全球商業經營管理學報
第十一期 108.09 page 121-132
ISSN：2076-9474

Research on Website Penetration Test

網站滲透測試研究

Wei-Ming Ma[a]

摘要

資訊技術時代的新趨勢，如：雲端運算、大數據、物聯網和人工智慧。企業被要求需建構許多與服務相關的服務資訊系統，以便在客戶和企業之間建立快速便捷的連結。本研究目的是透過分別由資訊安全攻擊方和防守方雙方的實際資訊安全攻防演練，瞭解企業外部服務資訊系統是否存在任何資訊安全漏洞，並提出建議立即修復，加強其安全防護能力，以及行使。採用的主要網站滲透測試工具，如：Hydra、NMAP、Burp Suite Professional 等，同時希望新手資訊安全調查員能夠獲得一些關於網站漏洞的實務傳承經驗，以提昇其滲透技能。

關鍵詞：資訊技術、安全漏洞、資訊安全、滲透測試

ABSTRACT

New trends in the information technology era such as cloud, big data, Internet of Things, and artificial intelligence. Enterprises are not actively building many service-related services information systems to build a fast and convenient connection between customers and enterprises. This research intends to understand whether there is any unfunded vulnerability in the external service information system of the enterprise through the actual information security attack and defense drills and to immediately repair and strengthen its security protection capabilities, as well as the exercise of the information security offensive and defensive team. The major website penetration testing tools used are Hydra, NMAP, Burp Suite Professional. At the meantime, the novice investigators may gain some hands-on experience on website vulnerability for improving their penetration skills.

Keywords: Information Technology, Vulnerability, Information Security, Penetration Testing

1. Introduction

In this section, the Research Background, Research Goal, and Research Method described.

1.1. Research Background

New trends in the information technology era such as cloud, big data, Internet of Things, and artificial intelligence. Enterprises are not actively building many service-related services information systems to build a fast and convenient connection between customers and enterprises. However, they are highly dependent on information service systems. At the same time, as a convenience, the harm caused by information security issues has also increased. If the information security problems occur in the enterprise, in addition to affecting the reputation of the enterprise, the more serious ones may allow the customer's sensitive personal information (address, account information, property, medical records.) leaked.

The company must implement the information security assessment attack and defense exercise program annually. Through the cooperation model of the project, the enterprise information center provides the external service information system as an empirical field, and through the academic community's security attack and defense team to conduct a practical operation network. Attack and defense drills to understand whether the enterprise information service system has potential weaknesses or security vulnerabilities and repair it immediately to enhance information security protection capabilities.

This research the enterprise cooperates with Cheng Shiu Universities to conduct practical information security attack and defense training exercises. On the one hand, it is expected to stimulate

[a] MIS, CSU Associate Professor Email: k3666@gcloud.csu.edu.tw

students' enthusiasm for information security learning and to train professionals with technical skills; on the other hand, they hope to be in the process of information security attack and defense drills. Understand whether there are any unfamiliar security loopholes in the information system of the government, and repair and strengthen its security protection capabilities. Finally, this success story will be extended to other enterprises to promote the cooperation model between the enterprise and the university. The effect of the area joint defense.

1.2. Research Goal

This research intends to understand whether there is any unfunded vulnerability in the external service information system of the enterprise through the actual information security attack and defense drills and to immediately repair and strengthen its security protection capabilities, as well as the exercise of the information security offensive and defensive team. The results are scored and rewarded to encourage students to continue to develop professional skills to become highly skilled professionals.

1.3. Research Method

The target websites for practicing web penetration testing setup, such as Dojo with Damn Vulnerable Web Application, and OWASP Broken Web Applications. The major website penetration tools used are Hydra, NMAP, Burp Suite Professional. The novice investigators may gain some hand-on experience for improving their penetration skills.

2. Literature Reviews

The previous studies about The Open Web Application Security Project (OWASP) Top 10 Application Security Risks, Hydra, Nmap, and Burp Suite Professional briefly described.

2.1. OWASP Top 10 Application Security Risks

OWASP Top 10 Application Security Risks include Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfiguration, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities, and

Insufficient Logging & Monitoring. Explanation and preventions for the security risks described as shown in Table 1.

2.2. Hydra

For any security investigator, ensuring Secure Shell (SSH) passwords are secure should be a top priority. Hydra is a network login cracker, and it can be used online to find login passwords by brute-force attack network services. A brute force attack is attempting all the possible combinations of characters to guess the correct password. The chance of hitting the right password is directly proportional to the quality of the dictionary file. Hydra tested over several protocols, including HTTP, POP3, SMB, SSHv2, RDP, and many more (Ansari, 2015).

