# I. Server-Side Vulnerability Testing Checklist

(Server-side vulnerabilities affect databases, files, authentication, logic, servers.)

| # | Vulnerability | How to Test | Tools to Use |
|---|---|---|---|
| 1 | SQL Injection (SQLi) | Inject payloads in URL, forms, headers | sqlmap, Burp Suite, Manual |
| 2 | Authentication Bypass | Try default creds, weak creds, brute-force | hydra, Burp Intruder, Manual |
| 3 | Authorization Bypass / IDOR | Change object IDs in URL or requests | Burp Repeater (Manual) |
| 4 | Remote Code Execution (RCE) | Inject OS commands | Manual, Burp Suite, commix |
| 5 | Server-Side Request Forgery (SSRF) | Input internal URLs, IPs, etc. | Burp Collaborator, Manual |
| 6 | Directory Traversal | Access ../../etc/passwd | dirsearch, Manual |
| 7 | File Upload Vulnerability | Upload PHP/JSP shells, bypass extensions | Manual with Burp |
| 8 | Command Injection | Try command separators (;, &&) | Manual, Burp Suite |
| 9 | Local File Inclusion (LFI) | Include local files via parameters | Manual testing, Burp Suite |
| 10 | XML External Entity (XXE) | Send crafted XML data | XXEinjector, Burp Suite |
| 11 | Broken Access Control | Access admin pages, APIs without permission | Manual, Burp Suite |
| 12 | Server Misconfigurations | Check HTTP headers, default pages, errors | nikto, testssl.sh, nmap |
| 13 | Sensitive Data Exposure | Find API keys, passwords, backups | gau, waybackurls, Manual |
| 14 | Insecure Deserialization | Send crafted objects (advanced) | Manual, Burp Suite extensions |

## II. Client-Side Vulnerability Testing Checklist

(Client-side vulnerabilities affect the browser, sessions, cookies, frontend.)

| # | Vulnerability | How to Test | Tools to Use |
|---|---|---|---|
| 1 | Reflected XSS | Inject <script>alert(1)</script> in URL, inputs | XSStrike, Dalfox, Burp |
| 2 | Stored XSS | Inject payloads into comments, profiles | Dalfox, Manual |
| 3 | DOM-Based XSS | Find unsanitized location.href, document.write usage | DOMInvader, Manual JS analysis |
| 4 | Cross-Site Request Forgery (CSRF) | Submit POST requests without CSRF token | Burp Suite, Manual POC generator |
| 5 | Clickjacking | Try loading site in <iframe> | Manual, X-Frame-Options header checker |
| 6 | Open Redirect | Change redirect URLs to external sites | Manual testing |
| 7 | JavaScript Sensitive Data | Search for secrets in JS files | LinkFinder, JSParser |
| 8 | CORS Misconfiguration | Try sending cross-origin requests | corsy, Burp Suite |
| 9 | HTML Injection | Inject HTML tags like <h1>hacked</h1> | Manual, Burp Suite |
| 10 | WebSocket Security | Inspect WebSocket messages | Burp Suite extensions (WebSocket Editor) |
| 11 | CSP (Content Security Policy) Issues | Missing or weak CSP header | csp-evaluator, browser devtools |
| 12 | Service Workers Vulnerabilities | Check registration scope, cache control | Manual, Chrome Devtools |
| 13 | Password Autofill Vulnerabilities | Check login forms' attributes (autocomplete=off missing) | Manual |
| 14 | Mixed Content Issues (HTTPS) | Find HTTP resources on HTTPS page | Chrome Devtools security tab |

## Summary: Tools for Server-Side + Client-Side

| Purpose | Tools |
|---|---|
| Manual Request Editing | **Burp Suite (Professional or Community)** |
| SQL Injection | **sqlmap**, Burp |
| XSS Testing | **Dalfox**, **XSStrike**, Manual |
| CSRF | Burp, CSRF POC Generator |
| Subdomain Discovery | **subfinder**, **amass** |
| JS File Analysis | **LinkFinder**, **JSParser** |
| CORS Scanner | **corsy** |
| Directory Brute Forcing | **dirsearch**, **ffuf** |
| WAF Detection | **wafw00f** |
| Server Misconfiguration | **nikto**, **nmap**, **testssl.sh** |
| Recon Automation | **gau**, **waybackurls** |
| Screenshot Websites | **aquatone**, **gowitness** |
| Vulnerability Templates Scan | **nuclei** |
| XML Injection | **XXEinjector** |

## Testing Strategy:

- Reconnaissance (find endpoints, files, technologies)
- Client-side testing (XSS, CSRF, Clickjacking)
- Server-side testing (SQLi, RCE, SSRF, IDOR)
- Manual Business Logic testing (payment, order flows)
- Sensitive data search (JS files, backup files, tokens)