漏洞链接<https://dts.cgnpc.biz/sysmgr/lgninfo/login.jsp?doSSO=0>

点击修改忘记



然后会出现所需修改的账号以及获取短信验证码这里随便填写直接抓包

图形用户界面, 应用程序

描述已自动生成

然后放包抓取返回包，将success：0 改成1

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

即可绕开前端验证(这里可以猜到 后端并没有做验证只是将数据进行了比对，然后返回0验证失败，1验证成功 然后由前端进行验证)

图形用户界面, 应用程序

描述已自动生成

然后修改密码成功

图形用户界面, 应用程序

描述已自动生成

## 漏洞整改：

1 一次性填写校验信息（原始密码、新密码等）后再提交修改密码请求

2 对客户端提交的修改密码请求，应对请求的用户身份与当前登录的用户身份进行校验，判断是否有权修改用户的密码并对原始密码是否正确也进行判断

3 不应将用于接收验证信息的手机、邮箱等信息全部明文传到客户端，应对手机、邮箱等信息进行屏蔽处理，或不将此类信息返回到客户端。

4 重置密码链接中的关键信息应随机化，不可预测（例如token机制），且禁止将关键信息返回到客户端。