1.Executive Summary

During security testing of the target DVWA instance, multiple vulnerabilities aligned with the OWASP Top 10 were identified, including SQL injection, XSS, weak authentication, and insufficient session protections. These weaknesses allow attackers to escalate privileges, exfiltrate data, compromise accounts, and achieve remote code execution. Immediate remediation is recommended, prioritizing proper input sanitization and improved authentication controls.

2.Technical Findings

Scope: DVWA Web Application
Environment: Kali Linux, Burp Suite, OWASP ZAP, sqlmap

Identified Vulnerabilities:

- SQL Injection
- Cross-Site Scripting (Reflected & Stored)
- Brute-forceable Login
- Session Hijacking
- Command Injection
- Insecure File Upload
- Weak Default Credentials

3.Remediation Plan

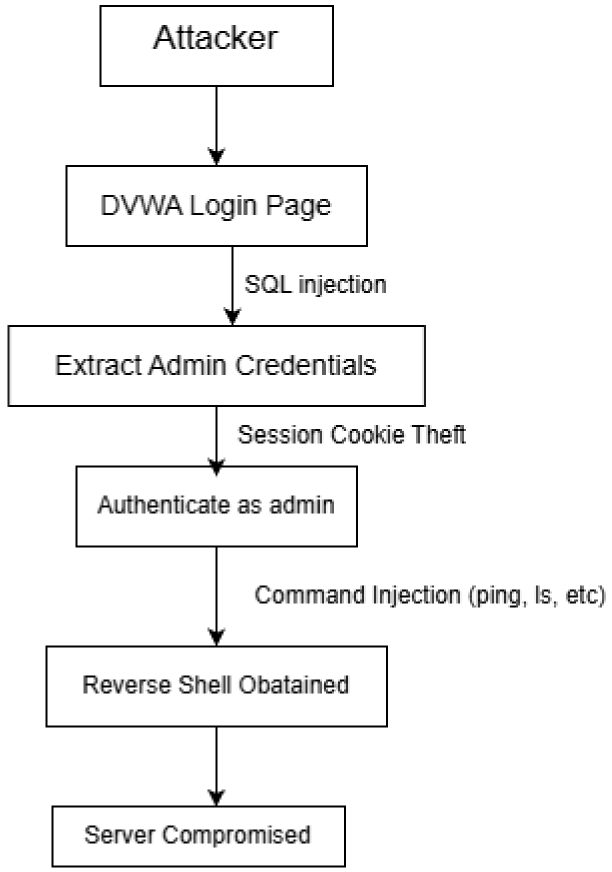
- Implement prepared statements & parameterized queries
- Sanitize user input and enforce output encoding

- Enable secure authentication and session management
- Patch application and underlying OS dependencies
- Restrict file upload validation and MIME checking
- Use WAF filtering for dangerous payload patterns

4.Findings Table

Finding ID	Vulnerability	CVSS Score	Remediation
F001	SQL Injection	9.1	Parameterized queries
F002	Weak Password Policy	7.5	Enforce complexity rules
F003	Stored XSS	8.2	Sanitize & output encode input
F004	Session Hijacking	8.0	HttpOnly, secure flags on cookies
F005	Command Injection	9.5	Shell sanitization & privilege limits
F006	Insecure File Upload	8.8	MIME validation & file-type restrictions

5.Attack Path Diagram



6.100-Word Non-Technical Summary for Management

Security evaluation of the DVWA system identified multiple vulnerabilities that could allow unauthorized users to gain administrative access, steal data, and potentially take over the server. These weaknesses include outdated security controls, insufficient validation of user input, and poor authentication mechanisms. If exploited, these issues may expose sensitive data, disrupt service availability, and result in compliance risk. We recommend implementing stronger password policies, validating and sanitizing all user inputs, and applying system patches. Addressing these issues promptly will significantly reduce the risk of cyber-attack and improve overall security posture.