

# HGAME 2024

## WEEK 1

### WEB

#### ezHTTP

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET / HTTP/1.1 2 Host: 47.100.137.175:30126 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)   Chrome/116.0.5845.141 Safari/537.36 5 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app   lication/signed-exchange,v=b3;q=0.7 6 Accept-Encoding: gzip, deflate, br 7 Accept-Language: zh-CN,zh;q=0.9 8 Connection: close 9 Referer: vidar.club</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.1 Python/3.11.6 3 Date: Wed, 31 Jan 2024 12:55:24 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 536 6 Hint: Maybe you can try changing http request headers? 7 Connection: close 8 9 &lt;!DOCTYPE html&gt; 10 &lt;html&gt; 11   &lt;head&gt; 12     &lt;meta charset="utf-8"&gt; 13     &lt;meta name="viewport" content="width=device-width"&gt; 14     &lt;meta http-equiv="X-UA-Compatible" content="ie=edge"&gt; 15     &lt;meta name="description" content="Challenge"&gt; 16     &lt;title&gt;       ezHTTP     &lt;/title&gt; 17   &lt;/head&gt; 18   &lt;body&gt; 19     &lt;p&gt;       请从vidar.club访问这个页面     &lt;/p&gt; 20   &lt;/body&gt; 21 &lt;/html&gt; 22 &lt;style&gt; 23   *{ 24     margin:0; 25     padding:0; 26     box-sizing:border-box; 27   } 28   body{ 29     position:relative; 30     width:100vw; 31     height:100vh; 32     display:flex; 33     justify-content:center; 34     align-items:center;</pre>			

#### 添加Referer

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre>1 GET / HTTP/1.1 2 Host: 47.100.137.175:30126 3 Upgrade-Insecure-Requests: 1 4 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 5 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app   lication/signed-exchange,v=b3;q=0.7 6 Accept-Encoding: gzip, deflate, br 7 Accept-Language: zh-CN,zh;q=0.9 8 Connection: close 9 Referer: vidar.club</pre>				<pre>1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.1 Python/3.11.6 3 Date: Wed, 31 Jan 2024 12:56:49 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 645 6 Connection: close 7 8 &lt;!DOCTYPE html&gt; 9 &lt;html&gt; 10   &lt;head&gt; 11     &lt;meta charset="utf-8"&gt; 12     &lt;meta name="viewport" content="width=device-width"&gt; 13     &lt;meta http-equiv="X-UA-Compatible" content="ie=edge"&gt; 14     &lt;meta name="description" content="Challenge"&gt; 15     &lt;title&gt;       ezHTTP     &lt;/title&gt; 16   &lt;/head&gt; 17   &lt;body&gt; 18     &lt;p&gt;       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     &lt;/p&gt; 19   &lt;/body&gt; 20 &lt;/html&gt; 21 &lt;style&gt; 22   *{ 23     margin:0; 24     padding:0; 25     box-sizing:border-box; 26   } 27   body{ 28     position:relative; 29     width:100vw; 30     height:100vh; 31     display:flex; 32     justify-content:center; 33     align-items:center;</pre>			

#### 修改User-Agent

## Request

```
1 GET / HTTP/1.1
2 Host: 47.100.137.175:30126
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
  lication/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: zh-CN,zh;q=0.9
8 Connection: close
9 Referer:vidar.club
10 X-Real-IP:127.0.0.1
11
12
```

## Response

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.1 Python/3.11.6
3 Date: Wed, 31 Jan 2024 12:57:51 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 532
6 Hint: Not XFF
7 Connection: close
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <meta charset="utf-8">
13     <meta name="viewport" content="width=device-width">
14     <meta http-equiv="X-UA-Compatible" content="ie=edge">
15     <meta name="description" content="Challenge">
16     <title>
      ezHTTP
    </title>
17   </head>
18   <body>
19     <p>
      请从本地访问这个页面
    </p>
20   </body>
21 </html>
22 <style>
23   *{
24     margin:0;
25     padding:0;
26     box-sizing:border-box;
27   }
28   body{
29     position:relative;
30     width:100vw;
31     height:100vh;
32     display:flex;
33     justify-content:center;
    align-items:center;
  }
</style>
```

添加X-Real-IP:127.0.0.1

## Response

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.1 Python/3.11.6
3 Date: Wed, 31 Jan 2024 12:58:53 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 540
6 Authorization: Bearer
  eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJjcmVudCI6ImVudarOSx86bWV7SFRUUP8hc18xbVhAwc1Q0bnR9In0.VKmdRQ1lG6lJTRe
  FhmbcfIdq7MvJDncYpjaT7ztEDc
7 Connection: close
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <meta charset="utf-8">
13     <meta name="viewport" content="width=device-width">
14     <meta http-equiv="X-UA-Compatible" content="ie=edge">
15     <meta name="description" content="Challenge">
16     <title>
      ezHTTP
    </title>
17   </head>
18   <body>
19     <p>
      Ok, the flag has been given to you ^-^
    </p>
20   </body>
21 </html>
22 <style>
23   *{
24     margin:0;
25     padding:0;
26     box-sizing:border-box;
27   }
28   body{
29     position:relative;
30     width:100vw;
31     height:100vh;
32     display:flex;
33     justify-content:center;
    align-items:center;
  }
</style>
```

