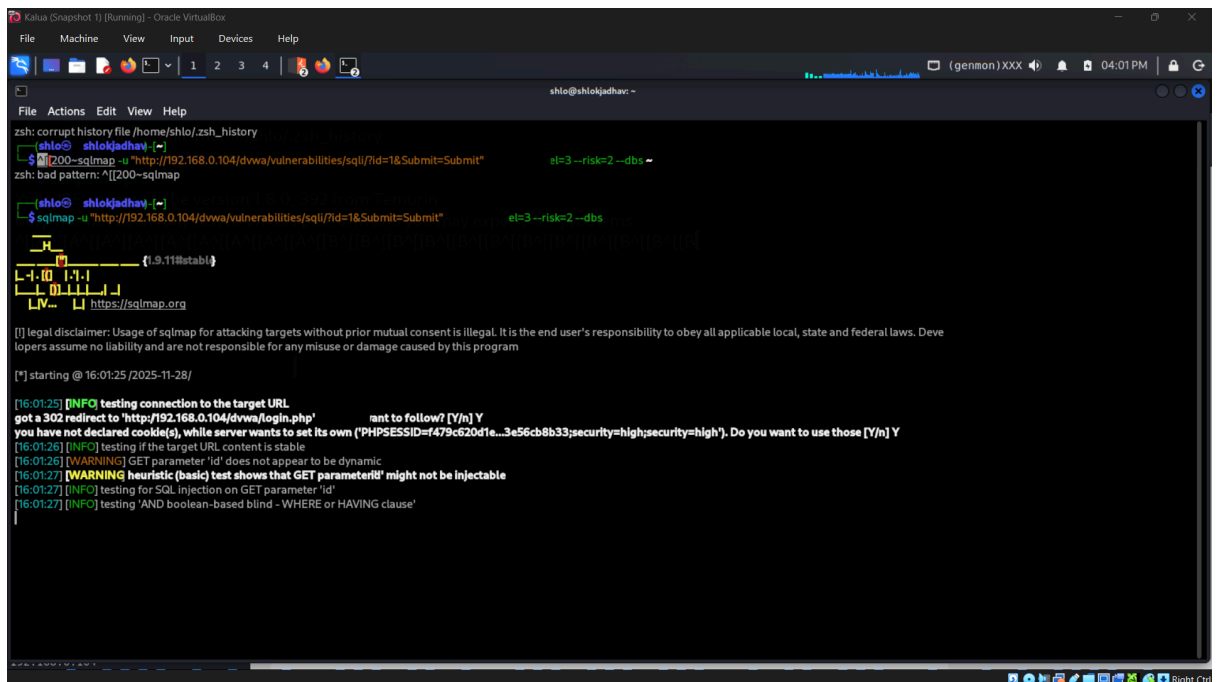# Web App Testing Checklist

✔ SQL Injection Testing

- Run sqlmap against vulnerable parameters

- Use GET & POST scanning

- Include session cookie during authenticated tests

- Dump DB if injection is confirmed
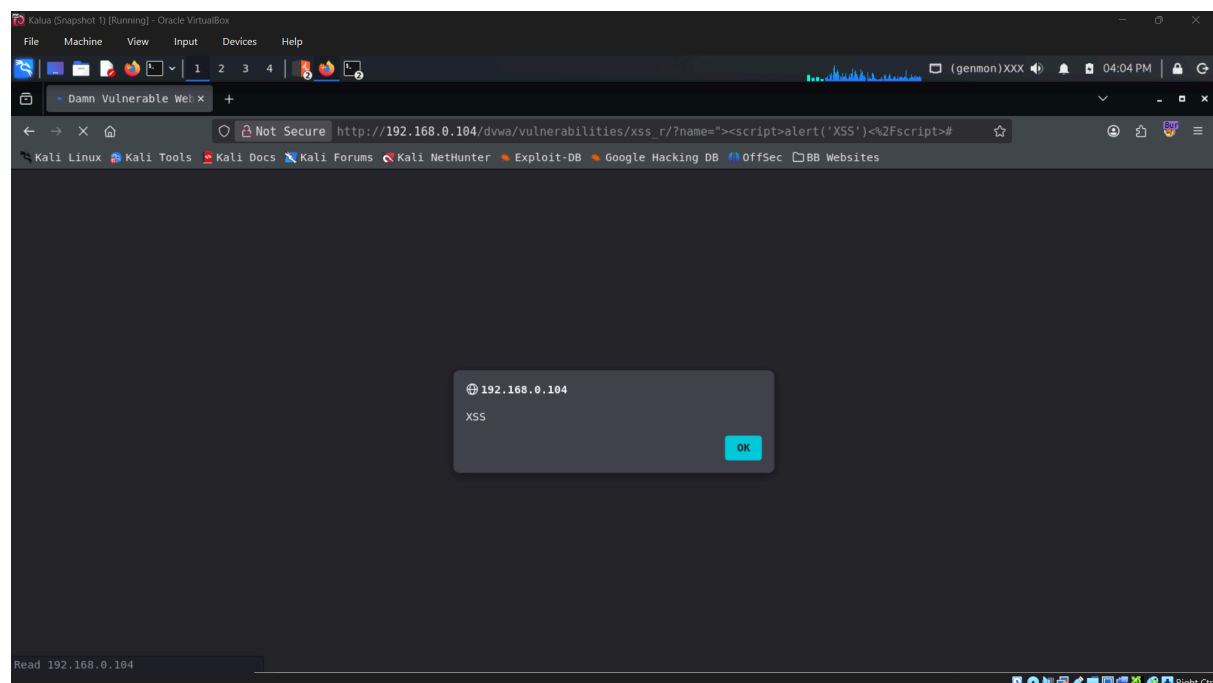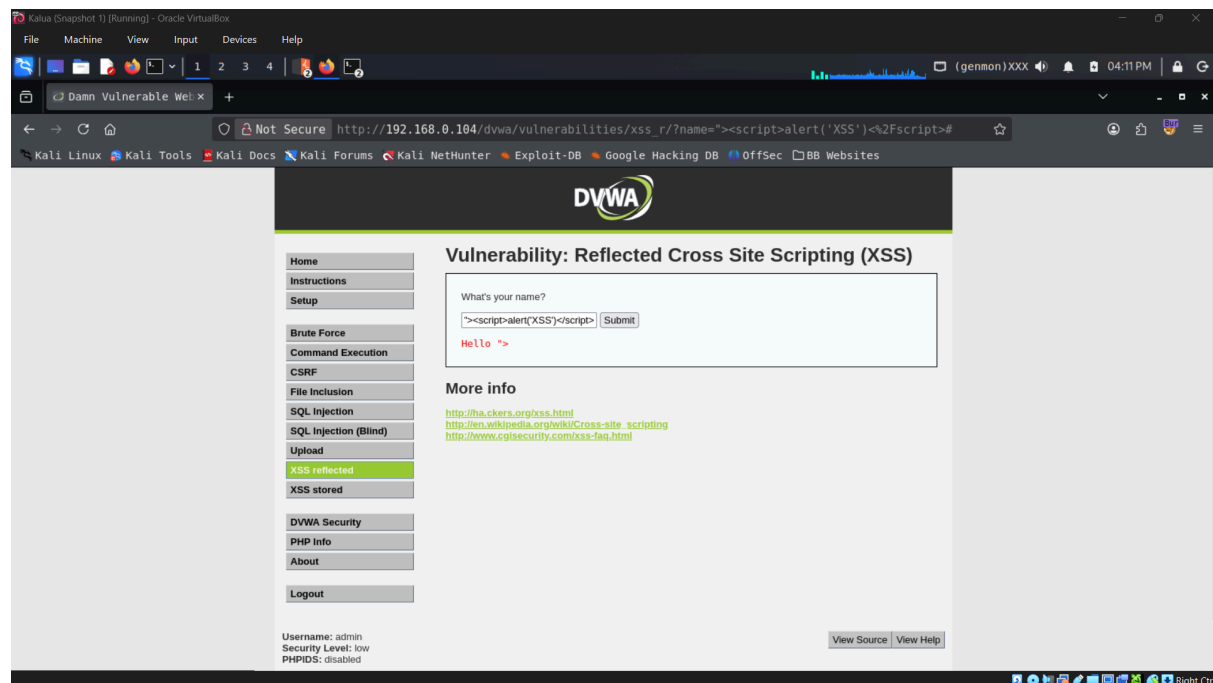
- Collect sqlmap output logs & screenshots

✔ XSS Testing (Manual)

- Inject standard payloads:

  - `<script>alert(1)</script>`

  - `"><script>alert(document.cookie)</script>`

- Test reflected XSS

- Test stored XSS

- Verify browser executes payload

- Record evidence screenshots

✔ Authentication Mechanism Checks

- Verify password strength enforcement

- Check session cookie flags:

  - Secure

  - HttpOnly

  - SameSite

- Test session fixation

- Test session hijacking

- Verify forced re-authentication

- Check for weak or reusable tokens

✔ Web Test Summary

Conducted a structured OWASP-aligned security assessment of DVWA, focusing on SQL injection, XSS, and authentication weaknesses. Used Burp Suite for interception and request manipulation, sqlmap for automated injection testing, and manual payload tests to confirm vulnerabilities. Documented findings, collected evidence, and prepared remediation recommendations.