|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OWASP Top Ten | 2003 | 2004 | 2007 | 2010 | 2013 | 2017  RC1 | 2017  RC2 |
| Unvalidated Input | A1 | A1[9] |  |  |  |  |  |
| Buffer Overflows | A5 | A5 |  |  |  |  |  |
| Denial of Service |  | A9[2] |  |  |  |  |  |
| Injection | A6 | A6[3] | A2 | A1[10] | A1 | A1 | A1 |
| Cross Site Scripting (XSS) | A4 | A4 | A1 | A2 | A3 | A3 | A7 |
| Broken Authentication and Session Management | A3 | A3 | A7 | A3 | A2 | A2 | A2 |
| Insecure Direct Object Reference |  | A2 | A4[11] | A4 | A4 | A4[20] | A5[20] |
| Cross Site Request Forgery (CSRF) |  |  | A5 | A5 | A8 | A8 |  |
| Security Misconfiguration | A10 | A10[3][5] |  | A6 | A5 | A5 | A6 |
| Broken Access Control | A2 | A2[1] | A10[13] | A8 | A7[16] | A4 | A5 |
| Insufficient Attack Protection |  |  |  |  |  | A7 |  |
| Unvalidated Redirects and Forwards |  |  |  | A10 | A10 |  |  |
| Information Leakage and Improper Error Handling | A7 | A7[14][4] | A6 | A6[8] |  |  |  |
| Malicious File Execution |  |  | A3 | A6[8] |  |  |  |
| Sensitive Data Exposure | A8 | A8[6][5] | A8 | A7 | A6[17] | A6 | A3 |
| Insecure Communications |  | A10 | A9[7] | A9 |  |  |  |
| Remote Administration Flaws | A9 |  |  |  |  |  |  |
| Using Known Vulnerable Components |  |  |  |  | A9 [18][19] | A9 | A9 |
| Unprotected APIs |  |  |  |  |  | A10 |  |
| Insecure Deserialization |  |  |  |  |  |  | A8 |
| XML External Entity (XXE) |  |  |  |  |  |  | A4 |
| Insufficient Logging & Monitoring |  |  |  |  |  |  | A10 |

|  |  |
| --- | --- |
| [1] Renamed “Broken Access Control” from T10 2003 | [11] Split “Broken Access Control” from T10 2004 |
| [2] Split “Broken Access Control” from T10 2003 | [12] Renamed “Insecure Configuration Management” from T10 2004 |
| [3] Renamed “Command Injection Flaws” from T10 2003 | [13] Split “Broken Access Control” from T10 2004 |
| [4] Renamed “Error Handling Problems” from T10 2003 | [14] Renamed “Improper Error Handling” from T10 2004 |
| [5] Renamed “Insecure Use of Cryptography” from T10 2003 | [15] Renamed “Insecure Storage” from T10 2004 |
| [6] Renamed “Web and Application Server” from T10 2003 | [16] Renamed “Failure to Restrict URL Access” from T10 2010 |
| [7] Split “Insecure Configuration Management” from T10 2004 | [17] Renamed “Insecure Cryptographic Storage” from T10 2010 |
| [8] Reconsidered during T10 2010 Release Candidate (RC) | [18] Split “Insecure Cryptographic Storage” from T10 2010 |
| [9] Renamed “Unvalidated Parameters” from T10 2003 | [19] Split “Security Misconfiguration” from T10 2010 |
| [10] Renamed “Injection Flaws” from T10 2007 | [20] Split “Broken Access Control” from T10 2013 |