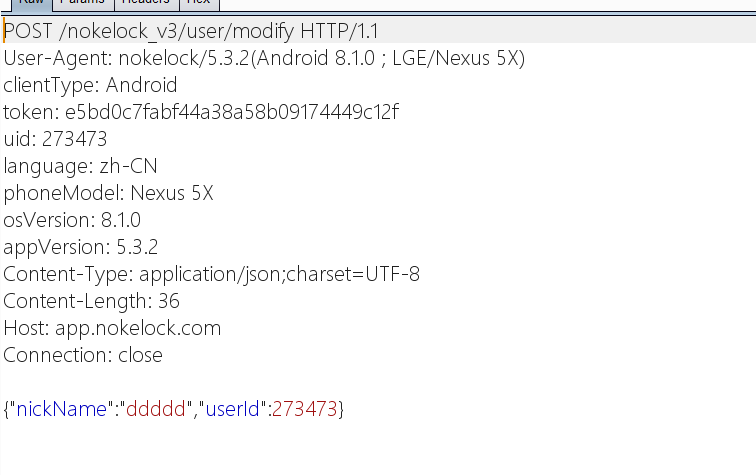
# NockLock越权修改他人信息，甚至能获取他人账户的完整控制权

NockLock应用中有修改个人信息的功能，如下所示：



修改信息的请求如下所示：

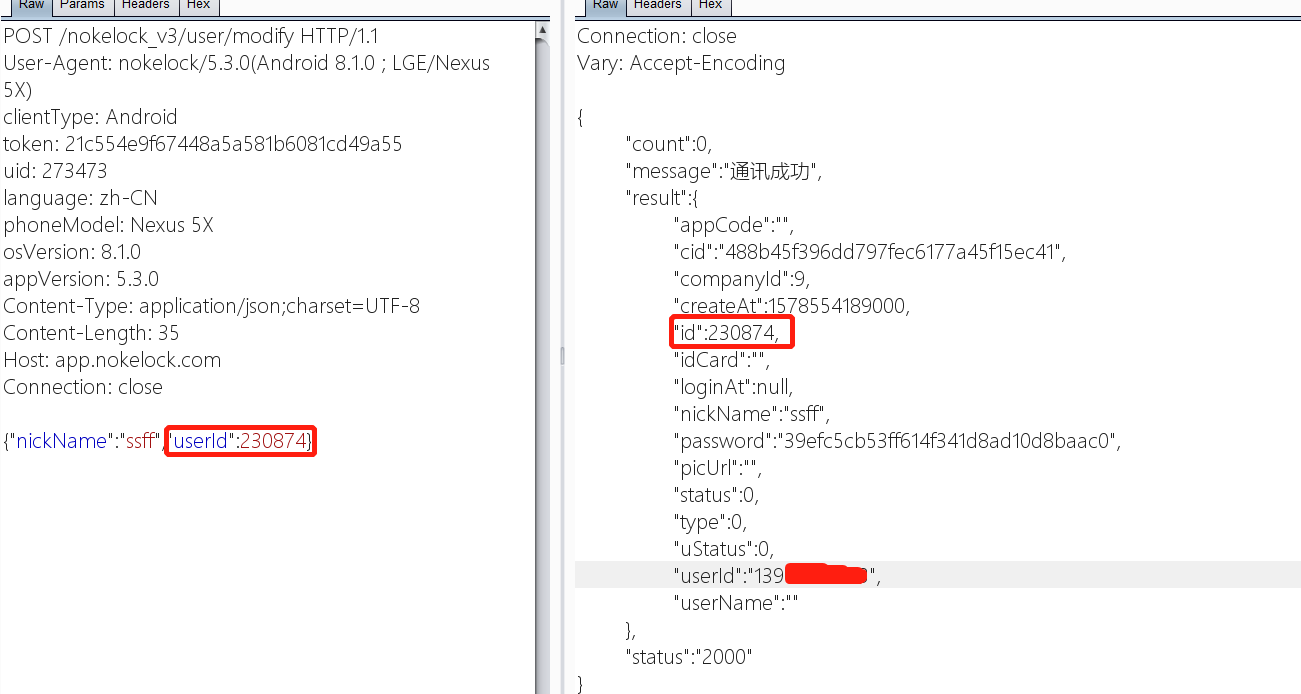


UserId为用户id，发送修改昵称的请求，响应如下：

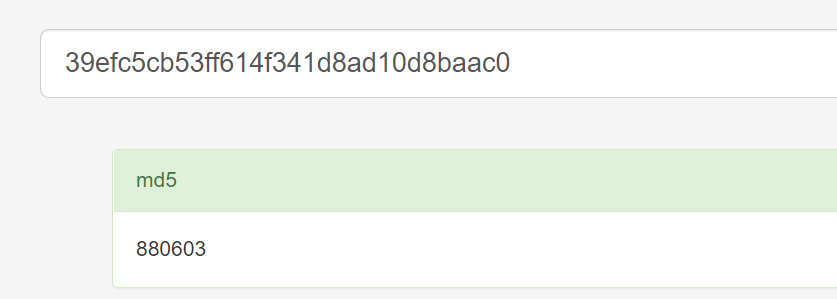


从响应中发现成功修改用户昵称，但是返回的响应中包含了用户的账号（如果是用手机号登录的话就是手机号码）以及用户密码的密文。

修改用户Id，能成功修改其他用户的昵称，成功修改他人用户昵称的响应如下：



根据密码的密文长度，推测密码是MD5加密的密文，尝试使用彩虹表破解密码，结果如下所示：



这样就能获取id为230874用户的账户和密码，就能完全控制改用户的账号了。