唯品会 vip.com

唯品会安全应急响应中心
VIP Security Response Center

2016唯品会互联网电商安全峰会

电商安全的闭环

电商安全体系建设的血与泪

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

探寻业务安全中的极(基)点

--江南天安猎户实验室.张洪骏

- 初探电商
- 电商安全现状
- 业务安全漏洞分析
- 如何应对业务安全漏洞

电子商务是基于计算机技术、网络技术、通信技术和应用软件开发基础上的新兴的、充满生气的经济活动。

电子商务主要基于Internet开展，Internet的特点就是随时随地、方便易用、即时互动并且结合多媒体传递，这些为电子商务的信息流、商流（如电子合同）、物流信息的交互与共享、全天候跨区域与低成本处理提供了很好的技术支撑。因此，电子商务无论是在中国还是在全球，都在快速的发展。

钱存在的地点

银行远程账户
资金支付

传输的渠道

商户渠道

消费者渠道

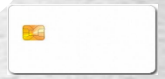
受理终端


终端


PC


移动

支付工具



预授权交易流程：电子交易实体间的关系

(1)创建账户

(2)注册会员

(3)账户绑定

(4)浏览商品提交订单

(5)预授权请求

(6)预授权请求

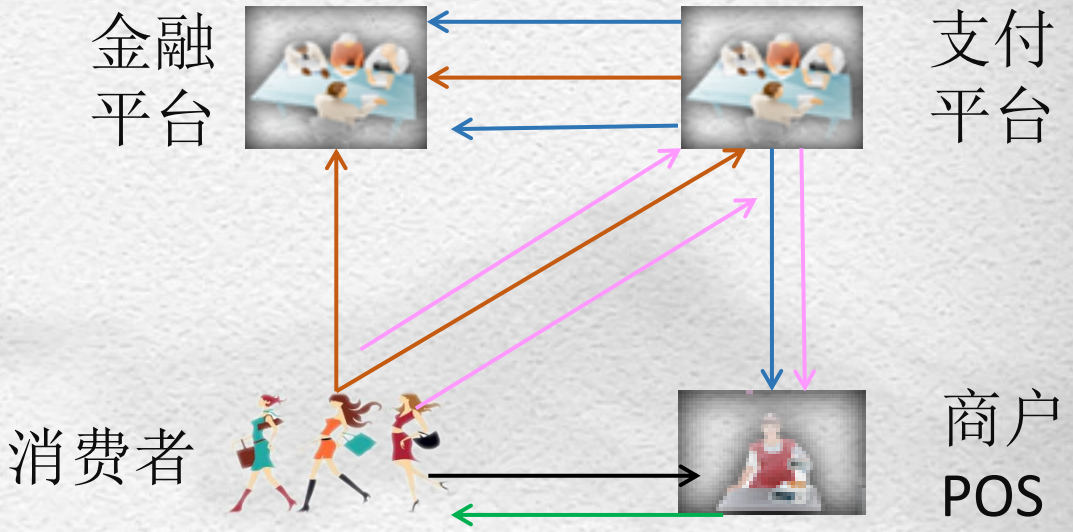
(7)预授权凭证

(8)提供商品或服务

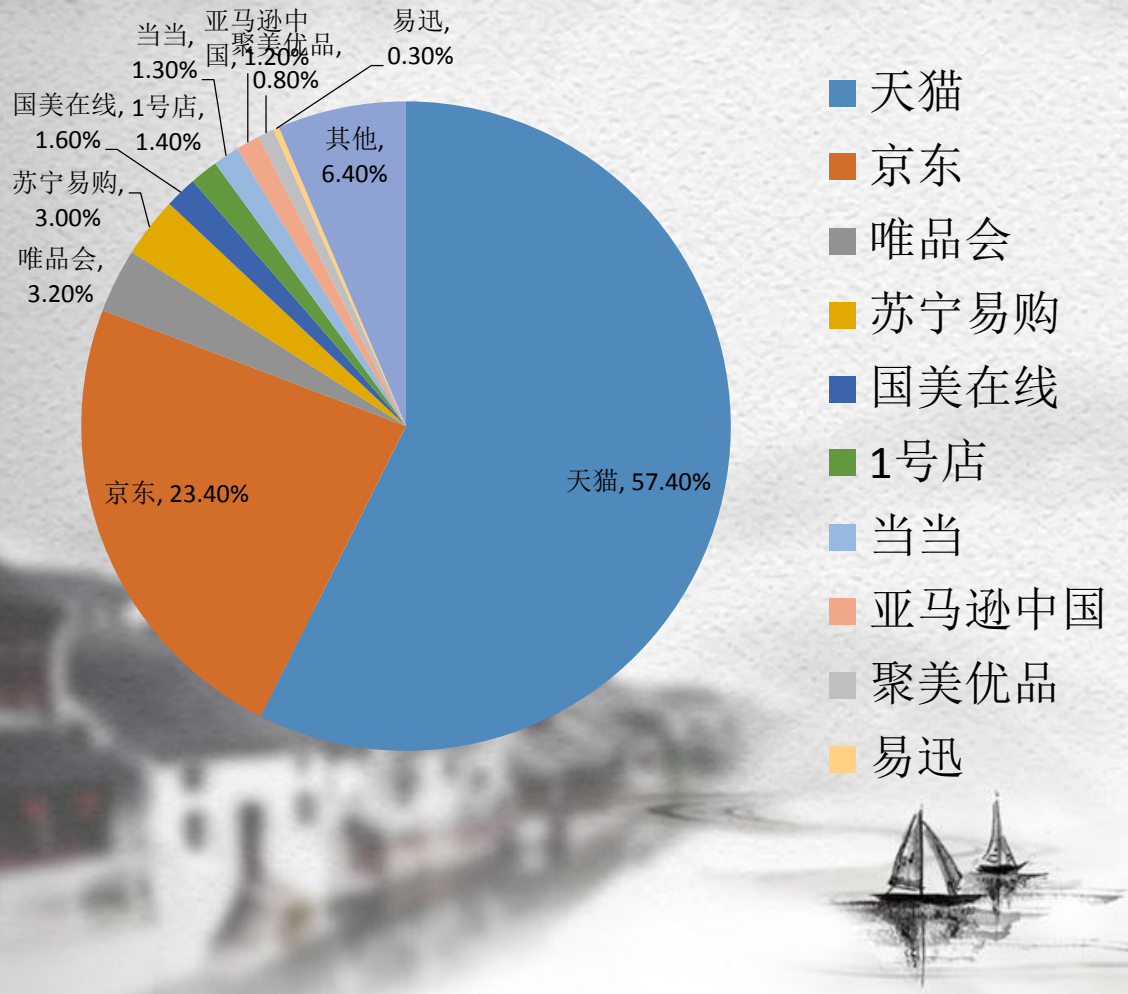
(9)支付请求

(10)转发支付请求

(11)支付凭证



2015 年，中国 B2C 网络零售市场.市场份额



市场规模：2015 年，中国网络零售市场交易规模 **38285** 亿元，同比增长 35.7%。

- 初探电商
- 电商安全现状
- 业务安全漏洞分析
- 如何应对业务安全漏洞

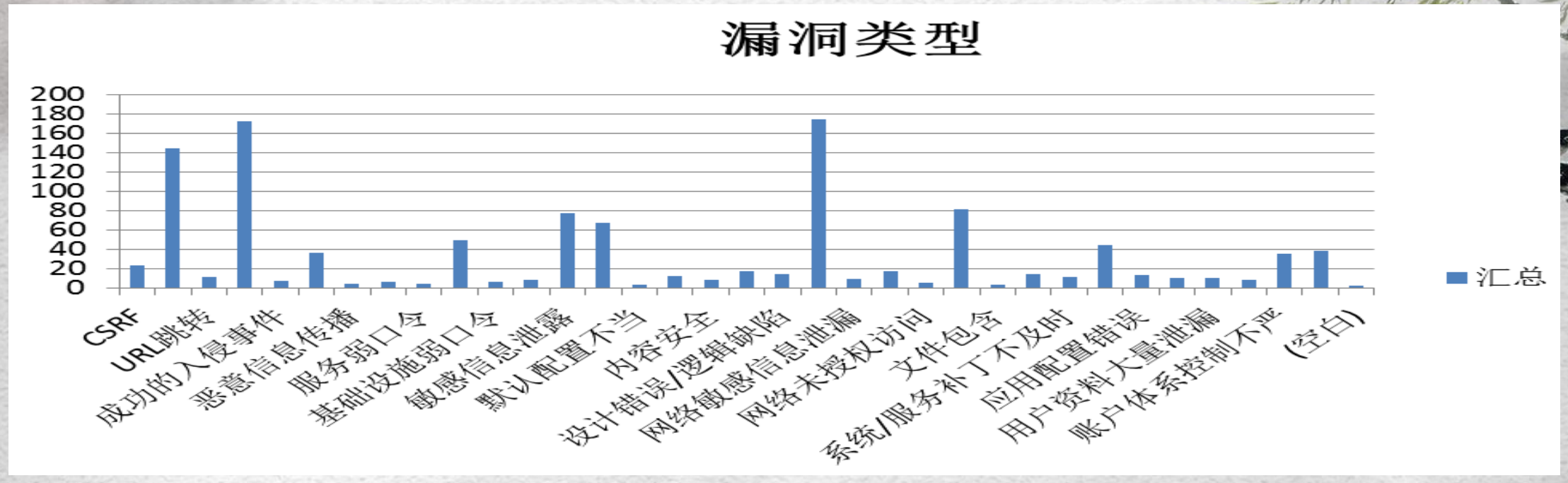
电子商务现状

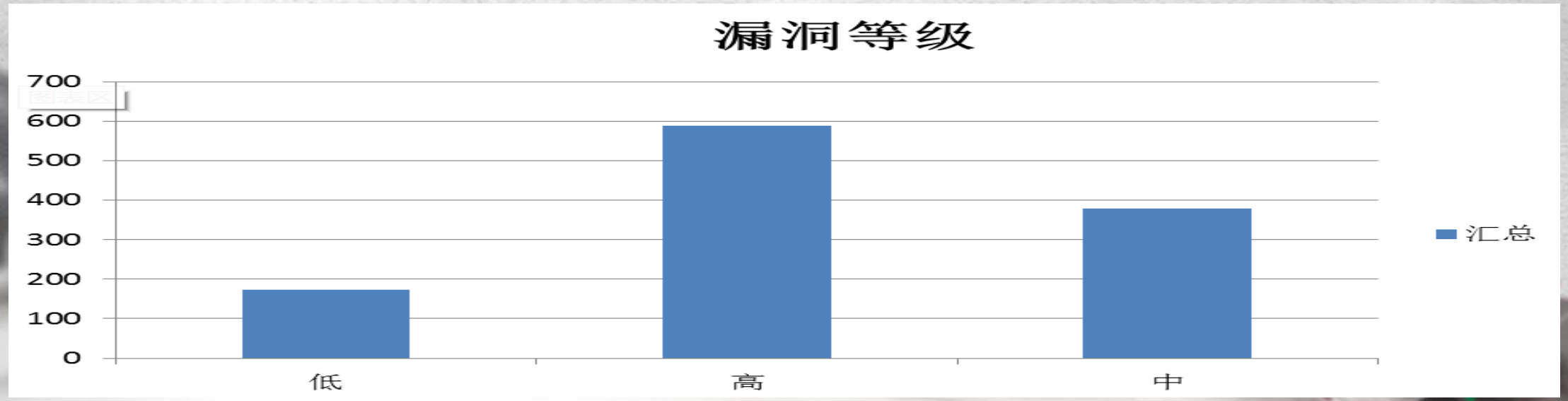
2014年全年，360网站安全检测平台共扫描各类网站164.2万个，其中存在安全漏洞的网站61.7万个。从行业来看，电子商务类网站存在高危漏洞的比例最高，达到26%，银行类网站安全性相对较高。 -

