

sqlsqlsql

发表于 2021-03-05 分类于 [Challenge](#) , [2020](#) , [SWPU CTF 2020](#) , [Web Challenge](#) | [2020](#) | [SWPU CTF 2020](#) | [Web](#) | [sqlsqlsql](#)

[点击此处](#) 获得更好的阅读体验

WriteUp来源

[官方WP](#)

题目考点

- SQL注入

解题思路

前言

此题参考了第三届CBCTF的sql-labs

过滤

自己测试可以发现如下过滤

□
□

解题思路

users表字段id, name, emile, salary

flllag表字段id, asuazttaz

查看源码可以获得提示

```
1 <!-- select * from users where id = '$id'-->
```

这个提示是想说明要闭合id字段的引号 结合页面的英文提示，很容易想到这个题是时间盲注

需要注意的点

- 用异或来闭合引号
- case when then else end来替代if
- 用join多个大表造成延时
- 通过mysql5.7的sys.schema_table_statistics_with_buffer表查询表名
- 通过无列名注入获取字段内容
- 通过括号，或者引号包裹来代替空格
- flllag表有两个字段且flag值在第二个字段
- 通过like或者regexp来匹配结果（但是这里不能用like，师傅们结合flag内容具体想想，卖个关子）

payload

两秒左右的延时，查表名

```
1 http://182.150.46.187:8801/ttttt/?id=1^(select(case'1'when((select(select(group_concat(table_name))from(sys.schema_table_statistics_with_buffer)where(table_schema=databas
```

查字段内容

```
1 http://182.150.46.187:8801/ttttt/?id=1^(select(case'1'when((select(select(group_concat(2))from(selectfrom(select(1))asa)join(select(2))asbunion(selectfrom(fillag)))asa)reg
```

脚本就不给了，因为这个题是0解，师傅们看payload自己重新做吧

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2020/SWPU-CTF-2020/Web/wNVhVQmbmi3yM5ilf7moa.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 #2020 #Web #SWPU CTF 2020](#)
[noobpy](#)
[find](#)