

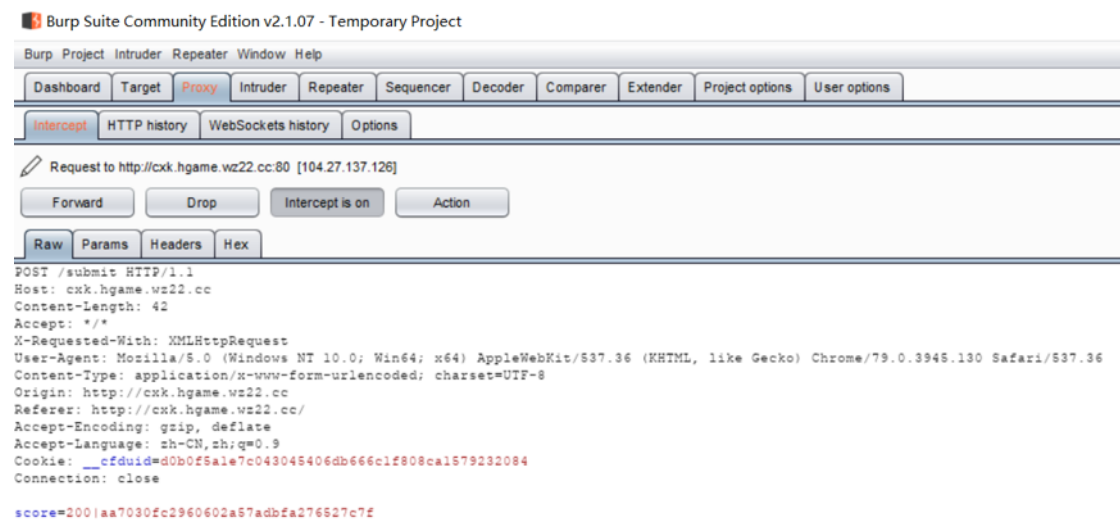
Web

4.尼泰玫：

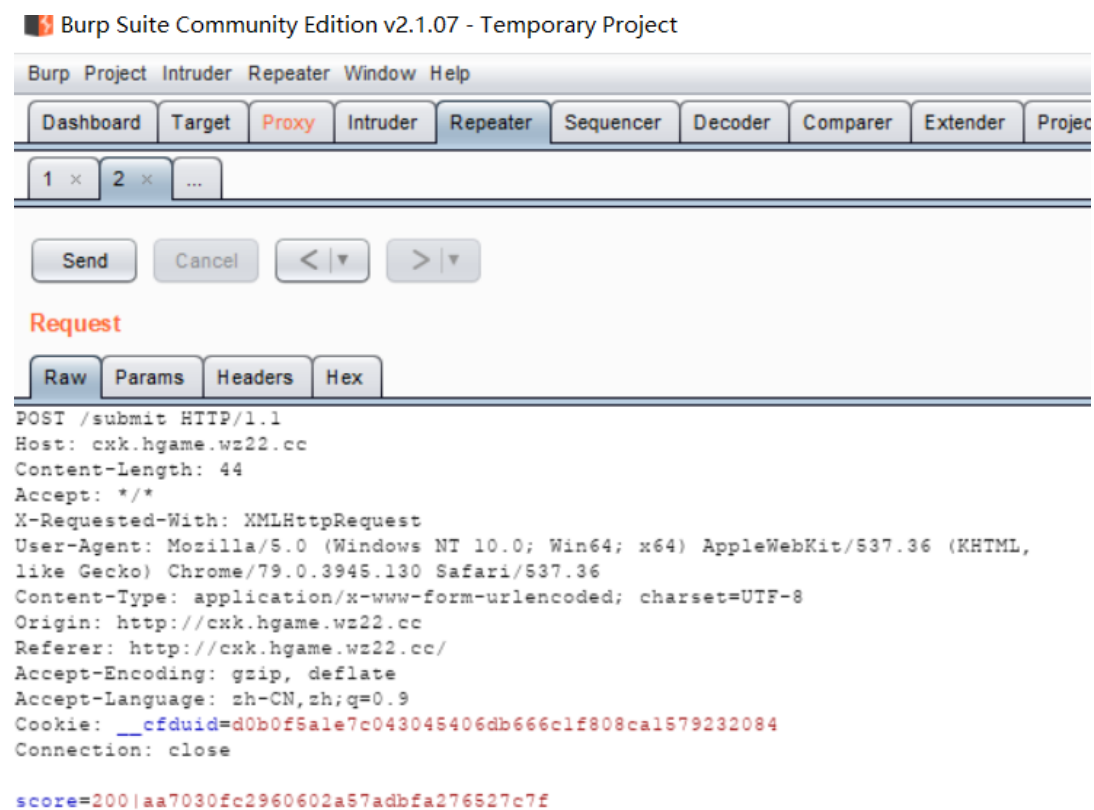
游戏要求得分在 30000 以上可以拿到 flag。

所以打开 burpsuite，设置代理，开始抓包。

开始游戏，然后轻松挂掉，同时 burpsuite 会显示



然后发送到 repeater,



接着修改 score 的值，使其大于 30000 再 send，便得到了 flag

Sniff Project: moudar Repeater window rep

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 x 2 x ...

Send Cancel < >

Target: http://cxk.hgame.wz22.cc

Request

Raw Params Headers Hex

```
POST /submit HTTP/1.1
Host: cxk.hgame.wz22.cc
Content-Length: 44
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cxk.hgame.wz22.cc
Referer: http://cxk.hgame.wz22.cc/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: __cfduid=d0b0f5ale7c043045406db666c1f808cal579232084
Connection: close

score=40000|aa7030fc2960602a57adbfa276527c75|
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Wed, 22 Jan 2020 14:45:45 GMT
Content-Type: text/plain; charset=utf-8
Connection: close
Access-Control-Allow-Origin: http://cxk.hgame.wz22.cc
Vary: Origin
Vary: Accept-Encoding
CF-Cache-Status: DYNAMIC
Alt-Svc: h3-24=":443"; ma=86400, h3-23=":443"; ma=86400
Server: cloudflare
CF-RAY: 6592503bfbblc991-SEA
Content-Length: 49

hgame{j4vASclpt_w1ll_tel1_y0u_someth1n9_u5efu1?!}
```

hgame{j4vASclpt\_w1ll\_tel1\_y0u\_someth1n9\_u5efu1?!}。(当然你可以选择老老实实地拿到30000分，滑稽.jpg)

Misc

## 1. 签到题

拿到一串字符串

Li0tIC4uLi0tIC4tLi4gLS4tLiAtLS0tLSAtLSAuIC4uLS0uLSAtIC0tLSAuLi0tLi0gLi4tLS0gLS0tLS0gLi4tLS0gLS0tLS0gLi4tLS4tIC4uLi4gLS0uIC4tIC0tIC4uLi0t

百度搜索了一下，找到一个类似的，说是 base64，那就转换一下，得到了摩斯密码，再用转换器转了，得到 hgame{W3LC0METO2020HGAM3}，原本满心欢喜，结果提交时怎么都不对，于是咨询了一下大佬，才知道中间下划线机器是不翻译的，所以要自己加上去。

最终 flag 为 hgame{W3LC0ME\_TO\_2020\_HGAM3}