Service Lab

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

Introduction

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 »

L'application vulnérable mise à disposition propose un large éventail de fonctionnalités, nous allons nous concentrer sur la partie authentification. Plus spécifiquement sur l'implémentation du protocole d'autorisation Oauth2.

Si vous n'êtes pas familier avec Oauth, il est vivement conseillé de se renseigner sur ce protocole.
https://auth0.com/fr/intro-to-iam/what-is-oauth-2#

Analyse du code

Il existe des recommandations sur comment implémenter Oauth2, mais finalement libre aux développeurs d'implémenter de leurs côté la gestion de la création de comptes liés à Oauth2.

Typiquement une fois qu'un utilisateur utilise cette fonctionnalité pour se connecter, le backend peut stocker ce compte. À priori le backend n'a pas accès au mot de passe du compte google de l'utilisateur (voir fonctionnement Oauth2, tokens etc..).

Il est donc libre de stocker diverses informations relatives au compte (mail, information personnelles renvoyée par Oauth2).

Analysez le fichier main.js, notamment les fonctions liées à Oauth2. Quels sont les données que la backend stocke quand un utilisateur se connecte avec Oauth2 ?

Hint : Vous pouvez « prettifier » le code source, et faire des recherches dans le code (oauth, save …)

Quel mot de passe est stocké du côté backend pour un utilisateur ayant utilisé Oauth2 ?

Quel est le problème avec cette manière de faire ?

Exploitation

Vous savez que votre ami Bjoern utilise ce site internet, vous retrouvez son adresse e-mail dans votre liste de contact « bjoern.kimminich@gmail.com ».

Abusez de cette mauvaise implémentation pour vous connecter en tant que Bjoern.