Anti Brute Force

Auteur : Weaponsb
Créé le : 20/06/2006 à 19h48
Modifié le : 02/12/2006 à 15h54
Noter et commenter ce tutorial
Imprimer ce tutorial

Vous vous apprêtez à lire un tutorial rédigé par un membre de ce site. Malgré tout le soin que ce membre a pu apporter au tutorial, nous ne pouvons pas garantir que les informations contenues sur cette page sont exactes à 100%. Merci de garder cela en tête lorsque vous lirez cette page ;o)

Bonjour chers ZéroS.
Aujourd'hui je vais vous proposer un tuto pour empêcher des personnes malveillantes d'essayer de casser les mots de passe de votre site Internet en utilisant la méthode du brute force.

Donc voilà comment faire ?

- Identifier l'ordinateur qui essaye de se logger
- Vérifier si il a déjà rentré plusieurs mdp faux
- En fonction du résultat lui autoriser ou non l'accés

Dans mon tuto il y aura la présence d'un système de login il ne sera pas expliqué ici car il n'y en a pas grande utilité je vous signale juste qu'il utilise mysql .

Sommaire du chapitre :

Le code

Tout d'abord il vous faudra créer une table mysql. Elle doit contenir les champs user(en texte), timestamp(en bigint(20)) et pour finir tentative(en decimal(10,0)).

Ensuite, il faut connaître la personne qui essaye de se logger. Nous allons utiliser les fonctions:

- gethostbyaddr => donne le DNS de l'adresse ip.
- REMOTE_ADDR => Avoir l'ip de l'utilisateur.

Code : PHP


```php
<?php
$user = gethostbyaddr(getenv('REMOTE_ADDR'));
```

Voilà maintenant on sait qui a essayé de se connecter

Code : PHP

```php
include ('./bdd.php'); //Identification et séléction de la Bdd mysql
$sql = mysql_query("SELECT * FROM log_brutf WHERE user='$user'") or die (mysql_error());
$sql_r = mysql_fetch_array($sql);
$temps = time();
$temps1 = $temps - 60;//Ici $temps1 vaut $temps - 60 donc l'heure actuelle moins 1 minute
(60 secondes). C'est le temps pendant lequel les erreurs de mots de passe peuvent être
effectuées.
```

Vous devriez en être à ce point là .

Bilan => utilisateur identifié et recherché dans la bdd.

Ensuite nous allons essayer de nous logger.

Code : PHP

```php
if ($sql_r['tentative'] < 4) // Si les tentatives de login sont inférieures à 5 (même si
la valeur et 4 au départ le champ 'tentative' n'a pas de valeur dans la bdd). Cette
valeur de 4 peut très bien être changée tout dépend de vous ;)
{
    $user_pseudo = mysql_real_escape_string($_POST['pseudo']);
    $user_pass = mysql_real_escape_string($_POST['pass']);
    $sql2 = mysql_query("SELECT user_pass FROM log_clients WHERE
user_pseudo='$user_pseudo'") or die (mysql_error());
    $sql2_r = mysql_fetch_array($sql2);
    $mdpmd5 = md5($_POST['pass']);
    if($sql2_r[0] == $mdpmd5)
/*----------------Si le mdp est bon on log l'utilisateur-------------------------*/
    {

    }
    else
/*----------------Si le mdp est faux => sécurité anti brute force--------------------*/
```

Voilà on a essayé de se logger. Aller on va dire que nous sommes **malveillants** et que nous avons utilisé un système de brute force pour essayer de nous logger. Bien sûr le mot de passe, à moins d'une chance inimaginable ne sera pas bon(une chance sur 2.4815578026752E+014 pour un mot de passe à 8 caractères alphanumérique).

Que va-t-il se passer maintenant ?

S'il y a eu plus de 1 minute depuis les 5 erreurs on remet la valeur de tentative à 0.

Code : PHP

```php
    {
        if ($temps1 >= $sql_r['timestamp'])
        {
            mysql_query("DELETE FROM log_brutf WHERE user='$user'") or die
(mysql_error());
        }
```

S'il n'y a jamais eu d'erreur alors on crée les valeurs dans la table de la bdd.

