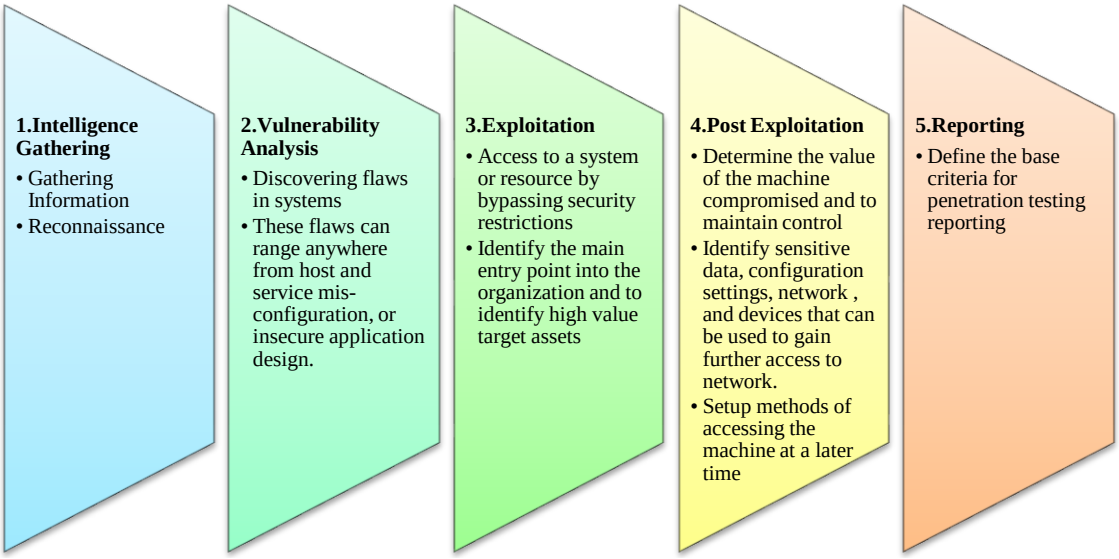


Figure 2.13 PTES Penetration test process

2.4.5 Sys-Admin Audit Networking and Security (SANS) [23] proposed approaching the penetration test process by dividing in to the following six steps: 1) Planning and Preparation; 2) Information Gathering and Analysis; 3) Vulnerability Detection; 4) Penetration Attempt; 5) Analysis and Reporting and 6) Cleaning Up as shown in Figure 2.14

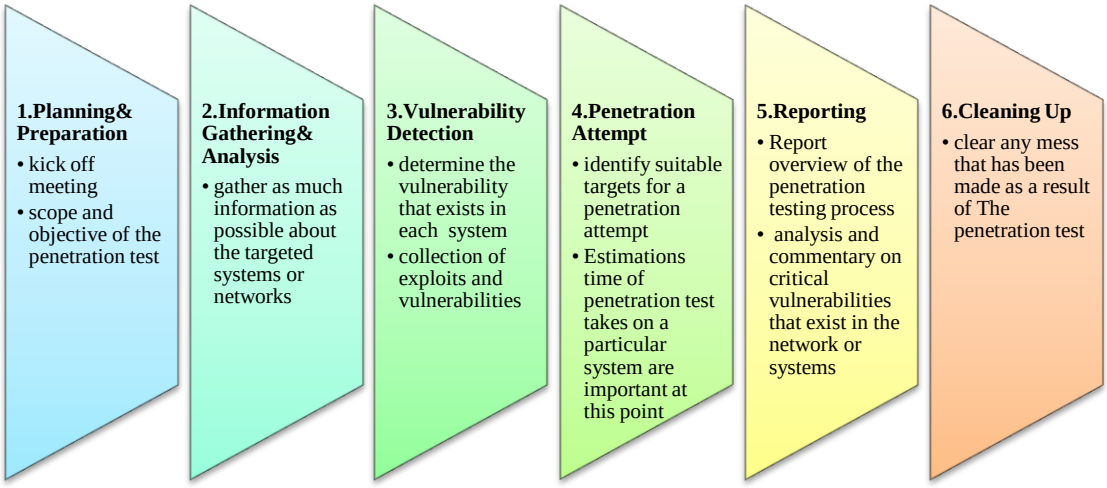


Figure 2.14 SANS Penetration test Process

2.5. Vulnerability Scoring System

This topic discusses the Common Vulnerability Scoring System (CVSS) and Tools supporting CVSS standards.

2.5.1 The Common Vulnerability Scoring System (CVSS) [24] is a vulnerability scoring system designed to provide a standard method for rating IT vulnerabilities. A CVSS base score can help prioritize security vulnerabilities. The CVSS v2 base score has been adopted as the primary method for quantifying the severity of recognized vulnerabilities including the following:

- The Open Source Vulnerability Database (OSVDB) [25] is an independent and open-source database created by and for the community. The paper provides accurate, detailed, current and unbiased technical information on security vulnerabilities.
- The Common Vulnerabilities and Exposures (CVE) [26] is a list of information security vulnerabilities and exposures aimed at providing common names for publicly known problems.

2.5.2 A Complete Guide to the Common Vulnerability Scoring System Version 2.0 [27] describes the CVSS base group as a means of defining and communicating the fundamental characteristics of vulnerability. The CVSS base metrics are assigned values in which the base equation calculates a score ranging from 0 to 10, and creates the following vector: "CVSS2#AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/ I:[N,P,C]/ A:[N,P,C]" as shown in Figure 2.15.

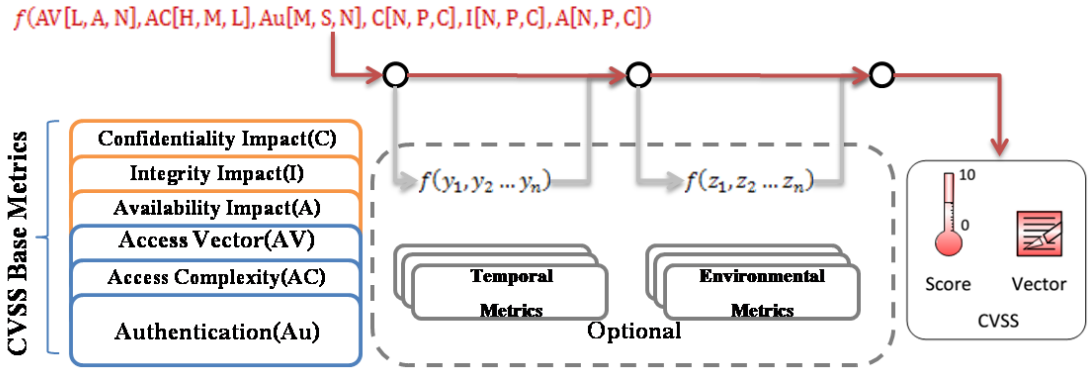


Figure 2.15 CVSS Base Metrics [27]

The base equation is the foundation of CVSS scoring v2 [27]. The base equation as shown below.

BaseScore= round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)–1.5)*f(Impact)) (1)

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact)) (2)

Exploitability = 20* Access Vector*Access Complexity*Authentication (3)

f(impact)= 0 if Impact=0, 1.176 otherwise

BaseVector: AV:[L,A,N] / AC:[H,M,L] / Au:[M,S,N] / :[N,P,C]/I:[N,P,C]/A:[N,P,C]

Table 2.4 CVSS Case of Base Metric

Base Metric	Case of Metric	Value
AccessVector	L: requires local access	0.395
	A: adjacent network accessible	0.646
	N: network accessible	1.000
AccessComplexity	H: high	0.350
	M: medium	0.610
	L: low	0.710
Authentication	M: requires multiple instances of authentication	0.450
	S: requires single instance of authentication	0.560
	N: requires no authentication	0.704
ConfidentialityImpact	N: none	0.000
IntegrityImpact	P: partial	0.275
AvailabilityImpact	C: complete	0.660

2.5.3 The Information Assurance Tools Report – Vulnerability Assessment, Sixth Edition [28] describes vulnerability assessment tools by dividing into the following seven types: 1) Network Scanners; 2) Host Scanners; 3) Database Scanners; 4) Web Application Scanners; 5) Multilevel Scanners; 6) Automated Penetration Test Tools and 7) Vulnerability Scan Consolidators as shown in Table 2.5.

Table 2.5 Vulnerability Assessment Tools Characteristic

Type	Tool	Target	License	Standards
Network Scanner	eEye Retina	Network, OS, Web App/Services, DB	Commercial	SCAP, OVAL, CVE, CVSS
	GFI LANguard	UNIX, Windows	Commercial/Free ware	OVAL, CVE
	Safety-Lab Shadow Security Scanner	Network host running, UNIX, Linux, Solaris, Windows	Commercial	NA
Host Scanner	Assuria Auditor / Auditor RA	Windows, UNIX, Linux	Shareware	CVE, CVSS
	NileSOFT Secuguard SSE		Commercial	CVE
	Proland Protector Plus	NA	Freeware	NA
DB Scanner	Imperva Scuba	Oracle, DB2, SQL Server, Sybase	Freeware	NA
	Safety-Lab Shadow	Oracle, DB2, SQL Server, Sybase, MySQL, SAP DB, Lotus	Commercial	
	DBAPPSecurity MatriXay	Oracle, DB2, SQL Server, Access		
Web Application Scanner	Acunetix	NA	Commercial	NA
	Burp Suite			
	Nikto	HTTP/HTTPS, Web Server	Open Source	
Multi Scanner	Open VAS	Network, Web App	Open Source	NA
	Symantec Risk Automation suite	Network devices, host Oss, DB, network app	Commercial	SCAP, OVAL, CVE, CVSS
	Nessus	Network, Windows, Unix, Linux, SQL DB, Web server	Commercial/Free ware	CVE,CVSS
Automated Penetration Test Tools	Arachni	Web app	Open Source	NA
	CANVAS	All common platform and app	Commercial	
	Metasploit	Web app, Network, DB Server		CVE
Vulnerability Scan Consolidators	Prolific Solutions pro VM Auditor	NA	Commercial	NA
	ASG			SCAP, OVAL, CVE, CVSS
	Skybox Risk Control	Systems, devices		CVE

2.5.4 AN OVERVIEW OF PENETRATION TESTING [29] describes penetration tools as shown in Table 2.6 -2.7.

Table 2.6 Penetration Testing Tools

Tool	Specific Purpose	License	Portability
Nmap	network scanning , port scanning, OS detection	free	Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga
Hping	port scanning , remote OS fingerprinting	free	Linux, FreeBSD, NetBSD, OpenBSD, Solaris, Mac OS X, Windows
SuperScan	• detect open TCP/UDP ports determine services are running • run queries like whois, ping, and hostname lookups	free	Windows 2000/XP/Vista/
Xprobe2	remote active OS, fingerprinting, TCP fingerprinting, port scanning	free	Linux
p0f	OS fingerprint, firewall detection	free	Linux, FreeBSD, NetBSD, OpenBSD, Mac OS X, Solaris, AIX, Windows
Httprint	web server fingerprint, detect web enabled devices, SSL detection	free	Linux, Mac OS X, FreeBSD, Win32 (command line and GUI)
Nessus	detect vulnerabilities , detect misconfiguration, default password, and denial of service	free trial version	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple
Shadow Security Scanner	detect network vulnerabilities, audit proxy and LDAP servers	free trial version	Windows but scan servers built on any platform
Iss Scanner	• detect network vulnerabilities	free trial version	Windows 2000 Professional with SP4, Windows Server 2003 Standard with SO1, XP Professional with SP1a
GFI LANguard	• detect network vulnerabilities	free trial version	Windows Server 2003/2008, 2000 Professional, 7 Ultimate/ Vista Business/XP Professional/Small Business Sever 2000/2003/2008
Brutus	• Telnet, ftp, and http password cracker	free	Windows 9x/NT/2000
Metasploit Framework	• develop and execute exploit code against a remote target • test vulnerability of computer systems	free	All versions of Unix and Windows

Table 2.7 Web Penetration Testing Tools

Tool	Specific Purpose	License	Portability
Nmap	Find web server	Free	Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga
Fiddler	A web debugging proxy	Free	Windows XP / 2K3 / Vista / 2K8 / Win7 / Win8 Microsoft .NET Frameworkv2.0or later
Nikto	Identifies web server type, version, add-on and other interesting files, performs quick analysis of web server and applications and reports back common server and software misconfigurations, default files and programs, insecure files and programs and outdated servers and programs	Open source	Windows, Mac OSX, Linux and Unix (including RedHat, Solaris, Debian, Knoppix, etc)
WebScarab	Interceptor, identifies new URLs on the test target, session ID analyzer, parameter fuzzer	Free	All platforms that support Java in any version not older than 1.4
w3af	Vulnerability tester, interceptor, fuzzer	Open source	Linux, Windows XP, Windows Vista, Open BSD and any platforms that support Python
Firefox Extension – Firebug	Inline editing, for breaking forms, messing with JavaScript, making rougue sites and man-in-the-middle components	Free	Any platforms that supports Firefox
Firefox Extension – TestGen4Web	Record and playback clicks during surfing	Free	Any platforms that support Firefox 1.5 beta
Cenzic Hailstorm	Web vulnerability scanner	1-week trial free	Windows 7 Pro or XP Professional with Service Pack 3
Core Impact	Identify, validate and exploit vulnerabilities, test web application for XSS, Reflective XSS, SQL Injection, Blind SQL Injection, Remote File Inclusion for PHP application	Commercial	Windows 7, Windows Vista, Windows Server 2008 SP2, Windows Server 2003 SP2
Nessus 4	Detect vulnerabilities that allow remote cracker to control or access sensitive data, misconfiguration, default password, and denial of service	Free for personal edition nonenterprise edition	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple
Metasploit Framework	Develop and execute exploit code against a remote target machine, test vulnerability of computer systems	Free	All versions of Unix and Windows

This research used the Nessus and Nikto vulnerability scanners that support CVSS standards and free licensing to vulnerability result assessment in hospitals including the use of Metasploit to exploit sample testing for vulnerabilities.

1. Nessus [30] is a vulnerability scanner tool that performs vulnerability scanning, analysis, compliance checking, asset discovery, configuration auditing and sensitive data discovery.

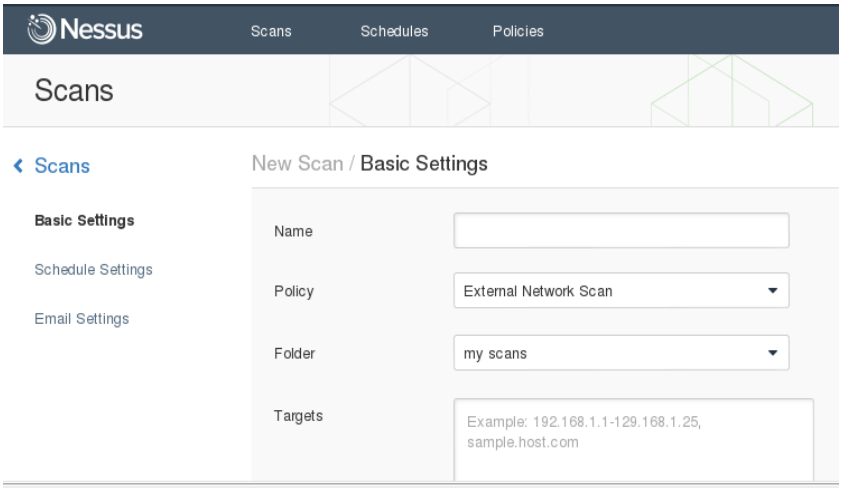


Figure 2.16 Nessus Scan Menu

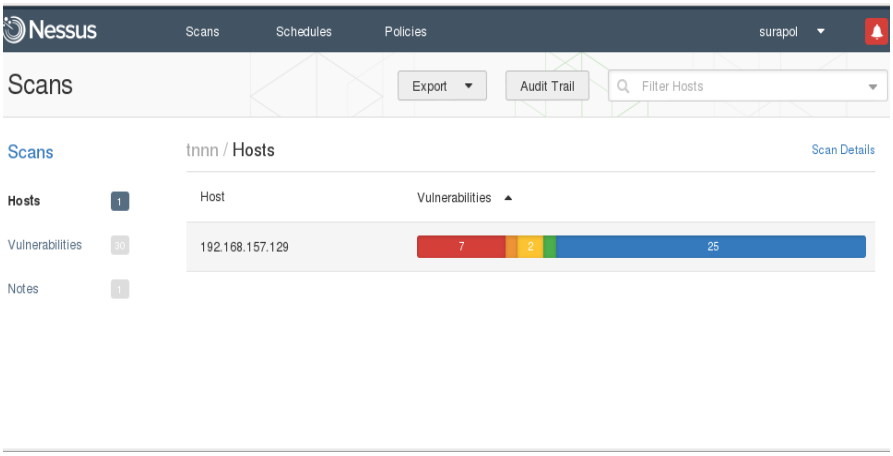


Figure 2.17 Nessus Scan Results

2. Nikto[31] is web application vulnerability scanner tool that tests for dangerous programs, dangerous files, CGI scripts, default files, outdated versions and software mis-configurations, including injection, XSS, file upload, remote file retrieval, remote shell, authentication bypass and denial of service, etc.

```
root@kali:~# nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

       Note: This is the short help output. Use -H for full help text.
```

Figure 2.18 Command Nikto

```
nikto –host http://localhost/WebGoat/attack OR
nikto –host www.google.com OR
nikto –host 127.0.0.1
```

Figure 2.19 Command Nikto Scan

```
+ Target IP:          XXXXXXXXXX
+ Target Hostname:    XXXXXXXXXX
+ Target Port:        80
+ Start Time:         2014-07-29 23:36:34
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ Retrieved x-powered-by header: Servlet 2.4; JBoss-4.0.2 (build: CVSTag=JBoss_4_0_2 date=200505022023)/Tomcat-5.5
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ETag header found on server, fields: 0xW/1437 0x1115040374000
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-3092: /status?full=true: Apache Tomcat and/or JBoss information page.
+ 6448 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2014-07-29 23:36:56 (22 seconds)
```

Figure 2.20 Nikto Scan Result

3. Metasploit [32] is a platform for writing, testing and using exploit code that performs penetration testing and shell code development. Either the command line interface (msfcli) is used to exploit in general, or the auxiliary module is used to exploit vulnerability.

```
root@kali:~# msfcli -h
[!] ****************************************************************************
[!] *               The utility msfcli is deprecated!                          *
[!] *            It will be removed on or about 2015-06-18                     *
[!] *              Please use msfconsole -r or -x instead                      *
[!] *  Details: https://github.com/rapid7/metasploit-framework/pull/3802       *
[!] ****************************************************************************
Usage: /opt/metasploit/apps/pro/msf3/msfcli <exploit_name> <option=value> [mode]
================================================================================

    Mode           Description
    ----           -----------
    (A)dvanced     Show available advanced options for this module
    (AC)tions      Show available actions for this module
    (C)heck        Run the check routine of the selected module
    (E)xecute      Execute the selected module
    (H)elp         You're looking at it baby!
    (I)DS Evasion  Show available ids evasion options for this module
    (M)issing      Show empty required options for this module
    (O)ptions      Show available options for this module
    (P)ayloads     Show available payloads for this module
    (S)ummary      Show information about this module
    (T)argets      Show available targets for this exploit module

Examples:
msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=IP E
msfcli auxiliary/scanner/http/http_version rhosts=IP encoder= post= nop= E
```

Figure 2.21 msfcli command

CHAPTER III
RESEARCH METHODOLOGY

The purpose of this chapter is to explain the process of security assessment and prototype tools development to support security assessment for hospital information technology security with the following four phases as shown in Figure 3.1.

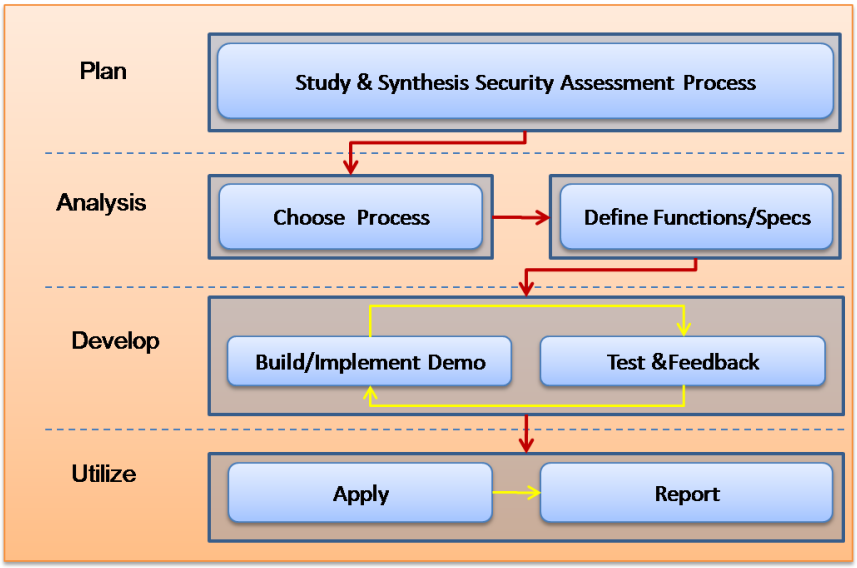


Figure 3.1 develop prototype tools process

3.1 Plan Phase

This procedure is concerned with the penetration testing and risk assessment processes based on the guidelines and standards aimed at finding a suitable process for security assessment in technical terms. The suitable process includes security assessment and develop prototype tools to support security assessment by using the penetration testing method and evaluating vulnerability ratings by using a risk assessment method in technical terms for security risks, namely, identifying vulnerabilities in servers that are not patched and exploiting them.

This process can be divided into the following two parts: 1) Educational standards and guidelines on penetration testing and risk assessment and 2) Synthesis of security assessment processes.

3.1.1 Educational Standards for Penetration Testing and Risk Assessment - This part discusses the educational standards and guidelines involved with penetration testing. The standards to be used in this application are NIST SP800-115, ISSAF, SANS, PTES and OWASP. Furthermore, the risk assessment standards for use in this application are ISMS, NIST SP800-30, OWASP and HIPPA.

3.1.2 Synthesis Security Assessment Process – This process is defined and classified as a process for finding the key processes of security assessment by dividing into the following four processes: 1) Planning; 2) Assessment; 3) Verification and 4) Reporting as shown in Figure 3.2.

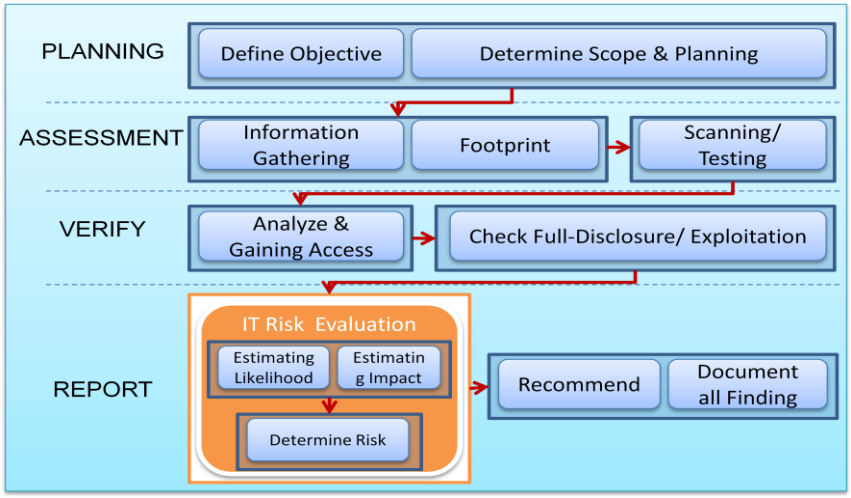


Figure 3.2 Security Assessment Process

Process 1 (Planning) is planning and determining the rules, scope and objectives of security assessment processes by dividing into the following two processes: 1) Defining Objectives and 2) Setting the Scope and Planning.

Process 2 (Assessment) is collecting an information system and testing for the vulnerability of vulnerability assessment by dividing into the following two processes: 1) Information and Footprint Gathering and 2) Scanning and Testing.

Process 3 (Verification) is testing and confirmation of vulnerabilities by dividing into the following two processes: 1) Analyze and Gain Access and 2) Check for Full Disclosure/Exploitation.

Process 4 (Reporting) is collecting and summarizing all information on security assessment processes by dividing into the following two phases: 1) IT Risk Evaluation and 2) Documentation and Recommendations.

3.2 Analysis Phase

3.2.1 Selecting a Process is the step for choosing a key process for developing prototype functions to support security assessment for Hospital IT Security including process planning with assessment, verification and reporting processes.

1) Planning involves strategizing and determining the rules, scope and objectives of a security assessment process by dividing into the following two steps: Defining Objectives and Setting the Scope/Planning.

1.1 Defining Objectives/Setting the Scope involves planning and setting the scope of a security assessment process by dividing into the following two steps: a) Interview/Questions b) Identification of Assets/Systems:

a. Interview/Questions is a step involving study and collection of data and information by searching the Internet for information about hospitals and using the questionnaire forms shown in Tables 3.1 and 3.2.

Table 3.1 Google Advance Search Operation

[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to a specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain
[allintitle:]	Restricts the results to those websites with all of the search keywords in the tit
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those with all of the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL

Table 3.2 Example Questionnaire Form

No	*Questions*	*Yes*	*No*	*Comments*
1	Do you have any security-related policies and standards?			
2	If so, do you want us to review them?			
3	What is the network layout (segments, DMZs, IDS, IPS, etc.)?			
4	If the client organization requires analysis of its Internet presence?			
5	If the organization requires pen testing of individual hosts?			
6	What security controls are deployed across the organization?			
7	If the organization requires assessment of wireless networks?			
8	If the organization deploys a mobile workforce? If so, if the mobile security assessment is required?			
9	What are the web application and services offered by the client?			

b. Identification of Assets/Systems is the step accomplished by using the target selection form in Table 3.3.

Table 3.3 Select Target Form

No	Select	Asset/Systems Target	Impact Factor Rating				Impact Rating (Average)	Comments
			Financial damage	Reputation damage	Non-compliance	Privacy violation		
1	☐							
2	☐							
3	☐							
4	☐							
5	☐							

1. Selection of a target for the vulnerability assessment process
2. Asset/Systems Target identifies assets/systems
3. Impact Factor - Value from Estimating Impact Factor Rating

Follow Table 3.4

Table 3.4 OWASP Impact Rating

	Rating	0	1	2	3	4	5	6	7	8	9
Impact Factors	Financial damage		Less than the cost to fix the vulnerability		Minor effect on annual profit				Significant effect on annual profit		Bankruptcy
	Reputation damage		Minimal damage			Loss of major accounts	Loss of goodwill				Brand damage
	Non-compliance			Minor violation			Clear violation		High profile violation		
	Privacy violation				One individual		Hundreds of people		Thousands of people		Millions of people

4. Impact Rating - The value of the average Impact Factor Rating
5. Comments

2) Assessment is an information system assessment of objectives for identifying the vulnerability occurrence in the information system, including Information/Footprint Gathering and Scanning/Testing.

2.1 Information/Footprint Gathering is the step involving the collection of necessary data on the security assessment process by dividing into the following two steps: a) Information gathering b) Footprint gathering:

a. Information gathering is the step involving a review of documents and collection of data on information systems by using the Data Collection Target Form in Table 3.5.

Table 3.5 Collection Data Target Form

No	Name_Service	Server	IP_Address	Other
EX	HIS (Hospital Information Systems)	AppServ	xxx.xx.xx.xxx	-
1				
2				
3				
4				
5				

b. Footprints are discovered to find information about a domain name, server name, IP address, network map, system and service by using the reconnaissance tools in Table 3.6.

Table 3.6 Tools for Information Gathering

Tools /Command	Details
1.Nbtstat Command	Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).
2.NBTEnum	Displays userlists, machine lists, sharelists, namelists, group and member lists, password and LSA policy information.
3.Nslookup Command	Querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.
4.Dig (domain information groper)	Querying Domain Name System (DNS) name servers.
5.Whois	Displays domain names, registrars and name servers.
6.NMAP (Network Mapper)	Discover hosts and services on a computer network, Enumerating the open ports on target hosts. Determining the operating system and hardware characteristics of network devices.
7.Nikto	Checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

- Nbtstat [33] is an MS-DOS Command of displayed lists and remote name tables, NBT remote names, Cache look-ups, NetBIOS names and session tables, etc.

Table 3.7 Nbtstat commands

-a	(adapter status) Lists the remote machine's name table given its name
-A	(Adapter status) Lists the remote machine's name table given its IP address.
-c	(cache) Lists NBT's cache of remote [machine] names and their IP addresses
-n	(names) Lists local NetBIOS names.
-r	(resolved) Lists names resolved by broadcast and via WINS
-R	(Reload) Purges and reloads the remote cache name table
-S	(Sessions) Lists sessions table with the destination IP addresses
-s	(sessions) Lists sessions table converting destination IP addresses to computer NETBIOS names
-RR	(Release Refresh) Sends Name Release packets to WINS and then, starts Refresh

Examples:

nbtstat -A XXX.XXX.XXX.XXX

- NBTEnum [34] is a utility used to display NetBIOS information including account lock-out thresholds, local groups and users, global groups and users, shares, etc.

Table 3.8 NBTEnum commands

-v	(version) Displays version information.
-h	(help) Displays this screen.
-q	(query) Enumerates NetBIOS information on the specified host or range of IP addresses. If a username and password is not specified the utility is run under the context of the null user. If a username and password is specified the utility is run under the context of the given username.
-a	(attack) Enumerates NetBIOS information on the specified host or range of IP addresses and also performs password checking. If a dictionary file is not specified the utility will check each user account for blank passwords and passwords the same as the username in lower case. If a dictionary file is specified the utility will check each user account for blank passwords and passwords the same as the username in lower case and all passwords specified in the dictionary file.
-s	(smart attack) Enumerates NetBIOS information on the specified host or range of IP addresses and performs password checking only if the account lockout threshold on the current host is set to 0. If a dictionary file is not specified the utility will check each user account for blank passwords and passwords the same as the username in lower case. If a dictionary file is specified the utility will check each user account for blank passwords and passwords the same as the username in lower case and all passwords specified in the dictionary file.

Examples:

nbtenum -q XXX.XXX.XXX.XXX test ""

- Nslookup [35] is a program used to display the domain names of servers, various hosts and lists of hosts in a domain as in the syntax below.

Table 3.9 Nslookup commands

host [*server*]	Look up information for host using the current default server, or *server* if specified. If host is an Internet address and the query type is **A** or **PTR**, the name of the host is returned. If host is a name and does not have a trailing period, the search list is used to qualify the name. To look up a host not in the current domain, append a period to the name.
server *domain*, **lserver** *domain*	Change the default server to *domain*; **lserver** uses the initial server to look up information about *domain*, while server uses the current default server. If an authoritative answer can't be found, the names of servers that might have the answer are returned.
exit	Exits the program.
set*keyword*[=*value*]	This command is used to change state information that affects the lookups. Valid keywords are:

all	Prints the current values of the frequently used options to set. Information about the current default server and host is also printed.
class=*value*	Change the query class to one of: *IN: the Internet class* *CH: the Chaos class* *HS: the Hesiod class* *ANY: wildcard* The class specifies the protocol group of the information. (Default = **IN**; abbreviation = **cl**)
[no]debug	Turn on or off the display of the full response packet and any intermediate response packets when searching. (Default = **nodebug**; abbreviation = **[no]deb**)
[no]d2	Turn debugging mode on or off. This displays more about what **nslookup** is doing. (Default = **nod2**)
domain=*name*	Sets the search list to *name*.
[no]search	If the lookup request contains at least one period but doesn't end with a trailing period, append the domain names in the domain search list to the request until an answer is received. (Default = **search**)
port=*value*	Change the default TCP/UDP name server port to *value*. (Default = **53**; abbreviation = **po**)
querytype=*value*, **type**=*value*	Change the type of the information query. (Default = **A**; abbreviations = **q**, **ty**)
[no]recurse	Tell the name server to query other servers if it does not have the information. (Default = **recurse**; abbreviation = **[no]rec**)
retry=*number*	Set the number of retries to *number*.
timeout=*number*	Change the initial timeout interval for waiting for a reply to *number* seconds.
[no]vc	Always use a virtual circuit when sending requests to the server. (Default = **novc**)
[no]fail	Try the next nameserver if a nameserver responds with SERVFAIL or a referral (nofail) or terminate query (fail) on such a response. (Default = **nofail**)

Examples:

nslookup XXX.XXX.XXX.XXX

- Dig [36] is a program used to display domain name servers as in the syntax below.

Table 3.10 Dig commands

-b *address*	The **-b** option sets the source IP address of the query to *address*. This must be a valid address on one of the host's network interfaces or "0.0.0.0" or "::". An optional port may be specified by appending "#<*port*>"
-c *class*	The default query class (**IN** for Internet) is overridden by the **-c** option. *class* is any valid class, such as **HS** for Hesiod records or **CH** for CHAOSNET records.
-f *filename*	The **-f** option makes **dig** operate in batch mode by reading a list of lookup requests to process from the file *filename*. The file contains a number of queries, one per line. Each entry in the file should be organized in the same way they would be presented as queries to dig using the command-line interface.
-p *port#*	If a non-standard port number is to be queried, the **-p** option is used. *port#* is the port number that dig will send its queries instead of the standard DNS port number 53. This option would be used to test a name server that has been configured to listen for queries on a non-standard port number.
-4	The **-4** option forces dig to only use IPv4 query transport.
-6	The **-6** option forces dig to only use IPv6 query transport.
-t *type*	The **-t** option sets the query type to *type*. It can be any valid query type which is supported in BIND9. The default query type "**A**", unless the **-x** option is supplied to indicate a reverse lookup. A zone transfer can be requested by specifying a**AXFR**. When an incremental zone transfer (**IXFR**) is required, type is set to**ixfr=N**. The incremental zone transfer will contain the changes made to the zone since the serial number in the zone's SOA record was **N**.
-x *addr*	Reverse lookups (mapping addresses to names) are simplified by the **-x** option.*addr* is an IPv4 address in dotted-decimal notation, or a colon-delimited IPv6 address. When this option is used, there is no need to provide the name, class, and type arguments. dig automatically performs a lookup for a name like**11.12.13.10.in-addr.arpa** and sets the query type and class to **PTR** and **IN**respectively. By default, IPv6 addresses are looked up using nibble format under the IP6.ARPA domain. To use the older RFC1886 method using the IP6.INT domain specify the **-i** option. Bit string labels (RFC2874) are now experimental and are not attempted.
-k *filename*	To sign the DNS queries sent by dig and their responses using transaction signatures (TSIG), specify a TSIG key file using the **-k** option.
-y*[hmac:]name:key*	You can also specify the TSIG key itself on the command line using the **-y**option; name is the name of the TSIG key and key is the actual key. The key is a base-64 encoded string, typically generated by **dnssec-keygen**. Caution should be taken when using the **-y** option on multi-user systems as the key can be visible in the output from ps or in the shell's history file. When using TSIG authentication with dig, the name server that is queried needs to know the key and algorithm that is being used. In BIND, this is done by providing appropriate key and server statements in **named.conf**.

Examples:

dig XXXXX.com

- Whois [37] is an Internet service used to find information about a domain name or IP address such as the name, address and phone number of the administrative officer as well as billing information, etc.

