TUGAS TEORI

Pertemuan Ke : 1 KEAMANAN BASIS DATA

NAMA	:	4342411005 - Keysya Arghinaya
		4342411008 - Muhammad Abi Nubli Rosyadi
		4342411018 - Angelina Maria Angwarmase
		4342411023 - Annisa Nabila Andrint
		4342411024 - Nauval Putra Widaya
		4342411030 - Ziva Dasfi Sadira
TIM	:	PBL-TRPL-301
KELAS	:	TRPL 3A MALAM

KOORDINATOR MATA KULIAH : Gilang Ramadhan

PENGAMPU PRAKTIKUM : Gilang Ramadhan

PROGRAM STUDI TEKNOLOGI REKAYASA PERANGKAT LUNAK JURUSAN TEKNIK INFORMATIKA

POLITEKNIK NEGERI BATAM

BATAM 2025

KUIS 01 – MINGGU 01

Kode Mata Kuliah	**:**	**RPL318**
Mata Kuliah	**:**	**Keamanan Basis Data**
Tujuan Pembelajaran	**:**	**TP1** Mahasiswa mampu mengilustrasikan konsep kontrol akses dan akses pengguna pada basis data
Bentuk Soal	**:**	**Essai**
Bobot	**:**	**100**

BENTUK KUIS:

Tulisan Essai

DESKRIPSI TUGAS:

1. Buatlah scenario bisnis tentang menganalisis ancaman keamanan basis data dan mengimplementasi Solusi praktis.
2. Gunakan scenario bisnis sesuai topik tim PBL:

METODE PENGERJAAN:

1. Soal dikerjakan tim sesuai Tim PBL.
2. Unggah di e-learning dengan nama file **Kuis01-Pagi/Malam-NIM.pdf**

INDIKATOR PENILAIAN:

Relevansi jawaban yang jelas, logis, akurat, dan sistematis.

JADWAL PELAKSANAAN:

Dilakukan pada minggu ke 01 dan dikumpulkan pada hari diberikan kuis tersebut.

Jawaban :

Skenario Bisnis – Analisis Keamanan Basis Data Aplikasi Mobile digiTA

1. Deskripsi Aplikasi

digiTA Mobile adalah aplikasi bimbingan Tugas Akhir berbasis mobile yang dirancang untuk:

Mempermudah mahasiswa dalam memilih dosen pembimbing, mengunggah dokumen, menjadwalkan bimbingan, dan melihat progres.

Membantu dosen dalam mengelola jadwal bimbingan, memberi komentar/feedback langsung pada dokumen, serta memantau progres mahasiswa.

Memfasilitasi admin untuk mengelola data mahasiswa, dosen, serta informasi akademik seputar TA.

Fitur utama:

Penjadwalan bimbingan dengan kalender dan notifikasi otomatis.

Feedback dosen langsung pada dokumen yang diunggah mahasiswa.

Monitoring progres melalui grafik persentase & checklist.

Laporan aktivitas bimbingan yang bisa diunduh.

Integrasi dokumen berupa template skripsi, riwayat versi, dan pendaftaran sidang.

Manajemen akun berbasis peran (mahasiswa, dosen, admin).

Karena berbasis mobile dan terhubung dengan server pusat, aplikasi ini menyimpan data sensitif (dokumen skripsi, data pribadi, status bimbingan, dan hasil sidang), sehingga keamanan basis data sangat penting.

2. Analisis Ancaman Keamanan

1. SQL Injections

Ancaman yang mungkin terjadi pada project digiTA:
a. Membobol Login

– Penyerang bisa masuk sebagai mahasiswa, dosen, bahkan admin tanpa perlu tahu password.

b. Mencuri Data
– Data penting seperti identitas mahasiswa, dokumen skripsi, atau jadwal bimbingan bisa dicuri.

c. Merusak Data

– Progres bimbingan bisa dihapus, nilai sidang diubah, atau isi database jadi berantakan.

