Title: Web App Testing Checklist — DVWA VM

Scope: http://192.168.132.130

Tools: Burp Suite, sqlmap, OWASP ZAP, browser devtools

Checklist:

- [ ] Capture baseline: record target URLs and screenshots.

- [ ] Intercept login and form requests with Burp Suite.

- [ ] Test for SQL injection (automated + manual):

- Use sqlmap with saved request: sqlmap -r request.txt --batch --dbs

- Enumerate DB, tables and dump sensitive tables.

- [ ] Test for XSS:

- Manual payloads: `<script>alert(1)</script>`, `"><img src=x onerror=alert(1)>`

- Check reflected and stored contexts.

- [ ] Test authentication mechanisms:

- Verify password reset flows, brute-force protections, account lockouts.

- Test session fixation, session invalidation after logout.

- Check cookie flags: HttpOnly, Secure, SameSite.

- [ ] Test for CSRF (look for missing anti-CSRF tokens).

- [ ] Test access control / authorization (IDOR).

- [ ] Run passive scan with OWASP ZAP and review alerts.

- [ ] Export logs and evidence (sqlmap output, Burp request.txt, screenshots).

- [ ] Create findings entries with PoC, risk rating, evidence, and remediation.

- Optional: Run self-curated scripts for bulk testing (document scripts and results).