BÀI TẬP CTF

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

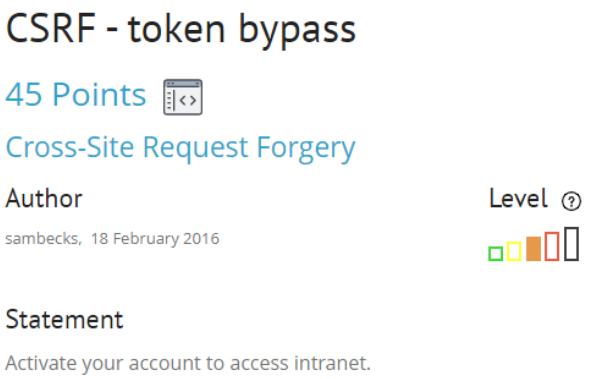
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

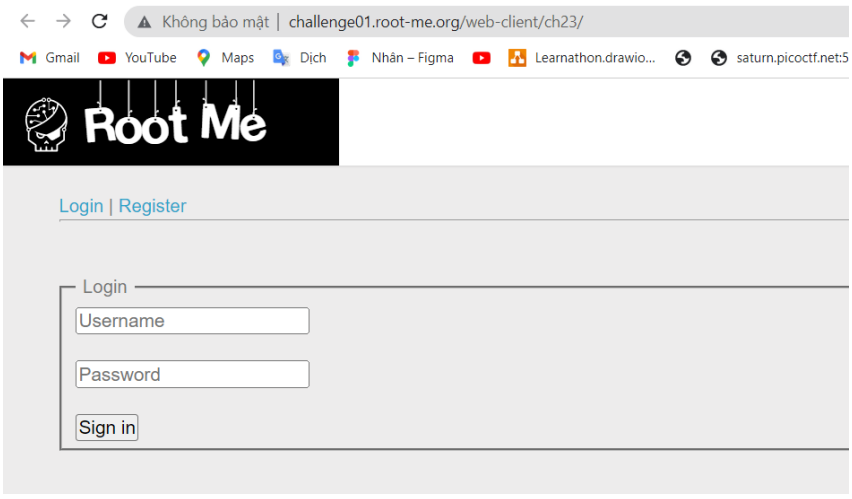
Challenge 11: CSRF - token bypass (level medium)

Link challenge: https://www.root-me.org/en/Challenges/Web-Client/CSRF-token-bypass

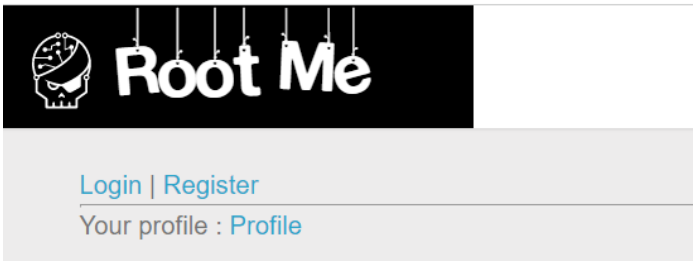
- ✓ Challenge yêu cầu ta kích hoạt tài khoản để truy cập vào intranet



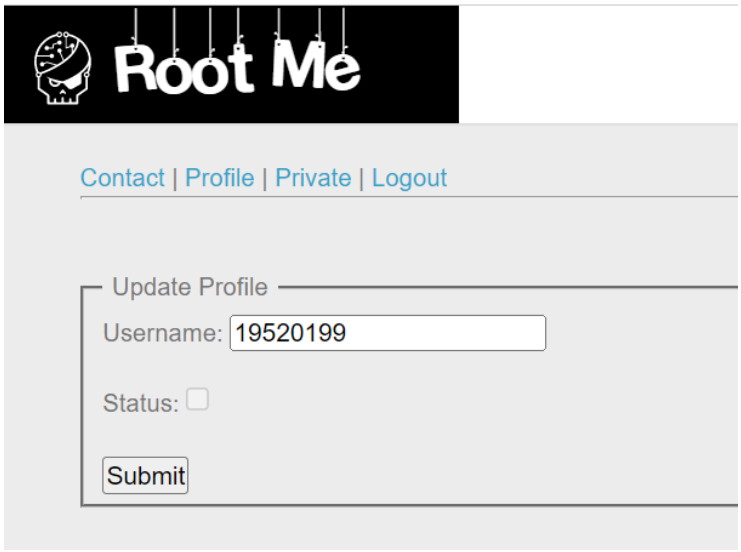
- ✓ Truy cập vào challenge



- ✓ Ta thấy có 2 tab là đăng nhập và đăng ký. Ta thử đăng ký 1 tài khoản là 19520199/12345
- ✓ Kết quả sau khi đăng nhập vào ta thấy có thêm mục profile.