--------《2014年中国网站安全报告》

中国平均每天有24.5个电商网站遭受入侵和攻击，在针对电商网站实施的侵害中，利用网站安全漏洞入侵占绝大多数 ，占比97%；另外3%为针对电商网站的CC攻击等攻击行为 。

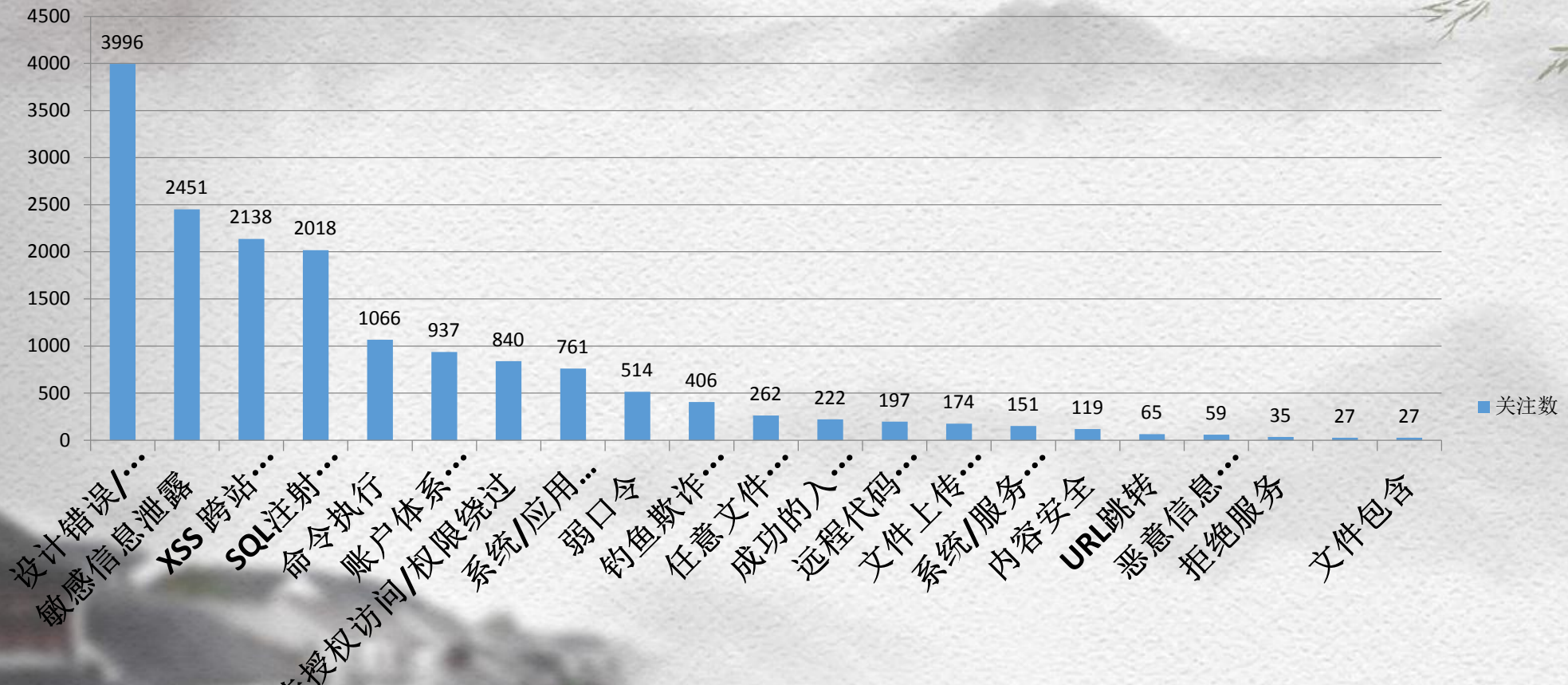
------《2013年中国电商行业网站安全检测报告》


漏洞类型
200
180
160
140
120
100
80
60
40
20
0
CSRF
URL跳转
成功的入侵事件
恶意信息传播
服务弱口令
基础设施弱口令
敏感信息泄露
默认配置不当
内容安全
设计错误/逻辑缺陷
网络敏感信息泄漏
网络未授权访问
文件包含
系统/服务补丁不及时
应用配置错误
用户资料大量泄漏
账户体系控制不严
(空白)
汇总