Figure 3.3 whois.net website

- NMAP [38] is a utility used to find information about a host discovery, port scan, OS fingerprinting, etc. as in the syntax below.

Host discovery

 # nmap -sP XXX.XXX.XXX.0/24

Port scan TCP SYN scan

 # nmap -sS XXX.XXX.XXX.XXX

OS fingerprinting

 # nmap -O XXX.XXX.XXX.XXX

- Nikto [31] is an Internet service used to find potentially dangerous files/programs and CGI scripts, default files and programs, outdated versions, version-specific problems with server and software miscounting, etc. as in the syntax below.

Scan the IP XXX.XXX.XXX.XXX on TCP port 80:

 # perl nikto.pl –h XXX.XXX.XXX.XXX

Scan the IP XXX.XXX.XXX.XXX on TCP port 443:

 # perl nikto.pl –h XXX.XXX.XXX.XXX –p 443

2.2 Scanning and Testing is the step of vulnerability assessment for identifying the vulnerabilities or weaknesses of a system and reporting vulnerability issues by using tools for vulnerability such as the following scanners: 1) Nessus and 2) Nikto.

a. Nessus [30] is an active vulnerability scanner for scanning, discovery, analysis, checking and detecting the vulnerabilities or weaknesses of a system as shown in Figure 3.3.

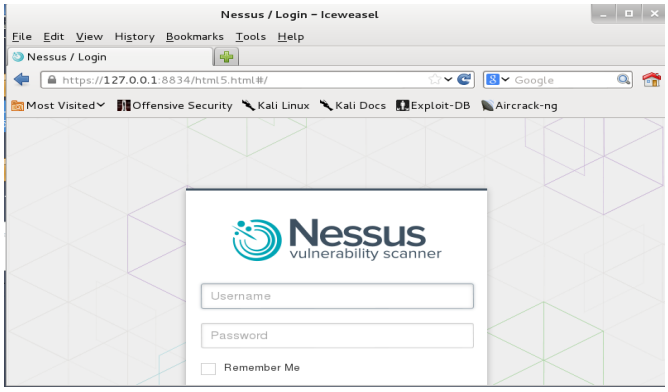


Figure 3.4 Nessus Scan

b. Nikto[31] is an open source web scanner that tests the weaknesses of a web server including potentially dangerous files, CGI scripts, default files and programs with outdated versions, software misconfigurations, injections, XSS and denial of service etc. as shown in Figure 3.4.

```
root@kali:~# nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.
```

Figure 3.5 Command Nikto

3) Verification involves using information from identified vulnerabilities detected in the assessment process for examining and confirming the direction of server attacks including Analysis/Gaining Access, and Checking Full-Disclosure or Exploitation

3.1 Analysis/Gaining Access is the step for using information by sampling vulnerabilities from the assessment process for examining and confirming the direction of server attacks.

3.2 Checking Full-Disclosure or Exploitation is the step of confirming the vulnerability of web applications/critical hosts by surveying the full-disclosure of websites or using tools for vulnerability attacks as shown in Figures 3.6 and 3.7.

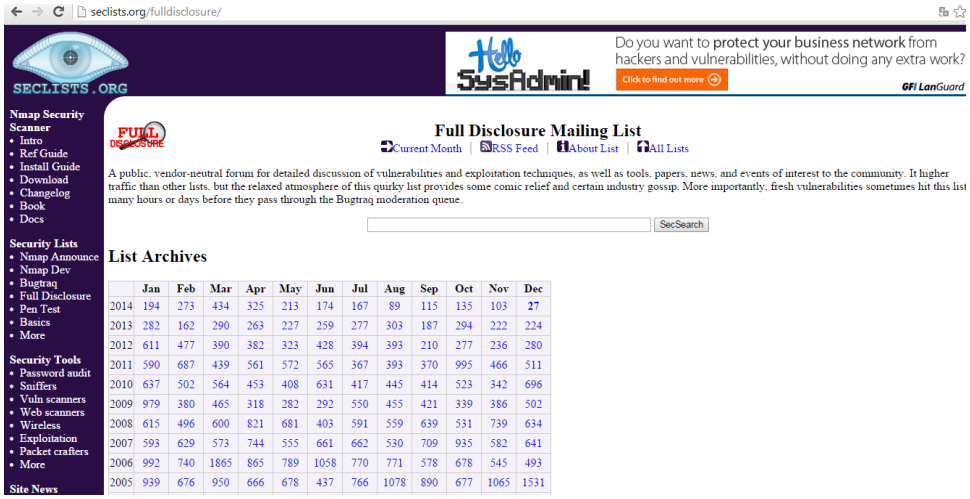


Figure 3.6 full-disclosure website[39]

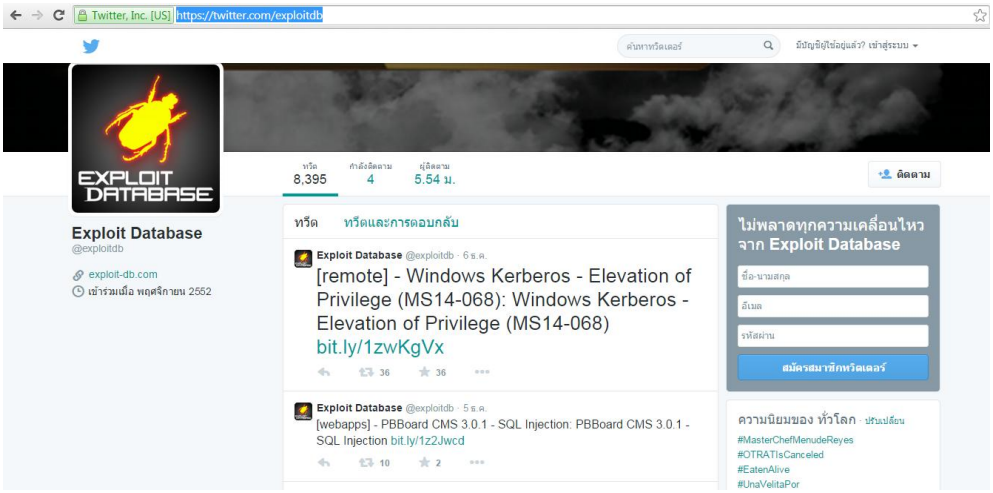


Figure 3.7 Exploit DB tool[40]

4) A report is a summary of all information obtained by collecting data and information from Pierce System Testing the vulnerability after the end of testing. The report will include the identification of vulnerabilities, risk assessment and suggestions. Also included are IT Risk Evaluation and Document/Recommendations.

4.1 The IT Risk Evaluation step determines or identifies risk/vulnerabilities and estimates likelihood and impact. It also determines risk levels.

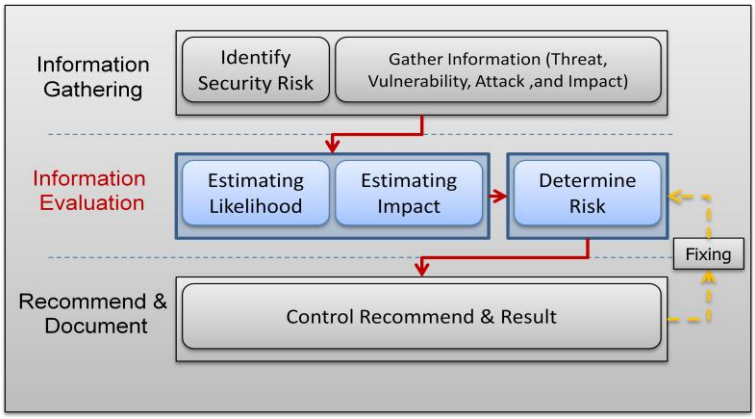


Figure 3.8 ITS Risk Assessment Methodology

Process 1 (Information Gathering) is Data Collection and Determines or Identifies IT Risks/Vulnerabilities

Process 2 (Information Evaluation) is estimating likelihood and impact; it also determines risk levels.

Process 3 (Recommendations and Documents) is reporting summary overviews and risk evaluation process improvement.

4.2 Document/Recommendations is the step where a report summarizes the results of operations. The evaluation of the test results on problems and vulnerabilities detected. It also offers a view of all technical data collected on levels of risk existing in websites/web applications and host security as well as assessment during the test. The conclusion also includes recommendations for improvement, while close vulnerabilities are detected.

3.2.2 Define Function

This procedure is the step of determining a function and detailed design of prototype tools to support security assessment following the step of selecting processes such as importing, evaluating and examining/confirming as shown in Table 3.1.

Table 3.11 Example define functions

No	Main Functions	Sub-Function	descriptions
1	Import is functions of bringing the vulnerability scan result, analyze data into risk evaluate data	1.1 XML Upload	functions of import xml result from nessus vulnerability scan tool.
		1.2 CSV Template Upload	functions of import csv template from insert vulnerability data into csv template.
		1.3 Manual Add/Edit Data	functions of insert and modify vulnerability data in prototype tool.
2	Evaluate is functions of analyze, determine, normalize risk data and calculate impact value , likelihood value, risk level, and risk rating.	2.1 analyze risk	functions of analyze, determine, normalize risk data.
		2.2 evaluate risk	functions of calculate impact value , likelihood value, risk level, and risk rating.
		2.3 risk report	functions of summary and reporting risk rating .
3	Examining/Confirm is functions of check vulnerability reference or mailing list full-disclosure or simulation exploit testing.	3.1 check full-disclosure	functions of mapping vulnerabilities that discovered and show reference or mailing list full-disclosure.
		3.2 simulation exploit	functions of simulation exploit testing sample.

1) Import is a function for supporting data imported from the results of Vulnerability Scan Tools as shown in Figures 3.9 and 3.10.

```
<ReportItem port="445" svc name="cifs" protocol="tcp" severity="3" pluginID="49174"
      pluginName="Opera &lt; 10.62 Path Subversion Arbitrary DLL Injection Code
      Execution" pluginFamily="Windows">
<exploitability_ease>Exploits are available</exploitability_ease>
<vuln publication date>2010/08/24</vuln publication date>
<cvss temporal vector>CVSS2#E:F/RL:W/RC:ND</cvss temporal vector>
<solution>Upgrade to Opera 10.62 or later.</solution>
<cvss temporal score>8.4</cvss temporal score>
<risk factor>High</risk factor>
<description>The version of Opera installed on the remote host is earlier than 10.62.
      Such versions insecurely look in their current
working directory when resolving DLL dependencies, such as for
&apos;dwmapi.dll&apos; [..] </description>
<plugin_publication_date>2010/09/10</plugin_publication_date>
<cvss vector>CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C</cvss vector>
<synopsis>The remote host contains a web browser that allows arbitrary code
execution.</synopsis>
<patch publication date>2010/09/09</patch publication date>
<see also>http://www.opera.com/docs/changelogs/windows/1062/</see also>
<see also>http://www.opera.com/support/kb/view/970/</see also>
<exploit available>true</exploit available>
<plugin_modification_date>2010/12/23</plugin_modification_date>
<cvss_base_score>9.3</cvss_base_score>
<bid>42663</bid>
<xref>OSVDB:67498</xref>
<xref>Secunia:41083</xref>
<xref>EDB-ID:14732</xref>
<plugin_output>
```

Figure 3.9 Nessus result

```
nikto -host XX.XXX.XXX.XX -vhost www.XXXXXXXX.XXX -p 80 443

- Nikto v2.1.1
---------------------------------------------------------------------------
+ Target IP:        XX.XXX.XXX.XX
+ Target Hostname:  IP.targethostname.com
+ Target Port:      80
+ Virtual Host:     www.XXXXXXXX.org
+ Start Time:       2010-XX-XX 13:02:35
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Microsoft-IIS/6.0 appears to be outdated (4.0 for NT 4, 5.0 for Win2k, current is at leas
+ Retrieved X-Powered-By header: ASP.NET
+ GET /: Retrieved X-Powered-By header: PHP/4.4.7
+ GET /: Uncommon header 'x-pingback' found, with contents: http:/www.XXXXXXXX.XXX/xmlrpc.p
+ Retrieved microsoftoffi cewebserver header: 5.0_Pub
+ Uncommon header 'microsoftoffi cewebserver' found, with contents: 5.0_Pub
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3092: /LICENSE.txt: License fi le found may identify site software.
+ OSVDB-3092: /xmlrpc.php: xmlrpc.php was found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' versi
+ /readme.html: This WordPress fi le reveals the installed version.
+ OSVDB-3092: /license.txt: License fi le found may identify site software.
+ OSVDB-3092: /LICENSE.TXT: License fi le found may identify site software.
+ 3823 items checked: 14 item(s) reported on remote host
+ End Time: 2010-03-11 13:47:19 (2684 seconds)
+ 1 host(s) tested
```

Figure 3.10 Nikto result

2. Evaluation is the step involving risk rating by using the information evaluation phase in IT risk assessment methodology divided into the following three processes: a) Data Preparation; b) Determining Impact/Likelihood and c) Risk Determination as shown in Figure 3.11.

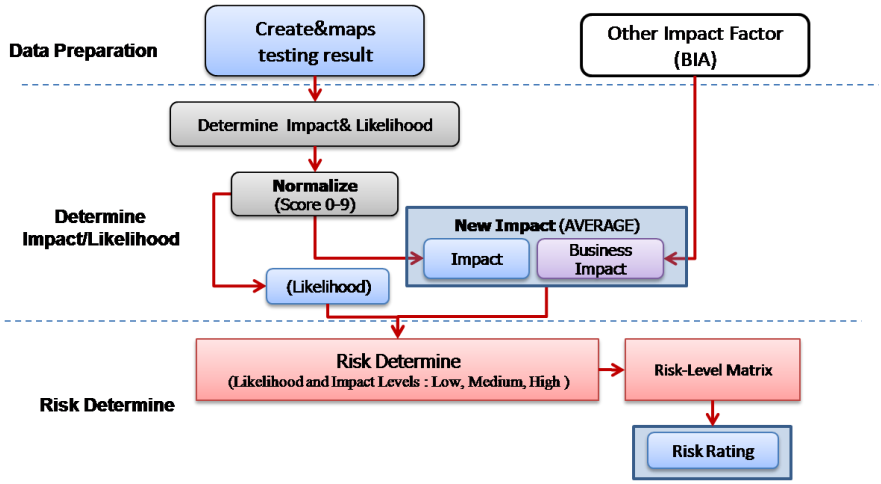


Figure 3.11 IT Risk Evaluation Process

a) Data Preparation is the process of creating and mapping test results in a valid document format.

b) Determining Impact/Likelihood is the process of determining, normalizing, and recalculating likelihood and impact values by using OWASP Risk Determination as shown in Table 3.12.

Table 3.12 OWASP Risk Determine

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

c) Risk Determination is the process of defining risk rating by using the OWASP Risk Level Matrix as shown in Tables 3.13 and 3.14.

Table 3.13 OWASP Risk Level Matrix

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
	Likelihood			

Table 3.14 OWASP Risk Level Definition

Risk Level	Definition
CRITICAL	Website / Web applications / Host computer may be attacked by intruders. And control information system completely. If the vulnerability assessment Or vulnerabilities that did not make the correction.
HIGH	Website / Web applications / Host computer may be attacked by intruders. And control information system If the vulnerability assessment Or vulnerabilities that did not make the correction.
MEDIUM	Website / Web applications / Host computer may be the attackers stole information from the target device to take advantage. Or modification sensitive information
LOW	Website / Web applications / Host computer provides information that is useful to attacks from intruders.

3. Examination/Confirmation is the step of testing and checking full disclosure or exploitation testing samples. This step is divided into the following two processes: 1) checking full-disclosure, and 2) exploit testing samples

3.1 Checking full disclosure is the step of confirming the vulnerability of web applications/critical hosts by surveying full-disclosure websites such as the following samples:

- http://seclists.org/fulldisclosure/
- http://nmap.org/mailman/listinfo/fulldisclosure
- https://twitter.com/SecLists
- http://lists.openwall.net/full-disclosure/
- http://archives.neohapsis.com/
- http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/
- http://www.gossamer-threads.com/lists/fulldisc/full-disclosure/
- http://www.mail-archive.com/full-disclosure@lists.netsys.com/
- http://www.mail-archive.com/full-disclosure@lists.grok.org.uk/
- https://marc.info/
- https://isc.sans.edu/diaryarchive.html
- http://www.governmentsecurity.org/archives/fulldisclosure/
- http://www.attrition.org/pipermail/vim/
- http://osdir.com/ml/security.full-disclosure/
- http://1.security-full-disclosure.securetalk.info/

3.2 Exploit testing samples is the step of confirming the vulnerability of web applications/critical hosts by using the Metasploit.

Metasploit [32] is a tool for penetration testing and using exploit code. Modules can be selected and viewed with use commands by specifying the module's name by an Msfconsole interface as shown in Figure 3.11.

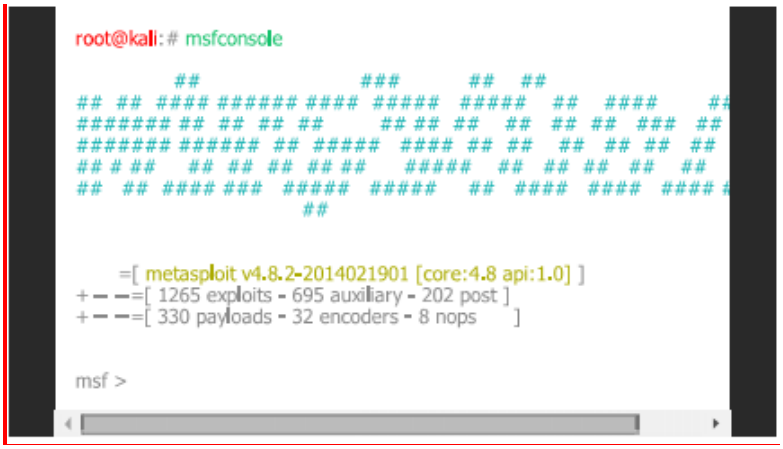


Figure 3.12 msfconsole interface

3.3 Development Phase

This procedure is the step of developing prototype tools to support security assessment processes divided into the following two processes: 1) Build/Implement Demo and 2) Test and Feedback.

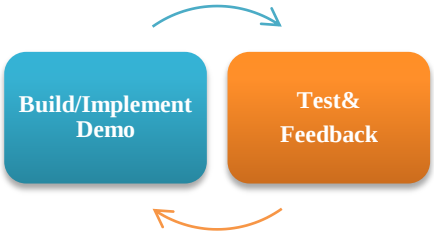


Figure 3.13 develop process

3.3.1 Build/Implement Demo is the step of creating prototypes on defined functions and integrating the programs divided into the following two processes: 1) Creating a database and 2) Coding.

1. Creating a database is the step for designing and creating table data on security assessment prototype tools such as risk evaluation data or vulnerability verification data.

a) Risk evaluation data is a table about risk issues, including impact factors, likelihood factors, impact and likelihood levels, risk levels and risk rating as shown in Tables 3.15 and 3.16.

Table 3.15 OWASP Likelihood Factor

	Rating	0	1	2	3	4	5	6	7	8	9
Threat Agent Factors	Skill level	N/A	No technical skills	N/A	Some technical skills	Advanced computer user	N/A	Network and programming skills	N/A	N/A	Security penetration skills
	Motive	N/A	Low/No reward	N/A	N/A	possible reward	N/A	N/A	N/A	N/A	High reward
	Opportunity	No known access	N/A	N/A	N/A	limited access	N/A	N/A	N/A	N/A	Full access
	Size	N/A	N/A	Developers /System administrators	N/A	intranet users	partners	Authenticated users	N/A	N/A	Anonymous Internet users
Vulnerability Factors	Ease of discovery	N/A	Practically impossible	N/A	Difficult	N/A	N/A	N/A	Easy	N/A	Automated tools available
	Ease of exploit	N/A	Theoretical	N/A	Difficult	N/A	N/A	N/A	Easy	N/A	Automated tools available
	Awareness	N/A	Unknown	N/A	N/A	Hidden	N/A	Obvious	N/A	N/A	Public knowledge
	Intrusion detection	N/A	Active detection in application	N/A	logged and reviewed	N/A	N/A	N/A	N/A	logged without review	Not logged

Table 3.16 OWASP Impact Factor

	Rating	0	1	2	3	4	5	6	7	8	9
Technical Impact Factors	Loss of confidentiality	N/A	N/A	Minimal non-sensitive data disclosed	N/A	N/A	N/A	Minimal critical data disclosed / Extensive non-sensitive data disclosed	N/A	N/A	Extensive critical data disclosed, all data disclosed
	Loss of integrity	N/A	Minimal slightly corrupt data	N/A	Minimal seriously corrupt data	N/A	Extensive slightly corrupt data	N/A	Extensive seriously corrupt data	N/A	All data totally corrupt
	Loss of availability	N/A	Minimal secondary services interrupted	N/A	N/A	N/A	Minimal primary services Interrupted/ Extensive secondary services interrupted	N/A	Extensive primary services interrupted	N/A	All services completely lost
	Loss of accountability	N/A	Fully traceable	N/A	N/A	N/A	N/A	N/A	Possibly traceable	N/A	Completely anonymous
Business Impact Factors	Financial damage	N/A	Less than the cost to fix the vulnerability	N/A	Minor effect on annual profit	N/A	N/A	N/A	Significant effect on annual profit	N/A	Bankruptcy
	Reputation damage	N/A	Minimal damage	N/A	N/A	Loss of major accounts	Loss of goodwill	N/A	N/A	N/A	Brand damage
	Non-compliance	N/A	N/A	Minor violation	N/A	N/A	Clear violation	N/A	High profile violation	N/A	N/A
	Privacy violation	N/A	N/A	N/A	One individual	N/A	Hundreds of people	N/A	Thousands of people	N/A	Millions of people

b) Vulnerability verification data is a table about references, full disclosure and exploit codes including mailing lists, exploit databases and Metasploit modules as shown in Tables 3.17 - 3.19.

Table 3.17 Sample Full – Disclosure Data

No	Full-disclosure	CVE
1	FULLDISC:20020717 TheServer cleartext password sillyness.	CVE-2002-2389
2	FULLDISC:20020719 Vulnerability found: Adobe Acrobat eBook Reader and Content Server	CVE-2002-1016
3	FULLDISC:20020720 Netscape Communicator META Refresh Denial of Service	CVE-2002-2308
4	FULLDISC:20020720 PHP Resource Exhaustion Denial of Service	CVE-2002-2309
5	FULLDISC:20020724 REFRESH: EUDORA MAIL 5.1.1	CVE-2002-2313
6	FULLDISC:20020808 Cross-Site Scripting Issues in Falcon Web Server	CVE-2002-2318
7	FULLDISC:20020829 RPM verification	CVE-2002-2204
8	FULLDISC:20020903 Check Point statement on use of IKE Aggressive Mode	CVE-2002-1623
9	FULLDISC:20020917 Trillian .74 and below, ident flaw.	CVE-2002-2390
10	FULLDISC:20020919 iDEFENSE OSF1/Tru64 3.x vuln clarification	CVE-2000-1031 CVE-2002-1604 CVE-2002-1605 CVE-2002-1614 CVE-2002-1616 CVE-2002-1617

Table 3.18 Sample Exploit DB Data

EDBID	File	Description	Date	Author	Type	Link
1	platforms/windows/remote/1.c	MS Windows WebDAV - (ntdll.dll) Remote Exploit	23/3/2003	kralor	remote	http://www.exploit-db.com/exploits/1/
2	platforms/windows/remote/2.c	MS Windows WebDAV - Remote PoC Exploit	24/3/2003	RoMaNSoFt	remote	http://www.exploit-db.com/exploits/2/
3	platforms/linux/local/3.c	Linux Kernel 2.2.x - 2.4.x ptrace/kmod Local Root Exploit	30/3/2003	Wojciech Purczynski	local	http://www.exploit-db.com/exploits/3/
4	platforms/solaris/local/4.c	Sun SUNWlldap Library Hostname - Buffer Overflow Exploit	1/4/2003	Andi	local	http://www.exploit-db.com/exploits/4/
5	platforms/windows/remote/5.c	MS Windows RPC Locator Service - Remote Exploit	3/4/2003	Marcin Wolak	remote	http://www.exploit-db.com/exploits/5/
6	platforms/php/webapps/6.php	WordPress <= 2.0.2 (cache) Remote Shell Injection Exploit	25/5/2006	rgod	webapps	http://www.exploit-db.com/exploits/6/
7	platforms/linux/remote/7.pl	Samba 2.2.x - Remote Root Buffer Overflow Exploit	7/4/2003	H D Moore	remote	http://www.exploit-db.com/exploits/7/
8	platforms/linux/remote/8.c	SETI@home Clients - Buffer Overflow Exploit	8/4/2003	zillion	remote	http://www.exploit-db.com/exploits/8/
9	platforms/windows/dos/9.c	Apache HTTP Server 2.x Memory Leak Exploit	9/4/2003	Matthew Murphy	dos	http://www.exploit-db.com/exploits/9/
10	platforms/linux/remote/10.c	Samba 2.2.8 - Remote Root Exploit	10/4/2003	eSDee	remote	http://www.exploit-db.com/exploits/10/

Table 3.19 Sample metasploit module Data

No	VulnID	Refname	File
1	CVE-2009-3699	aix/rpc_cmsd_opcode21	/usr/share/metasploit-framework/modules/exploits/aix/rpc_cmsd_opcode21.rb
2	CVE-2009-2727	aix/rpc_ttdbserverd_realpath	/usr/share/metasploit-framework/modules/exploits/aix/rpc_ttdbserverd_realpath.rb
3	CVE-2006-3459	apple_ios/browser/safari_libtiff	/usr/share/metasploit-framework/modules/exploits/apple_ios/browser/safari_libtiff.rb
4	CVE-2004-2221	bsdi/softcart/mercantec_softcart	/usr/share/metasploit-framework/modules/exploits/bsdi/softcart/mercantec_softcart.rb
5	CVE-2001-0797	dialup/multi/login/manyargs	/usr/share/metasploit-framework/modules/exploits/dialup/multi/login/manyargs.rb
6	CVE-2010-4221	freebsd/ftp/proftp_telnet_iac	/usr/share/metasploit-framework/modules/exploits/freebsd/ftp/proftp_telnet_iac.rb
7	CVE-2003-0201	freebsd/samba/trans2open	/usr/share/metasploit-framework/modules/exploits/freebsd/samba/trans2open.rb
8	CVE-2002-1473	hpux/lpd/cleanup_exec	/usr/share/metasploit-framework/modules/exploits/hpux/lpd/cleanup_exec.rb
9	CVE-2001-0800	irix/lpd/tagprinter_exec	/usr/share/metasploit-framework/modules/exploits/irix/lpd/tagprinter_exec.rb
10	CVE-2008-5499	linux/browser/adobe_flashplayer_aslaunch	/usr/share/metasploit-framework/modules/exploits/linux/browser/adobe_flashplayer_aslaunch.rb

2. Coding is created, modified, and compiled module functions using a programming language by dividing into the following two steps: 1) Creating a Function Demo and 2) Integrating modules.

a. Creating a Function Demo is the step for creating, writing and debugging functions and statements in a program by dividing into the following eight functions: 1) XML Upload; 2) CSV Template Upload; 3) Manual Add/Edit Data; 4) Analyze Risk; 5) Evaluate Risk; 6) Risk Report; 7) Check Full-Disclosure and 8) Simulation Exploit as shown in Tables 3.13 - 3.19.

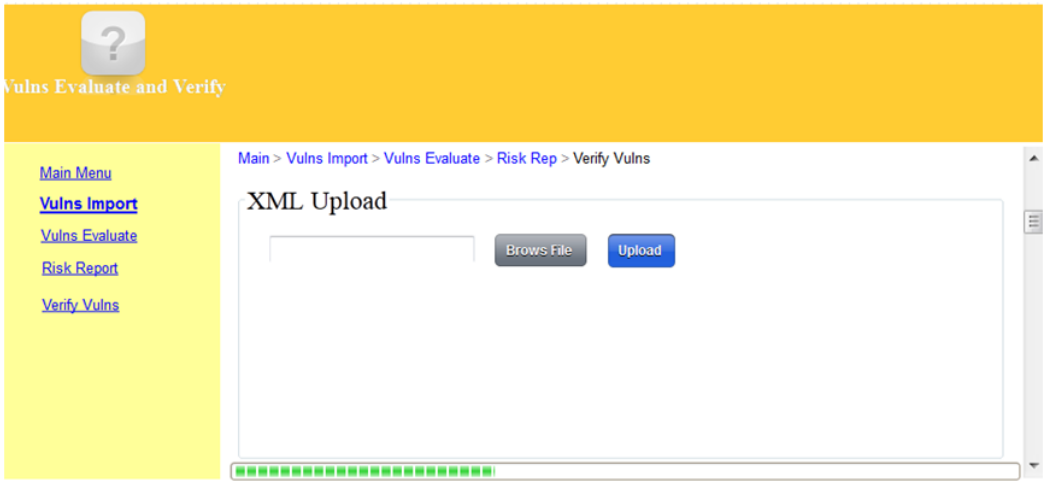


Figure 3.14 XML Upload Prototyping

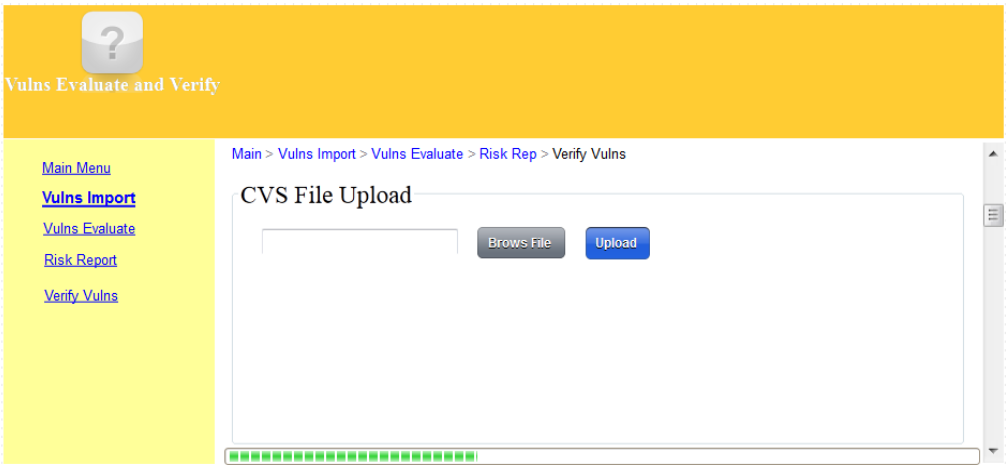


Figure 3.15 CSV Template Upload Prototyping

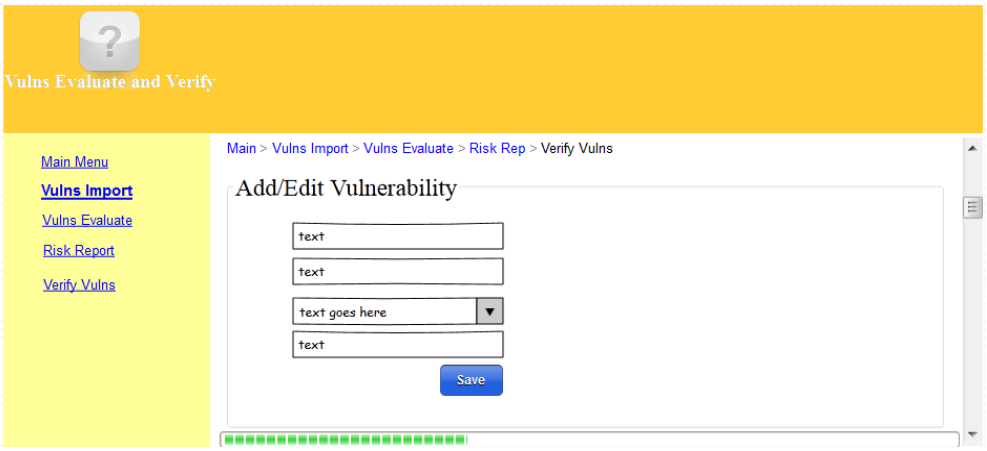


Figure 3.16 Manual Add/Edit Data Prototyping

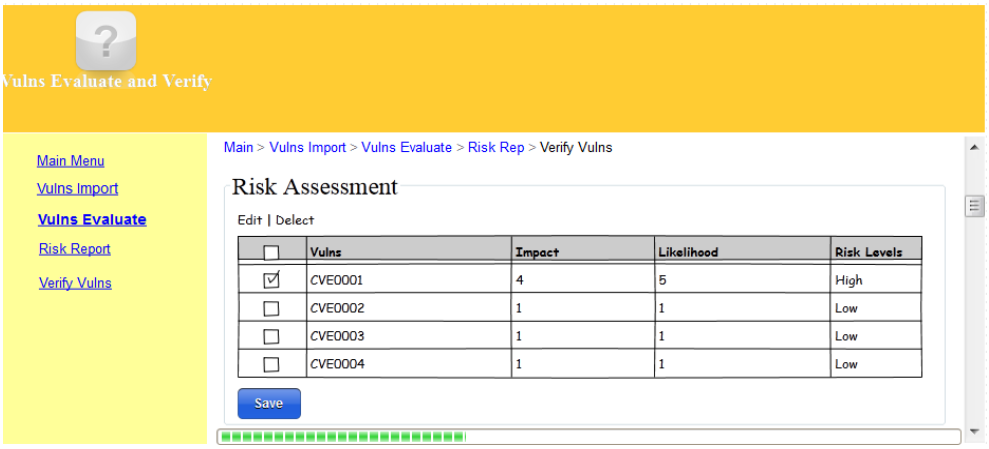


Figure 3.17 Analyze Risk and Evaluate Risk Prototyping

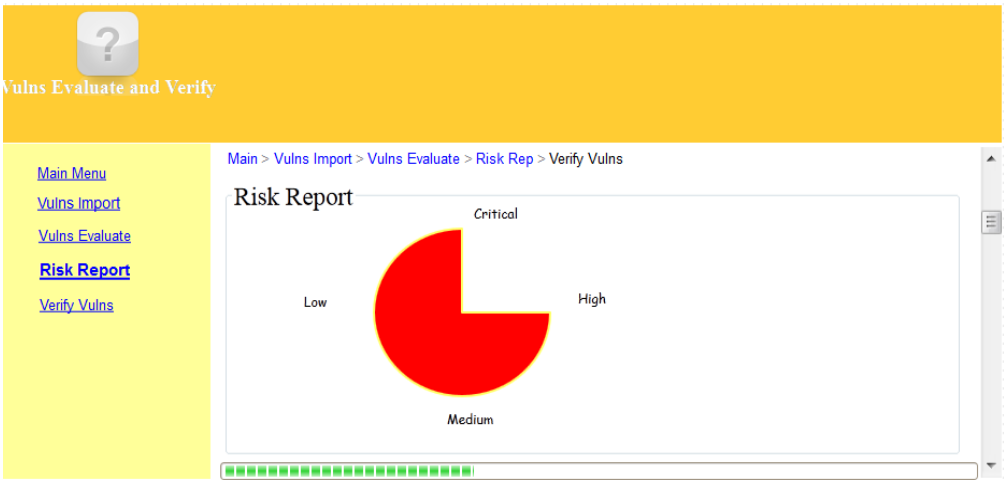


Figure 3.18 Risk Report Prototyping

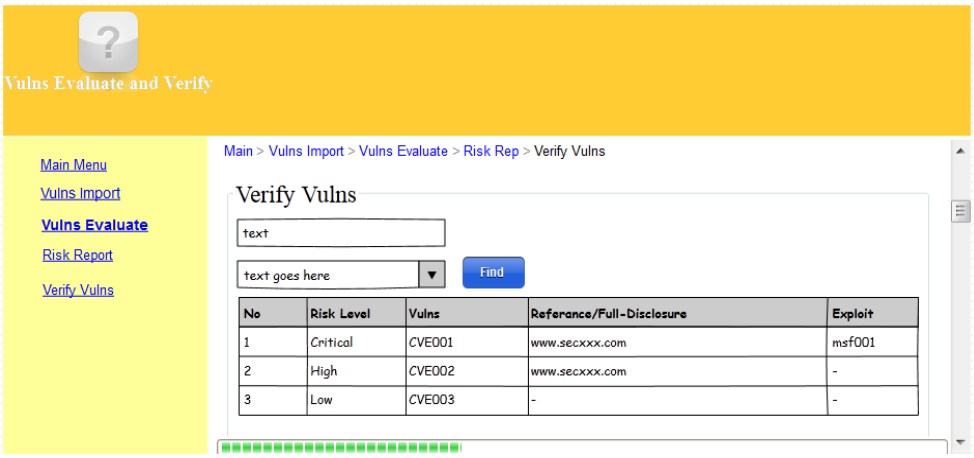


Figure 3.19 Check Full-Disclosure Prototyping

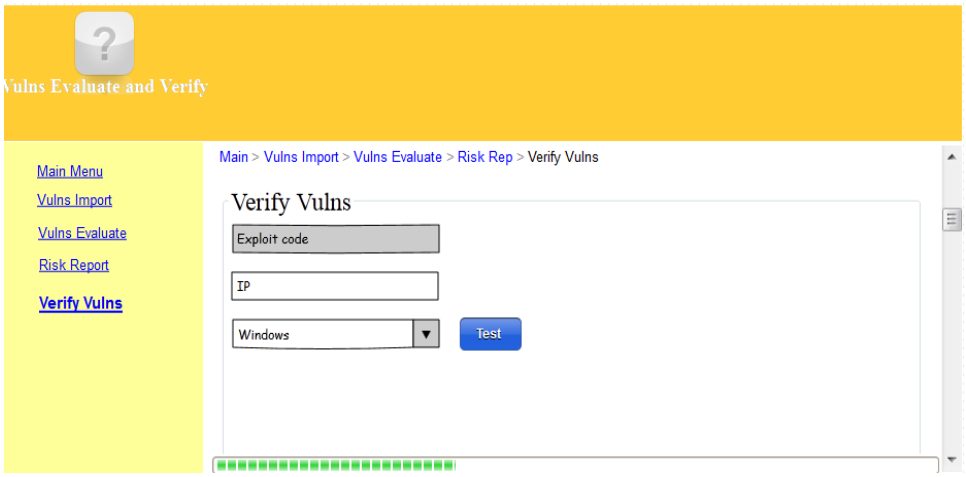


Figure 3.20 Simulation Exploit Prototyping

b. Integrating modules is the step combining all functions into one program including the following three main functions: 1) Import; 2) Evaluate and 3) Examine/Confirm as shown in Figure 3.20.

