

BÀI TẬP CTF

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

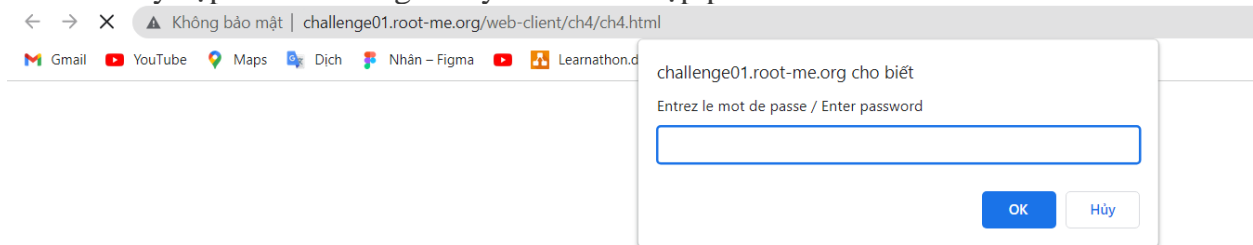
Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

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

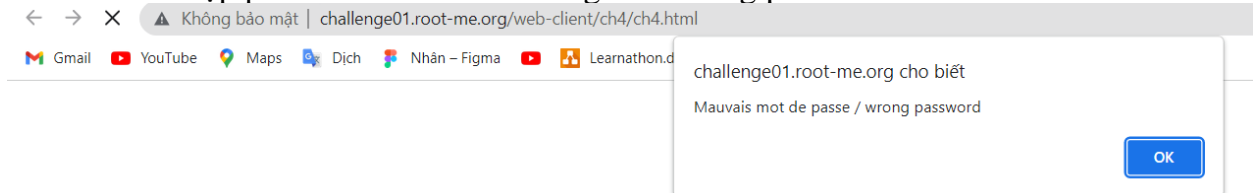
Challenge 5: Javascript - Obfuscation 1 (level very easy)

Link challenge <https://www.root-me.org/en/Challenges/Web-Client/Javascript-Obfuscation-1>

✓ Truy cập vào challenge thì yêu cầu ta nhập password



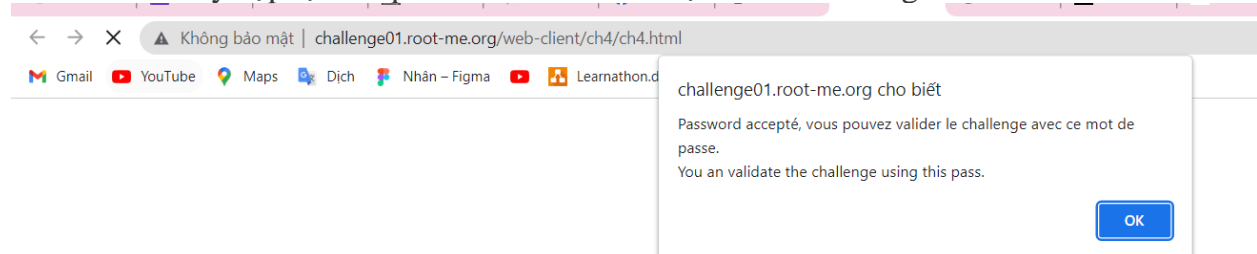
✓ Thử nhập pass là 1 thì xuất ra thông báo wrong password



✓ Sử dụng tổ hợp phím **ctr + u** để xem mã nguồn

```
Tự ngắt dòng
1 <html>
2   <head>
3     <title>Obfuscation JS</title>
4     <script type="text/javascript">
5       /* <![CDATA[ */
6
7       pass = '%63%70%61%73%62%69%65%6e%64%75%72%70%61%73%73%77%6f%72%64';
8       h = window.prompt('Entrez le mot de passe / Enter password');
9       if(h == unescape(pass)) {
10         alert('Password accepté, vous pouvez valider le challenge avec ce mot de passe.\nYou an validate the challenge using this pass.');
```

- ✓ Ta thấy có 1 biến pass được khai báo trước. Và biến h lưu password nhập vào, sau đó lệnh if kiểm tra xem nếu h=unescape(pass) thì hiển thị thông báo thành công và có thể dùng password để vượt qua challenge này. Do đó ta chỉ cần unescape(pass) là tìm được password
- ✓ Sử dụng console để tìm password
 - > pass = '%63%70%61%73%62%69%65%6e%64%75%72%70%61%73%73%77%6f%72%64';
 - < '%63%70%61%73%62%69%65%6e%64%75%72%70%61%73%73%77%6f%72%64'
 - > unescape(pass)
 - < 'cpasbiendurpassword'
- ✓ Ta thu được password là “cpasbiendurpassword”
- ✓ Thử truy cập lại với password vừa tìm được và thành công



Flag: cpasbiendurpassword