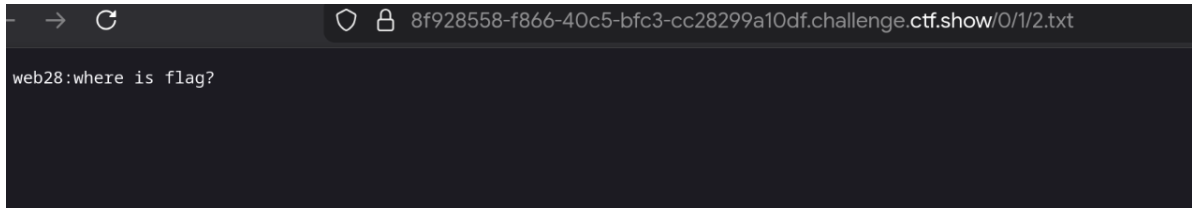
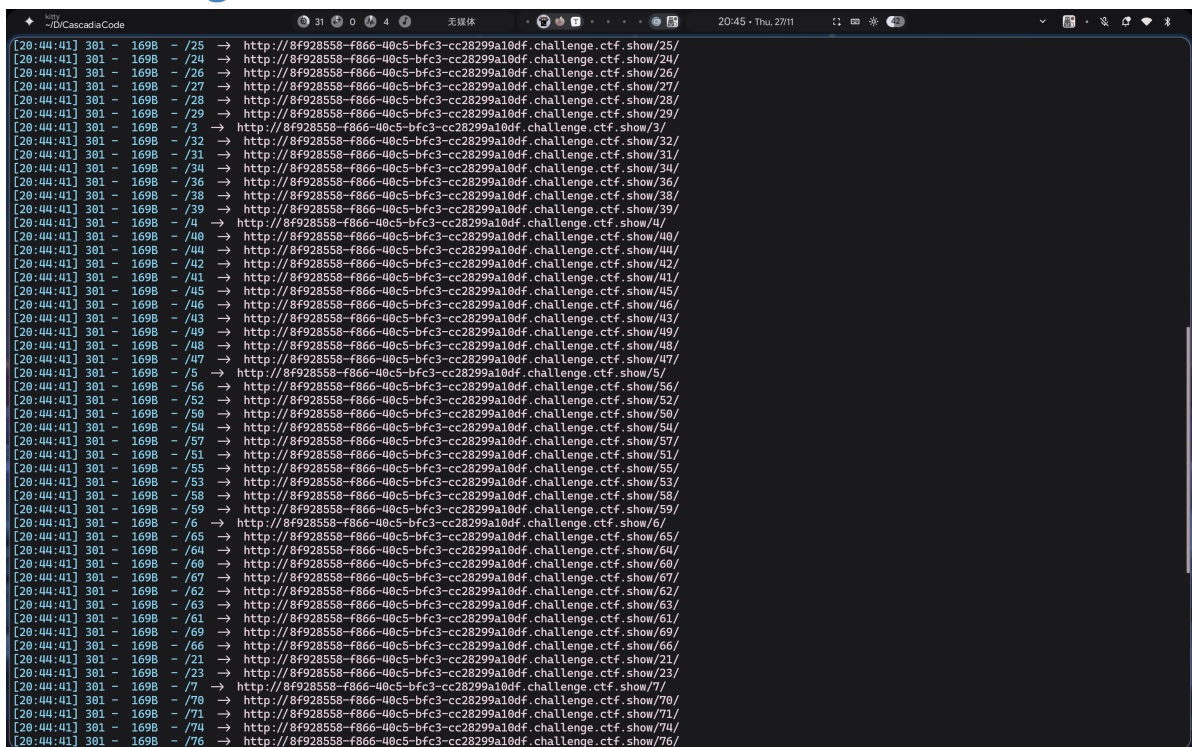


