# Bank Soal Lengkap: Keamanan Web & Aplikasi Mobile

Dokumen ini merupakan gabungan dari seluruh kuis materi keamanan web, mencakup konsep dasar, autentikasi, kerentanan, hingga infrastruktur keamanan.

## 🛡️ Konsep Dasar & Infrastruktur

### 1. Apa yang dimaksud dengan webification?

Jawaban:

Mengubah aplikasi native menjadi aplikasi web progresif (PWA) / Membuat aplikasi dapat diakses melalui browser.

Penjelasan:

Webification adalah proses membawa fitur-fitur yang biasanya ada di aplikasi native (mobile/desktop) ke dalam ekosistem web, atau mengubah sistem legacy menjadi aplikasi berbasis web yang dapat diakses lintas platform tanpa instalasi khusus.

### 2. Apa yang dimaksud dengan "appification" dalam konteks keamanan web?

Jawaban:

Mengubah aplikasi web menjadi aplikasi native mobile.

Penjelasan:

Appification merujuk pada tren membungkus (wrapping) aplikasi web atau situs web ke dalam wadah aplikasi native (seperti menggunakan WebView atau PWA) agar dapat didistribusikan melalui toko aplikasi dan mengakses fitur perangkat mobile.

### 3. Apa fungsi dari load balancer dalam keamanan web?

Jawaban:

Mendistribusikan lalu lintas jaringan secara merata ke beberapa server untuk meningkatkan kinerja dan ketahanan.

Penjelasan:

Dalam konteks keamanan, load balancer mendukung pilar Availability (Ketersediaan). Alat ini membantu sistem bertahan dari lonjakan trafik tiba-tiba, termasuk serangan DDoS ringan, sehingga layanan tetap bisa diakses.

### 4. Bagaimana firewall melindungi web dari ancaman eksternal?

Jawaban:

Dengan mendeteksi dan memblokir lalu lintas yang tidak sah atau berbahaya.

Penjelasan:

Firewall (termasuk WAF/Web Application Firewall) memfilter lalu lintas jaringan dan memblokir serangan umum seperti SQL Injection, XSS, bruteforce, dan DDoS ringan.

### 5. Pembaruan perangkat lunak yang sering penting untuk keamanan karena...

Jawaban:

Memperbaiki kerentanan yang diketahui dan meningkatkan keamanan.

Penjelasan:

Tujuan utama pembaruan keamanan (security patch) adalah menambal celah keamanan (vulnerabilities) yang ditemukan sejak versi sebelumnya. Mengabaikan ini membuat sistem rentan terhadap eksploitasi celah lama (known vulnerabilities).

### 6. Apa itu database dalam konteks keamanan aplikasi web?

Jawaban:

Sistem yang menyimpan dan mengelola data aplikasi dalam bentuk terstruktur.

Penjelasan:

Database adalah aset kritis karena menyimpan data sensitif pengguna (kredensial, info pribadi, transaksi) yang harus dilindungi secara ketat dari serangan seperti SQL Injection.

## 🔐 Autentikasi & Otorisasi

### 7. Apa tujuan dari OAuth?

Jawaban:

Untuk mengautentikasi pengguna tanpa memerlukan kata sandi.

Penjelasan:

OAuth adalah protokol authorization yang memungkinkan pengguna login menggunakan akun pihak ketiga (Google, Facebook) tanpa menyerahkan kata sandi langsung ke aplikasi tersebut.

### 8. Mana dari berikut ini adalah metode autentikasi HTTP?

Jawaban:

HTTP Basic Authentication.

Penjelasan:

HTTP Basic Authentication adalah mekanisme bawaan protokol HTTP di mana klien mengirim username dan password (biasanya dienkode Base64) dalam header. (OAuth 2.0 adalah framework otorisasi, bukan metode auth HTTP dasar).

### 9. Contoh HTTP Authentication lainnya?

Jawaban:

Menggunakan kunci API (API Key) dalam URL untuk mengakses sumber daya.

Penjelasan:

Selain Basic Auth, HTTP Authentication juga mencakup mekanisme seperti Bearer Token dan penggunaan API Key.

### 10. Jenis kontrol akses ketika aplikasi meminta izin kamera/lokasi?

Jawaban:

Kontrol akses berbasis dialog izin (Consent-based access control).

Penjelasan:

Aplikasi modern meminta akses ke sensor perangkat keras melalui dialog permission yang harus disetujui pengguna secara eksplisit.

### 11. Apa itu shoulder surfing?

Jawaban:

Proses mencuri kata sandi dengan mengamati seseorang yang memasukkannya (mengintip dari atas bahu).

Penjelasan:

Ini adalah teknik rekayasa sosial fisik di mana penyerang melihat langsung layar atau keyboard korban untuk mencuri PIN atau kata sandi.

### 12. Teknik yang sering digunakan dalam phishing adalah…

Jawaban:

Mengirim email palsu dengan tautan berbahaya untuk mencuri kredensial.

Penjelasan:

Phishing menipu pengguna agar mengklik tautan palsu yang menyerupai situs asli untuk mencuri data sensitif.

### 13. Pertahanan paling efektif terhadap serangan phishing?

Jawaban:

Menggunakan otentikasi multi-faktor (MFA).

