2022虎符网络安全CTF部分wp（1）

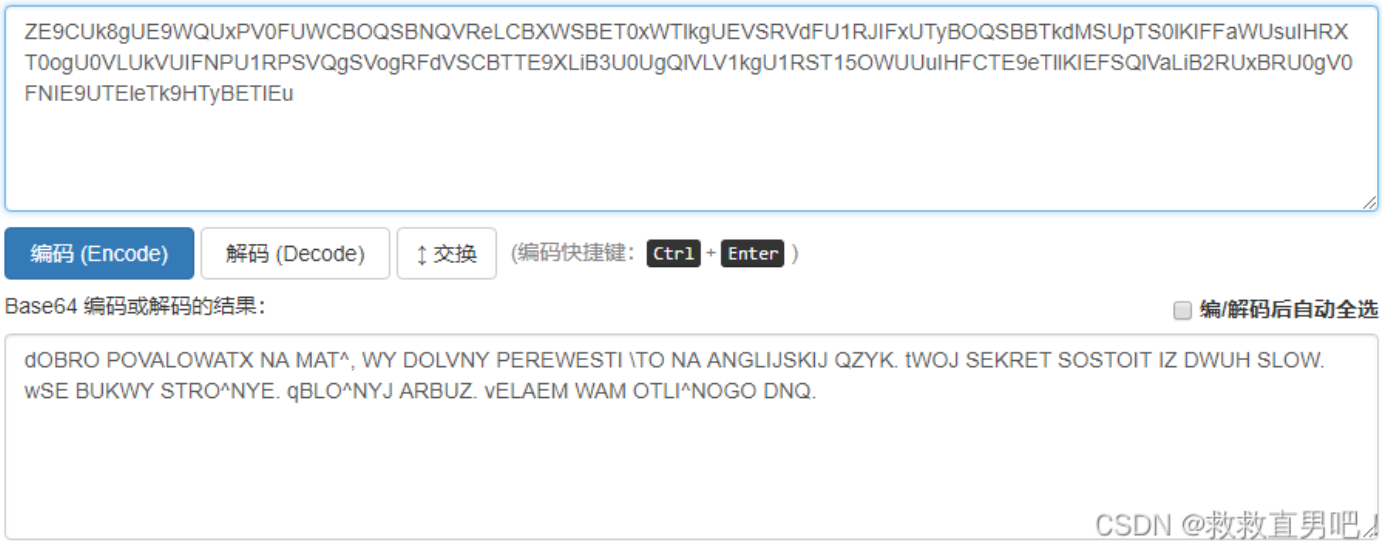
原创

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

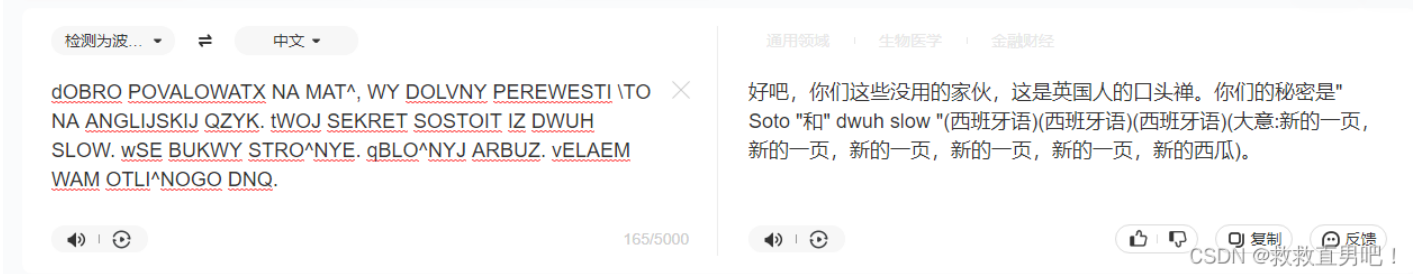
本文链接：https://blog.csdn.net/qq_20737293/article/details/123640668


