NON-PRÉSENTÉ_CTF_SQLii-Alex

Titre du défi : [SQL Injection Initiation]

Description du défi : Un site web simple est fourni avec une fonction de recherche. Votre tâche est d'exploiter une vulnérabilité d'injection SQL pour accéder sans autorisation à des informations et trouver le flag.

Challenge peu original, non retenu

Instructions de configuration :
Le joueur reçoit l'URL d'un site web simple avec une fonction de recherche. Le site web est relié à une BDD SQL. L'attaque est lancée une fois le point d'injection découvert.

Le site web contient une page "search.php" qui prend une variable "term" via la méthode GET et l'utilise dans une requête SQL. Voici le code pertinent de la page "search.php":

```php
<?php
    $term = $_GET['term'];
    $query = "SELECT * FROM products WHERE name LIKE '%" . $term . "%'";
    // Execution de la requete

?>
```

Solution :

Étape 1 : Identifier la vulnérabilité
En examinant la fonctionnalité du site web et en testant la fonction de recherche avec diverses entrées, le joueur devrait être en mesure d'identifier que le site est vulnérable à l'injection SQL.

Étape 2 : Exploiter la vulnérabilité
Le joueur doit alors exploiter cette vulnérabilité en créant une entrée qui modifie la requête SQL de manière à révéler le flag. Par exemple, le joueur pourrait entrer le terme de recherche suivant :

```
%' UNION SELECT flag FROM flags; --
```

Cela va terminer la requête SQL originale et en démarrer une nouvelle qui sélectionne le flag de la table "flags". Le commentaire SQL (`--`) à la fin est utilisé pour ignorer le reste de la requête originale.

Étape 3 : Exécuter la commande
En exécutant la recherche avec le terme d'injection SQL, le joueur devrait voir le flag affiché

sur la page des résultats de la recherche.

Flag : [NHM2I{4L_C4p0n}]

Conclusion : [Ce challenge est conçu pour introduire les joueurs aux concepts de base de l'injection SQL. En exploitant une vulnérabilité d'injection SQL, les joueurs peuvent manipuler les requêtes SQL exécutées par le site web pour accéder à des informations qui ne sont normalement pas accessibles.]