漏洞等级
700
600
500
400
300
200
100
0
低
高
中
汇总

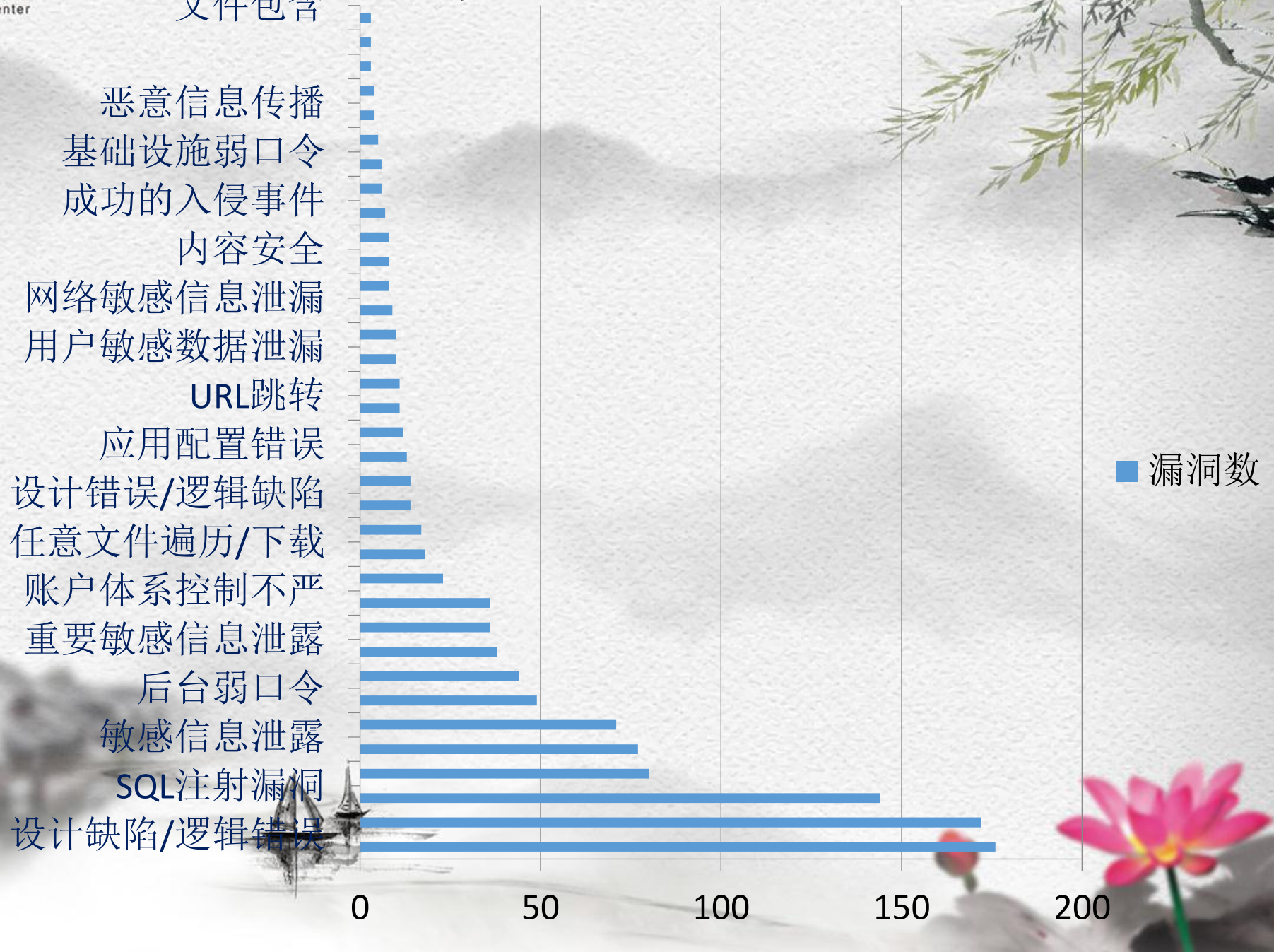
唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

