

BÀI TẬP CTF

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

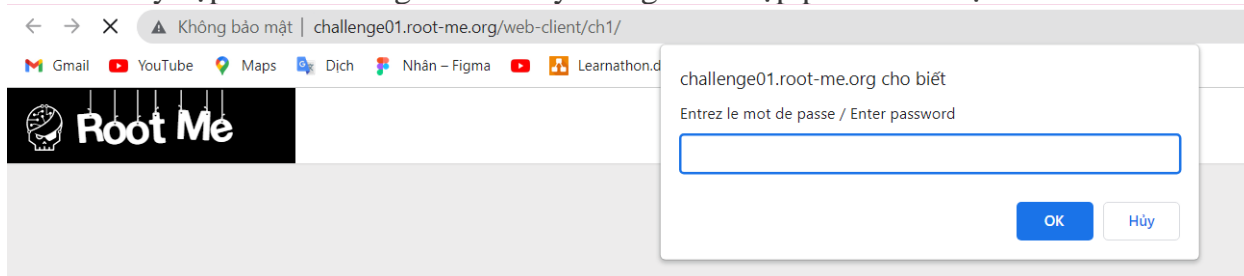
Giảng viên hướng dẫn: *Đỗ Hoàng Hiến*

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

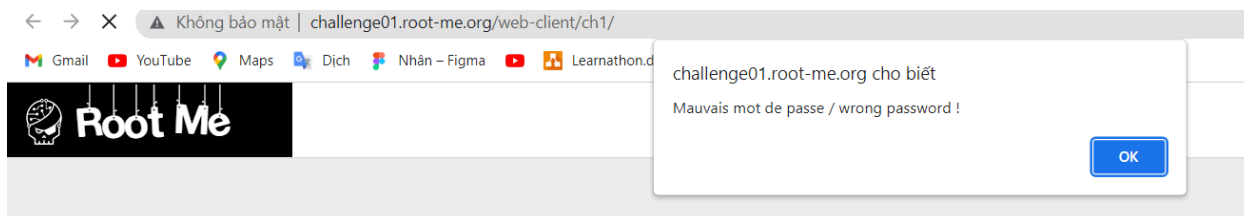
Challenge 3: Javascript – Source (level very easy)

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

✓ Truy cập vào challenge và ta thấy thông báo nhập password hiện lên



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



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

```
view-source:challenge01.root-me.org/web-client/ch1/

<html>
<head>
<script type="text/javascript">
/*  */
function login(){
pass=prompt("Entrez le mot de passe / Enter password");
if ( pass == "123456azerty" ) {
alert("Mot de passe accepté, vous pouvez valider le challenge avec ce mot de passe.\nYou can validate the challenge using this password."); }
else {
alert("Mauvais mot de passe / wrong password !");
}
}
/* ]]&gt; */
&lt;/script&gt;
&lt;/head&gt;
&lt;body onload="login();"&gt;&lt;link rel='stylesheet' property='stylesheet' id='s' type='text/css' href='/template/s.css' media='all' /&gt;&lt;iframe id='iframe' src='
&lt;/body&gt;
&lt;/html&gt;</pre></div><div data-bbox="143 311 876 407" data-label="List-Group"><ul><li>✓ Ta thấy trong function login() có dòng lệnh if dùng để kiểm tra password. Nếu pass == "123456azerty" thì hiển thị thông báo thành công và có thể dùng pass này để vượt qua challenge.</li><li>✓ Do đó pass là 123456azerty</li><li>✓ Nhập pass vừa tìm được và kiểm tra kết quả</li></ul></div><div data-bbox="113 407 875 533" data-label="Image"><img alt="Screenshot of a web browser showing the challenge01.root-me.org website. The browser address bar shows 'challenge01.root-me.org/web-client/ch1/'. The website has a black header with the 'Root Me' logo. A JavaScript alert box is displayed in the center of the screen with the text: 'challenge01.root-me.org cho biết', 'Mot de passe accepté, vous pouvez valider le challenge avec ce mot de passe.', and 'You can validate the challenge using this password.' with an 'OK' button."/></div><div data-bbox="112 551 291 570" data-label="Text"><p><b>Flag: 123456azerty</b></p></div>
```