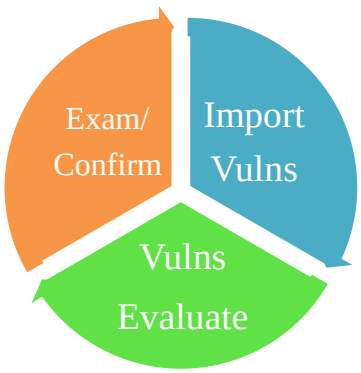


Figure 3.21 Integrated Functions

3.3.2 Test is the process of checking and confirming bugs in the functions of programs and one prototype tool, including fixing programs in the recommendations by dividing into the following two steps: 1) Test Demo and 2) Feedback.

1) Test Demo is the step of checking the function demo and debugging a program.

2) Feedback the step of fixing programs according to the recommendations.

3.4 Utilization Phase

This procedure is the process of utilizing prototype tools used to support risk evaluation and verification vulnerabilities divided into the following two steps: 1) Apply and 2) Report.

1. Application is the step of using prototype tools for risk rating and confirming the vulnerabilities detected in sample testing.

2. Reporting is the step of summarizing the results, including vulnerability scan issues, risk levels, risk rating, vulnerability references and recommendations.

3.5 Research Schedule

Table 3.20 Research Schedule

Phases	Activity	2014				KPI
		JAN-MAR	APR-JUN	JUL-SEP	OCT-DEC	
Plan	1) Literature Review : Study and analysis healthcare security , Security risk assessment guide, and Penetration testing or vulnerability assessment guide					Analysis result
Analysis& Develop	2.1) Defined and classify process to find key process of Security Assessment					Functions Scope
	2.2) Find key process to develop prototype functions					
	3.1) Determine function and detailed design					Prototype Tool
	3.2) Develop prototype tools					
Utilize	4) Apply prototype tools and Report					Security Risk Report

CHAPTER IV
RESULTS

This chapter summarizes security assessment and the development of a prototype tool to support the security assessment process in security risk evaluation and verification of vulnerabilities for hospital information security in Thailand.

.

4.1 Security Assessment Scope

4.1.1 Studying best practice for risk assessment with the following standards applied: ISMS, NIST SP800-30, OWASP and HIPPA. The aforementioned can be synthesized, compared and applied to the group risk assessment processes shown in Tables 4.1 - 4.3.

Table 4.1 IT Risk Assessment Guide Analysis Table

No	GUIDELINE				Grouping
	ISMS	NIST SP800-30	OWASP	HIPAA	
1	Identify major assets	System characterization	NA	Determine system characterization	Information Gathering
2	Assess asset value in terms			System mission	
3	Identify threats & vulnerabilities	Threat& Vulnerability identification	Identifying Risk	Identify any vulnerability or weakness in security procedures or safeguards	
4	NA	Control analysis			
5	NA	Likelihood determination	Estimating Likelihood	NA	Information Evaluation
6		Impact analysis	Estimating Impact	Identify impact	
7	Identify measures of risk	Risk determination	Determining Severity of the Risk	NA	
8	Security Requirements	Control recommendations	Deciding What to Fix	Recommend security controls	Recommend
9	Security Controls				
10	Reduce Risks	NA	NA	NA	
11	Risk Acceptance				
12	NA			Determine residual risk	
13	NA	Results documentation	NA	Document all outputs	Document
14	NA	NA	Customizing Your Risk Rating Model	NA	Fixing

Table 4.2 Risk Assessment Guide Comparison Table

No	Process	Activity	GUIDLINE			
			ISMS	NIST	OWASP	HIPPA
1	Information Gathering	System characterization	✓	✓	×	✓
2		Identify threats & vulnerabilities	✓	✓	✓	✓
3		Control analysis	×	✓	✓	✓
4	Information Evaluation	Likelihood determination	×	✓	✓	×
5		Identify Impact	×	✓	✓	✓
6		Risk determination	✓	✓	✓	×
7	Recommend	Recommend security controls	✓	✓	✓	✓
8		Reduce Risks & Risk Acceptance	✓	×	×	×
9		Determine residual risk	×	×	×	✓
10	Documentation	Results documentation	×	✓	×	✓
11	Improvement	Customizing Your Risk Rating Model	×	×	✓	×

Table 4.3 Risk Assessment Guide Grouping Table

No	Process	Activity	Guideline (ISMS, NIST, HIPPA, and OWASP)
1	Information Gathering	System characterization	Exclude (OWASP)
2		Identify threats	ALL
2		Identify vulnerabilities	ALL
3		Control analysis	Exclude (ISMS)
4	Information Evaluation	Likelihood determination	NIST, and OWASP
5		Identify Impact	Exclude (ISMS)
6		Risk determination	Exclude (HIPPA)
7	Recommend	Recommend security controls	ALL
8		Reduce Risks	ISMS
9		Risk Acceptance	ISMS
10		Determine residual risk	HIPPA
11	Documentation	Results documentation	ALL
12	Improvement	Customizing Your Risk Rating Model	OWASP

By this educational IT risk assessment guideline, we can define the methodology of IT risk assessment for this research as divided into the following three main processes: 1) Information Gathering; 2) Information Evaluation and 3) Recommendation and Documentation as shown in Figure 4.1.

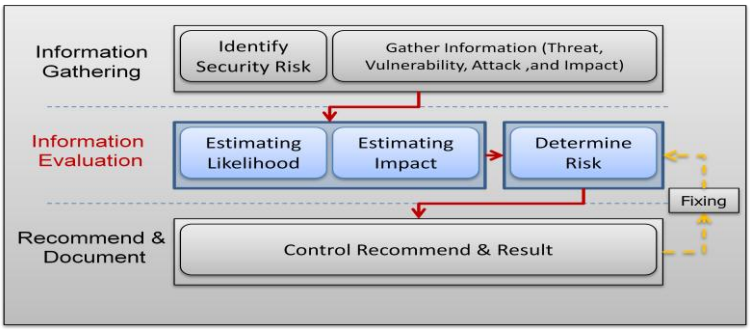


Figure 4.1 IT Risk Assessment Methodologies

Process 1 (Information Gathering) involves data collection and determining or identifying IT risk/vulnerability.

Process 2 (Information Evaluation) involves estimating likelihood and Impact, as well as determining risk levels.

Process 3 (Recommendation and Documentation) involves reporting a summary overview and risk evaluation of the process for improvement.

4.1.2 Studying best practice for penetration testing applied the following standards: NIST SP800-115, ISSAF, SANS, PTES and OWASP. The aforementioned can synthesize, compare and group penetration testing processes as shown in Tables 4.4 and 4.5.

Table 4.4 Penetration Testing/Vulnerability Assessment Guide Analysis

No	GUIDELINE					Grouping
	NIST SP800-115	OWASP	ISSAF(OISSG)	PTES	SANS	
1	Planning : rules are identified, management approval, and testing goals	NA	Planning and preparation : Determine object, scope	NA	Planning and Preparation	Planning
2	Discovery : actual testing, information gathering, and vulnerability analysis	*Passive* (information gathering, and understand application's logic)	Assessment: Information Gathering, Network Mapping, Vulnerability Identification, and Penetration, Gaining Access & Privilege Escalation, Enumerating Further, Compromise Remote Users/Sites, Maintaining Access, and Covering Tracks	Intelligence Gathering	Information Gathering an d Analysis	Assessme nt
		Active (testing: Management, Business Logic, Authentication , Authorization, Session Management, Data Validation , Denial of Service , Web Services, and Ajax)		Vulnerabilit y Analysis	Vulnerability Detection	
3	Attack: Gaining access, and Escalating privileges			Exploitation	Penetration Attempt	Verify/ Attack
4	Reporting: Risk assessment and Reporting	Risk rating and Report	Reporting : Cleaning , Risk assessment and Reporting	Reporting	Analysis and Reporting	Report
					Cleaning Up	

Table 4.5 Penetration Testing/Vulnerability Assessment Guide Synthesis & Comparison

No	Process	Activity	Guideline				
			NIST	*ISSAF*	*OWASP*	*PTES*	*SANS*
1	PLANING	Indentify objective	✓	✓	×	×	✓
2		Determine scope	✓	✓	×	×	✓
3	ASSESSMENT	Information gathering /Foot printing	✓	✓	✓	✓	✓
4		Vulnerability Scanning /Testing	✓	✓	✓	✓	✓
5	VERIFY /ATTACK	Gaining Access	✓	✓	✓	✓	✓
7		Exploitation	✓	✓	✓	✓	✓
8	REPORT	identifying vulnerability	✓	✓	✓	✓	✓
9		risk assessment	✓	✓	✓	✓	✓
10		recommended	✓	✓	✓	✓	✓
11		result testing or Finding	✓	✓	✓	✓	✓

From this educational penetration testing guideline, a security risk assessment process can be defined and divided into the following four main processes: 1) Planning; 2) Assessment; 3) Verification and 4) Reporting as shown in Figure 4.2.

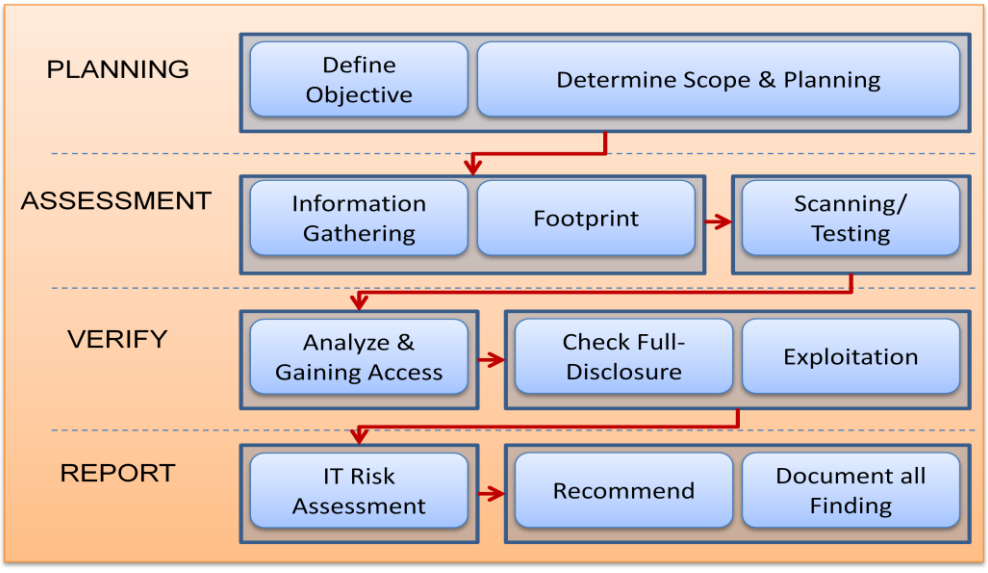


Figure 4.2 Security Risk Assessment methods

Process 1 (Planning) is a planning and determining the rules, scope and objectives of security assessment processes by dividing into the following two processes: 1) Defining Objectives and 2) Setting the Scope and Planning.

Process 2 (Assessment) is an information system assessment of objectives for identifying the vulnerability occurrence in the information system by dividing into the following two processes: 1) Information and Footprint Gathering and 2) Scanning and Testing.

Process 3 (Verification) is using information from identified vulnerabilities discovered by the assessment process for examining and confirming the direction of server attacks by dividing into the following two processes: 1) Analyze and Gain Access and 2) Check for Full Disclosure/Exploitation.

Process 4 (Report) is collecting all information from system testing on the vulnerability after the end of testing. The report will include the identification of vulnerabilities, risk assessment and suggestions indicated by the aforementioned vulnerabilities by dividing into the following two phases: 1) IT Risk Evaluation and 2) Documentation and Recommendations.

4.2 Prototype Tools

4.2.1 Process Selection is the step for analyzing and choosing a process for developing prototype functions supporting security risk assessment. For this process, the results involved the following two processes: 1) Risk Evaluation and 2) Vulnerability verification.

Table 4.6 Security Assessment Process Analysis

Factor Levels value :
[1] Minor or low Priority
[2] Moderate or Medium Priority
[3] Major or High Priority

No	Process	Activity	*Complex*	*Explicit*	*Specific knowledge*	*Tool supports*	Total	Rank
1	PLANING	Indentify objective / Determine scope	1	2	1	3	7	5
2	ASSESSMENT	Information gathering /Foot printing	2	2	2	2	8	4
		Vulnerability Scanning /Testing	2	3	3	2	10	3
3	VERIFY /ATTACK	Check Full-Disclosure/Exploitation	3	3	3	2	11	2
4	REPORT	risk assessment / result testing or Finding	3	3	3	3	12	1

4.2.2 Define Functions is the step for determining a function and detailed designs of prototype tools to support risk evaluation and verification vulnerabilities. For this step, the results involve the following three main functions: 1) Importing; 2) Evaluating and 3) Examining/Confirming as shown in Tables 4.7 and 4.8.

Table 4.7 Determine Functions

No	Main Functions	Sub-Function	Details Functions
1	Import is functions of bringing the vulnerability scan result, analyze data into risk evaluate data	1.1 XML Upload	Xml upload is functions of import xml result from nessus vulnerability scan tool. divided into 3 process that is 1) Brow and Choose File , 2) Import Data, and 3) Result upload
		1.2 CSV Template Upload	CSV Template Upload is functions of import csv template from insert vulnerability data into csv template. divided into 3 process that is 1) Brow and Choose File , 2) Import Data, and 3) Result upload
		1.3 Manual Add/Edit Data	Manual Add/Edit Data is functions of insert and modify vulnerability data in prototype tool. divided into 5 process that is 1) Insert, 2) Change, 3) Delete, 4) Show Data, and 5) Find Data
2	Evaluate is functions of analyze, determine, normalize risk data and calculate impact value, likelihood value, risk level, and risk rating.	2.1 Analyze risk	Analyze risk is functions of analyze, determine, normalize risk data. divided into 2 function that is 1) Decompose Data, and 2) Estimate Data
		2.2 Evaluate risk	Evaluate risk is functions of calculate impact value, likelihood value, risk level, and risk rating. divided into 2 function that is 1) Calculate Risk Value, and 2) Risk Rating Mapping
		2.3 Risk report	Risk report is functions of summary and reporting risk rating. divided into 4 function that is 1) Show Data, and 2) Show Report, 3) Export Data , and 4) Print Report
3	Examining/Confirm is functions of check vulnerability reference or mailing list full-disclosure or simulation exploit testing.	3.1 Check full-disclosure	Check full-disclosure is functions of mapping vulnerabilities that discovered and show reference or mailing list full-disclosure. divided into 3 function that is 1) Show Data , 2) Find Data, and 3) Details Reference
		3.2 Simulation exploit	Simulation exploit is functions of simulation exploit testing sample. divided into 5 function that is 1) Show Data , 2) Find Data, 3) Change Data, 4) Detail Exploit Code, and 5) Testing Sample

Table 4.8 Detailed Designs

No	Activity	Functions	Details
1	Brow and Choose File	Xml upload CSV Template Upload	1.System show User Interface 2.User choose XML file or CSV Text file form Local file
2	Import Data	Xml upload CSV Template Upload	1.System read data file 2.System connect Database 3.System write data into Database
3	Result upload / Show Data	Xml upload CSV Template Upload	1.System show write Data Result or show Table data Result
4	Insert Data	Manual Add/Edit Data	1.System show User Interface 2.User key in data Records 3.System read data Records 4.System connect Database 5.System write data into Database
5	Change Data	Manual Add/Edit Data	1.System show User Interface 2.User select data Record 3.User Edit data Record 4.System read data Records 5.System connect Database 6.System write data into Database
6	Delete Data	Manual Add/Edit Data	1.System show User Interface 2.User select data Record 3.System read data Records 4.System connect Database 5.System delete data into Database
7	Show Data	Manual Add/Edit Data Risk report Check full-disclosure Simulation exploit	1.System connect Database 2.System read data 3.System Show data in User Interface
8	Find Data	Manual Add/Edit Data Check full-disclosure Simulation exploit	1.System show User Interface 2.User key in data Find 3.System read data Records 4.System connect Database 5.System read data 6.System Show data in User Interface
9	Decompose Data	Analyze risk	1. System connect Database 2. System read data 3.System calculate and assess data 4.Database choose , combine , calculate, assess, and mapping risk data
10	Estimate Data	Analyze risk	
11	Calculate Risk Value	Evaluate risk	
12	Risk Rating Mapping	Evaluate risk	

Table 4.8 Detailed Designs (Cont.)

No	Activity	Functions	Details
13	Show Report	Risk report	1.System show User Interface 2.User choose report 3.System connect Database 4.System read data 5.System Show Report
14	Export Data	Risk report	1.System show User Interface 2.User choose report 3.System connect Database 4.System read data 5.System Export data
15	Print Report	Risk report	1.System show Report 2.User choose print report 3.System print report
16	Details Reference	Check full-disclosure	1.System connect Database 2.System read data 3.System Show data in User Interface
17	Detail Exploit Code	Simulation exploit	1.System show User Interface 2.User choose Record and select Info 3. System Show Exploit Info
18	Change Details	Simulation exploit	1.System show User Interface 2.User choose Record 3.User change Details 4.User choose Test 5.System exploit testing 6. System Show Exploit Result
19	Testing Sample	Simulation exploit	1.System show User Interface 2.User choose Record 3.User choose Test 4.System exploit testing 5. System Show Exploit Result

4.2.3 Prototype Design is the step for designing and creating a prototype model to construct a prototype tool. For this step, the results were the following 19 prototype models: 1) Browse and Choose Files; 2) Import Data; 3) Upload results/Show Data; 4) Enter Data; 5) Change Data; 6) Delete Data; 7) Show Data; 8) Find Data; 9) Decompose Data; 10) Estimate Data; 11) Calculate Risk Value; 12) Risk Rating Mapping; 13) Show Report; 14) Export Data; 15) Print Report; 16) Details Reference; 17) Detail Exploit Code; 18) Change Details and 19) Test Samples as shown in Appendix A . Examples of prototype designs are shown in Figures 4.3 – 4.4.

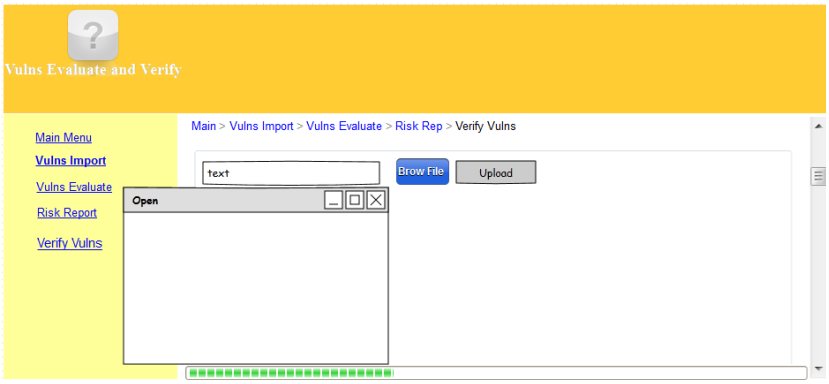


Figure 4.3 Brows and Choose File and Import Data Prototyping

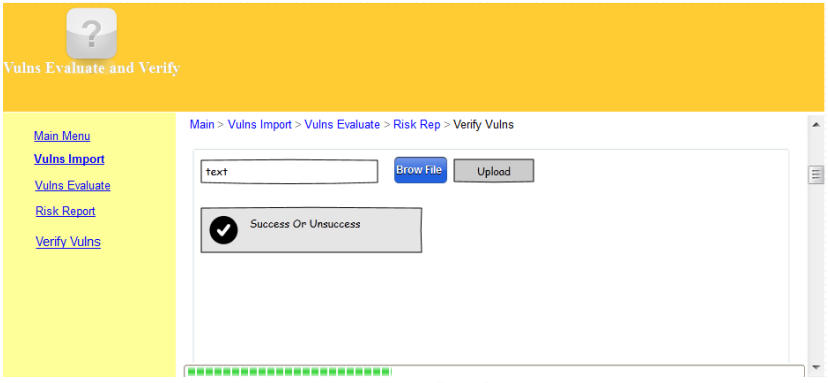


Figure 4.4 Result upload Prototyping

4.2.4 Development is the step for constructing prototype tools to support risk evaluation and verification of vulnerabilities by using PHP programming language and the MySQL database. The results were the following two prototype demos: 1) Risk evaluation module and 2) Vulnerability verification module.

1) Risk Evaluation Module

A. Create Risk Evaluation Data is the step for creating tables and views in database form. This step resulted in the following 15 tables: 1) Main Vulns Table; 2) Risk Desc Table; 3) Business Impact Table; 4) CVSS View; 5) OS View; 6) Solution View; 7) Desc View; 8) MTS View; 9) CVE View; 10) Vuln View; 11) Vuln1 View; 12) Vuln2 View; 13) Summary View; 14) Rep OWASP View and 15) Rep NOWASP (see Appendix B) as shown in Table 4.9.

Table 4.9 Example Vulns Table

No	Name	Type	Collation	Null	Default	Extra
1	no	int(11)		No	None	AUTO_INCREMENT
2	name	text	utf8_general_ci	Yes	NULL	
3	name2	varchar(15)	utf8_general_ci	Yes	NULL	
4	tag	text	utf8_general_ci	Yes	NULL	
5	name3	text	utf8_general_ci	Yes	NULL	
6	port	text	utf8_general_ci	Yes	NULL	
7	svc_name	text	utf8_general_ci	Yes	NULL	
8	protocol	text	utf8_general_ci	Yes	NULL	
9	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	
10	pluginName	text	utf8_general_ci	Yes	NULL	
11	pluginFamily	text	utf8_general_ci	Yes	NULL	
12	description	text	utf8_general_ci	Yes	NULL	
13	fname	text	utf8_general_ci	Yes	NULL	
14	plugin_type	text	utf8_general_ci	Yes	NULL	
15	risk_factor	text	utf8_general_ci	Yes	NULL	
16	solution	text	utf8_general_ci	Yes	NULL	
17	synopsis	text	utf8_general_ci	Yes	NULL	
18	cve	text	utf8_general_ci	Yes	NULL	
19	cvss_base_score	text	utf8_general_ci	Yes	NULL	
20	cvss_vector	text	utf8_general_ci	Yes	NULL	
21	see_also	text	utf8_general_ci	Yes	NULL	
22	metasploit_name	text	utf8_general_ci	Yes	NULL	

B. Create Risk Evaluation Module is the step for creating, writing and debugging function statements. This step resulted in the following nine prototype demos: 1) Vulnerability Assessment Menu; 2) Upload XML Menu; 3) Upload CSV Menu; 4) Add/Edit/Delete Vulnerability Menu; 5) Vulnerability Assessment Report; 6) Show Vulnerability Summary Report; 7) Show Vulnerability Report; 8) Export CSV Vulnerability Report and 9) Print Vulnerability Report as shown in Figure 4.5 - 4.13.

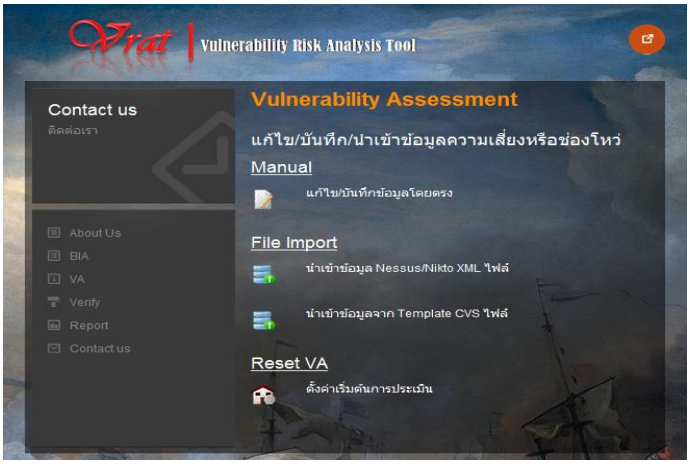


Figure 4.5 Vulnerability Assessment Menus

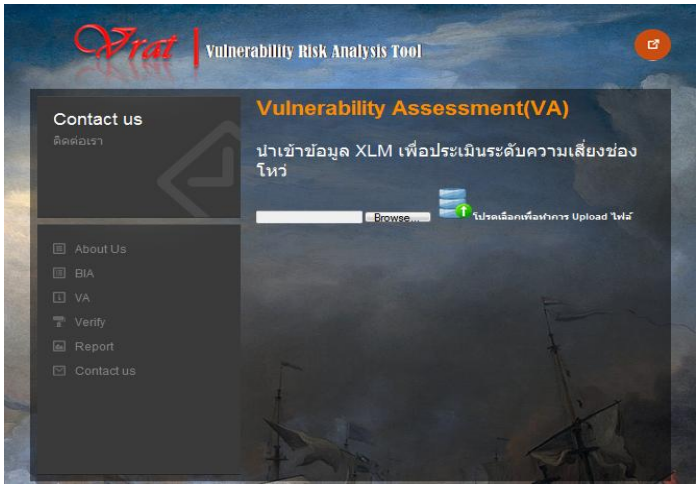


Figure 4.6 Upload XML Menus

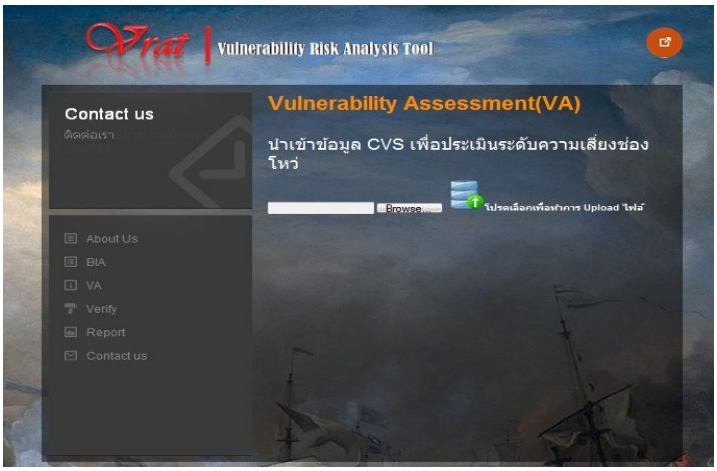


Figure 4.7 Upload CSV Menus

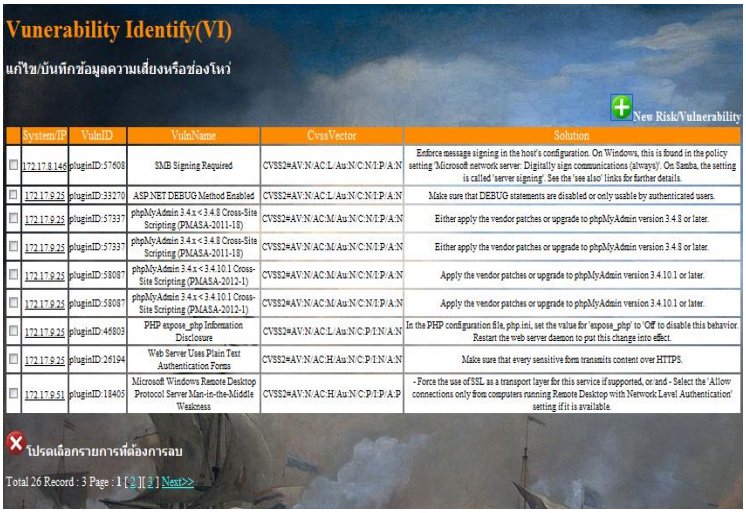


Figure 4.8 Add/Edit/Delete Vulnerability Menus

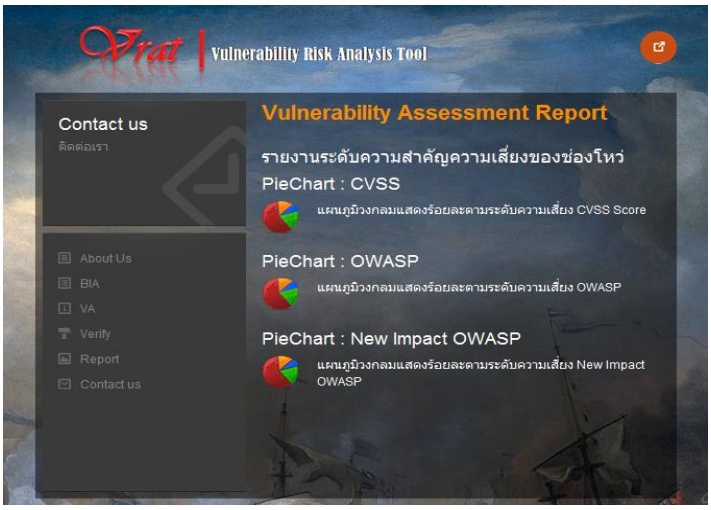


Figure 4.9 Vulnerability Assessment Report

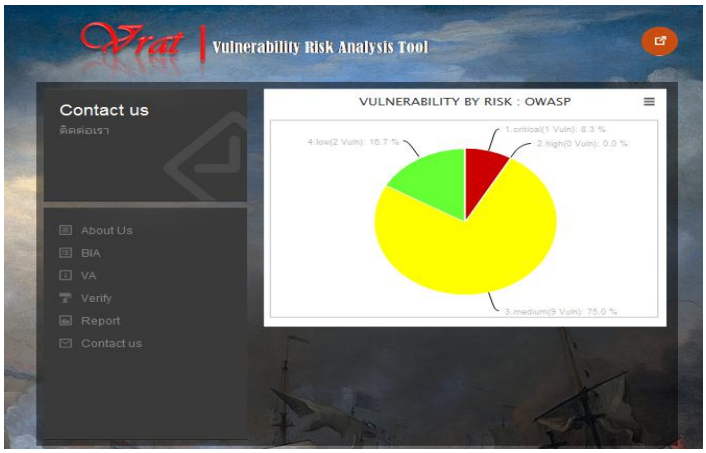


Figure 4.10 Show Vulnerability Summary Report

REPORT : OWASP

Risk	Name	OS	pluginID	pluginName	solution	metasploit_name	see_also	Asset Host
1.critical	gjoynape	Microsoft Windows Server 2003 Service Pack 2	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.	MS12-020 Microsoft Remote Desktop Checker	http://technet.microsoft.com/en-us/security/bulletin/ms12-020	xxx.xxx.xxx.53
3.medium	gjoservi	Microsoft Windows Server 2008 R2	pluginID:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.		http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.25
3.medium	gjoservi	Microsoft Windows Server 2008 R2	pluginID:46803	PHP expose_php Information Disclosure	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.		http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324	xxx.xxx.xxx.25
3.medium	gjoservi	Microsoft Windows Server 2008 R2	pluginID:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later.		http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	xxx.xxx.xxx.25
3.medium	gjoservi	Microsoft Windows Server 2008 R2	pluginID:58081	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later.		http://www.phpmyadmin.net/home_page/security/PMASA-2012-1.php	xxx.xxx.xxx.25

Figure 4.11 Show Vulnerability Report

3.medium	gjoynape	Microsoft Windows Server 2003 Service Pack 2	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.		http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.53
3.medium	gjoynape	Microsoft Windows Server 2003 Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.		http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2828096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.53
3.medium	gjoynape	Microsoft Windows Server 2003 Service Pack 2	pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant			xxx.xxx.xxx.53
4.low	gjoservi	Microsoft Windows Server 2008 R2	pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.			xxx.xxx.xxx.25
4.low	gjoynape	Microsoft Windows Server 2003 Service Pack 2	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant			xxx.xxx.xxx.53

Export

Figure 4.12 Export CSV Vulnerability Report

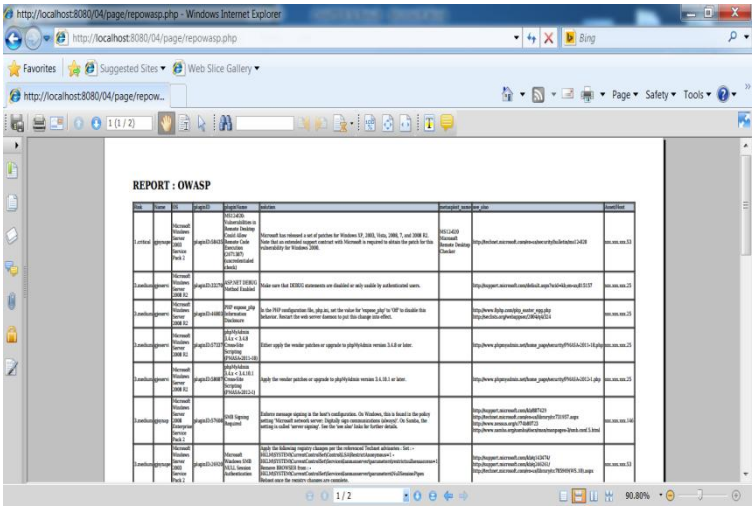


Figure 4.13 Print Vulnerability Report

C. Test/Feedback is the step for confirming bugs and fixing prototypes. This step resulted in the following two processes: 1) checking and confirming bugs and 2) fixing prototype demos as shown in Tables 4.10 and 4.11.

