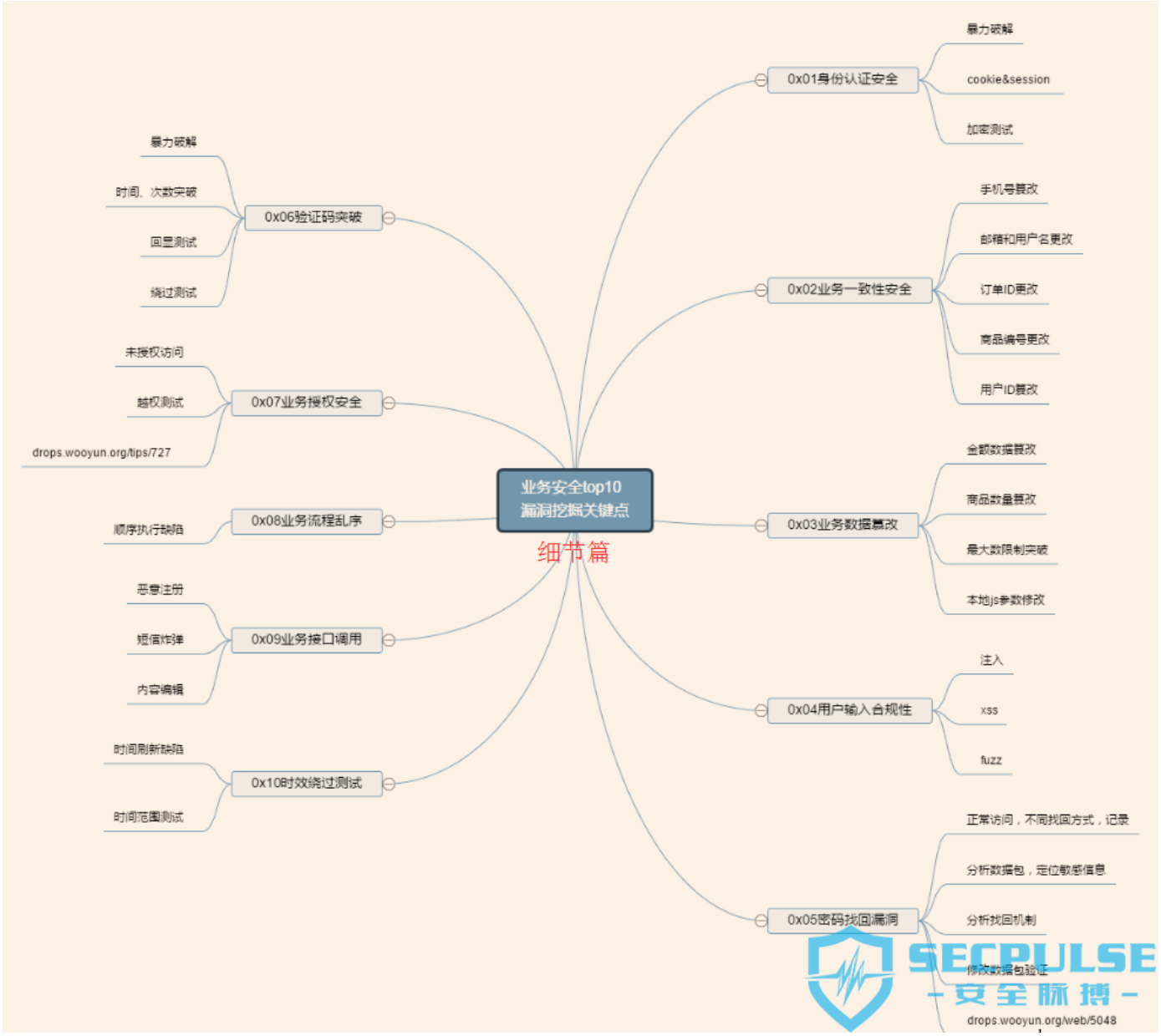
业务安全漏洞挖掘归纳总结

BurpSuitehtpwdScanspike 业务一致性安全业务安全业务安全漏洞业务安全的漏洞检测模型业务授权安全业务接口调用安全业务数据篡改业务流程乱序安全漏洞密码找回漏洞总结时效绕过测试漏洞漏洞挖掘漏洞检测模型用户输入合规性身份认证安全验证码突破
2015 /7/3 16:16
55
沙发

