Vulnerability Assessment Report

Target Application: http://127.0.0.1:8000 (DVWA Instance)

Assessment Tool: OWASP ZAP v2.14.0

Scan Type: Full Active Scan

Date: August 15, 2025

Assessor: Security Team

Executive Summary

The security assessment identified **12 vulnerabilities**, including **3 Critical/High**, **4 Medium**, and **5 Low**. The most severe issues include SQL Injection, Reflected XSS, and IDOR, which could lead to unauthorized data access, credential theft, and full system compromise.

Immediate remediation is recommended for critical issues. Medium and low-severity issues should be addressed as part of ongoing secure development practices.

Severity Rating Legend

Severity	Description
Critical	Exploitation leads to full system compromise or critical data leakage.
High	Exploitation may allow unauthorized access or privilege escalation.
Medium	Vulnerability may aid in further attacks or affect confidentiality/integrity.
Low	Informational issues or minor misconfigurations.

Top 5 Issues Found

1. Reflected Cross-Site Scripting (XSS)

Severity: High

CWE: CWE-79 | **OWASP Top 10:** A03:2021 - Injection

Description: Unsanitized input on `/search` endpoint is reflected in the response without escaping, allowing arbitrary JavaScript injection.

Test Payload: `<script>alert(1)</script>`

> **Proof of Concept (HTTP Response Snippet):**
>
> ```
> GET /search?q=%3Cscript%3Ealert(1)%3C/script%3E
> ...
> Search results for: <script>alert(1)</script>
> ```

> **Remediation:**
>
> - Use proper output encoding for HTML/JS contexts.
> - Sanitize user inputs with libraries (e.g., DOMPurify).
> - Implement a strict Content Security Policy (CSP).

CVSS v3.1 Base Score: 7.4 (High)

2. SQL Injection

Severity: Critical

CWE: CWE-89 | **OWASP Top 10:** A03:2021 - Injection

Description: Login form is vulnerable to SQL injection, enabling authentication bypass.

Test Payload: `' OR '1'='1`

> **Proof of Concept:**

```
POST /login HTTP/1.1
username=admin' OR '1'='1'--
password=anything
```

Remediation:

- Use parameterized queries or prepared statements.
- Apply strict input validation.
- Restrict DB user privileges (least privilege principle).

CVSS v3.1 Base Score: 9.8 (Critical)

3. Insecure Direct Object Reference (IDOR)

Severity: High

CWE: CWE-639 | **OWASP Top 10:** A01:2021 - Broken Access Control

Description: Manipulating the `user_id` parameter allows access to other users' data.

Example: `/profile?user_id=104`

Remediation:

- Enforce server-side authorization checks.
- Use indirect object references (UUIDs/tokens).

CVSS v3.1 Base Score: 8.7 (High)

4. Missing HTTP Security Headers

Severity: Medium

CWE: CWE-693 | **OWASP Top 10:** A05:2021 - Security Misconfiguration

Description: Application lacks important HTTP security headers, exposing it to XSS, clickjacking, and MIME-sniffing attacks.

Missing Headers: `X-Content-Type-Options` , `X-Frame-Options` , `Content-Security-Policy`

Remediation:

- Set `X-Frame-Options: DENY` or use CSP frame-ancestors.
- Add `X-Content-Type-Options: nosniff` .
- Configure Content-Security-Policy appropriately.

CVSS v3.1 Base Score: 6.5 (Medium)

5. Passwords Transmitted Over HTTP

Severity: Medium

CWE: CWE-319 | **OWASP Top 10:** A02:2021 - Cryptographic Failures

Description: Login credentials are transmitted in plaintext over HTTP.

Affected URL: `http://127.0.0.1:8000/login`

Remediation:

- Enforce HTTPS and redirect all HTTP traffic.
- Use TLS 1.2+ with strong ciphers.
- Enable HSTS for strict transport security.

CVSS v3.1 Base Score: 7.1 (High)

Conclusion & Recommendations

The scan identified multiple severe vulnerabilities that could allow attackers to compromise the target application and its data.

- **Immediate Priority:** Fix SQL Injection, Reflected XSS, and IDOR issues.
- **Short Term:** Enforce HTTPS, configure HTTP headers, and review access controls.
- **Ongoing:** Adopt secure coding practices, regular penetration testing, and developer security training.