Task 5 — Web Application Penetration Testing

ApexPlanet Cybersecurity Internship

Objective

Perform web application vulnerability assessment and penetration testing (VAPT) in a controlled lab (DVWA/bWAPP/WebGoat).

This teaches how web apps handle data and how misconfigurations lead to attacks like SQL injection or XSS.

Learning Outcomes

• Understand client–server web flow.

• Use Burp, ZAP, SQLMap for automated testing.

• Learn manual validation and report creation.

• Combine automated and manual testing for accuracy.

Lab Setup

Use Kali Linux (attacker) and DVWA/bWAPP (target) in Host-Only network. Snapshot target before testing.

Configure browser proxy (127.0.0.1:8080) for Burp.

Run DVWA at low security for exploitation, then medium/high to test fixes.

Phase 1 — Reconnaissance

Goal: Identify structure and parameters.

Steps:

- Browse and map URLs (/login.php, /vulnerabilities/sqli/)

- Use Burp to inspect requests and parameters

- Discover hidden files via ffuf

Command:

```
ffuf -u http://<TARGET>/FUZZ -w /usr/share/wordlists/dirb/common.txt -mc 200
```

Why: Understanding structure defines attack surface.

Phase 2 — SQL Injection

What: Manipulate SQL queries via user inputs.

```
Manual payloads:
```

' OR '1'='1

' UNION SELECT null, version(), user(), database() --

Automated:

```
sqlmap -u "http://<TARGET>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="PHPSESSID=xyz; security=low" --batch --dbs
```

Mitigation: Prepared statements, least privilege DB accounts, input validation.

Phase 3 — Cross-Site Scripting (XSS)

What: Inject scripts that execute in users' browsers.

```
Payloads:
<script>alert('XSS')</script>
```

<img src=x onerror=alert('XSS')>

Mitigation: Encode output, apply CSP, and set HttpOnly cookie flags to stop JS access to cookies.

Phase 4 — Authentication & Session

Goal: Detect weak logins and insecure session handling.

Tests:

- Try default creds admin/admin
- Examine cookies for Secure/HttpOnly flags
- Check if session persists post logout

Mitigation: strong password policy, short session timeouts, rotate session IDs.

Phase 5 — Cross-Site Request Forgery (CSRF)

Exploit: trigger unwanted actions from victim's browser.

Example:

```
<form action="http://<TARGET>/vuln/csrf/" method="POST">
```

<input type="hidden" name="password_new" value="hacked123">

</form><script>document.forms[0].submit()</script>

Mitigation: CSRF tokens, SameSite cookies, re-authentication for critical actions.

Phase 6 — File Inclusion & Command Injection

LFI: ../../../../etc/passwd reads local files.

Command injection: appending ; ls -la or | id executes OS commands.

Mitigation: Whitelist files, disable allow_url_include, use safe APIs, sanitize input.

Phase 7 — Automated Scanning

Tool: OWASP ZAP / Burp Scanner.

Run passive+active scan, verify findings manually.

Export HTML/PDF report to vuln_reports/.

Why: Saves time and finds known patterns quickly.

Risk Analysis

Critical: RCE, auth bypass → fix immediately.

High: Privilege escalation, sensitive data leaks.

Medium: Misconfigurations, missing headers.

Low: Minor info disclosure.

Prioritize based on impact × exploitability.

Tools & Commands

Burp Suite: Proxy/Repeater/Intruder

```
sqlmap: automate SQLi
```

```
ffuf: discover hidden paths
curl: inspect headers
```

ZAP: automated scan

Sample commands:

```
ffuf -u http://<TARGET>/FUZZ -w /usr/share/wordlists/dirb/common.txt -mc 200
curl -I http://<TARGET>/
sqlmap -u "http://<TARGET>/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="PHPSESSID=xyz; security=low" --batch --dbs
```

Evidence & Reporting

Collect:

```
- Request/response with payload
```

- Screenshots of exploits

- Scanner logs

- Risk + recommendation table

Structure: Title, URL, Steps, Evidence, Risk, Impact, Fix, References.

Ethics & Legal

Only test authorized targets. Unauthorized testing violates law.

Document permissions and scope before scanning.

Summary

This task builds hands-on understanding of finding and fixing OWASP Top 10 issues.

Learned to combine manual and automated testing for reliable VAPT,

and to communicate findings responsibly through clear reports.

Prepared by: [Your Name] — ApexPlanet Cybersecurity Internship — Task 5