0x00 索引说明

6.30 在 OWASP 的分享，关于业务安全的漏洞检测模型。进一步的延伸科普。



0x01 身份认证安全

---

1 暴力破解

在没有验证码限制或者一次验证码可以多次使用的地方，使用已知用户对密码进行暴力破解或者用一个通用密码对用户进行暴力破解。 简单的验证码爆破。URL: http://zone.wooyun.org/content/20839

一些工具及脚本

Burpsuite

htpwdScan 撞库爆破必备 URL: https://github.com/lijiejie/htpwdScan

hydra 源码安装 xhydra 支持更多的协议去爆破（可破 WEB，其他协议不属于业务安全的范畴）

2 session & cookie 类

会话固定攻击：利用服务器的 session 不变机制，借他人之手获得认证和授权，冒充他人。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！

Cookie 仿冒：修改 cookie 中的某个参数可以登录其他用户。 案例：益云广告平台任意帐号登录 WooYun: 益云广告平台任意帐号登录

3 弱加密

未使用 https，是功能测试点，不好利用。

前端加密，用密文去后台校验，并利用 smart decode 可解

0x02 业务一致性安全

---

1 手机号篡改

a）抓包修改手机号码参数为其他号码尝试，例如在办理查询页面，输入自己的号码然后抓包，修改手机号码参数为其他人号码，查看是否能查询其他人的业务。

2 邮箱或者用户篡改

a）抓包修改用户或者邮箱参数为其他用户或者邮箱

b）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

3 订单 id 篡改

a）查看自己的订单 id，然后修改 id（加减一）查看是否能查看其它订单信息。

b）案例： WooYun: 广之旅旅行社任意访问用户订单

4 商品编号篡改

a）例如积分兑换处，100 个积分只能换商品编号为 001,1000 个积分只能换商品编号 005，在 100 积分换商品的时候抓包把换商品的编号修改为 005，用低积分换区高积分商品。

b）案例：联想某积分商城支付漏洞再绕过 WooYun：联想某积分商城支付漏洞再绕过

5 用户 id 篡改

a）抓包查看自己的用户 id，然后修改 id（加减 1）查看是否能查看其它用户 id 信息。

b）案例： WooYun：拉勾网百万简历泄漏风险(包括手机、邮件、应聘职位等信息、还可冒充企业身份筛选简历、发面试通知等)

0x03 业务数据篡改

---

1 金额数据篡改

a）抓包修改金额等字段，例如在支付页面抓取请求中商品的金额字段，修改成任意数额的金额并提交，查看能否以修改后的金额数据完成业务流程。 b）案例： WooYun：12308 订单支付时的总价未验证漏洞(支付逻辑漏洞)

2 商品数量篡改

a）抓包修改商品数量等字段，将请求中的商品数量修改成任意数额，如负数并提交，查看能否以修改后的数量完成业务流程。 b）案例： WooYun：蔚蓝团支付逻辑漏洞(可负数支付)

3 最大数限制突破

a）很多商品限制用户购买数量时，服务器仅在页面通过 js 脚本限制，未在服务器端校验用户提交的数量，通过抓包修改商品最大数限制，将请求中的商品数量改为大于最大数限制的值，查看能否以修改后的数量完成业务流程。

