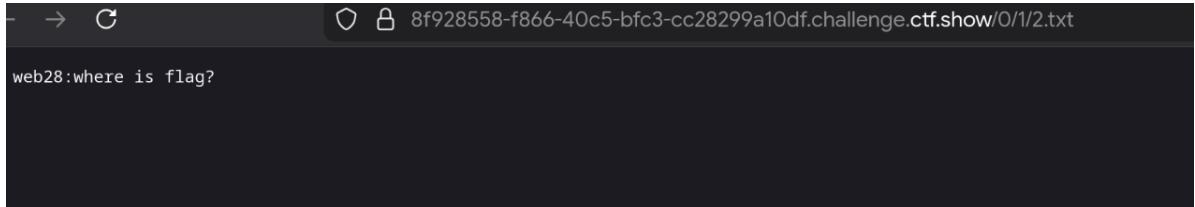


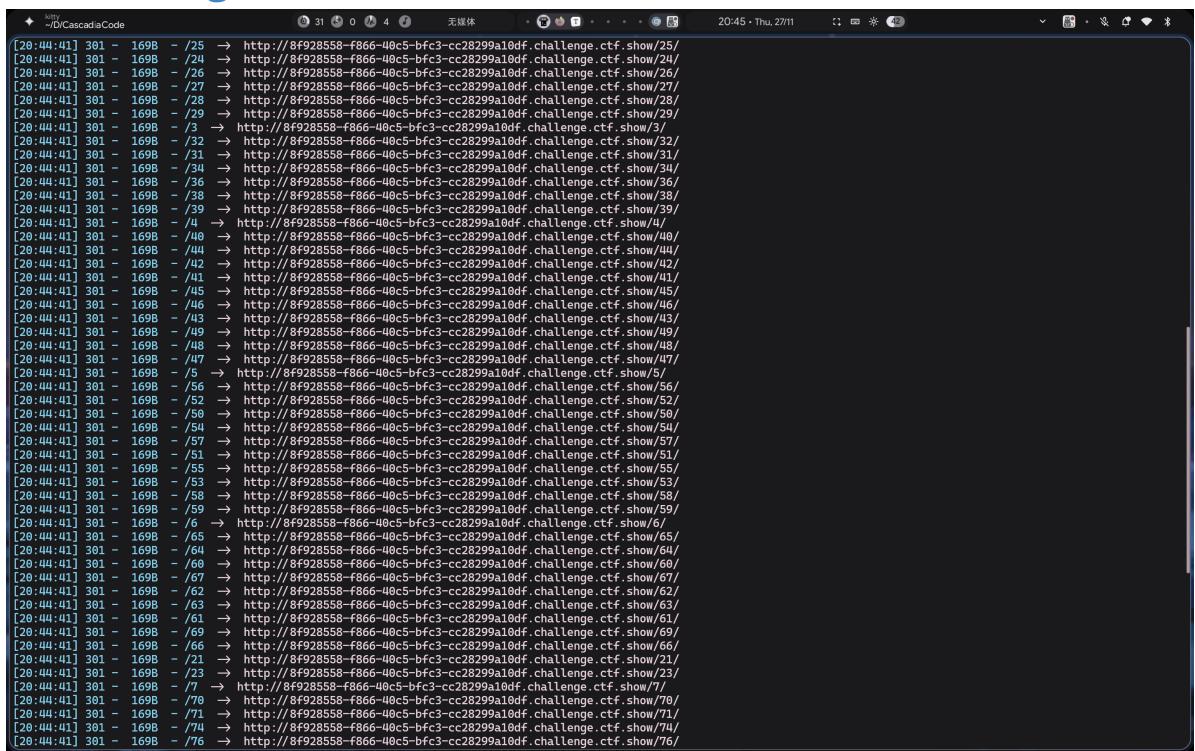
# 1. 打开靶场，没有发现任何东西



```
web28:where is flag?
```