得到一串jwt token，解密后得到flag

## Bypass it

把浏览器js关了就能注册账号。登陆后得到flag。

## Select Courses

点击选课，抓包看到是访问了/api/courses

```
1 POST /api/courses HTTP/1.1
2 Host: 47.100.137.175:30836
3 Content-Length: 8
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://47.100.137.175:30836
8 Referer: http://47.100.137.175:30836/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13 {
14   "id":1
15 }
```

直接访问这里，抓包放进repeater多发几次包，发现"is\_full"有几率由true变为false，考虑尝试不断发选课的包看看能不能选上。

```
"description": "(Axxxxxxx) \u64cd\u4f5c\u7cfb\u7edf\u53ca\u5b89\u5168 - 3.0 \u5b66\u5206",
"id":5,
"is_full":false,
"location": "\u7b2c7\u6559\u7814\u697c\u5317000",
"name": "\u64cd\u4f5c\u7cfb\u7edf\u53ca\u5b89\u5168",
"sort": "\u5b66\u79d1\u5fc5\u4fee",
"status":false,
"time": "\u661f\u671f\u4e8c\u7b2c3-5\u8282 {1-16\u5468}"
```

用intruder的sniper模式，在User-Agent里随便加一个变量

Positions

Payloads

Resource pool

Settings

?

Choose an attack type

Attack type: 

Sniper

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

+

Target:

http://47.100.137.175:31687

1 POST /api/courses HTTP/1.1
2 Host: 47.100.137.175:31687
3 Content-Length: 8
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36 \$a\$
5 Content-Type: application/json
6 Accept: \*/\*
7 Origin: http://47.100.137.175:31687
8 Referer: http://47.100.137.175:31687/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13 {"id":1}

Positions

**Payloads**

Resource pool

Settings

?

**Payload sets**

You can define one or more payload sets. The number of payload sets de

Payload set:

1

▼

Payload count: 9,999,999

Payload type:

Numbers

▼

Request count: 9,999,999

?

**Payload settings [Numbers]**

This payload type generates numeric payloads within a given range and i

Number range

Type: ☒ Sequential ☐ Random

From:

1

To:

9999999

Step:

1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

0

Max integer digits:

7

Min fraction digits:

0

Max fraction digits:

0

Examples

1

7654321

这样设置

开始攻击，发现成功了。

## REVERSE

### ezIDA

拖进IDA直接能看到flag。

## ezUPX

先upx脱壳

```
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("Cooooo!You really know a little of UPX!");
18            return 0;
19        }
20    }
21    sub_140001020("Sry,try again plz...");
22    return 0;
23 }
```

脚本

```
#include<stdio.h>
#include<string.h>
int main(){
    char flag[]={
        100,
        123,
        118,
        115,
        96,
        73,
        101,
        93,
        69,
        19,
        107,
        2,
        71,
        109,
        89,
        92,
        2,
        69,
        109,
        6,
        109,
        94,
        3,
```

```

    70,
    70,
    94,
    1,
    109,
    2,
    84,
    109,
    103,
    98,
    106,
    19,
    79,
    50,
    0,};
int i;
for(i=0;i<strlen(flag);i++){
    flag[i]^=0x32;
}
printf("%s",flag);
return 0;
}

```

## ezASM

进行了异或0x22

脚本

```

#include<stdio.h>
int main(){
    int c[]={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};
    char flag[33];
    for(int i=0;i<33;i++){
        flag[i]=c[i]^0x22;
    }
    printf("%s",flag);
    return 0;
}

```

## ezPYC

反编译得到部分代码

```

flag = [
    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]
c = [
1,
2,
3,
4]
input = input('plz input flag:')

```

盲猜是异或，脚本

```

#include<stdio.h>
int main(){
    char flag[] = {
        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,  
2,0};  
int c[]={1,  
2,  
3,  
4};  
for(int i=0;i<38;i++){  
    flag[i]^=c[i%4];  
}  
printf("%s",flag);  
return 0;  
}
```

---