Pencegahan yang bisa dilakukan:

a. Validasi Input

– Semua data yang dimasukkan harus dicek dulu.

– Misalnya NIM hanya boleh angka, email harus sesuai format, dan dokumen hanya boleh PDF.

b. Batasi Hak Akses Database

– Akun database yang dipakai aplikasi jangan diberi hak penuh.

– Cukup bisa SELECT, INSERT, dan UPDATE, supaya kalau ada serangan, dampaknya tidak terlalu besar.

c. Error Handling

– Jangan menampilkan pesan error database secara detail ke pengguna.

– Cukup tampilkan pesan umum seperti “Terjadi kesalahan, silakan coba lagi”.

2. Unauthorized Data Access

Ancaman yang mungkin terjadi pada project digiTA:

a. Password yang lemah

– Penyerang bisa menebak password sederhana seperti “Password123” dan masuk ke sistem.

b. Pengambilan Data Sensitif

– Dengan teknik seperti SQL Injection, penyerang bisa menjalankan perintah berbahaya dan mengambil data sensitif.

c. Data yang tersebarluaskan

– Jika hak akses diberikan terlalu luas, pengguna bisa mendapatkan data yang seharusnya tidak boleh mereka lihat.

Pencegahan yang bisa dilakukan:
a. Penguatan Mekanisme Autentikasi

– Gunakan password yang kuat (kombinasi huruf besar, kecil, angka, simbol).

– Tambahkan Two-Factor Authentication (2FA) agar hanya pemilik akun yang bisa

masuk.

b. Pengaturan Hak Akses (Principle of Least Privilege)

– Mahasiswa, dosen, dan admin hanya boleh punya akses sesuai perannya.

– Lakukan review berkala untuk memastikan izin akses tetap sesuai kebutuhan.

c. Pembaruan Sistem Secara Berkala

– Update software basis data dan aplikasi secara rutin.

– Segera terapkan patch keamanan untuk menutup celah yang ditemukan.

3. Data Breach

DigiTA adalah platform digital berbasis mobile yang dirancang untuk memfasilitasi proses bimbingan Tugas Akhir (TA) di sebuah universitas. Platform ini menyimpan berbagai data sensitif, termasuk:

- Data Pribadi Mahasiswa: Nama, NIM, alamat email, nomor telepon.
- Data Akademik: Judul TA, proposal, bab-bab TA, catatan bimbingan, transkrip nilai.
- Data Dosen Pembimbing: Nama, NIP, bidang keahlian, jadwal bimbingan.
- Data Hak Kekayaan Intelektual (HKI): Informasi tentang potensi paten atau hak cipta terkait TA.

DigiTA telah diadopsi secara luas oleh mahasiswa dan dosen, sehingga platform ini menjadi target yang menarik bagi pelaku kejahatan siber.

Ancaman yang terjadi pada DigiTA:

- Serangan pada API: Serangan injection, otentikasi yang lemah, pembatasan rate limiting yang tidak memadai.
- Serangan pada Aplikasi Mobile: Reverse engineering, malware pada perangkat mobile, phishing melalui SMS.
- Ancaman Internal: Karyawan yang tidak puas, kesalahan konfigurasi, kurangnya pelatihan keamanan.

Implementasi Solusi DigiTA:

- Gunakan teknik obfuscation dan tamper detection untuk melindungi aplikasi dari reverse engineering.

- Implementasikan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan login.

- Lakukan pengujian keamanan aplikasi mobile secara rutin.

Keamanan Basis Data:

- Gunakan enkripsi untuk melindungi data sensitif saat disimpan dan saat transit.

- Terapkan kontrol akses berbasis peran (RBAC) untuk membatasi akses ke data.

- Lakukan backup data secara rutin dan simpan di lokasi yang aman.

- Monitor aktivitas basis data untuk mendeteksi aktivitas mencurigakan.