
Certified Secure Web Application Security Test Checklist

About

Certified Secure exists to encourage and fulfill the growing interest in IT security knowledge and skills. We stand for openness, transparency and the sharing of knowledge; making sure everybody can experience and enjoy IT security. Security is serious fun!

All Certified Secure certifications, products and training are developed by IT security professionals with international recognized expertise. Our involvement in the IT security community worldwide, ensures relevant and high-quality standards. Delivering a wide variety of online challenges, videos, tools and more, Certified Secure is the authoritative source for practical IT security know-how.

Scope

This checklist can be used as a standard when performing a remote security test on a web application. For developers and auditors a separate Web Application Secure Development Checklist is available from <https://www.certifiedsecure.com/checklists>.

Usage




Security testers should use this checklist when performing a remote security test of a web application. A risk analysis for the web application should be performed before starting with the checklist. Every test on the checklist should be completed or explicitly marked as being not applicable. Once a test is completed the checklist should be updated with the appropriate result icon and a document cross-reference.

The completed checklist should never be delivered standalone but should be incorporated in a report detailing the risk analysis and checklist results and the scope and context of the performed remote security test.

License

This work is licensed under a Creative Commons Attribution No Derivatives 4.0 International License. The complete Creative Commons license text can be found online at <https://creativecommons.org/licenses/by-nd/4.0/legalcode>

Result Icon Legend

| Icon | Explanation |
|---|--|
|  | Test was performed and results are okay |
|  | Test was performed and results require attention |
|  | Test was not applicable |



| # | Certified Secure Web Application Security Test Checklist | Result | Ref |
|------------|--|--------|-----|
| 1.0 | Deployment | | |
| 1.1 | Test for missing security updates | | |
| 1.2 | Test for unsupported or end-of-life software versions | | |
| 1.3 | Test for HTTP TRACK and TRACE methods | | |
| 1.4 | Test for extraneous functionality | | |
| 1.5 | Test the server using the Server Security Test Checklist | | |
| 2.0 | Information Disclosure | | |
| 2.1 | Test for extraneous files in the document root | | |
| 2.2 | Test for extraneous directory listings | | |
| 2.3 | Test for accessible debug functionality | | |
| 2.4 | Test for sensitive information in log and error messages | | |
| 2.5 | Test for sensitive information in robots.txt | | |
| 2.6 | Test for sensitive information in source code | | |
| 2.7 | Test for disclosure of internal addresses | | |
| 3.0 | Privacy and Confidentiality | | |
| 3.1 | Test for URLs containing sensitive information | | |
| 3.2 | Test for unencrypted sensitive information stored at the client side | | |
| 3.3 | Test for sensitive information stored in (externally) archived pages | | |
| 3.4 | Test for content included from untrusted sources | | |
| 3.5 | Test for caching of pages with sensitive information | | |
| 3.6 | Test for insecure transmission of sensitive information | | |
| 3.7 | Test for non-SSL/TLS pages on sites processing sensitive information | | |
| 3.8 | Test for SSL/TLS pages served with mixed content | | |



| # | Certified Secure Web Application Security Test Checklist | Result | Ref |
|------------|--|--------|-----|
| 3.9 | Test for missing HSTS header on full SSL sites | | |
| 3.10 | Test for known vulnerabilities in SSL/TLS | | |
| 3.11 | Test for cache poisoning | | |
| 4.0 | State Management | | |
| 4.1 | Test for client-side state management | | |
| 4.2 | Test for invalid state transitions | | |
| 4.3 | Test for race conditions | | |
| 5.0 | Authentication and Authorization | | |
| 5.1 | Test for missing or insufficient authentication | | |
| 5.2 | Test for missing or insufficient authorization | | |
| 5.3 | Test for client-side authentication or authorization | | |
| 5.4 | Test for predictable and default credentials | | |
| 5.5 | Test for predictable authentication or authorization tokens | | |
| 5.6 | Test for authentication or authorization based on obscurity | | |
| 5.7 | Test for insecure direct object references (IDOR) | | |
| 5.8 | Test for acceptance of weak passwords | | |
| 5.9 | Test for plaintext storage of passwords | | |
| 5.10 | Test for missing rate limiting on authentication functionality | | |
| 5.11 | Test for missing re-authentication when changing credentials | | |
| 5.12 | Test for missing logout functionality | | |
| 6.0 | Cryptography | | |
| 6.1 | Test for the usage of unproven cryptographic algorithms | | |
| 6.2 | Test for the incorrect usage of cryptographic algorithms | | |



