BÀI TẬP CTF

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

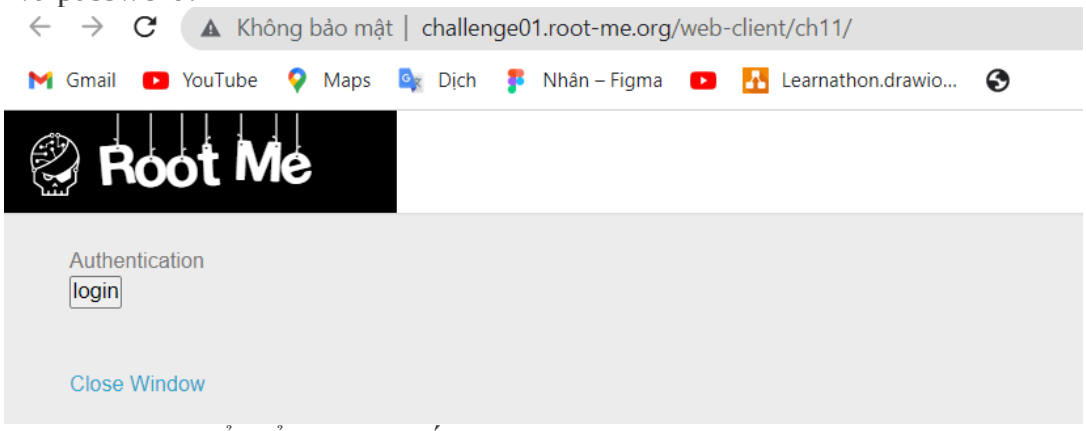
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

Challenge 4: Javascript - Authentication 2 (level very easy)

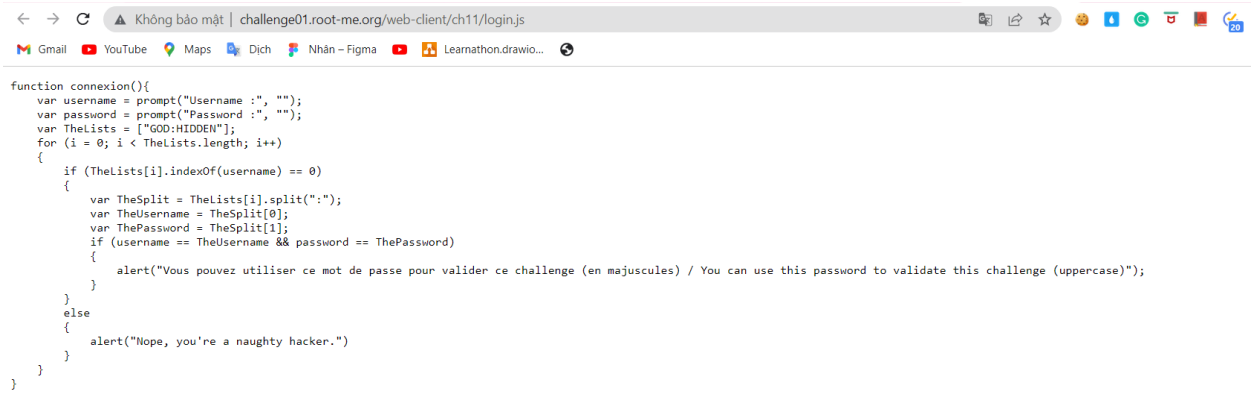
Link challenge **https://www.root-me.org/en/Challenges/Web-Client/Javascript-Authentication-2**

- ✓ Truy cập vào challenge ta thấy nút login và để login thành công cần biết username và password.

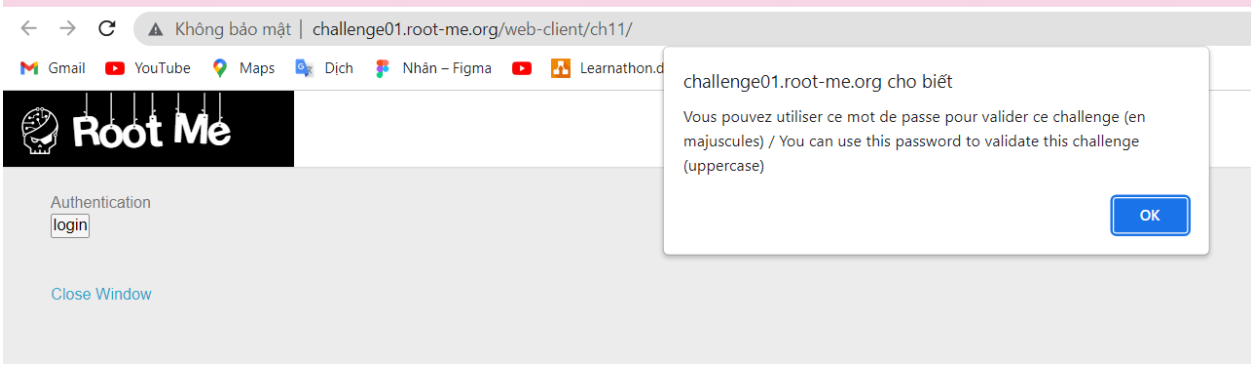


- ✓ Sử dụng F12 để kiểm tra ta thấy hàm connextion() sẽ được kích hoạt khi click vào nút login

- ✓ Ta thấy đoạn script liên quan đến việc login có src=”login.js”
- ✓ Truy cập vào login.js ta thấy được đoạn code của hàm connextion()



- ✓ Ta thấy rằng, chương trình yêu cầu nhập username và password, biến username sẽ lưu username ta nhập vào và biến password sẽ lưu password ta nhập vào. TheLists ban đầu sẽ có giá trị là "GOD:HIDDEN". Có 1 vòng for duyệt qua list này sau đó sẽ kiểm tra nếu giá trị username không xuất hiện ở vị trí đầu tiên (vị trí thử 0) của TheLists thì sẽ xuất ra thông báo "Không, bạn là một hacker nghịch ngợm.". Ngược lại khi qua được câu lệnh if, TheSplit sẽ có 2 phần tử là GOD và HIDDEN tách ra từ TheLists (ngăn cách bởi dấu :). Sau đó TheUsername gán bằng TheSplit[0] = GOD, ThePassword gán bằng TheSplit[1] = HIDDEN. Cuối cùng là câu lệnh if kiểm tra username và password ta nhập vào có tương ứng với TheUsername và ThePassword không nếu đúng thì xuất ra dòng thông báo và ta có thể sử dụng password để vượt qua thử thách.
- ✓ Thử chạy lại với username và password vừa tìm được ta nhận được thông báo tương ứng.



Flag: HIDDEN