Keamanan Siber (CAK3CAB3)
S1 Informatika; 2526-1

TUGAS 1 – Analisis dan Peningkatan Keamanan Program

Dalam tugas ini, mahasiswa akan lebih mendalami dan mengaplikasikan konsep keamanan siber terutama dalam pembuatan perangkat lunak yang aman, dengan cara menganalisis, menguji, dan memperbaiki keamanan sebuah program. Tugas ini terdiri dari beberapa tahap yang terkait dengan aktifitas mengenali celah keamanan dalam sebuah program, melakukan serangan untuk membuktikan kerentanannya, memperbaiki kode program agar lebih aman, dan membuktikan peningkatan keamanan yang dilakukan.

Langkah-langkah tugas:

I. Instalasi program:
   Diberikan sebuah contoh program *Create Read Update Delete* (CRUD) sederhana yang bisa diakses di: https://github.com/aquarink/python-sqlite
   1. *Install* program tersebut di komputer Anda dengan langkah seperti yang tertulis dalam README. Boleh juga jika Anda ingin meng-*install*-nya di *virtual machine* atau *cloud* (dengan penyesuaian seperlunya). Pastikan yang Anda unduh dan install adalah versi terakhirnya.
   2. Baca dan pahami kode program tersebut.

II. Analisis dan peningkatan keamanan program
   a. Identifikasi celah keamanan:
      Anda diminta untuk mendokumentasikan setiap celah keamanan (*vulnerability*) yang ditemukan dalam program. Untuk setiap celah, Anda harus memberikan deskripsi yang jelas, termasuk jenis kerentanannya, dan bagian program mana yang terkait dengan kerentanan tersebut.
   b. Pembuktian dengan melakukan serangan:
      Berdasarkan hasil identifikasi terhadap celah keamanan, Anda diminta untuk melakukan serangan terhadap program tersebut. Setiap serangan yang dilakukan harus dicatat secara terperinci, meliputi metode serangan, hasil serangan, dan bagaimana itu membuktikan bahwa program tidak aman.
   c. Peningkatan keamanan program:
      Pada tahap ini, Anda diminta untuk memperbaiki program yang diberikan agar lebih aman. Setiap kerentanan yang ditemukan pada langkah analisis harus diperbaiki. Pastikan perbaikan yang dilakukan terdokumentasi dengan baik, termasuk alasan pemilihan teknik pengamanan, dan bagaimana setiap perbaikan menangani celah keamanan yang ada.
   d. Pengujian keamanan setelah perbaikan:
      Setelah program diperbaiki, Anda harus melakukan serangan yang sama seperti pada tahap (II.b) untuk membuktikan bahwa program kini lebih aman. Jika serangan tidak lagi berhasil, dokumentasikan hasil tersebut sebagai bukti peningkatan keamanan. Namun, jika serangan masih berhasil, lakukan analisis ulang dan perbaikan lebih lanjut. Dokumentasikan seluruh hasil uji keamanan ini sebagai bukti bahwa program telah menjadi lebih aman.

Ulangi bagian (a) sampai (d) di atas untuk minimal 4 (empat) kerentanan yang ada pada program.

III. Penulisan laporan:
Susun laporan untuk mendokumentasikan seluruh proses yang dilakukan, mulai dari analisis program awal, identifikasi celah keamanan, pelaksanaan serangan, langkah perbaikan, dan uji keamanan setelah perbaikan. Gunakan template yang sudah disediakan untuk penulisan laporan (file: KamSib 2425-1 - Template Laporan Tugas 1.docx)

Di dalam template laporan sudah ada 2 (dua) kerentanan program yang dituliskan pada bagian B.1 dan B.2 (dengan tulisan berwarna merah). Anda tidak perlu mengubahnya, dan hanya perlu melanjutkan mengisi bagian yang masih kosong (ditandai dengan "……..").
Untuk bagian B.3 dan B.4, Anda bebas memilih kerentanan apa yang akan dianalisis dan ditangani, kemudian lengkapi. Batasi kerentanan yang Anda pilih pada yang bersumber dari kelemahan kode program, bukan yang ada pada aspek infrastruktur, platform, atau elemen lainnya sebagai pendukung berjalannya program.

Tulisan berwarna biru di dalam template adalah petunjuk pengisian. Hapuslah bagian tersebut di dalam versi akhir laporan Anda.

Penilaian:

- Bagian A: maks 5 poin
- Bagian B.1 dan B.2: masing-masing maks 20 poin
- Bagian B.3 dan B.4: masing-masing maks 25 poin
- Bagian C: maks 5 poin

Ketentuan umum:

- Dikerjakan secara berkelompok (3 – 4 mahasiswa per kelompok).
- Kerjakan tanpa bantuan aplikasi / tool AI. Jika terbukti menggunakan aplikasi / tool AI, maka nilai tugas = 0.
- Laporan dikumpulkan dalam format pdf melalui LMS selambatnya tanggal 21 Desember 2025 jam 23:59 WIB (akhir pekan ke-14).
- Presentasi pengerjaan tugas diatur oleh dosen kelas.
- Seluruh tindakan yang dilakukan dalam tugas ini bertujuan untuk pembelajaran. Mahasiswa diharapkan untuk menjaga etika dalam keamanan siber, dan menerapkan pemahaman mereka secara bertanggung jawab.

---===@===---