Table 4.10 Check/Confirm Bugs Report (Vuln)

No	Prototype/Function	Test Case	Results	Comment
1	Upload XML	Test import xml files	✓	-
2	Upload CSV	Test import csv template files	✓	-
3	Add/Edit/Delete Vulnerability	Test Add Records/Edit and Delete Record	✓	-
4	Show Vulnerability Summary Report	Test open vulnerability report	✓	-
5	Show Vulnerability Report	Test open vulnerability report	✓	-
6	Export CSV Vulnerability Report	Test export csv files	✓	-
7	Print Vulnerability Report	Test print vulnerability report	✓	-

Table 4.11 Feedbacks and Fixing Prototype Demo Report (Vuln)

No	Prototype/Function	Recommend
1	Upload XML	-
2	Upload CSV	-
3	Add/Edit/Delete Vulnerability	-
4	Show Vulnerability Summary Report	-
5	Show Vulnerability Report	-
6	Export CSV Vulnerability Report	-
7	Print Vulnerability Report	-

D. Integration is the step for combining all prototype demos into a module. This step resulted in the following risk evaluate module as shown in Figure 4.14.

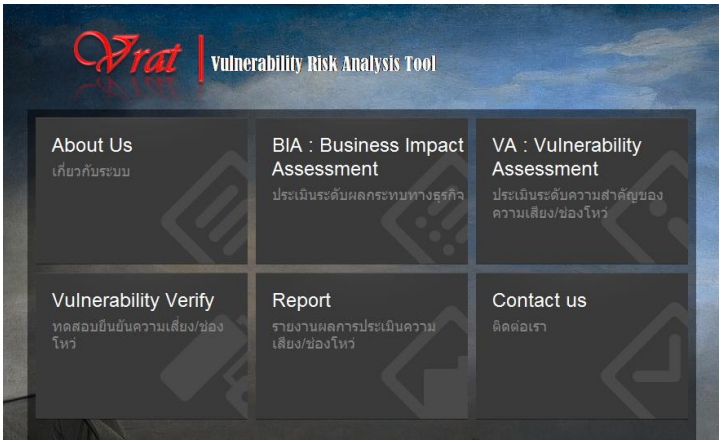


Figure 4.14 Vulnerability Risk Analysis Tool Main Menu

2) Vulnerability verification module

A. Create Vulnerability Verification Data is the step for creating tables and views in database form. This step resulted in the following six tables: 1) Full Disclosure Table; 2) ExploDB Table; 3) Msfvulns Table; 4) Paylo Table; 5) Vmsfall View and 6) Rep_cvss View as shown in Table 4.12 -4.13.

Table 4.12 Example Full-disclosure Table

No	Name	Type	Collation	Null	Default	Extra
1	CVE	varchar(13)	utf8_general_ci	Yes	NULL	
2	FullDisc	varchar(196)	utf8_general_ci	Yes	NULL	
3	Date	varchar(11)	utf8_general_ci	Yes	NULL	
4	Link	varchar(67)	utf8_general_ci	Yes	NULL	

Table 4.13 Example ExploDB Table

No	Name	Type	Collation	Null	Default	Extra
1	EDB_ID	int(5)		Yes	NULL	
2	CVE	varchar(14)	utf8_general_ci	Yes	NULL	
3	file	varchar(42)	utf8_general_ci	Yes	NULL	
4	description	varchar(142)	utf8_general_ci	Yes	NULL	
5	date	int(5)		Yes	NULL	
6	author	varchar(30)	utf8_general_ci	Yes	NULL	
7	platform	varchar(10)	utf8_general_ci	Yes	NULL	
8	type	varchar(7)	utf8_general_ci	Yes	NULL	
9	port	int(5)		Yes	NULL	
10	link	varchar(41)	utf8_general_ci	Yes	NULL	

B. Create Vulnerability Verification Module is the step for creating, writing and debugging function statements. This step resulted in the following four prototype demos: 1) Vulnerability Verification Usage Report Menu; 2) Vulnerability Verification Report Menu; 3) Finding Exploit Code Menu and 4) Changing Exploit Code Menu as shown in Figures 4.15 -4.18.

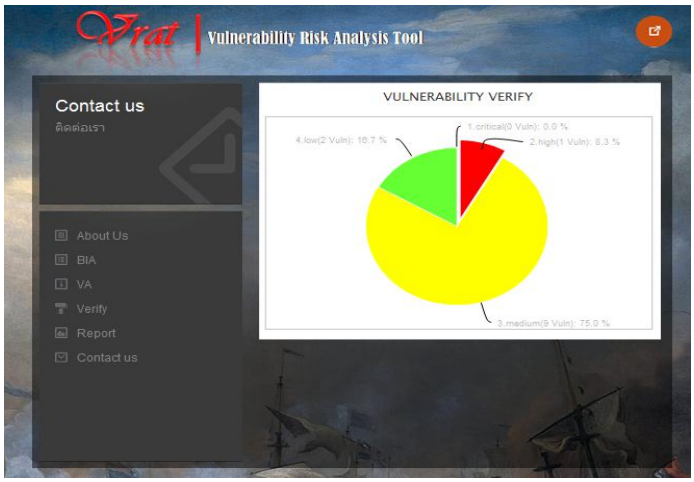
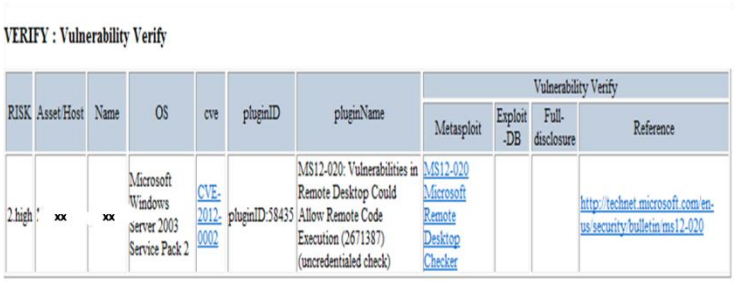


Figure 4.15 Vulnerability Verify Using Report Menu



VERIFY : Vulnerability Verify

RISK	Asset/Host	Name	OS	cve	pluginID	pluginName	Vulnerability Verify			
							Metasploit	Exploit -DB	Full-disclosure	Reference
2.high	xx	xx	Microsoft Windows server 2003 Service Pack 2	CVE-2012-0002	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	MS12-020 Microsoft Remote Desktop Checker			http://technet.microsoft.com/en-us/security/bulletin/ms12-020

Figure 4.16 Vulnerability Verify Report Menu

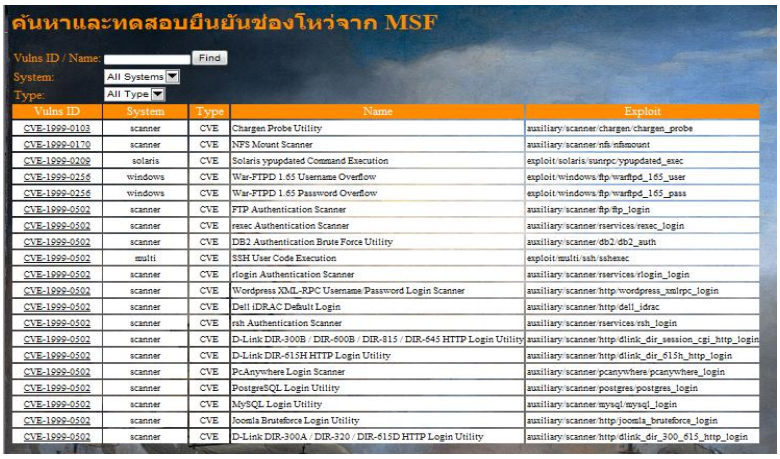


Figure 4.17 Find Exploit Code Menu

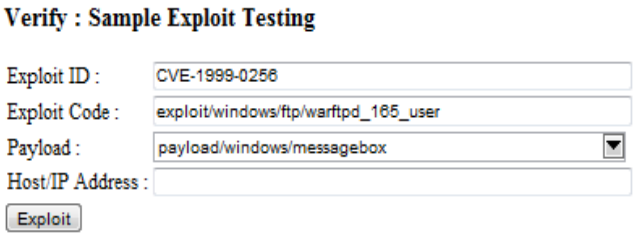


Figure 4.18 Change Exploit Code Menu

C. Test/Feedback is the step for checking, confirming bugs and fixing prototypes. This step resulted in the following two processes: 1) checking and confirming bugs and 2) fixing prototype demos as shown in Tables 4.14 and 4.15.

Table 4.14 Check/Confirm Bugs Report (Vuln)

No	Prototype/Function	Test Case	Results	Comment
1	Vulnerability Verify Report Prototyping	Test select and use exploit code	✓	-
2	Find Exploit Code Prototyping	Test search and use exploit code	✓	-
3	Change Exploit Code Prototyping	Test change and use exploit code	✓	-

Table 4.15 Feedback and Fixing Prototype Demo Report (Verify)

No	Prototype/Function	Recommend
1	Vulnerability Verify Report Prototyping	Add Check Full-Disclosure
2	Find Exploit Code Prototyping	Use MS Windows Exploit code
3	Change Exploit Code Prototyping	-

D. Integration is the step for combining all prototype demos into modules. This step resulted in a vulnerability verification module as shown in Figure 4.19.

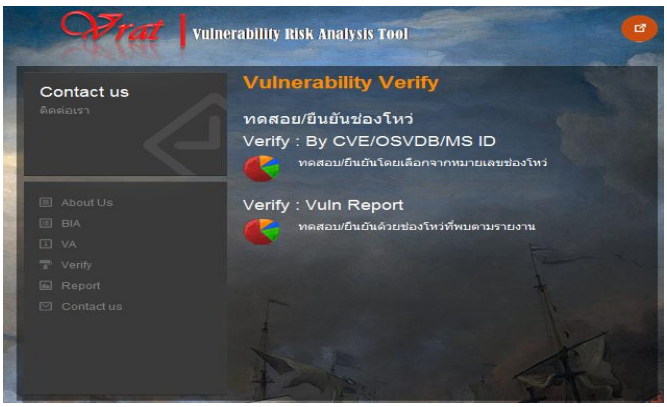


Figure 4.19 Simulation Exploit Prototyping

3) Integration is the step for combining all prototype demos into one prototype tool. This step resulted in security risk evaluation and vulnerability verification tools as shown in Figure 4.20.

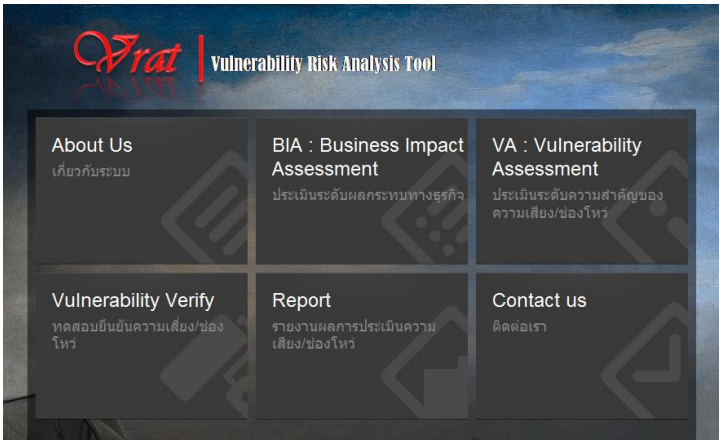


Figure 4.20 Vulnerability Risk Analysis Tool Main Menu

4.3 Utilization and Security Risk Report

4.3.1 Utilization is the step of developing prototype tools used for risk evaluation and confirmation of vulnerabilities samples testing. This step resulted in security risk evaluation, a risk assessment report and a vulnerability verification report. The results of the risk evaluation are shown in about Appendix C. Examples of risk evaluation are shown in the data in Table 4.16 -4.17.

Table 4.16 Risk Evaluate Result Hospital A

NO	Vulnerability	Cvss Vector	Exploit ability	Im pact	Business Impact	NewI mpact	Likh xImp	CVSS	Likhx New Imp	OWASP +	IP
1	ASP.NET DEBUG Method Enabled	CVSS2#AV:N/AC:L /Au:N/C:N/I:P/A:N	9	2.57	4.75	3.42	31	3.medium	32	2.high	xxx.xxx. xxx.25
2	Dell OpenManage Server Administrator omalogin.html DOM-based XSS	CVSS2#AV:N/AC: M/Au:N/C:N/I:P/A: N	7.73	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx. xxx.11
3	FTP Supports Clear Text Authentication	CVSS2#AV:N/AC: H/Au:N/C:P/I:N/A: N	4.44	2.57	3.5	2.86	21	4.low	21	4.low	xxx.xxx. xxx.11
4					4.75	3.42	21	4.low	22	3.medium	xxx.xxx. xxx.25
5	HP System Management Homepage < 7.0 Multiple Vulnerabilities	CVSS2#AV:N/AC:L /Au:N/C:C/I:C/A:C	9	9	4.75	6.64	33	1.critical	33	1.critical	xxx.xxx. xxx.25
6	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities	CVSS2#AV:N/AC:L /Au:N/C:C/I:C/A:P	9	8.59	4.75	6.43	33	2.high	33	1.critical	xxx.xxx. xxx.25
7	HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution	CVSS2#AV:N/AC: M/Au:N/C:C/I:C/A: C	7.73	9	4.75	6.64	33	2.high	33	1.critical	xxx.xxx. xxx.25
8	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	CVSS2#AV:N/AC:L /Au:N/C:C/I:N/A:N	9	6.18	4.75	5.23	33	2.high	32	2.high	xxx.xxx. xxx.25
9	HP System Management Homepage < 7.3 Multiple Vulnerabilities	CVSS2#AV:N/AC: M/Au:N/C:P/I:P/A:P	7.73	5.8	4.75	5.04	32	3.medium	32	2.high	xxx.xxx. xxx.25
10	HP System Management Homepage ginkgosnmp.inc Command Injection	CVSS2#AV:N/AC:L /Au:S/C:C/I:C/A:C	7.16	9	4.75	6.64	33	2.high	33	1.critical	xxx.xxx. xxx.25
11	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	CVSS2#AV:N/AC:L /Au:N/C:P/I:N/A:N	9	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx. xxx.100
12	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC: H/Au:N/C:P/I:P/A:P	4.44	5.8	3.75	4.59	22	3.medium	22	3.medium	xxx.xxx. xxx.100
13	Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L /Au:N/C:P/I:N/A:N	9	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx. xxx.11
14	Multiple Server Crafted Request WEB-INF Directory Information Disclosure	CVSS2#AV:N/AC:L /Au:N/C:P/I:N/A:N	9	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx. xxx.100
15	MySQL Protocol Remote User Enumeration	CVSS2#AV:N/AC:L /Au:N/C:P/I:N/A:N	9	2.57	4.75	3.42	31	3.medium	32	2.high	xxx.xxx. xxx.25
16	Oracle TNS Listener Remote Poisoning	CVSS2#AV:N/AC:L /Au:N/C:P/I:P/A:P	9	5.8	3.75	4.59	32	2.high	32	2.high	xxx.xxx. xxx.100

Table 4.16 Risk Evaluate Result Hospital A (Cont.)

NO	Vulnerability	Cvss Vector	Exploitability	Impact	BusinessImpact	NewImpact	LikhxImp	CVSS	LikhxNewImp	OWASP+	IP
17	PHP < 5.2.10 Multiple Vulnerabilities	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	4.44	5.8	3.5	4.47	22	3.medium	22	3.medium	xxx.xxx.xxx.11
18	PHP < 5.2.11 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	9	5.8	3.5	4.47	32	2.high	32	2.high	xxx.xxx.xxx.11
19	PHP < 5.2.12 Multiple Vulnerabilities	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P	7.73	5.8	3.5	4.47	32	3.medium	32	2.high	xxx.xxx.xxx.11
20	PHP < 5.2.9 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	9	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx.xxx.11
21	PHP < 5.3.11 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	9	5.8	3.5	4.47	32	2.high	32	2.high	xxx.xxx.xxx.11
22	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P	7.73	7.7	3.5	5.42	33	2.high	32	2.high	xxx.xxx.xxx.11
23	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	9	4.45	3.5	3.8	32	3.medium	32	2.high	xxx.xxx.xxx.11
24	PHP < 5.3.9 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	9	5.8	3.5	4.47	32	2.high	32	2.high	xxx.xxx.xxx.11
25	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	9	5.8	3.5	4.47	32	2.high	32	2.high	xxx.xxx.xxx.11
26	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P	7.73	5.8	3.5	4.47	32	3.medium	32	2.high	xxx.xxx.xxx.11
27	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	9	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx.xxx.11
28	PHP expose_php Information Disclosure	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	9	2.57	4.75	3.42	31	3.medium	32	2.high	xxx.xxx.xxx.25
29	PHP Unsupported Version Detection	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	9	9	3.5	6.08	33	1.critical	33	1.critical	xxx.xxx.xxx.11
30	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	7.73	2.57	4.75	3.42	31	3.medium	32	2.high	xxx.xxx.xxx.25
31	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	7.73	2.57	4.75	3.42	31	3.medium	32	2.high	xxx.xxx.xxx.25
32	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	7.73	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx.xxx.11
33	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	9	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx.xxx.146
34					4.75	3.42	31	3.medium	32	2.high	xxx.xxx.xxx.25
35					5.25	3.65	31	3.medium	32	2.high	xxx.xxx.xxx.21
36											xxx.xxx.xxx.27
37											xxx.xxx.xxx.3
38											xxx.xxx.xxx.33
39											xxx.xxx.xxx.35
40											xxx.xxx.xxx.5

Table 4.16 Risk Evaluate Result Hospital A (Cont.)

NO	Vulnerability	Cvss Vector	Exploitability	Impact	BusinesImpact	NewImpact	LikhxImp	CVSS	LikhxNewImp	OWASP+	IP
41	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	4.44	2.57	3.75	2.97	21	4.low	21	4.low	xxx.xxx.xxx.100
42	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	9	4.45	3.75	3.91	32	3.medium	32	2.high	xxx.xxx.xxx.100
43					5.25	4.59	32	3.medium	32	2.high	xxx.xxx.xxx.35
44	SSL Certificate Signed using Weak Hashing Algorithm	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N	4.44	4.45	3.75	3.91	22	3.medium	22	3.medium	xxx.xxx.xxx.100
45	SSL Medium Strength Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx.xxx.100
46	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	3.75	2.97	21	4.low	21	4.low	xxx.xxx.xxx.100
47					4.75	3.42	21	4.low	22	3.medium	xxx.xxx.xxx.25
48					5.25	3.65	21	4.low	22	3.medium	xxx.xxx.xxx.35
49	SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	9	4.45	3.75	3.91	32	3.medium	32	2.high	xxx.xxx.xxx.100
50					5.25	4.59	32	3.medium	32	2.high	xxx.xxx.xxx.35
51	SSL Weak Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx.xxx.100
52	Symantec Backup Exec for Windows Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	9	9	3.75	6.19	33	1.critical	33	1.critical	xxx.xxx.xxx.100
53					5.25	6.86	33	1.critical	33	1.critical	xxx.xxx.xxx.3
54	Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx.xxx.100
55	Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	3.75	2.97	21	4.low	21	4.low	xxx.xxx.xxx.100
56	Unsupported Web Server Detection	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	9	5.8	3.75	4.59	32	2.high	32	2.high	xxx.xxx.xxx.100
57	Web Server Directory Traversal Arbitrary File Access	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	9	2.57	3.75	2.97	31	3.medium	31	3.medium	xxx.xxx.xxx.100
58	Web Server info.php / phpinfo.php Detection	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	9	2.57	3.5	2.86	31	3.medium	31	3.medium	xxx.xxx.xxx.11
59	Web Server Uses Plain Text Authentication Forms	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	4.75	3.42	21	4.low	22	3.medium	xxx.xxx.xxx.25

Table 4.17 Risk Evaluate Result Hospital B

No	Vulnerability	Cvss Vector	Exploitability	Impact	BusinesImpact	NewImpact	LikhxImp	CVSS	LikhxNewImp	OWASP+	IP
1	ASP.NET DEBUG Method Enabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	9	2.57	4	3.09	31	3.medium	32	2.high	xxx.xxx.xxx.33
2	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	4.44	5.8	4	4.7	22	3.medium	22	3.medium	xxx.xxx.xxx.33
3					5	5.15	22	3.medium	22	3.medium	xxx.xxx.xxx.1
4											xxx.xxx.xxx.38
5					5.5	5.37	22	3.medium	22	3.medium	xxx.xxx.xxx.3
6					6.5	5.82	22	3.medium	22	3.medium	xxx.xxx.xxx.13
7											xxx.xxx.xxx.14
8	Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	9	2.57	6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.12
9											xxx.xxx.xxx.13
10											xxx.xxx.xxx.14
11	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	9	9	5	6.75	33	1.critical	33	1.critical	xxx.xxx.xxx.38
12	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	7.73	9	5	6.75	33	2.high	33	1.critical	xxx.xxx.xxx.38
13					6.5	7.43	33	2.high	33	1.critical	xxx.xxx.xxx.13
14											xxx.xxx.xxx.14
15	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	9	2.57	4	3.09	31	3.medium	32	2.high	xxx.xxx.xxx.33
16					5	3.54	31	3.medium	32	2.high	xxx.xxx.xxx.1
17											xxx.xxx.xxx.38
18					5.5	3.76	31	3.medium	32	2.high	xxx.xxx.xxx.3
19					6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.11
20											xxx.xxx.xxx.13
21											xxx.xxx.xxx.14
22											xxx.xxx.xxx.16
23	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	4.44	2.57	6.5	4.21	21	4.low	22	3.medium	xxx.xxx.xxx.13
24											xxx.xxx.xxx.14
25	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	9	4.45	4	4.02	32	3.medium	32	2.high	xxx.xxx.xxx.33
26					5	4.47	32	3.medium	32	2.high	xxx.xxx.xxx.1
27											xxx.xxx.xxx.38
28					5.5	4.7	32	3.medium	32	2.high	xxx.xxx.xxx.3
29					6.5	5.15	32	3.medium	32	2.high	xxx.xxx.xxx.13
30											xxx.xxx.xxx.14

Table 4.17 Risk Evaluate Result Hospital B (Cont.)

No	Vulnerability	Cvss Vector	Exploit ability	Im pact	Busines sImpact	NewI mpact	Likh xImp	CVSS	Likhx NewI mp	OWASP+	IP
31	SSL Certificate Signed using Weak Hashing Algorithm	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N	4.44	4.45	6.5	5.15	22	3.medium	22	3.medium	xxx.xxx.xxx.13
32											xxx.xxx.xxx.14
33	SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	9	2.57	5	3.54	31	3.medium	32	2.high	xxx.xxx.xxx.1
34											xxx.xxx.xxx.38
35					5.5	3.76	31	3.medium	32	2.high	xxx.xxx.xxx.3
36					6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.13
37											xxx.xxx.xxx.14
38	SSL Medium Strength Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.13
39											xxx.xxx.xxx.14
40	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	4	3.09	21	4.low	22	3.medium	xxx.xxx.xxx.33
41					5	3.54	21	4.low	22	3.medium	xxx.xxx.xxx.1
42											xxx.xxx.xxx.38
43					5.5	3.76	21	4.low	22	3.medium	xxx.xxx.xxx.3
44					6.5	4.21	21	4.low	22	3.medium	xxx.xxx.xxx.13
45											xxx.xxx.xxx.14
46	SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	9	4.45	4	4.02	32	3.medium	32	2.high	xxx.xxx.xxx.33
47					5	4.47	32	3.medium	32	2.high	xxx.xxx.xxx.1
48											xxx.xxx.xxx.38
49					5.5	4.7	32	3.medium	32	2.high	xxx.xxx.xxx.3
50					6.5	5.15	32	3.medium	32	2.high	xxx.xxx.xxx.13
51											xxx.xxx.xxx.14
52	SSL Weak Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.13
53											xxx.xxx.xxx.14
54	Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.73	2.57	4	3.09	31	3.medium	32	2.high	xxx.xxx.xxx.33
55					5	3.54	31	3.medium	32	2.high	xxx.xxx.xxx.1
56											xxx.xxx.xxx.38
57					5.5	3.76	31	3.medium	32	2.high	xxx.xxx.xxx.3
58					6.5	4.21	31	3.medium	32	2.high	xxx.xxx.xxx.13
59											xxx.xxx.xxx.14

Table 4.17 Risk Evaluate Result Hospital B (Cont.)

No	Vulnerability	Cvss Vector	Exploit ability	Im pact	Busines sImpact	NewI mpact	Likh xImp	CVSS	Likhx NewI mp	OWASP+	IP
60	Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	4	3.09	21	4.low	22	3.medium	xxx.xxx.xxx.33
61					5	3.54	21	4.low	22	3.medium	xxx.xxx.xxx.1
62											xxx.xxx.xxx.38
63					5.5	3.76	21	4.low	22	3.medium	xxx.xxx.xxx.3
64					6.5	4.21	21	4.low	22	3.medium	xxx.xxx.xxx.13
65											xxx.xxx.xxx.14
66	Web Server Uses Plain Text Authentication Forms	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.44	2.57	4	3.09	21	4.low	22	3.medium	xxx.xxx.xxx.33

4.3.2 The Security Risk Assessment Report is the result of using a prototype tool for creating a risk assessment report. The result was risk assessment as shown in Appendix D. Examples of risk assessment reports are shown in Tables 4.18 -4.19.

1) Risk Assessment Report Hospital A

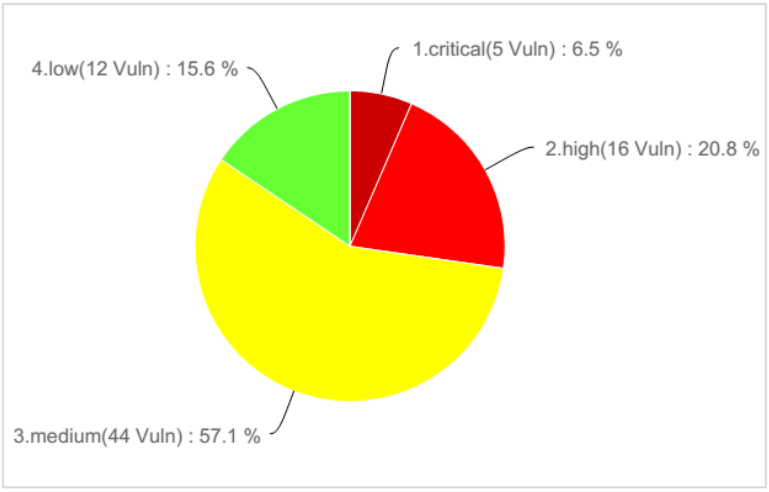


Figure 4.21 Pre- Add Business Impact Factor (CVSS Score)

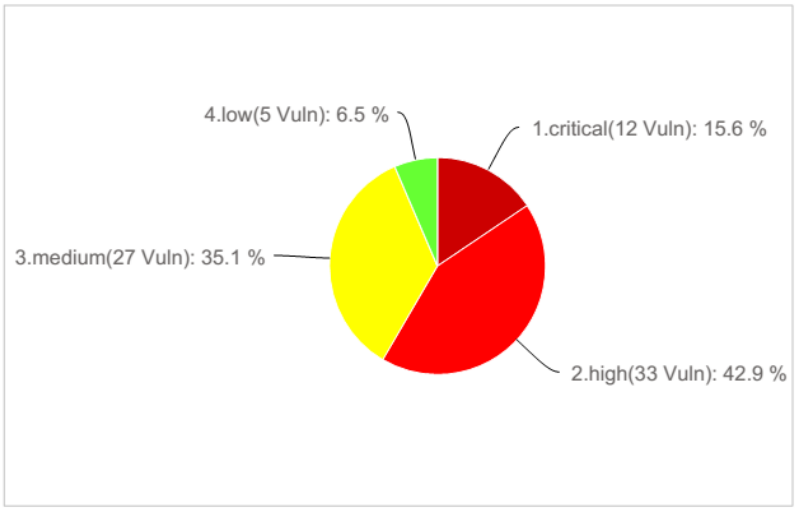


Figure 4.22 Add Business Impact Factor (OWASP + Business Impact)

Table 4.18 Risk Assessment Report Hospital A (CVSS Score)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
1.critical	DB	Microsoft Windows Server 2008 R2 Enterprise SP1	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xxx.3
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginI D:58987	PHP Unsupported Version Detection	Upgrade to a version of PHP that is currently supported.	(blank)	https://wiki.php.net/rfc/releaseprocess	xxx.xxx.xxx.11
		Microsoft Windows Server 2008 R2	pluginI D:58811	HP System Management Homepage < 7.0 Multi Vulnerabilities	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/u?a467ff94	xxx.xxx.xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:58811	HP System Management Homepage < 7.0 Multi Vulnerabilities	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/u?a467ff94	xxx.xxx.xxx.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xxx.100

Table 4.19 Risk Assessment Report Hospital A (OWASP + Business Impact)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
1.critical	DB	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xxx.3
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginI D:58987	PHP Unsupported Version Detection	Upgrade to a version of PHP that is currently supported.	(blank)	https://wiki.php.net/rfc/releaseprocess	xxx.xxx.xxx.11
		Microsoft Windows Server 2008 R2	pluginI D:58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/u?a467ff94	xxx.xxx.xxx.25
			pluginI D:59851	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.1.1 or later.	PHP CGI Argument Injection	http://www.nessus.org/u?541c7466 http://www.securityfocus.com/archive/1/523320/30/0/threaded	xxx.xxx.xxx.25
			pluginI D:66541	HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution	Upgrade to HP System Management Homepage 7.2.0.14 or later.	HP System Management Anonymous Access Code Execution	http://www.nessus.org/u?f2db75ce	xxx.xxx.xxx.25
			pluginI D:70118	HP System Management Homepage ginkgosnmp.inc Command Injection	Upgrade to HP System Management Homepage 7.2.2 or later.	HP System Management Homepage JustGetSNMPQueue Command Injection	http://www.nessus.org/u?81ed4efd http://www.nessus.org/u?9b81af89 http://www.nessus.org/u?7a9cf2bb http://www.securityfocus.com/archive/1/528713/30/0/threaded	xxx.xxx.xxx.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xxx.100

2) Risk Assessment Report Hospital B

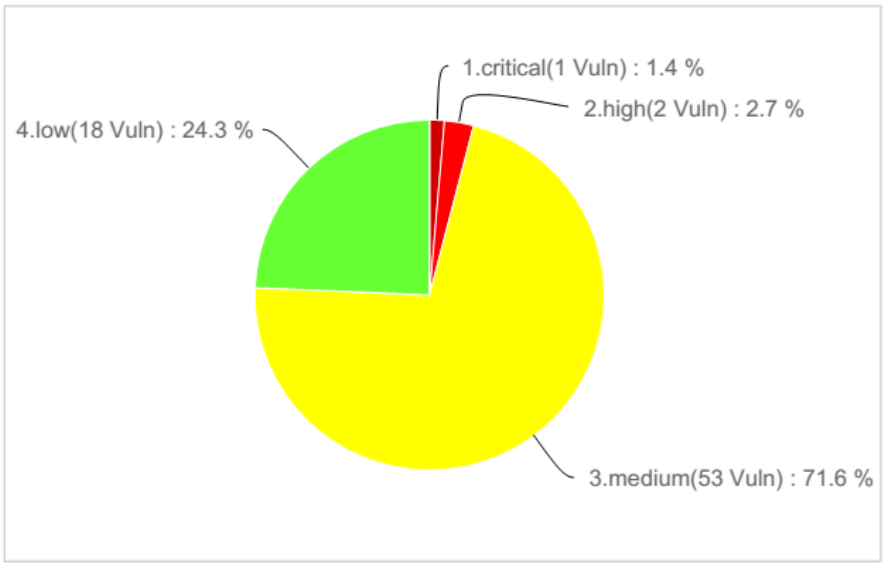


Figure 4.23 Pre- Add Business Impact Factor (CVSS Score)

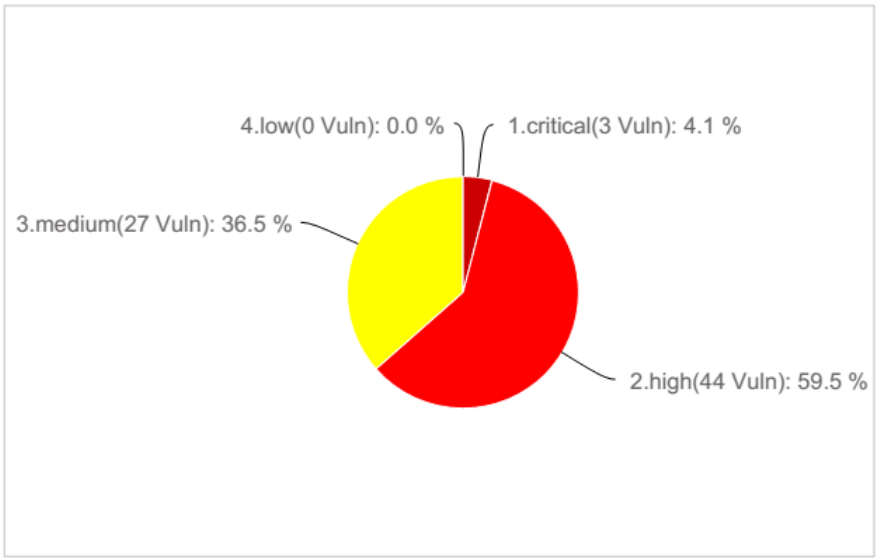


Figure 4.24 Add Business Impact Factor (OWASP + Business Impact)

Table 4.20 Risk Assessment Report Hospital B (CVSS Score)

Risk	name	OS	pluginID	pluginName	solution	metasploit_ name	see_also	IP
1.criti cal	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:4 0887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProvide rCallback() Vulnerability (975497) (uncredentialed check)	Microsoft has released a patch for Windows Vista and Windows Server 2008.	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	http://www.nessus .org/u?0f72ec72 http://technet.micr osoft.com/en- us/security/bulleti n/MS09-050	xxx.xxx. xxx.38

Table 4.21 Risk Assessment Report Hospital B (OWASP + Business Impact)

risk	name	tag	pluginID	pluginName	solution	metasploit_ name	see_also	IP
1.criti cal	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:4 0887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProvide rCallback() Vulnerability (975497) (uncredentialed check)	Microsoft has released a patch for Windows Vista and Windows Server 2008.	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	http://www.nessus .org/u?0f72ec72 http://technet.micr osoft.com/en- us/security/bulleti n/MS09-050	xxx.xxx. xxx.38
			pluginID:5 8435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.co m/en- us/security/bulletin/ms12- 020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx. xxx.38
	pacsc cc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:5 8435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.co m/en- us/security/bulletin/ms12- 020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx. xxx.13

4.3.3 Vulnerability Verification Results involve the use of a prototype tool for reviewing full disclosure/references or samples of exploit testing. The result was verification of the vulnerability results shown in Appendix E. And examples of verification of the vulnerability results are shown in Tables 4.22 -4.23.

