

Write up challenge SQL Truncation

Tác giả:

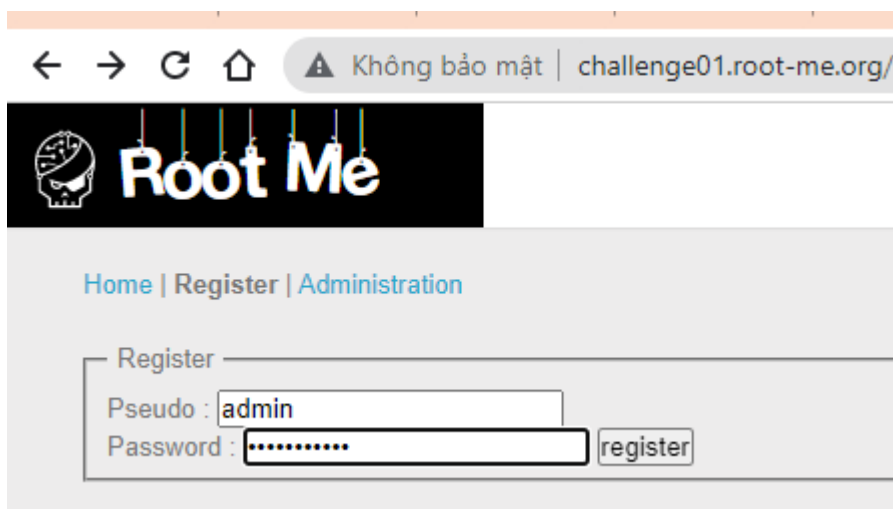
- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

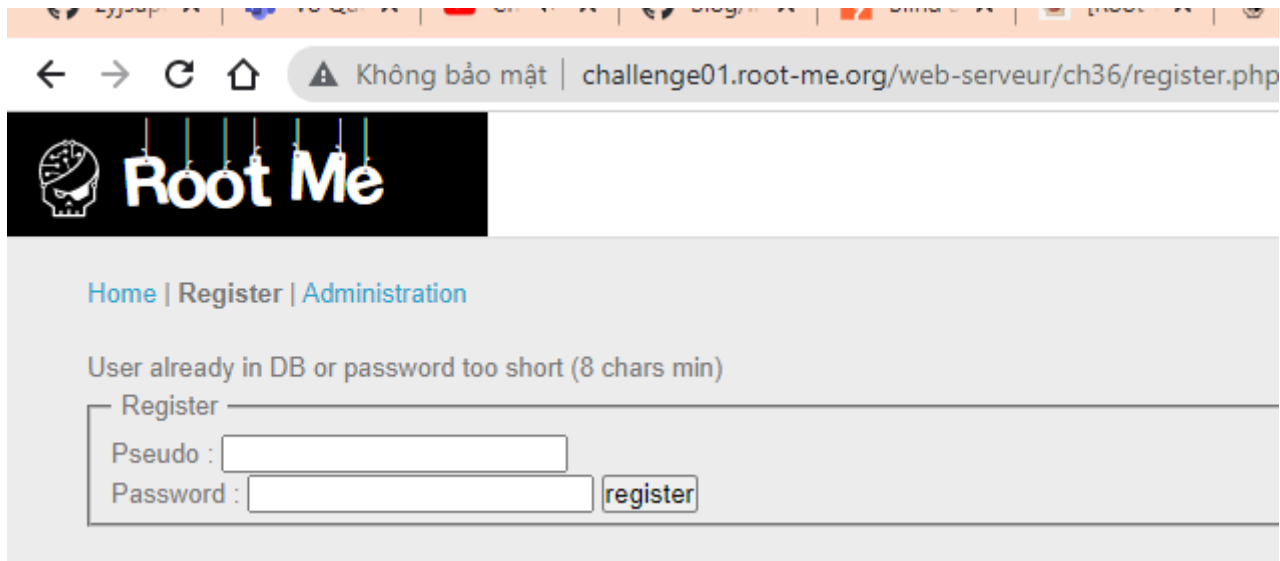
Truy cập challenge ta thấy gồm 3 trang Home | Register | Administration



Mục tiêu chúng ta là có truy cập vào được admin zone. Để làm được ta cần có pass. Tiến hành đăng kí thử tài khoản admin:



Thông báo không thành công và ta biết được hai thông tin: một là tài khoản admin đã tồn tại, hai là độ dài mật khẩu cần lớn hơn hoặc bằng 8.



Như tên challenge đã gợi ý, tiến hành tìm hiểu SQL Truncation và biết được:

- Lỗi hỏng SQL Truncation xảy ra khi độ dài input đầu vào không được validate. Khi độ dài chuỗi input nhập vào lớn hơn độ dài đã được define tương ứng thì nó sẽ bị cắt đi sao cho đúng bằng độ dài đã được define đó.
- Một chú ý khác là trong quá trình so sánh MySQL sẽ bỏ qua các ký tự dấu cách ở cuối chuỗi. Nghĩa là 'admin' sẽ bằng 'admin '.