关注点



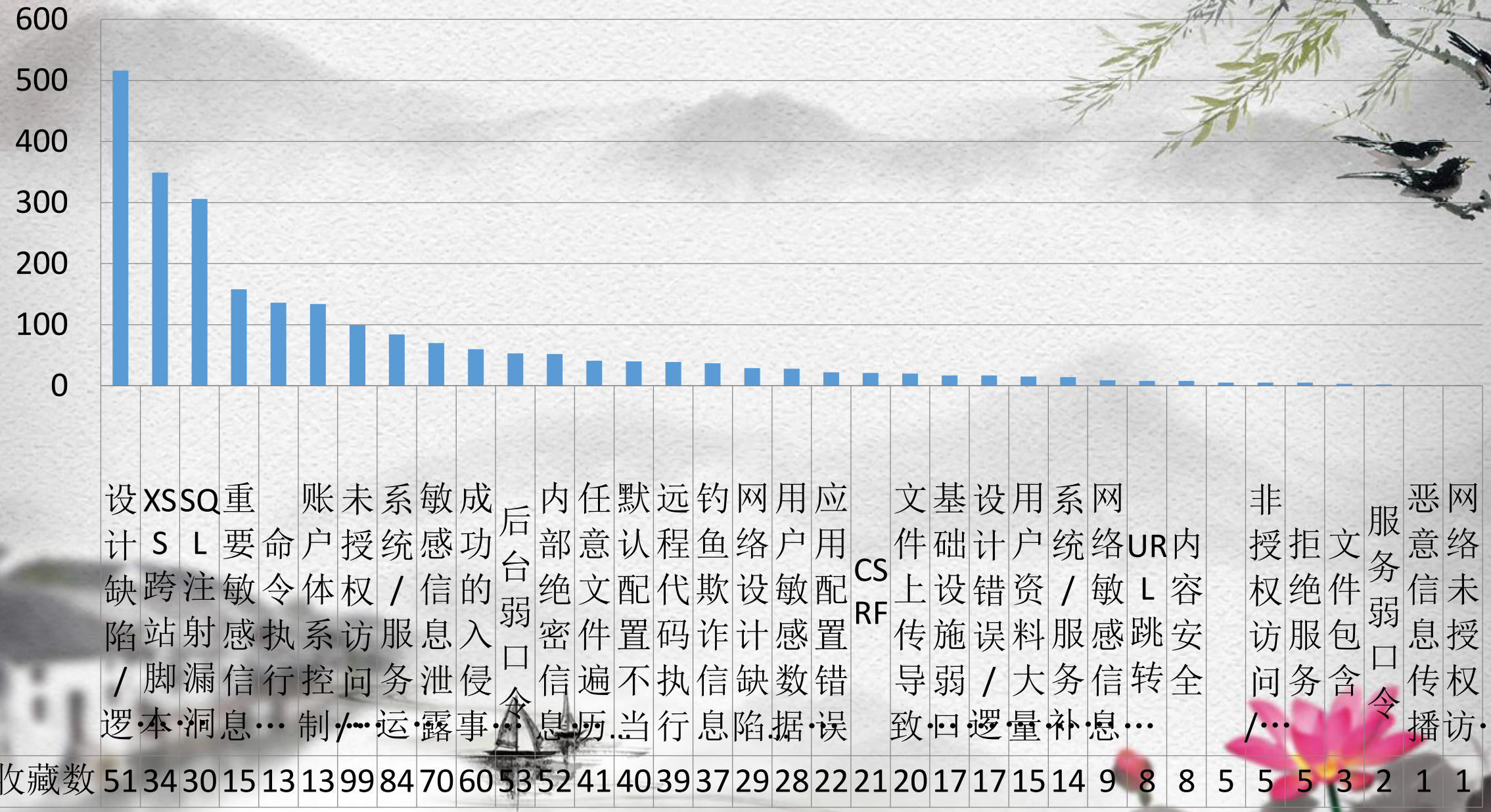
漏洞类型	关注数
	27
CSRF	101
SQL注射漏洞	2018
URL跳转	65
XSS 跨站脚本攻击	2037
成功的入侵事件	222
钓鱼欺诈信息	406
恶意信息传播	59
非授权访问/认证绕过	24
服务弱口令	25
后台弱口令	410
基础设施弱口令	79
拒绝服务	35
敏感信息泄露	639
命令执行	1066
默认配置不当	149
内部绝密信息泄漏	381
内容安全	119

漏洞类型排名


文件包含
恶意信息传播
基础设施弱口令
成功的入侵事件
内容安全
网络敏感信息泄漏
用户敏感数据泄漏
URL跳转
应用配置错误
设计错误/逻辑缺陷
任意文件遍历/下载
账户体系控制不严
重要敏感信息泄露
后台弱口令
敏感信息泄露
SQL注射漏洞
设计缺陷/逻辑错误
0
50
100
150
200
漏洞数

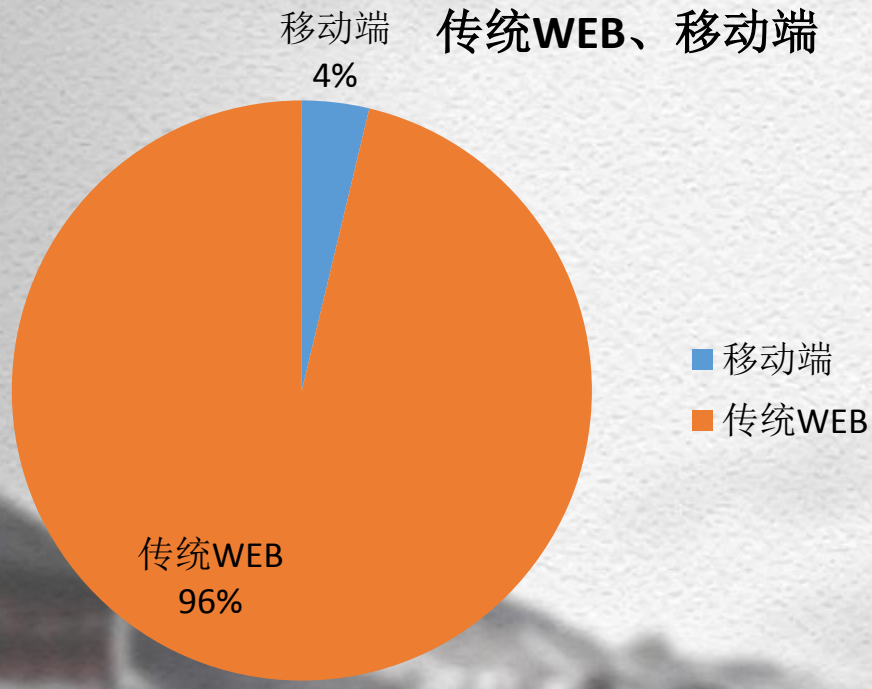
唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

