

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Vulnerable and Outdated Components	✗	✗	✗	✗	A9 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

- |  |   |
|--|---|
| [1] Renamed "Broken Access Control" from 2003              | [14] Renamed "Improper Error Handling" from 2004                      |
| [2] Split "Broken Access Control" from 2003                | [15] Renamed "Insecure Storage" from 2004                             |
| [3] Renamed "Command Injection Flaws" from 2003            | [16] Renamed "Failure to Restrict URL Access" from 2010               |
| [4] Renamed "Error Handling Problems" from 2003            | [17] Renamed "Insecure Cryptographic Storage" from 2010               |
| [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                                     |

Colour Legend
Ranked Category
Split
Unranked Category