SQL Truncation

Title: SQL limits

Point: 35 Points

**Description: **Retrieve an access to the administration's zone.

Solution:

Challenge này không liên quan gì đến hàm **truncate()** hay từ khóa **truncate**, mà là lỗi **Truncate Error** . Reference Document

Mình không thể "thông chốt" chiếc form này, đồng thời không thể trực tiếp thêm một tài khoản 'admin'

Một cách đơn giản, **Truncate Error** xảy ra khi size dữ liệu đưa vào lớn hơn size được khai báo tại trường đó thì khi đưa vào DB, nó sẽ bị cắt bớt đúng bằng size đã được khai báo. Ví dụ, khai báo biến abc varchar(3), nhưng mình nhập vào "1234567890" thì khi lưu vào database sẽ còn "123".

NOTE: Trong database, mình có thể chèn dữ liệu có các trường giống giá trị với nhau, mình có thể thực hiện việc testing cái này.

Vào Source Code trong trang "Register" , giờ thì ngạc nhiên chưa

```
<!DOCTYPE html>
<html>
    <head>
        <title>Root-Me | Register</title>
    </head>

<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=e
            <a href="index.php">Home</a> | <b>Register</b> | <a href="admin.php">Administration</a>
            <br/><br/>
<form action="" method="POST">
            <fieldset>
            <legend>Register</legend>
                <label>Pseudo : </label> <input type="text" name="login"><br>
                <label>Password : </label> <input type="password" name="password">
                <input type="submit" value="register">
            </fieldset>
        </form>

<!--
CREATE TABLE IF NOT EXISTS user(
    id INT NOT NULL AUTO_INCREMENT,
    login VARCHAR(12),
    password CHAR(32),
    PRIMARY KEY (id));
-->
    </body>

</html>
```

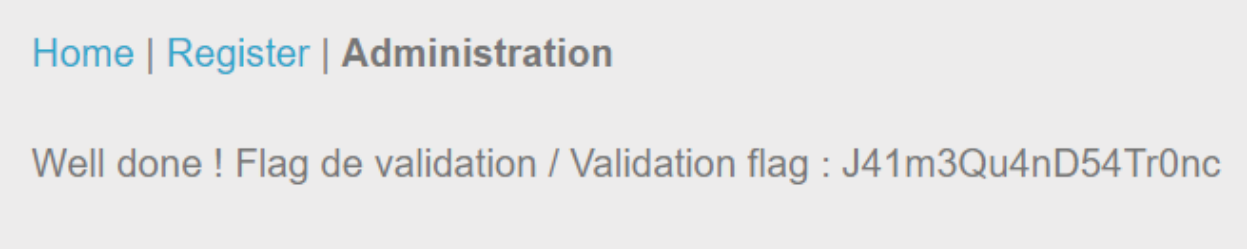
Giờ mình biết được size của các trường, mình sẽ tạo tài khoản "admin" mới thôi

Pseudo :

admin hackerisnothere

Password: (We can choose freely as long as having a length be greater or equal to **8**)

khangtictoc123



NOTE: Thông báo “User already in DB” là từ back-end server, không liên quan đến phía "Database". Theo mình đoán, khi mình đăng ký trực tiếp tài khoản “admin” thì server kiểm tra xem trong DB có user này chưa và sẽ xuất lỗi. Còn khi mình điền payload trên “admin hackerisnothere**” thì server đối chiếu sẽ thấy khác, nên accept, nhưng khi vào DB thì nó cắt xén luôn và còn mỗi chuỗi “admin” nên mình mới có thể làm vậy được.**

Dễ quá phải không 😊. Nhưng nhớ phân biệt 2 trường hợp mình đăng ký “admin” thì server nhận, còn trường hợp kia thì không. Làm được thì phải hiểu rõ nhớ….

Flag: **J41m3Qu4nD54Tr0nc**