任意密码重置总结

作者：HuixiaZhang
原文链接：https://ld246.com/article/1538028801561
来源网站：链滴

0x00 前言

密码重置是业务中十分重要且敏感的一环，在这里产生过很多任意密码重置的问题，是逻辑漏洞中很见的一种。在这里总结一下任意密码重置的常见姿势。

0x01 验证码不失效

原理：

验证码不失效是多年前最常见的一种逻辑漏洞，其原理是找回密码判断时，仅判断验证码是否正确，有对验证码的过期时间进行限制，导致可以进行爆破。

测试方法：

通过枚举验证码直到找到真正的验证码跳转更改密码页面。

0x02 验证码回显

原理：

验证码回显是指发送验证码后，可以通过抓包等方式得到正确的验证码，直接填写验证码跳转更改密页面。

测试方法：

通过截断数据包分析验证码是否直接写在cookie或者其他的字段中，如果捕获到，就可以直接填写。

0x03 验证码不绑定用户

原理：

输入手机号和验证码进行重置密码的时候，仅对验证码是够正确进行了判断，未对该验证码是否与手号匹配做验证。

测试方法：

在提交手机号和验证码的时候，替换手机号为其他手机号进行测试，成功通过验证并重置其密码。

0x04 用户名未绑定邮箱号/手机号

原理：

用户名、手机号、验证码三者没有统一进行验证，仅判断了三者中的手机号和验证是否匹配和正确，果正确则判断成功并进入密码修改界面。

测试方法：

输入用户名获取验证码，通过抓包修改接收验证码的手机号为自己的号码，自己手机成功接收验证码提交到网站进行验证，验证成功并进入密码修改界面。

0x05 客户端验证绕过

原理：

客户端在本地进行验证码是否正确的判断，主要是根据接收到验证成功或验证失败的包判断是否验证

功，而该判断结果也可以在本地修改，最终导致欺骗客户端，进入密码修改界面。

测试方法：

重置目标用户，输入错误验证码，修改返回包，把返回错误信息的包改为返回正确信息的包，即可绕验证步骤，最终重置用户密码。

0x06 跳过身份检验

原理：

信任域问题，用户输入验证码，直接跳转到设置新密码的这一步，服务器默认已经通过检验，值得信，于是便未再次作检验，就可以直接重置密码。

测试方法：

使用一个已知验证码账户记录每一步的链接，然后重置他人账户，点击获取验证码步骤之后直接手动制网址跳转到输入新密码界面，重置其密码。

0x07 修改新密码时未校验用户字段

原理：

在重置密码界面，没有再次对用户ID进行校验，导致提交参数时可以将用户ID更改，从而修改其他用的密码。

测试方法：

使用自己账号和自己手机号进行密码重置，在最后重置密码时，抓包修改用户id相关信息，修改他人码。

0x08 cookie替换

原理：

重置密码时通过用户cookie判断用户是否通过了手机验证，而cookie值是用户可控的，可以通过修改ookie中的值欺骗服务器自己通过了验证来修改密码。

测试方法：

是用自己账号和手机号进行密码重置，在重置密码时，将cookie提取出来分析，如果服务器通过cooki判断是否通过手机验证，就使用他人账号进行重置，然后将cookie中判断是否通过验证的值改为已通状态，即可重置密码。

0x09 利用CSRF漏洞重置密码

原理：

如果登陆状态可直接修改密码，且密码修改的请求没有验证token、referer也没有设置跨域权限。

测试方法：

用自己账号重置密码，在修改密码部分将请求截断，然后伪装链接发给他人，受害者在登陆状态误点接即会被修改密码。

0x10 总结

任意密码重置是各个提供用户注册的企业都会面临的一个问题，在这方面稍有不慎就会产生很严重的果。

而这类漏洞，黑盒测试的效果远大于白盒审计，所以总结了各种常见情况的测试方法，通过渗透测试寻找漏洞，规避风险。

原文链接：任意密码重置总结