Penjelasan:

Meskipun password tercuri lewat phishing, akun tetap aman karena penyerang tidak memiliki faktor kedua (seperti kode OTP atau biometrik).

## 🌐 Keamanan Browser & Penyimpanan Klien

### 14. Bagaimana cara kerja client-side storage di browser web?

Jawaban:

Dengan menyimpan data terkait sesi secara lokal di perangkat pengguna.

Penjelasan:

Penyimpanan ini (Cookies, LocalStorage) menyimpan data langsung di browser pengguna, bukan di server, untuk keperluan cache atau sesi.

### 15. Penyimpanan sisi klien umumnya digunakan untuk apa?

Jawaban:

Menyimpan pengaturan (preferensi) dan data sesi pengguna.

Penjelasan:

Ideal untuk data non-sensitif seperti tema (gelap/terang), bahasa, atau token sesi. Tidak disarankan untuk menyimpan data sensitif tanpa enkripsi.

### 16. Langkah untuk meningkatkan keamanan client-side storage?

**Jawaban:**

1. Mengenkripsi data sensitif sebelum disimpan.
2. Menandatangani data secara kriptografis untuk menjamin integritas.  
   Penjelasan:  
   Data di browser mudah diakses pengguna, jadi harus dienkripsi agar tidak terbaca dan ditandatangani (signed) agar tidak bisa dimodifikasi sembarangan.

### 17. Apa yang benar tentang cookie dalam keamanan web?

Jawaban:

Cookie dapat digunakan untuk melacak pengguna di berbagai situs web.

Penjelasan:

Risiko privasi utama cookie (third-party cookies) adalah pelacakan (tracking) aktivitas pengguna lintas situs untuk keperluan iklan/profiling.

### 18. Same Origin Policy (SOP) digunakan untuk...

Jawaban:

Mencegah skrip dari satu situs mengakses data situs lain.

Penjelasan:

SOP membatasi interaksi antar-situs yang berbeda asal (origin), mencegah situs jahat membaca data sensitif dari situs lain yang sedang dibuka pengguna.

### 19. CSP (Content Security Policy) digunakan untuk mencegah serangan seperti…

Jawaban:

Cross-Site Scripting (XSS) dan Injection code.

Penjelasan:

CSP memungkinkan pemilik situs mengontrol sumber mana saja yang boleh memuat skrip, memitigasi risiko eksekusi skrip berbahaya.

## 🦠 Kerentanan & Serangan (Vulnerabilities)

### 20. Apa kerentanannya jika input pengguna tidak dikontrol (uncontrolled input)?

Jawaban:

SQL Injection.

Penjelasan:

Kegagalan memvalidasi input memungkinkan penyerang menyisipkan perintah database berbahaya.

### 21. Cara penting untuk mencegah SQL Injection?

**Jawaban:**

1. Menggunakan *prepared statements* dengan *placeholder*.
2. Melakukan validasi dan sanitasi input.  
   Penjelasan:  
   Prepared statements memisahkan kode SQL dari data, sehingga input pengguna tidak akan dieksekusi sebagai perintah.

### 22. Apa itu Command Injection?

Jawaban:

Teknik menyisipkan perintah sistem operasi berbahaya ke dalam aplikasi.

Penjelasan:

Terjadi jika aplikasi meneruskan input mentah ke shell OS, memungkinkan penyerang menjalankan perintah sistem (seperti cmd.exe atau bash).

### 23. Apa itu Local File Inclusion (LFI)?

Jawaban:

Kerentanan di mana aplikasi mengizinkan penyerang memuat file sistem lokal secara tidak sah.

Penjelasan:

Penyerang bisa memanipulasi path input untuk membaca file sensitif di server (misal: /etc/passwd).

### 24. Manakah langkah aman dalam menangani file yang diunggah pengguna?

**Jawaban:**

1. Menghindari eksekusi langsung file yang diunggah.
2. Memeriksa tipe MIME dan isi file.  
   Penjelasan:  
   File upload harus dicegah agar tidak bisa dieksekusi (cegah webshell) dan harus divalidasi isinya (pastikan benar-benar gambar/dokumen, bukan skrip).

### 25. Apa itu serangan Clickjacking?

Jawaban:

Kerentanan yang membuat pengguna mengklik sesuatu yang berbeda dari yang mereka lihat ("UI Redressing").

Penjelasan:

Penyerang menumpuk lapisan transparan (iframe) di atas situs sah. Pengguna mengira mengklik tombol "Play", padahal mengklik tombol tersembunyi milik penyerang.

## 🔒 Kriptografi & HTTPS

### 26. Fungsi utama sertifikat digital pada HTTPS?

**Jawaban:**

1. Memungkinkan pembentukan kanal komunikasi terenkripsi.
2. Mengautentikasi identitas server kepada klien.  
   Penjelasan:  
   Sertifikat memverifikasi keaslian server dan memungkinkan enkripsi data (SSL/TLS) agar tidak bisa disadap.

### 27. Protokol mana yang digunakan untuk mengamankan komunikasi HTTP menggunakan sertifikat?

Jawaban:

Web PKI (Public Key Infrastructure).

Penjelasan:

Meskipun protokol transport-nya TLS, infrastruktur yang mengatur penerbitan dan validasi sertifikat digital (CA, Public/Private Key) adalah Web PKI.