2022虎符 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

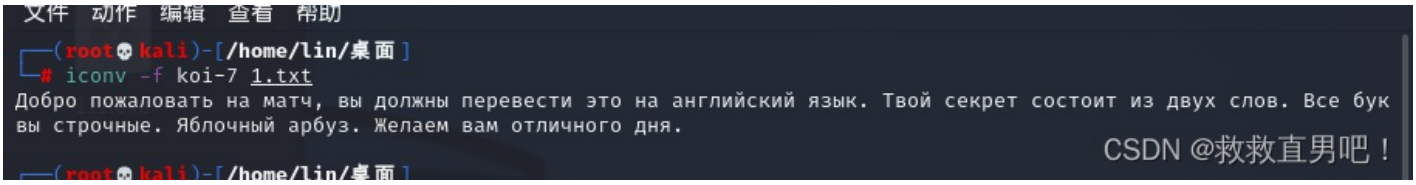
Misc | Plain Text



进行base64解码



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}

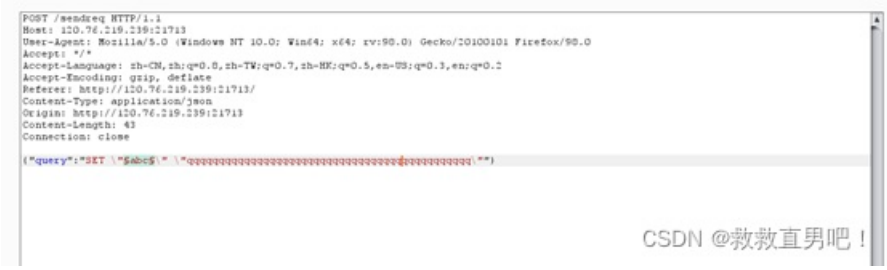
Misc | Quest-Crash

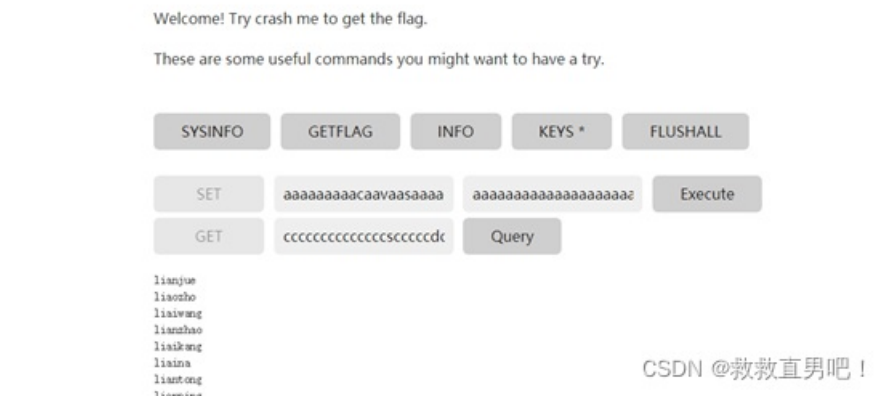
进到页面

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

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





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

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

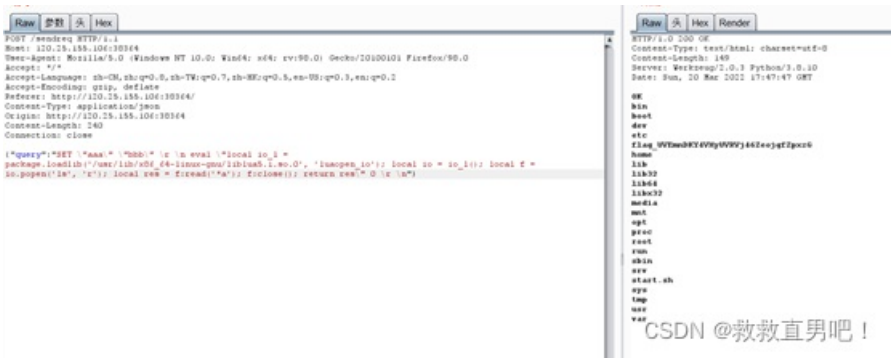
此题和前段时间爆出的（CVE-2022-0543）有相似之处，我们可以利用package提供的方法加载动态链库的函数，进行任意命令执行。

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



发现了一个flag文件，通过cat查看

直接得到flag

明天更新web