## 1.打开靶场，没有发现任何东西



## 2.先扫一下当前目录，发现好多文件夹

```
dirsearch -u https://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/
```

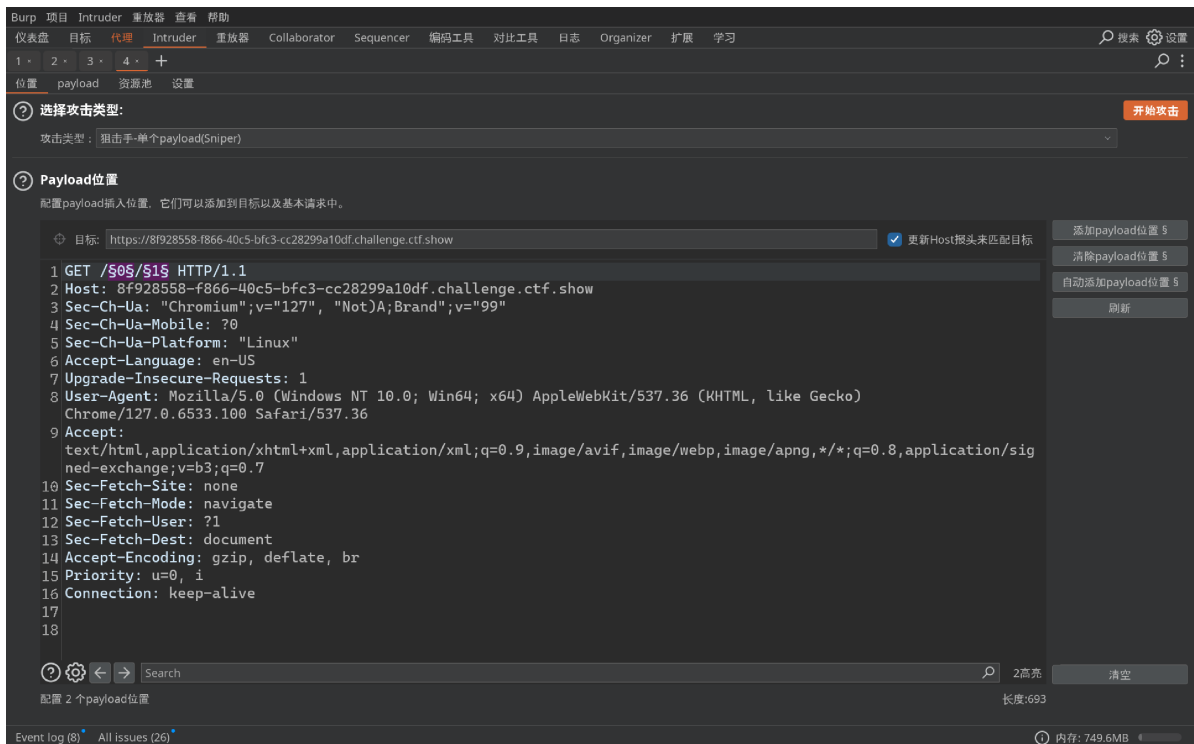


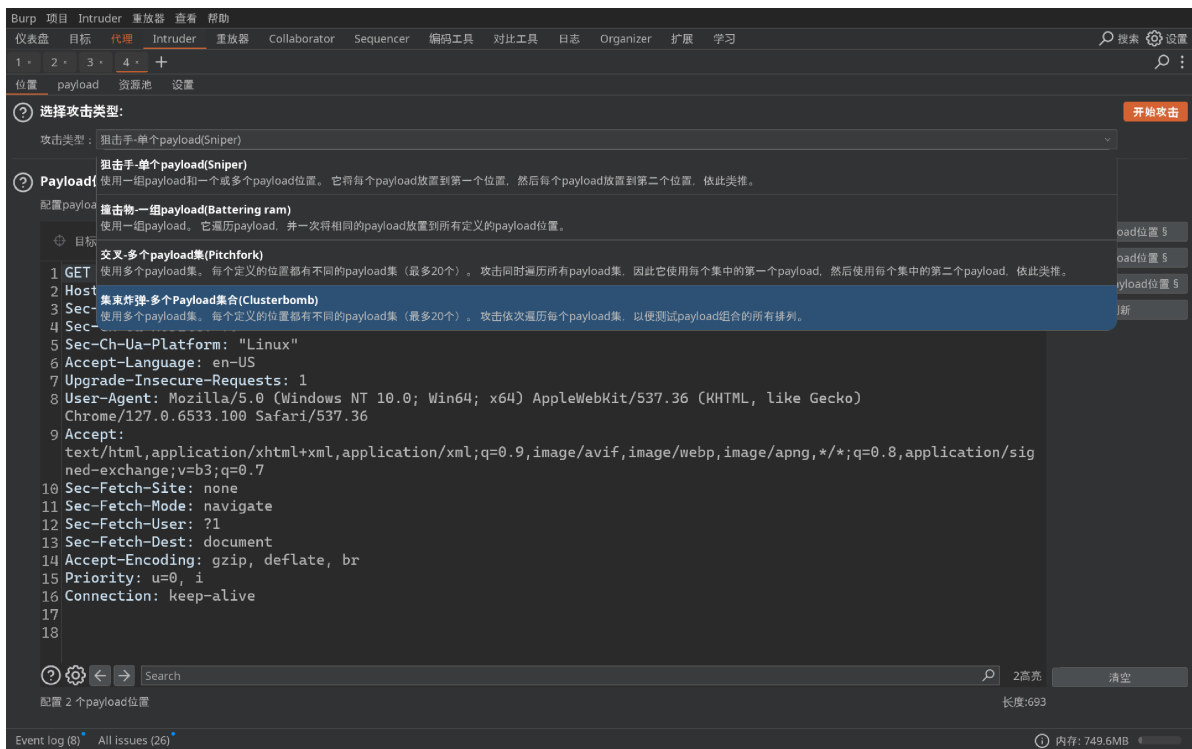
3.再随便扫一个文件夹，发现还是好多文件夹，还都是数字名字，得知这是要我们到目录海中爆破出flag

```
dirsearch -u https://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/
```

