

周报

wsl

URL编码：

url编码又叫百分号编码，是统一资源定位(URL)编码方式。URL地址（常说网址）规定了常用地数字，字母可以直接使用，另外一批作为特殊用户字符也可以直接用（/,:@等），剩下的其它所有字符必须通过%xx编码处理。现在已经成为一种规范了，基本所有程序语言都有这种编码。

base32由A-Z、2-7和'='组成

base16由A-F、0-9组成

base100由表情组成

kali:unzip+ 文件名 解压压缩包

```
(kali㉿kali)-[~/桌面/new]
$ exiftool * | grep flag
XP Comment          : 恭喜你！找到一半了，还有另一半哦！flag{ae58d0408e26e8f
XP Comment          : 这是另一半flag : MjZhM2MwNTg5ZDIzZWRLZWN9
```

盲水印隐写：

隐藏式的水印是以数字数据的方式加入音频、图片或影片中，但在一般的状况下无法被看见。隐藏式水印的重要应用之一是保护版权，期望能借此避免或阻止数字媒体未经授权的复制和拷贝。工具:WaterMark JPG：开头：FF D8
结尾：FF D9 PNG：开头：89 50 4E 47 0D 0A 1A 0A 结尾：无 ZIP：开头：50 4B 03 04 结尾：无 RAR：开头：52 61 72 21 结尾：无

明文攻击：

题目：请攻击这个压缩包 压缩包内只有一个文件且真加密加密，暴力破解失败，发现加密方式为

flag.png*	5,335	5,323 PNG 图片文件	2022/11/3 8:47:24	Store ZipCrypto OS:Dos, UTF8...
-----------	-------	----------------	-------------------	---------------------------------

所以符合明文攻击条件，已知png文件的开头为89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 使用
kali:echo 89504E470D0A1A0A0000000D49484452 | xxd -r -ps > png_header 然后下载bkbrack，下载后将其复制到kali中解压，然后运行sudo cp ./bkcrack /usr/loacl/bin/ sudo chmod +x /usr/local/bin/bkcrack 将其写入系统命令 time bkcrack -C file.zip -c flag.png -p png_header -o 0 > 1.log& 查看破解进度：tail -f 1.log bkcrack -C

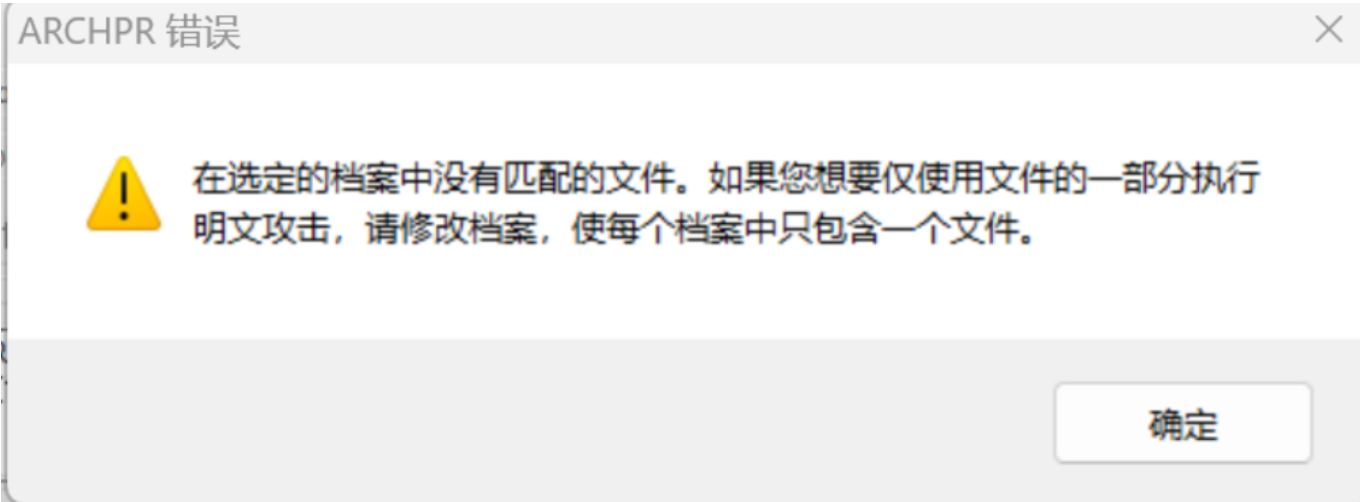


file.zip -c flag.png -k 92802c24 9955f8d6 65c652b8 -d 1.png

BugKu{不是非得两个文件你才能明文攻击}

明文攻击2：

题目：神秘的文件 下载后发现压缩包里有两个文件，且加密算法同上，满足明文攻击条件。将图片压缩用 ARCHPR进行明文攻击，却报错，因为明文压缩方式与flag.zip不同。



此题需要用WinRAR压缩，攻击得出口令

名称	压缩后大小	原始大小	类型
2018山东省大学生网络安全技能大赛决赛writeup....	259,726	272,070	DOCX 文档
logo.png*	27,405	27,870	PNG 图片文件

在文档中发现

⋮



哪有什么 WriteUP，别想了，老老实实做题吧！

~~~~~

改变字体颜色后

哪有什么 WriteUP，别想了，老老实实做题吧！

⋮



FLAG{fl4g\_is\_n0t\_here\_hhhhhhh!!!!}

但是flag不正确，用010打开png，发现里面有个压缩包

| 名称       | 压缩后大小 | 原始大小 | 类型 |
|----------|-------|------|----|
| docProps |       |      |    |

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==

解密结果 ↓  

一键解码:

解码结果 (注: 在线解密密码不参与一键解码)

base64解码:

flag{d0cX\_1s\_ziP\_file}

base32解码:

base16解码: