

## 1.打开靶场，盲猜username为admin

🌐 99994f00-94be-44b4-9907-f3be9a62ce0a.challenge.ctf.show

此网站要求您登录。

用户名

密码

取消 登录

## 2.打开bp，随便输入密码，进行抓包，发现我们发送过去的内容被base64编码了，还用了:分割

The screenshot shows a web browser's developer tools with the 'Request' tab selected. The request is a GET to the URL `99994f00-94be-44b4-9907-f3be9a62ce0a.challenge.ctf.show`. The 'Authorization' header is set to `Basic YWRtaW46MTIz`. The 'Inspector' panel on the right shows the selected text `YWRtaW46MTIz` decoded from Base64 to `admin:123`.

**请求**

美化 Raw Hex

```
1 GET / HTTP/1.1
2 Host: 99994f00-94be-44b4-9907-f3be9a62ce0a.challenge.ctf.show
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46MTIz
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 1
10 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
11 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
12 Sec-Fetch-Site: none
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18 Connection: keep-alive
19
20
```

**Inspector**

选择 12 (0xc)

选中文本

YWRtaW46MTIz

解码: Base64

admin:123

取消 应用变更

请求属性 2

请求查询参数 0

请求主体参数 0

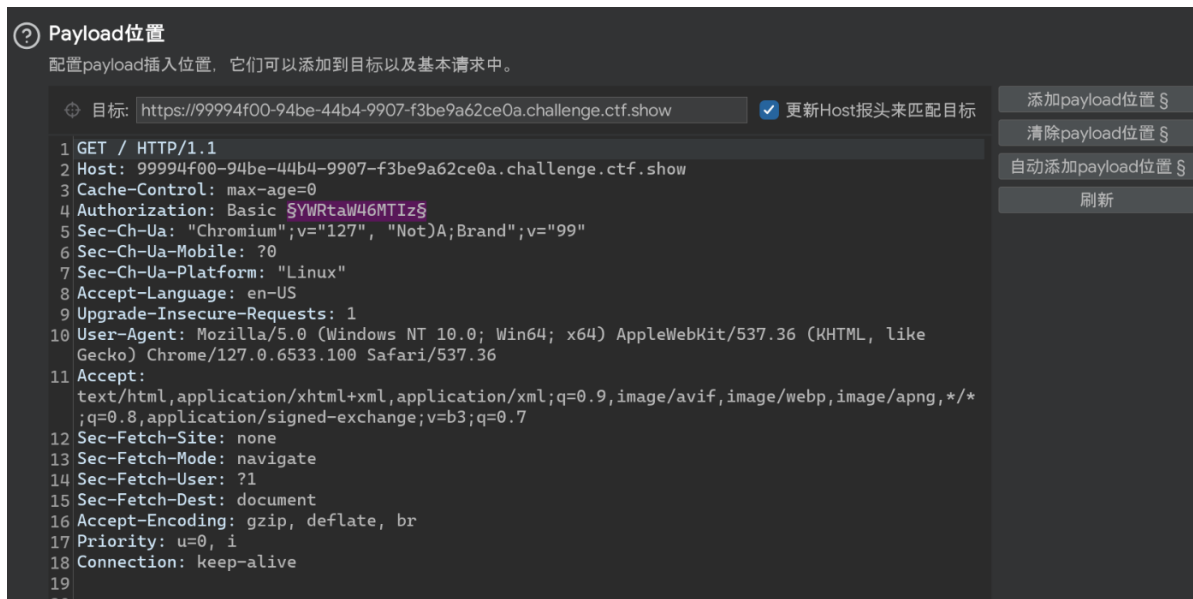
请求cookies 0

请求头 17

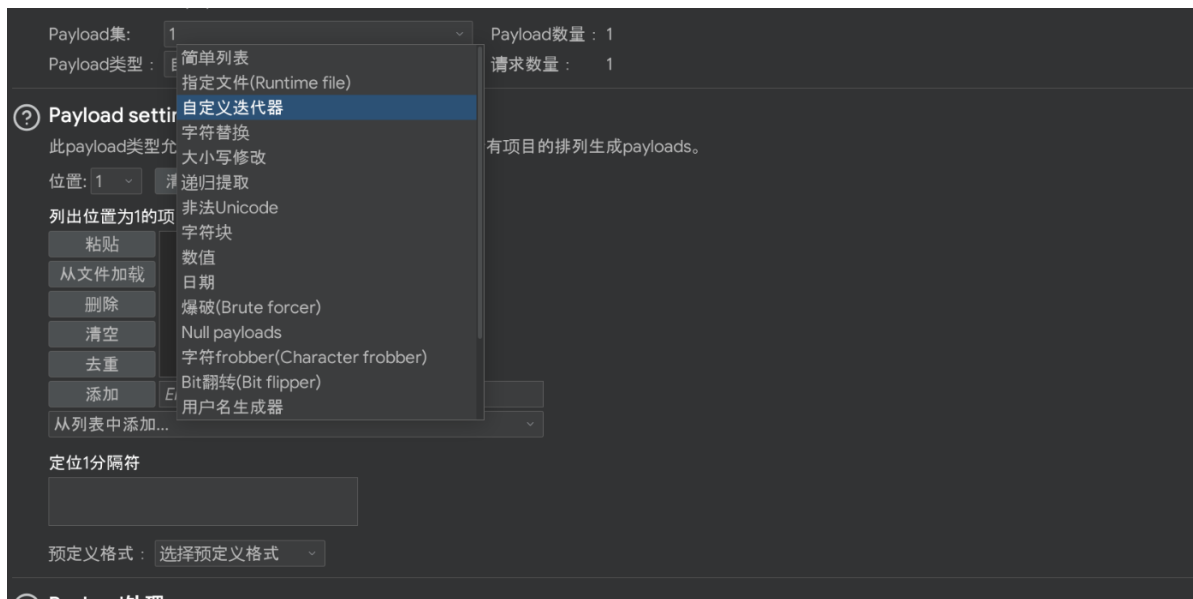
Event log (2) All issues (1)

内存: 221.8MB

### 3. Ctrl+I 发送到Intruder，给我们要爆破的内容“添加payload位置”



### 4. 进入payload模块，给Payload类型改为“自定义迭代器”



### 5. 在第一个位置添加，admin(没有提示用户名的一般是admin)

Payload集: 1 Payload数量: 1  
Payload类型: 自定义迭代器 请求数量: 1

### ② Payload settings [Custom iterator]

此payload类型允许您配置多个项目列表，并使用列表中所有项目的排列生成payloads。

位置: 1 清空所有

列出位置为1的项目 (1)

粘贴	admin
从文件加载	
删除	
清空	
去重	
添加	
从列表中添加...	

定位1分隔符

预定义格式: 选择预定义格式

6.第二个位置添加":", 在添加框内输入":", 然后回车

此payload类型允许您配置多个项目列表，并使用

位置: 2 清空所有

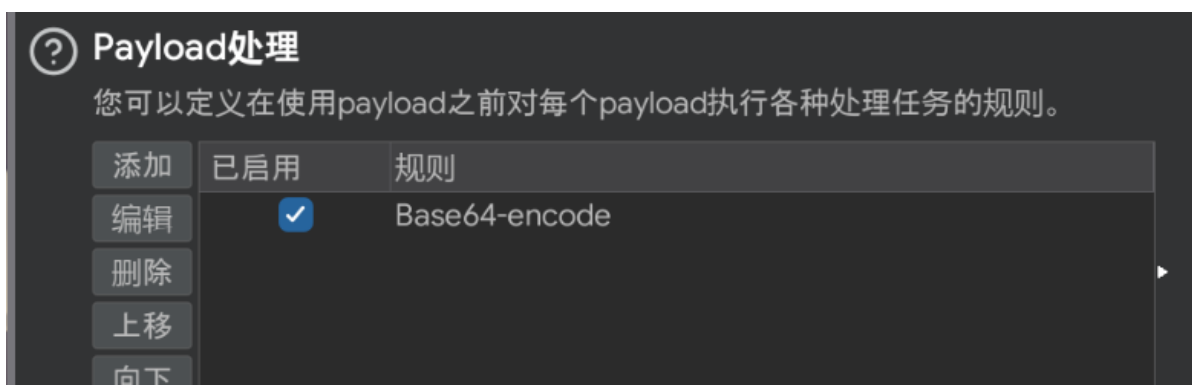
列出位置为2的项目 (1)

粘贴	:
从文件加载	
删除	
清空	
去重	
添加	
从列表中添加...	