收藏数

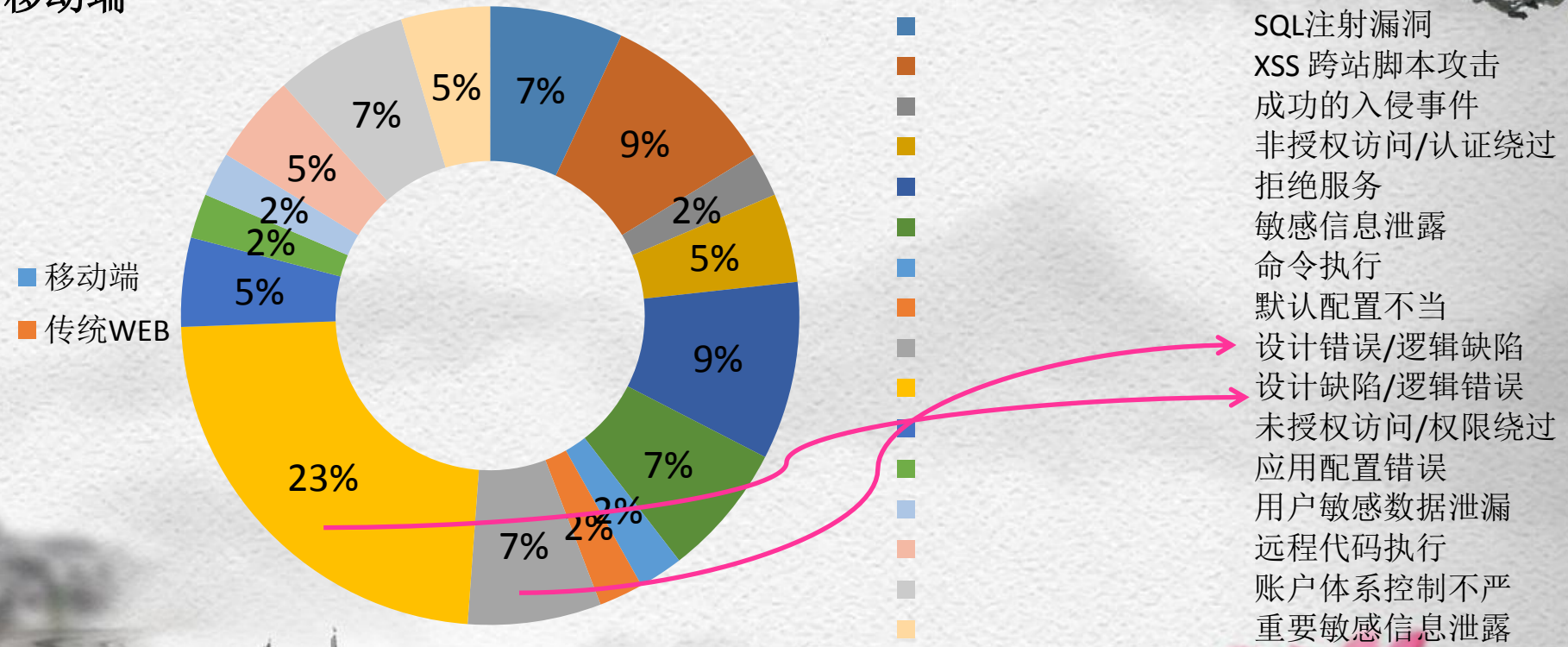


传统WEB---移动端的兴起

传统WEB、移动端



移动端漏洞类型



- 初探电商
- 电商安全现状
- 业务安全漏洞分析
- 如何应对业务安全漏洞


业务漏洞挖掘
0x01身份认证安全
0x02业务一致性安全
0x03业务数据篡改
0x04用户输入合规性
0x05密码找回漏洞
0x06验证码突破
0x07业务授权安全
0x08业务流程乱序
0x09业务接口调用
0x10时效绕过测试

