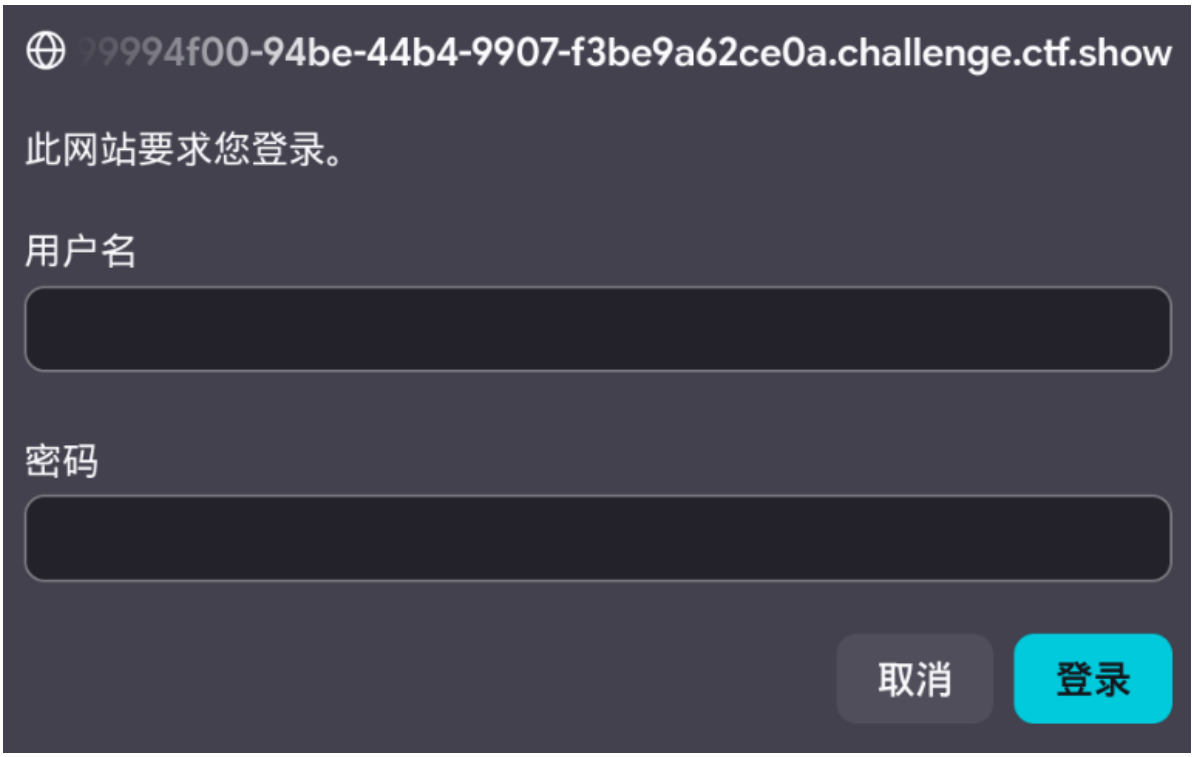
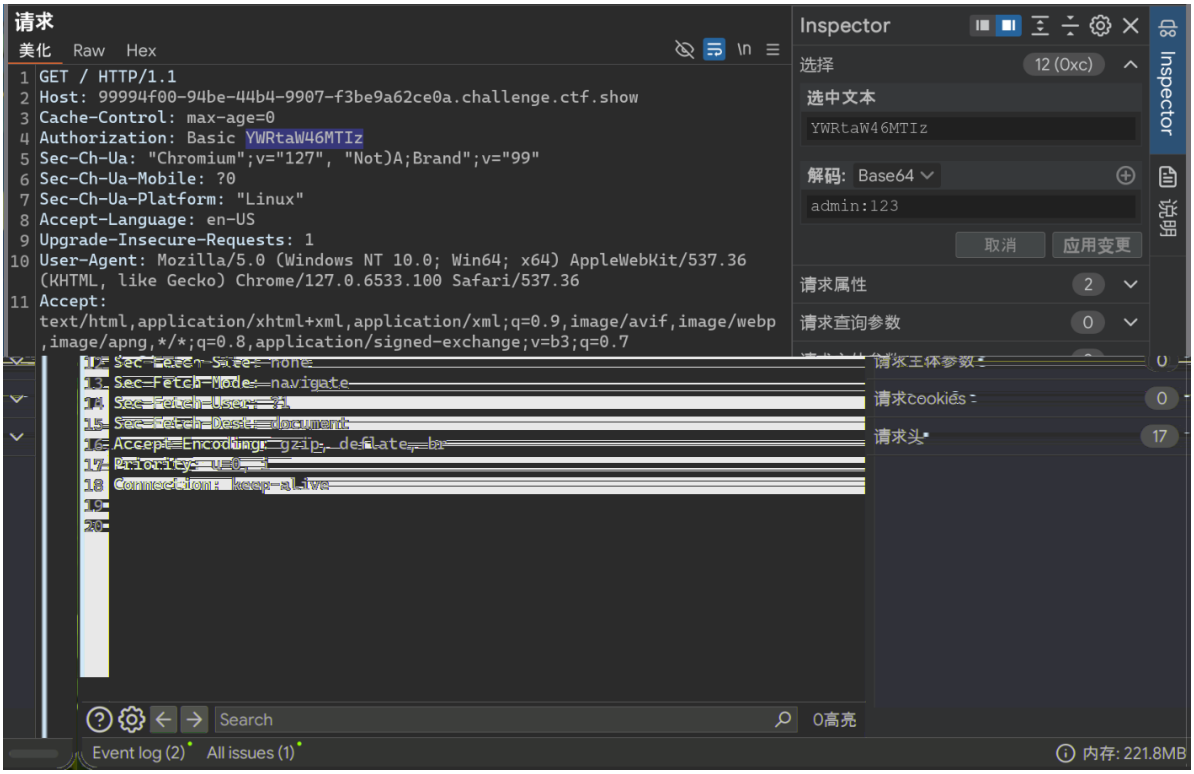
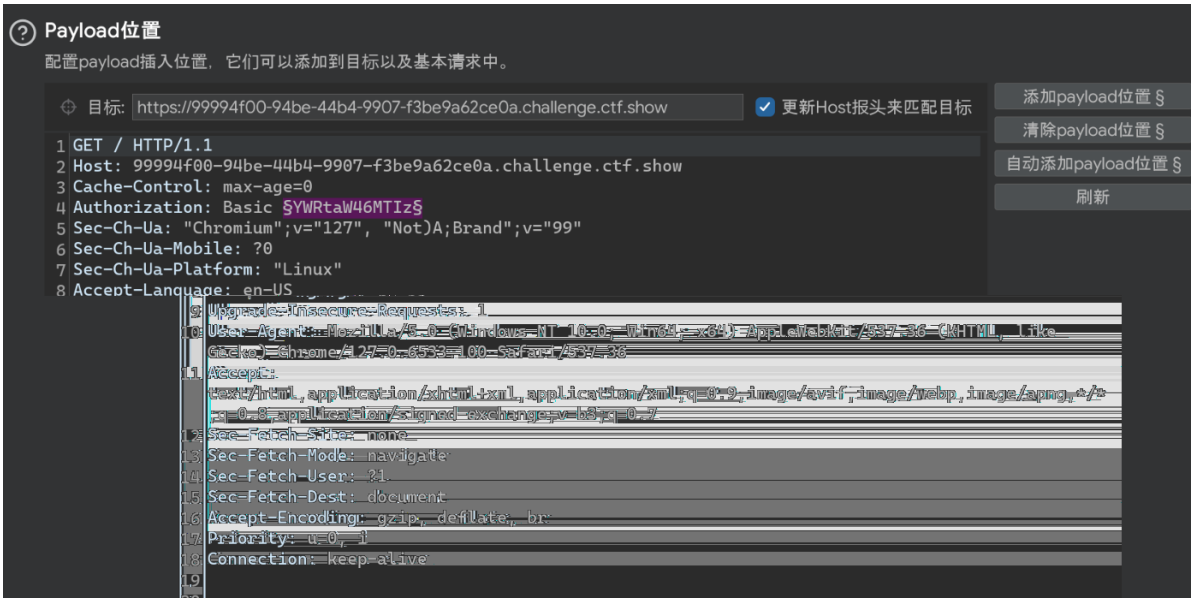
1.打开靶场，盲猜username为admin



