PEN Consultants

Web App/API Penetration Testing Coverage - Comparison

DISCLAIMER: The following is an approximation of coverage for each tier. Exact tests are chosen based on technologies being used, the OWASP top-10, client's risk concerns, current attacker trends, dynamic results of previous testing, etc.

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
[Sub]domain Takeover	1) Full Coverage	1) Full Coverage
Account Enumeration	1) Full Coverage	1) Full Coverage
Blocks	1) Full Coverage	1) Full Coverage
MFA	1) Full Coverage	1) Full Coverage
Port scans	1) Full Coverage	1) Full Coverage
Service Enumeration	1) Full Coverage	1) Full Coverage
Verify Accesses	1) Full Coverage	1) Full Coverage
Verify Scope	1) Full Coverage	1) Full Coverage
Vulnerability Analysis	1) Full Coverage	1) Full Coverage
Vulnerability Scanning (Web)	1) Full Coverage	1) Full Coverage
Account Permissions	2) Partial Coverage	1) Full Coverage
Account Suspension	2) Partial Coverage	1) Full Coverage
Alternative channels	2) Partial Coverage	1) Full Coverage
Application Configuration	2) Partial Coverage	1) Full Coverage
Authentication	2) Partial Coverage	1) Full Coverage
Browser Storage	2) Partial Coverage	1) Full Coverage
Brute Force	2) Partial Coverage	1) Full Coverage
Cache weakness	2) Partial Coverage	1) Full Coverage
Ciphers	2) Partial Coverage	1) Full Coverage
Code Injection	2) Partial Coverage	1) Full Coverage
Command Injection	2) Partial Coverage	1) Full Coverage
Cookies	2) Partial Coverage	1) Full Coverage
Cross domain policy	2) Partial Coverage	1) Full Coverage
Cross Origin Resource Sharing	2) Partial Coverage	1) Full Coverage
Cross Site Scripting (XSS)	2) Partial Coverage	1) Full Coverage
Cryptography	2) Partial Coverage	1) Full Coverage
Default Credentials	2) Partial Coverage	1) Full Coverage
Detect & Respond	2) Partial Coverage	1) Full Coverage
Direct object reference	2) Partial Coverage	1) Full Coverage
Directory traversal	2) Partial Coverage	1) Full Coverage
DNS	2) Partial Coverage	1) Full Coverage
Encryption	2) Partial Coverage	1) Full Coverage
Enumeration	2) Partial Coverage	1) Full Coverage
Error Codes	2) Partial Coverage	1) Full Coverage
Error Handling	2) Partial Coverage	1) Full Coverage
Expression Language Injection	2) Partial Coverage	1) Full Coverage
External service interaction	2) Partial Coverage	1) Full Coverage
Familiarization	2) Partial Coverage	1) Full Coverage
File Extensions	2) Partial Coverage	1) Full Coverage
File inclusion	2) Partial Coverage	1) Full Coverage
Fingerprinting	2) Partial Coverage	1) Full Coverage
Forged Requests	2) Partial Coverage	1) Full Coverage
Format string	2) Partial Coverage	1) Full Coverage
Guessable User Account	2) Partial Coverage	1) Full Coverage