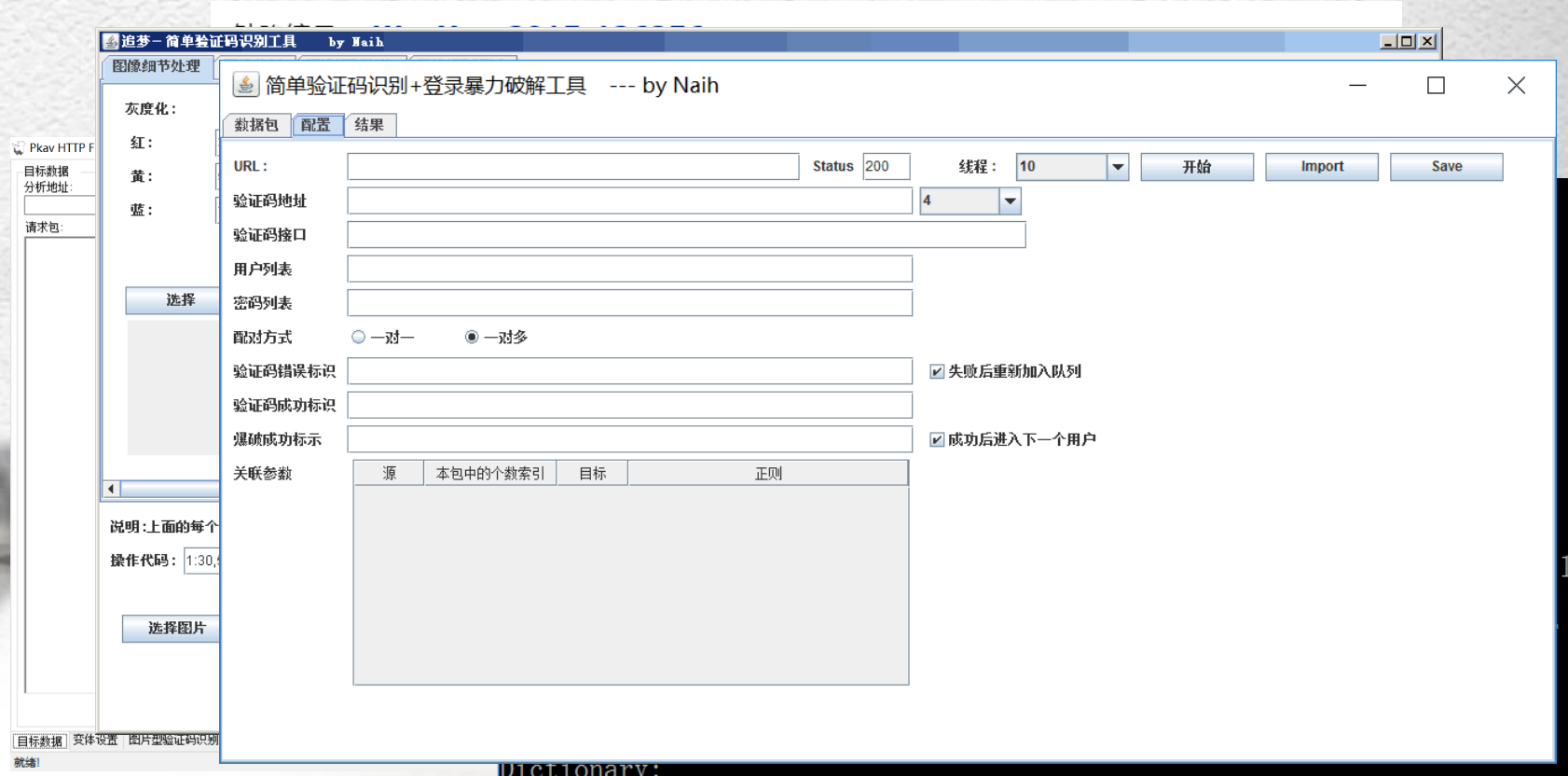
0X01身份认证

暴力破解

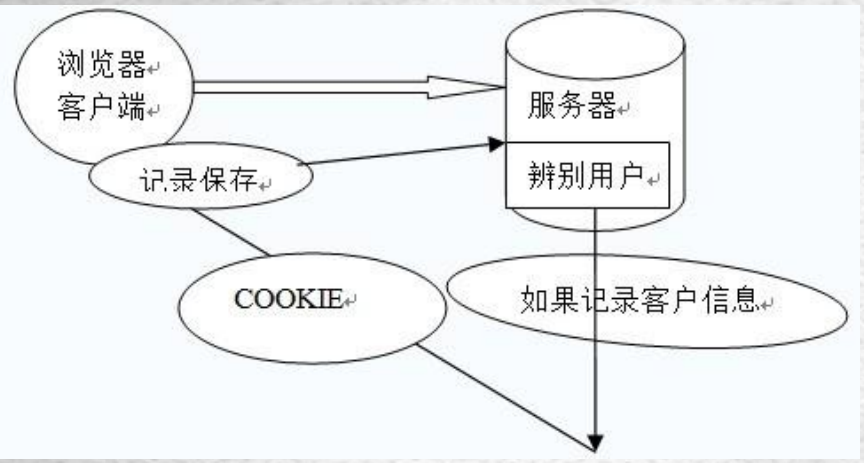
*无验证码限制，或验证码可多次使用，或有验证码但仅作当前页面验证,接口无视

*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

验证码：



Cookie



简要描述：

益云广告平台任意帐号登录

详细说明：

只需要添加cookie

yibouid=数字 即可登录任意用户帐号！

漏洞证明：

通过遍历 找到一个官方管理的ID 291

登录

Session

一些网站对于用户是否成功登录不是看用户名与密码是否与数据库里面的匹配，而是看cookies是否为空或session是否为true。这样的问题的假设就是开发者认为用户能够登录，那么cookies就不会为空或session就不会为false。但是逻辑缺陷很明显，那么只要能知道用户ID，然后构造一个cookies或让session值为true就可以绕过这样的认证了。