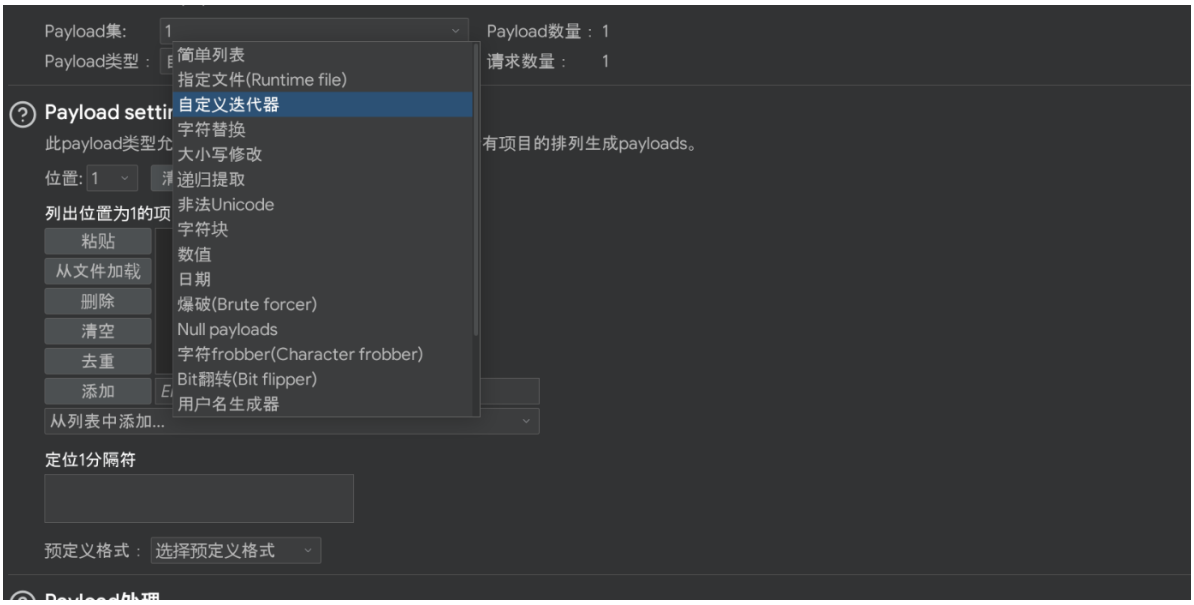
2.打开bp，随便输入密码，进行抓包，发现我们发送过去的内容被base64编码了，还用了:分割



