BÀI TẬP CTF

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

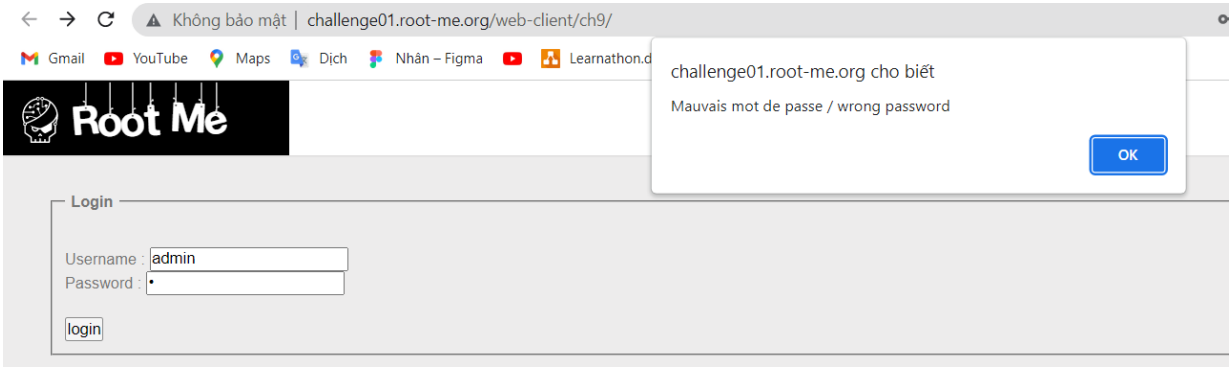
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

Challenge 2: Javascript – Authentication (level very easy)

Link challenge **https://www.root-me.org/en/Challenges/Web-Client/Javascript-Authentication**

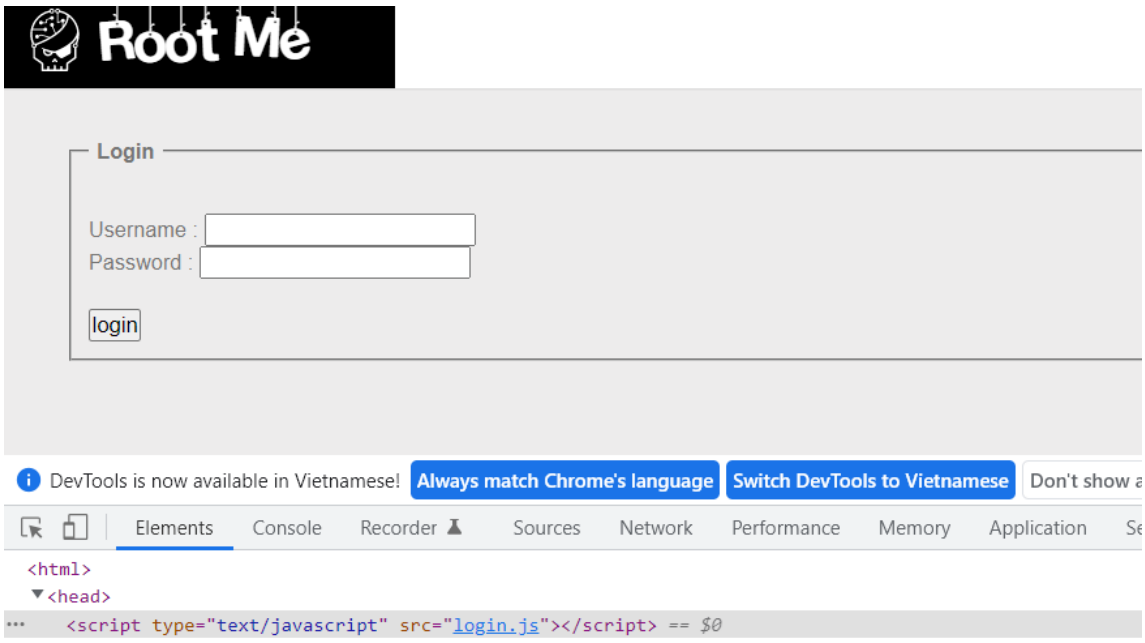
- ✓ Thử thách bắt ta login vào, thử login và hiện ra dòng thông báo là wrong password



- ✓ Sử dụng F12 để kiểm tra

```
<input onclick="Login()" type="button" value="login"
name="button"> == $0
```

- ✓ Ta thấy có sự kiện onlick sẽ gọi hàm Login() khi click vào nút login. Ta sẽ, tìm đoạn script liên quan đến hàm Login()



✓ Ta thấy có đoạn script với src=login.js, truy cập vào file đó

✓ Giá trị username nhập vào sẽ lưu vào biến pseudo, giá trị password sẽ lưu vào biến password

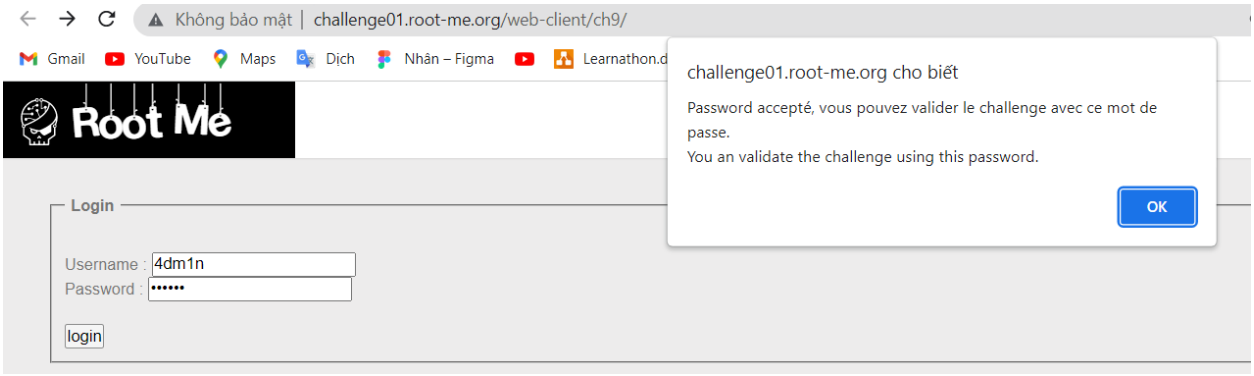
✓ Sau đó, chuyển đổi chuỗi pseudo thành chữ thường với hàm toLowerCase() và lưu vào biến username. Nhưng biến username sau đó không dùng tới, do đó ta không cần quan tâm tới biến này

✓ Tương tự, biến password sẽ tự chuyển đổi thành chữ thường và lưu lại.

✓ Tiếp theo, ta thấy có dòng điều kiện, với pseudo = “4dm1n” và password=”sh.org” thì sẽ thỏa mãn điều kiện và xuất ra thông báo “Mật khẩu được chấp nhận, bạn có thể xác nhận thử thách bằng mật khẩu này.” Ngược lại in ra dòng mật khẩu sai.

✓ Do đó ta suy ra được user name nhập vào phải là “4dm1n” và password phải là “sh.org” (có thể viết hoa bất kỳ chữ nào ở password)

✓ Thử đăng nhập với username và password vừa tìm được ta thu được thông báo thành công như trên



Flag: sh.org