Table 4.22 Verify Vulnerability Result Hospital A

cvss	Owasp+	PlugInID	PluginName	Full-Disclosure / Referances				Exploit
				See_also	Fulldisc	Fullink	Exdbink	Metasploit_name
1.critical	1.critical	pluginID:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	NULL	NULL	NULL	NULL
		pluginID:58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities	http://www.nessus.org/u?a467ff94	NULL	NULL	NULL	Apache Reverse Proxy Bypass Vulnerability Scanner
		pluginID:58987	PHP Unsupported Version Detection	https://wiki.php.net/rfc/releaseprocess	NULL	NULL	NULL	NULL
2.high	1.critical	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	http://technet.microsoft.com/en-us/security/bulletin/ms12-020	NULL	NULL	NULL	MS12-020 Microsoft Remote Desktop Checker
		pluginID:70118	HP System Management Homepage ginkgosnmp.inc Command Injection	http://www.nessus.org/u?81ed4efd http://www.nessus.org/u?9b81af89 http://www.nessus.org/u?7a9cf2bb http://www.securityfocus.com/archive/1/528713/30/0/threaded	NULL	NULL	NULL	HP System Management Homepage JustGetSNMPQueue Command Injection

Table 4.23 Verify Vulnerability Result Hospital B

cvss	Owasp+	PlugInID	PluginName	Full-Disclosure / Referances				Exploit
				See_also	Fulldisc	Fullink	Exdbink	Metasploit_name
1.critical	1.critical	pluginID:40887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	http://www.nessus.org/u?0f72ec72 http://technet.microsoft.com/en-us/security/bulletin/MS09-050	FULLDISC:20090907 Windows Vista/7 : SMB2.0 NEGOTIATE PROTOCOL REQUEST Remote B.S.O.D.	http://seclists.org/fulldisclosure/2009/Sep/date.html	NULL	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
2.high	1.critical	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	http://technet.microsoft.com/en-us/security/bulletin/ms12-020	NULL	NULL	NULL	MS12-020 Microsoft Remote Desktop Checker

4.3.4 30+ Samples of Microsoft Security Bulletins on Vulnerability Testing are a result of the use of the prototype tool to sample exploitation testing. The result was sample testing as shown in Table 4.24 and Figures 4.25 – 4.32.

Table 4.24 Sample 30+ Microsoft Security Bulletins Published

No	TypeExploit	WIN	ExploitID	ExploitCode	Actions/Results
1	Overflow	2000	MSB-MS00-094	exploit/windows/isapi/ms00_094_pbserver	add user
2			MSB-MS01-023	exploit/windows/iis/ms01_023_printer	add user
3			MSB-MS03-007	exploit/windows/iis/ms03_007_ntdll_webdav	add user
4			MSB-MS04-011	exploit/windows/smb/ms04_011_lsass	add user
5			MSB-MS04-007	exploit/windows/smb/ms04_007_killbill	meterpreter
6			MSB-MS05-039	exploit/windows/smb/ms05_039_pnp	add user
7			MSB-MS06-040	exploit/windows/smb/ms06_040_netapi	add user
8		2000 SevS P4	MSB-MS03-022	exploit/windows/isapi/ms03_022_nsiislog_post	meterpreter
9			MSB-MS04-045	exploit/windows/wins/ms04_045_wins	add user
10			MSB-MS10-025	exploit/windows/mmsp/ms10_025_wmss_connect_funnel	add user
11		2000 SP4	MSB-MS05-017	exploit/windows/dcerpc/ms05_017_msmq	meterpreter
12		2003	MSB-MS03-026	exploit/windows/dcerpc/ms03_026_dcom	add user
13			MSB-MS09-053	exploit/windows/ftp/ms09_053_ftpd_nlst	Auxiliary module execution completed (FTP services loss)
14		XP	MSB-MS03-049	exploit/windows/smb/ms03_049_netapi	calling the vulnerable function
15			MSB-MS06-066	exploit/windows/smb/ms06_066_nwapi	CSNW not start
16				exploit/windows/smb/ms06_066_nwwks	CSNW not start
17	Bypass something	2000	MSB-MS08-067	exploit/windows/smb/ms08_067_netapi	add user
18			MSB-MS10-065	auxiliary/admin/http/iis_auth_bypass	Auxiliary module execution completed (no basic authentication enabel)
19		2003	MSB-MS09-020	auxiliary/scanner/http/dir_webdav_unicode_bypass	Scan completed
20				auxiliary/scanner/http/ms09_020_webdav_unicode_bypass	Scan completed

Table 4.24 Sample 30+ Microsoft Security Bulletins Published (Cont.)

No	TypeExploit	WIN	ExploitID	ExploitCode	Actions/Results
21	Code Execution	2000	MSB-MS01-026	exploit/windows/iis/ms01_026_dbldecode	* Executing cmd: copy cmd.exe to web root/script as xxx.exe
22		VISTA	MSB-MS09-050	auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh	*send eploit packet 858 byte
23				exploit/windows/smb/ms09_050_smb2_negotiate_func_index	[*] Auxiliary module execution completed (dos ok)
24			MSB-MS11-030	auxiliary/dos/windows/llmnr/ms11_030_dnsapi	Auxiliary module execution completed wait 5 minin
25		XP	MSB-MS12-020	auxiliary/scanner/rdp/ms12_020_check	*scan completed
26			MSB-MS10-061	exploit/windows/smb/ms10_061_spoolss	add user
27			MSB-MS06-070	exploit/windows/smb/ms06_070_wkssvc	calling the vulnerable function
28			MSB-MS02-065	exploit/windows/iis/ms02_065_msadc	started bind handler
29	DoS	2000	MSB-MS02-063	auxiliary/dos/pptp/ms02_063_pptp_dos	Auxiliary module execution (dos complate)
30			MSB-MS05-047	auxiliary/dos/windows/smb/ms05_047_pnp	Auxiliary module execution completed (systems shutdow)
31			MSB-MS06-035	auxiliary/dos/windows/smb/ms06_035_mailslot	Auxiliary module execution completed
32			MSB-MS06-063	auxiliary/dos/windows/smb/ms06_063_trans	Auxiliary module execution completed (Exploit susscess)
33		2003	MSB-MS09-053	auxiliary/dos/windows/ftp/iis_list_exhaustion	Auxiliary module execution completed (FTP services loss)
34			MSB-MS12-020	auxiliary/dos/windows/rdp/ms12_020_maxchannelids	*Auxiliary module execution completed (dos ok)
35		VISTA	MSB-MS09-001	auxiliary/dos/windows/smb/ms09_001_write	[*] Auxiliary module execution completed
36			MSB-MS09-050	auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff	[*] Auxiliary module execution completed (dos ok)

4.3.5 Simulated Exploit Attack by using the prototype tool in the sample, 30+ Microsoft Security Bulletins. The testing results are divided into the following four methods: 1) Denial of Service; 2) Code Execution; 3) Buffer Overflows and 4) Bypass Something.

1) Denial of service (DoS): The server or system can be stopped in order to prevent or disrupt a system. The results from the examination of the prototype tool are shown in Figures 4.25 – 4.26.

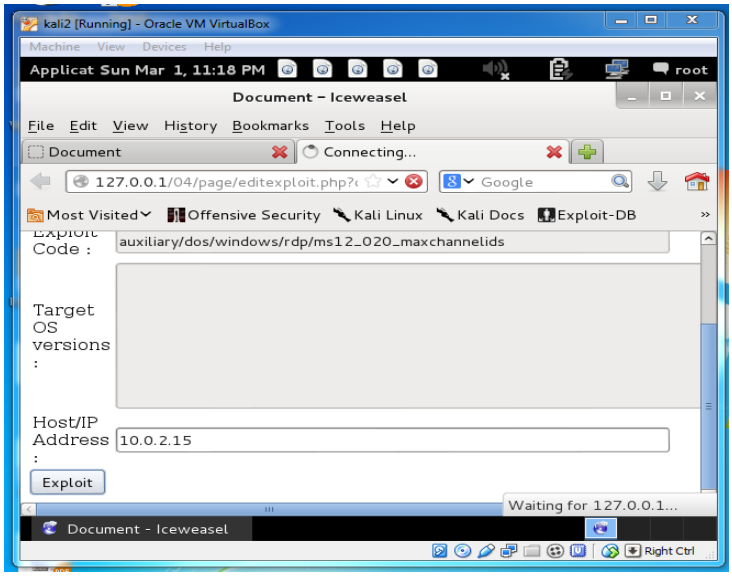


Figure 4.25 Sampling DoS Exploit ID MS12-020 in Window 2003

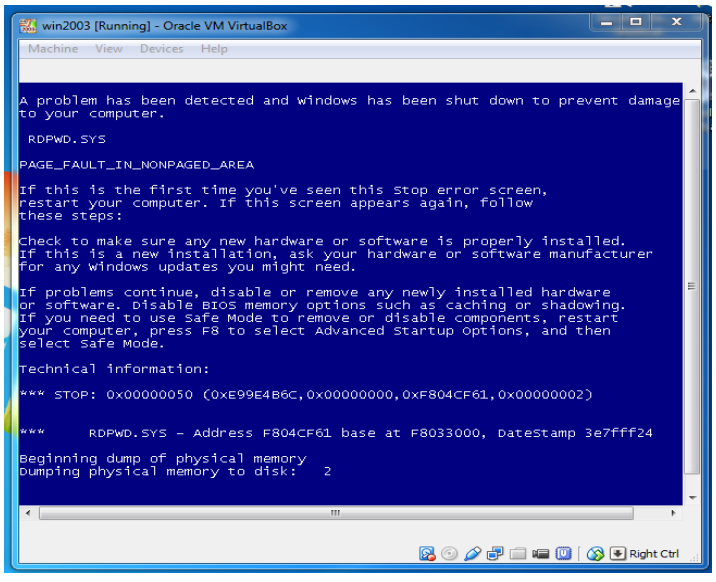


Figure 4.26 Result Exploit ID MS12-020

2) Code Execution: The attacker can send malicious commands through an operating system's vulnerability in order to enable an attacker to take control of the server, including installation, view or editing of the information and creation of an account on the server. The results from the examination of the prototype tool are shown in Figures 4.27 – 4.28.

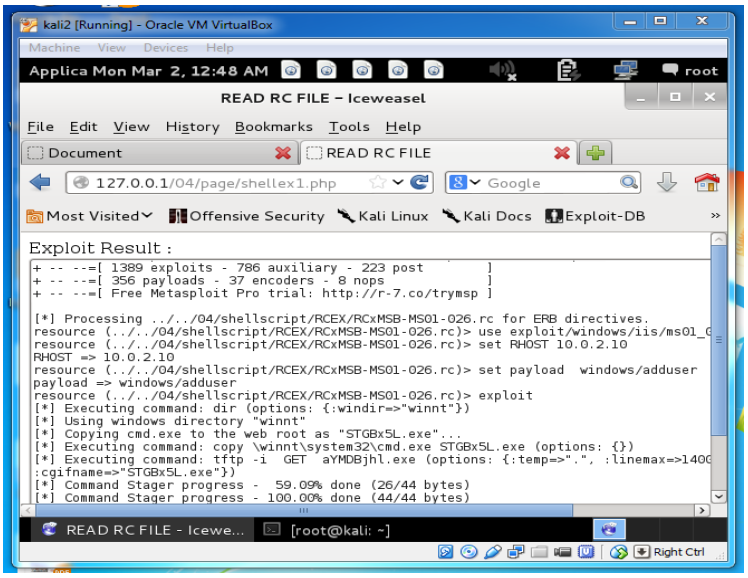


Figure 4.27 Sampling Execute Code Exploit ID MS01-026 in Window 2000

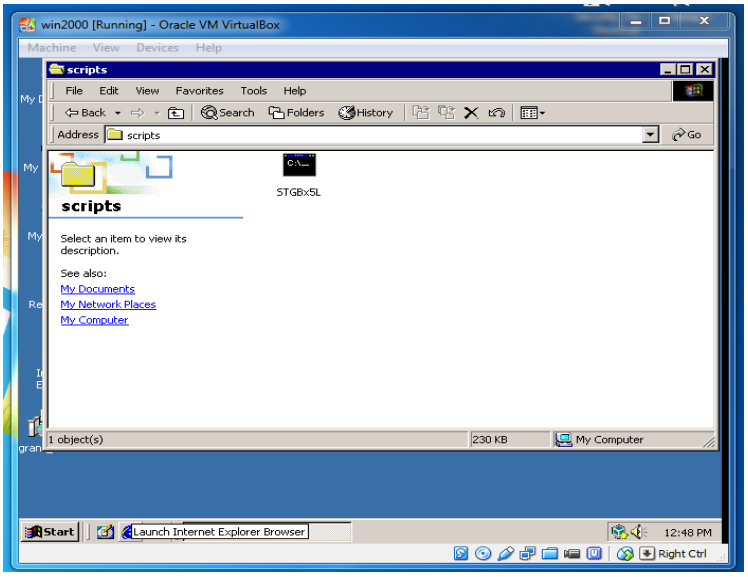


Figure 4.28 Result Exploit ID MS01-026

3) Buffer overflows: The input is greater than the extent to which the program is backed up. As a result, the server or system can be stopped. The results from the examination of the prototype tool are shown in Figures 4.29 – 4.30.

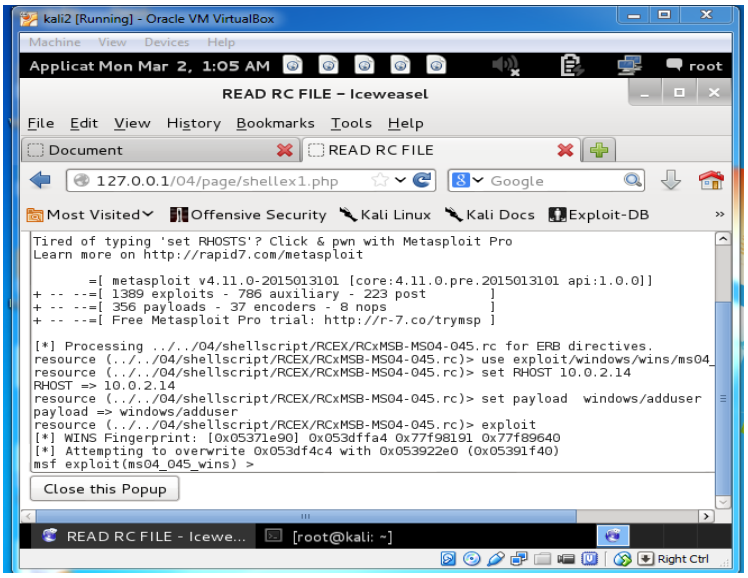


Figure 4.29 Sampling Overflow Exploit ID MS04-045 in Window XP

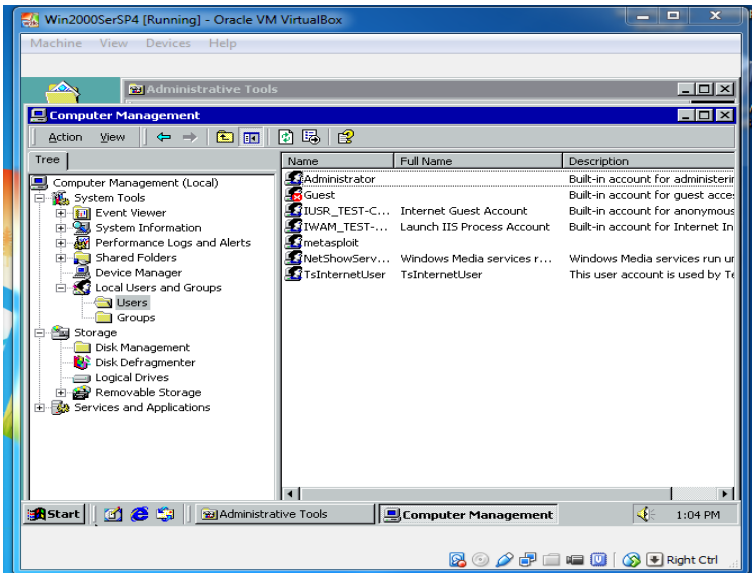


Figure 4.30 Result Exploit ID MS04-045

4) Authentication bypass: Pass the system's vulnerability without having to go through identity verification. The results from the examination of the prototype tool are shown in Figures 4.31 – 4.32.

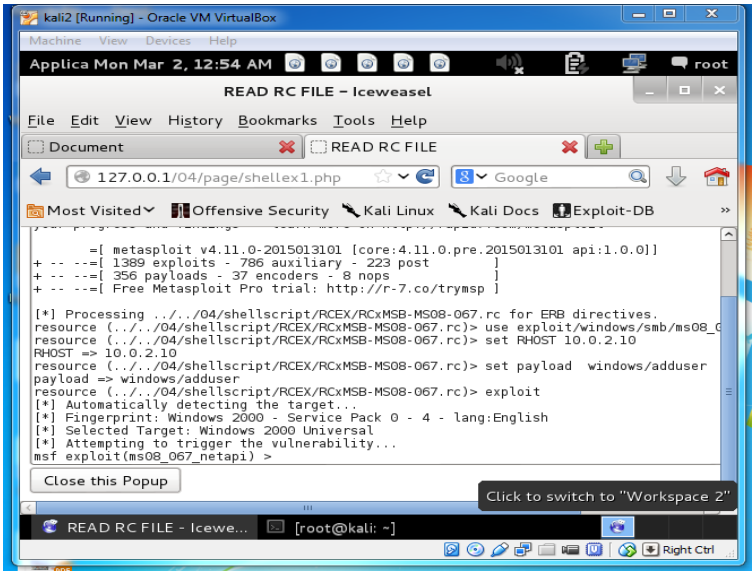


Figure 4.31 Sampling Overflow Exploit ID MS08-067 in Window 2000

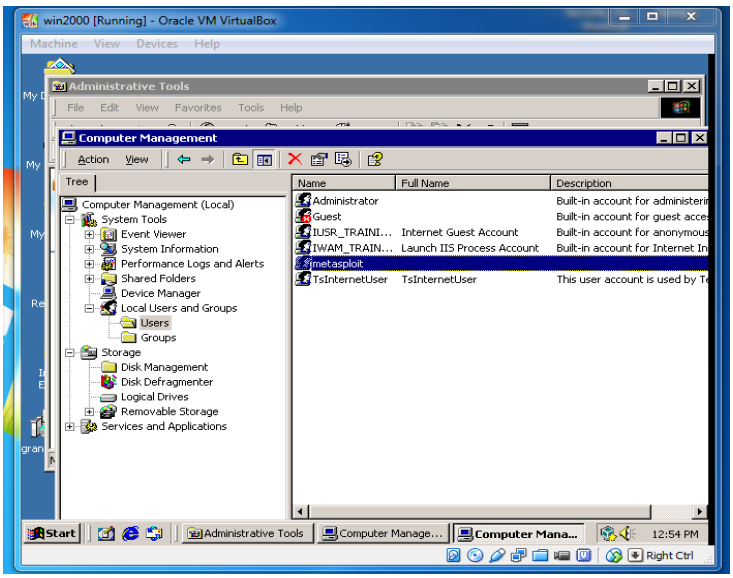


Figure 4.32 Result Exploit ID MS08-067

CHAPTER V
DISCUSSION

The security assessment in Chapter 4 experimented with the prototyping tools to support risk assessment, and the tests confirmed the vulnerability (Vulnerability Verification). The risk evaluation results on the information security level of hospital case studies found the risk assessment of the two hospitals in the study to be suitable with the environments of the case study hospitals. Before increasing business impact, Hospital A had a moderate risk level. After the increase in business impact, the risk level was also found to be at a moderate level. For Hospital B, the increase in business impact before increasing the risk level was moderate. After increasing the business impact, however, the risk level was found to be high as shown in Figures 5.1 and 5.2.

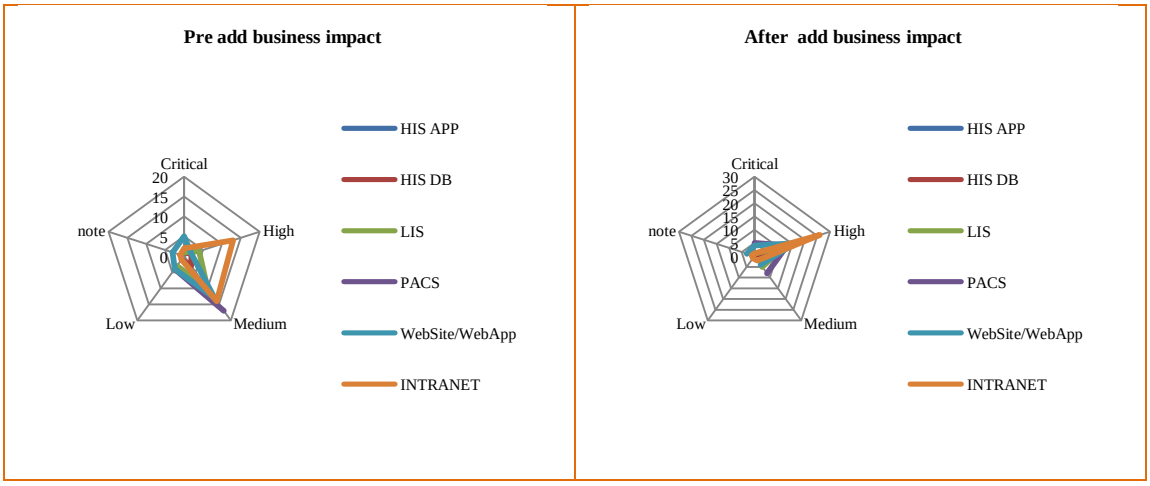


Figure 5.1 Security Rating Hospitals A

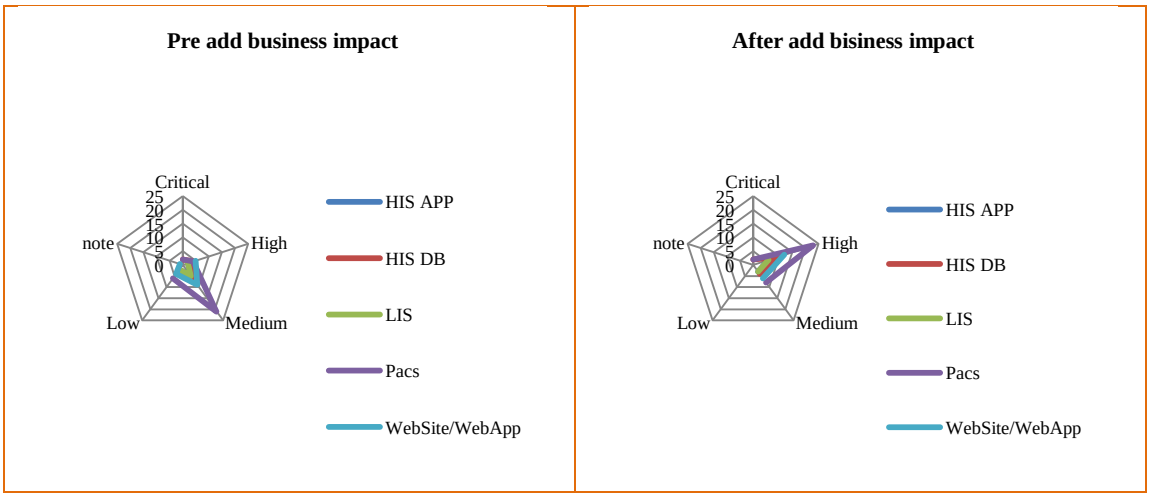


Figure 5.2 Security Rating Hospitals B

5.1 Identify IT Systems and Business Impact

This research determined the business impact factors of information technology systems by assessment methods based on standard guidelines (OWASP business impact rating) to assess the business impact score by case study on hospital information systems administered for assessing the impact level suitable for the actual environment of the hospitals. The results obtained from the assessment of the business impacts are represented in Table 5.1.

Table 5.1 Business Impact Rating

Asset/Systems (Target)		Impact Factor Rating				Impact Rating
		Financial damage	Reputation damage	Non-compliance	Privacy violation	
Hospital A	APPLICATIONS SERVER	7	5	2	7	5.25
	DATABASE SERVER	7	5	2	7	5.25
	WEB	3	9	2	5	4.75
	LIS	3	5	2	5	3.75
	PACS	3	5	2	5	3.75
	INTRANET	3	4	2	5	3.50
Hospital B	PACS	7	5	7	7	6.5
	LIS	3	5	7	7	5.5
	HIS	1	5	7	7	5
	Txxx-Registry Website	1	1	7	7	4
	Tele-redio Website	1	1	7	7	4

5.2 Risk Evaluation

5.2.1 The risk evaluation by OWASP Risk Rating Methodology can be evaluated by comparing opportunity factors with likelihood for impact.

The likelihood is a potential event estimating the trend of a threat agent and vulnerability based on factors such as skill level, motive, ease of discovery and the ease of exploitation, etc.

The impact is the level of effects occurring if the attack/exploit is successful, which can be evaluated based on business and technical impact factors based on damage to information systems such as breaches in confidentiality, integrity, availability and accountability, etc.

As the above risk evaluation used judgment of the evaluators, the risk may not have been specified properly. Thus, the researcher selected the impact value and used exploitability calculated based on the CVSS vector as the impact value. The researcher then used exploitability as the likelihood value to simulate a calculation prototyping model template for development which might have remained inappropriate. To increase accuracy in future risk assessment, the likelihood value should be leveled by collecting the occurrence/threat frequency statistics to be implemented/improved in the risk assessment model for other further researches.

5.2.2 The prototyping tools developed in accordance with Chapter 4 supported the result files from the vulnerability scan tool supporting only the CVSS score. And the Information Technology Security Evaluation of the prototyping tool used a basic format in accordance with the OWASP risk assessment rating by leveling the impact results, opportunities and risk priorities. The details are shown in Tables 3.13-3.14.

Table 3.13 OWASP Risk Level Matrix

Overall Risk Severity				
Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Note	Low	Medium
		Low	Medium	High
	Likelihood			

Table 3.14 OWASP Risk Level Definition

Risk Level	Definition
CRITICAL	Website / Web applications / Host computer may be attacked by intruders. And control information system completely. If the vulnerability assessment Or vulnerabilities that did not make the correction.
HIGH	Website / Web applications / Host computer may be attacked by intruders. And control information system If the vulnerability assessment Or vulnerabilities that did not make the correction.
MEDIUM	Website / Web applications / Host computer may be the attackers stole information from the target device to take advantage. Or modification sensitive information
LOW	Website / Web applications / Host computer provides information that is useful to attacks from intruders.

However, using the exploitability value instead of the likelihood value (likelihood) to evaluate the risk level may be simulated as a model calculation in the tool template for development. A new impact score was calculated by using business impact to adjust the score level for compatibility with the environment of the information technology function. The prototyping tools showed the risk levels in both pre- and post business impact adding.

5.3 Vulnerability Verification

In the vulnerability verification process developed in accordance with Chapter 4, the sample prototyping model was tested to verify the vulnerability of the Microsoft Windows operating system by using the Metasploit command line (msfcli) and reliable reference source examples were searched and verified. The verification results are shown in Chapter 4.3.3 and 4.3.4. Moreover, if the prototyping tool is needed for actual use, the tool should have more references for completeness and remaining up-to-date on a regular basis.

CHAPTER VI
CONCLUSION AND RECOMMENDATIONS

This chapter summarizes the results of all research stages and can be divided into the following two parts: 1) Conclusion and 2) Recommendations.

6.1 Conclusion

This research evaluated the information security of the case studies by using a prototyping tool that supported the risk evaluation and vulnerability verification of the tool to be developed by applying the best practices of security and IT risk assessment. The experimental data imported from the vulnerability scan results were used to add/adjust the score levels of business impact factors in the case study hospitals. According to the findings, the prototyping tool was able to re-order the levels of information security with consistent reflection of the environments at the case study hospitals. The prototyping tool was also able to obtain an assessment report and a security report with recommendations (risk assessment report) in order to consider security information improvement. Moreover, the prototyping tool was able to imitate, exploit test and display reliable reference sources. The risk assessment report is shown in Chapter 4.3.2 and the vulnerability verification is shown in Chapter 4.3.4 and 4.3.5.

6.2 Recommendation

6.2.1 Vulnerability Assessment - The prototyping tool was developed by using OWASP risk rating methodology and adjusted by business impact factors obtained from the questionnaire completed by the case study hospitals' IT security

staff. If the function preferred appropriation, the function was able to add more factors, including opportunity factors. The researcher used the impact score and exploitability usage calculated based on the CVSS vector as the impact value. The exploitability usage was applied instead of likelihood for imitation as a prototyping tool for development which might be inappropriate. To increase accuracy in risk assessment, further assessment should set more scoring levels on opportunity factors by collecting the frequency statistics of the event/threat actually occurring to implement/improve the risk assessment model for future research.

6.2.2 Vulnerability Verification - This tool supports the Metasploit command line (msfcli) and reliable full disclosure references. In the vulnerability verification process, the tool was able to verify the limit reference sources. For more complete verification results, full disclosure or reference websites should be added or updated.

6.2.3 Limitations - This research selected the results of vulnerability scan tools only supporting the standards of the Common Vulnerability Scoring System (CVSS). However, there are other tools that do not support CVSS such a the Open Source Vulnerability Database (OSVDB), Common Vulnerabilities and Exposures (CVE) etc. Although the function can use imported CSV templates, it needs to be done with searching and configuration of the CVSS Vector. The necessary data field for calculation of the priority risks are ranked according to the defined format.

REFERENCES

1 Compilation Of The Social Security Laws, http://www.ssa.gov/OP_Home /ssact/title11/1171.htm, accessed on Jul. 25, 2014.

2 The Health Information Technology for Economic and Clinical Health Act (HITECH) Act, January 6, 2009.

3 HIMSS Electronic Health Record Definitional Model Version 1.0, http://healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference, January 4, 2011.

4 HIMSS Electronic Health Record Definitional Model Version 1.0, HIMSS EHR Committee, June 9, 2003.

5 D. Garets and M. Davis, Electronic Patient Records, Healthcare Informatics online , October, 2005.

6 The conceptual framework of interoperable electronic health record and ePrescribing systems Version 1.0, DG INFSO and Media, April, 2008.

7 ProtectingPersonalHealth InformationinResearch: Understandingthe HIPAAPrivacy Rule, Department of Health and Human Services, April 14, 2003.

8 ISO 27799:2008(E) Health informatics - Information security management in health using ISO/IEC 27002,ISO, 2008

9 HA-SPA(Standards Practice Assessment), Healthcare Accreditation Institute (Public Organisation), October, 2009.

10 Hospital IT Quality Improvement Framework (HITQIF), Thai Medical Informatics Association, March 15, 2012.

11 P. Chanyagorn and B. Kungwannarongkun. ICT Readiness Assessment Model for Public and Private Organizations in Developing Country. International Journal of Information and Education Technology, Vol. 1, No. 2, June, 2011

12 S. Dynes, S. Pixley, and D. Madory,Managing Risk of IT Disruptions in HealthcareSettings: A Continuity of Operations Planning Process, in Proc. the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th, 2009.

13 P. Chaitasanangam, Risk Analysis and Security Management of IT Information in Hospital., in Proc. the 2nd National and International Graduate Study Conference; 2012 May 10-11; Bangkok, Thailand, 2012.

14 S. Tritilanunt and A. Tongsrisomboon, Risk Analysis and Security Management of IT Information in Hospital, 2014.

15 ISMS-201 IT Risk Management Standard Version 2.0,ISO, 2012.

16 G. Stoneburner, A. Goguen, and A. Feringa, Risk Management Guide for Information Technology System, National Institute of Standards and Technology, july, 2002.

17 OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008.

18 HIPAA Security Procedures Resource Manual, North Dakota State University (NDSU),September, 2012.

19 K. Graves, Certified Ethical Hacker STUDY GUIDE , Wiley Publishing, Inc,2010.

20 K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, Technical Guide to Information Security Testing and Assessment, the National Institute of Standards and Technology (NIST), September, 2008.

21 Information Systems Security Assessment Framework (ISSAF) draft 0.2.1b, Open Information Systems Security Group, May 01,2006.

22 PTES Technical Guidelines,the Penetration Testing Execution Standard, 2012.

23 Conducting a Penetration Test on an Organization, SANS Institute InfoSec Reading Room, SANS Institute, 2002.

24 Common Vulnerability Scoring System, http://www.first.org/cvss accessed on August 6, 2014.

25 OSVDB Synopsis ,http://osvdb.org/ , accessed on August 6, 2014.

26 About CVE, https://cve.mitre.org/ , accessed on August 6, 2014.

27 P. Mell, K. Scarfone, and S. Romanosky, “CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0”, National Institute of Standards and Technology, June 2006.

28 Information Assurance Tools Report – Vulnerability Assessment, Information Assurance Technology Analysis Center (IATAC),Sixth Edition, ,May 2, 2011.

29 A.G. Bacudio, X. Yuan, B.T. Bill Chu, and M. Jones , AN OVERVIEW OF PENETRATION TESTING, Dept. of Computer Science, North Carolina A&T StateUniversity, Greensboro, North Carolina, USA,in Proc. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

30 Nessus user guide,http://static.tenable.com/documentation /nessus_5.0_user_guide.pdf, April 22, 2013.

31 Nikto v2.1.5 - The Manual, http://www.cirt.net/nikto2-docs/index.html, November, 2007.

32 Metasploit Framework User Guide., http://66.14.166.45/whitepapers/netforensics /crafting/Metasploit%20Framework%20User%20Guide%20Version%203. 2.pdf, accessed on Jul. 25, 2014.