| # | Certified Secure Web Application Security Test Checklist | Result | Ref |
|------------|---|--------|-----|
| 6.3 | Test for weak, untrusted or expired certificates | | |
| 6.4 | Test for weak cryptographic secrets | | |
| 6.5 | Test for missing, incomplete or insecure cryptographic signatures | | |
| 6.6 | Test for replay attacks | | |
| 7.0 | User Input | | |
| 7.1 | Test for SQL injection | | |
| 7.2 | Test for path traversal and filename injection | | |
| 7.3 | Test for cross-site scripting | | |
| 7.4 | Test for system command injection | | |
| 7.5 | Test for XML injection | | |
| 7.6 | Test for XPath injection | | |
| 7.7 | Test for XSL(T) injection | | |
| 7.8 | Test for SSI injection | | |
| 7.9 | Test for HTTP header injection | | |
| 7.10 | Test for HTTP parameter injection | | |
| 7.11 | Test for LDAP injection | | |
| 7.12 | Test for dynamic scripting injection | | |
| 7.13 | Test for regular expression injection | | |
| 7.14 | Test for data property/field injection | | |
| 7.15 | Test for expression language injection | | |
| 7.16 | Test for context-specific injection | | |
| 7.17 | Test for insecure deserialization | | |
| 8.0 | Sessions | | |



| # | Certified Secure Web Application Security Test Checklist | Result | Ref |
|------------|---|--------|-----|
| 8.1 | Test for cross-site request forgery (CSRF) | | |
| 8.2 | Test for predictable CSRF tokens | | |
| 8.3 | Test for missing session revocation on logout | | |
| 8.4 | Test for missing session regeneration on login | | |
| 8.5 | Test for missing session regeneration when changing credentials | | |
| 8.6 | Test for missing session revocation when changing credentials | | |
| 8.7 | Test for missing Secure flag on session cookies | | |
| 8.8 | Test for missing HttpOnly Flag on session cookies | | |
| 8.9 | Test for non-restrictive or missing "SameSite" attribute on session cookies | | |
| 8.10 | Test for non-restrictive "Domain" attribute on session cookies | | |
| 8.11 | Test for non-restrictive or missing "Path" attribute on session cookies | | |
| 8.12 | Test for missing "_Host-" or "_Secure-" cookie prefix for session cookies | | |
| 8.13 | Test for predictable session identifiers | | |
| 8.14 | Test for session identifier collisions | | |
| 8.15 | Test for session fixation | | |
| 8.16 | Test for insecure transmission of session identifiers | | |
| 8.17 | Test for missing expiration of sessions and tokens | | |
| 9.0 | File Uploads | | |
| 9.1 | Test for storage of uploaded files in the document root | | |
| 9.2 | Test for execution or interpretation of uploaded files | | |
| 9.3 | Test for uploading outside of designated upload directory | | |
| 9.4 | Test for missing size restrictions on uploaded files | | |
| 9.5 | Test for missing type validation on uploaded files | | |



| # | Certified Secure Web Application Security Test Checklist | Result | Ref |
|-------------|---|--------|-----|
| 10.0 | Content | | |
| 10.1 | Test for missing or non-specific content type specifications | | |
| 10.2 | Test for missing character set specifications | | |
| 10.3 | Test for missing measures against content sniffing | | |
| 11.0 | XML Processing | | |
| 11.1 | Test for XML external entity expansion | | |
| 11.2 | Test for external DTD parsing | | |
| 11.3 | Test for extraneous or dangerous XML extensions | | |
| 11.4 | Test for recursive entity expansion | | |
| 12.0 | Miscellaneous | | |
| 12.1 | Test for missing anti-clickjacking measures | | |
| 12.2 | Test for open redirection | | |
| 12.3 | Test for server-side request forgery (SSRF) | | |
| 12.4 | Test for insecure cross-domain access policy | | |
| 12.5 | Test for missing rate limiting on email functionality | | |
| 12.6 | Test for missing rate limiting on resource-intensive functionality | | |
| 12.7 | Test for inappropriate rate limiting resulting in a denial of service | | |
| 12.8 | Test for HTTP request smuggling | | |
| 12.9 | Test for application- or setup-specific problems | | |