

## 1.打开靶场，没有发现任何东西

```
→ ↻ 8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/1/2.txt  
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.challenge.ctf.show/>

```
~/D/CascadiaCode 31 0 4 无媒体 20:45 · Thu, 27/11  
[20:44:41] 301 - 1698 - /25 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/25/  
[20:44:41] 301 - 1698 - /24 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/24/  
[20:44:41] 301 - 1698 - /26 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/26/  
[20:44:41] 301 - 1698 - /27 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/27/  
[20:44:41] 301 - 1698 - /28 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/28/  
[20:44:41] 301 - 1698 - /29 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/29/  
[20:44:41] 301 - 1698 - /3 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/3/  
[20:44:41] 301 - 1698 - /32 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/32/  
[20:44:41] 301 - 1698 - /31 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/31/  
[20:44:41] 301 - 1698 - /34 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/34/  
[20:44:41] 301 - 1698 - /36 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/36/  
[20:44:41] 301 - 1698 - /38 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/38/  
[20:44:41] 301 - 1698 - /39 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/39/  
[20:44:41] 301 - 1698 - /4 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/4/  
[20:44:41] 301 - 1698 - /40 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/40/  
[20:44:41] 301 - 1698 - /44 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/44/  
[20:44:41] 301 - 1698 - /42 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/42/  
[20:44:41] 301 - 1698 - /41 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/41/  
[20:44:41] 301 - 1698 - /45 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/45/  
[20:44:41] 301 - 1698 - /46 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/46/  
[20:44:41] 301 - 1698 - /43 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/43/  
[20:44:41] 301 - 1698 - /49 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/49/  
[20:44:41] 301 - 1698 - /48 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/48/  
[20:44:41] 301 - 1698 - /47 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/47/  
[20:44:41] 301 - 1698 - /5 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/5/  
[20:44:41] 301 - 1698 - /56 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/56/  
[20:44:41] 301 - 1698 - /45 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/52/  
[20:44:41] 301 - 1698 - /50 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/50/  
[20:44:41] 301 - 1698 - /54 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/54/  
[20:44:41] 301 - 1698 - /57 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/57/  
[20:44:41] 301 - 1698 - /51 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/51/  
[20:44:41] 301 - 1698 - /55 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/55/  
[20:44:41] 301 - 1698 - /53 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/53/  
[20:44:41] 301 - 1698 - /52 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/58/  
[20:44:41] 301 - 1698 - /59 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/59/  
[20:44:41] 301 - 1698 - /6 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/6/  
[20:44:41] 301 - 1698 - /65 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/65/  
[20:44:41] 301 - 1698 - /64 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/64/  
[20:44:41] 301 - 1698 - /60 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/60/  
[20:44:41] 301 - 1698 - /67 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/67/  
[20:44:41] 301 - 1698 - /58 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/62/  
[20:44:41] 301 - 1698 - /63 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/63/  
[20:44:41] 301 - 1698 - /61 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/61/  
[20:44:41] 301 - 1698 - /69 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/69/  
[20:44:41] 301 - 1698 - /66 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/66/  
[20:44:41] 301 - 1698 - /21 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/21/  
[20:44:41] 301 - 1698 - /23 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/23/  
[20:44:41] 301 - 1698 - /71 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/71/  
[20:44:41] 301 - 1698 - /70 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/70/  
[20:44:41] 301 - 1698 - /71 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/71/  
[20:44:41] 301 - 1698 - /74 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/74/  
[20:44:41] 301 - 1698 - /76 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/76/  
[20:44:41] 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.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 - /0/31 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/31/
[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 - /0/33 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/33/
[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 - /0/44 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/44/
[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 - /0/57 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/57/
[20:47:09] 301 - 1698 - /0/58 → http://8f928558-f866-40c5-bfc3-cc28299a10df.challenge.ctf.show/0/58/
[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”

The screenshot shows the Burp Suite interface with the 'Payload Position' configuration window open. The 'Attack Type' is set to 'Sniper' and the 'Payload Position' is configured with a target URL and a list of HTTP headers. The headers include GET /\$05/\$1\$, Host, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Accept-Language, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Accept-Encoding, Priority, and Connection.



**? 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”选项卡中定义的

Payload集: 2 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:

## 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

The screenshot shows the Burp Suite interface for an intruder attack. The table below represents the 'Intruder attack results' shown in the image.

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	

The response for the successful request (2073) is shown below:

```
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
```

The screenshot shows the Burp Suite interface for an intruder attack. The table below represents the 'Intruder attack results' shown in the image.

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	

The response for the successful request (2073) is shown below:

```
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,Cookie,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,Coo
  kies,Aaa,Date,Server,Content-Length,Connection
11 Access-Control-Max-Age: 1728000
12 Content-Length: 45
13
14 ctshow{9aac8991-2991-4721-9c08-c01f5b5278c8}
```