# 🛡️ OWASP Top 10 Compliance Checklist for DVWA Assessment

This document provides a comprehensive OWASP Top 10 compliance checklist tailored to the DVWA penetration testing assessment performed on a vulnerable web application. Each row in the table maps a known vulnerability class to observed behavior and appropriate security guidance.

| **OWASP Category** | **Description** | **Observed in DVWA** | **Risk Status** | **Mitigation Required** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| **A01:2021 – Broken Access Control** | Failures that allow users to act outside of their intended permissions | ❌ Not Tested | Unknown | Test higher DVWA levels for role bypass |
| **A02:2021 – Cryptographic Failures** | Weak or missing encryption in transit/storage | ❌ Not Tested | Unknown | Use HTTPS, hash passwords securely |
| **A03:2021 – Injection** | SQL, OS, LDAP, and other injection flaws | ✅ SQL, Command | ✅ Critical Risk | Use prepared statements, input sanitization |
| **A04:2021 – Insecure Design** | Missing security controls in design phase | ✅ Application-wide | ✅ High Risk | Apply security-by-design principles |
| **A05:2021 – Security Misconfiguration** | Default configs, open directories, error messages | ✅ File Upload, Error 500 | ✅ High Risk | Harden server & app configs |
| **A06:2021 – Vulnerable and Outdated Components** | Use of old libraries/frameworks without patches | ✅ DVWA intentionally vulnerable | ✅ High Risk | Apply patch management policies |
| **A07:2021 – Identification & Authentication Failures** | Weak credentials, brute force attacks | ✅ Brute Force | ✅ High Risk | Rate limiting, MFA, strong passwords |
| **A08:2021 – Software and Data Integrity Failures** | CI/CD pipeline tampering or unverified software | ❌ Not Tested | Unknown | Use code signing, SCA tools |
| **A09:2021 – Security Logging & Monitoring Failures** | Insufficient logging, no alerts, undetected attacks | ❌ Not Tested | Unknown | Implement SIEM, alert rules |
| **A10:2021 – Server-Side Request Forgery (SSRF)** | Server can be tricked into making requests to unintended locations | ❌ Not Tested | Unknown | Validate URLs, restrict internal access |

## 📊 Summary

**Fully Exploited Categories:**  
✅ A03 – Injection  
✅ A04 – Insecure Design  
✅ A05 – Security Misconfiguration  
✅ A06 – Vulnerable Components  
✅ A07 – Authentication Failures

**Partially Covered or Not Explored:**  
🔶 A01, A02, A08, A09, A10