白帽子昵称：IU的老公

漏洞描述

漏洞URL：如果是Web就填写此项

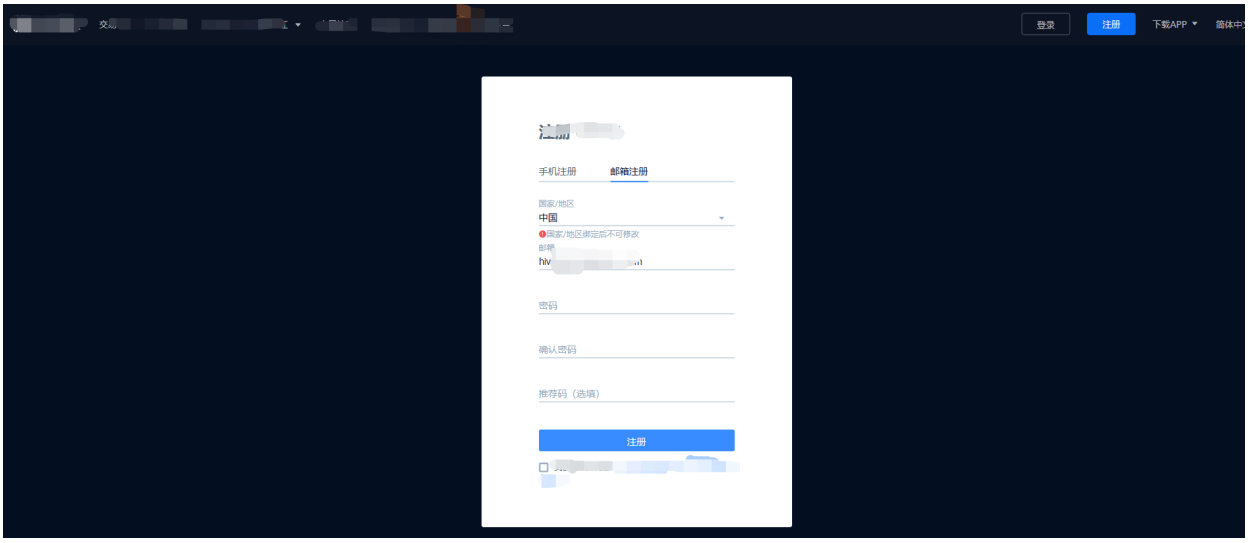
https://www.****.me/#/***/register

简要描述：漏洞说明、利用条件、危害等

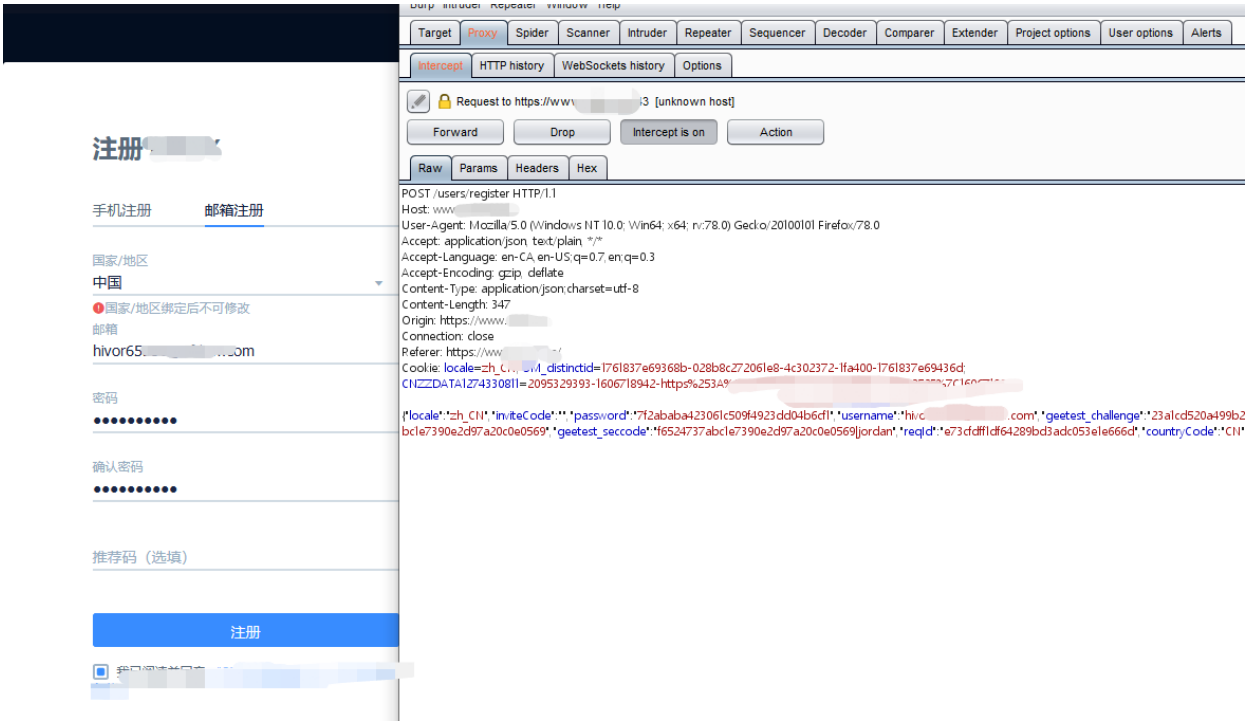
访问 https://www.****.me/#/****/register 进入注册页面