4 本地 js 参数修改

a）部分应用程序通过 Javascript 处理用户提交的请求，通过修改 Javascript 脚本，测试修改后的数据是否影响到用户。

0x04 用户输入合规性

---

1 注入测试 请参考 http://wiki.wooyun.org/web:sql

2 XSS 测试 请参考 http://wiki.wooyun.org/web:xss

3 Fuzz

a) 功能测试用的多一些，有可能一个超长特殊字符串导致系统拒绝服务或者功能缺失。（当然 fuzz 不单单这点用途。）

b) 不太符合的案例，但思路可借鉴： WooYun: 建站之星模糊测试实战之任意文件上传漏洞

c) 可能会用的工具 —— spike

4 其他用用户输入交互的应用漏洞

0x05 密码找回漏洞

---

1 大力推荐 BMa 的《密码找回逻辑漏洞总结》

http://drops.wooyun.org/web/5048

a) 密码找回逻辑测试一般流程

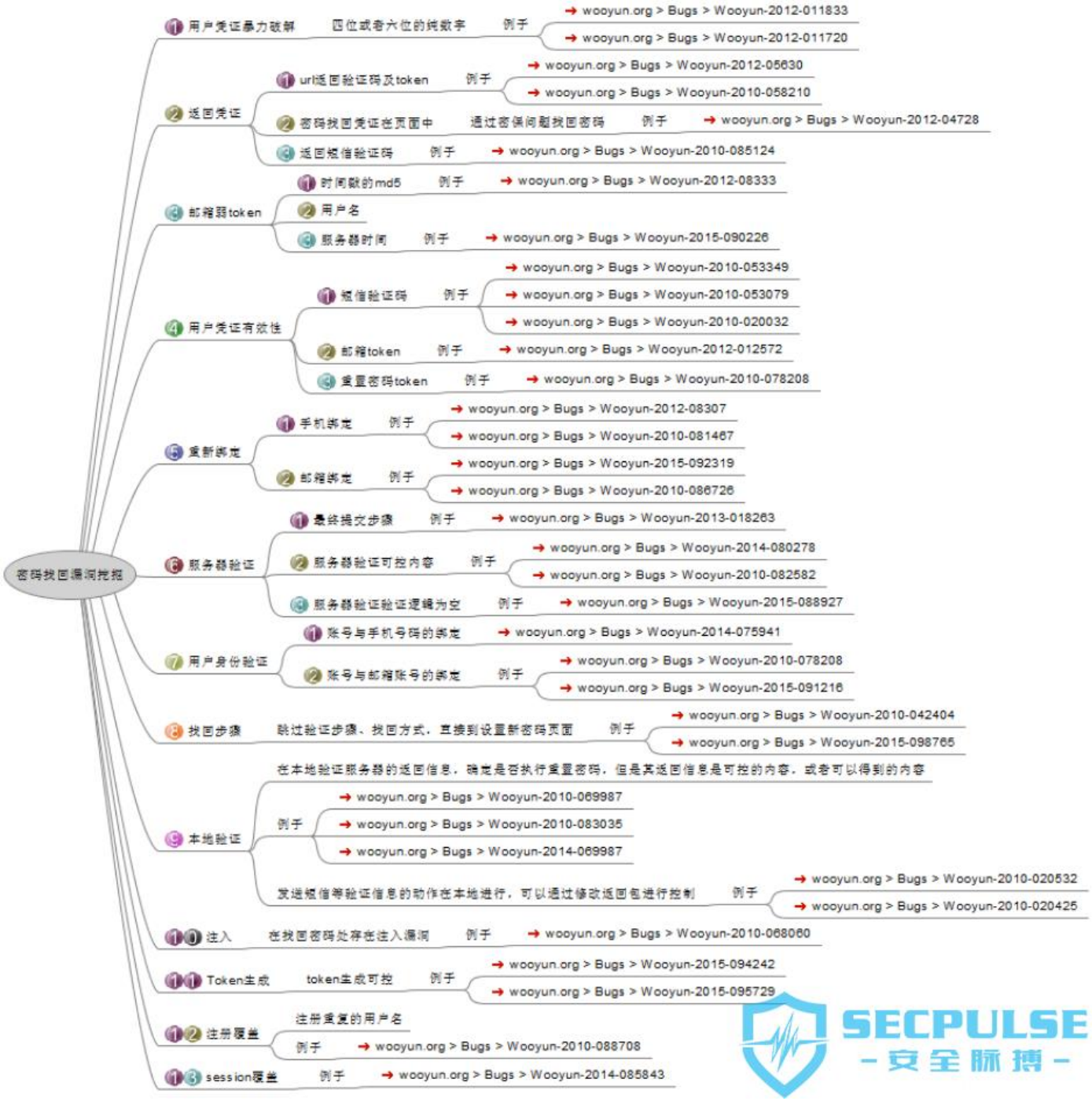
i. 首先尝试正常密码找回流程，选择不同找回方式，记录所有数据包

ii. 分析数据包，找到敏感部分

iii. 分析后台找回机制所采用的验证手段

iv. 修改数据包验证推测

b) 脑图 （详情请参考 BMa 的《密码找回逻辑漏洞总结》）



0x06 验证码突破

验证码不单单在登录、找密码应用，提交敏感数据的地方也有类似应用，故单独分类，并进一步详情说明。

1 验证码暴力破解测试

a）使用 burp 对特定的验证码进行暴力破解

b）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

2 验证码时间、次数测试

a）抓取携带验证码的数据包不断重复提交，例如：在投诉建议处输入要投诉的内容信息，及验证码参数，此时抓包重复提交数据包，查看历史投诉中是否存在重复提交的参数信息。

b）案例：

3 验证码客户端回显测试

a 当客户端有需要和服务器进行交互，发送验证码时，即可使用 firefox 按 F12 调出 firebug 就可看到客户端与服务器进行交互的详细信息

4 验证码绕过测试

