Checklist Pentest Website Lengkap

Dibuat pada: 19 May 2026

Dokumen ini berisi checklist lengkap pengujian keamanan website berdasarkan praktik umum penetration testing dan referensi OWASP. Checklist ini cocok digunakan untuk aplikasi Laravel, Next.js, React, Node.js, PHP, maupun framework web lainnya.

1. Reconnaissance & Information Gathering

- ■ Identifikasi teknologi website (PHP, Laravel, Next.js, Nginx, Apache, dll)
- ■ Enumerasi subdomain
- ■ Cek DNS record
- ■ Cek exposed port
- ■ Cek file robots.txt
- ■ Cek sitemap.xml
- ■ Identifikasi framework dan library
- ■ Cek metadata file publik
- ■ Identifikasi admin panel
- ■ Cek backup file yang terekspos

2. Authentication Testing

- ■ Tes brute force login
- ■ Tes default credential
- ■ Tes bypass login
- ■ Tes session fixation
- ■ Tes remember me token
- ■ Tes multi-factor authentication
- ■ Tes reset password
- ■ Tes lockout mechanism
- ■ Tes logout invalidation
- ■ Tes cookie security

3. Authorization Testing

- ■ Tes akses horizontal
- ■ Tes akses vertikal

- ■ Tes IDOR
- ■ Tes akses endpoint tanpa login
- ■ Tes privilege escalation
- ■ Tes role validation
- ■ Tes akses file sensitif
- ■ Tes API authorization

4. Input Validation Testing

- ■ Tes SQL Injection
- ■ Tes XSS reflected
- ■ Tes XSS stored
- ■ Tes DOM XSS
- ■ Tes Command Injection
- ■ Tes SSTI
- ■ Tes LDAP Injection
- ■ Tes XML Injection
- ■ Tes NoSQL Injection
- ■ Tes path traversal

5. File Upload Testing

- ■ Tes upload PHP shell
- ■ Tes double extension
- ■ Tes MIME type bypass
- ■ Tes executable upload
- ■ Tes upload oversized file
- ■ Tes file overwrite
- ■ Tes upload SVG berbahaya
- ■ Tes upload ZIP berbahaya

6. API Security Testing

- ■ Tes JWT validation
- ■ Tes API rate limit
- ■ Tes exposed API key
- ■ Tes mass assignment
- ■ Tes debug endpoint
- ■ Tes hidden endpoint

- ■ Tes CORS misconfiguration
- ■ Tes GraphQL introspection

7. Session Management

- ■ Tes session timeout
- ■ Tes cookie HttpOnly
- ■ Tes Secure flag
- ■ Tes SameSite cookie
- ■ Tes session hijacking
- ■ Tes token reuse
- ■ Tes token predictability

8. Server & Configuration Testing

- ■ Pastikan debug mode OFF
- ■ Tes akses .env
- ■ Tes akses .git
- ■ Tes directory listing
- ■ Tes phpinfo exposure
- ■ Tes backup exposure
- ■ Tes SSL/TLS configuration
- ■ Tes HTTP security header

9. Dependency & Package Audit

- ■ Jalankan npm audit
- ■ Jalankan composer audit
- ■ Cek CVE dependency
- ■ Cek package deprecated
- ■ Audit third-party library

10. Logging & Monitoring

- ■ Cek sensitive data di log
- ■ Tes audit logging
- ■ Tes alert monitoring
- ■ Tes failed login logging
- ■ Tes API abuse logging

11. Hardening Checklist

- ■ Aktifkan HTTPS
- ■ Gunakan CSP
- ■ Gunakan HSTS
- ■ Matikan server signature
- ■ Batasi upload file
- ■ Batasi rate request
- ■ Gunakan WAF
- ■ Aktifkan backup rutin

Klasifikasi Severity

Severity	Deskripsi
Critical	Dapat menyebabkan compromise penuh sistem
High	Dapat menyebabkan akses tidak sah atau kebocoran data
Medium	Memiliki dampak sedang terhadap keamanan
Low	Dampak kecil namun tetap perlu diperbaiki
Info	Temuan informasional

Gunakan checklist ini secara legal dan hanya terhadap sistem yang Anda miliki atau memiliki izin tertulis untuk diuji.