Hydra installed by default on Kali. There are both command line and graphical versions of Hydra. Hydra is capable of running through massive lists of usernames, passwords, and targets to test if a user is applying a potentially vulnerable password. It can also be tuned using its many flags for accounting for several additional situations and providing an investigator with detailed output, as shown in Table 2.

2.3. Nmap

Nmap, Network Mapper, is a free and open-source utility for network discovery and information security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services such as application name and version, those hosts are offering, what operating systems and OS versions they are running, what type of packet filters/firewalls are in use, and other characteristics. It was designed to scan large networks but works fine against single hosts rapidly. Nmap runs on all major computer operating systems such as Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results in Zenmap viewer, a flexible data transfer, redirection, and Ncat debugging tool, a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nmap, 2019)

2.4. Burp Suite Professional

Burp Suite is an application also a local web proxy that allows the investigator to manually modify, intercept, and inspect Http/Https requests and responses between an investigator's browser and the target website that are trying to test web application security. While the investigator navigates

through the web application manually, the tool intercepts all of the necessary details on all visited pages. The traffic between the server and the browser can be analyzed, modified, visualized, and, eventually, repeated multiple times. The professional version of Burp allows the investigator to scan and find web application vulnerabilities (Khawaja, 2018).

Table 1 2017 OWASP Top 10 Application Security Risks

Security Risks	Explanation	Preventions
Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.	● The preferred option is to use a safe API. ● Use positive or "whitelist" server-side input validation. ● It uses the specific escape syntax for that interpreter. ● Use LIMIT and other SQL controls within queries
Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	● Implement multi-factor authentication. ● Do not ship or deploy with any default credentials. ● Align password length, complexity, and rotation policies. ● Ensure registration, credential recovery. ● Limit or increasingly delay failed login attempts. ● Use a server-side, secure.
Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.	● Classify data processed, stored, or transmitted by an application. ● Apply controls as per the classification. ● Don't store sensitive data unnecessarily. ● Make sure to encrypt all sensitive data at rest. ● Ensure up-to-date and strong standard algorithms, protocols, and keys are in place. ● Encrypt all data in transit with secure protocols. ● Disable caching for a response that contains sensitive data. ● Store passwords using strong adaptive and salted hashing functions with a work factor. ● Verify the effectiveness of configuration and settings independently.
XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	● Whenever possible, use less complex data formats ● Patch or upgrade all XML processors and libraries ● Disable XML external entity and DTD processing in the application. ● Implement positive ("whitelisting") server-side input validation. ● Verify that XML or XSL file upload functionality validates incoming XML using XSD validation or similar. ● SAST tools can help detect XXE in source code
Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and data, such as access to other users' accounts, view sensitive files, modify other users' data, change access rights, and so forth.	● Except public resources, deny by default. ● Implement access control mechanisms once and re-use throughout. ● Model access controls should enforce record ownership. ● Unique application business limit requirements ● Disable web server directory listing and ensure file metadata. ● Log access control failures. ● Rate limit API and controller access. ● JWT tokens should invalidate on the server after logout.

Table 1 2017 OWASP Top 10 Application Security Risks(continued.)

Security Risks	Explanation	Preventions
Security Misconfiguration	Security misconfiguration is the most commonly seen issue. It is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must patch/upgrade in a timely fashion.	● A repeatable hardening process is properly locked down. ● A minimal platform is without any unnecessary features, components, documentation, and samples. ● A task to review and update the configurations appropriate to all security notes. ● A segmented application architecture. ● It is sending security directives to clients. ● An automated process to verify the effectiveness.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation, escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	● It uses frameworks that automatically escape XSS by design. ● It escapes untrusted HTTP request data based on the context in the HTML output. ● It applies context-sensitive encoding on the client-side acts against DOM XSS. ● Enabling a defense-in-depth mitigating control against XSS
Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.	● It implemented integrity checks such as digital signatures on any serialized objects. ● It enforces strict type constraints during deserialization. ● Isolating and running code. ● Log deserialization exceptions and failures. ● Restricting or monitoring incoming and outgoing network connectivity. ● Monitoring deserialization.
Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component exploited, such an attack could facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.	● Remove unused dependencies unnecessary features, components, files, and documentation. ● Continuously inventory the versions of both client-side and server-side components and their dependencies using tools. ● Only obtain components from official sources over secure links. ● Monitor for libraries and components that are unmaintained or do not create security patches for older versions.
Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to attack systems further, maintain persistence, pivot to more systems, and tamper, extract or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.	● Ensure all login, access control failures sufficient time to allow delayed forensic analysis. ● Ensure that logs generated in a format. ● Ensure high-value transactions have an audit trail with integrity controls. ● Establish effective monitoring and alerting. ● Establish or adopt an incident response and recovery plan.