- ✓ Click vào profile



- ✓ Có 4 tab là Contact, Profile, Private và Logout.
- ✓ Tại tab Profile, ta thấy có 2 trường username và status. Với username là username của ta, và trường status là một disable checkbox. Bài này khá giống với CSRF-0 protection, tuy nhiên có thêm 1 trường ẩn nữa là token

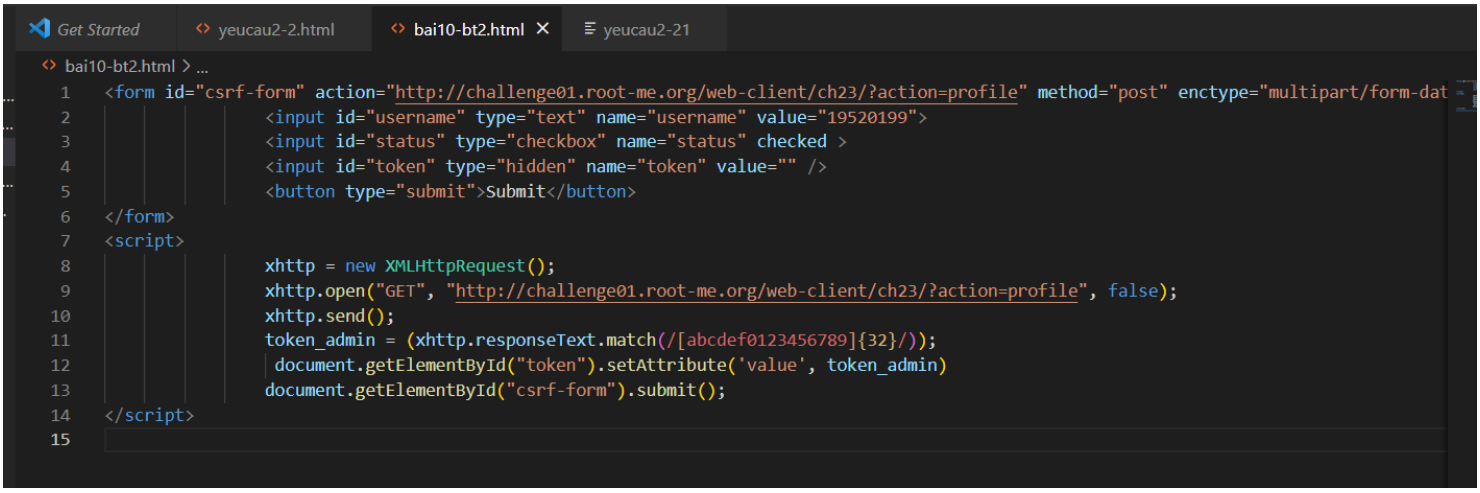
```
<legend>Update Profile</legend>
<form id="profile" action="?action=profile" method="post" enctype="multipart/form-data">
  <div>…</div>
  <br>
  <div>
    <label>Status:</label>
    <input id="status" type="checkbox" name="status" disabled> == $0
  </div>
  <br>
  <input id="token" type="hidden" name="token" value="7bbdbd96d6d80ac83787ba5c6be25599">
```

- ✓ Do đó để submit được form dưới quyền admin thì ta cần phải ta cần phải lấy được token của admin. Ta sẽ khai thác XSS để lấy token, sau đó sử dụng token này để tạo form tương tự bài CSRF-0 protection

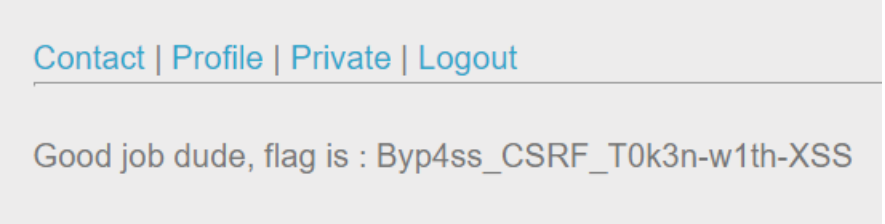
✓ Copy form tại trang Profile, sau đó chỉnh sửa một vài chỗ:

- Thêm id cho form: csrf-form
- Thay đổi đường link của action, gán bằng đường link tới trang Profile
- Tại trường **status:** thay đổi từ khoá **disabled** thành **checked.** Như vậy admin không cần tick vào checkbox này, măc định nó sẽ tự check.
- Trường **token** trong form ta để trống
- Sau đó là đoạn script để thu thập token của admon. Để lấy được token ta tạo một request GET tới trang web profile và thu thập token của admin lại
- Tiếp theo ta sẽ gán giá trị của token bằng giá trị vừa thu thập được
- Cuối cùng là lệnh tự động submit form khi trang được load.

✓ Đoạn code để exploit như sau



✓ Sau khi submit form trên, Chờ khoảng 2 phút, sau đó chuyển sang tab Private, ta nhận được flag



FLAG: Byp4ss_CSRF_T0k3n-w1th-XSS