Capstone Project: Security Assessment and Exploitation Report

Intern name: Cinchana S
Date: 23-01-2026

Executive Summary

The assessment was performed on two deliberately vulnerable lab environments: the TryHackMe *Network Services* room and the OWASP Broken Web Applications (OWASP-BWA) virtual machine. The objective of the project was to identify vulnerabilities, exploit them safely, and understand their security impact. During testing, multiple issues were successfully identified and exploited, including weak FTP authentication, command injection, and insecure direct object reference (IDOR). These vulnerabilities allowed unauthorized access to services, execution of system commands, and disclosure of sensitive system files.

Scope

- TryHackMe – Network Services (FTP service)
- OWASP Broken Web Applications (OWASP-BWA) – Mutillidae application

Tools Used

- **Kali Linux** – Attacking system
- **Nmap** – Network and service enumeration
- **Hydra** – FTP password brute-force attack
- **Burp Suite** – Web and API testing (Intercept, Intruder, Repeater)
- **Nikto** – Web server vulnerability scanning
- **OpenVAS** – Recommended for post-remediation scanning

Exploitation Log

Test ID	Target IP	Vulnerability	PTES Phase
001	10.48.185.189	FTP Weak Credentials	Exploitation
002	192.168.0.15	Command Injection	Exploitation
003	192.168.0.15	IDOR / Path Traversal	Exploitation

Vulnerability Findings and Exploitation Details

FTP Weak Authentication

Target: TryHackMe – Network Services
Severity: High

- During reconnaissance, an FTP service was identified running on port 21. The service allowed repeated login attempts without any account lockout or rate limiting.
- Hydra was used to perform a password brute-force attack using a known username and a wordlist. Due to weak password security, valid credentials were successfully obtained.
- After logging in with the discovered credentials, directory listing and file access were possible. This confirmed unauthorized access to the FTP service.

Impact:
An attacker could download sensitive files, upload malicious files, or misuse the FTP service for further attacks.

Command Injection

Target: OWASP-BWA – Mutillidae (DNS Lookup)
Severity: Critical

- The DNS Lookup functionality in Mutillidae was tested for input validation issues. Initially, a valid IP address (8.8.8.8) was submitted, and normal output was returned.
- The request was intercepted using Burp Suite and sent to the Intruder tool. The IP input parameter was marked as the payload position. Payloads from SecLists were used, and URL encoding was disabled to ensure correct execution.
- When the attack was executed, the server responded with command output, including:

    uid=33(www-data) gid=33(www-data) groups=33(www-data)

This confirmed that user input was being executed directly on the server.

Impact:
An attacker could execute system commands with web server privileges, potentially leading to further compromise.

IDOR / Path Traversal

Target: OWASP-BWA – Mutillidae (Source Viewer)
Severity: High

- The Source Viewer feature allowed users to specify a file name using the **phpfile** parameter. The default value loaded a PHP source file.
- The request was intercepted in Burp Suite and sent to Repeater. The **phpfile** parameter was modified to traverse directories and access **/etc/passwd**.
- The server responded with the contents of the file, confirming successful path traversal and unauthorized file access.

Impact:
Sensitive system files can be read, allowing attackers to gather system and user information.

Nikto Scan Summary

Nikto was used to scan the OWASP-BWA web server. The scan identified multiple insecure configurations and exposed files. These findings support the manual testing results and highlight the need for better server hardening.

Risk Impact Summary

Area	Impact
Confidentiality	High
Integrity	Medium
Availability	Medium
Overall Risk	High

Remediation Plan

- Enforce strong password policies for FTP services
- Disable brute-force-prone authentication mechanisms
- Validate and sanitize all user input on the server side
- Implement proper authorization checks for file access
- Run services with least-privileged accounts
- Patch and harden web and network services

Verification

After applying fixes, a vulnerability rescan using **OpenVAS** should be performed on the OWASP-BWA environment to confirm that vulnerabilities have been resolved.

Stakeholder Summary

This project identified several security weaknesses in network and web services, including weak passwords, improper input handling, and insecure file access. These issues could allow unauthorized users to access sensitive information or execute commands on the system.The testing was performed in a controlled environment and focused only on identifying and validating vulnerabilities. Addressing these issues through stronger authentication, secure coding practices, and system hardening will significantly improve security. A follow-up scan is recommended to ensure remediation is effective.