(From OWASP, 2019)

Table 2 Hydra Commands for Different Services

Service	Protocol	Port Number	Command
FTP	FTP	21	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] ftp://[IP address]
SSH	SSH	22	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] ssh://[IP address]
Telnet	Telnet	23	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] telnet://[IP address]
Microsoft SQL Server (MSSQL)	TCP	1433	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] mssql://[IP address]
MySQL	TCP	3306	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] mysql://[IP address]
Remote Desktop Protocol (RDP)	TCP/UDP	3389	hydra -t 10 -V -f -L [users dic file path] -P [passwords dic file path] rdp://[IP address]

(From Hauser, and Kessler, 2013)

Burp Suite has two editions that are available for download: Burp Suite Community Edition is free, but another Burp Suite Professional Edition should pay for a yearly license. In this research, the Burp Suite Professional Trail Edition for 30 days was used to investigate web application security. A penetration tester requires to use of the Burp Suite to test a target application. This research explained on downloading and installing OWASP applications contained within a virtual machine (VM). Such applications use throughout the study as targeted vulnerable web applications. Burp suite Pro was configured a Firefox web browser to use the Burp Proxy Listener. This listener is required to capture HTTP traffic between the Burp and the target web application in VM. Default settings for the listener include an Internet Protocol (IP) address, 127.0.0. 1, and port number 8080 (Stuttard and Pinto, 2011; Gilberto, 2016; Portswigger, 2019; Wear, 2018).

2.5. The Target Website for Practicing Web Penetration Testing

In this research, the Dojo, OWASP are used to demonstrate the website vulnerability. Web Security Dojo is a preconfigured, stand-alone training environment for Web Application Security with IP: 192.168.168.5. For learning and practicing web-app security testing techniques. It does not need a network connection since it contains both tools and targets. Therefore, it is ideal for self-study, training classes, and conferences. Also, this removes the possibility of a remote attack on the targets, which are insecure by design. Manual proxy configures HTTP proxy 127.0.0.1:8001 to access the internet and use this proxy server for all protocols.

In Dojo, open a Firefox browser to click Damn Vulnerable Web Application (DVWA) which is a PHP/MySQL web application that is damn vulnerable. DVWA is free software: Its' main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a classroom environment.

OWASP Broken Web Applications (BWA) Project is a collection of vulnerable web applications that distributed on a Virtual Machine (VM). The OWASPBWA produces a VM running a variety of applications with known vulnerabilities for studying in learning about web application security, testing manual assessment techniques, testing automated tools, source code analysis tools, observing web attacks, testing WAFs and similar code technologies. All the while saving learner interested in doing either learning or testing the pain of having to compile, configure and catalog all of the things normally involved in doing this process from scratch (OWASP, 2019).

3. Implementation of Website Penetration Testing

In this section described Building Attacking Computer Environment, Attack Principles, and Defensive Working Instructions, Major Violations,

Network Map for the VM Target Website, Password Cracked for the VM Target Website.

3.1. Building Attacking Computer Environment

(1) The attacking computer environment: Provide attacker computer (Windows and Kali Linux) environment:

a. Windows operating system: (a) Version: windows seven Professional X64. (b) Permission: User.

b. Software: (a) John the riper, (b) Nmap, (c) SQL map, (d) hydra, (e) Burp Suite

c. Kali Linux operating system: The visual requirements determine whether to remove the scanning software (such as Nessus), and the rest remain applications.

d. Monitoring software: (a) Install software that monitors and records the behavior of the attacker as evidence of incident handling.

(2) The defensive side of the computer environment: Provide defensive computer Windows environment, the operating system version is windows seven Professional X64.

(3) The attacker should pay attention to the following when logging in:

a. Each member provided with a dedicated account number. Please change his/her password when he/she log in for the first time and do not inform others of the password information.

b. Please do not try to crack other people's accounts, and please remember the password information of individual systems.

c. At the end of the operation, please log out the account, but do not "shut down."

(4) Website Security Impact Assessment, as shown in Table 3.

