bWAPP

/ A1 - Injection /

|  |
| --- |
| 類型 |
| 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  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) |

/ A2 - Broken Auth. & Session Mgmt. /

|  |
| --- |
| 類型 |
| 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  Session Management - Administrative Portals  Session Management - Cookies (HTTPOnly)  Session Management - Cookies (Secure)  Session Management - Session ID in URL  Session Management - Strong Sessions |

/ A3 - Cross-Site Scripting (XSS) /

|  |
| --- |
| 類型 |
| Cross-Site Scripting - Reflected (GET)  Cross-Site Scripting - Reflected (POST)  Cross-Site Scripting - Reflected (JSON)  Cross-Site Scripting - Reflected (AJAX/JSON)  Cross-Site Scripting - Reflected (AJAX/XML)  Cross-Site Scripting - Reflected (Back Button)  Cross-Site Scripting - Reflected (Custom Header)  Cross-Site Scripting - Reflected (Eval)  Cross-Site Scripting - Reflected (HREF)  Cross-Site Scripting - Reflected (Login Form)  Cross-Site Scripting - Reflected (phpMyAdmin)  Cross-Site Scripting - Reflected (PHP\_SELF)  Cross-Site Scripting - Reflected (Referer)  Cross-Site Scripting - Reflected (User-Agent)  Cross-Site Scripting - Stored (Blog)  Cross-Site Scripting - Stored (Change Secret)  Cross-Site Scripting - Stored (Cookies)  Cross-Site Scripting - Stored (SQLiteManager)  Cross-Site Scripting - Stored (User-Agent) |

/ A4 - Insecure Direct Object References /

|  |
| --- |
| 類型 |
| Insecure DOR (Change Secret)  Insecure DOR (Reset Secret)  Insecure DOR (Order Tickets) |

/ A5 - Security Misconfiguration /

|  |
| --- |
| 類型 |
| Arbitrary File Access (Samba)  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 |

/ A6 - Sensitive Data Exposure /

|  |
| --- |
| 類型 |
| 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) |

/ A7 - Missing Functional Level Access Control /

|  |
| --- |
| 類型 |
| 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) |

/ A8 - Cross-Site Request Forgery (CSRF) /

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

/ A9 - Using Known Vulnerable Components /

|  |
| --- |
| 類型 |
| 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 |

/ A10 - Unvalidated Redirects & Forwards /

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

/ Other bugs... /

|  |
| --- |
| 類型 |
| ClickJacking (Movie Tickets)  Client-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 |