

## ***TASK 2 PENETRATION TESTING ON WEB APPLICATIONS***

### **INTRODUCTION TO PROJECT:**

The project titled “Penetration Testing on Web Applications” was created. Vulnerabilities and Penetration Testing (VAPT) are both security services that focus on identifying vulnerabilities in the network, server and system infrastructure. Both the services serve a different purpose and are carried out to achieve different but complimentary goals. Vulnerability Assessment focuses on internal organizational security, while Penetration Testing focuses on external real-world risk. Vulnerability Assessment (VA) is a rapid automated review of network devices, servers and systems to identify key vulnerabilities and configuration issues that an attacker may be able to take advantage of. It is generally conducted within the network on internal devices and due to its low footprint can be carried out as often as every day. Penetration Testing (PT or PenTest) is an in-depth expert-driven activity focused on identifying various possible routes an attacker could use to break into the network. In addition with the vulnerabilities it also identifies the potential damage and further internal compromise an attacker could carry out once they are past the perimeter. Web Application Penetration Testing is security testing methods for security holes or vulnerabilities in web applications and corporate websites. Due to these vulnerabilities, websites are left open for exploitation.

In this Project, Penetration Testing is conducted on Open source web application and the web application name is Altoro Mutual (testfire.net). It is a banking web application and it is provided by HCL company. A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

### **ASSESSMENT OVERVIEW:**

Our Task to evaluate the security posture of its Company infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the OWASP Testing Guide, and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.

- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

#### DIFFERENT TYPES OF WEB APPLICATION PENETRATION TESTING TOOLS:

The project was conducted through the use of one Penetration Tester on Kali Linux. The rationale behind using various sources and methods was to ensure a comprehensive and wide range of vulnerabilities to be detected. It was also to ensure a lack of overreliance on one source, but to implement various sources to increase accuracy in results and findings.

#### TOOLS:

- NMAP:

NMAP is short for Network Mapper. It is an open-source tool that helps you map a network by scanning ports, discovering operating systems, and creating an inventory of devices and the services running on them. It sends differently structured packets for different transport layer protocols which return with IP addresses and other information. You can use this information for Metasploit currently includes nearly 1677 exploits along with almost 500 payloads that include

- Command shell payloads
- Dynamic payloads
- Meterpreter payloads
- Static payloads

The framework also includes listeners, encoders, post-exploitation code, and whatnot.

- Host discovery
- OS fingerprinting
- Service discovery

- Security auditing

You can use the tool for a large network with thousands of devices and ports.

- Wireshark:

Wireshark is another famous open-source tool that you can use for protocol analysis. It allows you to monitor network activities at a microscopic level. It is a growing platform with thousands of developers contributing from across the world.

With Wireshark you can perform

- Live capture and offline analysis
- Inspection of hundreds of different protocols
- Browse captured data via GUI
- Decrypt protocols
- Read live data from Ethernet, and a number of other mediums
- Export output to XML, PostScript, CSV, or plain text

Wireshark is the industry standard for protocol analysis in many different sectors. If you know what you are doing, it is a great tool to use.

- Metasploit:

Metasploit is a Ruby-based open-source framework, used by both ethical hackers and malicious actors to probe systematic vulnerabilities on networks and servers. The Metasploit framework also contains portions of fuzzing, anti-forensic, and evasion tools. It is easy to install and can work on a wide range of platforms regardless of the languages they run on. The popularity and the wide availability of Metasploit among professional hackers make it an important tool for Penetration Testers as well.

- Burp Suite:

Burp Suite is a set of penetration testing tools by Portswigger Web Security. It is used by ethical hackers, pen-testers, and security engineers. It is like a one-stop-shop for bug bounty hunters and security researchers. Let us take a look at a few tools included in Burp Suite.

- Spider: It is a web crawler. You can use it to map the target application. It lets you create an inventory of all the endpoints, monitor their functionalities, and look for vulnerabilities.
- Proxy: As explained earlier, a proxy sits between the browser and the internet to monitor, and modify the requests and responses in transit.
- Intruder: It runs a set of values through an input point and lets you analyze the output for success, failure and content length. These aside the suite includes Repeater, Sequencer, Decoder, Extender, and some other add-on tools.

