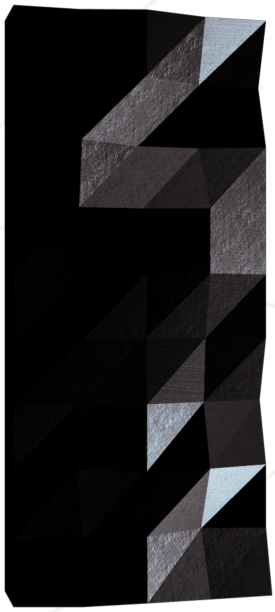

Bootcamp Cybersecurité | 42

Vaccine

Résumé: Injection SQL

Version: 1

Table des matières

Chapitre I

Introduction

Nous savons tous combien la programmation sécurisée est importante. Dans ce cas, vous allez essayer de trouver `des erreurs de filtrage dans l'entrée des données`. `L'injection SQL` est l'injection de commandes SQL pour modifier le comportement d'un programme et exécuter des commandes sur la base de données. Dans ce projet, vous allez créer un outil capable de détecter les injections SQL en fournissant une URL.

Chapitre II

Partie obligatoire

Nom de la fonction	`vaccine`
Fichiers de rendu	`Code source du programme, Makefile et documentation dans le fichier README.md`
Fonctions externes autorisées	
Description	`Détecter et réaliser une injection SQL`

L'outil doit disposer d'une batterie de tests à exécuter contre une URL donnée et, en fonction des réponses, être capable de détecter les injections SQL. Il est possible de détecter le type de moteur de base de données afin de rendre les tests plus performants (2 minimum). Les tests peuvent être basés sur plusieurs types : union, erreur, booléen, temps et même aveugle (2 minimum).

S'il est confirmé qu'un site web est vulnérable, on peut obtenir ce qui suit :

- Les paramètres vulnérables.
- La charge utile utilisée.
- Noms des bases de données.
- Noms des tables.
- Noms des colonnes.
- Vidage complet de la base de données.

L'outil doit avoir un fichier de stockage pour les données, s'il n'existe pas, il sera créé lors de la première exécution.

Le programme `vaccine` vous permettra de réaliser une injection SQL en fournissant une url en paramètre. Vous gérerez les options suivantes du programme :

```
./vaccine [-oP] URL
```

- Option `-o` : Fichier d'archive, s'il n'est pas spécifié, il sera stocké dans un fichier par défaut.
- Option `-X` : Type de demande, si non spécifié GET sera utilisé.

Vous pouvez utiliser n'importe quel langage de programmation, vous ne devez pas utiliser les bibliothèques qui automatisent l'injection SQL.

Chapitre III

Partie bonus

L'évaluation des bonus se fera `SI ET SEULEMENT SI` la partie obligatoire est `PARFAITE`. Dans le cas contraire, les bonus seront totalement `IGNORÉES`.

Vous pouvez améliorer votre projet grâce aux fonctionnalités suivantes :

- Un plus large éventail de moteurs de base de données.
- Un éventail plus large de méthodes d'injection SQL.
- L'outil vous permet de modifier divers paramètres de la demande, par exemple l'agent utilisateur.

Chapitre IV

Évaluations peer 2 peer

Ce projet sera corrigé par d'autres étudiants. Remettez les fichiers dans le dépôt Git et assurez-vous que tout fonctionne comme prévu.