BWAPP Labs

1.Injection

- HTML Injection-Reflected(GET)
- HTML Injection-Reflected(POST)
- HTML Injection-Reflected(Current URL)
- HTML Injection-Stored(Blog)
- iFrame Injection
- LDAP Injection(Search)
- Mail Header Injection(SMTP)
- OS Command Injection
- OS Command Injection-Blind
- PHP Code Injection
- Server - Side Includes(SSI) Injection

2. SQL Injection

- SQL Injection(GET/Search)
- SQL Injection(GET/Select)
- SQL Injection(POST/Search)
- SQL Injection(POST/Select)
- SQL Injection(AJAX/JSON/jQuery)
- SQL Injection(CAPTCHA)
- SQL Injection(Login Form/Hero)
- SQL Injection(Login Form/User)
- SQL Injection(SQLite)
- SQL Injection(Drupal)
- SQL Injection - Stored(Blog)
- SQL Injection - Stored(SQLite)
- SQL Injection - Stored(User-Agent)
- SQL Injection - Stored(XML)
- SQL Injection - Blind - Boolean-Based
- SQL Injection - Blind - Time-Based
- SQL Injection - Blind(SQLite)
- SQL Injection - Blind(Web Services/SOAP) –
- XML/XPath Injection(Login Form)
- XML/XPath Injection(Search)

3.Broken Auth. & Session Mgmt

- Broken Authentication - CAPTCHA Bypassing
- Broken Authentication - Forgotten Function
- Broken Authentication - Insecure Login Forms
- Broken Authentication - Logout Management
- Broken Authentication - Password Attacks
- Broken Authentication - Weak Passwords
- Broken Authentication - Administrative Portals
- Broken Authentication - Cookies (HTTPOnly)

- Broken Authentication - Cookies(Secure)
- Broken Authentication - Session ID in URL
- Session Management - Strong Sessions

4. Insecure Direct Object References
   - Insecure DOR (Change Secret)
   - Insecure DOR (Reset Secret)
   - Insecure DOR (Order Tickets)

5.Security Misconfiguration
   - ➔ Arbitrary File Access (Samba)----------(completed)
   - ➔ Cross-Domain Policy File(Flash)
   - ➔ Cross-Origin Resource Sharing(AJAX)
   - ➔ Cross-Site Tracing(XST)
   - ➔ Denial-of Service(Large Chunk Size)
   - ➔ Denial-of Service(Slow HTTP Dos)
   - ➔ Denial-of Service(SSL-Exhaustion)
   - ➔ Denial-of Service(XML Bomb)
   - ➔ Insecure FTP Configuration
   - ➔ Insecure SNMP Configuration
   - ➔ Insecure WebDAV Configuration
   - ➔ Local Privilege Escalation(sendpage)
   - ➔ Local Privilege Escalation(udev)
   - ➔ Man-in-the-Middle Attack(HTTP)
   - ➔ Man-in-the-Middle Attack(SMTP)
   - ➔ Old/Backup & Unreferenced Files
   - ➔ Robots File

6. Sensitive Data Exposure/
   - Base64 Encoding(Secret)
   - BEAST/CRIME/BREACH Attacks
   - Clear Text HTTP(Credentials)
   - Heartbleed Vulnerability
   - Host Header Attack(Reset Poisoning)
   - HTML5 Web Storage(Secret)
   - POODLE Vulnerability
   - SSL 2.0 Deprecated Protocol
   - Text Files(Accounts)

7.Missing Functional Level Access Control/
   - ★ Directory Traversal - Directories
   - ★ Directory Traversal - Files
   - ★ Host Header Attack (Cache Poisoning)
   - ★ Host Header Attack(Reset Poisoning)

- ★ Local File Inclusion(SQLiteManager)
- ★ Remote & Local File Inclusion(RFI/LFI)
- ★ Restrict Device Access
- ★ Restrict Folder Access
- ★ Server Side Request Forgery(SSRF)
- ★ XML External Entity Attacks(XXE)

8.Using Known Vulnerable Components/

- ❖ Buffer Overflow(Local)
- ❖ Buffer Overflow(Remote)
- ❖ Drupal SQL Injection (Drupageddon)
- ❖ Heartbleed Vulnerability
- ❖ PHP CGI Remote Code Execution
- ❖ PHP Eval Function
- ❖ phpMyAdmin BBCode Tag XSS
- ❖ Shellshock Vulnerability(CGI)
- ❖ SQLiteManager Local File Inclusion
- ❖ SQLiteManager PHP Code Injection
- ❖ SQLiteManager XSS

9.-Unvalidated Redirects & Forwards/

- Unvalidated Redirects & Forwards (1)
- Unvalidated Redirects & Forwards (2)

10.Other bugs…./

- ★ ClickJacking (Movie Tickets)
- ★ Click-Side Validation(Password)
- ★ HTTP Parameter Pollution
- ★ HTTP Response Splitting
- ★ HTTP Verb Tampering
- ★ Information Disclosure - Favicon
- ★ Information Disclosure - Headers
- ★ Information Disclosure - PHP Version
- ★ Information Disclosure - Robots File
- ★ Insecure iFrame (Login Form)
- ★ Unrestricted File Upload

11.Extras

- A.I.M. - No-authentication Mode
- Client Access Policy File
- Cross- Domain Policy File
- Evil 666 Fuzzing Page
- Manual Intervention Required!
- Unprotected Admin Portal

- We Steal Secrets…..(html)
- We Steal Secrets…(Plain)
- WSDL File (Web Services/SOAP)

12 - Cross-Site Request Forgery(CSRF)/ (noe needed)

- Cross-Site Request Forgery (Change Password)
- Cross-Site Request Forgery (Change Secret)
- Cross-Site Request Forgery (Transfer Amount)

Portswigger Labs

1. SQL Injection
2. Cross-site scripting
3. Cross-site request forgery (CSRF)
4. Clickjacking
5. DOM-based vulnerabilities
6. Cross-origin resource sharing (CORS)
7. XML external entity (XXE) injection
8. Server-side request forgery (SSRF)
9. HTTP request smuggling
10. OS command injection (skipped done in dvwa)
11. Server-side template injection
12. Directory traversal
13. Access control vulnerabilities
14. Authentication
15. WebSockets
16. Web cache poisoning
17. Insecure deserialization
18. Information disclosure
19. Business logic vulnerabilities
20. HTTP Host header attacks
21. OAuth authentication
22. File upload vulnerabilities (skipped done in dvwa)
23. JWT

DVWA Labs

1. Brute force
2. Command execution

3. CSRF
4. File inclusion
5. SQL Injection
6. SQL Injection (Blind)
7. Upload
8. XSS reflected
9. XSS stored