33 Nbtstat Command for DOS and Windows, http://www.comentum.com /nbtstat.html, accessed on Jul. 25, 2014.

34 Enumeration tools, http://home.ubalt.edu/abento/753/enumeration /enumerationtools.html, accessed on Jul. 25, 2014.

35 Microsoft DOS nslookup command, http://www.computerhope.com/nslookup.htm, accessed on Jul. 25, 2014.

36 Linux / Unix Command: dig, http://linux.about.com/od/commands/l /blcmdl1_dig.htm, accessed on Jul. 25, 2014.

37 Whois, http://www.whois.net/, accessed on Jul. 25, 2014.

38 Nmap Reference Guide, http://nmap.org/book/man.html, accessed on August 6, 2014.

39 Fulldisclosure, http://seclists.org/fulldisclosure/, accessed on August 6, 2014.

40 Exploitdb, https://twitter.com/exploitdb, accessed on August 6, 2014.

APPENDICES

APPENDIX A
PROTYPE DESIGN

Prototype Design was 19 prototype models that is 1) Brow and Choose File, 2) Import Data, 3) Result upload / Show Data, 4) Insert Data, 5) Change Data, 6) Delete Data, 7) Show Data, 8) Find Data, 9) Decompose Data, 10) Estimate Data, 11) Calculate Risk Value, 12) Risk Rating Mapping, 13) Show Report, 14) Export Data, 15) Print Report, 16) Details Reference, 17) Detail Exploit Code, 18) Change Details, and 19) Testing Sample following: Figure A-1 to A-15

1. Brow and Choose File Function is the method of choose XML or CSV Text file and read data into string data.

2. Import Data Function is the method of insert string data into database.

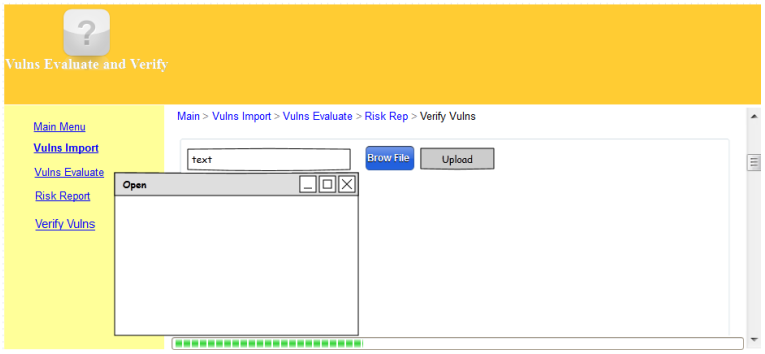


Figure A-1 Brow and Choose File and Import Data Prototyping

3. Result upload Function is the method of show import results .

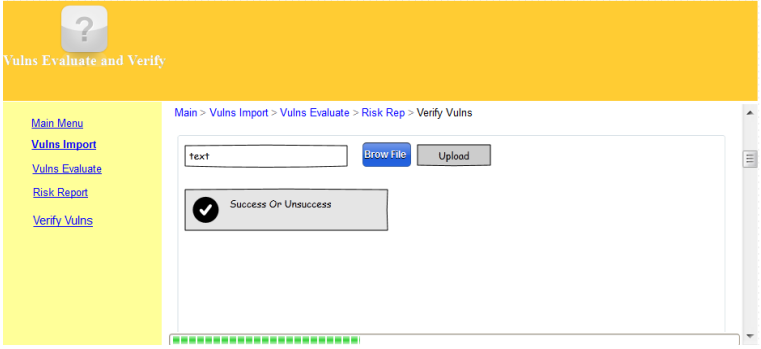


Figure A-2 Result upload Prototyping

4. Insert Data Function is the method of input data in text values and insert data into database.

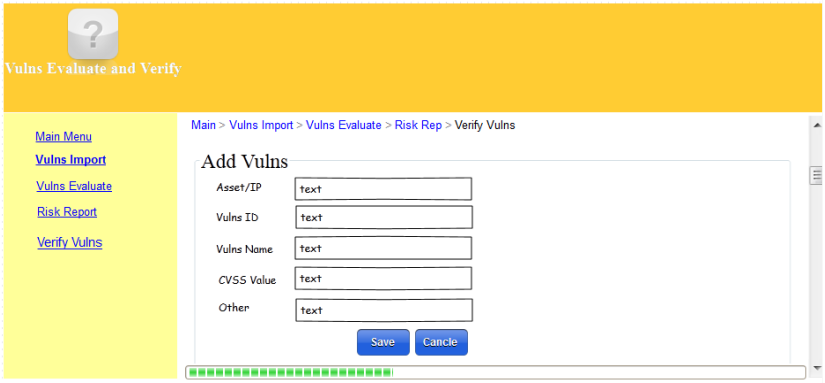


Figure A-3 Insert Data Prototyping

5. Delete Data Function is the method of find, and select records and delete data in database.

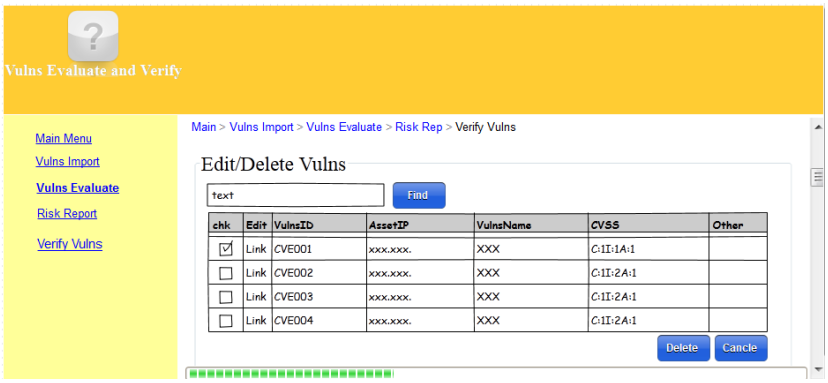


Figure A-4 Delete Data Prototyping

6. Change Data Function is the method of find, and select record and change text values and update data in database.

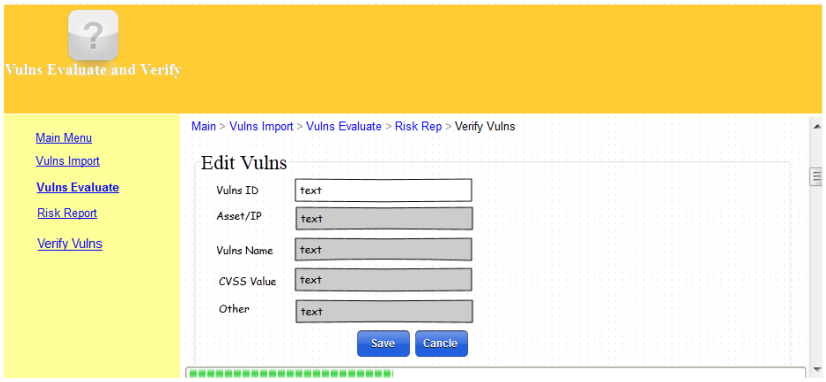


Figure A-5 Change Data Prototyping

7. Show Data Function is the method of select data from tables and create and show view records in grid.

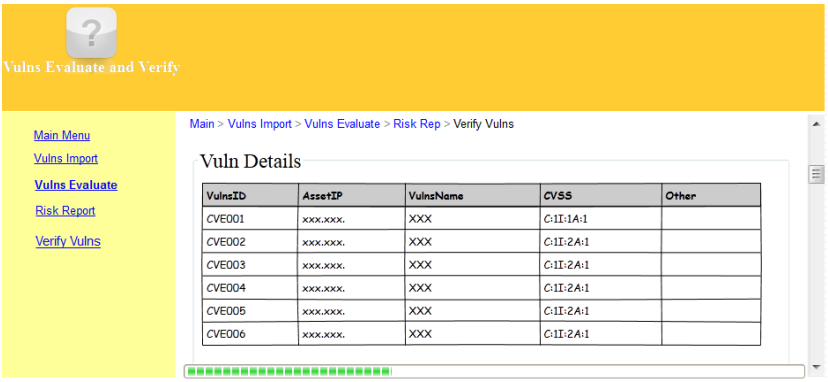


Figure A-6 Show Data Prototyping

8. Find Data Function is the method of find data from tables and create and show view records in grid.

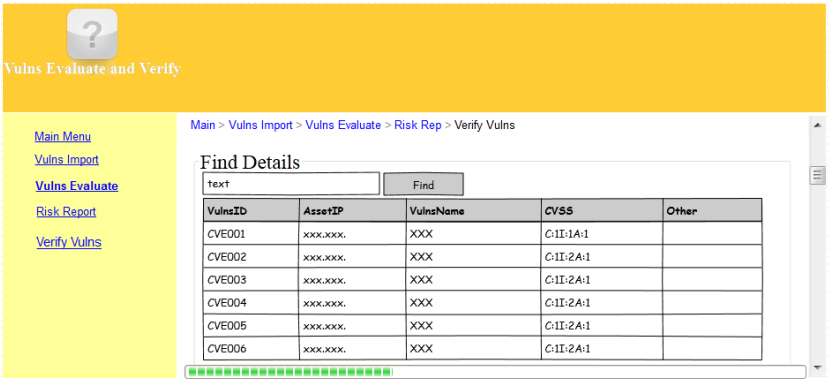
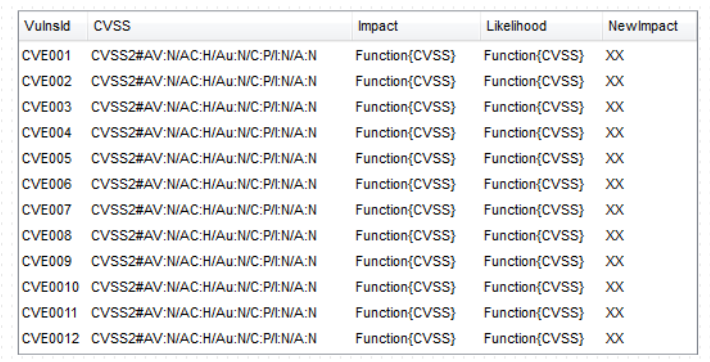


Figure A-7 Find Data Prototyping

9. Find Data Function is the method of split data into 2 sections that is impact, and likelihood data using database functions.



VulnsId	CVSS	Impact	Likelihood	NewImpact
CVE001	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE002	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE003	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE004	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE005	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE006	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE007	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE008	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE009	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE0010	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE0011	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX
CVE0012	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Function{CVSS}	Function{CVSS}	XX

Figure A-8 Decompose Data Prototyping

10. Estimate Data Function is the method of calculate, and normalize impact, and likelihood values using database functions.

VulnId	Impact	ImpactVule	NormImpact	Likelihood	LikeLiVule	NormLikeli	BusinessImpact	NewImpact
[No]	Substing[CVSS]	CAL[Impact]	Norm[ImpactV]	Substing[CVSS]	CAL[Likeli]	Norm[LikeliV]	BImpactV	Avg[ImpactV,BImpactV]
CVE001	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE002	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE003	AV:AC:Au	5	4	C:I:A	10	9	4	4
CVE004	AV:AC:Au	10	9	C:I:A	6	5	5	5
CVE005	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE006	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE007	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE008	AV:AC:Au	6	5	C:I:A	10	9	5	5
CVE009	AV:AC:Au	10	9	C:I:A	10	9	9	9
CVE0010	AV:AC:Au	10	9	C:I:A	5	4	4	4

Figure A-9 Estimate Data Prototyping

11. Calculate Risk Value Function is the method of calculate impact and likelihood levels using database functions.

VulnId	NormImpact	ImpactLevel	NormLikeli	LikeliLevel	NewImpact	NImpactLevel	RiskValues	RiskValuesNew
[No]	NormImpact	CAL[NormImpact]	NormLikeli	CAL[NormLikeli]	NewImpact	CAL[NewImpact]	CAL[ImpactLevel,LikeliLevel]	CAL[NImpactLevel,LikeliLevel]
CVE001	10	3	10	3	10	3	33	33
CVE002	10	3	10	3	10	3	33	33
CVE003	10	3	10	3	10	3	33	33
CVE004	10	3	10	3	10	3	33	33
CVE005	10	3	10	3	10	3	33	33
CVE006	10	3	10	3	10	3	33	33
CVE007	10	3	10	3	10	3	33	33
CVE008	10	3	10	3	10	3	33	33
CVE009	10	3	10	3	10	3	33	33

Figure A-10 Calculate Risk Value Prototyping

12. Risk Rating Mapping Function is the method of calculate, and mapping risk rating using database functions.

VulnId	ImpactL	ImpactRating	LikeliL	LikeLiRating	NewImpactL	NImpactRating	RiskValues	RiskRating	RiskValuesNew	NRiskRating
[No]	ImpactL	CAL[ImpactL]	LikeliL	CAL[LikeliL]	NImpactL	CAL[NImpactL]	RiksV	CAL[RiskV]	NewRiskV	CAL[NewRiskV]
CVE001	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE002	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE003	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE004	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE005	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE006	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE007	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE008	3	High	3	High	3	High	33	Critical	33	Cirtical
CVE009	3	High	3	High	3	High	33	Critical	33	Cirtical

Figure A-11 Risk Rating Mapping Prototyping

13. Show Report Function is the method of select and summarize data and show report chart.

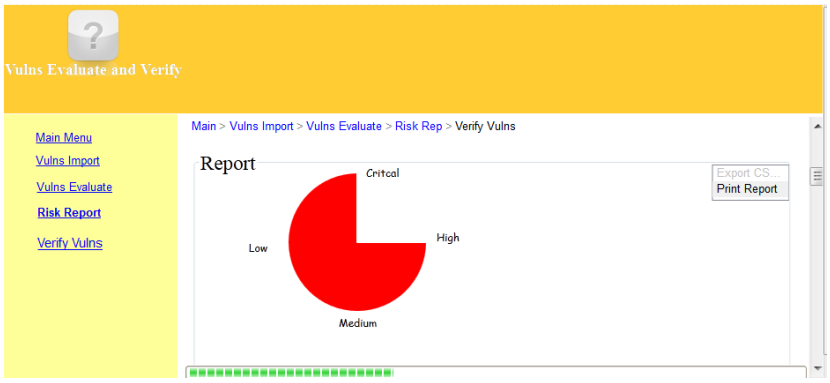


Figure A-12 Show Report Prototyping

14. Export Data Function is the method of select data and export csv file into local drive.

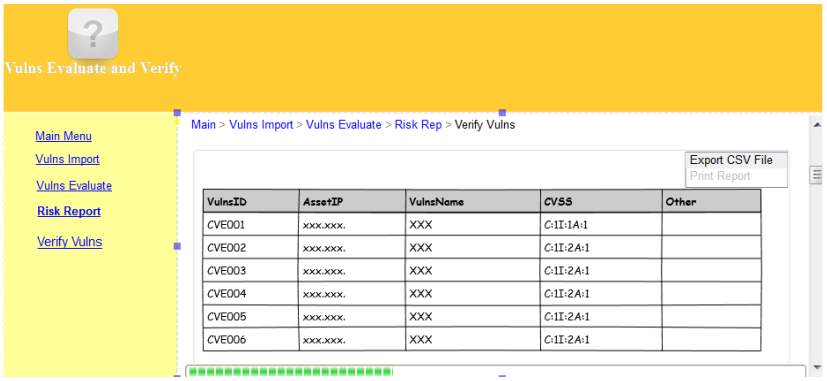


Figure A-13 Export Data Prototyping

15. Print Report Function is the method of select, and show data and print pdf file.

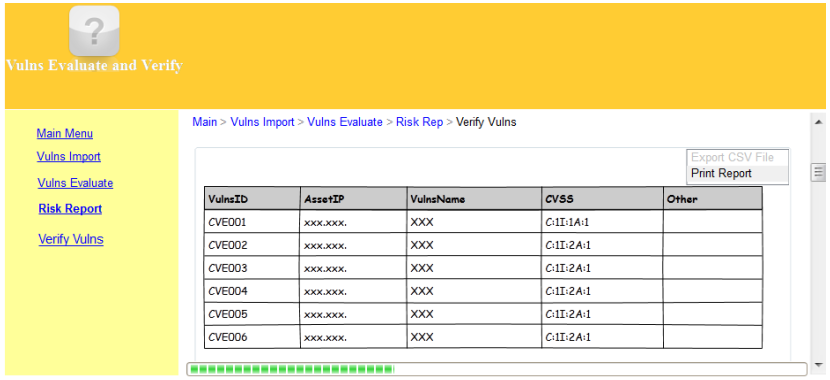


Figure A-14 Print Report Prototyping

16. Details Reference Function is the method of select record and show details of reference or full-disclosure.

17. Detail Exploit Code Function is the method of select record, and show details of exploit info.

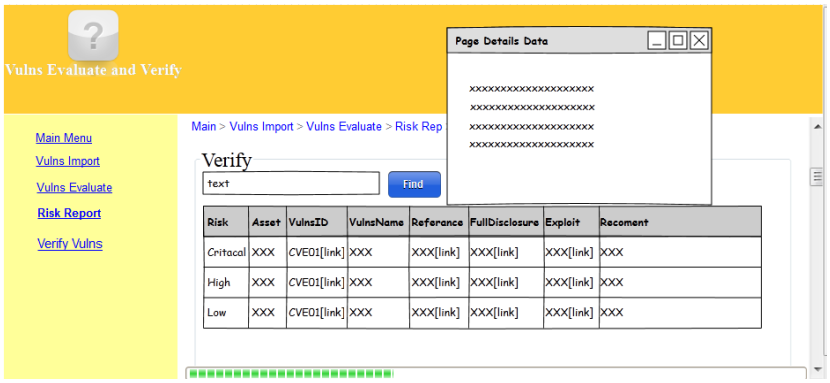


Figure A-15 Details Reference and Detail Exploit Code Prototyping

18. Change Details Function is the method of select record and change or edit text values for testing exploit code using msfconsole command of metasploit framework.

19. Testing Sample Function is the method of testing exploit code using msfconsole command of metasploit framework.

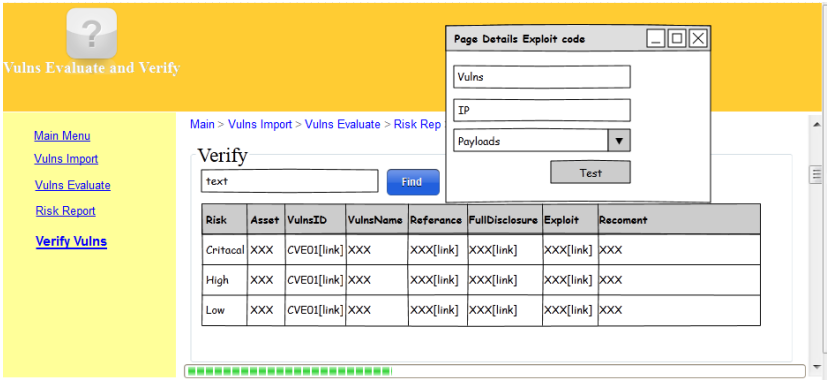


Figure A-15 Change Details and Testing Sample Prototyping

APPENDIX B
DATABASE DESIGN AND CREATE COMMAND

1) Risk Evaluate Tables and Views has 15 Table that is 1) Main Vulns Table, 2) Risk Desc Table, 3) Business Impact Table, 4) CVSS View, 5) OS View, 6) Solution View, 7) Desc View, 8) MTS View, 9) CVE View, 10) Vuln View, 11) Vuln1 View, 12) Vuln2 View, 13) Summary View, 14) Rep OWASP View, and 15) Rep NOWASP View following: Table B-1 to B-15

1. Main Vulns Table is table for collect vulnerabilities data obtained from the vulnerability scanning process. We can create table using SQL Command below and data structure following: Table B-1

```
CREATE TABLE IF NOT EXISTS `main` ( `no` int(11) NOT NULL AUTO_INCREMENT, `name` text, `name2` varchar(15) DEFAULT NULL, `tag` text, `name3` text, `port` text, `svc_name` text, `protocol` text, `pluginID` varchar(20) DEFAULT NULL, `pluginName` text, `pluginFamily` text, `description` text, `fname` text, `plugin_type` text, `risk_factor` text, `solution` text, `synopsis` text, `cve` text, `cvss_base_score` text, `cvss_vector` text, `see_also` text, `metasploit_name` text, PRIMARY KEY (`no`));
```

Table B-1 Main Vulns Table

No	Name	Type	Collation	Null	Default	Extra
1	no	int(11)		No	None	Order Number
2	name	text	utf8_general_ci	Yes	NULL	System Name
3	name2	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
4	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
5	name3	text	utf8_general_ci	Yes	NULL	Descriptions2
6	port	text	utf8_general_ci	Yes	NULL	Port Number
7	svc_name	text	utf8_general_ci	Yes	NULL	Service Name
8	protocol	text	utf8_general_ci	Yes	NULL	Protocol
9	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
10	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
11	pluginFamily	text	utf8_general_ci	Yes	NULL	Plugin Family
12	description	text	utf8_general_ci	Yes	NULL	Descriptions3
13	fname	text	utf8_general_ci	Yes	NULL	Fname
14	plugin_type	text	utf8_general_ci	Yes	NULL	Plugin Type
15	risk_factor	text	utf8_general_ci	Yes	NULL	Risk Factor
16	solution	text	utf8_general_ci	Yes	NULL	Solution
17	synopsis	text	utf8_general_ci	Yes	NULL	Synopsis
18	cve	text	utf8_general_ci	Yes	NULL	CVE Number
19	cvss_base_score	text	utf8_general_ci	Yes	NULL	CVSS Base Score

20	cvss_vector	text	utf8_general_ci	Yes	NULL	CVSS Vector
21	see_also	text	utf8_general_ci	Yes	NULL	See Also
22	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name

2. Risk Desc Table is table for record risk description data We can create table using SQL Command below and data structure following: Table B-2

```
CREATE TABLE IF NOT EXISTS `risk` ( `risk` text, `desc` text, PRIMARY KEY (`no`));
```

Table B-2 Risk Desc Table

No	Name	Type	Collation	Null	Default	Extra
1	risk	text	utf8_general_ci	No	None	Risk Level
2	desc	text	utf8_general_ci	No	None	Descriptions

3. Business Impact Table is table for record risk description data We can create table using SQL Command below and data structure following: Table B-3

```
CREATE TABLE IF NOT EXISTS `bia` ( `name6` varchar(15) NOT NULL, `fd` int(1) NOT NULL, `rd` int(1) NOT NULL, `nc` int(1) NOT NULL, `pv` int(1) NOT NULL, UNIQUE KEY `name6` (`name6`)) ;
```

Table B-3 Business Impact Table

No	Name	Type	Collation	Null	Default	Extra
1	name6	varchar(15)	tis620_thai_ci	No	None	IP Address
2	fd	int(1)		No	None	Financial damage
3	rd	int(1)		No	None	Reputation damage
4	nc	int(1)		No	None	Non-compliance
5	pv	int(1)		No	None	Privacy violation

4. CVSS View is table view for record vulnerability data. We can create view using SQL Command below and data structure following: Table B-4

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `cvss` AS select `main`.`name` AS `name`,`main`.`name2` AS `name2`,`main`.`port` AS `port`,`main`.`svc_name` AS `svc_name`,`main`.`protocol` AS `protocol`,`main`.`pluginID` AS `pluginID`,`main`.`pluginName` AS `pluginName`,`main`.`pluginFamily` AS `pluginFamily`,`main`.`cvss_vector` AS `cvss_vector` from `main` where (`main`.`cvss_vector` <> '')
```

Table B-4 CVSS View

No	Name	Type	Collation	Null	Default	Extra
1	name	text	utf8_general_ci	Yes	NULL	System Name
2	name2	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
3	port	text	utf8_general_ci	Yes	NULL	Port Number
4	svc_name	text	utf8_general_ci	Yes	NULL	Service Name
5	protocol	text	utf8_general_ci	Yes	NULL	Protocol
6	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
7	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name

8	pluginFamily	text	utf8_general_ci	Yes	NULL	Plugin Family
9	cvss_vector	text	utf8_general_ci	Yes	NULL	CVSS Vector

5. OS View is table view for record Operation systems data. We can create view using SQL Command below and data structure following: Table B-5

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `os` AS select `main`.`name2` AS `name2`,`main`.`tag` AS `tag`,`main`.`name3` AS `name3` from `main` where (`main`.`name3` = 'operating-system')
```

Table B-5 OS View

No	Name	Type	Collation	Null	Default	Extra
1	name2	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
2	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
3	Name3	text	utf8_general_ci	Yes	NULL	Descriptions2

6. Solution View is table view for record solution data. We can create view using SQL Command below and data structure following: Table B-6

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `solution` AS select distinct `main`.`pluginID` AS `pluginID`,`main`.`solution` AS `solution` from `main` where (`main`.`solution` <> '') order by 1
```

Table B-6 Solution View

No	Name	Type	Collation	Null	Default	Extra
1	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
2	solution	text	utf8_general_ci	Yes	NULL	Solution

7. Desc View is table view for record referance data. We can create view using SQL Command below and data structure following: Table B-7

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `disc` AS select distinct `main`.`pluginID` AS `pluginID`,`main`.`see_also` AS `see_also` from `main` where (`main`.`see_also` <> '')
```

Table B-7 Desc View

No	Name	Type	Collation	Null	Default	Extra
1	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
2	see_also	text	utf8_general_ci	Yes	NULL	See Also

8. MTS View is table view for record metasploit data. We can create view using SQL Command below and data structure following: Table B-8

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `mts` AS select distinct `main`.`pluginID` AS `pluginID`,`main`.`metasploit_name` AS `metasploit_name` from `main` where (`main`.`metasploit_name` <> '')
```

Table B-8 MTS View

No	Name	Type	Collation	Null	Default	Extra
1	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
2	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name

9. CVE View is table view for record cve data. We can create view using SQL Command below and data structure following: Table B-9

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `cve`
AS select distinct `main`.`pluginID` AS `pluginID`,`main`.`cve` AS `cve` from `main` where (`main`.`pluginID`
<> '')
```

Table B-9 CVE View

No	Name	Type	Collation	Null	Default	Extra
1	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
2	cve	text	utf8_general_ci	Yes	NULL	CVE Number

10. Vuln View is table view for record vulnerability summary data. We can create view using SQL Command below and data structure following: Table B-10

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `vuln`
AS select distinct `main2`.`name` AS `name`,`main2`.`name2` AS
`name2`,concat(`main2`.`svc_name`,'(',`main2`.`protocol`,`main2`.`port`,')') AS `service`,`main2`.`tag` AS
`tag`,`main2`.`pluginID` AS `pluginID`,`main2`.`pluginName` AS `pluginName`,`main2`.`solution` AS
`solution`,`main2`.`cvss_vector` AS `cvss_vector`,`main2`.`metasploit_name` AS
`metasploit_name`,`main2`.`see_also` AS `see_also`,`vbia`.`bi` AS `BI` from (`main2` left join `vbia`
on((`main2`.`name2` = convert(`vbia`.`name6` using utf8)))) where (`main2`.`cvss_vector` <> ' ')
```

Table B-10 Vuln View

No	Name	Type	Collation	Null	Default	Extra
1	name	text	utf8_general_ci	Yes	NULL	System Name
2	name2	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
3	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
4	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
5	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
6	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
7	solution	text	utf8_general_ci	Yes	NULL	Solution
8	cvss_vector	text	utf8_general_ci	Yes	NULL	CVSS Vector
9	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
10	see_also	text	utf8_general_ci	Yes	NULL	See Also
11	BI	decimal(17,4)		Yes	NULL	Business Impact Value

11. Vuln1 View is table view for record vulnerability risk determine data. We can create view using SQL Command below and data structure following: Table B-11

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `vuln1`
AS select `vuln`.`name` AS `name`,concat('xxx.xxx.xxx.',substring_index(`vuln`.`name2`,'.',-(1))) AS
`name2`,`vuln`.`name2` AS `nameip`,`vuln`.`service` AS `service`,`vuln`.`tag` AS `tag`,`vuln`.`pluginID` AS
`pluginID`,`vuln`.`pluginName` AS `pluginName`,`vuln`.`solution` AS `solution`,`vuln`.`cvss_vector` AS
`cvss_vector`,(case substr(`vuln`.`cvss_vector`,10,1) when 'L' then 0.395 when 'A' then 0.646 when 'N' then 1 end)
AS `AV`,(case substr(`vuln`.`cvss_vector`,15,1) when 'H' then 0.35 when 'M' then 0.61 when 'L' then 0.71 end) AS
`AC`,(case substr(`vuln`.`cvss_vector`,20,1) when 'M' then 0.45 when 'S' then 0.56 when 'N' then 0.704 end) AS
`AU`,(case substr(`vuln`.`cvss_vector`,24,1) when 'N' then 0 when 'P' then 0.275 when 'C' then 0.66 end) AS
`C`,(case substr(`vuln`.`cvss_vector`,28,1) when 'N' then 0 when 'P' then 0.275 when 'C' then 0.66 end) AS `I`,(case
substr(`vuln`.`cvss_vector`,32,1) when 'N' then 0 when 'P' then 0.275 when 'C' then 0.66 end) AS
`A`,`vuln`.`metasploit_name` AS `metasploit_name`,`vuln`.`see_also` AS `see_also`,`vuln`.`BI` AS `BI` from
`vuln` where 1
```

Table B-11 Vuln1 View

No	Name	Type	Collation	Null	Default	Extra
1	name	text	utf8_general_ci	Yes	NULL	System Name
2	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address (hide)
3	nameip	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
4	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
5	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
6	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
7	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
8	solution	text	utf8_general_ci	Yes	NULL	Solution
9	cvss_vector	text	utf8_general_ci	Yes	NULL	CVSS Vector
10	AV	decimal(4,3)		Yes	NULL	Access Vector
11	AC	decimal(3,2)		Yes	NULL	Access Complexity
12	AU	decimal(4,3)		Yes	NULL	Authentication
13	C	decimal(4,3)		Yes	NULL	Confidentiality
14	I	decimal(4,3)		Yes	NULL	Integrity
15	A	decimal(4,3)		Yes	NULL	Availability
16	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
17	see_also	text	utf8_general_ci	Yes	NULL	See Also
18	BI	decimal(17,4)		Yes	NULL	Business Impact Value

12. Vuln2 View is table view for vulnerability risk values data. We can create view using SQL Command below and data structure following: Table B-12

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `vuln3`
AS select `vuln2`.`name` AS `name`,`vuln2`.`name2` AS `name2`,`vuln2`.`nameip` AS `nameip`,`vuln2`.`service`
AS `service`,`vuln2`.`tag` AS `tag`,`vuln2`.`pluginID` AS `pluginID`,`vuln2`.`pluginName` AS
`pluginName`,`vuln2`.`solution` AS `solution`,`vuln2`.`AV` AS `AV`,`vuln2`.`AC` AS `AC`,`vuln2`.`AU` AS
`AU`,`vuln2`.`C` AS `C`,`vuln2`.`I` AS `I`,`vuln2`.`A` AS `A`,`vuln2`.`likh` AS `likh`,`vuln2`.`imp` AS
`imp`,`vuln2`.`BI` AS `BI`,`vuln2`.`Nimp` AS `Nimp`,`vuln2`.`norm_Likh` AS `norm_Likh`,`vuln2`.`norm_imp`
AS `norm_imp`,`vuln2`.`norm_nimp` AS `norm_nimp`,if((`vuln2`.`norm_Likh` > 6),3,if((`vuln2`.`norm_Likh` <
3),1,2)) AS `owasp_Likh`,if((`vuln2`.`norm_imp` > 6),3,if((`vuln2`.`norm_imp` < 3),1,2)) AS
`owasp_imp`,if((`vuln2`.`norm_nimp` > 6),3,if((`vuln2`.`norm_nimp` < 3),1,if((`vuln2`.`norm_nimp` between 3
and 6),2,NULL))) AS `owasp_nimp`,round(((((0.6 * `vuln2`.`imp`) + (0.4 * `vuln2`.`likh`)) - 1.5) * 1.176),2) AS
`cv`,concat(if((`vuln2`.`norm_Likh` > 6),3,if((`vuln2`.`norm_Likh` < 3),1,2)),if((`vuln2`.`norm_imp` >
6),3,if((`vuln2`.`norm_imp` < 3),1,2))) AS `LxI`,concat(if((`vuln2`.`norm_Likh` > 6),3,if((`vuln2`.`norm_Likh` <
3),1,2)),if((`vuln2`.`norm_nimp` > 6),3,if((`vuln2`.`norm_nimp` < 3),1,if((`vuln2`.`norm_nimp` between 3 and
6),2,NULL)))) AS `LxnI`,`vuln2`.`metasploit_name` AS `metasploit_name`,`vuln2`.`see_also` AS `see_also` from
`vuln2` where 1
```

Table B-12 Vuln2 View

No	Name	Type	Collation	Null	Default	Extra
1	name	text	utf8_general_ci	Yes	NULL	System Name
2	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address (hide)
3	nameip	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
4	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
5	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
6	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
7	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
8	solution	text	utf8_general_ci	Yes	NULL	Solution
9	AV	decimal(4,3)		Yes	NULL	Access Vector
10	AC	decimal(3,2)		Yes	NULL	Access Complexity
11	AU	decimal(4,3)		Yes	NULL	Authentication
12	C	decimal(4,3)		Yes	NULL	Confidentiality
13	I	decimal(4,3)		Yes	NULL	Integrity
14	A	decimal(4,3)		Yes	NULL	Availability
15	likh	decimal(8,2)		Yes	NULL	Likelihood
16	imp	decimal(12,2)		Yes	NULL	Impact
17	BI	decimal(17,4)		Yes	NULL	Business Impact
18	Nimp	decimal(22,8)		Yes	NULL	New Impact
19	norm_Likh	decimal(13,2)		Yes	NULL	Normalize Likelihood
20	norm_imp	decimal(17,2)		Yes	NULL	Normalize Impact
21	norm_nimp	decimal(21,2)		Yes	NULL	Normalize New Impact
22	owasp_Likh	int(1)		No	0	Owasp Likelihood
23	owasp_imp	int(1)		No	0	Owasp Impact
24	owasp_nimp	int(1)		Yes	NULL	Owasp New Impact
25	cv	decimal(17,2)		Yes	NULL	CVSS Score
26	LxI	varchar(2)	utf8_general_ci	No		Likelihood X Impact
27	LxnI	varchar(2)	utf8_general_ci	Yes	NULL	Likelihood X NewImpact
28	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
29	see_also	text	utf8_general_ci	Yes	NULL	See Also

13. Summary View is table view for vulnerability risk summary data. We can create view using SQL Command below and data structure following: Table B-13

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW
`sumary` AS select distinct `vuln3`.`name` AS `name`,`vuln3`.`name2` AS `name2`,`vuln3`.`nameip` AS
`nameip`,`vuln3`.`service` AS `service`,`vuln3`.`tag` AS `tag`,`vuln3`.`pluginID` AS
`pluginID`,`vuln3`.`pluginName` AS `pluginName`,`vuln3`.`solution` AS `solution`,`vuln3`.`likh` AS
`likh`,`vuln3`.`imp` AS `imp`,`vuln3`.`BI` AS `BI`,`vuln3`.`Nimp` AS `Nimp`,`vuln3`.`norm_Likh` AS
`norm_Likh`,`vuln3`.`norm_imp` AS `norm_imp`,`vuln3`.`norm_nimp` AS `norm_nimp`,`vuln3`.`owasp_Likh`
AS `owasp_Likh`,`vuln3`.`owasp_imp` AS `owasp_imp`,`vuln3`.`owasp_nimp` AS `owasp_nimp`,`vuln3`.`cv` AS
`cv`,`vuln3`.`LxI` AS `LxI`,`vuln3`.`LxnI` AS `LxnI`,if((`vuln3`.`cv` = 10),'1.critical',if(((`vuln3`.`cv` < 10) and
(`vuln3`.`cv` >= 7)),'2.high',if(((`vuln3`.`cv` < 7) and (`vuln3`.`cv` >= 4)),'3.medium',if(((`vuln3`.`cv` < 4) and
(`vuln3`.`cv` >= 0)),'4.low','5.note')))) AS `risk_cvss`,(case `vuln3`.`LxI` when 11 then '5.note' when 12 then '4.low'
when 21 then '4.low' when 22 then '3.medium' when 13 then '3.medium' when 31 then '3.medium' when 23 then
'2.high' when 32 then '2.high' when 33 then '1.critical' end) AS `risk_owasp`,(case `vuln3`.`LxnI` when 11 then
'5.note' when 12 then '4.low' when 21 then '4.low' when 22 then '3.medium' when 13 then '3.medium' when 31 then
'3.medium' when 23 then '2.high' when 32 then '2.high' when 33 then '1.critical' end) AS
`risk_nowasp`,`vuln3`.`metasploit_name` AS `metasploit_name`,`vuln3`.`see_also` AS `see_also`,`cve`.`cve` AS
`cve` from (`vuln3` join `cve`) where (`vuln3`.`pluginID` = `cve`.`pluginID`)
```

