# 乌云越权总结

## 乌云知识库：

http://www.anquan.us/static/drops/tips-727.html

我的越权之道--小川

越权可能存在的地方

增删改查

越权成因

程序员开发时未对权限进行判断而进行操作

个人成见

测试必须准备两个账号

目前测试越权的最好的方法是在burp的重放模块进行cookie替换，查看 两个账号是否会发送操作

增：一般比较少见，因为增基本会与用户进行绑定

删：比较多，删与改是最容易出现权限未绑定的地方

改：比较多，删与改是最容易出现权限未绑定的地方

查：一般比较少见，因为查基本会与用户进行绑定

## 乌云公开漏洞：

（从后往前看，有意思即记录，有经验即总结）

多修改url的传参、多修改post的传参

### 1.优酷网持久设计缺陷、用户权限越权

http://www.anquan.us/static/bugs/wooyun-2010-0129.html

Get参数的越权，参数id使用伪静态镶嵌在url中

http://u.youku.com/my\_mail/type\_read\_ref\_inbox\_id\_52379500\_desc\_1?\_\_rt=1&\_\_ro=myInboxList

http://u.youku.com/my\_mail/type\_read\_ref\_outbox\_id\_52380790\_desc\_1?\_\_rt=1&\_\_ro=myOutboxList

http://u.youku.com/my\_video/type\_editfolder\_step\_1\_id\_4774704?\_\_rt=1&\_\_ro=myPlaylistList

修复方案：

1.严谨判断用户输入

2.严谨判断用户权限

### 2. 起点中文网网络收藏夹越权

http://www.anquan.us/static/bugs/wooyun-2011-01399.html

Post请求的越权更改和删除

### 3. 京东商城我的投诉查看信息越权

<http://www.anquan.us/static/bugs/wooyun-2011-03276.html>

Get型的我的投诉查看信息越权查看

### 4. 丁香人才任意简历查看越权

Get型下载处越权

<http://www.anquan.us/static/bugs/wooyun-2012-05390.html>

### 5. 苏宁越权礼包—较多泄露个人信息

<http://www.anquan.us/static/bugs/wooyun-2013-017670.html>

订单遍历

### 6. 百度某分站越权访问漏洞

<http://www.anquan.us/static/bugs/wooyun-2013-020356.html>

作品遍历

### 7. 江苏苏宁易购某越权操作缺陷

<http://www.anquan.us/static/bugs/wooyun-2013-020651.html>

订单取消遍历

### 8. 百伯越权浏览下载任意用户简历

<http://www.anquan.us/static/bugs/wooyun-2013-020723.html>

越权修改头像、查看简历

### 9. 咦~中粮我买网越权操作缺陷03（删除/修改任意用户信息）

<http://www.anquan.us/static/bugs/wooyun-2013-022249.html>

越权删除/修改 POST包

### 10. 格瓦拉越权删除用户信息问题

<http://www.anquan.us/static/bugs/wooyun-2013-025242.html>

越权删除信息

### 11. 苏宁旅行之越权完全版

<http://www.anquan.us/static/bugs/wooyun-2013-028045.html>

越权修改、删除、查看

### 12.搜狐某分站审核后台越权访问

<http://www.anquan.us/static/bugs/wooyun-2013-028518.html>

未授权访问

### 13.新浪微人脉存储型XSS漏洞(长度限制绕过)与越权双剑合并

http://www.anquan.us/static/bugs/wooyun-2013-037401.html

存储xss+越权双剑组合

### 14. 百度旅游某功能越权

<http://www.anquan.us/static/bugs/wooyun-2013-037166.html>

越权修改的id为加密字符串