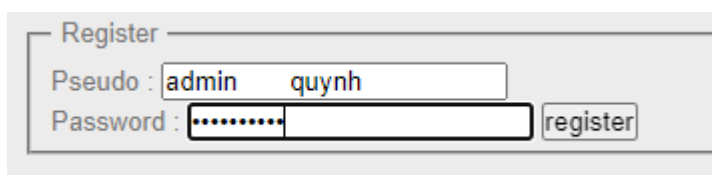
Ý tưởng sẽ là lợi dụng SQL Truncation để đăng kí tài khoản admin với thông tin mình cung cấp.

Tiến hành inspect thử ta thấy được definition table user:

```
Tự ngắt dòng ☐
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <title>Root-Me | Register</title>
5   </head>
6
7   <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=externe_header'></if
8     <a href='index.php'>Home</a> | <b>Register</b> | <a href='admin.php'>Administration</a>
9   </body><br/>
10  User already in DB or password too short (8 chars min)<br><form action="" method="POST">
11    <fieldset>
12      <legend>Register</legend>
13      <label>Pseudo : </label> <input type="text" name="login"><br>
14      <label>Password : </label> <input type="password" name="password">
15      <input type="submit" value="register">
16    </fieldset>
17  </form>
18
19  <!--
20  CREATE TABLE IF NOT EXISTS user(
21    id INT NOT NULL AUTO_INCREMENT,
22    login VARCHAR(12),
23    password CHAR(32),
24    PRIMARY KEY (id));
25  -->
26  </body>
27 </html>
28
29
```

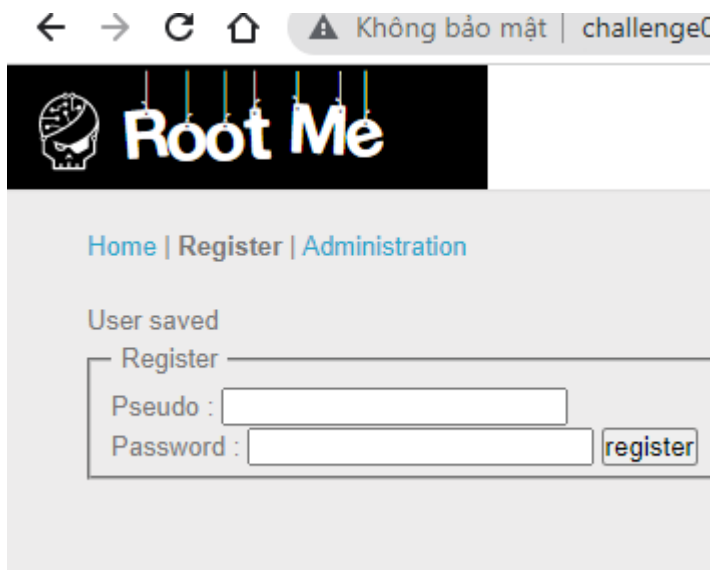
Ok, vậy là ta đã biết được trường login trong cơ sở dữ liệu được giới hạn tối đa 12 kí tự.

Tiến hành đăng kí với login là 'admin quynh' và pass 123456789

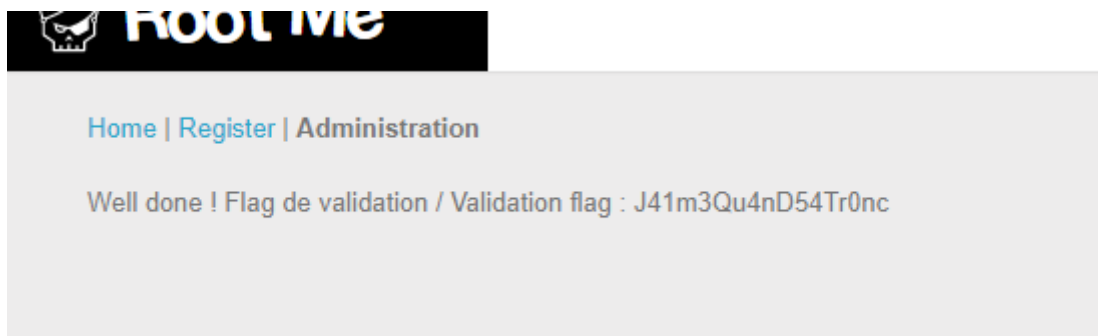


Như đã phân tích ở trên, khi kiểm tra 'admin quynh' sẽ không trùng với login trong cơ sở dữ liệu nhưng khi dữ liệu được đưa vào database cột login sẽ cắt bớt và dữ liệu lúc này sẽ là 'admin ' hay khi so sánh cũng là 'admin'.

Đăng kí thành công!




Tiến hành vào admin zone với pass 123456789 vừa đăng kí và có được flag.



Submit thành công


HOME / CHALLENGES / WEB - SERVER


SQL Truncation

35 Points 

SQL limits

Author: Geluchat, 1 May 2015

Level 




Statement

Retrieve an access to the administration's zone.

[Start the challenge](#)


1 related ressource(s)

-  [Blackhat US 2006 : SQL Injections by truncation](#) (Exploitation - W

Validation

Well done, you won 35 Points

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

 [twittez le !](#)

Enter password

Flag: J41m3Qu4nD54Tr0nc