如果遇到重置密码是分几步走的（比如先验证验证码是否正确，然后再让你改密码）， 这种可以注意验证验证码的响应数据包



像这里， 响应包没有出现任何可校验的信息，比如token，sign之类的， 百分之90存在重置任意用户的漏洞

输入别人账户，直接修改验证的响应包，进入页面重置即可