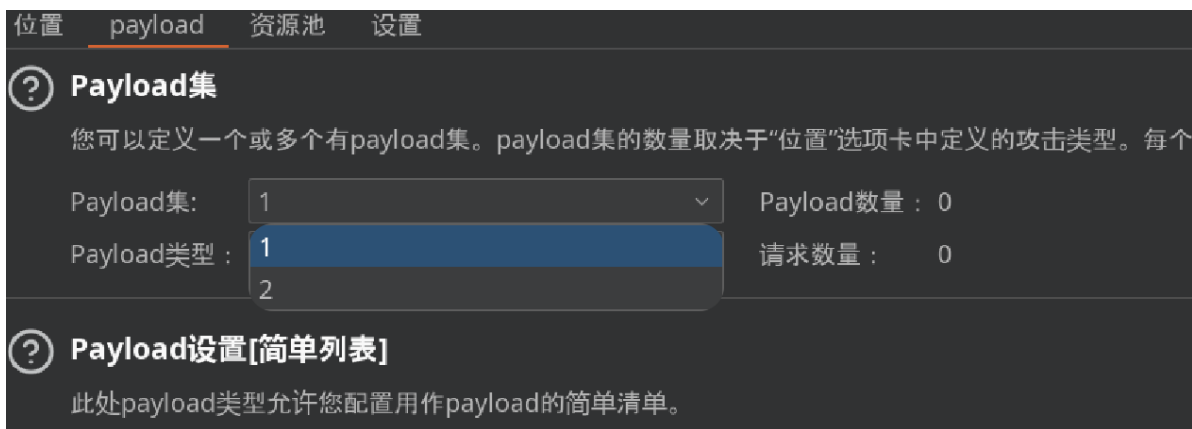
```
[20:47:09] 301 - 1698 - /0/19 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/19/
[20:47:09] 301 - 1698 - /0/2 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/2/
[20:47:09] 301 - 1698 - /0/20 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/20/
[20:47:09] 301 - 1698 - /0/22 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/22/
[20:47:09] 301 - 1698 - /0/21 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/21/
[20:47:09] 301 - 1698 - /0/25 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/25/
[20:47:09] 301 - 1698 - /0/23 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/23/
[20:47:09] 301 - 1698 - /0/24 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/24/
[20:47:09] 301 - 1698 - /0/26 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/26/
[20:47:09] 301 - 1698 - /0/29 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/29/
[20:47:09] 301 - 1698 - /0/27 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/27/
[20:47:09] 301 - 1698 - /0/3 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/3/
[20:47:09] 301 - 1698 - /0/32 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/32/
[20:47:09] 301 - 1698 - /0/30 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/30/
[20:47:09] 301 - 1698 - /0/31 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/31/
[20:47:09] 301 - 1698 - /0/34 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/34/
[20:47:09] 301 - 1698 - /0/35 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/35/
[20:47:09] 301 - 1698 - /0/36 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/36/
[20:47:09] 301 - 1698 - /0/37 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/37/
[20:47:09] 301 - 1698 - /0/38 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/38/
[20:47:09] 301 - 1698 - /0/39 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/39/
[20:47:09] 301 - 1698 - /0/4 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/4/
[20:47:09] 301 - 1698 - /0/40 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/40/
[20:47:09] 301 - 1698 - /0/41 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/41/
[20:47:09] 301 - 1698 - /0/43 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/43/
[20:47:09] 301 - 1698 - /0/42 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/42/
[20:47:09] 301 - 1698 - /0/45 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/45/
[20:47:09] 301 - 1698 - /0/46 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/46/
[20:47:09] 301 - 1698 - /0/47 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/47/
[20:47:09] 301 - 1698 - /0/48 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/48/
[20:47:09] 301 - 1698 - /0/49 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/49/
[20:47:09] 301 - 1698 - /0/5 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/5/
[20:47:09] 301 - 1698 - /0/52 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/52/
[20:47:09] 301 - 1698 - /0/50 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/50/
[20:47:09] 301 - 1698 - /0/51 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/51/
[20:47:09] 301 - 1698 - /0/55 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/55/
[20:47:09] 301 - 1698 - /0/54 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/54/
[20:47:09] 301 - 1698 - /0/53 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/53/
[20:47:09] 301 - 1698 - /0/56 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/56/
[20:47:09] 301 - 1698 - /0/58 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/58/
[20:47:09] 301 - 1698 - /0/57 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/57/
[20:47:09] 301 - 1698 - /0/59 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/59/
[20:47:09] 301 - 1698 - /0/6 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/6/
[20:47:09] 301 - 1698 - /0/60 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/60/
[20:47:09] 301 - 1698 - /0/63 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/63/
[20:47:09] 301 - 1698 - /0/61 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/61/
[20:47:09] 301 - 1698 - /0/62 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/62/
[20:47:09] 301 - 1698 - /0/64 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/64/
[20:47:09] 301 - 1698 - /0/69 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/69/
[20:47:09] 301 - 1698 - /0/7 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/7/
[20:47:09] 301 - 1698 - /0/65 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/65/
```

