Introduction à la sécurité informatique
TP : sécurité web

Sujet de projet

Le sujet de projet en introduction à la sécurité consiste en **un rapport contenant les réponses aux différentes questions des sujets de TP et expliquant vos choix, ainsi que les codes sources produits pour résoudre les exercices**. En plus de la qualité technique des réponses, les points suivants seront évalués :

- La qualité de rédaction et la clarté du rapport,
- La facilité d'utilisation des codes sources fournis.

Le projet peut être réalisé seul ou en binôme.

1 Exercices

Dans ce TP, vous devez utiliser des environnements volontairement vulnérables afin de tester les vulnérabilités web les plus classiques. Vous devrez réaliser les attaques suivantes :

- CSRF,
- File inclusion,
- SQL Injection,
- XSS (Reflected et stored).

Vous pouvez bien sur aller plus loin et étudier/réaliser des attaques plus complexes !

2 Environnement de travail

Vous avez plusieurs possibilités afin de réaliser ces attaques. La première est d'utiliser une plateforme d'entrainement comme **Root-me**, qui propose des exercices permettant d'étudier ces vulnérabilités. **Lors des séances de TP**

uniquement, vous pourrez avoir un accès spécial au site, vous permettant d'avoir accès à plus d'exercices que sur le site "classique".

Pour travailler en local sur votre machine, vous pouvez également utiliser l'application DVWA (**Damn Vulnerable Web Application**). Pour installer cet environnement, suivez les instructions disponibles sur `https://github.com/digininja/DVWA`

Lorsque vous démarrez la machine il faut lancer les services suivants :

```
service apache2 start
service mysql start
```

Lorsque ces services sont démarrés, vous pouvez accéder à DVWA à l'URL `localhost/DVWA`. Les identifiants de l'application sont `admin / password`.

L'environnement propose différents niveaux de difficulté pour chacune des vulnérabilités. Pour configurer le niveau de difficulté, vous pouvez accéder au menu intitulé "DVWA Security" et choisir la difficulté. Commencez par le niveau `low` pour chacune des vulnérabilités.