Table B-13 Summary View

No	Name	Type	Collation	Null	Default	Extra
1	name	text	utf8_general_ci	Yes	NULL	System Name
2	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address (hide)
3	nameip	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
4	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
5	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
6	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
7	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
8	solution	text	utf8_general_ci	Yes	NULL	Solution
9	likh	decimal(8,2)		Yes	NULL	Likelihood
10	imp	decimal(12,2)		Yes	NULL	Impact
11	BI	decimal(17,4)		Yes	NULL	Business Impact
12	Nimp	decimal(22,8)		Yes	NULL	New Impact
13	norm_Likh	decimal(13,2)		Yes	NULL	Normalize Likelihood
14	norm_imp	decimal(17,2)		Yes	NULL	Normalize Impact
15	norm_nimp	decimal(21,2)		Yes	NULL	Normalize New Impact
16	owasp_Likh	int(1)		No	0	Owasp Likelihood
17	owasp_imp	int(1)		No	0	Owasp Impact
18	owasp_nimp	int(1)		Yes	NULL	Owasp New Impact
19	cv	decimal(17,2)		Yes	NULL	CVSS Score
20	LxI	varchar(2)	utf8_general_ci	No		Likelihood X Impact
21	LxnI	varchar(2)	utf8_general_ci	Yes	NULL	Likelihood X NewImpact
22	risk_cvss	varchar(10)	utf8_general_ci	No		Risk CVSS
23	risk_owasp	varchar(10)	utf8_general_ci	Yes	NULL	Risk OWASP
24	risk_nowasp	varchar(10)	utf8_general_ci	Yes	NULL	Risk NewOwasp
25	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
26	see_also	text	utf8_general_ci	Yes	NULL	See Also
27	cve	text	utf8_general_ci	Yes	NULL	CVE Number

14. Rep OWASP View is table view for OWASP security risk assessment report . We can create view using SQL Command below and data structure following: Table B-14

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW
`rep_owasp` AS select `sumary`.`risk_owasp` AS `risk_owasp`,`sumary`.`name` AS `name`,`sumary`.`service` AS
`service`,`sumary`.`tag` AS `tag`,`sumary`.`pluginID` AS `pluginID`,`sumary`.`pluginName` AS
`pluginName`,`sumary`.`solution` AS `solution`,`sumary`.`metasploit_name` AS
`metasploit_name`,`sumary`.`see_also` AS `see_also`,`sumary`.`name2` AS `name2` from `sumary` where 1 group
by 1,2,3,4,5 order by 1
```

Table B-14 Rep OWASP View

No	Name	Type	Collation	Null	Default	Extra
1	risk_owasp	varchar(10)	utf8_general_ci	Yes	NULL	Risk OWASP
2	name	text	utf8_general_ci	Yes	NULL	System Name
3	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
4	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
5	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
6	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
7	solution	text	utf8_general_ci	Yes	NULL	Solution
8	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
9	see_also	text	utf8_general_ci	Yes	NULL	See Also
10	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address

15. Rep NOWASP View is table view for New Impact OWASP security risk assessment report . We can create view using SQL Command below and data structure following: Table B-15

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW
`rep_nowasp` AS select `sumary`.`risk_nowasp` AS `risk_nowasp`,`sumary`.`name` AS `name`,`sumary`.`service`
AS `service`,`sumary`.`tag` AS `tag`,`sumary`.`pluginID` AS `pluginID`,`sumary`.`pluginName` AS
`pluginName`,`sumary`.`solution` AS `solution`,`sumary`.`metasploit_name` AS
`metasploit_name`,`sumary`.`see_also` AS `see_also`,`sumary`.`name2` AS `name2` from `sumary` where 1 group
by 1,2,3,4,5 order by 1
```

Table B-15 Rep NOWASP View

No	Name	Type	Collation	Null	Default	Extra
1	risk_nowasp	varchar(10)	utf8_general_ci	Yes	NULL	Risk New OWASP
2	name	text	utf8_general_ci	Yes	NULL	System Name
3	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
4	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
5	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
6	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
7	solution	text	utf8_general_ci	Yes	NULL	Solution
8	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
9	see_also	text	utf8_general_ci	Yes	NULL	See Also
10	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address

2) Verification Vulnerabilities Tables and Views has 6 Table that is 1) Full-disclosure Table, 2) ExploDB Table, 3) Msfvulns Table, 4) Paylo Table, 5) Vmsfall View, and 6) Rep_cvss View following: Table B-16 to B-20

1. Full-disclosure Table is table for full-disclosure reference data. We can create table using SQL Command below and data structure following: Table B-16

```
CREATE TABLE IF NOT EXISTS `fulldisc` ( `CVE` varchar(13) DEFAULT NULL, `FullDisc` varchar(196) DEFAULT NULL, `Date` varchar(11) DEFAULT NULL, `Link` varchar(67) DEFAULT NULL)
```

Table B-16 Full-disclosure Table

No	Name	Type	Collation	Null	Default	Extra
1	CVE	varchar(13)	utf8_general_ci	Yes	NULL	CVE Number
2	FullDisc	varchar(196)	utf8_general_ci	Yes	NULL	full-disclosure
3	Date	varchar(11)	utf8_general_ci	Yes	NULL	Date
4	Link	varchar(67)	utf8_general_ci	Yes	NULL	Link

2. ExploDB Table is table for exploitDB reference data. We can create table using SQL Command below and data structure following: Table B-17

```
CREATE TABLE IF NOT EXISTS `explodb` ( `EDB_ID` int(5) DEFAULT NULL, `CVE` varchar(14) DEFAULT NULL, `file` varchar(42) DEFAULT NULL, `description` varchar(142) DEFAULT NULL, `date` int(5) DEFAULT NULL, `author` varchar(30) DEFAULT NULL, `platform` varchar(10) DEFAULT NULL, `type` varchar(7) DEFAULT NULL, `port` int(5) DEFAULT NULL, `link` varchar(41) DEFAULT NULL)
```

Table B-17 ExploDB Table

No	Name	Type	Collation	Null	Default	Extra
1	EDB_ID	int(5)		Yes	NULL	EDB ID
2	CVE	varchar(14)	utf8_general_ci	Yes	NULL	CVE Number
3	file	varchar(42)	utf8_general_ci	Yes	NULL	File Name
4	description	varchar(142)	utf8_general_ci	Yes	NULL	Descriptions
5	date	int(5)		Yes	NULL	Date
6	author	varchar(30)	utf8_general_ci	Yes	NULL	author
7	platform	varchar(10)	utf8_general_ci	Yes	NULL	platform
8	type	varchar(7)	utf8_general_ci	Yes	NULL	type
9	port	int(5)		Yes	NULL	Port Number
10	link	varchar(41)	utf8_general_ci	Yes	NULL	Link

3. Msfvulns Table is table for Metasploit code reference data. We can create table using SQL Command below and data structure following: Table B-18

```
CREATE TABLE IF NOT EXISTS `msfvulns` ( `CVE` varchar(13) DEFAULT NULL, `Typ` varchar(3) DEFAULT NULL, `Sys` varchar(9) DEFAULT NULL, `fullname` varchar(69) DEFAULT NULL, `name` varchar(123) DEFAULT NULL)
```

Table B-18 Msfvulns Table

No	Name	Type	Collation	Attributes	Null	Default	Extra
1	CVE	varchar(13)	utf8_general_ci		Yes	NULL	CVE Number
2	Typ	varchar(3)	utf8_general_ci		Yes	NULL	Types
3	Sys	varchar(9)	utf8_general_ci		Yes	NULL	Systems
4	fullname	varchar(69)	utf8_general_ci		Yes	NULL	Full Name
5	name	varchar(123)	utf8_general_ci		Yes	NULL	Metasploit Name

4. Paylo Table is table for Playloads code data. We can create table using SQL Command below and data structure following: Table B-19

```
CREATE TABLE IF NOT EXISTS `msfvulns` ( `CVE` varchar(13) DEFAULT NULL, `Typ` varchar(3) DEFAULT NULL, `Sys` varchar(9) DEFAULT NULL, `fullname` varchar(69) DEFAULT NULL, `name` varchar(123) DEFAULT NULL)
```

Table B-19 Paylo Table

No	Name	Type	Collation	Null	Default	Extra
1	paylo	varchar(55)	utf8_general_ci	Yes	NULL	Payload Path
2	typ	varchar(7)	utf8_general_ci	Yes	NULL	Type
3	name	varchar(94)	utf8_general_ci	Yes	NULL	Payload Name

5. Vmsfall View is table for Metasploit code data. We can create view using SQL Command below and data structure following: Table B-20

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW `vmsfall` AS select `msfvulns`.`Sys` AS `Sys`,`msfvulns`.`Typ` AS `Typ`,`msfvulns`.`CVE` AS `CVE`,`msfvulns`.`name` AS `name`,`msfvulns`.`fullname` AS `fullname` from `msfvulns` where 1
```

Table B-20 Vmsfall View

No	Name	Type	Collation	Null	Default	Extra
1	Sys	varchar(9)	utf8_general_ci	Yes	NULL	Systems
2	Typ	varchar(3)	utf8_general_ci	Yes	NULL	Type
3	CVE	varchar(13)	utf8_general_ci	Yes	NULL	CVE Number
4	name	varchar(123)	utf8_general_ci	Yes	NULL	Metasploit Name
5	fullname	varchar(69)	utf8_general_ci	Yes	NULL	Metasploit Path

6. Vpaylo View is table for Payloads code data. We can create view using SQL Command below and data structure following: Table B-21

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW vpaylo`
AS select `paylo`.`typ` AS `sys`,`paylo`.`paylo` AS `paylo`,`paylo`.`name` AS `name` from `paylo` where 1
```

Table B-21 Vmsfall View

No	Name	Type	Collation	Null	Default	Extra
1	paylo	varchar(55)	utf8_general_ci	Yes	NULL	Payload Path
2	typ	varchar(7)	utf8_general_ci	Yes	NULL	Type
3	name	varchar(94)	utf8_general_ci	Yes	NULL	Payload Name

7. Rep_cvss View is table for vulnerability reference/exploit report. We can create view using SQL Command below and data structure following: Table B-22

```
ALTER ALGORITHM=UNDEFINED DEFINER=`root`@`localhost` SQL SECURITY DEFINER VIEW
`rep_cvss` AS select `sumary`.`risk_cvss` AS `cvss`,`sumary`.`name` AS `name`,`sumary`.`service` AS
`service`,`sumary`.`tag` AS `tag`,`sumary`.`pluginID` AS `pluginID`,`sumary`.`pluginName` AS
`pluginName`,`sumary`.`solution` AS `solution`,`sumary`.`metasploit_name` AS
`metasploit_name`,`sumary`.`see_also` AS `see_also`,`sumary`.`name2` AS `name2`,`sumary`.`nameip` AS
`nameip`,`sumary`.`cve` AS `cve`,`fulldisc`.`FullDisc` AS `fulldisc`,`fulldisc`.`Link` AS `fullink`,`explodb`.`link`
AS `exdbink` from ((`sumary` left join `fulldisc` on((`sumary`.`cve` = `fulldisc`.`CVE`))) left join `explodb`
on((`sumary`.`cve` = `explodb`.`CVE`))) group by 1,2,3,4,5
```

Table B-22 Rep_cvss View

No	Name	Type	Collation	Null	Default	Extra
1	cvss	varchar(10)	utf8_general_ci	No		Risk
2	name	text	utf8_general_ci	Yes	NULL	Systems
3	service	mediumtext	utf8_general_ci	Yes	NULL	Service Name
4	tag	text	utf8_general_ci	Yes	NULL	Descriptions1
5	pluginID	varchar(20)	utf8_general_ci	Yes	NULL	Plugin ID
6	pluginName	text	utf8_general_ci	Yes	NULL	Plugin Name
7	solution	text	utf8_general_ci	Yes	NULL	Solution
8	metasploit_name	text	utf8_general_ci	Yes	NULL	Metasploit Name
9	see_also	text	utf8_general_ci	Yes	NULL	See Also
10	name2	varchar(27)	utf8_general_ci	Yes	NULL	IP Address (hide)
11	nameip	varchar(15)	utf8_general_ci	Yes	NULL	IP Address
12	cve	text	utf8_general_ci	Yes	NULL	CVE Number
13	fulldisc	varchar(196)	utf8_general_ci	Yes	NULL	full-disclosure1
14	fullink	varchar(67)	utf8_general_ci	Yes	NULL	full-disclosure2
15	exdbink	varchar(41)	utf8_general_ci	Yes	NULL	full-disclosure3

APPENDIX C
SECURITY RISK EVALUATE RESULT

1) Risk Evaluate Result Hospital A

Table C-1 Risk Rating Hospital A

CVSS Risk Rating	Likh xImp	OWASP+ Risk Rating	Likhx New Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	Business Imp	New Imp
1.critical	33	1.critical	33	xxx.xxx.xxx.100	Symantec Backup Exec for Windows Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	1	0.7	0.7	9	0.66	0.66	0.66	9	3.75	6.19
				xxx.xxx.xxx.11	PHP Unsupported Version Detection	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	1	0.7	0.7	9	0.66	0.66	0.66	9	3.5	6.08
				xxx.xxx.xxx.25	HP System Management Homepage < 7.0 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	1	0.7	0.7	9	0.66	0.66	0.66	9	4.75	6.64
				xxx.xxx.xxx.3	Symantec Backup Exec for Windows Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	1	0.7	0.7	9	0.66	0.66	0.66	9	5.25	6.86
2.high	32	2.high	32	xxx.xxx.xxx.100	Oracle TNS Listener Remote Poisoning	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.75	4.59
					Unsupported Web Server Detection	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.75	4.59
				xxx.xxx.xxx.11	PHP < 5.2.11 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.5	4.47
					PHP < 5.3.11 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.5	4.47
					PHP < 5.3.9 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.5	4.47
					PHP 5.2 < 5.2.14 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P	1	0.7	0.7	9	0.28	0.28	0.28	5.8	3.5	4.47

Table C-1 Risk Rating Hospital A (Cont.)

CVSS Risk Rating	Likh xImp	OWASP+ Risk Rating	Likhx New Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	Business Imp	New Imp
2.high	33	1.critical	33	xxx.xxx.xxx.25	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:P	1	0.7	0.7	9	0.66	0.66	0.28	8.59	4.75	6.43
					HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	1	0.6	0.7	7.73	0.66	0.66	0.66	9	4.75	6.64
					HP System Management Homepage ginkgosnmp.inc Command Injection	CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C	1	0.7	0.56	7.16	0.66	0.66	0.66	9	4.75	6.64
		2.high	32	xxx.xxx.xxx.11	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	CVSS2#AV:N/AC:M/Au:N/C:C/I:P/A:P	1	0.6	0.7	7.73	0.66	0.28	0.28	7.7	3.5	5.42
				xxx.xxx.xxx.25	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:C/I:N/A:N	1	0.7	0.7	9	0.66	0	0	6.18	4.75	5.23
3.medium	22	3.medium	22	xxx.xxx.xxx.100	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	3.75	4.59
					SSL Certificate Signed using Weak Hashing Algorithm	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N	1	0.4	0.7	4.44	0.28	0.28	0	4.45	3.75	3.91
				xxx.xxx.xxx.11	PHP < 5.2.10 Multiple Vulnerabilities	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	3.5	4.47
	31	2.high	32	xxx.xxx.xxx.21	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
				xxx.xxx.xxx.25	ASP.NET DEBUG Method Enabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	4.75	3.42
					MySQL Protocol Remote User Enumeration	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	4.75	3.42
					PHP expose_php Information Disclosure	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	4.75	3.42

Table C-1 Risk Rating Hospital A (Cont.)

CVSS Risk Rating	LikhxImp	OWASP + Risk Rating	Likhx New Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	Business Imp	New Imp
3.medium	31	2.high	32	xxx.xxx.xxx.25	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	1	0.6	0.7	7.73	0	0.28	0	2.57	4.75	3.42
					phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	1	0.6	0.7	7.73	0	0.28	0	2.57	4.75	3.42
					SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	4.75	3.42
				xxx.xxx.xxx.27	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
				xxx.xxx.xxx.3	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
				xxx.xxx.xxx.33	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
				xxx.xxx.xxx.35	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
				xxx.xxx.xxx.5	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.25	3.65
		3.medium	31	xxx.xxx.xxx.100	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	3.75	2.97
					Multiple Server Crafted Request WEB-INF Directory Information Disclosure	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	3.75	2.97
					SSL Medium Strength Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	3.75	2.97
					SSL Weak Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	3.75	2.97
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	3.75	2.97
					Web Server Directory Traversal Arbitrary File Access	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	3.75	2.97

Table C-1 Risk Rating Hospital A (Cont.)

CVSS Risk Rating	Likh xImp	OWASP + Risk Rating	Likhx New Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	Business Imp	New Imp
3.medium	31	3.medium	31	xxx.xxx.xxx.11	Dell OpenManage Server Administrator omalogin.html DOM-based XSS	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	1	0.6	0.7	7.73	0	0.28	0	2.57	3.5	2.86
					Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	3.5	2.86
					PHP < 5.2.9 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	1	0.7	0.7	9	0	0	0.28	2.57	3.5	2.86
					PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	1	0.7	0.7	9	0	0	0.28	2.57	3.5	2.86
					phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	1	0.6	0.7	7.73	0	0.28	0	2.57	3.5	2.86
					Web Server info.php / phpinfo.php Detection	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	3.5	2.86
				xxx.xxx.xxx.146	SMB Signing Required	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	3.75	2.97
	32	2.high	32	xxx.xxx.xxx.100	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	3.75	3.91
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	3.75	3.91
				xxx.xxx.xxx.11	PHP < 5.2.12 Multiple Vulnerabilities	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P	1	0.6	0.7	7.73	0.28	0.28	0.28	5.8	3.5	4.47
					PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	3.5	3.8
					PHP 5.2 < 5.2.15 Multiple Vulnerabilities	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P	1	0.6	0.7	7.73	0.28	0.28	0.28	5.8	3.5	4.47
				xxx.xxx.xxx.25	HP System Management Homepage < 7.3 Multiple Vulnerabilities	CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P	1	0.6	0.7	7.73	0.28	0.28	0.28	5.8	4.75	5.04
				xxx.xxx.xxx.35	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5.25	4.59
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5.25	4.59

Table C-1 Risk Rating Hospital A (Cont.)

CVSS Risk Rating	Likh xImp	OWASP + Risk Rating	Likhx New Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	Business Imp	New Imp
4.low	21	3.medium	22	xxx.xxx.xxx.25	FTP Supports Clear Text Authentication	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4.75	3.42
					SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4.75	3.42
					Web Server Uses Plain Text Authentication Forms	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4.75	3.42
				xxx.xxx.xxx.35	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5.25	3.65
		4.low	21	xxx.xxx.xxx.100	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	1	0.4	0.7	4.44	0	0.28	0	2.57	3.75	2.97
					SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	3.75	2.97
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	3.75	2.97
				xxx.xxx.xxx.11	FTP Supports Clear Text Authentication	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	3.5	2.86

2) **Risk Evaluate Result Hospital B**

Table C-2 Risk Rating Hospital B

CVSS Risk Rating	Likhx Imp	OWASP + Risk Rating	Likh xNew Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	BusinessImpact	New Impact
1.critical	33	1.critical	33	xxx.xxx.xxx.38	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C	1	0.7	0.7	9	0.66	0.66	0.66	9	5	6.75
2.high	33	1.critical	33	xxx.xxx.xxx.13	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	1	0.6	0.7	7.73	0.66	0.66	0.66	9	6.5	7.43
				xxx.xxx.xxx.14	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	1	0.6	0.7	7.73	0.66	0.66	0.66	9	6.5	7.43
				xxx.xxx.xxx.38	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C	1	0.6	0.7	7.73	0.66	0.66	0.66	9	5	6.75
3.medium	22	3.medium	22	xxx.xxx.xxx.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	5	5.15
				xxx.xxx.xxx.13	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	6.5	5.82
					SSL Certificate Signed using Weak Hashing Algorithm	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N	1	0.4	0.7	4.44	0.28	0.28	0	4.45	6.5	5.15
				xxx.xxx.xxx.14	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	6.5	5.82
					SSL Certificate Signed using Weak Hashing Algorithm	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N	1	0.4	0.7	4.44	0.28	0.28	0	4.45	6.5	5.15

Table C-2 Risk Rating Hospital B (Cont.)

CVSS Risk Rating	Likhx Imp	OWASP + Risk Rating	Likh xNew Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	BussinessImpact	New Impact
3.medium	22	3.medium	22	xxx.xxx.xxx.3	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	5.5	5.37
				xxx.xxx.xxx.33	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	4	4.7
				xxx.xxx.xxx.38	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P	1	0.4	0.7	4.44	0.28	0.28	0.28	5.8	5	5.15
	31	2.high	32	xxx.xxx.xxx.1	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5	3.54
					SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5	3.54
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	5	3.54
				xxx.xxx.xxx.11	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
				xxx.xxx.xxx.12	Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	6.5	4.21
				xxx.xxx.xxx.13	Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	6.5	4.21
					SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
					SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
					SSL Medium Strength Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21
					SSL Weak Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21

Table C-2 Risk Rating Hospital B (Cont.)

CVSS Risk Rating	Likhx Imp	OWASP + Risk Rating	Likh xNew Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	BusinessImpact	New Impact
3.medium	31	2.high	32	xxx.xxx.xxx.14	Microsoft Windows SMB NULL Session Authentication	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	1	0.7	0.7	9	0.28	0	0	2.57	6.5	4.21
					SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
					SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
					SSL Medium Strength Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21
					SSL Weak Cipher Suites Supported	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	6.5	4.21
				xxx.xxx.xxx.16	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	6.5	4.21
				xxx.xxx.xxx.3	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.5	3.76
					SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5.5	3.76
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	5.5	3.76
				xxx.xxx.xxx.33	ASP.NET DEBUG Method Enabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	4	3.09
					SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	4	3.09
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	4	3.09
				xxx.xxx.xxx.38	SMB Signing Disabled	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5	3.54
					SSL Certificate with Wrong Hostname	CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	1	0.7	0.7	9	0	0.28	0	2.57	5	3.54
					Terminal Services Encryption Level is Medium or Low	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	1	0.6	0.7	7.73	0.28	0	0	2.57	5	3.54

Table C-2 Risk Rating Hospital B (Cont.)

CVSS Risk Rating	Likhx Imp	OWASP + Risk Rating	LikhxNew Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	BusinessImpact	New Impact
3.medium	32	2.high	32	xxx.xxx.xxx.1	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5	4.47
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5	4.47
				xxx.xxx.xxx.13	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	6.5	5.15
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	6.5	5.15
				xxx.xxx.xxx.14	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	6.5	5.15
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	6.5	5.15
				xxx.xxx.xxx.3	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5.5	4.7
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5.5	4.7
				xxx.xxx.xxx.33	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	4	4.02
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	4	4.02
				xxx.xxx.xxx.38	SSL Certificate Cannot Be Trusted	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5	4.47
					SSL Self-Signed Certificate	CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N	1	0.7	0.7	9	0.28	0.28	0	4.45	5	4.47

Table C-2 Risk Rating Hospital B (Cont.)

CVSS Risk Rating	Likhx Imp	OWASP + Risk Rating	Likh xNew Imp	IP	Vulnerability	Cvss Vector	AV	AC	AU	Exploitability	C	I	A	Impact	BusinessImpact	New Impact
4.low	21	3.medium	22	xxx.xxx.xxx.1	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5	3.54
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5	3.54
				xxx.xxx.xxx.13	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	1	0.4	0.7	4.44	0	0.28	0	2.57	6.5	4.21
					SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	6.5	4.21
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	6.5	4.21
				xxx.xxx.xxx.14	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	1	0.4	0.7	4.44	0	0.28	0	2.57	6.5	4.21
					SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	6.5	4.21
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	6.5	4.21
				xxx.xxx.xxx.3	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5.5	3.76
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5.5	3.76
				xxx.xxx.xxx.33	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4	3.09
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4	3.09
					Web Server Uses Plain Text Authentication Forms	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	4	3.09
				xxx.xxx.xxx.38	SSL RC4 Cipher Suites Supported	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5	3.54
					Terminal Services Encryption Level is not FIPS-140 Compliant	CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	1	0.4	0.7	4.44	0.28	0	0	2.57	5	3.54

APPENDIX D
RISK ASSESSMENT REPORT

1) Risk Assessment Report Hospital A

Table D-1 Risk Assessment Report Hospital A [CVSS Score] Factor

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
1.critical	DB	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xx.x.3
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginI D:58987	PHP Unsupported Version Detection	Upgrade to a version of PHP that is currently supported.	(blank)	https://wiki.php.net/rfc/releaseprocess	xxx.xxx.xx.x.11
		Microsoft Windows Server 2008 R2	pluginI D:58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/u?a467ff94	xxx.xxx.xx.x.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/u?a467ff94	xxx.xxx.xx.x.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	xxx.xxx.xx.x.100
2.high	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginI D:41014	PHP < 5.2.11 Multiple Vulnerabilities	Upgrade to PHP version 5.2.11 or later.	(blank)	http://www.php.net/ChangeLog-5.php#5.2.11 http://www.php.net/releases/5_2_11.php http://news.php.net/php.internals/45597 http://www.php.net/ChangeLog-5.php#5.2.11	xxx.xxx.xx.x.11
			pluginI D:48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Upgrade to PHP version 5.2.14 or later.	(blank)	http://www.php.net/releases/5_2_14.php http://www.php.net/ChangeLog-5.php#5.2.14	xxx.xxx.xx.x.11
			pluginI D:57537	PHP < 5.3.9 Multiple Vulnerabilities	Upgrade to PHP version 5.3.9 or later.	Hashtable Collisions	http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5 http://www.php.net/archive/2012.php#id2012-01-11-1 http://archives.neohapsis.com/archives/bugtraq/2012-01/0092.html https://bugs.php.net/bug.php?id=55475 https://bugs.php.net/bug.php?id=55776 https://bugs.php.net/bug.php?id=53502 http://www.php.net/ChangeLog-5.php#5.3.9	xxx.xxx.xx.x.11

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	pluginID	pluginName	solution	metasploit_name	see_also	IP
2.high	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:58966	PHP < 5.3.11 Multiple Vulnerabilities	Upgrade to PHP version 5.3.11 or later.	(blank)	http://www.nessus.org/u?e81d4026 https://bugs.php.net/bug.php?id=61043 https://bugs.php.net/bug.php?id=54374 https://bugs.php.net/bug.php?id=60227 http://marc.info/?l=oss-security&m=134626481806571&w=2 http://www.php.net/archive/2012.php#id2012-04-26-1 http://www.php.net/ChangeLog-5.php#5.3.11	xxx.xxx.xxx.11
			pluginID:58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.	PHP CGI Argument Injection	http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/ https://bugs.php.net/bug.php?id=61910 http://www.php.net/archive/2012.php#id2012-05-03-1 http://www.php.net/ChangeLog-5.php#5.3.12 http://www.php.net/ChangeLog-5.php#5.4.2	xxx.xxx.xxx.11
		Microsoft Windows Server 2008 R2	pluginID:59851	HP System Management Homepage < 7.1.1 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.1.1 or later.	PHP CGI Argument Injection	http://www.nessus.org/u?541c7466 http://www.securityfocus.com/archive/1/523320/30/0/threaded	xxx.xxx.xxx.25
			pluginID:66541	HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution	Upgrade to HP System Management Homepage 7.2.0.14 or later.	HP System Management Anonymous Access Code Execution	http://www.nessus.org/u?f2db75ce	xxx.xxx.xxx.25
			pluginID:69020	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.2.1.0 or later.	PHP apache_request_headers Function Buffer Overflow	http://www.zerodayinitiative.com/advisories/ZDI-13-204/ http://www.nessus.org/u?647212eb http://www.nessus.org/u?5e861a23 http://www.securityfocus.com/archive/1/528723/30/0/threaded	xxx.xxx.xxx.25
			pluginID:70118	HP System Management Homepage ginkgosnmp.inc Command Injection	Upgrade to HP System Management Homepage 7.2.2 or later.	HP System Management Homepage JustGetSNMPQueue Command Injection	http://www.nessus.org/u?81ed4efd http://www.nessus.org/u?9b81af89 http://www.nessus.org/u?7a9cf2bb http://www.securityfocus.com/archive/1/528713/30/0/threaded	xxx.xxx.xxx.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginID:34460	Unsupported Web Server Detection	Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:69552	Oracle TNS Listener Remote Poisoning	Apply the work-around in Oracle's advisory.	(blank)	http://www.nessus.org/u?e3d5ec0b http://www.nessus.org/u?1feaed5b http://www.nessus.org/u?29d9db9b	xxx.xxx.xxx.100

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	pluginID	pluginName	solution	metasploit_name	see_also	IP
3.medium	DB	Microsoft Windows Server 2003 Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows 7 Microsoft Windows Server 2008 R2	pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.35
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.35
			pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.35
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.3
	E-Service	Microsoft Windows Server 2008 R2	pluginID:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.25
			pluginID:46803	PHP expose_php Information Disclosure	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.	(blank)	http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324	xxx.xxx.xxx.25
			pluginID:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	xxx.xxx.xxx.25
			pluginID:58087	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2012-1.php	xxx.xxx.xxx.25

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	E-Service	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.25
			pluginID:46803	PHP expose_php Information Disclosure	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.	(blank)	http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324	xxx.xxx.xxx.25
			pluginID:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	xxx.xxx.xxx.25
			pluginID:58087	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2012-1.php	xxx.xxx.xxx.25
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:11229	Web Server info.php / phpinfo.php Detection	Remove the affected file(s).	(blank)	(blank)	xxx.xxx.xxx.11
			pluginID:35750	PHP < 5.2.9 Multiple Vulnerabilities	Upgrade to PHP version 5.2.9 or later.	(blank)	http://news.php.net/php.internals/42762 http://www.php.net/releases/5_2_9.php http://www.php.net/ChangeLog-5.php#5.2.9	xxx.xxx.xxx.11
			pluginID:39480	PHP < 5.2.10 Multiple Vulnerabilities	Upgrade to PHP version 5.2.10 or later.	(blank)	http://bugs.php.net/bug.php?id=45997 http://bugs.php.net/bug.php?id=48378 http://www.php.net/releases/5_2_10.php http://www.php.net/ChangeLog-5.php#5.2.10	xxx.xxx.xxx.11
			pluginID:43351	PHP < 5.2.12 Multiple Vulnerabilities	Upgrade to PHP version 5.2.12 or later.	(blank)	http://www.nessus.org/u?57f2d08f http://www.php.net/releases/5_2_12.php http://www.php.net/ChangeLog-5.php#5.2.12	xxx.xxx.xxx.11
			pluginID:44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	Upgrade to PHP version 5.3.2 / 5.2.13 or later.	(blank)	http://securityreason.com/achievement_securityalert/82 http://securityreason.com/securityalert/7008 http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.html http://www.php.net/releases/5_3_2.php http://www.php.net/ChangeLog-5.php#5.3.2 http://www.php.net/releases/5_2_13.php http://www.php.net/ChangeLog-5.php#5.2.13	xxx.xxx.xxx.11

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:51139	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	Upgrade to PHP version 5.2.15 or later.	(blank)	http://www.php.net/releases/5_2_15.php http://www.php.net/ChangeLog-5.php#5.2.15	xxx.xxx.xx.x.11
			pluginID:51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	Upgrade to phpMyAdmin 3.4.0-beta1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2010-9.php	xxx.xxx.xx.x.11
			pluginID:51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	Upgrade to PHP 5.2.17/5.3.5 or later.	(blank)	http://bugs.php.net/bug.php?id=53632 http://www.php.net/distributions/test_bug53632.txt http://www.php.net/releases/5_2_17.php http://www.php.net/releases/5_3_5.php	xxx.xxx.xx.x.11
			pluginID:62974	Dell OpenManage Server Administrator omalogin.html DOM-based XSS	For Windows systems, upgrade to version 6.5, 7.0, or 7.1 (if necessary) and apply the appropriate patch referenced in US-CERT VU#558132. For Linux systems, there is no known solution at this time.	(blank)	http://www.nessus.org/u?c34c744f http://www.nessus.org/u?578ea62e http://www.nessus.org/u?1f5bf40c	xxx.xxx.xx.x.11
		Microsoft Windows Server 2003 Service Pack 2	pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSER from : - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes Reboot once the registry changes are complete.	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xx.x.11

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	PluginName	Solution	Metasploit_name	See_also	IP
3.medium	Intranet	Microsoft Windows Server 2008 R2	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.25
			pluginID:64263	MySQL Protocol Remote User Enumeration	There is no known solution at this time.	(blank)	http://archives.neohapsis.com/archives/fulldisclosure/2012-12/0010.html https://mariadb.atlassian.net/browse/MDEV-3909	xxx.xxx.xxx.25
			pluginID:72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.3 or later.	(blank)	http://www.nessus.org/u?ec3c1b58 http://www.securityfocus.com/archive/1/531406/30/0/threaded	xxx.xxx.xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.25
			pluginID:64263	MySQL Protocol Remote User Enumeration	There is no known solution at this time.	(blank)	http://archives.neohapsis.com/archives/fulldisclosure/2012-12/0010.html https://mariadb.atlassian.net/browse/MDEV-3909	xxx.xxx.xxx.25
			pluginID:72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.3 or later.	(blank)	http://www.nessus.org/u?ec3c1b58 http://www.securityfocus.com/archive/1/531406/30/0/threaded	xxx.xxx.xxx.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginID:10297	Web Server Directory Traversal Arbitrary File Access	Contact the vendor for an update, use a different product, or disable the service altogether.	Indusoft WebStudio NTWebServer Remote File Access	(blank)	xxx.xxx.xxx.100
			pluginID:11037	Multiple Server Crafted Request WEB-INF Directory Information Disclosure	Contact the vendor for a patch.	(blank)	(blank)	xxx.xxx.xxx.100

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	PluginName	Solution	Metasploit_name	see_also	IP
3.medium	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.100
			pluginID:26928	SSL Weak Cipher Suites Supported	Reconfigure the affected application, if possible to avoid the use of weak ciphers.	(blank)	http://www.openssl.org/docs/apps/ciphers.html	xxx.xxx.xxx.100
			pluginID:33869	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	Upgrade to JBoss EAP version 4.2.0.CP09 / 4.3.0.CP08.	(blank)	https://bugzilla.redhat.com/show_bug.cgi?id=457757 https://bugzilla.redhat.com/show_bug.cgi?id=585900	xxx.xxx.xxx.100
			pluginID:35291	SSL Certificate Signed using Weak Hashing Algorithm	Contact the Certificate Authority to have the certificate reissued.	(blank)	http://tools.ietf.org/html/rfc3279 http://www.phreedom.org/research/rogue-ca/ http://technet.microsoft.com/en-us/security/advisory/961509	xxx.xxx.xxx.100
			pluginID:42873	SSL Medium Strength Cipher Suites Supported	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.100
	PACS	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.146
	APP	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.21

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	Plugin Name	solution	metasploit_name	see_also	IP
4.low	DB	Microsoft Windows Server 2003 Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows 7 Microsoft Windows Server 2008 R2	pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.35
	E-Service	Microsoft Windows Server 2008 R2	pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx.xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx.xxx.25
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:34324	FTP Supports Clear Text Authentication	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.	(blank)	(blank)	xxx.xxx.xxx.11
		Microsoft Windows Server 2008 R2	pluginID:34324	FTP Supports Clear Text Authentication	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.	(blank)	(blank)	xxx.xxx.xxx.25
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:34324	FTP Supports Clear Text Authentication	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.	(blank)	(blank)	xxx.xxx.xxx.25
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.25

Table D-1 Risk Assessment Report Hospital A [CVSS Score] (Cont.)

