KEAMANAN DATABASE: ANCAMAN DAN CONTOH EKSPLOITASI

ANISA INTANIA PUTRI - 2024071010
NAYLA PUTRI CAHYA RAMADANI - 2024071020

PENGANTAR KEAMANAN DATABASE

Keamanan database adalah upaya untuk melindungi data agar tidak bisa diakses, diubah, atau disalahgunakan oleh pihak yang tidak berwenang. Database biasanya menyimpan data penting seperti akun pengguna, password, dan informasi pribadi, sehingga jika keamanannya lemah dampaknya bisa sangat besar.

1 UNAUTHORIZED ACCESS

Unauthorized access adalah kondisi ketika seseorang berhasil masuk ke sistem database tanpa izin resmi. Hal ini bisa terjadi karena password lemah, kebocoran akun, atau celah keamanan pada aplikasi.

Dampaknya data bisa dibaca, diubah, atau dihapus oleh pihak yang tidak berwenang.

Contoh Sederhana

Jika penyerang sudah masuk ke database, ia bisa menjalankan query seperti:

```
SELECT user_pass FROM wp_users WHERE ID = 1;
```

Query ini digunakan untuk mengambil data password user tertentu.

Cara Penanganan:

- Gunakan autentikasi kuat (password kompleks + MFA).
- Batasi akses hanya dari IP tertentu (firewall).

2 DATA LEAKAGE / DATA THEFT

Data leakage adalah kebocoran data ke pihak yang tidak seharusnya menerima data tersebut. Biasanya terjadi karena:

1. SQL Injection
2. Phising
3. Malware
4. Human Error

Contohnya, penyerang mendapatkan akses database lalu menyalin seluruh data pengguna dan menyimpannya di luar sistem.

Cara Penanganan:

- Enkripsi data sensitif, baik saat disimpan maupun dikirim.
- Pantau akses ke data sensitif untuk mendeteksi kebocoran.

3 PENYALAHGUNAAN HAK AKSES

Privilege abuse terjadi ketika akun yang punya hak akses tinggi, seperti admin, digunakan untuk hal yang tidak semestinya. Masalah ini sering muncul karena satu akun digunakan untuk banyak keperluan.

Cara Penanganan:

- Review dan batasi hak akses user
- Pantau aktivitas user internal yang mencurigakan.

Contoh query penyalahgunaan:

Jika penyerang sudah masuk ke database, ia bisa menjalankan query seperti:

```
SELECT TABLE_NAME
FROM INFORMATION_SCHEMA.TABLES
WHERE TABLE_SCHEMA = 'nama_database';
```

Query ini dipakai untuk melihat semua tabel dalam database, yang kemudian bisa diambil isinya satu per satu.

4 DENIAL OF SERVICE (DOS)

Jenis serangan di mana penyerang mengirimkan perintah SQL yang sengaja dibuat sangat kompleks, sehingga database menjadi lambat, penuh beban, atau bahkan berhenti merespons.

Contoh Query:

```
SELECT * FROM products
WHERE name LIKE '%n%n%n%n%n%n%n%n%n%n%n%n%n%n%n!';
```

Jika query ini dijalankan database harus mengecek pola panjang terhadap seluruh baris, pemrosesan LIKE dengan pola rumit memakan CPU besar, query menjadi sangat lambat -> server overload -> DoS tercapai.

Cara Penanganan:

- Gunakan WAF dan anti-DDoS (Cloudflare, AWS Shield).
- Update patch untuk mencegah exploit yang menyebabkan crash.

5 SQL INJECTION

SQL Injection adalah teknik serangan dengan menyisipkan perintah SQL melalui input pengguna yang tidak divalidasi dengan baik. Serangan ini bisa digunakan untuk membaca, mengubah, bahkan menghapus data.

Contoh Input Berbahaya:

```
' OR '1'='1
```

Jika dimasukkan ke form login yang tidak aman, kondisi ini selalu bernilai benar sehingga login bisa dilewati tanpa password.

Cara Penanganan:

- Validasi dan filter semua input pengguna (whitelist).
- Gunakan prepared statement / parameterized query.

KESIMPULAN PRESENTASI

Sebagai kesimpulan, bisnis internasional menawarkan banyak peluang bagi perusahaan untuk memperluas pasar, mengakses teknologi baru, dan meningkatkan daya saing. Namun, tantangan seperti perbedaan budaya, fluktuasi mata uang, dan kompleksitas regulasi harus dihadapi dengan strategi yang tepat. Kepatuhan terhadap standar global dan pemahaman mendalam tentang regulasi lokal sangat penting untuk menghindari risiko hukum dan memastikan keberhasilan jangka panjang

TERIMA KASIH

Databases