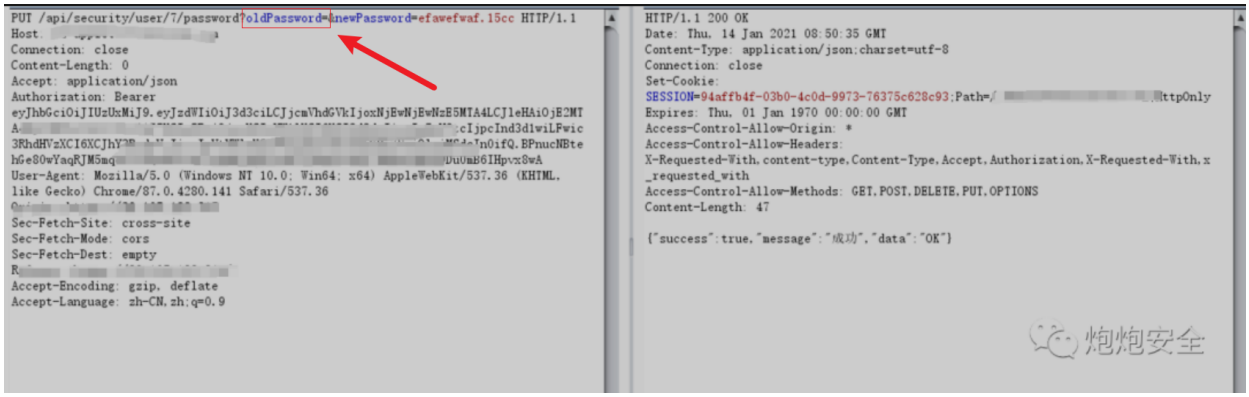
05 系统后台存在任意用户密码重置漏洞

漏洞名称：系统后台存在任意用户密码重置漏洞
漏洞类别：任意密码重置
危害等级：严重
漏洞赏金：/
漏洞触发点：系统后台
漏洞细节简述：置空旧密码字段+越权
参考来源：https://mp.weixin.qq.com/s/coUcU8q-I7POJhKpytdVdA
记录时间：2023.11.09

如何发现密码重置逻辑漏洞?

- 在密码重置的数据包中，存在旧密码参数
- 删去 oldpasswd 的值，该字段并未验证
- 无需旧密码可以直接修改



是否存在 CSRF ?

- 由于该 url 的特殊性，写入了用户 id 进行控制，难以实现 CSRF

如何提升为任意用户密码重置漏洞?

- 正是由于 url 中存在用户 id， 导致越权修改任意用户密码