a）当第一步向第二步跳转时，抓取数据包，对验证码进行篡改清空测试，验证该步骤验证码是否可以绕过。

b）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

5 验证码 js 绕过

a）短信验证码验证程序逻辑存在缺陷，业务流程的第一步、第二部、第三步都是放在同一个页面里，验证第一步验证码是通过 js 来判断的，可以修改验证码在没有获取验证码的情况下可以填写实名信息，并且提交成功。

0x07 业务授权安全

---

1 未授权访问

a）非授权访问是指用户在没有通过认证授权的情况下能够直接访问需要通过认证才能访问到的页面或文本信息。可以尝试在登录某网站前台或后台之后，将相关的页面链接复制于其他浏览器或其他电脑上进行访问，看是否能访问成功。

2 越权访问

越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定

a）垂直越权（垂直越权是指使用权限低的用户可以访问权限较高的用户）

b）水平越权（水平越权是指相同权限的不同用户可以互相访问）（wooyun-2010-0100991 PHPEMS多处存在水平权限问题）

c）《我的越权之道》URL：http://drops.wooyun.org/tips/727

0x08 业务流程乱序

---

1 顺序执行缺陷

a）部分网站逻辑可能是先 A 过程后 B 过程然后 C 过程最后 D 过程

b）用户控制着他们给应用程序发送的每一个请求，因此能够按照任何顺序进行访问。于是，用户就从 B 直接进入了 D 过程，就绕过了 C。如果 C 是支付过程，那么用户就绕过了支付过程而买到了一件商品。如果 C 是验证过程，就会绕过验证直接进入网站程序了。

c）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://wooyun.org/bugs/wooyun-2010-0108184

0x09 业务接口调用安全

---

1 重放攻击

在短信、邮件调用业务或生成业务数据环节中（类：短信验证码，邮件验证码，订单生成，评论提交等），对其业务环节进行调用（重放）测试。如果业务经过调用（重放）后被多次生成有效的业务或数据结果

