|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OWASP Top Ten | 2003 | 2004 | 2007 | 2010 | 2013 | 2017 | 2021 |
| Broken Access Control | A2 | A2[1] | A10[13] | A8 | A7[16] | A5 | A1 |
| Cryptographic Failures | A8 | A8[6][5] | A8 | A7 | A6[17] | A3 | A2[21] |
| Injection | A6 | A6[3] | A2 | A1[10] | A1 | A1 | A3 |
| Insecure Design | û | û | û | û | û | û | A4 |
| Security Misconfiguration | A10 | A10[3][5] | û | A6 | A5 | A6 | A5 |
| XML External Entity (XXE) | û | û | û | û | û | A4 | A5 |
| Vulnerable and Outdated Components | û | û | û | û | A9 [18][19] | A9 | A6[25] |
| Identification and Authentication Failures | A3 | A3 | A7 | A3 | A2 | A2 | A7[22] |
| Software and Data Integrity Failures | û | û | û | û | û | A8 | A8[23] |
| Security Logging and Monitoring Failures | û | û | û | û | û | A10 | A9[24] |
| Server-Side Request Forgery (SSRF) | û | û | û | û | û | û | A10 |
| Code Quality Issues | û | û | û | û | û | û | A11[26] |
| Denial of Service | û | û | û | û | û | û | A11[26] |
| Memory Management Errors | û | û | û | û | û | û | A11[26] |
| Unvalidated Input | A1 | A1[9] | û | û | û | û | û |
| Buffer Overflows | A5 | A5 | û | û | û | û | û |
| Denial of Service | û | A9[2] | û | û | û | û | û |
| Cross Site Scripting (XSS) | A4 | A4 | A1 | A2 | A3 | A7 | û |
| Insecure Direct Object Reference | û | A2 | A4[11] | A4 | A4 | A5[20] | û |
| Cross Site Request Forgery (CSRF) | û | û | A5 | A5 | A8 | û | û |
| Insufficient Attack Protection | û | û | û | û | û | û | û |
| Unvalidated Redirects and Forwards | û | û | û | A10 | A10 | û | û |
| Information Leakage and Improper Error Handling | A7 | A7[14][4] | A6 | A6[8] | û | û | û |
| Malicious File Execution | û | û | A3 | A6[8] | û | û | û |
| Insecure Communications | û | A10 | A9[7] | A9 | û | û | û |
| Remote Administration Flaws | A9 | û | û | û | û | û | û |
| Unprotected APIs | û | û | û | û | û | û | û |

|  |  |  |
| --- | --- | --- |
| [1] Renamed “Broken Access Control” from 2003 | [14] Renamed “Improper Error Handling” from 2004 | Colour Legend |
| [2] Split “Broken Access Control” from 2003 | [15] Renamed “Insecure Storage” from 2004 | Ranked Category |
| [3] Renamed “Command Injection Flaws” from 2003 | [16] Renamed “Failure to Restrict URL Access” from 2010 | Subcategory |
| [4] Renamed “Error Handling Problems” from 2003 | [17] Renamed “Insecure Cryptographic Storage” from 2010 | Unranked Category |
| [5] Renamed “Insecure Use of Cryptography” from 2003 | [18] Split “Insecure Cryptographic Storage” from 2010 |  |
| [6] Renamed “Web and Application Server” from 2003 | [19] Split “Security Misconfiguration” from 2010 |  |
| [7] Split “Insecure Configuration Management” from 2004 | [20] Split “Broken Access Control” from 2013 |  |
| [8] Reconsidered during T10 2010 Release Candidate (RC) | [21] Renamed “Sensitive Data Exposure” from 2017 |  |
| [9] Renamed “Unvalidated Parameters” from 2003 | [22] Renamed “Broken Authentication and Session Management” from 2017 |  |
| [10] Renamed “Injection Flaws” from 2007 | [23] Renamed “Insecure Deserialization” from 2017 |  |
| [11] Split “Broken Access Control” from 2004 | [24] Renamed “Insufficient Logging & Monitoring” from 2017 |  |
| [12] Renamed “Insecure Configuration Management” from 2004 | [25] Renamed “Using Known Vulnerable Components” from 2017 |  |
| [13] Split “Broken Access Control” from 2004 | [26] Split "Next Steps" from 2021 |  |
|  |  |  |