

# BÀI TẬP CTF

## Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

### Challenge 2: SQL injection - Authentication - GBK (level medium)

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

- Thử thách yêu cầu ta nhận quyền truy cập administrator

SQL injection - Authentication - GBK

30 Points 🏆

Do you speak chinese ?

Author

dvor4x, 2 December 2015


Level ①



Statement

Get an administrator access.

- Truy cập vào thử thách, ta nhận được một form đăng nhập



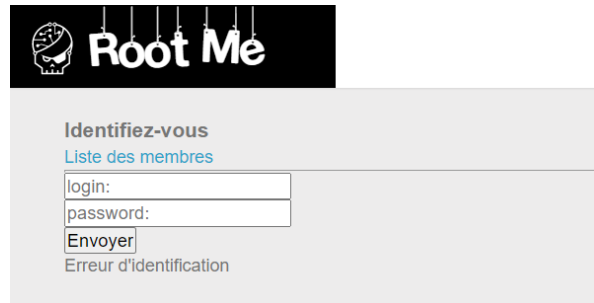
Identifiez-vous

[Liste des membres](#)

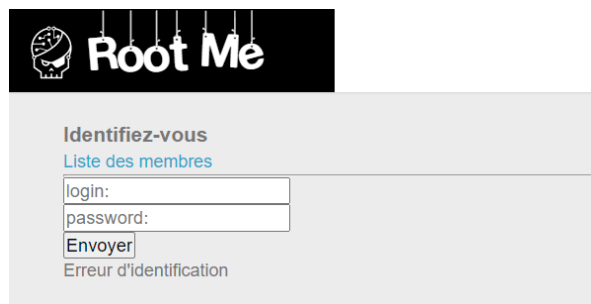
login:

password:

- Thử đăng nhập với user/password là 19520199/1 ta thấy xuất hiện dòng **Erreur d'identification** (lỗi nhận diện)



- Thử tấn công với payload đơn giản 1' OR 1=1 ta cũng nhận được kết quả tương tự là lỗi nhận diện
- Dựa vào tên thử thách thì ta cần tìm hiểu GBK là gì ( [GBK \(character encoding\)](#) )
- Sau khi tìm hiểu về GBK, ta tiếp tục tìm kiếm thì đều thu được một điểm chung là sử dụng cách bypass addslashes()
- Khi sử dụng hàm addslashes() thì nó sẽ tự động thêm ký tự / (0x5c) vào trước các ký tự như ' , " , / , NUL byte ( [function.addslashes.php](#) ). Ví dụ đơn giản với ' sẽ trở thành '/'
- Do đó ta thử tấn công với payload 1' OR 1=1. Kết quả vẫn thất bại



- Điều đó có nghĩa là máy chủ đang mong đợi một ký tự GBK hợp lệ làm đầu vào. Do đó ta cần thêm một symbol đặc biệt để khi nối với **0x5c** (ký tự /) sẽ thành một symbol khác không bị filter bởi server. Ở đây có thể là **0xbf0x5c** hoặc **0xaf0x5c** hoặc **0xdf0x5c** hoặc **0xef0x5c** ... sẽ là một ký tự trung quốc để bypass được server.
- Ở đây ta chọn **0xaf0x5c** để tấn công. Khi chèn **0xaf0x27** (với 0x27 là ') thì hàm addslashes sẽ tự động chuyển ở đây thành **0xaf0x5c0x27**. Sử dụng tool onl để chuyển đổi sang gbk ([gbk](#)) và nó sẽ tương ứng là


Bytes to decode

af 27

Convert



- Lưu ý ở bài này ta sử dụng comment là -- - đối với Mysql. Tùy vào từng loại database mà sử dụng các comment khác nhau
- Đăng nhập với chuỗi `❖' or 1=1 -- -` và password bất kỳ ta thu được flag thành công



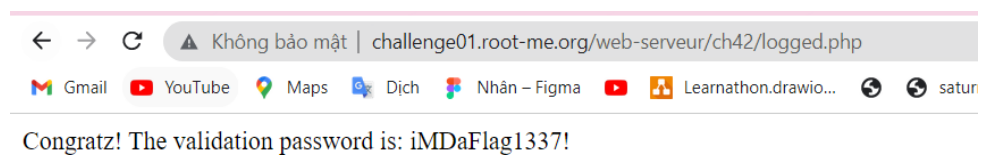
# Root Me

Identifiez-vous

[Liste des membres](#)

Envoyer

- Hình ảnh kết quả



**FLAG: iMDaFlag1337!**