🛡️ Advanced Web Application Pentesting Checklist

✅ 1. Advanced Recon & Fingerprinting

- [ ] Use `Wappalyzer`, `BuiltWith`, `WhatWeb` to identify technologies
- [ ] Identify 3rd party libraries and look for known CVEs
- [ ] Analyze JS files for sensitive data (keys, endpoints)

✅ 2. Advanced Injection Attacks

- [ ] Time-based blind SQLi
- [ ] Second-order SQLi
- [ ] NoSQL Injection (MongoDB, etc.)
- [ ] XPath Injection
- [ ] SSRF (Server-Side Request Forgery)
- [ ] XXE (XML External Entity)

✅ 3. Cross-Site Scripting (XSS) Advanced

- [ ] DOM-based XSS
- [ ] Bypass WAF and filters using payload obfuscation
- [ ] Use different contexts: `<script>`, attributes, JS event handlers

✅ 4. CSRF & Business Logic Testing

- [ ] Check CSRF protections (token validation, same-origin policy)
- [ ] Perform logic abuse (e.g., coupon reuse, price modification)
- [ ] Abuse workflows (e.g., password reset without email verification)

✅ 5. Authentication & Token Handling

- [ ] JWT token manipulation (e.g., change algorithm to `none`)

[ ] Replay attacks with tokens

[ ] OAuth and OpenID misconfigurations

✅ 6. Privilege Escalation & Access Control

[ ] Tamper with user roles in cookies or tokens

[ ] Modify hidden fields to access restricted functions

[ ] Access internal APIs through a public interface

✅ 7. File Upload & RCE

[ ] Bypass MIME type/content-type validation

[ ] Upload web shells and test for RCE

[ ] Try PHP filters and wrappers to bypass restrictions

✅ 8. Client-Side Security

[ ] Test for insecure use of `localStorage`, `sessionStorage`

[ ] Analyze client-side logic in JS files

[ ] CSP (Content Security Policy) misconfigurations

✅ 9. WebSockets & APIs

[ ] Test WebSockets for input validation

[ ] Enumerate and fuzz API endpoints

[ ] Test for GraphQL introspection, mutations

✅ 10. Tools to Use

[ ] Recon: Amass, Sublist3r, Nmap

[ ] Scanning: Burp Suite Pro, OWASP ZAP, Nikto

[ ] Fuzzing: ffuf, wfuzz

[ ] Exploitation: SQLmap, XSStrike, JWT Cracker