(5) Impact Assessment for Types of Attack, as shown in Table 4.

Table 3 Impact Assessment

	High impact	**Low impact**	**Info impact**
Confidentiality Obtaining information or file content that is unpublished or authorized	● The authorized management account password ● Sensitive information ● Sensitive and successful further use of web code ● A large number of customer (10 or more)	● Test account password ● Non-Sensitive but non-public information ● Sensitive but not successful in further exploiting web code (SQL field, may affect website security code) ● A small number of customers	● The general user account password ● Public information but abnormal access ● Generally, no further use of web code (pure functional code) ● currently, there is no direct and effective impact exploit
Integrity Modify internal data or documents without certification or authorization	Modify sensitive or public information Modify content to write to the database, and other users can directly trigger the syntax while is browsing	● Modify non-sensitive but non-public information ● The modified content writes to the database, but the syntax can be triggered directly only when the user browses ● The modified content cannot write to the database, but other users can directly trigger the syntax when browsing	● Modify general user profile ● The modified content cannot write to the database, and the syntax can be triggered directly only when the user browses.

Table 4 Impact Assessment for Types of Attack

Types of Attack	High impact	Low impact	Info impact
Cross-site scripting attacks	Storage cross-site scripting attack vulnerabilities, trigger web pages can be viewed directly by anyone.	"Storage-type cross-site scripting attack vulnerabilities, but only affect the logged-in user" or "reflective cross-site scripting attack vulnerabilities, triggering webpages can be triggered directly by clicking on a link to a social engineering letter."	Reflective cross-site scripting attack trigger webpages cannot exploit by clicking on links to social engineering letters, only on webpages that are visible to individuals.
SQL injection attack	Get more than ten groups of capital using SQL Injection syntax	SQL Injection only causes the SQL data field exposed to the error message	Only SQL Injection is confirmed to be different for logical judgment, but no further information is obtained or utilized
Application or system vulnerabilities	If the FTP service password successfully guessed, the server contains sensitive data	If the FTP service password successfully guessed, the server contains internal general information	If the FTP service password successfully guessed, the server only contains public data

3.2. Attack Principles

(1) It can only attack an attack target that has authorized. The target within the unauthorized scope cannot attack.

(2) It cannot use a jump host or VPN to attack.

(3) It is forbidden to use vulnerability scan software (except Nmap) for attack targets to avoid blocking attack IP.

(4) It is forbidden to use social engineering techniques to attack (such as sending phishing letters and calling the authorities).

(5) It should avoid entering more than the high-rank manager's box or the high-rank manager's mailbox and other functions (do not wash the board).

(6) If any unknown attack marks were found (such as data package and suspicious program), please report it to the authorized personnel immediately, and notify the agency as soon as possible.

(7) In the course of the attack, if the data needs to repair on the target, the principles are as follows:

a. New data, such as uploading files, registering accounts, or depositing attack strings, are based on COM2019PT, COM, and 11223344. The examples are as follows:

(a) Filename: COM2019PTXXX.docx

(b) Account name: xxxCOM

(c) Attack string: COM2019PT_XSS, XX11223344XX

b. It is forbidden to tamper with or delete any original information on the target of the attack.

(8) In the process of the attack, if it needs to insert a picture on the target, the principles are as follows:

a. Attack records that do not use the special screen for the attack and defense of the network will not score.

b. Please download the special image from the COM's website.

3.3. Defensive Working Instructions

(1) Operation process: The defensive party should perform the drill according to the operation procedure given.

(2) Step description

a. The defensive side monitors the entire network activity record.

b. The defending team uses the enterprise-information-center monitoring system and the defense equipment log to check, and after finding the suspected attack behavior, it

provides relevant explanations and corresponding actions.

(3) The information center judges the instructions made by the defensive team and performs subsequent disposal:

a. Non-attack behavior: It will not be processed and closed.

b. General attack behavior: According to the defense team's response, it should be set as a defense device and continuously observed.

c. High-risk attack behavior: Perform standard procedures for emergency response notification.

(4) If the defense team set by the defender causes the network to operate abnormally, the information center must immediately restore the settings before the transaction.

(5) Personal belongings

a. It is forbidden to use private laptops and storage devices.

b. The mobile phone carrier, but it cannot use the attacking or defensive working site. If it needs to answer or use the mobile phone, please leave the working site.

c. The information center provides the exclusive storage location, and the personal items of the attacking or defending members must place at the designated location.

