Sécurité des Réseaux - TP4

Injections SQL

Monroe Samuel

6 janvier 2016

1 Préambule

Ce tp est réalisé avec l'image Debian 2.6.32 fournie sur le site de Pentesterlab.

2 Fingerprinting

Le hostname ne fonctionnant pas, j'ai lancé le telnet sur 127.0.0.1 port 80.

La requête **GET** indique effectivement que le serveur tourne sous Apache 2.2.6 avec PHP 5.3.3.

3 Détection et exploitation d'injections SQL

3.1 Détection sur les entiers

La manipulation des entiers dans l'url peut mettre en lumière une faille sur la façon dont ils sont traités.
Dans ce cas-ci, on remarque qu'en tappant **?id=2-1** dans l'url, PHP traite cette valeur comme une soustraction et nous affiche la page correspondant à **?id=1**.

3.2 Détection sur les strings

L'ajout d'apostrophes dans l'url peut être utilisé pour tester les chaînes de caractères, si elles sont mal traitées, un seul apostrophe mettra fin à la requête et provoquera probablement une erreur. C'est également le cas ici.

4 Exploitation d'injections SQL

Nous avons donc ici découvert une faille sur la façon dont les entiers sont traités.

4.1 Utilisation du UNION

L'important est de trouver le nombre de colonnes.

La première façon est de faire UNION SELECT 1 en ajoutant à chaque fois un nombre en plus jusqu'à obtenir un résultat, ici il faut aller jusqu'à UNION SELECT 1,2,3,4, il y a donc 4 colonnes.

Cette information s'obtient aussi en utilisant ORDER BY, avec un nombre croissant jusqu'à obtenir une erreur, de nouveau ici on peut aller jusqu'à ORDER BY 4, ce qui signifie qu'il y a 4 colonnes.

4.2 Retrouver les informations

On sait que le serveur utilise PHP et MySQL, on va donc essayer d'injecter des fonctions propres à ces systèmes pour obtenir de l'info.

L'injection **UNION SELECT 1,@@version,3,4** nous ramène la version de PHP 5.1.63+squeeze1 à la place d'une image précédente.

Avec current_user(), on obtient **pentesterlab@localhost**

Et avec **database()** on découvre qu'elle s'apelle photoblog.

MySQL propose une table information_schema sur laquelle on va pouvoir aller rechercher les informations de la base de données.

En ayant accès aux tables et à leurs champs, on peut ensuite facilement générer la requête nous listant les users et leurs mots de passe, on obtient ici celui de l'admin en hash md5 8efe310f9ab3efeae8d410a8e0166eb2. Il suffit de le tapper sur Google pour avoir son reverse : **P4ssw0rd**

4.3 Utilisation des informations

On peut maintenant se connecter au compte admin, et profiter d'une faille dans l'upload de fichiers, et envoyer un script php qui lance la console.
De là, on a un accès direct au système Linux hôte du site web via une ligne de commande.