Web Lab

Ce laboratoire fonctionne dans un environnement remote, des instructions / directives vous ont étés fournies pour accéder à l'infrastructure distante.

Introduction

Pour ce laboratoire il est fortement conseillé d'utiliser BurpSuite, la machine sur laquelle vous vous trouvez dispose de Burpsuite.

BurpSuite est un outil très puissant et massivement utilisé dans le cadre de tests d'application web. Nous vous recommandons de vous familiariser avec cet outil, il vous sera très utile pour ce laboratoire, de plus il existe de nombreux tutoriels sur internet sur son utilisation.

Burpsuite intègre un navigateur web qui est préconfiguré pour utiliser le proxy de Burpsuite, il est donc très facile de l'utiliser pour intercepter et modifier les requêtes HTTP.

Firefox est aussi disponible sur la machine, il faut néanmoins le configurer pour utiliser le proxy de Burpsuite.

Il vous a été fourni 2 IP par votre professeur de la forme :

172.22.100.x et 172.22.200.x

La première IP correspond à la machine attaquant sur laquelle vous devez vous connecter (Burpsuite et Firefox y sont installés).
L'autre machine est la machine ayant une application web vulnérable, elle est joignable sur le **port 3000.**

/ !\ Pour que les applications graphiques fonctionnent correctement merci d'éxécuter le script « clean.sh » lorsque vous vous connectez à la machine attaquant / !

« source ./clean.sh »

Warmup

Mauvaise validation d’inputs

En visitant le shop, vous ne l'aimez pas du tout, vous décidez donc le de faire savoir en postant un feedback.

1. Trouvez un moyen de poster un feedback avec une note de 0 étoile.

2. Quel est le problème dans l'implémentation du système de feedback ?

3. Trouvez un moyen de vous créer un compte admin

   Pour cette étape il est peut-être utile d'obtenir le schéma de la base de donnée que vous récupérerez dans la partie suivante !

4. Quel est le problème dans cet appel à l'API ?

Injection

Schéma de la base de donnée

Dans cette partie on souhaite récupérer le schéma de la base de donnée pour ensuite pouvoir "crafter" d'autres requêtes SQL pour récupérer des données.

5. Quel est le point d'entrée pour injecter du SQL ?

6. Quel est le moteur de la base de donnée ?

7. Quel est la requête utilisée de base pour récupérer un produit ?

8. En fonction du moteur de la base de donnée, existe-t-il des fonctions spécifiques pour récupérer le schéma de la base de donnée ? Ou existe-t-il une table contenant par exemple le script de création de la base de donnée ?

9. Trouvez un moyen de récupérer le schéma de la base de donnée.
   Hint: UNION SELECT '1', '2', '3', ... –

Récupération du compte admin

Maintenant que nous avons une bonne idée de la structure de la base de donnée, nous allons pouvoir récupérer des informations précises, tel que des comptes utilisateurs, notamment celui de l'administrateur.

On peut réutiliser le même point d'entrée que précédemment.

10. Trouvez un moyen de récupérer le compte admin.

11. Quel est le mot de passe de l'administrateur ?

JWT

Pour cette section Burpsuite propose des plugins pour manipuler les JWT (JWT Editor et/ou JSON Web Tokens), sinon vous pouvez utiliser jwt.io.

En vous connectant avec votre nouveau compte admin, vous remarquez que le site utilise des JWT pour gérer les sessions.

12. Quel est l'algorithme utilisé pour signer les JWT ?

13. Trouvez un moyen de vous connecter en tant que "jwtn3d@juice-sh.op" sans connaitre son mot de passe.

14. Montrez le payload du JWT utilisé

En utilisant DirBuster, vous trouvez un endpoint (/encryptionkeys) qui vous permet de récupérer des informations intéressantes.

15. Montrez que vous êtes capable de vous connecter en tant que "rsa_lord@juice-sh.op" en forgeant un nouveau JWT.
    Hint : https://portswigger.net/web-security/jwt/algorithm-confusion

16. Pourquoi êtes-vous capable de forger ce JWT, quel est le problème d'implémentation coté serveur ?