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
Hidden folders/files	2) Partial Coverage	1) Full Coverage
Host Header Injection	2) Partial Coverage	1) Full Coverage
HTML Injection	2) Partial Coverage	1) Full Coverage
HTTP Methods	2) Partial Coverage	1) Full Coverage
HTTP Parameter pollution	2) Partial Coverage	1) Full Coverage
Insecure Deserialization	2) Partial Coverage	1) Full Coverage
Integrity Checks	2) Partial Coverage	1) Full Coverage
JavaScript	2) Partial Coverage	1) Full Coverage
JSON Web Tokens (JWT)	2) Partial Coverage	1) Full Coverage
Local File Inclusion	2) Partial Coverage	1) Full Coverage
Metafiles	2) Partial Coverage	1) Full Coverage
OAuth	2) Partial Coverage	1) Full Coverage
Open Directory Browsing	2) Partial Coverage	1) Full Coverage
ORM Injection	2) Partial Coverage	1) Full Coverage
Padding Oracle	2) Partial Coverage	1) Full Coverage
Password policy	2) Partial Coverage	1) Full Coverage
Penetration	2) Partial Coverage	1) Full Coverage
Public Exploits	2) Partial Coverage	1) Full Coverage
Redirects	2) Partial Coverage	1) Full Coverage
Remote File Inclusion	2) Partial Coverage	1) Full Coverage
REST	2) Partial Coverage	1) Full Coverage
Reverse Tabnabbing	2) Partial Coverage	1) Full Coverage
SAML	2) Partial Coverage	1) Full Coverage
Server Side Template Injection	2) Partial Coverage	1) Full Coverage
Session Cookie attacks	2) Partial Coverage	1) Full Coverage
Session Fixation	2) Partial Coverage	1) Full Coverage
Session Hijacking	2) Partial Coverage	1) Full Coverage
Session Management	2) Partial Coverage	1) Full Coverage
Session puzzling	2) Partial Coverage	1) Full Coverage
Shared Web Hosting	2) Partial Coverage	1) Full Coverage
SQL Injection	2) Partial Coverage	1) Full Coverage
SSI Injection	2) Partial Coverage	1) Full Coverage
SSL/TLS	2) Partial Coverage	1) Full Coverage
SSRF	2) Partial Coverage	1) Full Coverage
Stack Traces	2) Partial Coverage	1) Full Coverage
Unencrypted channels	2) Partial Coverage	1) Full Coverage
URL Redirect	2) Partial Coverage	1) Full Coverage
User enumeration	2) Partial Coverage	1) Full Coverage
User-agent testing	2) Partial Coverage	1) Full Coverage
VDP & Bug Bounty	2) Partial Coverage	1) Full Coverage
Verbose messages	2) Partial Coverage	1) Full Coverage
WAF	2) Partial Coverage	1) Full Coverage
Wordpress	2) Partial Coverage	1) Full Coverage
XML Injection	2) Partial Coverage	1) Full Coverage
Xpath Injection	2) Partial Coverage	1) Full Coverage
Authentication History	3) Coverage if time permits	1) Full Coverage
Authentication Notifications	3) Coverage if time permits	1) Full Coverage
Business impact attacks	3) Coverage if time permits	1) Full Coverage
Bypassing authentication	3) Coverage if time permits	1) Full Coverage
Clickjacking	3) Coverage if time permits	1) Full Coverage
Client-Side Resource Manipulation	3) Coverage if time permits	1) Full Coverage
Email Verification	3) Coverage if time permits	1) Full Coverage
Entry points	3) Coverage if time permits	1) Full Coverage

