

# 2022虎符网络安全CTF部分wp（1）

原创

救救直男吧! 已于 2022-03-21 19:12:13 修改 1962 收藏 1

分类专栏: [2022虎符](#) 文章标签: [web安全](#) [安全](#) [数据库](#)

于 2022-03-21 17:22:29 首次发布

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\\_20737293/article/details/123640668](https://blog.csdn.net/qq_20737293/article/details/123640668)

版权



[2022虎符](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

## Misc | Plain Text

```
ZE9CUk8gUE9WQUxPV0FUWCBOQSBNQVReLCBXWSBET0xWTIKgUEVSRVdFU1RJIJFUTyBOQSBBTkdMSUpTS0IKIFFaWUsulHRX  
T0ogU0VLUKVUIFNPU1RPSVQgSVogRFdVSCBTTE9XLiB3U0UgQIVLV1kgU1RST15OWUuIHfCTE9eTIKIEFSQIVaLiB2RUxBRU0gV0  
FNIE9UTEIeTk9HTyBETIEu
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
dOBRO POVALOWATX NA MAT^, WY DOLVNY PEREWESTI \TO NA ANGLIJSKIJ QZYK. tWOJ SEKRET SOSTOIT IZ DWUH SLOW.  
wSE BUKWY STRO^NYE. qBLO^NYJ ARBUZ. vELAEM WAM OTLI^NOGO DNQ.
```

CSDN @救救直男吧!

进行base64解码

检测为波... 中文

通用领域 | 生物医学 | 金融财经

dOBRO POVALOWATX NA MAT^, WY DOLVNY PEREWESTI \TO NA ANGLIJSKIJ QZYK. tWOJ SEKRET SOSTOIT IZ DWUH SLOW. wSE BUKWY STRO^NYE. qBLO^NYJ ARBUZ. vELAEM WAM OTLI^NOGO DNQ.

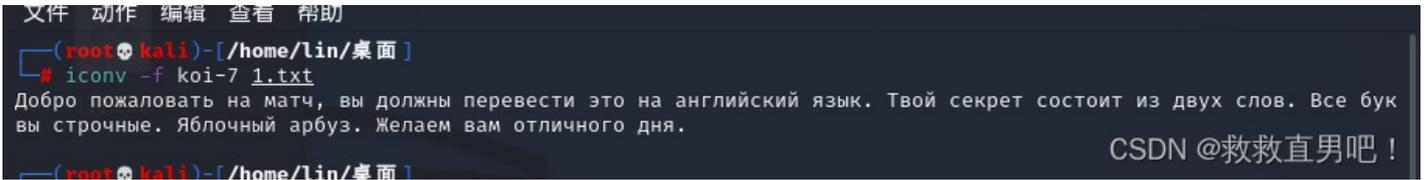
165/5000

好吧, 你们这些没用的家伙, 这是英国人的口头禅。你们的秘密是" Soto "和" dwuh slow "(西班牙语)(西班牙语)(西班牙语)(大意:新的一页, 新的一页, 新的一页, 新的一页, 新的一页, 新的西瓜)。

复制 反馈

CSDN @救救直男吧!

解码后尝试放到翻译软件



翻译软件判断为波兰语，但是翻译出来的语句不通顺，且有几个单词没翻译。所以判断是为其他语言编码。经过几次尝试，判断是俄语编码，找到俄语的编码方式用linux可编译

(这题有点坑，这个苹果西瓜一直连不起来，后面才看到\_)

HFCTF{apple\_watermelon}

## Misc | Quest-Crash

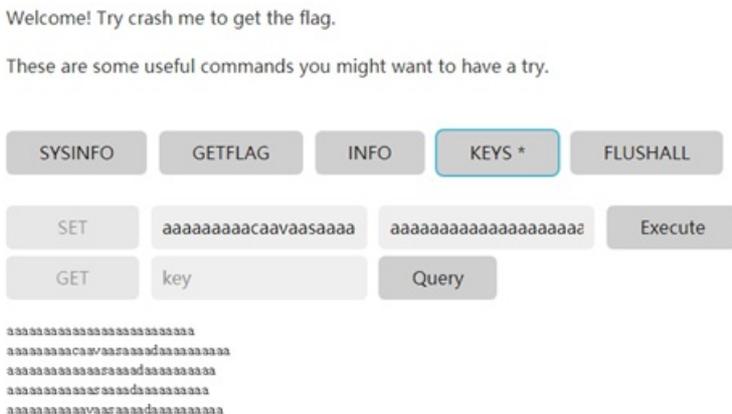
进到页面

### Crash me!



CSDN @救救直男吧!

Get方式尝试了下没什么作用，就试了一下SET请求。然后请求了几次发现，请求的数据都将呈现在页面上



CSDN @救救直男吧!

那我们可以打开bp，开启抓包，使用爆破功能一直往set输入数据，直到他溢出。Flag就出来了  
字典够大就行了，开始跑，set就会往里面存入数据

```
POST /sendreq HTTP/1.1
Host: 120.76.219.239:21713
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: */*
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
Referer: http://120.76.219.239:21713/
Content-Type: application/json
Origin: http://120.76.219.239:21713
Content-Length: 43
Connection: close

{"query": "SET \"/>

```

CSDN @救救直男吧！

Welcome! Try crash me to get the flag.

These are some useful commands you might want to have a try.

lianjue  
 liaozho  
 liaiwang  
 lianshao  
 liankang  
 liaina  
 liantong

CSDN @救救直男吧！

在info中，滑到最底下keys可以看存入了多少数据  
 只要value值大一点，写入的条数就可以少一点，  
 然后等着爆破就行

Welcome! Try crash me to get the flag.

These are some useful commands you might want to have a try.

### Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

CSDN @救救直男吧！

发现页面开始报错了，显示服务器内部错误。点击getflag，即可得到flag

## Misc | Quest-RCE

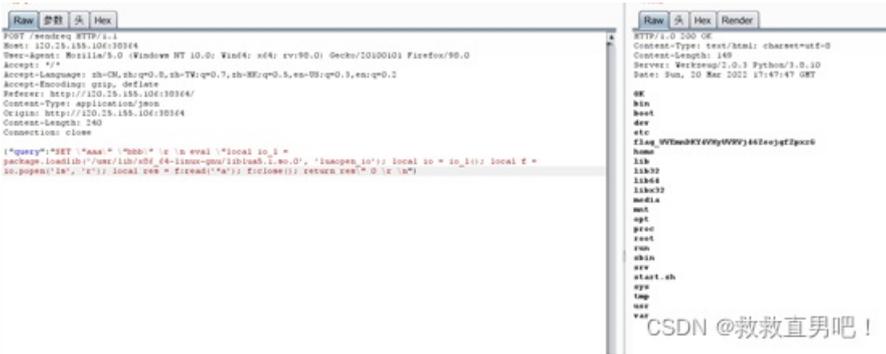
此题和前段时间爆出的（CVE-2022-0543）有相似之处，我们可以利用package提供的方法加载动态链库的函数，进行任意命令执行。

本次有参考CVE-2022-0543: <https://github.com/vulhub/vulhub/blob/master/redis/CVE-2022-0543/README.zh-cn.md>

Payload直接出。 题目和环境完全一致，都无需修改，lib路径，直接RCE。

然后通过%0a发现无果 \r\n 执行多条语句

执行ls, 查看目录



CSDN @救救直男吧!

发现了一个flag文件, 通过cat查看



CSDN @救救直男吧!

直接得到flag

明天更新web