密码找回逻辑漏洞小总结—安全小课堂第三十五期

原创：京东安全应急响应 京东安全应急响应中心 2016-11-25

安全小课堂第三十五期

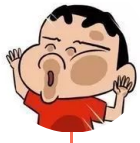
密码找回功能出现逻辑漏洞，利用漏洞修改他人帐号密码。比如重置了管理权限的账户密码，可能导致修改页面，上传shell，服务器被黑掉，可能使得订单与收货地址信息泄露，涉及用户隐私、账户被盗刷等。本期，我们来进行密码找回逻辑漏洞小总结。

本期我们邀请到
JSRC资深白帽子
种田、紫霞仙子
ヽ(*°▽°*)ノ

1

豌豆妹

什么是逻辑漏洞？



小新

开发在开发程序中，根据假设条件来执行一系列操作，假设条件设计的不够全面，程序执行多步流程时设计不到位，就可能导致逻辑问题。使得一些用户的功能操作偏离了程序员的预想范围，进而对公司业务造成一定的影响。

2

豌豆妹

密码找回功能的逻辑漏洞以何种形式展现？

小丸子 

利用漏洞修改他人帐号密码，甚至修改管理员的密码。

3

豌豆妹

密码找回功能出现逻辑漏洞的严重性，能说说吗？

哆啦A梦 

比如重置了具有管理权限的账户密码，就有可能导致修改页面，上传shell，进而导致服务被入侵，也可能导致订单与收货地址信息等用户隐私泄露，还可能导致用户账户被盗刷等一系列安全问题。

总得来说，密码找回功能如果出现逻辑漏洞可能导致公司的敏感数据泄露、服务器被入侵甚至直接造成经济损失。

4

豌豆妹

那如何测试密码找回功能是否存在逻辑漏洞呢？

葫芦娃 

找回密码的逻辑漏洞存在形式比较多，可从检验参考可控和校验用户身份放在前端两个角度入手。

1、后端直接返回身份校验凭证到前端，还有一些凭证是弱算法，比如基于时间戳的凭证，基于用户id的凭证，很容易被猜解出来，进而通过服务身份验证；还有些基于验证码的验证，可以通过工具爆破出来等等；

2、前端校验也是比较常见的问题。攻击者可以直接修改返回结果，修改校验结果，可以直接绕过身份验证。前端校验还有一个常见的问题，用户通过身份验证后，进行修改密码操作时，未对重置会话进行绑定，导致修改用户名或者ID，就可以重置其他用户密码，这里还有一种案例，未对操作顺序进行检查，可以直接修改操作步骤，跳到最后一步，绕过身份验证，进行密码重置；

除了从前端的两个角度外，还有如下的方法：

1、在平时测试过程中，遇到过几个重置密码的地方存在注入，都是在检测用户名是否存在的这个参数上，通过注入可以做的事情比较多，就不说了；

2、还有一种遇到案例比较少的重置方法，可以在绑定或者修改绑定手机或邮箱时，修改绑定账户为被攻击者的账户，就可以把别人的账号帮到自己手机或邮箱上，通过这样来重置，这个前提是需要绑定的地方也存在安全问题。

柴可夫斯基 

我再补充一个遇到过的案例。注册账号的时候，存在前端校验，比如注册A，返回用户已存在，把已存在的状态修改为可注册，填写信息提交注册，就把A账号覆盖了。覆盖的方法还有session覆盖等，遇到的案例比较少，欢迎大家补充。

5

豌豆妹

密码找回功能的逻辑漏洞如何产生？

哆啦A梦

1、验证码爆破的，对验证码有效期和请求次数没有进行限制；
2、token验证之类的，直接将验证内容返回给用户；
3、找回密码功能的进行身份验证内容未加密或者加密算法较弱，容易被猜解；
4、对用户的身份验证在前端进行，导致验证被抓包绕过；
5、在最后一步修改密码的动作时，没有校验帐号是否通过了验证、短信与手机号是否对应。

6

豌豆妹

密码找回功能的逻辑漏洞如何修复呢？

小丸子

1、验证码爆破的，从验证码有效期和请求次数进行限制；
2、token验证之类的，不要直接返回给用户；
3、修改加密算法和加密内容，一定要是强加密，也要做到增加猜解难度或密文不可猜解；
4、用户身份验证一定要在后端实现；
5、在最后一步修改密码的动作时，一定要校验帐号是否通过了验证、短信与手机号是否对应、发送短信与已校验帐号不要使用同一个session名称；
6、非常重要的一点：上线前一定要经过安全测试！！！

微信公众号：jsrc_team
新浪官方微博：京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