(6) Matters need to attend

a. The information center uses the monitoring software to record the whole process of the offensive and defensive drills. The team members perform the computer process and arrange the on-site monitoring of the coordinated personnel. It is strictly forbidden to bring any information through the network or other storage devices. If there are special needs, please contact the security personnel.

b. If members of the information security offensive and defensive team need to install other software, please respond to the security personnel first. After the information center agrees, they must install the computer on their own.

c. During the implementation of the security attack and defense drills, the same team members can discuss and exchange experiences with each other, but please pay attention to the volume to avoid disturbing others.

3.4. Major Violations

If any of the following violations occur, that is, if a major violation imposed, it will not be allowed to participate in the follow-up of the security attack and defense exercise this year, and in the future, it will not be allowed to participate in the security attack and defense drills organized by the Information Center in the future.

(1) All materials during the exercise period shall not violate the protection and close cooperation, and it is forbidden to bring any information on the attack and defense exercises of the security. It is forbidden to upload or carry out the exercise data by any means such as communication software (mobile phone, APP), cloud drive, portable hard disk, images, recording, or manuscript. If it has special needs, it can report the request for assistance to the information center security personnel.

(2) Prohibition of deliberate destruction of the target system or data: After the attack is successful, it is forbidden to destroy the original data of the exercise target deliberately.

(3) It is strictly forbidden to attack websites or systems that are not practicing targets.

(4) Daily drills will be announced every morning to prohibit damage or attacks on websites or systems other than the target (including network attack and defense drill systems, attacker environments, and attack site equipment).

(5) The use of jump host is prohibited. The attack site uses a dedicated IP for the actual drill. Do not use the jump host to ensure the legitimacy of the drill.

(6) Other violations occurred, and those who did not cooperate after being persuaded.

Whether the above facts are deliberate acts, the relevant evidence determined by the information center.

3.5. Network Map for the VM Target Website

The NMAP application was used to map the VM Target Website, and NMAP command used is:

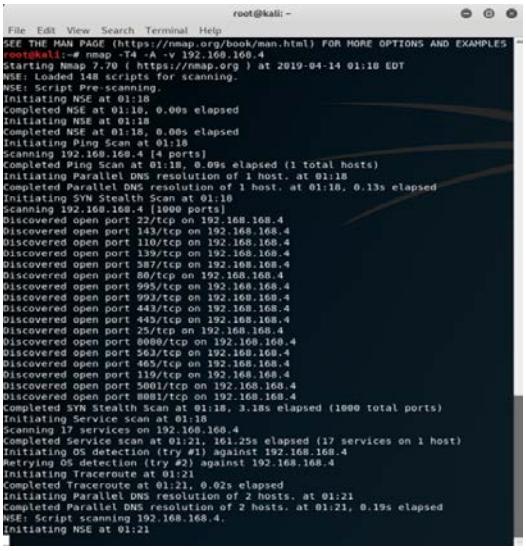
Intense scan: nmap -T4 -A –v 192.168.168.4

Quick scan: nmap -T4 -F

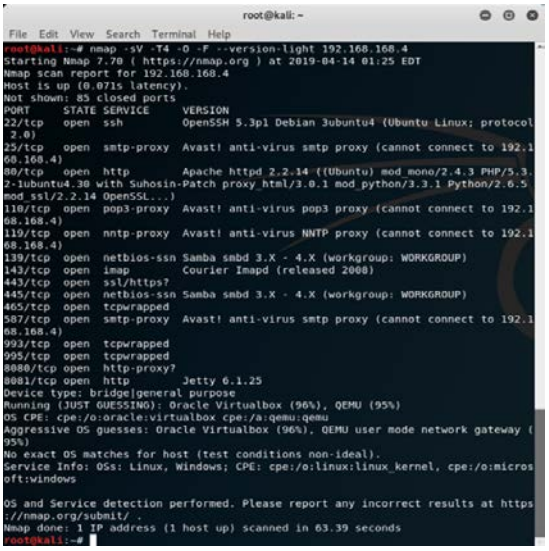
Quick scan plus: nmap -sV -T4 -O -F --version-light 192.168.168.4

Intense scan, all TCP ports: nmap -p 1-65535 -T4 -A –v 192.168.168.4

The network map for VM Target Website, as shown in Figure 1:



