

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	×	×	×	×	×	×	A4
Security Misconfiguration	A10	A10 ^{[3][5]}	×	A6	A5	A6	A5
XML External Entity (XXE)	×	×	×	×	×	A4	A5
Vulnerable and Outdated Components	×	×	×	×	A9 ^{[18][19]}	A9	A6 ^[25]
Identification and Authentication Failures	A3	A3	A7	A3	A2	A2	A7 ^[22]
Software and Data Integrity Failures	×	×	×	×	×	A8	A8 ^[23]
Security Logging and Monitoring Failures	×	×	×	×	×	A10	A9 ^[24]
Server-Side Request Forgery (SSRF)	×	×	×	×	×	×	A10
Code Quality Issues	×	×	×	×	×	×	A11 ^[26]
Denial of Service	×	×	×	×	×	×	A11 ^[26]
Memory Management Errors	×	×	×	×	×	×	A11 ^[26]
Unvalidated Input	A1	A1 ^[9]	×	×	×	×	×
Buffer Overflows	A5	A5	×	×	×	×	×
Denial of Service	×	A9 ^[2]	×	×	×	×	×
Cross Site Scripting (XSS)	A4	A4	A1	A2	A3	A7	×
Insecure Direct Object Reference	×	A2	A4 ^[11]	A4	A4	A5 ^[20]	×
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 ^{[14][4]}	A6	A6 ^[8]	×	×	×
Malicious File Execution	×	×	A3	A6 ^[8]	×	×	×
Insecure Communications	×	A10	A9 ^[7]	A9	×	×	×
Remote Administration Flaws	A9	×	×	×	×	×	×
Unprotected APIs	×	×	×	×	×	×	×

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