Code : PHP

```
        if ($sql_r['user'] != $user)
        {
            mysql_query("INSERT INTO log_brutf VALUES('$user','".time()."','')") or die
(mysql_error());
        }
```

Et s'il y a déjà eu une tentative on augmente la valeur de 1.

Code : PHP

```
            else // Sinon on augmente la valeur de tentative de 1
        {
            mysql_query("UPDATE log_brutf SET tentative=tentative++ WHERE user='$user'")
or die (mysql_error());
        }
    }
```

Maintenant rappelez vous, nous avions dit plus haut

Citation : plus haut

> // Si les tentatives de login sont inférieures à 5 (même si la valeur et 4 au départ le champ 'tentative' n'a pas de valeur dans la bdd).

Mais si elles sont égales à X (où X est le nombre de tentatives) ?

Il y a 2 solutions : soit ça fait plus de 60 secondes que les tentatives ont été faites et alors on supprime l'utilisateur de la bdd de brute force

Code : PHP

```
}
else
{
    if ($temps1 >= $sql_r['timestamp'])
    {
        mysql_query("DELETE FROM log_brutf WHERE user='$user'") or die (mysql_error());
    }
    else
    {
    // BRUTE FORCE
    }
}
?>
```

Si non, s'il y a eu plus de 5 tentatives en 60 secondes alors bah là c'est à vous de voir soit vous pouvez bannir l'utilisateur, soit vous pouvez laisser couler le mec va se casser les dents car il ne pourra faire que 5 tentatives toutes les 60 secondes ce qui sera extrêmement long et donc je pense qu'il finira par abandonner.

Corriger

Voilà je vous ait expliqué pas à pas le code donc je pense qu'il ne devrai pas avoir de problème
Voilà quand même tout le code .

Code : PHP

```
<?php
$user = gethostbyaddr(getenv('REMOTE_ADDR'));
include ('./bdd.php'); //Identification et séléction de la Bdd mysql
$sql = mysql_query("SELECT * FROM log_brutf WHERE user='$user'") or die (mysql_error());
$sql_r = mysql_fetch_array($sql);
$temps = time();
$temps1 = $temps - 60;//Ici $temps1 vaut $temps - 61 donc l'heure actuelle moins 1 minute
(60 secondes). C'est le temps pendant lequel les erreurs de mots de passe peuvent être
effectuées.
if ($sql_r['tentative'] < 4) // Si les tentatives de login sont inférieures à 5 (même si
la valeur et 4 au départ le champ 'tentative' n'a pas de valeur dans la bdd). Cette
valeur de 4 peut très bien être changée tout dépend de vous ;)
{
    $user_psedo = mysql_real_escape_string($_POST['psedo']);
    $user_pass = mysql_real_escape_string($_POST['pass']);
    $sql2 = mysql_query("SELECT user_pass FROM log_clients WHERE
user_psedo='$user_psedo'") or die (mysql_error());
    $sql2_r = mysql_fetch_array($sql2);
    $mdpmd5 = md5($_POST['pass']);
    if($sql2_r[1] == $mdpmd5)
/*----------------Si le mdp est bon on log l'utilisateur-------------------------*/
    {

    }
    else
/*----------------Si le mdp est faux => sécurité anti brute force--------------------*/
    {
        if ($temps1 >= $sql_r['timestamp'])
        {
            mysql_query("DELETE FROM log_brutf WHERE user='$user'") or die
(mysql_error());
        }
        if ($sql_r['user'] != $user)
        {
            mysql_query("INSERT INTO log_brutf VALUES('$user','".time()."','')") or die
(mysql_error());
        }
        else // Sinon on augmente la valeur de tentative de 1
        {
            mysql_query("UPDATE log_brutf SET tentative=tentative++ WHERE user='$user'")
or die (mysql_error());
        }
    }
}
else
{
    if ($temps1 >= $sql_r['timestamp'])
    {
        mysql_query("DELETE FROM log_brutf WHERE user='$user'") or die (mysql_error());
    }
    else
    {
    echo 'BRUTE FORCE';
    }
}
?>
```

Et voilà mon premier tuto de fini. Je pense avoir été assez clair et le code en lui même n'est pas très compliqué si jamais vous avez des améliorations à mon code et bien envoyez moi un mp , je suis ouvert à toutes remarques constructives.

Auteur : Weaponsb
Noter et commenter ce tutorial
Imprimer ce tutorial