TP CSRF

Contexte : Le site Super Forum est un forum de discussion en ligne. Vous avez découvert récement que le site était vulnérable, en effet, il y a une faille CSRF dans le formulaire d'edition des profils utilisateur. Vous allez donc exploiter cette faille afin de prendre possession du compte admin.

Vous trouverez dans le dossier /csrf le site à attaquer, pour lancer le script, ouvre un terminal dans ce dossier puis lancez la commande : php -S localhost:8080 pour lancer votre serveur.
Le site est maintenant accessible sur votre navigateur à l'adresse http://localhost:8080/
Note : Le script du site est volontairement obfusqué afin de vous forcer à vous mettre réellement dans la peau d'un hacker qui ne connaît rien du code du site qu'il est en train attaquer.

1. Lancez deux navigateurs différents, sur le premier navigateur connectez vous en tant que « admin » en utilisant les logins admin : admin puis créez un deuxième compte : celui du pirate.

2. Une fois le compte pirate créé, connectez vous dessuis puis inspecter le site. La vulnérabilité se trouve dans la page « Modifier mon compte », inspectez le formulaire

3. Créez un script permettant de modifier le mot de passe en choisissant le mot de passe de votre choix en exploitant la faille CSRF via un formulaire pirate.

4. Envoyez le script à la victime (ici vous devez faire executer le formulaire dans le navigateur connecté sur le compte admin).

5. Essayez de vous connecter au compte admin avec le mot de passe modifié, si cela fonctionne, féliciation, vous êtes devenu un hacker !