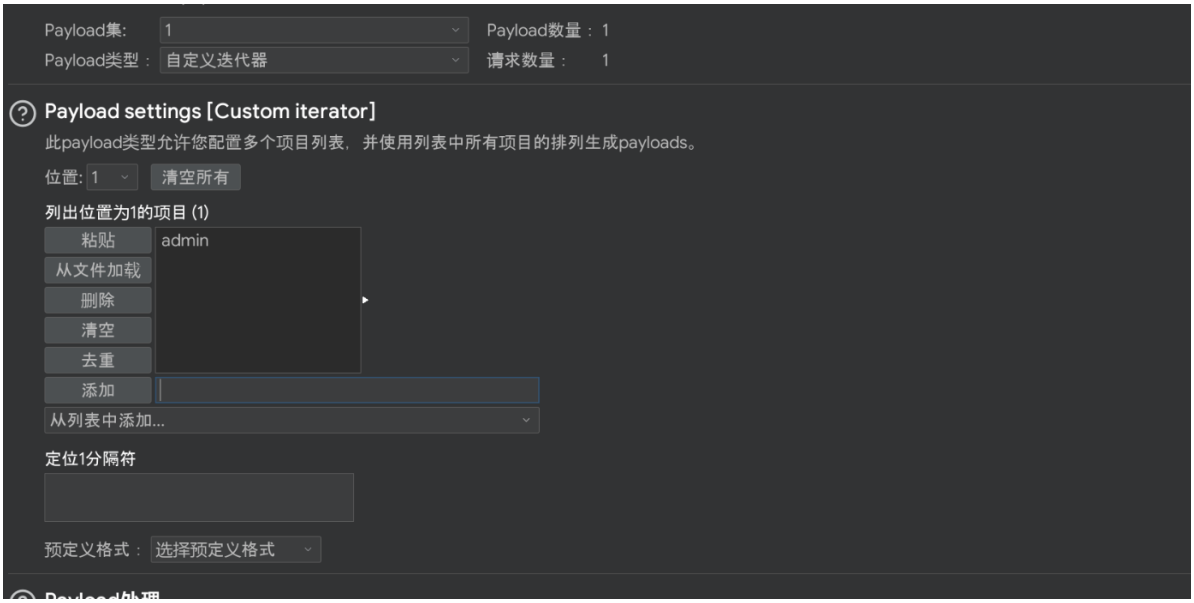
3.Chrl+I发送到Intruder，给我们要爆破的内容”添加payload位置“



