Vulnerability Assessment Report

1. Executive Summary

I conducted a web application security assessment using DVWA as the target environment. The testing identified high-risk vulnerabilities including SQL Injection and weak password practices. These flaws can allow attackers to compromise the application, steal sensitive data, or gain unauthorized access. Immediate remediation is required to safeguard the environment against exploitation.

2. Technical Findings

Finding ID	Vulnerability	CVSS Score	Remediation
F001	SQL Injection	9.1	Implement strict input validation and use parameterized queries.
F002	Weak Password	7.5	Enforce strong password complexity rules and disable default credentials.

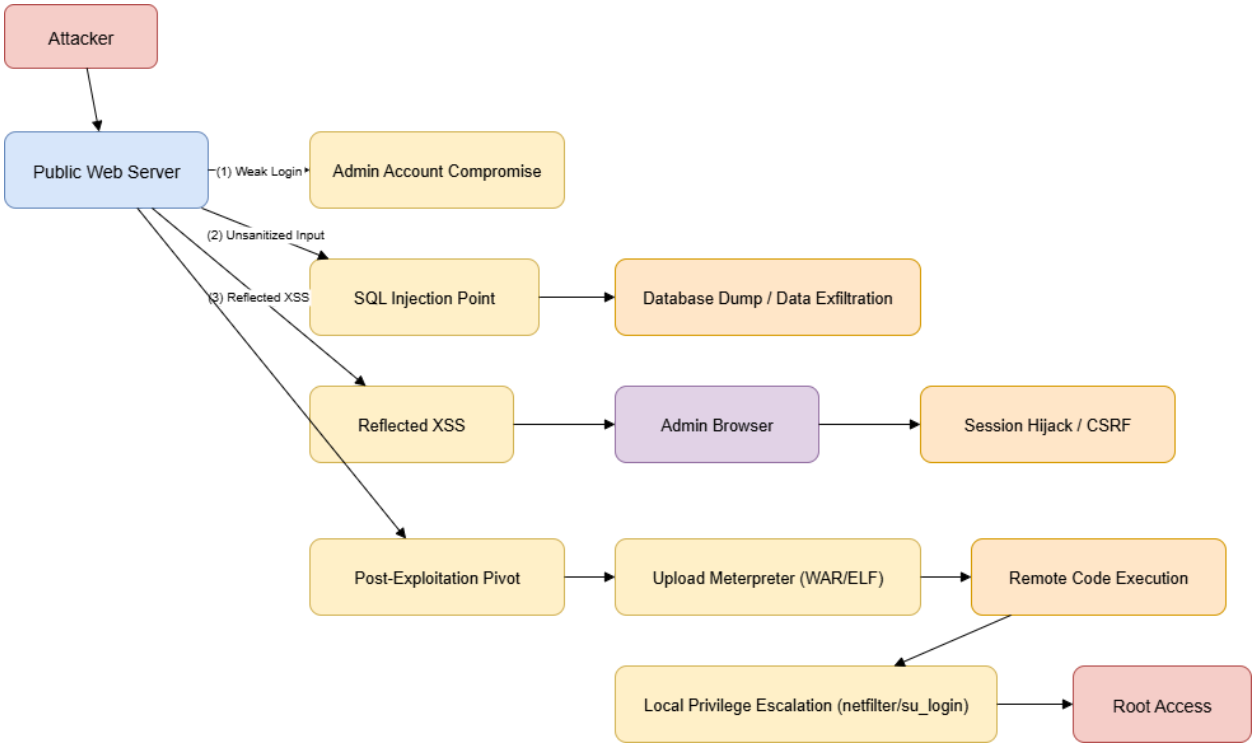
i. Remediation Plan

- **SQL Injection:** Sanitize all inputs, implement prepared statements, and deploy Web Application Firewall (WAF) rules.

- **Weak Passwords:** Enforce password policies (minimum 12 characters, alphanumeric with special symbols), disable default accounts, and integrate MFA.

3. Visualization

A simple **attack path diagram** showing:



4. Stakeholder Brief (100 words)

During the recent vulnerability assessment of our DVWA test environment, I identified two significant risks: SQL Injection (CVSS 9.1) and weak password practices (CVSS 7.5). These vulnerabilities allow attackers to bypass authentication, extract sensitive data, and compromise administrative accounts. If exploited in a real environment, they could result in severe data breaches and reputational loss. To mitigate these risks, I recommend immediate implementation of input validation, secure coding practices, strong password enforcement, and multifactor authentication. Addressing these issues quickly will strengthen the organization's security posture and reduce exposure to common web-based attacks.