

# 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 6: SQL Truncation (level medium)

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

- Bài này yêu cầu ta lấy quyền truy cập vào khu vực của quản trị viên

#### SQL Truncation

35 Points 🏆

SQL limits

Author

Geluchat, 1 May 2015

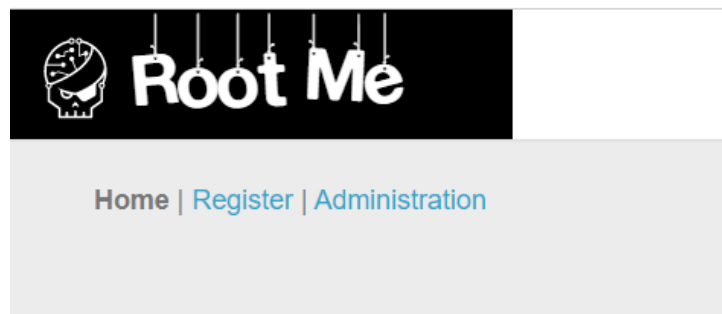
Level ①




Statement

Retrieve an access to the administration's zone.

- Truy cập vào thử thách ta thấy 2 tab là Register và Administration



- Ở tab Register thực hiện đăng ký 1 tài khoản




[Home](#) | [Register](#) | [Administration](#)

Register

Pseudo :

Password :


- Ở tab Administration thì nhập password của admin



[Home](#) | [Register](#) | [Administration](#)

Password :

- Thử đăng ký với account **19520199/19520199** ta thấy có xuất hiện dòng **User saved**



[Home](#) | [Register](#) | [Administration](#)

User saved

Register

Pseudo :

Password :

- Ở tab register chỉ dùng để đăng kí với phương thức POST nên chỉ trả về thành công hay không. Không thể dùng cách tấn công ' or 1=1-- như mọi khi được.
- Kiểm tra mã nguồn ta thấy đoạn comment cần lưu ý

Home | Register | Administration

User already in DB or password too short (8 chars min)

Register

Pseudo :

Password :

DevTools is now available in Vietnamese! [Always match Chrome's language](#) [Switch](#)

Elements Console Recorder Sources Network Performance

```
<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));
-->
```

- Trường login với length là 12 do đó nếu giá trị nhập vào vượt quá 12 thì chuỗi sau vị trí thứ 12 sẽ bị cắt bỏ, và chỉ nhận giá trị ở trước vị trí 12
- Nhiệm vụ của ta là tạo tài khoản admin và login với quyền admin để lấy được flag.
- Nhưng tài khoản admin đã tồn tại nhưng mình không có password chính xác cho admin đó. Tạo username với admin thì thông báo username đã tồn tại.
- Vậy ta cần dựa vào tính năng truncate để bypass kiểm tra username tồn tại và tạo được account admin và control password login để lấy flag.
- Tiến hành đăng ký với user là **admin** **111** và password là **19520199**

pl

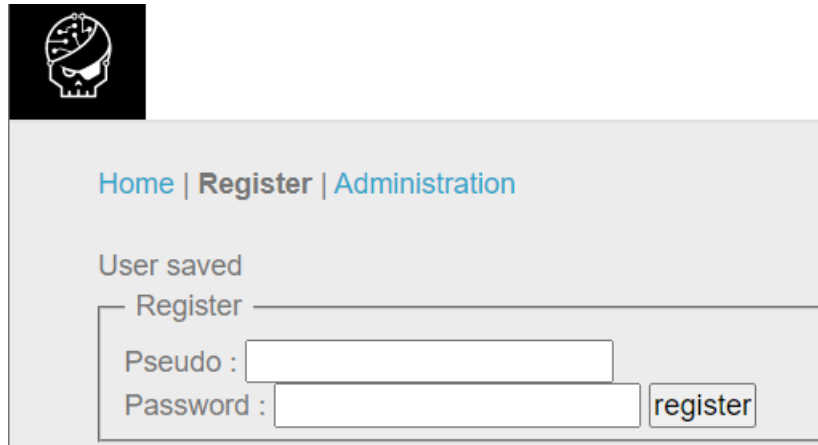
Home | Register | Administration

Register

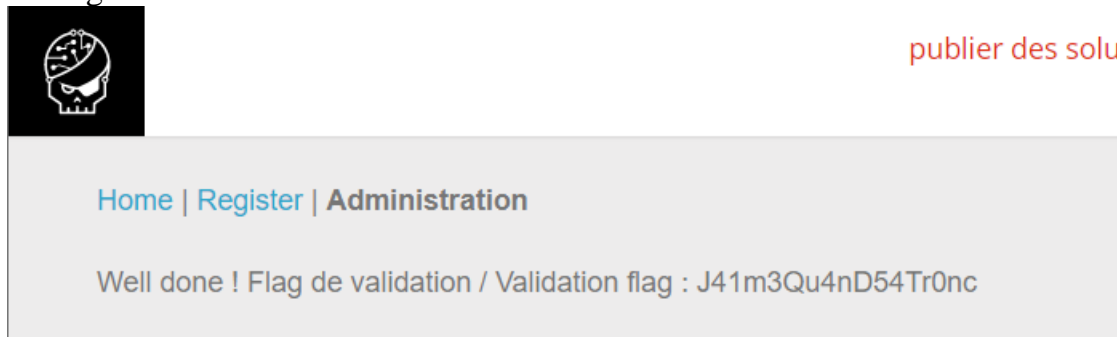
Pseudo :

Password :

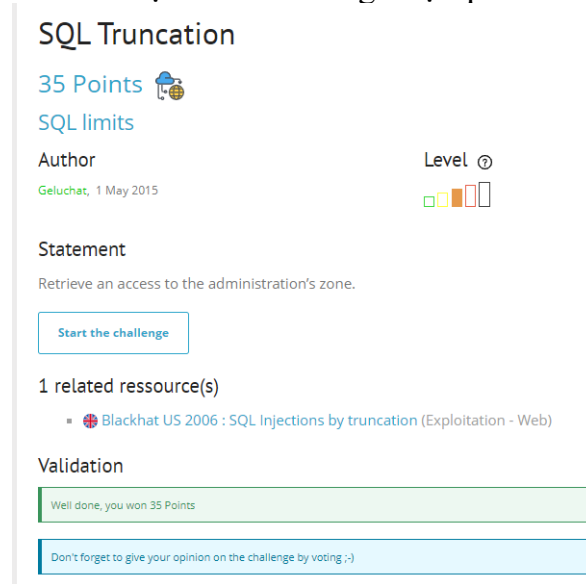
- Kết quả cho ta thấy ta đã tạo thành công tài khoản admin khi xuất hiện dòng user saved



- Qua tab Administrator và nhập password vừa đăng ký vào ta thu được flag thành công



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



**FLAG: J41m3Qu4nD54Tr0nc**