使用邮箱注册，并发送验证码邮件

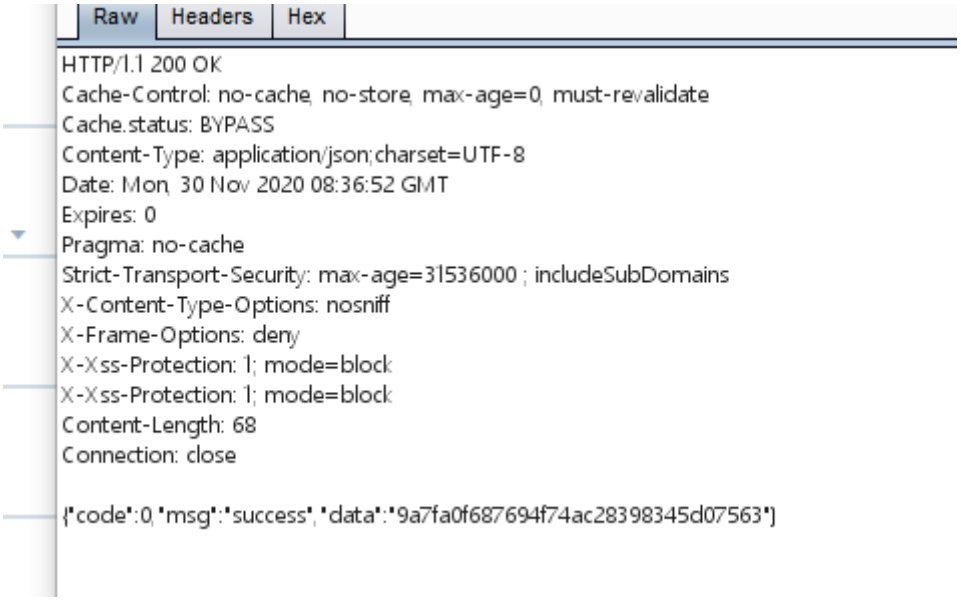
漏洞证明：



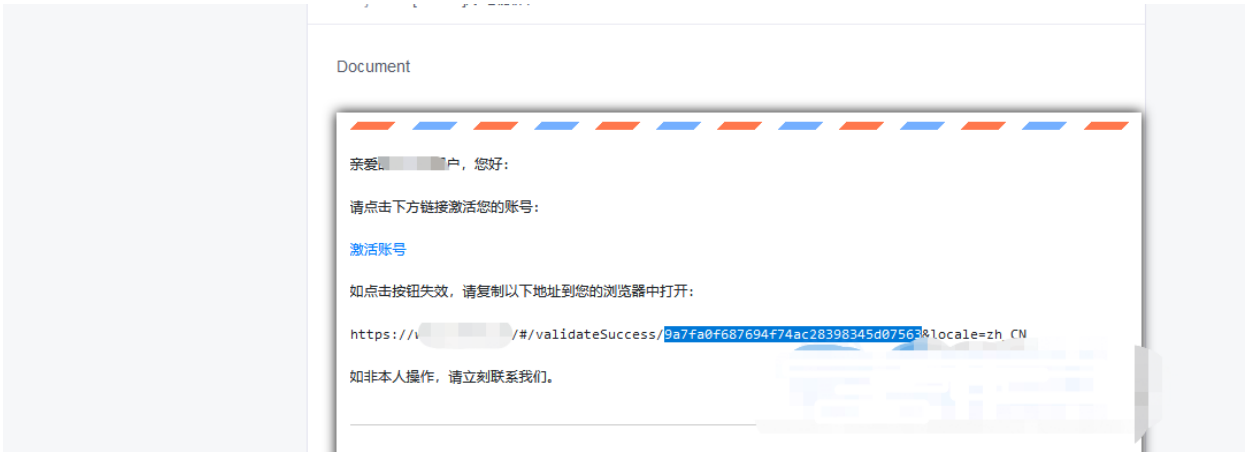
填写好相关信息后点击注册，此时使用Burpsuit抓到对应的注册请求如下：



在响应体里面可以看到有个data字段，这个就是用户注册的token



看一下已收到的邮件内容，可以发现激活链接中的token和响应包中的token一致，所以攻击者可以通过响应包拿到任意用户的激活链接



漏洞利用代码：

https://www.*****.me/#/*****/register

修复方案：

响应包中去掉敏感信息

漏洞总结

任何形式的凭证信息都应该得到严格保护，类似的情况在其他场景下可能导致更为严重的安全风险