# 2. 先扫一下当前目录，发现好多文件夹

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

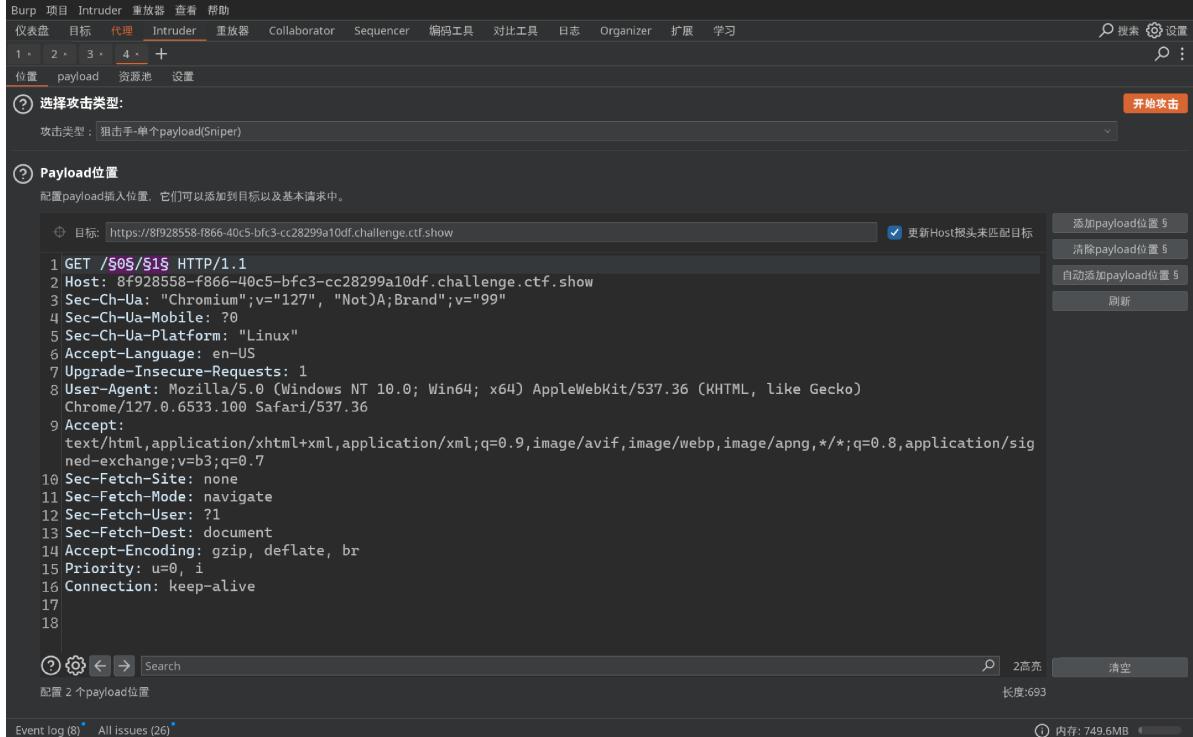


```
[29:44:41] 301 - 1698 - /25 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/25/[29:44:41] 301 - 1698 - /24 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/24/[29:44:41] 301 - 1698 - /26 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/26/[29:44:41] 301 - 1698 - /27 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/27/[29:44:41] 301 - 1698 - /28 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/28/[29:44:41] 301 - 1698 - /29 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/29/[29:44:41] 301 - 1698 - /3 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/3/[29:44:41] 301 - 1698 - /32 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/32/[29:44:41] 301 - 1698 - /31 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/31/[29:44:41] 301 - 1698 - /34 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/34/[29:44:41] 301 - 1698 - /36 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/36/[29:44:41] 301 - 1698 - /38 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/38/[29:44:41] 301 - 1698 - /39 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/39/[29:44:41] 301 - 1698 - /4 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/4/[29:44:41] 301 - 1698 - /40 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/40/[29:44:41] 301 - 1698 - /44 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/44/[29:44:41] 301 - 1698 - /42 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/42/[29:44:41] 301 - 1698 - /41 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/41/[29:44:41] 301 - 1698 - /45 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/45/[29:44:41] 301 - 1698 - /46 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/46/[29:44:41] 301 - 1698 - /43 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/43/[29:44:41] 301 - 1698 - /49 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/49/[29:44:41] 301 - 1698 - /48 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/48/[29:44:41] 301 - 1698 - /47 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/47/[29:44:41] 301 - 1698 - /5 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/5/[29:44:41] 301 - 1698 - /56 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/56/[29:44:41] 301 - 1698 - /52 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/52/[29:44:41] 301 - 1698 - /58 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/58/[29:44:41] 301 - 1698 - /54 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/54/[29:44:41] 301 - 1698 - /57 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/57/[29:44:41] 301 - 1698 - /51 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/51/[29:44:41] 301 - 1698 - /55 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/55/[29:44:41] 301 - 1698 - /53 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/53/[29:44:41] 301 - 1698 - /58 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/58/[29:44:41] 301 - 1698 - /59 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/59/[29:44:41] 301 - 1698 - /6 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/6/[29:44:41] 301 - 1698 - /65 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/65/[29:44:41] 301 - 1698 - /64 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/64/[29:44:41] 301 - 1698 - /66 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/66/[29:44:41] 301 - 1698 - /67 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/67/[29:44:41] 301 - 1698 - /62 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/62/[29:44:41] 301 - 1698 - /63 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/63/[29:44:41] 301 - 1698 - /61 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/61/[29:44:41] 301 - 1698 - /69 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/69/[29:44:41] 301 - 1698 - /66 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/66/[29:44:41] 301 - 1698 - /21 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/21/[29:44:41] 301 - 1698 - /23 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/23/[29:44:41] 301 - 1698 - /7 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/7/[29:44:41] 301 - 1698 - /71 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/71/[29:44:41] 301 - 1698 - /74 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/74/[29:44:41] 301 - 1698 - /76 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/76/
```

# 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.ctf.show/0/
```

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)

## ② 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   |

## ② 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设置跟第一个一样

## ② 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数量 : | 100 |
| Payload类型 : | 数值 | 请求数量 :      | 0   |

## ② 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

结果 | Payload 1 | Payload 2 | 状态码 | 接收到响应 | 错误 | 超时 | 长度 | 注释

| 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.ctf.show
3 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?
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
```

② ⚙️ ← → Search 0高亮 已完成

结果 | Payload 1 | Payload 2 | 状态码 | 接收到响应 | 错误 | 超时 | 长度 | 注释

| 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 ctfshow{9aac8991-2991-4721-9c08-c01f5b5278c8}
```

② ⚙️ ← → Search 0高亮 已完成