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
Execution paths	3) Coverage if time permits	1) Full Coverage
File Uploads	3) Coverage if time permits	1) Full Coverage
HSTS	3) Coverage if time permits	1) Full Coverage
HTTP headers	3) Coverage if time permits	1) Full Coverage
HTTP Splitting/ Smuggling	3) Coverage if time permits	1) Full Coverage
HTTP Verb Tampering	3) Coverage if time permits	1) Full Coverage
Input Encoding	3) Coverage if time permits	1) Full Coverage
Java Remote Method Invocation	3) Coverage if time permits	1) Full Coverage
Lock outs	3) Coverage if time permits	1) Full Coverage
Logout functionality	3) Coverage if time permits	1) Full Coverage
Mass Assignment / Auto-Binding	3) Coverage if time permits	1) Full Coverage
Open Mail Relay	3) Coverage if time permits	1) Full Coverage
Password change change/reset	3) Coverage if time permits	1) Full Coverage
Payment Functionality	3) Coverage if time permits	1) Full Coverage
Privilege Escalation	3) Coverage if time permits	1) Full Coverage
Provisioning Analysis	3) Coverage if time permits	1) Full Coverage
Rate Limit Email	3) Coverage if time permits	1) Full Coverage
Registration Analysis	3) Coverage if time permits	1) Full Coverage
Remember password	3) Coverage if time permits	1) Full Coverage
Role Analysis	3) Coverage if time permits	1) Full Coverage
Security question/answer	3) Coverage if time permits	1) Full Coverage
Session Control	3) Coverage if time permits	1) Full Coverage
Session timeout	3) Coverage if time permits	1) Full Coverage
Session Variables	3) Coverage if time permits	1) Full Coverage
Threat Modeling	3) Coverage if time permits	1) Full Coverage
User permissions	3) Coverage if time permits	1) Full Coverage
Username policy	3) Coverage if time permits	1) Full Coverage
Username Predictability	3) Coverage if time permits	1) Full Coverage
Vulnerability Scanning (Network)	3) Coverage if time permits	1) Full Coverage
Webhooks	3) Coverage if time permits	1) Full Coverage
Business Logic Validation	4) No Coverage	1) Full Coverage
Bypassing authorization	4) No Coverage	1) Full Coverage
Certificate transparency searches	4) No Coverage	1) Full Coverage
Cross Site Flashing	4) No Coverage	1) Full Coverage
Cross Site Request Forgery (CSRF)	4) No Coverage	1) Full Coverage
Cross Site Script Inclusion	4) No Coverage	1) Full Coverage
CSS Injection	4) No Coverage	1) Full Coverage
File Permissions	4) No Coverage	1) Full Coverage
Fuzzing	4) No Coverage	1) Full Coverage
IMAP/ SMTP Injection	4) No Coverage	1) Full Coverage
LDAP Injection	4) No Coverage	1) Full Coverage
LLM / AI	4) No Coverage	1) Full Coverage
MiTM	4) No Coverage	1) Full Coverage
Multiple Password Array	4) No Coverage	1) Full Coverage
Resumption Process	4) No Coverage	1) Full Coverage
Salting	4) No Coverage	1) Full Coverage
SMTP	4) No Coverage	1) Full Coverage
Unreferenced Files	4) No Coverage	1) Full Coverage
Attacking the User	2) Partial Coverage	2) Partial Coverage
Client Side	2) Partial Coverage	2) Partial Coverage
Cloud	2) Partial Coverage	2) Partial Coverage
Content Security Policy (CSP)	2) Partial Coverage	2) Partial Coverage
3rd Party Auth+Sessions	3) Coverage if time permits	2) Partial Coverage

Testing Category	Standard Testing / Prioritized	Premium Testing / Full Coverage
Admin Interfaces	3) Coverage if time permits	2) Partial Coverage
Architecture testing	3) Coverage if time permits	2) Partial Coverage
Backup Files	3) Coverage if time permits	2) Partial Coverage
Data Handling	3) Coverage if time permits	2) Partial Coverage
File Types	3) Coverage if time permits	2) Partial Coverage
Function Limits	3) Coverage if time permits	2) Partial Coverage
Infrastructure Testing	3) Coverage if time permits	2) Partial Coverage
Network Configuration	3) Coverage if time permits	2) Partial Coverage
Network related vulnerabilities	3) Coverage if time permits	2) Partial Coverage
Process Timing	3) Coverage if time permits	2) Partial Coverage
Stack overflow	3) Coverage if time permits	2) Partial Coverage
Third-Party Software	3) Coverage if time permits	2) Partial Coverage
Token Stealing and Reuse	3) Coverage if time permits	2) Partial Coverage
Web Messaging	3) Coverage if time permits	2) Partial Coverage
WebSockets	3) Coverage if time permits	2) Partial Coverage
Buffer overflow	4) No Coverage	2) Partial Coverage
Comments	4) No Coverage	2) Partial Coverage
Contact Form	4) No Coverage	2) Partial Coverage
DoS	4) No Coverage	2) Partial Coverage
Heap overflow	4) No Coverage	2) Partial Coverage
OSINT	4) No Coverage	2) Partial Coverage
Reconnaissance	4) No Coverage	2) Partial Coverage
Source Code Analysis	4) No Coverage	2) Partial Coverage
Client-Side Software	4) No Coverage	3) Coverage if time permits
Containerization	4) No Coverage	3) Coverage if time permits
Defense Evasion	4) No Coverage	3) Coverage if time permits
Device Search Engines	4) No Coverage	3) Coverage if time permits
Reverse engineering	4) No Coverage	3) Coverage if time permits
Services on the endpoint	4) No Coverage	3) Coverage if time permits
Sessions Across Apps	4) No Coverage	3) Coverage if time permits
Source code repos	4) No Coverage	3) Coverage if time permits
Stored passwords	4) No Coverage	3) Coverage if time permits