**Security Assessment Report**

**Project:** DVWA Localhost Testing **Assessment Tool:** ZAP by Checkmarx **Date:** July 27, 2025 **Scan Scope:** http://localhost/DVWA/

### **Summary of Risks**

| Risk Level | Number of Alerts |
| --- | --- |
| **High** | 0 |
| **Medium** | 4 |
| **Low** | 3 |
| **Informational** | 3 |

### **Risk Ratings and Findings**

#### **1. Content Security Policy (CSP) Header Not Set**

* **Risk Level:** Medium
* **Affected URLs:** /DVWA/, /login.php, /robots.txt, /sitemap.xml
* **Issue:** Absence of CSP header can allow XSS and data injection attacks.
* **Recommendation:** Implement the Content-Security-Policy header on all HTTP responses.
* **References:**
  + https://developer.mozilla.org/en-US/docs/Web/Security/CSP
  + https://owasp.org/www-project-secure-headers/
* **Screenshot Placeholder:** *(Insert screenshot of response headers showing CSP missing)*

#### **2. Directory Browsing Enabled**

* **Risk Level:** Medium
* **Affected URLs:** /dvwa/, /dvwa/css/, /dvwa/images/
* **Issue:** Directory listings expose internal structure and may reveal sensitive files.
* **Recommendation:** Disable directory browsing in server configuration.
* **Reference:** https://httpd.apache.org/docs/current/mod/core.html#options
* **Screenshot Placeholder:** *(Insert screenshot of directory listing page)*

#### **3. Hidden File Found (Apache Server-Status)**

* **Risk Level:** Medium
* **Affected URL:** /server-status
* **Issue:** May expose server stats and config.
* **Recommendation:** Restrict access to internal IPs or disable entirely in production.
* **Screenshot Placeholder:** *(Insert screenshot showing server-status output)*

#### **4. Missing Anti-Clickjacking Headers**

* **Risk Level:** Medium
* **Affected URLs:** /DVWA/, /login.php
* **Issue:** Pages vulnerable to clickjacking attacks.
* **Recommendation:** Use X-Frame-Options: DENY or CSP frame-ancestors 'none'.
* **Reference:** https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
* **Screenshot Placeholder:** *(Insert response headers showing absence of X-Frame-Options)*

#### **5. Cookie Without SameSite Attribute**

* **Risk Level:** Low
* **Affected URL:** /DVWA/
* **Issue:** Cookies can be sent cross-site.
* **Recommendation:** Set SameSite=Lax or SameSite=Strict in cookie attributes.
* **Reference:** https://owasp.org/www-community/controls/SameSite
* **Screenshot Placeholder:** *(Insert Set-Cookie header output)*

#### **6. Server Leaks Version Information**

* **Risk Level:** Low
* **Affected URLs:** Multiple (e.g., /DVWA/, /robots.txt, /login.php)
* **Issue:** Reveals Apache/2.4.64 (Debian) version in response headers.
* **Recommendation:** Configure server to suppress the Server header.
* **Reference:** https://httpd.apache.org/docs/current/mod/core.html#servertokens
* **Screenshot Placeholder:** *(Insert server header showing version leak)*

#### **7. X-Content-Type-Options Header Missing**

* **Risk Level:** Low
* **Affected URLs:** /DVWA/, /login.php, others
* **Issue:** Risk of MIME-sniffing attacks.
* **Recommendation:** Add X-Content-Type-Options: nosniff to HTTP responses.
* **Reference:** https://owasp.org/www-project-secure-headers/
* **Screenshot Placeholder:** *(Insert HTTP response showing missing nosniff header)*

### **Informational Alerts (No Immediate Fix Required)**

#### - Authentication Request Identified

* **URL:** /login.php
* **Info:** Password parameter identified. Not a vulnerability.

#### - Session Management Tokens Detected

* **URLs:** /DVWA/, /login.php
* **Info:** PHPSESSID and other tokens detected.

#### - User Agent Fuzzer Response Detected

* **Info:** 84 variations of user-agent tested; changes in responses detected.

### **Overall Recommendations**

1. **Security Headers:** Implement essential headers (CSP, X-Frame-Options, X-Content-Type-Options).
2. **Directory Control:** Disable unnecessary directory browsing.
3. **Server Hardening:** Remove version identifiers and unnecessary services.
4. **Cookie Security:** Use secure cookie flags like HttpOnly, Secure, SameSite.
5. **Monitor Hidden Files:** Audit and restrict sensitive endpoints like /server-status.

**Report Prepared By:** *Navneet Bhatt*