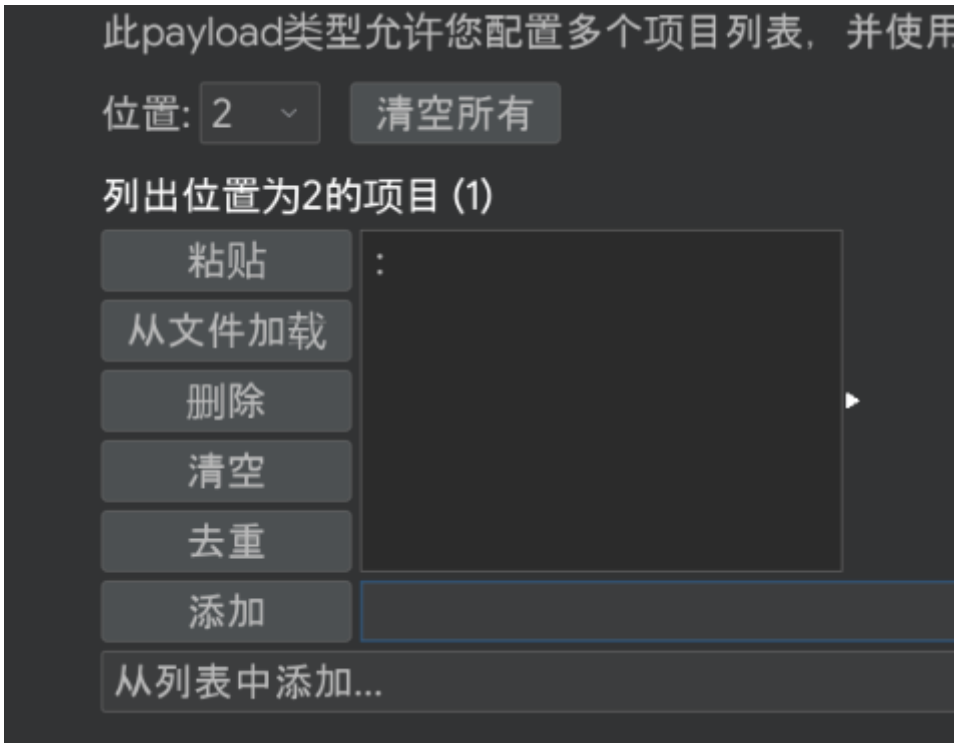
4.进入payload模块，给Payload类型改为“自定义迭代器”



5.在第一个位置添加，admin(没有提示用户名的一般是admin)

