**Web业务安全问题概述**

1. **业务安全关键点概述**
2. **身份认证安全**

暴力破解

cookie&session

加密测试

1. **业务一致性安全**

手机号篡改

用户名和邮箱更改

订单ID更改

商品编号的更改

用户ID篡改

1. **业务数据篡改**

金额数据篡改

商品数量篡改

数量限制突破

本地JS参数修改

1. **用户输入合法性**

注入

XSS

FUZZ

1. **密码找回漏洞**

正常访问，不通过找回方式，记录

分析数据包，定位敏感信息

分析找回机制

修改数据包验证

1. **验证码突破**

爆破

时间、次数突破

回显测试

绕过测试

1. **业务授权安全**

未授权访问

越权测试

1. **业务流程乱序**

顺序执行缺陷

1. **业务接口调用**

恶意注册

短息炸弹

内容编辑

1. **时效绕过测试**

时间刷新缺陷

时间范围测试

1. **业务安全问题描述及案例说明**
2. **身份认证安全**

**1.1暴力破解**

使用burpsuite、hydra等工具爆破没有验证码认证过程

**案例：**<http://zone.wooyun.org/content/20839>

**1.2 session&cookie**

会话固定攻击：如果登录前后的session不变，那么可以先利用未登录的session访问，获取sessionID，然后诱使用户利用这个session登录，从而伪造身份

**案例：**[WooYun: 新浪广东美食后台验证逻辑漏洞，直接登录后台，566764名用户资料暴露！](http://www.wooyun.org/bugs/wooyun-2013-025427" \t "_blank)

Cookie攻击：设置id=1这种伪装成管理员或者其他用户登录

**案例：**[WooYun: 益云广告平台任意帐号登录](http://www.wooyun.org/bugs/wooyun-2014-051424" \t "_blank)

**1.3弱加密**

未使用https或者前端加密到到后端验证，容易被嗅探截获用户的用户名密码

1. **业务一致安全**

**2.1手机号 邮箱篡改**

抓包修改手机号或者邮箱为其他人的手机号或者邮箱，来实现越权访问

**案例：**[WooYun: 绿盟RSAS安全系统全版本通杀权限管理员绕过漏洞，包括最新 RSAS V5.0.13.2](http://www.wooyun.org/bugs/wooyun-2014-074441" \t "_blank)

**2.2订单id修改**

查看自己的订单id，尝试+1看能否访问到其他的订单信息

**案例：**[WooYun: 广之旅旅行社任意访问用户订单](http://www.wooyun.org/bugs/wooyun-2013-044137" \t "_blank)

**2.3商品编号的篡改**

例如积分兑换处，100个积分可以兑换商品id为001的商品，1000个积分可以兑换商品id为002的商品，那么在100积分的兑换处，把兑换的商品改成002

**案例：**[WooYun: 联想某积分商城支付漏洞再绕过](http://www.wooyun.org/bugs/wooyun-2013-041617" \t "_blank)

**3、业务数据篡改**

**3.1金额数据的篡改**

抓包修改总的支付金额

**案例：**[WooYun: 12308订单支付时的总价未验证漏洞(支付逻辑漏洞)](http://www.wooyun.org/bugs/wooyun-2015-0117083" \t "_blank)

**3.2商品数量的篡改**

修改商品数量为负数来支付负金额

**案例：**[WooYun: 蔚蓝团支付逻辑漏洞(可负数支付)](http://www.wooyun.org/bugs/wooyun-2015-0109037" \t "_blank)

**3.3最大数量突破**

在购买数量等地方的最大限制仅适用js来实现，通过修改js来绕过

**4、输入的合法性**（下划线为用户的输入）

**4.1 SQL注入：**id=1’ union select 1,2,3 from xxx –

**4.2 XSS：**

1、标签内输出:

<div><script>alert("1")</script></div>

2、在属性内输出

<input type="text" name="username" value="" onclick="alert(/xss/)" />

<input type="text" name="username" value=""><script>alert(/xxs/)</script>" />

<a href="javascript:alert(/xxs/)">Hello</a>

3、在事件中输出

<input type="text" value="test" onclick="fun('')" onkeyup="alert(/xss/);//')" />

4、在CSS中输出

body {background-image: url("javascript:alert('XSS')");}

body {background-image: expression(alert(/XSS/));}

5、在Script标签中输出

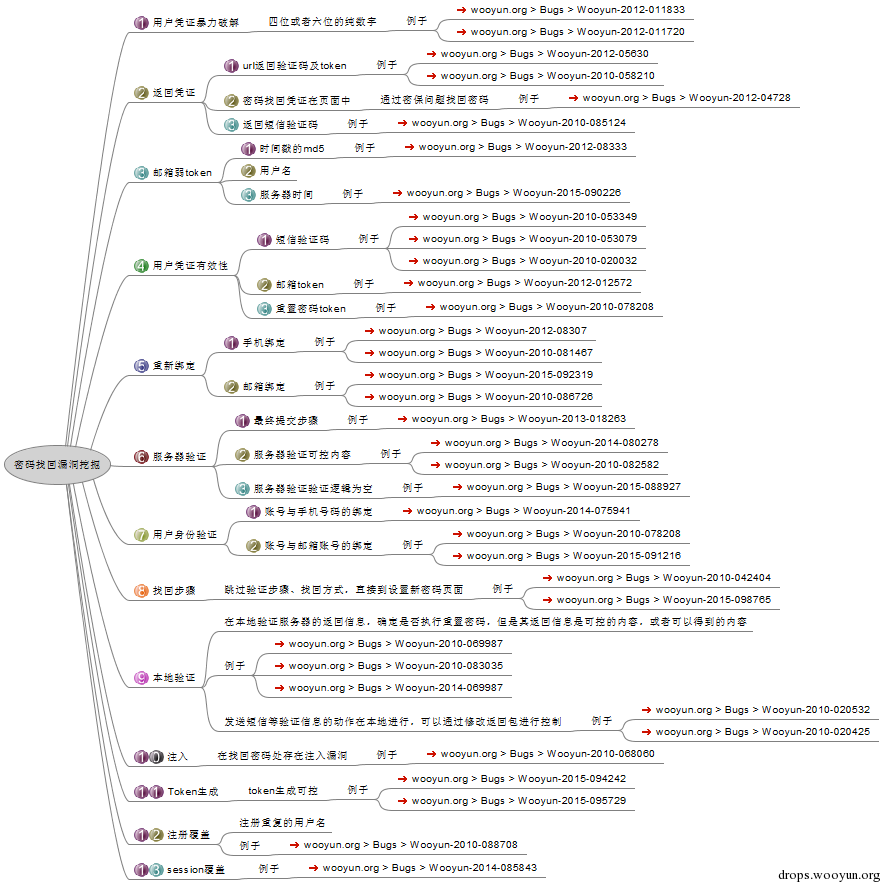
<script>

var username="1";alert(/XSS/);//";

</script>

**5、密码找回逻辑**

**案例：**<http://drops.wooyun.org/web/5048>



**6、验证码突破**

6.1验证码短且一段时间内不更改，可以爆破

**案例：**[WooYun: 盟友88电商平台任意用户注册与任意用户密码重置漏洞打包](http://www.wooyun.org/bugs/wooyun-2015-093932" \t "_blank)

6.2有些验证码的内容会回显到客户端

6.3绕过，看能否通过访问下一步的url直接绕过验证码

**案例：**[WooYun: 中国电信某IDC机房信息安全管理系统设计缺陷致使系统沦陷](http://www.wooyun.org/bugs/wooyun-2015-098765" \t "_blank)

6.4Js绕过，如果使用js前端验证可以直接绕过

**7、业务授权**

7.1未授权访问：利用google hacking，探查到网站后台，直接进行访问，或者只利用js进行跳转（曾出现过这个问题）

7.2越权访问：例如使用合法账户登录后，修改id为其他值，来实现越权访问

**案例：**[PHPEMS多处存在水平权限问题](http://www.wooyun.org/bugs/wooyun-2010-0100991)

**8、业务流程乱序**

8.1执行顺序缺陷，例如一个步骤需要A🡺B🡺C🡺D，假设可以A🡺C🡺D就可以直接绕

过一个步骤，比如支付、身份验证等

**案例：**[WooYun: 万达某分站逻辑错误可绕过支付直接获得取票密码](http://www.wooyun.org/bugs/wooyun-2014-047677" \t "_blank)

**9、业务接口安全**

9.1无限制发送短信验证码

**案例：**[WooYun: 一亩田交易网逻辑漏洞（木桶原理）](http://www.wooyun.org/bugs/wooyun-2015-094545" \t "_blank)

**10、时效绕过**

10.1例如利用JS实现搜索等业务必须间隔一定时间才能第二次操作，那么在控制台中就可以直接将这个时间缩短到1s来实现无限制访问

**案例：**[WooYun: 12306自动刷票时间可更改漏洞](http://www.wooyun.org/bugs/wooyun-2014-048391" \t "_blank)