# Rangkuman Lengkap Quiz Keamanan Perangkat Lunak (M09)

Dokumen ini merupakan gabungan dari 30 soal latihan keamanan perangkat lunak, mencakup topik injeksi, validasi input, manajemen memori, dan kerentanan umum (OWASP/CWE).

## Bagian 1: Dasar Keamanan & Serangan Web

### 1. Cara mencegah serangan Cross-Site Scripting (XSS) yang efektif

**Jawaban Benar:**

* **Melakukan validasi input dari pengguna**
* **Melakukan encoding output sebelum ditampilkan**

Penjelasan:

XSS terjadi ketika skrip berbahaya disisipkan ke dalam halaman web.

* **Validasi Input:** Mencegah karakter berbahaya masuk ke dalam sistem sejak awal.
* **Encoding Output:** Mengubah karakter spesial (seperti < menjadi <) agar browser menerjemahkannya sebagai teks biasa, bukan kode yang bisa dieksekusi. Ini adalah pertahanan utama melawan XSS.

### 2. Modularisasi program membantu...

**Jawaban Benar:**

* **Meningkatkan keamanan dan isolasi komponen**

Penjelasan:

Modularisasi memecah program menjadi bagian-bagian kecil (modul). Jika satu modul diretas atau mengalami error, kerusakan dapat dibatasi hanya pada modul tersebut tanpa menyebar ke seluruh sistem (containment).

### 3. Operasi atomik berarti...

**Jawaban Benar:**

* **Operasi dilakukan tanpa bisa disela**

Penjelasan:

Dalam pemrograman concurrent, operasi atomik berjalan sepenuhnya atau tidak sama sekali. Operasi ini tidak bisa dipotong (interrupted) oleh thread lain, sehingga mencegah kondisi Race Condition.

### 4. Program yang dijalankan dengan hak khusus disebut...

**Jawaban Benar:**

* **Privileged program**

Penjelasan:

Program yang diizinkan berjalan dengan hak akses lebih tinggi (misalnya root/admin) meskipun dijalankan oleh pengguna biasa (contoh: menggunakan SetUID di Linux).

### 5. Jenis serangan injeksi yang umum terjadi pada aplikasi web meliputi...

**Jawaban Benar:**

* **SQL injection**
* **Command injection**

**Penjelasan:**

* **SQL Injection:** Memanipulasi database dengan perintah SQL berbahaya.
* **Command Injection:** Menyisipkan perintah sistem operasi (OS) untuk dieksekusi server.

### 6. Apa fungsi sandbox dalam keamanan program?

**Jawaban Benar:**

* **Membatasi program agar tidak merusak sistem**

Penjelasan:

Sandbox adalah lingkungan terisolasi. Program di dalamnya dibatasi aksesnya (file/memori), sehingga malware di dalam sandbox tidak bisa merusak sistem operasi utama (host).

### 7. Langkah untuk meningkatkan keamanan interaksi program dengan sistem operasi adalah...

**Jawaban Benar:**

* **Menjalankan program dengan hak minimum (least privilege)**
* **Menetapkan PATH dan variabel lingkungan ke nilai aman**
* **Mengabaikan LD\_LIBRARY\_PATH**

Penjelasan:

Membatasi hak akses (least privilege) dan membersihkan variabel lingkungan mencegah serangan seperti DLL Hijacking atau eksekusi library palsu.

### 8. Contoh serangan yang memanfaatkan output program adalah...

**Jawaban Benar:**

* **Cross-Site Scripting (XSS)**

Penjelasan:

XSS terjadi karena aplikasi mengambil data (input) dan menampilkannya kembali (output) ke pengguna lain tanpa filter, sehingga skrip dieksekusi di browser pengguna.

### 9. Program “secure file shredding” digunakan untuk...

**Jawaban Benar:**

* **Menghapus file secara permanen**

Penjelasan:

Secure shredding menimpa (overwrite) lokasi fisik data dengan data acak berkali-kali agar data asli tidak bisa dipulihkan (recovery) dengan software forensik.

### 10. Bug Heartbleed adalah contoh dari...

**Jawaban Benar:**

* **Buffer over-read**

Penjelasan:

Heartbleed menipu server untuk membaca memori lebih banyak dari yang seharusnya (over-read), sehingga data rahasia di memori server ikut terkirim ke penyerang.

## Bagian 2: Pemrograman Aman (Secure Coding) & Kerentanan

### 11. Fungsi C yang aman untuk membuat file sementara adalah...

**Jawaban Benar:**

* **mkstemp()**
* **tmpfile()**

**Penjelasan:**

* mkstemp(): Membuat nama unik dan langsung membuka file (mencegah pembajakan nama file).
* tmpfile(): Membuat file sementara mode biner dan otomatis menghapusnya saat ditutup.
* *Hindari tempnam() karena rentan Race Condition.*

### 12. Pemrograman defensif berarti...

**Jawaban Benar:**

* **Memeriksa dan menangani semua kemungkinan kesalahan**

Penjelasan:

Mengantisipasi masalah dan memastikan software tetap aman (fail-safe) meskipun menerima input tidak valid, bukan berasumsi "semua input aman".

### 13. Encoding karakter penting karena...

**Jawaban Benar:**

* **Mempengaruhi interpretasi simbol**

Penjelasan:

Kesalahan encoding bisa mengubah simbol menjadi karakter acak atau dimanfaatkan peretas untuk menyembunyikan skrip berbahaya (bypass filter).

