Mutillidae

A1 - Injection (SQL)

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| SQLi - Extract Data | User Info (SQL) |
| SQLi - Bypass Authentication | Login |
| SQLi - Insert Injection | Add to your blog  Register  View Captured Data |
| Blind SQL via Timing | Login  User Info (SQL) |
| SQLMAP Practice | SQLMAP Practice Targets  Login  View Someones Blog  User Info (SQL) |
| Via JavaScript Object Notation (JSON) | Pen Test Tool Lookup  Pen Test Tool Lookup (AJAX) |
| Via SOAP Web Service | Lookup User |
| Via REST Web Service | User Account Management |

A1 - Injection (Other)

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| Application Log Injection | Add to your blog  Document Viewer  Capture Data Page  Login  Register User  Source Viewer  DNS Lookup  Text File Viewer |
| Buffer Overflow | Repeater |
| Capture Data Page | Set Background Color |
| CBC-bit Flipping |  |
| Command Injection | DNS Lookup  DNS Lookup (SOAP Web Service) |
| Frame Source Injection | Document Viewer  Styling with Mutilidae |
| HTML Injection (HTMLi) | Browser Info  Pen Test Tool Lookup  Text File Viewer  User Info (SQL)  User Info (XPath)  Set Background Color  HTML5 Web Storage  Capture Data Page  View Captured Data  Document Viewer  Arbitrary File Inclusion  Poll Question  Register User  Login  Those “Back” Buttons  Styling with Mutilidae  Password Generator |
| HTMLi via HTTP Headers | Those “Back” Buttons  Browser Info  Site Footer  HTTP Response Splitting (Hint: Difficult) |
| HTMLi Via DOM Injection | HTML5 Web Storage  Password Generator |
| HTMLi Via Cookie Injection | Capture Data Page |
| HTTP Parameter Pollution | Poll Question  Document Viewer |
| JavaScript Injection | Those “Back” Buttons  Password Generator  Browser Info |
| JavaScript Object Notation (JSON) Injection | Pen Test Tool Lookup  Pen Test Tool Lookup (AJAX) |
| Parameter Addition | Repeater  View User Privileges |
| XML External Entity Injection | XML Validator |
| XML Entity Expansion | XML Validator |
| XML Injection | XML Validator |
| XPath Injection | User Info (XPath) |

A2 - Broken Authentication and Session Management

|  |  |  |
| --- | --- | --- |
| 類別1 | 類別2 | 類別3 |
| Authentication Bypass | Via Brute Force | Login |
|  | Via Cookies |  |
|  | Via SQL Injection | Login |
| Priviliege Escalation | Via Cookies  Login  Via CBC-bit Flipping |  |
| Username Enumeration | Login  User Account Management (REST Web Service) |  |

A3 - Sensitive Data Exposure

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| Information Disclosure | PHP MyAdmin Console  PHP Info Page  Robots.txt  Secret" Administrative Pages  HTML5 Web Storage  HTML/JavaScript Comments  Cache-Control  Click-Jacking  Cross-Site Framing (Third-Party Framing)  X-Frame-Options (Click-Jacking)  X-Frame-Options (Cross-frame Scripting) |
| Application Path Disclosure | PHP MyAdmin Console  PHP Info Page  Robots.txt |
| Platform Path Disclosure | PHP MyAdmin Console  PHP Info Page  SSL Misconfiguration |

A4 - XML External Entitie

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| XML External Entity Injection | XML Validator |

A5 - Broken Access Control

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| Insecure Direct Object References | Local File Inclusion  Remote File Inclusion  Text File Viewer  Source Viewer  Credits |
| Missing Function Level Access Contro | Cookies as Auth Tokens  “Secret" Administrative Pages  Robots.txt |

A6 - Security Misconfiguration

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| Directory Browsing | Method Tampering (GET for POST)  Add to your blog  User Info (SQL)  User Info (XPath)  Poll Question  DNS Lookup  User-Agent Impersonation  Unrestricted File Upload  SSL Misconfiguration  PHP MyAdmin Console  PHP Info Page  Robots.txt  Cache-Control  Click-Jacking  Cross-Site Framing (Third-Party Framing) |

A7 - Cross Site Scripting (XSS)

|  |  |
| --- | --- |
| 類別1 | 類別2 |
| Reflected (First Order) | DNS Lookup  Pen Test Tool Lookup  Text File Viewer  User Info (SQL)  Set Background Color  HTML5 Web Storage  Capture Data Page  Document Viewer  Arbitrary File Inclusion  XML Validator  User Info (XPath)  Poll Question  Register User  Browser Info  Those “Back” Buttons  Styling with Mutilidae  Password Generator  Client-side Control Challenge |
| Persistent (Second Order) | Add to your blog  View someone's blog  Show Log |
| DOM-Based | HTML5 Web Storage  Password Generator |
| Via "Input" (GET/POST) | Add to your blog  View someone's blog  Show Log  Text File Viewer  DNS Lookup  User Info (SQL)  User Info (XPath)  Missing HTTPOnly Attribute  Set Background Color  Pen Test Tool Lookup  Document Viewer |
| Via HTTP Headers | Browser Info  Show Log  Site Footer  Those “Back” Buttons |
| Via HTTP Attribute | Document Viewer |
| Via Misconfiguration | Missing HTTPOnly Attribute |
| Against HTML5 Web Storage | HTML5 Web Storage |
| Against JSON | Pen Test Tool Lookup |
| Via Cookie Injection | Capture Data Page |
| Via XML Injection | XML Validator |
| Via XPath Injection | User Info (XPath) |
| Via Path Relative Style Sheet Injection | Styling with Mutilidae |
| BeeF Framework Targets | Add to your blog  View someone's blog  Show Log  DNS Lookup  Pen Test Tool Lookup  Text File Viewer  User Info (SQL)  Set Background Color  HTML5 Web Storage  Capture Data Page  Document Viewer  Arbitrary File Inclusion  XML Validator  User Info (XPath)  Poll Question  Register User  Password Generator |

A8 - Insecure Deserialization

|  |
| --- |
| 類別1 |
| A8 - Insecure Deserialization |

A9 - Using Components with Known Vulnerabilities

|  |
| --- |
| 類別1 |
| PHP MyAdmin Console |
| PHP Info Page |
| CBC-bit Flipping |
| SSL Misconfiguration |

A10 - Insufficient Logging and Monitoring

|  |
| --- |
| 類別1 |
| A10 - Insufficient Logging and Monitoring |