**Projet Sécurité Informatique**

***ZENATI Mohamed***

***TEYEB Nidhal***

***MANKOUR Ines***

Le but de ce projet est d’implémenter une attaque sur une machine vulnérable et proposer une solution qui peut nous protéger contre cette attaque. Ce projet se réalise en plusieurs étapes. Nous présenterons ces étapes sous forme d’un tutoriel avec des captures d’écran.

**Etape 1 :** Création d’une simple page Web en PHP (sur WAMP)

Une image contenant texte

Description générée automatiquement

Cette page web qui a été faite en PHP (dont vous trouverez le code dans le fichier index.php) est une simple page de connexion classique.

**Etape 2 :** Création de notre DataBase

Une image contenant texte

Description générée automatiquement

Notre DataBase faite sur phpMyAdmin est tout aussi classique. En effet, on y a créer une simple table « users » contenant comme données des IDusers, un username et un password nous permettant de nous connecter à notre page web de connexion.

**Etape 3 :** Connexion entre notre DataBase et notre page Web

Une image contenant texte

Description générée automatiquement

Une fois la page web et la DataBase créer, il faut connecter les deux. Pour ça, dans notre script PHP on ajoute le code ci-dessus.

Etape 4 : Vérification de la connexion entre notre application web et notre DataBase

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Une fois la connexion faite, il faut maintenant tester notre page web. Pour cela, on entre un nom d’utilisateur et un mot de passe valide qu’on a créée dans notre DataBase afin de vérifier le succès de notre page Web. Le message « Bienvenue mohamed » montre bien que l’utilisateur mohamed a réussi à se connecter. Dans le second screen on entre un nom d’utilisateur et un mot de passe faux afin de voir si notre page web refuse bien l’accès à celui-ci. Le message « Mauvais nom d’utilisateur et/ou mot de passe ! » signifie qu’un utilisateur quelconque ne peut pas se connecter.

Ces deux screens montrent donc bien que la connexion entre notre DataBase et notre page Web est réussi !

**Etape 5 :** Injection SQL

Une image contenant texte

Description générée automatiquement

Pour cette partie, dans l’URL il faut mettre en commentaire la partie password, cela modifie la requête et il suffit donc d’avoir un username correct pour pouvoir nous connecter ! Pour supprimer le Password, ici on inclus « ‘%23 » dans l’URL devant le password. En requête SQL ce changement d’URL donne :

Une image contenant texte

Description générée automatiquement

**Etape 6 :** Comment éviter ça ?

Une image contenant texte

Description générée automatiquement

Pour prévenir les injections SQL, il faut faire appel aux requêtes préparées. Ce sont des requêtes dans lesquels les paramètres sont interprétés indépendamment de la requête elle-même. De cette manière, il est impossible d'effectuer des injections. Dans tous les systèmes de gestion de bases de données, deux méthodes sont utilisées : prepare() qui prépare la requête et execute() qui exécute la requête avec les paramètres.

La fonction mysqli\_real\_escape\_string permet d’ajouter un “\” devant un caractère spécial (par exemple des guillemets) afin d’en faire un caractère “neutre”

**FIN DU TUTO**