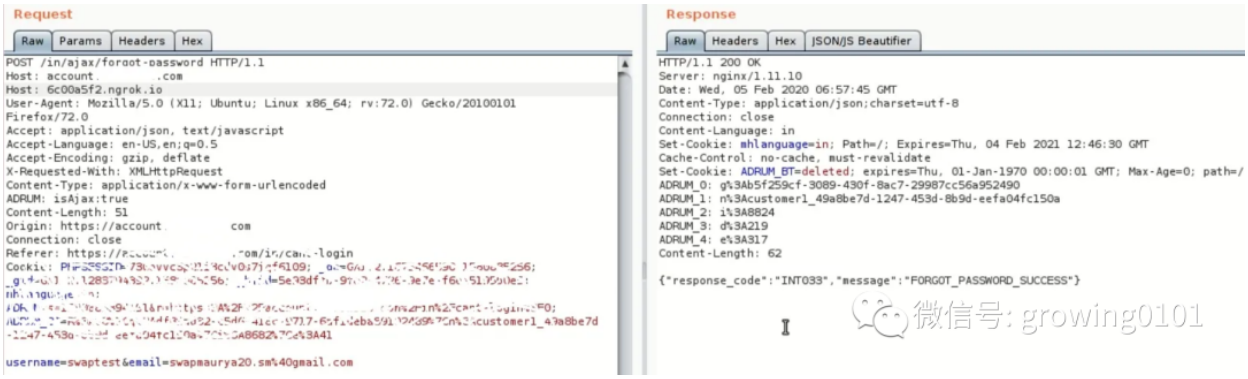
06 重置密码处存在账号劫持漏洞

漏洞名称：重置密码处存在账号劫持漏洞
漏洞类别：账号劫持、CSRF
危害等级：中危
漏洞赏金：/
漏洞触发点：重置密码处
漏洞细节简述：重置密码请求包中进行主机头毒化，诱导访问获取其重置令牌
参考来源：https://mp.weixin.qq.com/s/teWvleEFG1fJ1jh4_vBRHg
记录时间：2023.11.09

如何发现可能存在漏洞的迹象?

- 分析逻辑，重置密码通过邮箱链接重置
- 邮箱字段可控



如何发现存在账号劫持?

- 存在主机头毒化缺陷，可导致重置链接篡改为恶意链接，进而在用户访问时可获取重置令牌

We have received a password reset request. To continue to reset your password, simply click on the button below.

Please note that this link will expire in 24 hrs.

Reset Password

If you are having trouble accessing the link, please copy and paste the link below into the address bar on your browser.

https://6c00a5f2.ngrok.io/en/cant-login?sbfpw=0c8452e8-0a68-4bea-8992-bf6932c9b001

If you did not make this request, please ignore and delete this email.