对于任何一个设有权限的系统，都有登陆功能、注册功能，当然为了方便用户忘记密码而存在的密码找回功能。

登陆功能存在的安全问题很大部分是弱密码和密码暴力破解，注册功能存在的安全问题是大量恶意注册。本文重点还是要谈的是密码找回功能的安全漏洞，实现任意用户的密码重置。

对任何一个业务功能进行渗透前，首先要搞清楚该功能的业务逻辑。一般系统的找回密码功能的业务流程图如下。



为了熟悉密码找回功能的流程，我们需要自己先注册一个用户，走一遍该流程，画出流程图，同时把每一步的接口调用情况的url、入参、出参都要做好记录。推荐的工具是fiddle。

分析整个业务流程，找回密码最大的安全风险点，在输入新密码前的环节，也就是说，输入新密码前的环节必须严谨，验证合理。

举一个某网站的例子，更能说明问题。



第一步，填写账户名，



当我们填写一个任意用户名，如果该用户名不存在，则提示。



通过该步骤，我们可以不断试探出一个存在的用户名。

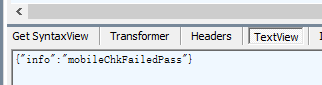
试探成功一个正确的用户名。则会跳转到第二步。如下：



现在遇到一个最大的拦路虎，就是“短信验证码”。他人的短信验证码是很难拿到的！除非有这样low的漏洞，就是在获取短信验证码时，验证码存在接口请求的入参或出参中。

这时，我们就要换一个思路。看下验证身份的接口返回结果是什么。

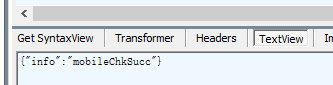
比如，随便输入短信验证码和正确的图形验证码。通过fiddle可以看到。它的返回是：



网站界面的提示语是：



那我们输入一个正确的短信验证码，看下接口返回是：



同时，界面便跳转到设置新密码界面。



所以，现在最关键的问题，就是如何做，输入错误的短信验证码，也可以跳转到设置新密码的这一步。

这就要看网站这一步业务逻辑是否严谨和合理。

很多网站，在业务流程上设计相当简单，在如何跳转到设置新密码的时候，只判断上一步的服务器返回内容。以本网站为例，只判断返回是否是“mobileChkSucc”，是的话，就会跳转到设置新密码页面。否则，返回的是“mobileChkFailedPass”就不会跳转。

如果该网站的业务流程是这样设计的，恭喜你，中奖了！

**只要我们篡改服务器给前端的返回内容是“mobileChkSucc”，我们就可以对任何用户的密码进行重置了。**

当然，如何篡改？同样使用fiddle工具。不是本文谈的重点。（嘿嘿。。。）

对于安全渗透人员，渗透思路是关键。

对于设计开发人员，业务流程的逻辑合理和严谨是关键。

希望通过本文，让安全渗透人员把控好自己所负责的产品，让设计开发人员把业务逻辑设计的更合理更严谨。