NMAP Result for intense scan



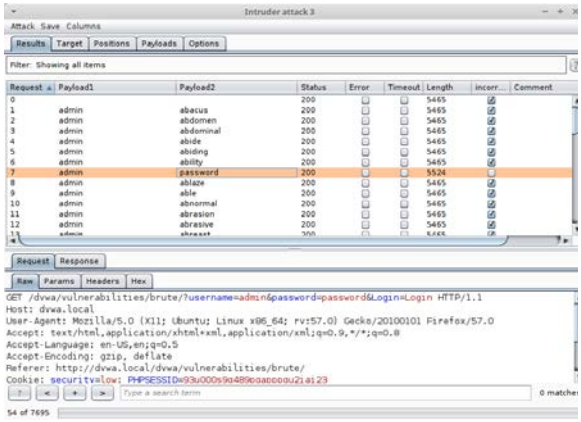
NMAP Result for Quick scan plus

Figure 1 NMAP Result for Intense scan and VM Target Website

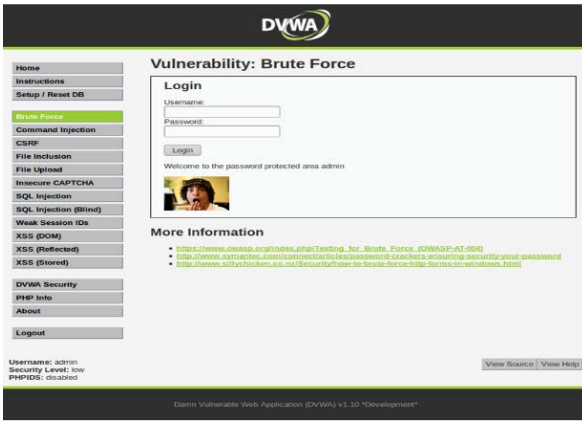
The result showed 17 services running, and 17 ports opened on 192.168.168.4. The operating system on VM Target Website is Ubuntu Linux. The investigator can verify the collected information about the VM Target Website.

3.6. Password Cracked for the VM Target Website

The Burp suite community edition was used to brute force crack password in the website's vulnerability and then send to the intruder. The intruder was set up by configuring Proxy in intercept mode to capture the Raw and then forward to Firefox browser. The burp suite was used to check and clear payload positions and then add payload positions, set attack type to a Cluster bomb; Payloads set 1 to select a wordlist file in runtime; Payloads set 2, setting grep-Match by input incorrect. The intruder started to attack DVWA: Brute Force website to find the username and password match, as shown in Figure 2:



The intruder started an attack to find the username and password matched



Welcome to the password area admin

Figure 2 Password Cracked for the DVWA VM Target Website

4. Results and Analysis of Website Penetration Testing

In this section, Results and Analysis of the Network Mapping, the Cross-Site Scripting Attacks,

and Web Application Security Risks Penetration Testing described.

4.1. Results and Analysis of the Network Mapping

Nmap output for 192.168.168.4 displayed seven ports opened. OS is Linux Kernel 2.6, as shown in Figure 3:

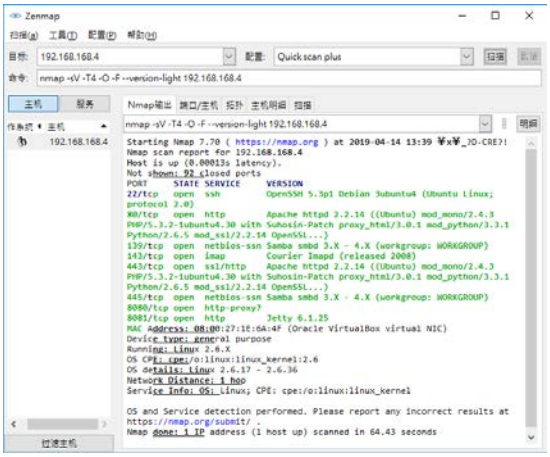
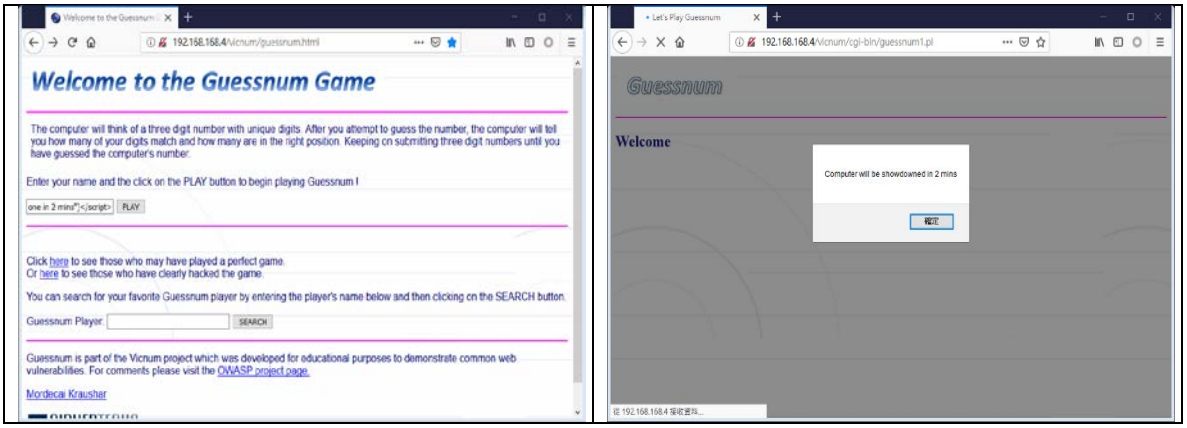