Risk Rating	name	OS	Plugin ID	Plugin Name	solution	metasploit _name	see_also	IP
4.low	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Contact the vendor for specific patch information.	(blank)	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	xxx.xxx.xxx.100
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.100

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact]

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
1.critical	DB	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabiliti es	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.c om/avcenter/security/C ontent/2008.11.19.html	xxx.xxx .xxx.3
	Intran et	Microsoft Windows Server 2003 Service Pack 2	pluginI D:58987	PHP Unsupported Version Detection	Upgrade to a version of PHP that is currently supported.	(blank)	https://wiki.php.net/rfc/ releaseprocess	xxx.xxx .xxx.11
	Intran et	Microsoft Windows Server 2008 R2	pluginI D:58811	HP System Management Homepage < 7.0 Multiple Vulnerabiliti es	Upgrade to HP System Management Homepage 7.0 or later.	Apache Reverse Proxy Bypass Vulnerability Scanner	http://www.nessus.org/ u?a467ff94	xxx.xxx .xxx.25
			pluginI D:59851	HP System Management Homepage < 7.1.1 Multiple Vulnerabiliti es	Upgrade to HP System Management Homepage 7.1.1 or later.	PHP CGI Argument Injection	http://www.nessus.org/ u?541c7466 http://www.securityfoc us.com/archive/1/5233 20/30/0/threaded	xxx.xxx .xxx.25
			pluginI D:66541	HP System Management Homepage < 7.2.0.14 iprange Parameter Code Execution	Upgrade to HP System Management Homepage 7.2.0.14 or later.	HP System Management Anonymous Access Code Execution	http://www.nessus.org/ u?f2db75ce	xxx.xxx .xxx.25
			pluginI D:70118	HP System Management Homepage ginkgosnmp.i nc Command Injection	Upgrade to HP System Management Homepage 7.2.2 or later.	HP System Management Homepage JustGetSNMPQ ueue Command Injection	http://www.nessus.org/ u?81ed4efd http://www.nessus.org/ u?9b81af89 http://www.nessus.org/ u?7a9cf2bb http://www.securityfoc us.com/archive/1/5287 13/30/0/threaded	xxx.xxx .xxx.25
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginI D:34820	Symantec Backup Exec for Windows Multiple Vulnerabiliti es	Apply the appropriate hotfix referenced in the vendor advisory.	(blank)	http://www.symantec.c om/avcenter/security/C ontent/2008.11.19.html	xxx.xxx .xxx.10 0
2.high	DB	Microsoft Windows Server 2003 Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows 7 Microsoft Windows Server 2008 R2	pluginI D:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx .xxx.35
			pluginI D:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx .xxx.35
			pluginI D:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft .com/kb/887429 http://technet.microsoft .com/en-us/library/cc731957.as px http://www.nessus.org/ u?74b80723 http://www.samba.org/ samba/docs/man/manp ages-3/smb.conf.5.html	xxx.xxx .xxx.35

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit _ name	see_also	IP
2.high	DB	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx .xxx.3
	E-Servi ce	Microsoft Windows Server 2008 R2	pluginI D:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx .xxx.25
			pluginI D:46803	PHP expose_php Information Disclosure	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.	(blank)	http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324	xxx.xxx .xxx.25
			pluginI D:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	xxx.xxx .xxx.25
			pluginI D:58087	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2012-1.php	xxx.xxx .xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx .xxx.25
			pluginI D:46803	PHP expose_php Information Disclosure	In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.	(blank)	http://www.0php.com/php_easter_egg.php http://seclists.org/webappsec/2004/q4/324	xxx.xxx .xxx.25
2.high	E-Servi ce	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	Either apply the vendor patches or upgrade to phpMyAdmin version 3.4.8 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	xxx.xxx .xxx.25
			pluginI D:58087	phpMyAdmin 3.4.x < 3.4.10.1 Cross-Site Scripting (PMASA-2012-1)	Apply the vendor patches or upgrade to phpMyAdmin version 3.4.10.1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2012-1.php	xxx.xxx .xxx.25

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
2.high	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:41014	PHP < 5.2.11 Multiple Vulnerabilities	Upgrade to PHP version 5.2.11 or later.	(blank)	http://www.php.net/ChangeLog-5.php#5.2.11 http://www.php.net/releases/5_2_11.php http://news.php.net/php.internals/45597 http://www.php.net/ChangeLog-5.php#5.2.11	xxx.xxx.xxx.11
			pluginID:43351	PHP < 5.2.12 Multiple Vulnerabilities	Upgrade to PHP version 5.2.12 or later.	(blank)	http://www.nessus.org/u?57f2d08f http://www.php.net/releases/5_2_12.php http://www.php.net/ChangeLog-5.php#5.2.12	xxx.xxx.xxx.11
			pluginID:44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	Upgrade to PHP version 5.3.2 / 5.2.13 or later.	(blank)	http://securityreason.com/achievement_securityalert/82 http://securityreason.com/securityalert/7008 http://archives.neohapsis.com/archives/fulldisclosure/2010-02/0209.html http://www.php.net/releases/5_3_2.php http://www.php.net/ChangeLog-5.php#5.3.2 http	xxx.xxx.xxx.11
			pluginID:48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	Upgrade to PHP version 5.2.14 or later.	(blank)	http://www.php.net/releases/5_2_14.php http://www.php.net/ChangeLog-5.php#5.2.14	xxx.xxx.xxx.11
			pluginID:51139	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	Upgrade to PHP version 5.2.15 or later.	(blank)	http://www.php.net/releases/5_2_15.php http://www.php.net/ChangeLog-5.php#5.2.15	xxx.xxx.xxx.11
			pluginID:57537	PHP < 5.3.9 Multiple Vulnerabilities	Upgrade to PHP version 5.3.9 or later.	Hashtable Collisions	http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5 http://www.php.net/archive/2012.php#id2012-01-11-1 http://archives.neohapsis.com/archives/bugtraq/2012-01/0092.html https://bugs.php.net/bug.php?id=55475 https://bugs.php.net/bug.php?id=55776 htt	xxx.xxx.xxx.11
			pluginID:58966	PHP < 5.3.11 Multiple Vulnerabilities	Upgrade to PHP version 5.3.11 or later.	(blank)	http://www.nessus.org/u?e81d4026 https://bugs.php.net/bug.php?id=61043 https://bugs.php.net/bug.php?id=54374 https://bugs.php.net/bug.php?id=60227 http://marc.info/?l=oss-security&m=134626481806571&w=2 http://www.php.net/archive/2012.php#id2012-04-26-1 ht	xxx.xxx.xxx.11
			pluginID:58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod_rewrite' workaround is available as well.	PHP CGI Argument Injection	http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/ https://bugs.php.net/bug.php?id=61910 http://www.php.net/archive/2012.php#id2012-05-03-1 http://www.php.net/ChangeLog-5.php#5.3.12 http://www.php.net/ChangeLog-5.php#5.4.2	xxx.xxx.xxx.11

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit _ name	see_also	IP
2.high	Intranet	Microsoft Windows Server 2008 R2	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.25
			pluginID:64263	MySQL Protocol Remote User Enumeration	There is no known solution at this time.	(blank)	http://archives.neohapsis.com/archives/fulldisclosure/2012-12/0010.html https://mariadb.atlassian.net/browse/MDEV-3909	xxx.xxx.xxx.25
			pluginID:69020	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.2.1.0 or later.	PHP apache_request_headers Function Buffer Overflow	http://www.zerodayinitiative.com/advisories/ZDI-13-204/ http://www.nessus.org/u?647212eb http://www.nessus.org/u?5e861a23 http://www.securityfocus.com/archive/1/528723/30/0/threaded	xxx.xxx.xxx.25
			pluginID:72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.3 or later.	(blank)	http://www.nessus.org/u?ec3c1b58 http://www.securityfocus.com/archive/1/531406/30/0/threaded	xxx.xxx.xxx.25
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.25
			pluginID:64263	MySQL Protocol Remote User Enumeration	There is no known solution at this time.	(blank)	http://archives.neohapsis.com/archives/fulldisclosure/2012-12/0010.html https://mariadb.atlassian.net/browse/MDEV-3909	xxx.xxx.xxx.25
			pluginID:69020	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.2.1.0 or later.	PHP apache_request_headers Function Buffer Overflow	http://www.zerodayinitiative.com/advisories/ZDI-13-204/ http://www.nessus.org/u?647212eb http://www.nessus.org/u?5e861a23 http://www.securityfocus.com/archive/1/528723/30/0/threaded	xxx.xxx.xxx.25
			pluginID:72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities	Upgrade to HP System Management Homepage 7.3 or later.	(blank)	http://www.nessus.org/u?ec3c1b58 http://www.securityfocus.com/archive/1/531406/30/0/threaded	xxx.xxx.xxx.25

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
2.high	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginID:34460	Unsupported Web Server Detection	Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.100
			pluginID:69552	Oracle TNS Listener Remote Poisoning	Apply the work-around in Oracle's advisory.	(blank)	http://www.nessus.org/u?e3d5ec0b http://www.nessus.org/u?1feaed5b http://www.nessus.org/u?29d9db9b	xxx.xxx.xxx.100
	PACS	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.21

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	DB	Microsoft Windows Server 2003 Microsoft Windows Vista Microsoft Windows Server 2008 Microsoft Windows 7 Microsoft Windows Server 2008 R2	pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.35
	E-Service	Microsoft Windows Server 2008 R2	pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx.xxx.25
	Intranet	Microsoft Windows Server 2003 Service Pack 2	pluginID:11229	Web Server info.php / phpinfo.php Detection	Remove the affected file(s).	(blank)	(blank)	xxx.xxx.xxx.11
			pluginID:35750	PHP < 5.2.9 Multiple Vulnerabilities	Upgrade to PHP version 5.2.9 or later.	(blank)	http://news.php.net/php.internals/42762 http://www.php.net/releases/5_2_9.php http://www.php.net/ChangeLog-5.php#5.2.9	xxx.xxx.xxx.11
			pluginID:39480	PHP < 5.2.10 Multiple Vulnerabilities	Upgrade to PHP version 5.2.10 or later.	(blank)	http://bugs.php.net/bug.php?id=45997 http://bugs.php.net/bug.php?id=48378 http://www.php.net/releases/5_2_10.php http://www.php.net/ChangeLog-5.php#5.2.10	xxx.xxx.xxx.11
			pluginID:51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	Upgrade to phpMyAdmin 3.4.0-beta1 or later.	(blank)	http://www.phpmyadmin.net/home_page/security/PMASA-2010-9.php	xxx.xxx.xxx.11
			pluginID:51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	Upgrade to PHP 5.2.17/5.3.5 or later.	(blank)	http://bugs.php.net/bug.php?id=53632 http://www.php.net/distributions/test_bug53632.txt http://www.php.net/releases/5_2_17.php http://www.php.net/releases/5_3_5.php	xxx.xxx.xxx.11
			pluginID:62974	Dell OpenManage Server Administrator omalogin.html DOM-based XSS	For Windows systems, upgrade to version 6.5, 7.0, or 7.1 (if necessary) and apply the appropriate patch referenced in US-CERT VU#558132. For Linux systems, there is no known solution at this time.	(blank)	http://www.nessus.org/u?c34c744f http://www.nessus.org/u?578ea62e http://www.nessus.org/u?1f5bf40c	xxx.xxx.xxx.11
			pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSE	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xxx.11

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
3.mediu m	Intran et	Microso ft Window s Server 2008 R2	pluginI D:34324	FTP Supports Clear Text Authentication	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.	(blank)	(blank)	xxx.xxx. xxx.25
			pluginI D:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx. xxx.25
	LIS	Microso ft Window s Server 2003 Service Pack 2	pluginI D:10297	Web Server Directory Traversal Arbitrary File Access	Contact the vendor for an update, use a different product, or disable the service altogether.	Indusoft WebStudio NTWebServe r Remote File Access	(blank)	xxx.xxx. xxx.100
			pluginI D:11037	Multiple Server Crafted Request WEB-INF Directory Information Disclosure	Contact the vendor for a patch.	(blank)	(blank)	xxx.xxx. xxx.100
			pluginI D:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx. xxx.100
			pluginI D:26928	SSL Weak Cipher Suites Supported	Reconfigure the affected application, if possible to avoid the use of weak ciphers.	(blank)	http://www.openssl.org/docs/apps/ciphers.html	xxx.xxx. xxx.100
			pluginI D:33869	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	Upgrade to JBoss EAP version 4.2.0.CP09 / 4.3.0.CP08.	(blank)	https://bugzilla.redhat.com/show_bug.cgi?id=457757 https://bugzilla.redhat.com/show_bug.cgi?id=585900	xxx.xxx. xxx.100
			pluginI D:35291	SSL Certificate Signed using Weak Hashing Algorithm	Contact the Certificate Authority to have the certificate reissued.	(blank)	http://tools.ietf.org/html/rfc3279 http://www.phreedom.org/research/rogue-ca/ http://technet.microsoft.com/en-us/security/advisory/961509	xxx.xxx. xxx.100
			pluginI D:42873	SSL Medium Strength Cipher Suites Supported	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	(blank)	(blank)	xxx.xxx. xxx.100
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.100
	PACS	Microso ft Window s Server 2008 Enterpri se Service Pack 2	pluginI D:57608	SMB Signing Required	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for furthe	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx. xxx.146

Table D-2 Risk Assessment Report Hospital A [OWASP + Business Impact] (Cont.)

Risk Rating	name	OS	Plugin ID	pluginName	solution	metasploit_ name	see_also	IP
4.low	Intran et	Microsoft Windows Server 2003 Service Pack 2	pluginI D:34324	FTP Supports Clear Text Authentication	Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server so that control connections are encrypted.	(blank)	(blank)	xxx.xxx. xxx.11
	LIS	Microsoft Windows Server 2003 Service Pack 2	pluginI D:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.100
			pluginI D:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Contact the vendor for specific patch information.	(blank)	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	xxx.xxx. xxx.100
			pluginI D:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx. xxx.100

Table D-3 Risk Assessment Report Hospital B [CVSS Score]

Risk	name	OS	pluginID	pluginName	solution	metasploit_name	see_also	IP
1.critical	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:40887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Microsoft has released a patch for Windows Vista and Windows Server 2008.	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	http://www.nessus.org/u?0f72ec72 http://technet.microsoft.com/en-us/security/bulletin/MS09-050	xxx.xxx.xxx.38
2.high	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx.xxx.38
	pacsccc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx.xxx.13
3.medium	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.38
			pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.38
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.38

Table D-3 Risk Assessment Report Hospital B [CVSS Score] (Cont.)

Risk	name	OS	pluginID	pluginName	solution	metasploit_name	see_also	IP
3.medium	ccchis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.1
			pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.1
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.1
	ccclis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.3
			pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.3
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.3

Table D-3 Risk Assessment Report Hospital B [CVSS Score] (Cont.)

Risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	pacsccc1	Microsoft Windows Server 2003	pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSE	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xxx.12
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.11
		Microsoft Windows Server 2003 Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.13
			pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSE	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xxx.13
			pluginID:26928	SSL Weak Cipher Suites Supported	Reconfigure the affected application, if possible to avoid the use of weak ciphers.	(blank)	http://www.openssl.org/docs/apps/ciphers.html	xxx.xxx.xxx.13
			pluginID:35291	SSL Certificate Signed using Weak Hashing Algorithm	Contact the Certificate Authority to have the certificate reissued.	(blank)	http://tools.ietf.org/html/rfc3279 http://www.phreedom.org/research/rogue-ca/ http://technet.microsoft.com/en-us/security/advisory/961509	xxx.xxx.xxx.13
			pluginID:42873	SSL Medium Strength Cipher Suites Supported	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.13
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.13

Table D-3 Risk Assessment Report Hospital B [CVSS Score] (Cont.)

Risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	web33ccc	Microsoft Windows Server 2008 R2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.33
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.33
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.33
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.33
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
	webcc1	Microsoft Windows Server 2008 R2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.33
			pluginID:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.33
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33

Table D-3 Risk Assessment Report Hospital B [CVSS Score] (Cont.)

Risk	name	OS	Plugin ID	pluginName	solution	metasploit _ name	see_also	IP
3.medium	webccc1	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xxx.33
			pluginID:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.33
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
4.low	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.38
	ccchis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.1
	ccclis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.3
	pacsccc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Contact the vendor for specific patch information.	(blank)	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	xxx.xxx.xxx.13
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xxx.13

Table D-3 Risk Assessment Report Hospital B [CVSS Score] (Cont.)

Risk	name	OS	Plugin ID	pluginName	solution	metasploit _ name	see_also	IP
4.low	web3 3ccc	Microsoft Windows Server 2008 R2	pluginI D:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.33
	webc cc1	Microsoft Windows Server 2008 R2	pluginI D:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx. xxx.33
			pluginI D:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.33
			pluginI D:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slide s.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx. xxx.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx. xxx.33
			pluginI D:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx. xxx.33
			pluginI D:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slide s.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx. xxx.33

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact]

risk	name	tag	pluginID	pluginName	solution	metasploit_name	see_also	IP
1.critical	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:40887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	Microsoft has released a patch for Windows Vista and Windows Server 2008.	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	http://www.nessus.org/u?0f72ec72 http://technet.microsoft.com/en-us/security/bulletin/MS09-050	xxx.xxx.xxx.38
			pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx.xxx.38
	pacsccc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2 : http://technet.microsoft.com/en-us/security/bulletin/ms12-020	MS12-020 Microsoft Remote Desktop Checker	(blank)	xxx.xxx.xxx.13
2.high	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.38
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.38
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.38
	ccchis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.1
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.1
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.1

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact] (Cont.)

risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
2.high	ccclis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.3
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.3
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.3
	pacsccc1	Microsoft Windows Server 2003	pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSE	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xxx.12
			pluginID:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.11
		Microsoft Windows Server 2003 Service Pack 2	pluginID:26920	Microsoft Windows SMB NULL Session Authentication	Apply the following registry changes per the referenced Technet advisories : Set : HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1 HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1 Remove BROWSE	(blank)	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	xxx.xxx.xxx.13
			pluginID:26928	SSL Weak Cipher Suites Supported	Reconfigure the affected application, if possible to avoid the use of weak ciphers.	(blank)	http://www.openssl.org/docs/apps/ciphers.html	xxx.xxx.xxx.13
			pluginID:42873	SSL Medium Strength Cipher Suites Supported	Reconfigure the affected application if possible to avoid use of medium strength ciphers.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:45411	SSL Certificate with Wrong Hostname	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13
			pluginID:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.13

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact] (Cont.)

risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
2.high	pacsc cc1	Microsoft Windows Server 2003 Service Pack 2	pluginI D:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.13
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.13
	web33ccc	Microsoft Windows Server 2008 R2	pluginI D:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.33
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57608	SMB Signing Disabled	Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	(blank)	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	xxx.xxx.xxx.33
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
	webcc1	Microsoft Windows Server 2008 R2	pluginI D:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.33
			pluginI D:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginI D:33270	ASP.NET DEBUG Method Enabled	Make sure that DEBUG statements are disabled or only usable by authenticated users.	(blank)	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	xxx.xxx.xxx.33
			pluginI D:51192	SSL Certificate Cannot Be Trusted	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57582	SSL Self-Signed Certificate	Purchase or generate a proper certificate for this service.	(blank)	(blank)	xxx.xxx.xxx.33
			pluginI D:57690	Terminal Services Encryption Level is Medium or Low	Change RDP encryption level to one of : 3. High 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xxx.33

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact] (Cont.)

risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	cccdb	Microsoft Windows Server 2008 Enterprise Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.38
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.38
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls	xxx.xxx.xx.38
	ccchis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.1
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.1
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls	xxx.xxx.xx.1
	ccclis	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.3
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.3
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls	xxx.xxx.xx.3
	pacsccc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.13
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.13
			pluginID:35291	SSL Certificate Signed using Weak Hashing Algorithm	Contact the Certificate Authority to have the certificate reissued.	(blank)	http://tools.ietf.org/html/rfc3279 http://www.phreedom.org/research/rogue-ca/ http://technet.microsoft.com/en-us/security/advisory/961509	xxx.xxx.xx.13

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact] (Cont.)

risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	pacsccc1	Microsoft Windows Server 2003 Service Pack 2	pluginID:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Contact the vendor for specific patch information.	(blank)	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	xxx.xxx.xx.x.13
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xx.x.13
	web33ccc	Microsoft Windows Server 2008 R2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.x.33
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.x.33
		Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.x.33
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.x.33
	webccc1	Microsoft Windows Server 2008 R2	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.x.33
			pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx.xx.x.33
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.x.33
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xx.x.33

Table D-4 Risk Assessment Report Hospital B [OWASP + Business Impact] (Cont.)

risk	name	OS	Plugin ID	pluginName	solution	metasploit_name	see_also	IP
3.medium	webccl	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	- Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	(blank)	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	xxx.xxx.xx.33
			pluginID:26194	Web Server Uses Plain Text Authentication Forms	Make sure that every sensitive form transmits content over HTTPS.	(blank)	(blank)	xxx.xxx.xx.33
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	Change RDP encryption level to : 4. FIPS Compliant	(blank)	(blank)	xxx.xxx.xx.33
			pluginID:65821	SSL RC4 Cipher Suites Supported	Reconfigure the affected application, if possible, to avoid use of RC4 ciphers.	(blank)	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	xxx.xxx.xx.33

APPENDIX E
VULNERABILITY VERIFY RESULT

Table E-1 Verify Vulnerability Hospital A

cvss	Owasp+	cve	pluginID	pluginName	see_also	fulldisc	fullink	exdbink	metasploit_name	IP
1.critical	1.critical	CVE-2008-5407	pluginID:34820	Symantec Backup Exec for Windows Multiple Vulnerabilities	http://www.symantec.com/avcenter/security/Content/2008.11.19.html	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100 xxx.xxx.xxx.3
		CVE-2009-0037	pluginID:58811	HP System Management Homepage < 7.0 Multiple Vulnerabilities	http://www.nessus.org/u?a467ff94	NULL	NULL	NULL	Apache Reverse Proxy Bypass Vulnerability Scanner	xxx.xxx.xxx.25
		(blank)	pluginID:58987	PHP Unsupported Version Detection	https://wiki.php.net/rfc/releaseprocess	NULL	NULL	NULL	NULL	xxx.xxx.xxx.11
2.high	1.critical	CVE-2012-0002	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	http://technet.microsoft.com/en-us/security/bulletin/ms12-020	NULL	NULL	NULL	MS12-020 Microsoft Remote Desktop Checker	xxx.xxx.xxx.51
		CVE-2013-3576	pluginID:70118	HP System Management Homepage ginkgosnmp.inc Command Injection	http://www.nessus.org/u?81ed4efd http://www.nessus.org/u?9b81af89 http://www.nessus.org/u?7a9cf2bb http://www.securityfocus.com/archive/1/528713/30/0/threaded	NULL	NULL	NULL	HP System Management Homepage JustGetSNMPQueue Command Injection	xxx.xxx.xxx.25
	2.high	CVE-2011-3379	pluginID:57537	PHP < 5.3.9 Multiple Vulnerabilities	http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application_PHP5 http://www.php.net/archive/2012.php#id2012-01-11-1 http://archives.neohapsis.com/archives/bugtraq/2012-01/0092.html https://bugs.php.net/bug.php?id=55475 https://bugs.php.net/bug.php?id=55776 htt	NULL	NULL	NULL	Hashtable Collisions	xxx.xxx.xxx.11
		CVE-2011-3389	pluginID:69020	HP System Management Homepage < 7.2.1.0 Multiple Vulnerabilities	http://www.zerodayinitiative.com/advisories/ZDI-13-204/ http://www.nessus.org/u?647212eb http://www.nessus.org/u?5e861a23 http://www.securityfocus.com/archive/1/528723/30/0/threaded	NULL	NULL	NULL	PHP apache_request_headers Function Buffer Overflow	xxx.xxx.xxx.25
		CVE-2012-1675	pluginID:69552	Oracle TNS Listener Remote Poisoning	http://www.nessus.org/u?e3d5ec0b http://www.nessus.org/u?1feaed5b http://www.nessus.org/u?29d9db9b	FULLDISC:20120418 The history of a -probably- 13 years old Oracle bug: TNS Poison	http://seclists.org/fulldisclosure/2012/Apr/date.html	http://www.exploit-db.com/exploits/34361/	NULL	xxx.xxx.xxx.100
		(blank)	pluginID:34460	Unsupported Web Server Detection	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100

Table E-1 Verify Vulnerability Hospital A (Cont.)

cvss	Owasp+	cve	pluginID	pluginName	see_also	fulldisc	fullink	exdbink	metasploit_name	IP
3.medium	2.high	CVE-2009-3557	pluginID:43351	PHP < 5.2.12 Multiple Vulnerabilities	http://www.nessus.org/u?57f2d08f http://www.php.net/releases/5_2_12.php http://www.php.net/ChangeLog-5.php#5.2.12	NULL	NULL	NULL	NULL	xxx.xxx.xxx.11
		CVE-2011-4634	pluginID:57337	phpMyAdmin 3.4.x < 3.4.8 Cross-Site Scripting (PMASA-2011-18)	http://www.phpmyadmin.net/home_page/security/PMASA-2011-18.php	http://archives.neohapsis.com/archives/vulnwatch/2007-q1/index.html	http://archives.neohapsis.com/archives/vulnwatch/2007-q1/index.html	NULL	NULL	xxx.xxx.xxx.25
		CVE-2012-5615	pluginID:64263	MySQL Protocol Remote User Enumeration	http://archives.neohapsis.com/archives/fulldisclosure/2012-12/0010.html https://mariadb.atlassian.net/browse/MDEV-3909	FULLDISC:20121201 MySQL Remote Preauth User Enumeration Zeroday	http://seclists.org/fulldisclosure/2012/Dec/date.html	NULL	NULL	xxx.xxx.xxx.25
		CVE-2013-4846	pluginID:72959	HP System Management Homepage < 7.3 Multiple Vulnerabilities	http://www.nessus.org/u?ec3c1b58 http://www.securityfocus.com/archive/1/531406/30/0/threaded	NULL	NULL	NULL	NULL	xxx.xxx.xxx.25
		(blank)	pluginID:51192	SSL Certificate Cannot Be Trusted	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100 xxx.xxx.xxx.35
			pluginID:57608	SMB Signing Required	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	NULL	NULL	NULL	NULL	xxx.xxx.xxx.21 xxx.xxx.xxx.25 xxx.xxx.xxx.3 xxx.xxx.xxx.35
	3.medium	CVE-1999-0519	pluginID:26920	Microsoft Windows SMB NULL Session Authentication	http://support.microsoft.com/kb/q143474/ http://support.microsoft.com/kb/q246261/ http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx	NULL	NULL	NULL	NULL	xxx.xxx.xxx.11
		CVE-2000-0920	pluginID:10297	Web Server Directory Traversal Arbitrary File Access	NULL	NULL	NULL	NULL	Indusoft WebStudio NTWebServer Remote File Access	xxx.xxx.xxx.100
		CVE-2005-1794	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100 xxx.xxx.xxx.51
		CVE-2008-3273	pluginID:33869	JBoss Enterprise Application Platform (EAP) Status Servlet Request Remote Information Disclosure	https://bugzilla.redhat.com/show_bug.cgi?id=457757 https://bugzilla.redhat.com/show_bug.cgi?id=585900	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100

Table E-1 Verify Vulnerability Hospital A (Cont.)

cvss	Owasp+	cve	pluginID	pluginName	see_also	fulldisc	fullink	exdbink	metasploit_name	IP
3.medium	3.medium	CVE-2010-4480	pluginID:51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)	http://www.phpmyadmin.net/home_page/security/PMASA-2010-9.php	NULL	NULL	http://www.exploit-db.com/exploits/15699/	NULL	xxx.xxx.xxx.11
		CVE-2012-4955	pluginID:62974	Dell OpenManage Server Administrator omalogin.html DOM-based XSS	http://www.nessus.org/u?c34c744f http://www.nessus.org/u?578ea62e http://www.nessus.org/u?1f5bf40c	NULL	NULL	NULL	NULL	xxx.xxx.xxx.11
		(blank)	pluginID:42873	SSL Medium Strength Cipher Suites Supported	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100
			pluginID:57608	SMB Signing Required	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	NULL	NULL	NULL	NULL	xxx.xxx.xxx.146 xxx.xxx.xxx.51
4.low	3.medium	CVE-2013-2566	pluginID:65821	SSL RC4 Cipher Suites Supported	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	NULL	NULL	NULL	NULL	xxx.xxx.xxx.25 xxx.xxx.xxx.35
		(blank)	pluginID:26194	Web Server Uses Plain Text Authentication Forms	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.25
			pluginID:34324	FTP Supports Clear Text Authentication	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.25
	4.low	CVE-2009-3555	pluginID:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	FULLDISC:20091111 Re: SSL/TLS MiTM PoC	http://seclists.org/fulldisclosure/2009/Nov/date.html	NULL	NULL	xxx.xxx.xxx.100
		(blank)	pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.100 xxx.xxx.xxx.51
			pluginID:34324	FTP Supports Clear Text Authentication	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.11

Table E-2 Verify Vulnerability Hospital B

cvss	Owasp +	cve	PluginID	Plugin Name	See_also	Fulldisc	Fullink	Exdbink	Metasploit_name	IP
1.critical	1.critical	CVE-2009-3103	pluginID:40887	MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)	http://www.nessus.org/u?0f72ec72 http://technet.microsoft.com/en-us/security/bulletin/MS09-050	FULLDISC:20090907 Windows Vista/7 : SMB2.0 NEGOTIATE PROTOCOL REQUEST Remote B.S.O.D.	http://seclists.org/fulldisclosure/2009/Sep/date.html	NULL	Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference	xxx.xxx.xxx.38
2.high	1.critical	CVE-2012-0002	pluginID:58435	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	NULL	NULL	NULL	NULL	MS12-020 Microsoft Remote Desktop Checker	xxx.xxx.xxx.13
										xxx.xxx.xxx.38
3.medium	2.high	(blank)	pluginID:33270	ASP.NET DEBUG Method Enabled	http://support.microsoft.com/default.aspx?scid=kb;en-us;815157	NULL	NULL	NULL	NULL	xxx.xxx.xxx.33
			pluginID:45411	SSL Certificate with Wrong Hostname	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.13
										xxx.xxx.xxx.38
			pluginID:57608	SMB Signing Disabled	http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html	NULL	NULL	NULL	NULL	xxx.xxx.xxx.1
										xxx.xxx.xxx.11
										xxx.xxx.xxx.13
										xxx.xxx.xxx.3
										xxx.xxx.xxx.33
										xxx.xxx.xxx.38
			pluginID:57690	Terminal Services Encryption Level is Medium or Low	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.1
										xxx.xxx.xxx.13
										xxx.xxx.xxx.3
										xxx.xxx.xxx.33

Table E-2 Verify Vulnerability Hospital B (Cont.)

cvss	Owasp +	cve	PluginID	Plugin Name	See_also	Fulldisc	Fullink	Exdbink	Metasploit_name	IP
3.medium	3.medium	CVE-2004-2761	pluginID:35291	SSL Certificate Signed using Weak Hashing Algorithm	http://tools.ietf.org/html/rfc3279 http://www.phreedom.org/research/rogue-ca/ http://technet.microsoft.com/en-us/security/advisory/961509	NULL	NULL	NULL	NULL	xxx.xxx.xxx.13
		CVE-2005-1794	pluginID:18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	http://www.oxid.it/downloads/rdp-gbu.pdf http://www.nessus.org/u?e2628096 http://technet.microsoft.com/en-us/library/cc782610.aspx	NULL	NULL	NULL	NULL	xxx.xxx.xxx.1 xxx.xxx.xxx.13 xxx.xxx.xxx.3 xxx.xxx.xxx.33 xxx.xxx.xxx.38
4.low	3.medium	CVE-2009-3555	pluginID:42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	http://www.ietf.org/mail-archive/web/tls/current/msg03948.html http://www.g-sec.lu/practicaltls.pdf http://tools.ietf.org/html/rfc5746	FULLDISC:20091111 Re: SSL/TLS MiTM PoC	http://seclists.org/fulldisclosure/2009/Nov/date.html	NULL	NULL	xxx.xxx.xxx.13
		CVE-2013-2566	pluginID:65821	SSL RC4 Cipher Suites Supported	http://www.nessus.org/u?217a3666 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/	NULL	NULL	NULL	NULL	xxx.xxx.xxx.1 xxx.xxx.xxx.3 xxx.xxx.xxx.33 xxx.xxx.xxx.38
		(blank)	pluginID:26194	Web Server Uses Plain Text Authentication Forms	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.33
			pluginID:30218	Terminal Services Encryption Level is not FIPS-140 Compliant	NULL	NULL	NULL	NULL	NULL	xxx.xxx.xxx.13 xxx.xxx.xxx.33

BIOGRAPHY

NAME	Mr. Surapol Ruaysungnoen
DATE OF BIRTH	16 April 1982
PLACE OF BIRTH	Chiyaphum, Thailand
INSTITUTION ATTENDED	Kanchanabhishek Institute of Medical and Public Health Technology Praboromarajchanok Institute, 2001-2002 Certificate in Medical Record Science Mahidol University, 2004-2005 Bachelor of Science (Computer Science) Mahidol University, 2012-2015 Master of Engineering (Computer Engineering)
HOME ADDRESS	365/1 Moo 2 Pakpung Phukhieo Chaiyaphum 3610 Tel. 084-0809005 E-mail : sprspr_or@hotmail.com
PUBLICATION/ PRESENTATION	Surapol Ruaysungnoen, A Prototype Tool for Security and Risk Assessment in Hospital IT System