#### FINDING SEVERITY RATINGS:

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

##### Critical

9.0-10.0      Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.

##### High

7.0-8.9 Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.

##### Moderate

4.0-6.9 Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.

##### Low

0.1-3.9 Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.

## Informational

N/A No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

## RISK FACTORS

Risk is measured by two factors: Likelihood and Impact:

### Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

### Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

## Scope Exclusions

Our Project did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

## TESTING SUMMARY

The Web Application assessment evaluated TestFire Web Application security posture. From an internal perspective, the pen tester performed manual vulnerability assessment against the

website link provided by testfire to evaluate the overall patching health of the website. The pen tester found many vulnerabilities on the web app and exploited it.

The pen tester used some manual techniques to exploit basic level of vulnerabilities and was successfully able to get admin access to the web app using various exploitation methods. The security of the web app is completely compromised by basic level of exploitation which are mentioned below along with the evidence. Since it was a time bound assessment so most the vulnerabilities were reported by the pen tester in the given time. However, there are more serious exploits still present in the system but due to the time limit only some of them are reported.

#### KEY STRENGTHS AND WEAKNESSES:

The following identifies the key strengths identified during the assessment: The following identifies the key weaknesses identified during the assessment:

- Default credentials were used in web app
- Broken Authentication.
- Improper input validation on various input parameters
- Internal server error being displayed.
- Insecure direct object reference allowed.
- Injection allowed on various input parameters.
- No mechanism to stop brute force of login information
- Displaying user information on web page.
- GitHub source code link of web app displayed on screen.

#### VULNERABILITY SUMMARY & REPORT CARD

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

#### Web Application Penetration Test Findings

Critical

High

Moderate

Low

Informational

| Finding | Severity | Recommendation |
|---------|----------|----------------|
|---------|----------|----------------|

#### Web Application Penetration Test

|   |        |                             |
|---|--------|-----------------------------|
| 1: Apache Tomcat insecure default administrative password | (High) | Change the default password |
|---|--------|-----------------------------|

|                                     |        |   |
|-------------------------------------|--------|---|
| 2: Insecure Direct Object reference | (High) | Validate and filter any sort of input even if it's not malicious. |
|-------------------------------------|--------|---|

|   |            |  |
|---|------------|--|
| 3: SQL Injection Vulnerability allowing login bypass. | (Critical) | Use parametrized query instead of string concatenation within the query. |
|---|------------|--|

|  |        |  |
|--|--------|--|
| 4: Login Brute on username and password. | (High) | Restrict multiple requests from a same source. |
|--|--------|--|

|                               |        |  |
|-------------------------------|--------|--|
| 5: Improper input Validation. | (High) | Proper validation and filter of input to be performed. |
|-------------------------------|--------|--|

|                   |            |   |
|-------------------|------------|---|
| 6: Reflected XSS. | (Moderate) | Implement proper filtration of various characters during input. |
|-------------------|------------|---|

|                                    |       |   |
|------------------------------------|-------|---|
| 7. Displaying user info on web app | (Low) | Properly check for any user info displayed on screen. |
|------------------------------------|-------|---|

|                                      |                 |  |
|--------------------------------------|-----------------|--|
| 8. Displaying internal server error. | (Informational) | Properly check error log and error messages displayed on screen. |
|--------------------------------------|-----------------|--|

## TECHNICAL FINDINGS

### Web Application Penetration Test Findings

#### Finding 001: Apache Tomcat Insecure Default Administrative Password (High)

**Description:** Test fire allows the use of default admin password being used on the login page due to which any unauthenticated user knowing the default password available on the internet can gain access to the admin account and have admin privileges.

**Risk:** Likelihood: High – This attack is effective on web app and have major consequences to it.

**Impact:** Very High – This attack gives admin privilege to a user who can make any changes on the web application.

**System:** All

**Tools Used:** Manually

**References:** <https://www.acunetix.com/vulnerabilities/web/apache-geronimo-default-administrative-credentials/>

## CONCLUSION:

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber-crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.