Figure 3 Nmap output for 192.168.168.4

4.2. Results and Analysis of the Cross-Site Scripting Attacks

The <script>alert("Computer will be show downed in 5 mins")</script> was input to the field of a user name, and the warning message was pop-up on the webpage, as shown in Figure 4:



The script injected to the input area　　Alert message pop out to the webpage

Figure 4 Results and Analysis of the XXS for

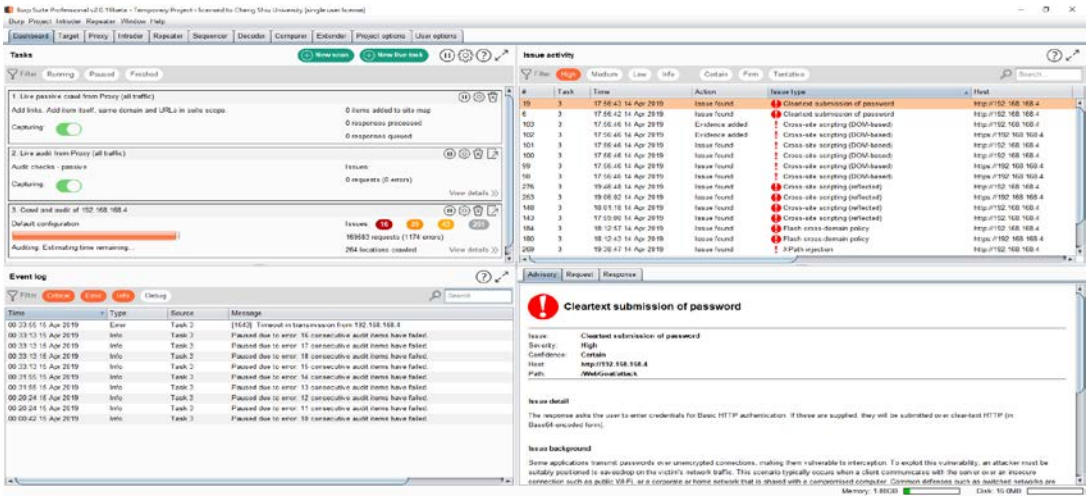


Figure 5 The issues activity for the VM of the OWASP Broken Web Applications Project on Burp Suite Professional Dashboard.

4.3. Results and Analysis of Web Application Security Risks Penetration Testing

The dashboard in Burp Suite Professional shown issues activity for the VM of the OWASPBWA Project. The issues were found 16 high severity, 20 medium severity, 43 Low severity, 201 Information, and 1174 errors, as shown in Figure 5:

The report from Burp Suite Professional v2.0.19beta Issue Activity for OWASPBWA Project are showed as following: Cross-site scripting (reflected), XPath injection, Flash cross-domain policy, Cross-site scripting (DOM-based), Cleartext submission of password, SSL certificate, SSL cookie without secure flag set, Cookie without HttpOnly flag set, Cross-site scripting (reflected), Open redirection (DOM-based), Password field with autocomplete enabled, Strict transport security not enforced, Unencrypted communications. The issue type, severity, and issue details, as shown in Table 5:

