

漏洞描述

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

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

漏洞证明:

交易

登录

注册

下载APP

简体中文

注册

手机注册

邮箱注册

国家/地区

中国

国家/地区绑定后不可修改

邮箱

hiv

密码

确认密码

推荐码 (选填)

注册

☐

The image shows a web application registration form on the left and a Burp Suite proxy log on the right.

Web Application Registration Form:

- 注册:** The main heading.
- 手机注册** | **邮箱注册** (selected): Two tabs for registration methods.
- 国家/地区:** A dropdown menu with "中国" (China) selected.
- 国家/地区绑定后不可修改**: A note indicating that the country/region cannot be changed after binding.
- 邮箱:** The email field contains "hivor65.@[redacted].com".
- 密码:** The password field is masked with dots.
- 确认密码:** The confirmation password field is also masked with dots.
- 推荐码 (选填):** An optional field for a referral code.
- 注册:** A blue button to submit the registration form.

Burp Suite Proxy Log:

- Target:** Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts
- Intercept:** HTTP history | WebSockets history | Options
- Request to https://www.[redacted].cn/3 [unknown host]:**
 - Forward** | **Drop** | **Intercept is on** | **Action**
 - Raw** | **Params** | **Headers** | **Hex**
- POST /users/register HTTP/1.1**
 - Host: www.[redacted].cn
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
 - Accept: application/json, text/plain, */*
 - Accept-Language: en-CA, en-US;q=0.7, en;q=0.3
 - Accept-Encoding: gzip, deflate
 - Content-Type: application/json; charset=utf-8
 - Content-Length: 347
 - Origin: https://www.[redacted].cn
 - Connection: close
 - Referer: https://www.[redacted].cn/
 - Cookie: locale=zh_CN, WAI_distinctid=1761837e69368b-028b8c272061e8-4c302372-1fa400-1761837e69436d; CINZDATA1Z74330811=2095329393-1606718942-https%253A%2F%2Fwww.[redacted].cn%2F3
 - !locale:'zh_CN','inviteCode','password':'712ababa423061c5094923dd04b6d1','username':'hivor65@[redacted].com','geetest_challenge':'23alcdd520a499b3b1e7390e2d97a20c0e0569','geetest_seccode':'f6524737abc1e7390e2d97a20c0e0569|jordan','reqId':'e73cdf11df64289bd3adc053e1e666d','countryCode':'CN'

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

Raw	Headers	Hex
HTTP/1.1 200 OK		
Cache-Control: no-cache, no-store, max-age=0, must-revalidate		
Cache-status: BYPASS		
Content-Type: application/json; charset=UTF-8		
Date: Mon, 30 Nov 2020 08:36:52 GMT		
Expires: 0		
Pragma: no-cache		
Strict-Transport-Security: max-age=31536000 ; includeSubDomains		
X-Content-Type-Options: nosniff		
X-Frame-Options: deny		
X-Xss-Protection: 1; mode=block		
X-Xss-Protection: 1; mode=block		
Content-Length: 68		
Connection: close		
{ "code": 0, "msg": "success", "data": "9a7fa0f687694f74ac28398345d07563" }		

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