#	Certified Secure Web Application Security Test Checklist	Status
1	**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	[ ]
1.6	Are abandoned/dead projects taken offline?	[ ]
2	**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	**Privacy and Confidentiality**	
3.1	Test for sensitive information stored in URLs	[ ]
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	[ ]
3.9	Test for missing HSTS header on full SSL sites	[ ]
3.10	Test for known vulnerabilities in SSL/TLS	[ ]
3.11	Test for weak, untrusted or expired SSL certificates	[ ]
3.12	Test for the usage of unproven cryptographic primitives	[ ]
3.13	Test for the incorrect usage of cryptographic primitives	[ ]
4	**State Management**	
4.1	Test for client-side state management	[ ]
4.2	Test for invalid state transitions	[ ]
5	**Authentication and Authorization**	
5.1	Test for missing authentication or authorization	[ ]
5.2	Test for client-side authentication	[ ]
5.3	Test for predictable and default credentials	[ ]
5.4	Test for predictable authentication or authorization tokens	[ ]

5.5	Test for authentication or authorization based on obscurity	[ ]
5.6	Test for identifier-based authorization	[ ]
5.7	Test for acceptance of weak passwords	[ ]
5.8	Test for plaintext retrieval of passwords	[ ]
5.9	Test for missing rate limiting on authentication functionality	[ ]
5.10	Test for missing re-authentication when changing credentials	[ ]
5.11	Test for missing logout functionality	[ ]
6	**User Input**	
6.1	Test for SQL injection	[ ]
6.2	Test for path traversal and filename injection	[ ]
6.3	Test for cross-site scripting	[ ]
6.4	Test for system command injection	[ ]
6.5	Test for XML injection	[ ]
6.6	Test for XPath injection	[ ]
6.7	Test for XSL(T) injection	[ ]
6.8	Test for SSI injection	[ ]
6.9	Test for HTTP header injection	[ ]
6.10	Test for HTTP parameter injection	[ ]
6.11	Test for LDAP injection	[ ]
6.12	Test for dynamic scripting injection	[ ]
6.13	Test for regular expression injection	[ ]
6.14	Test for data property/field injection	[ ]
6.15	Test for protocol-specific injection	[ ]
6.16	Test for expression language injection	[ ]
7	**Sessions**	
7.1	Test for cross-site request forgery (CSRF)	[ ]
7.2	Test for predictable CSRF tokens	[ ]
7.3	Test for missing session revocation on logout	[ ]
7.4	Test for missing session regeneration on login	[ ]
7.5	Test for missing session regeneration when changing credentials	[ ]
7.6	Test for missing revocation of other sessions when changing credentials	[ ]
7.7	Test for missing Secure flag on session cookies	[ ]
7.8	Test for missing HttpOnly Flag on session cookies	[ ]
7.9	Test for non-restrictive domain on session cookies	[ ]
7.10	Test for non-restrictive or missing path on session cookies	[ ]
7.11	Test for predictable session identifiers	[ ]
7.12	Test for session identifier collisions	[ ]
7.13	Test for session fixation	[ ]
7.14	Test for insecure transmission of session identifiers	[ ]

7.15	Test for external session hijacking	[ ]
7.16	Test for missing periodic expiration of sessions	[ ]

8	**File Uploads**	
8.1	Test for storage of uploaded files in the document root	[ ]
8.2	Test for execution or interpretation of uploaded files	[ ]
8.3	Test for uploading outside of designated upload directory	[ ]
8.4	Test for missing size restrictions on uploaded files	[ ]
8.5	Test for missing type validation on uploaded files	[ ]
9	**Content**	
9.1	Test for missing or non-specific content type definitions	[ ]
9.2	Test for missing character set definitions	[ ]
9.3	Test for missing anti content sniffing measures	[ ]
10.0	**XML Processing**	[ ]
10.1	Test for XML external entity expansion	[ ]
10.2	Test for external DTD parsing	[ ]
10.3	Test for extraneous or dangerous XML extensions	[ ]
10.4	Test for recursive entity expansion	[ ]
11	**Miscellaneous**	
11.1	Test for missing anti-clickjacking measures	[ ]
11.2	Test for open redirection	[ ]
11.3	Test for insecure cross-domain access policy	[ ]
11.4	Test for missing rate limiting on e-mail functionality	[ ]
11.5	Test for missing rate limiting on resource intensive functionality	[ ]
11.6	Test for inappropriate rate limiting resulting in a denial of service	[ ]
11.7	Test for application- or setup-specific problems	[ ]
11.8	Test for validity of keys i.e are keys being recycled or expired	[ ]
12	**Databases**	
12.1	Test for storage of data in plain text	[ ]
12.2	Test of common access credentials for databases	[ ]
13	XML Processing	[ ]
13.1	Test for XML external entity expansion	[ ]
13.2	Test for external DTD parsing	[ ]
13.3	Test for extraneous or dangerous XML extensions	[ ]
13.4	Test for recursive entity expansion	[ ]
14	**Logging and Monitoring**	
14.1	Test for storage of sensitive information in plain text in logs	[ ]
14.2	Test for defensive measures to protect against repudiation attacks, such as verifiable and protected transaction logs, audit trails or system logs	[ ]
14.3	Test for real time monitoring in highly sensitive systems	[ ]
14.4	Test for generation of event logs	[ ]

15	**Incident Management**	
15.1	Test for continuous monitoring of security incidents	[ ]
15.2	Test for delayed response for resolution of critical incidents	[ ]
15.3	Test for non-availability of escalation matrix	[ ]
15.4	Test for wrong classification of incidents as per criticality	[ ]
16	**Miscellaneous**	
16.1	Test for missing anti-clickjacking measures	[ ]
16.2	Test for open redirection	[ ]
16.3	Test for insecure cross-domain access policy	[ ]
16.4	Test for missing rate limiting on e-mail functionality	[ ]
16.5	Test for missing rate limiting on resource intensive functionality	[ ]
16.6	Test for inappropriate rate limiting resulting in a denial of service	[ ]
16.7	Test for application- or setup-specific problems	[ ]