Table 5 Burp Suite Professional Issue Activity for OWASPBWA Project

Issue type	Severity	Issue detail
Cross-site scripting (reflected)	High	The value of the URL path filename copied into the HTML document as plain text between tags. This proof-of-concept attack demonstrates that it is possible to inject arbitrary JavaScript into the application's response.
XPath injection	High	The User-Agent HTTP header appears to be vulnerable to XPath injection attacks. The payload ' submitted in the User-Agent HTTP header, and an XPath error message returned.
Flash cross-domain policy	High	The application publishes a Flash cross-domain policy which allows access from any domain. Allowing access from all domains means that any domain can perform two-way interaction with this application.
Cross-site scripting (DOM-based)	High	The application may be vulnerable to DOM-based cross-site scripting. Data is read from location.href and passed to document.write().
Cleartext submission of password	High	The response asks the user to enter credentials for Basic HTTP authentication. If these, they will be submitted over clear-text HTTP (in Base64-encoded form).
SSL certificate	Medium	The server's certificate is not valid for the server's hostname. The server's certificate is not trusted.
SSL cookie without secure flag set	Medium	JSESSIONID The cookie appears to contain a session token, which may increase the risk associated with this issue.
Cookie without HttpOnly flag set	Low	PHPSESSID The cookie appears to contain a session token, which may increase the risk associated with this issue.
Cross-site scripting (reflected)	Low	The value of the User-Agent HTTP header copied into the HTML document as plain text between tags.
Open redirection (DOM-based)	Low	The application may be vulnerable to DOM-based open redirection. Data is read from window.location.href and passed to location.
Password field with autocomplete enabled	Low	The form contains the following password field with autocomplete enabled: password
Strict transport security not enforced	Low	This issue found in multiple locations under the reported path.
Unencrypted communications	Low	The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies.

(From Burp Suite Professional v2.0.19, 2019)

The table below shows the numbers of issues identified in different categories. Issues classified according to severity as High, Medium, Low, or Information. It reflects the likely impact of each issue for a typical organization. Issues also classified according to confidence as Certain, Firm, or Tentative. IT reflects the inherent reliability of the technique that was used to identify the issue, as shown in Figure 6:

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	2	4	0	6
	Medium	1	19	0	20
	Low	7	18	1	26
	Information	56	19	4	79

Figure 6 Severity and Confidence for the issue activity

The investigator's role is to identify false positives. Logically speaking, when Burp is telling that confidence is Certain that is more than 90%, it is a real flaw. When the confidence is Firm, it means 60% it is not a false positive, and Tentative most probably is a false positive. Flaws and vulnerabilities are called issues in Burp—to make sure that they understand the terminology this application uses to identify web application vulnerabilities.

5. Conclusions and Recommendations

The steps of the web application penetration test were verified. First, making test cases: recording the diagnosis object, making the situation. Second, implementing the vulnerability diagnosis: using the automatic or manual diagnostic tool for diagnosis. Third, verify the diagnosis result: verifying the diagnosis result using the manual operation. Forth, Consolidation report: The report is output by the diagnostic tool, and the report is manually collected. Before the website penetration testing, the attacking computer environment laboratory is building. The regulations for penetration testing were announced, such as attack principles, defensive working instructions, and major violations. Implementation of penetration testing was network mapping, password cracked, and cross-site script attack for the VM Target Website.

The report from Burp Suite Professional Issue activity for OWASPBWA project are showed as following: Cross-site scripting (reflected), XPath injection, Flash cross-domain policy, Cross-site scripting (DOM-based), Cleartext submission of password, SSL certificate, SSL cookie without secure flag set, Cookie without HttpOnly flag set, Cross-site scripting (reflected), Open redirection (DOM-based), Password field with autocomplete enabled, Strict transport security not enforced, Unencrypted communications.

References

1. Ansari, Juned, Ahmed. (2015). Web Penetration Testing with Kali Linux, 2nd ed. Birmingham: UK. Packt Publishing.
2. Gilberto, Nájera-Gutiérrez. (2016). Kali Linux Web Penetration Testing Cookbook. Birmingham: UK, Packt Publish. pp. 297.
3. Hauser, Van, and Roland Kessler. (2013). https://tools.kali.org/password-attacks/hydra, Browsed on July 16, 2019.
4. NMAP. (2019). https://nmap.org/ Browsed on July 10, 2019.
5. OWASP. (2019). https://www.owasp.org/ Browsed on July 10, 2019.
6. Portswigger. (2019). Burp Suite Professional. https://portswigger.net/ Browsed on July 10, 2019.
7. Stuttard, Dafydd, and Marcus Pinto. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Ed., Wiley. pp. 912.
8. Wear, Sunny. (2018). Burp Suite Cookbook: Practical recipes to help you master web penetration testing with Burp Suite. Packt Publishing. pp. 358.