a）恶意注册

b）短信炸弹

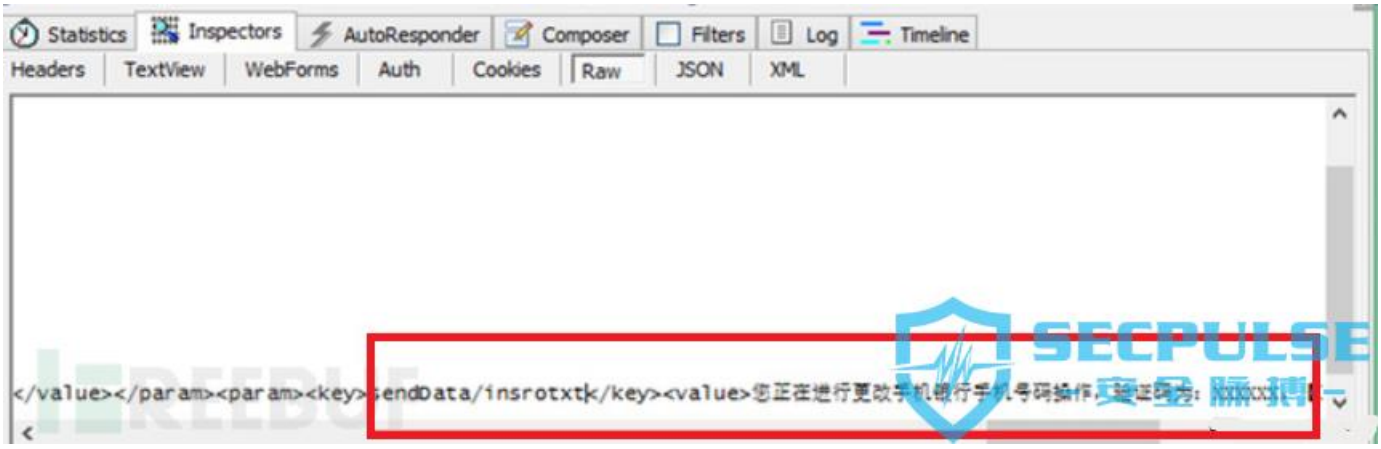
在测试的过程中，我们发现众多的金融交易平台仅在前端通过 JS 校验时间来控制短信发送按钮，但后台并未对发送做任何限制，导致可通过重放包的方式大量发送恶意短信

案例： WooYun: 一亩田交易网逻辑漏洞（木桶原理）

2 内容编辑

类似案例如下：

点击“获取短信验证码”，并抓取数据包内容，如下图。通过分析数据包，可以发现参数 sendData/insrotxt 的内容有客户端控制，可以修改为攻击者想要发送的内容



内容修改“恭喜你获得由 xx 银行所提供的 iphone6 一部，请登录 http://www.xxx.com 领取，验证码为 236694”并发送该数据包，手机可收到修改后的短信内容，如下图：

0x10 时效绕过测试

大多有利用的案例发生在验证码以及业务数据的时效范围上，在之前的总结也有人将 12306 的作为典型，故，单独分类。

1 时间刷新缺陷

12306 网站的买票业务是每隔 5s，票会刷新一次。但是这个时间确实在本地设置的间隔。于是，在控制台就可以将这个时间的关联变量重新设置成 1s 或者更小，这样刷新的时间就会大幅度缩短（主要更改 autoSearchTime 本地参数）。 案例：

WooYun: 12306 自动刷票时间可更改漏洞

2 时间范围测试

针对某些带有时间限制的业务，修改其时间限制范围，例如在某项时间限制范围内查询的业务，修改含有时间明文字段的请求并提交，查看能否绕过时间限制完成业务流程。例如通过更改查询手机网厅的受理记录的 month 范围，可以突破默认只能查询六个月的记录。

0x11 参考

@eversec

应用程序逻辑错误总结 http://drops.wooyun.org/papers/1418

密码找回功能可能存在的问题 http://drops.wooyun.org/papers/287

密码找回功能可能存在的问题（补充） http://drops.wooyun.org/web/3295

密码找回逻辑漏洞总结 http://drops.wooyun.org/web/5048

支付漏洞的三种常见类型——加固方案 http://zone.wooyun.org/content/878

在线支付逻辑漏洞总结 http://drops.wooyun.org/papers/345

金融行业平台常见安全漏洞与防御 http://www.freebuf.com/news/special/61082.html

我的越权之道 http://drops.wooyun.org/tips/727

安全科普：看视频理解 Web 应用安全漏洞 TOP10（IBM 内部视频）
http://www.freebuf.com/vuls/63426.html