🔰 Beginner Web Application Pentesting Checklist

These tasks are ideal for someone just starting out in web application security testing.

✅ 1. Information Gathering

- [ ] Identify the domain/IP and subdomains
- [ ] Check for HTTP/HTTPS and security headers
- [ ] Identify web server and technologies used (e.g., Apache, Nginx, PHP, Node.js)
- [ ] Enumerate directories and files using tools like `dirb`, `gobuster`, `feroxbuster`
- [ ] Identify CMS (WordPress, Joomla, etc.)

✅ 2. Authentication Testing

- [ ] Test for default credentials
- [ ] Brute-force login page (use rate limiting and account lockout detection)
- [ ] Check for username enumeration
- [ ] Check password reset functionalities

✅ 3. Session Management

- [ ] Inspect session cookies (flags: `HttpOnly`, `Secure`, `SameSite`)
- [ ] Test for session fixation
- [ ] Check if sessions expire after logout or inactivity

✅ 4. Input Validation & Injection

- [ ] Test input fields for:
    - { } SQL Injection (use `'`, `OR 1=1`, etc.)
    - { } Command Injection
    - { } HTML Injection

[ ] Check for reflected and stored XSS

[ ] Test URL parameters for tampering

✅ 5. File Upload Testing

[ ] Try uploading:

{ } Executable files

{ } PHP/ASP shells

{ } Scripts disguised with alternate extensions (`.php.jpg`)

[ ] Bypass file validation checks

✅ 6. Authorization Testing

[ ] Test Insecure Direct Object References (IDOR)

[ ] Check for vertical privilege escalation (user → admin)

[ ] Check for horizontal privilege escalation (user1 accessing user2's data)

✅ 7. Security Misconfigurations

[ ] Test for directory listing

[ ] Check for exposed `.git`, `.env`, `backup` files

[ ] Default error messages revealing technology/version