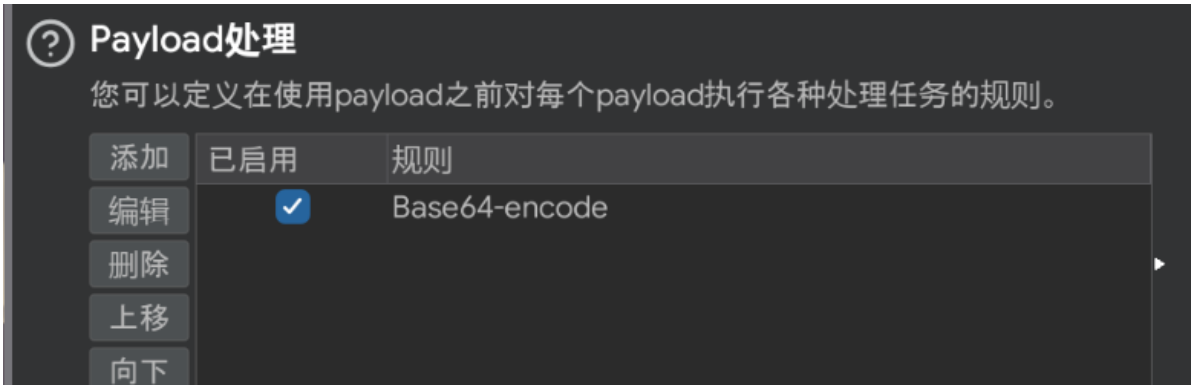


6.第二个位置添加":"，在添加框内输入“:”，然后回车



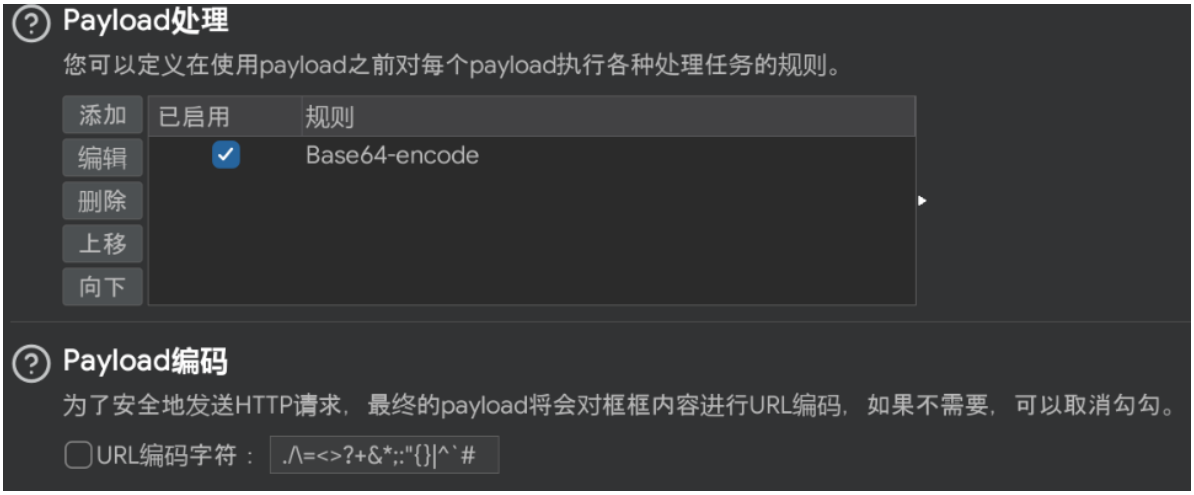
7.第三个位置加入题目给的字典，“从文件加载”->选择文件->open

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”

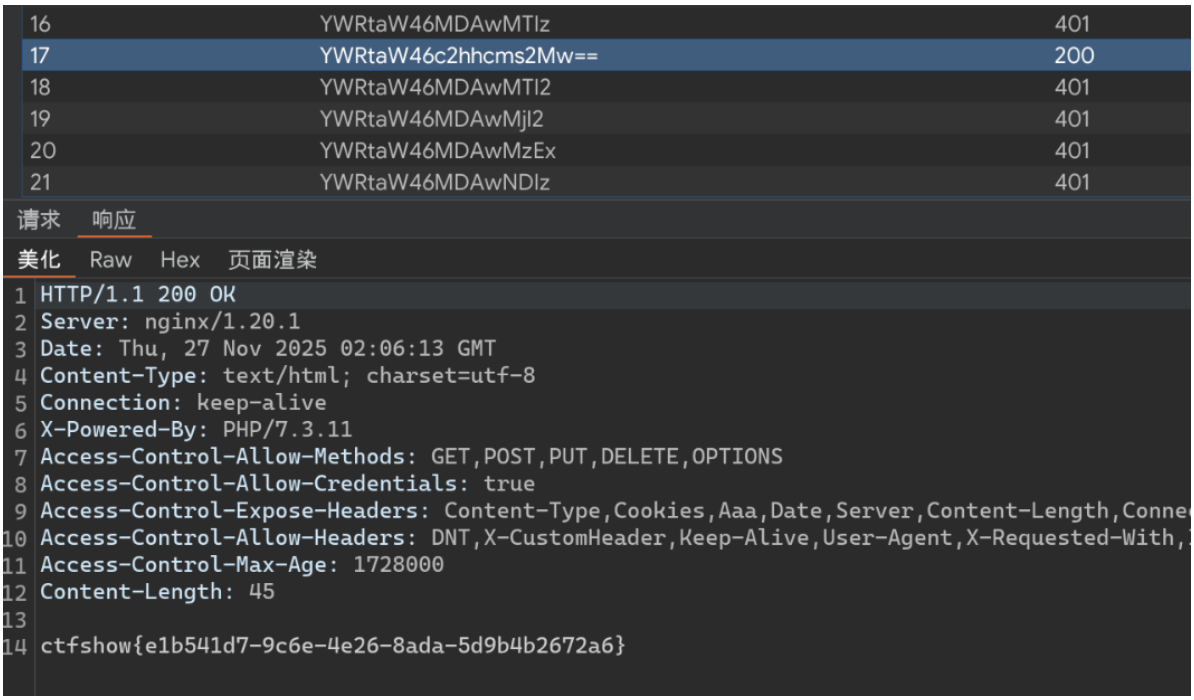


9.“添加”->“base64-encode”

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

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

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