## 4.用bp抓包，先爆破两层目录，添加上两个“payload位置”，攻击类型选择“集束炸弹”





5.进入payload模块，这时候我们发现Payload集有两个，这是因为我们加了两个payload位置加payload类型为集束炸弹，接下来要设置两个payload集



6.第一个payload集设置为“数值”类型，范围为0-99(因为扫描的目录中没有超过100的名字，缩短一下爆破时间)

?

Payload集

您可以定义一个或多个有payload集。payload集的数量取决于“位置”选项卡中定义的

Payload集:

1

▼

Payload数量 : 100

Payload类型 :

数值

▼

请求数量 : 0

?

Payload settings [Numbers]

生成给定范围内指定格式的有效数值内容。

数字范围

类型:

☒ 顺序 ☐ 随机

从:

0

到(To):

99

间隔:

1

数量 :

数值格式

7.第二个payload设置根第一个一样

?

Payload集

您可以定义一个或多个有payload集。payload集的数量取决于“位置”选

Payload集:

2

▼

Payload

Payload类型 :

数值

▼

请求数量

?

Payload settings [Numbers]

生成给定范围内指定格式的有效数值内容。

数字范围

类型:

☒ 顺序 ☐ 随机

从:

0

到(To):

99

间隔:

1

数量 :

8.开始攻击，成功了在/72/20/中，这次设置为升序可以直接找到，查看响应得到flag

攻击 保存

7. Intruder attack of https://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show

攻击 保存

结果 位置 payload 资源池 设置

Intruder attack results filter: 显示所有条目

请求	Payload 1	Payload 2	状态码	接收到响应	错误	超时	长度 ^	注释
2073	72	20	200	37			671	
9465	64	94	403	42			1048	
9485	84	94	403	31			1048	
9577	76	95	403	29			1048	
9937	36	99	403	35			1048	
0			403	34			1053	
1	0	0	403	33			1053	
2	1	0	403	41			1053	
3	2	0	403	34			1053	

请求 响应

美化 Raw Hex

1 GET /72/20/ HTTP/1.1  
2 Host: 8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show  
3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"  
4 Sec-Ch-Ua-Mobile: ?0  
5 Sec-Ch-Ua-Platform: "Linux"  
6 Accept-Language: en-US  
7 Upgrade-Insecure-Requests: 1,,  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36  
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7  
10 Sec-Fetch-Site: none  
11 Sec-Fetch-Mode: navigate  
12 Sec-Fetch-User: ?1  
13 Sec-Fetch-Dest: document  
14 Accept-Encoding: gzip, deflate, br  
15 Priority: u=0, i

0高亮

已完成

攻击 保存

7. Intruder attack of https://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show

攻击 保存

结果 位置 payload 资源池 设置

Intruder attack results filter: 显示所有条目

请求	Payload 1	Payload 2	状态码	接收到响应	错误	超时	长度 ^	注释
2073	72	20	200	37			671	
9465	64	94	403	42			1048	
9485	84	94	403	31			1048	
9577	76	95	403	29			1048	
9937	36	99	403	35			1048	
0			403	34			1053	
1	0	0	403	33			1053	
2	1	0	403	41			1053	
3	2	0	403	34			1053	

请求 响应

美化 Raw Hex 页面渲染

1 HTTP/1.1 200 OK  
2 Server: nginx/1.20.1  
3 Date: Thu, 27 Nov 2025 13:06:08 GMT  
4 Content-Type: text/html; charset=UTF-8  
5 Connection: keep-alive  
6 X-Powered-By: PHP/7.3.11  
7 Access-Control-Allow-Methods: GET,POST,PUT,DELETE,OPTIONS  
8 Access-Control-Allow-Credentials: true  
9 Access-Control-Expose-Headers: Content-Type,Cookies,Aaa,Date,Server,Content-Length,Connection  
10 Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization,x-auth-token,Cookies,Aaa,Date,Server,Content-Length,Connection  
11 Access-Control-Max-Age: 1728000  
12 Content-Length: 45  
13  
14 ctفشow{9aac8991-2991-4721-9c08-c01f5b5278c8}

0高亮

已完成