### 14. Race condition terjadi ketika...

**Jawaban Benar:**

* **Dua proses berjalan bersamaan tanpa sinkronisasi**

Penjelasan:

Terjadi saat perilaku program bergantung pada urutan eksekusi proses yang tidak terkendali, biasanya saat berebut akses data yang sama (shared resource).

### 15. Salah satu langkah penting dari NISTIR 8151 adalah...

**Jawaban Benar:**

* **Mencegah kerentanan sejak awal**

Penjelasan:

Fokus pada pendekatan Secure by Design: mencegah masuknya celah keamanan sejak tahap desain/coding, bukan hanya menambal (patch) di akhir.

### 16. Apa penyebab utama banyak kerentanan dalam keamanan perangkat lunak?

**Jawaban Benar:**

* **Cara penulisan kode yang tidak aman**

Penjelasan:

Akar masalah mayoritas kerentanan (SQLi, XSS, Buffer Overflow) adalah logika kode manusia yang lalai memvalidasi input atau mengelola memori.

### 17. Buffer overflow terjadi ketika...

**Jawaban Benar:**

* **Data yang dimasukkan melebihi kapasitas buffer**

Penjelasan:

Data berlebih "tumpah" ke memori bersebelahan, menyebabkan crash atau eksekusi kode berbahaya.

### 18. Daftar CWE/SANS Top 25 Most Dangerous Software Errors berisi...

**Jawaban Benar:**

* **Kesalahan kode paling berbahaya**

Penjelasan:

Daftar panduan prioritas yang merangkum kelemahan perangkat lunak yang paling sering dieksploitasi dan berdampak parah.

### 19. Fitur sistem operasi yang menyediakan variabel konfigurasi disebut...

**Jawaban Benar:**

* **Environment variable**

Penjelasan:

Nilai dinamis (seperti PATH, USER) yang mempengaruhi proses berjalan. Bisa menjadi vektor serangan jika tidak diamankan.

### 20. Cross-Site Scripting (XSS) menyerang...

**Jawaban Benar:**

* **Pengguna yang melihat output**

Penjelasan:

XSS menargetkan client-side (browser pengguna), bukan server database secara langsung. Tujuannya mencuri cookies/session pengguna.

## Bagian 3: Validasi Lanjut & Manajemen Risiko

### 21. Canonicalization digunakan untuk...

**Jawaban Benar:**

* **Menstandarkan variasi encoding karakter**

Penjelasan:

Proses menyederhanakan data menjadi format standar sebelum validasi. Penting untuk mendeteksi serangan yang disembunyikan lewat encoding aneh (misal: URL encoding berlebih).

### 22. Salah satu kelemahan dalam OWASP Top Ten adalah...

**Jawaban Benar:**

* **Cross-Site Scripting (XSS)**

Penjelasan:

XSS adalah kerentanan klasik yang konsisten masuk dalam daftar risiko keamanan aplikasi web teratas menurut OWASP.

### 23. Contoh hak istimewa berlebihan dapat terjadi pada...

**Jawaban Benar:**

* **Web server dengan hak tulis penuh**

Penjelasan:

Melanggar prinsip Least Privilege. Web server seharusnya hanya perlu hak baca (read). Hak tulis penuh memungkinkan peretas memodifikasi kode situs jika server jebol.

### 24. Kegagalan program untuk memvalidasi output dapat menyebabkan...

**Jawaban Benar:**

* **Serangan terhadap pengguna**

Penjelasan:

Jika output tidak divalidasi/di-encode, skrip jahat dari input penyerang akan terkirim dan dieksekusi di browser pengguna lain (mekanisme XSS).

### 25. Bug Heartbleed disebabkan oleh...

**Jawaban Benar:**

* **Salah menghitung ukuran data yang diminta**

Penjelasan:

Server OpenSSL gagal memverifikasi bahwa jumlah data yang diminta klien sesuai dengan data yang dikirim, menyebabkan server membaca memori berlebih (buffer over-read).

### 26. Salah satu metode pencegahan injeksi adalah...

**Jawaban Benar:**

* **Menghentikan input otomatis ke variabel**

Penjelasan:

Mencegah fitur seperti register\_globals (PHP lama) di mana input URL otomatis jadi variabel program. Variabel harus diinisialisasi secara eksplisit agar tidak bisa ditimpa penyerang.

### 27. Konsep chroot jail digunakan untuk...

**Jawaban Benar:**

* **Membatasi akses program ke bagian tertentu dari sistem file**

Penjelasan:

Mengubah direktori root (/) untuk sebuah proses, sehingga proses tersebut "terpenjara" dan tidak bisa melihat file sistem di luar direktori tersebut.

### 28. Langkah aman dalam validasi input mencakup...

**Jawaban Benar:**

* **Melakukan canonicalization agar data seragam**
* **Menggunakan whitelisting untuk membatasi input**

Penjelasan:

Canonicalization mencegah bypass filter. Whitelisting (hanya terima yang baik) jauh lebih aman daripada Blacklisting (menolak yang jahat).

### 29. Siapa yang bertanggung jawab memastikan keamanan data antarprogram?

**Jawaban Benar:**

* **Programmer dari program baru**

Penjelasan:

Programmer bertanggung jawab memvalidasi dan mengamankan data saat aplikasinya berkomunikasi (API/IPC) dengan program lain, tidak bisa hanya mengandalkan OS/Admin.

### 30. Fungsi tempnam() dianggap tidak aman karena...

**Jawaban Benar:**

* **Dapat ditebak dan disalahgunakan**

Penjelasan:

tempnam() hanya menghasilkan nama file, tidak membukanya secara atomik. Ada jeda waktu (Race Condition) di mana peretas bisa membuat file dengan nama itu sebelum program sempat melakukannya.