OWASP-Based Website Security Testing Checklist

Information Gathering

- [ ] Manually explore the site
- [ ] Spider/crawl for missed or hidden content
- [ ] Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store
- [ ] Check the caches of major search engines for publicly accessible sites
- [ ] Check for differences in content based on User Agent
- [ ] Perform Web Application Fingerprinting
- [ ] Identify technologies used
- [ ] Identify user roles
- [ ] Identify application entry points
- [ ] Identify client-side code
- [ ] Identify multiple versions/channels (e.g., web, mobile web, mobile app)
- [ ] Identify co-hosted and related applications
- [ ] Identify all hostnames and ports
- [ ] Identify third-party hosted content

Configuration Management

- [ ] Check for commonly used application and administrative URLs
- [ ] Check for old, backup, and unreferenced files
- [ ] Check HTTP methods supported and Cross Site Tracing (XST)
- [ ] Test file extensions handling
- [ ] Test for security HTTP headers (e.g., CSP, X-Frame-Options, HSTS)
- [ ] Test for policies (e.g., Flash, Silverlight, robots)
- [ ] Test for non-production data in live environment
- [ ] Check for sensitive data in client-side code (e.g., API keys, credentials)

Secure Transmission

- [ ] Check SSL Version, Algorithms, Key length
- [ ] Check for Digital Certificate Validity

- [ ] Check credentials only delivered over HTTPS
- [ ] Ensure the login form is delivered over HTTPS
- [ ] Ensure session tokens are only delivered over HTTPS
- [ ] Check if HTTP Strict Transport Security (HSTS) is in use

Authentication

- [ ] Test for user enumeration
- [ ] Test for authentication bypass
- [ ] Test for brute force protection
- [ ] Test password quality rules
- [ ] Test "remember me" functionality
- [ ] Test for autocomplete on password forms
- [ ] Test password reset and/or recovery
- [ ] Test password change process
- [ ] Test CAPTCHA
- [ ] Test multi-factor authentication
- [ ] Test for logout functionality
- [ ] Test cache management on HTTP (e.g., Pragma, Expires, Max-age)
- [ ] Test for default logins
- [ ] Test for user-accessible authentication history

Session Management

- [ ] Check session management methods (e.g., tokens in cookies, URL)
- [ ] Check session tokens for cookie flags (httpOnly and secure)
- [ ] Check session cookie scope (path and domain)
- [ ] Check session cookie duration (expires and max-age)
- [ ] Test session termination after logout or timeout
- [ ] Test for multiple simultaneous sessions
- [ ] Test session cookies for randomness
- [ ] Confirm new session tokens are issued after login, role change, and logout

Authorization

- [ ] Test for path traversal
- [ ] Test for authorization schema bypass
- [ ] Test for vertical and horizontal access control issues (Privilege Escalation)
- [ ] Test for missing authorization

Data Validation

- [ ] Test for Cross-Site Scripting (XSS)
- [ ] Test for SQL Injection
- [ ] Test for LDAP Injection
- [ ] Test for Code Injection
- [ ] Test for Local File Inclusion (LFI)
- [ ] Test for Remote File Inclusion (RFI)
- [ ] Test for NoSQL Injection
- [ ] Test for HTTP parameter pollution
- [ ] Test for auto-binding and mass assignment vulnerabilities

Denial of Service (DoS)

- [ ] Test for anti-automation mechanisms
- [ ] Test for account lockout
- [ ] Test for HTTP protocol DoS
- [ ] Test for SQL wildcard DoS

Business Logic

- [ ] Test for feature misuse
- [ ] Test for lack of non-repudiation
- [ ] Test for trust relationships
- [ ] Test for integrity of data
- [ ] Test segregation of duties

Cryptography

- [ ] Check if sensitive data is encrypted
- [ ] Test for weak or improper encryption algorithms
- [ ] Test for proper use of salting
- [ ] Check for random number generation flaws

Risky Functionality - File Uploads

- [ ] Test acceptable file types (whitelisting)
- [ ] Test file size limits, upload frequency, and total file counts
- [ ] Test file contents to ensure they match the defined file type
- [ ] Test anti-virus scanning on uploads

- [ ] Test for unsafe filenames sanitization
- [ ] Ensure uploaded files are not accessible in the web root

Risky Functionality - Card Payment

- [ ] Test for known vulnerabilities in Web Server and Web Application
- [ ] Test for default or guessable passwords
- [ ] Test for Injection vulnerabilities
- [ ] Test for Buffer Overflows
- [ ] Test for Insecure Cryptographic Storage
- [ ] Test for Insufficient Transport Layer Protection

HTML5

- [ ] Test Web Messaging
- [ ] Test for Web Storage SQL Injection
- [ ] Check CORS implementation
- [ ] Check Offline Web Application