7.第三个位置加入题目给的字典，“从文件加载”->选择文件->open



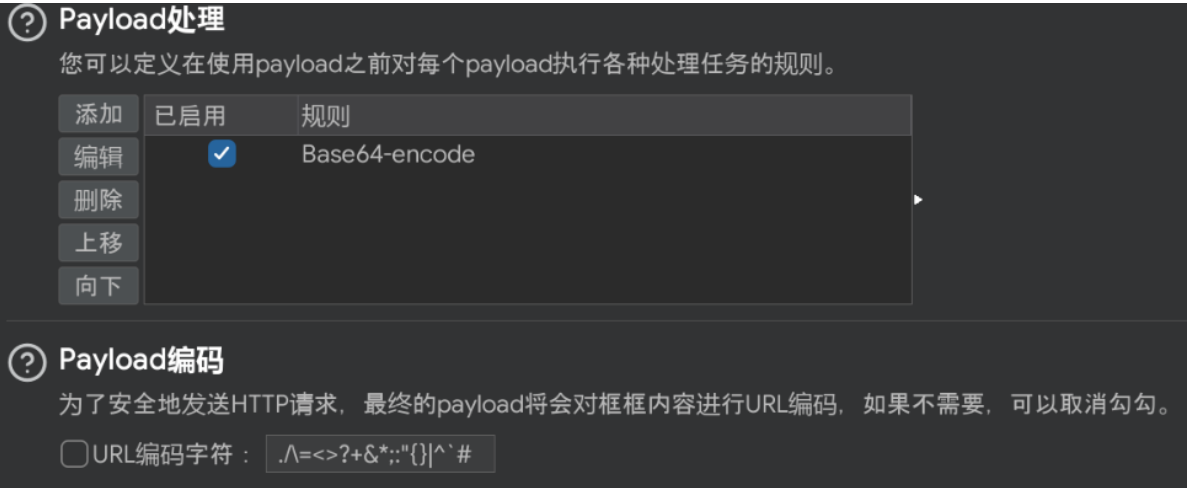
8.因为内容被base64加密了，所以还要加一个“Payload处理”，“添加”->类型选择“编码”



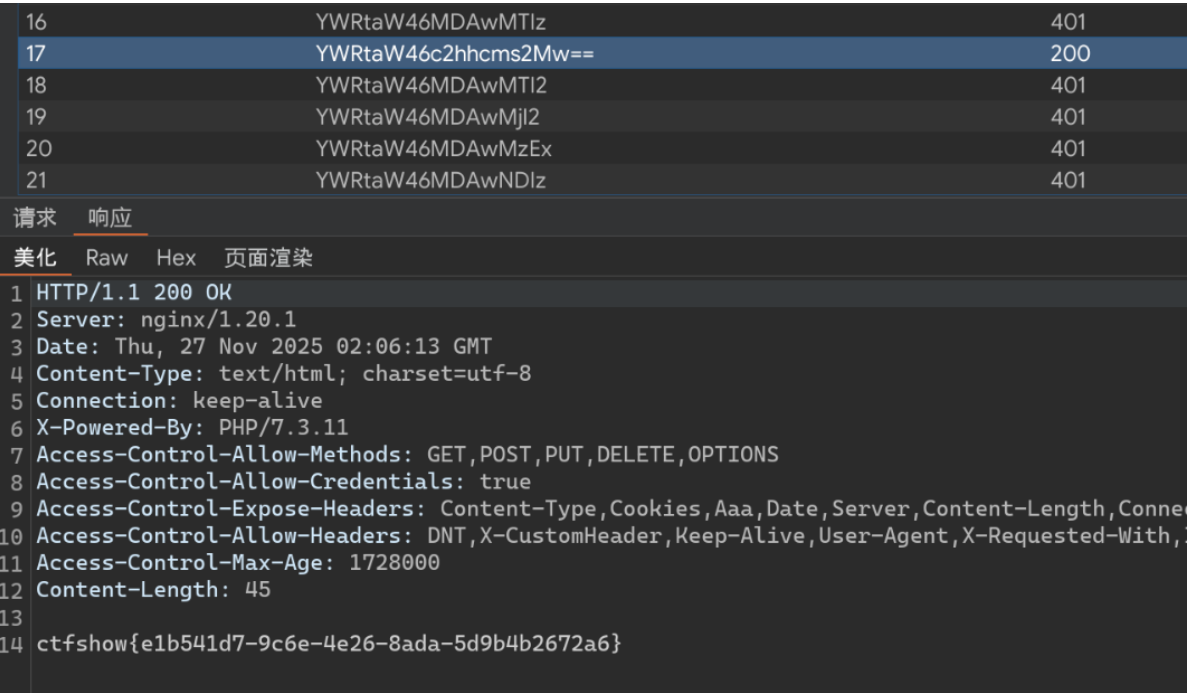
9.“添加”->“base64-encode”



10.还要取消“URL编码字符”的方框，这样就好了（不取消会影响我们的payload）



11.“开始攻击”，要找的一般通过状态码和长度判断，显然要找的是第17个（200状态码表示请求成功）



12.把payload进行解密，得到密码

## Base64 编码/解码

YWRtaW46c2hhcms2Mw==

字符编码: UTF-8

admin:shark63

13.返回靶场，输入username(admin)和密码(shark63)得到flag

ctfshow{e1b541d7-9c6e-4e26-8ada-5d9b4b2672a6}