0X01身份认证

弱加密

前端js校验

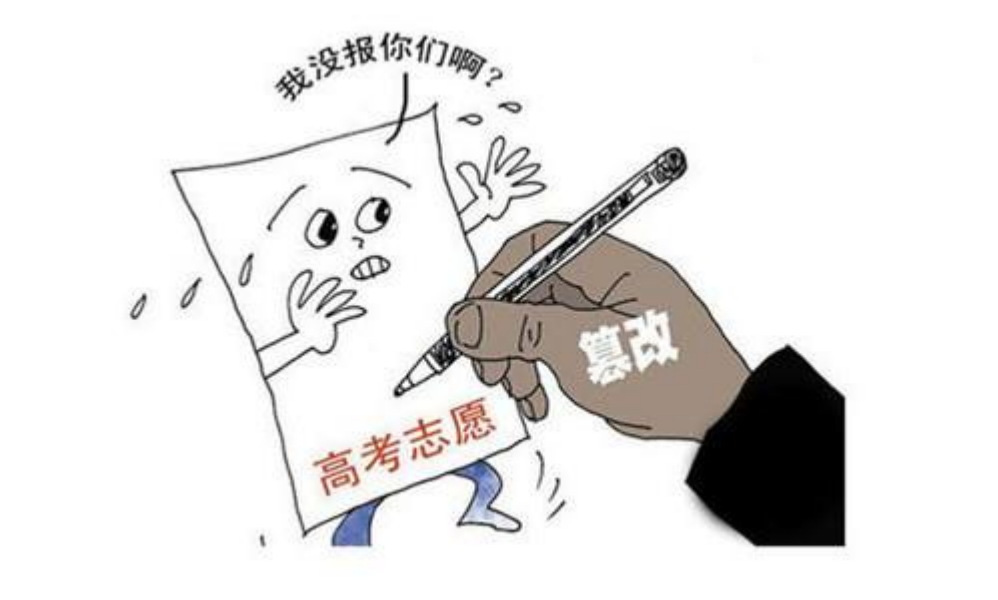
0X02业务一致性安全

0X02业务一致性安全

手机号篡改　订单号篡改　用户id篡改　商品编号篡改　其他业务篡改

抓包修改手机号码参数为
尝试，例如在办理查询
自己的号码然后抓包，修
码参数为其他人号码，查
查询其他人的业务

0X03业务数据篡改



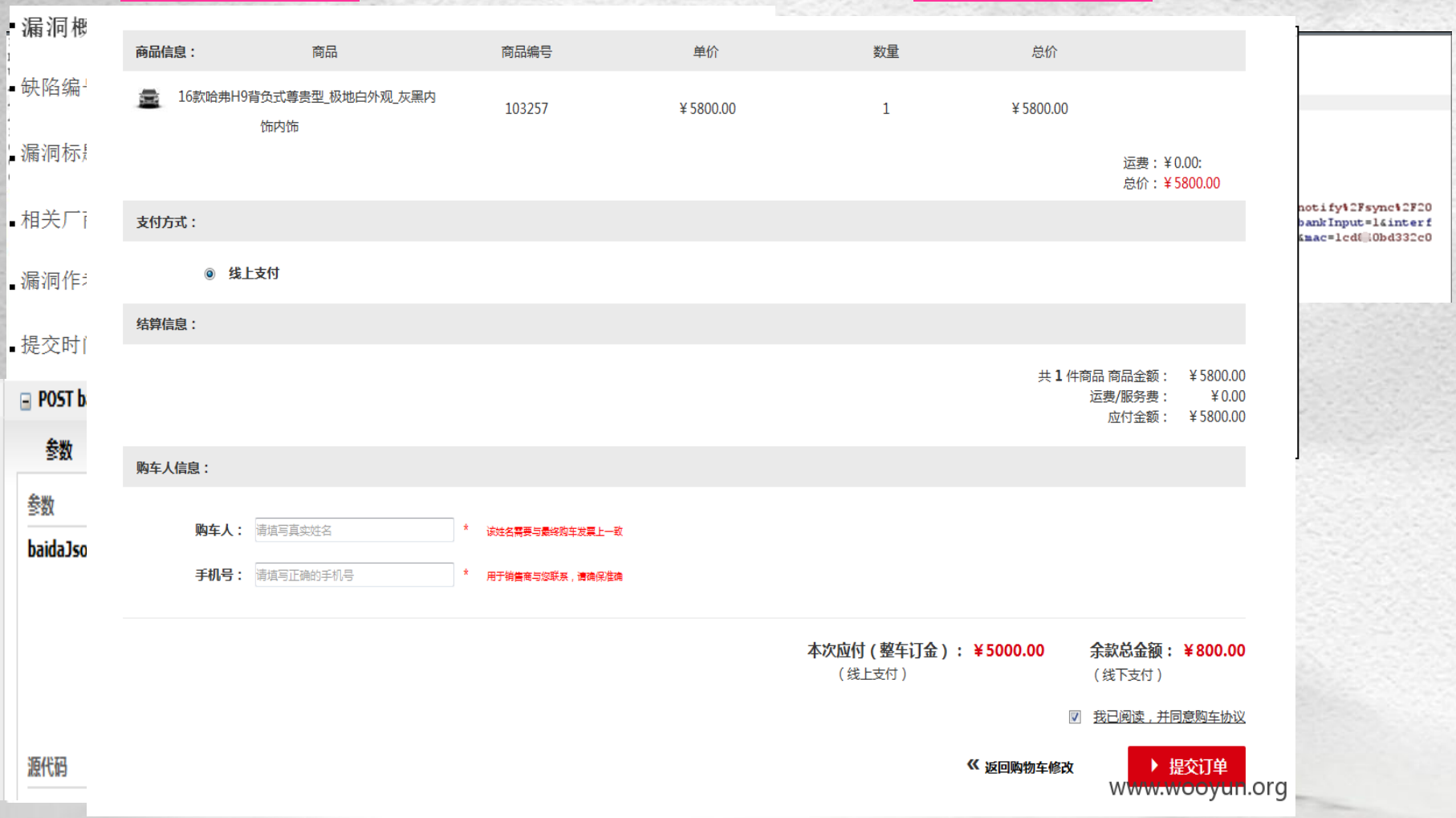
唯品会安全应急响应中心
VIP Security Response Center

0X03业务数据篡改

金额篡改

数量篡改

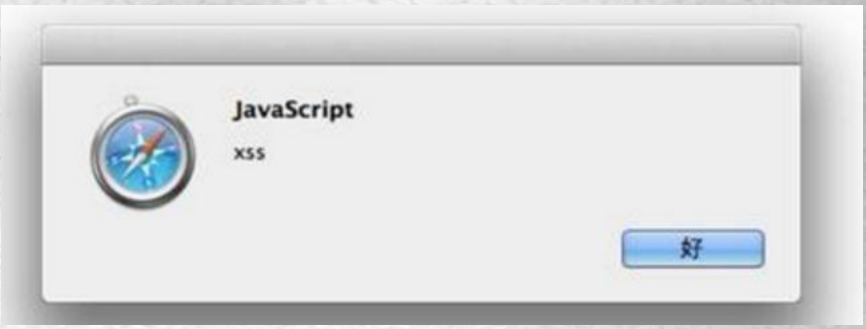
突破限制



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

0X04用户输入合规性

- 注入
- 跨站XSS
- 其他交互功能导致的应用漏洞



唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

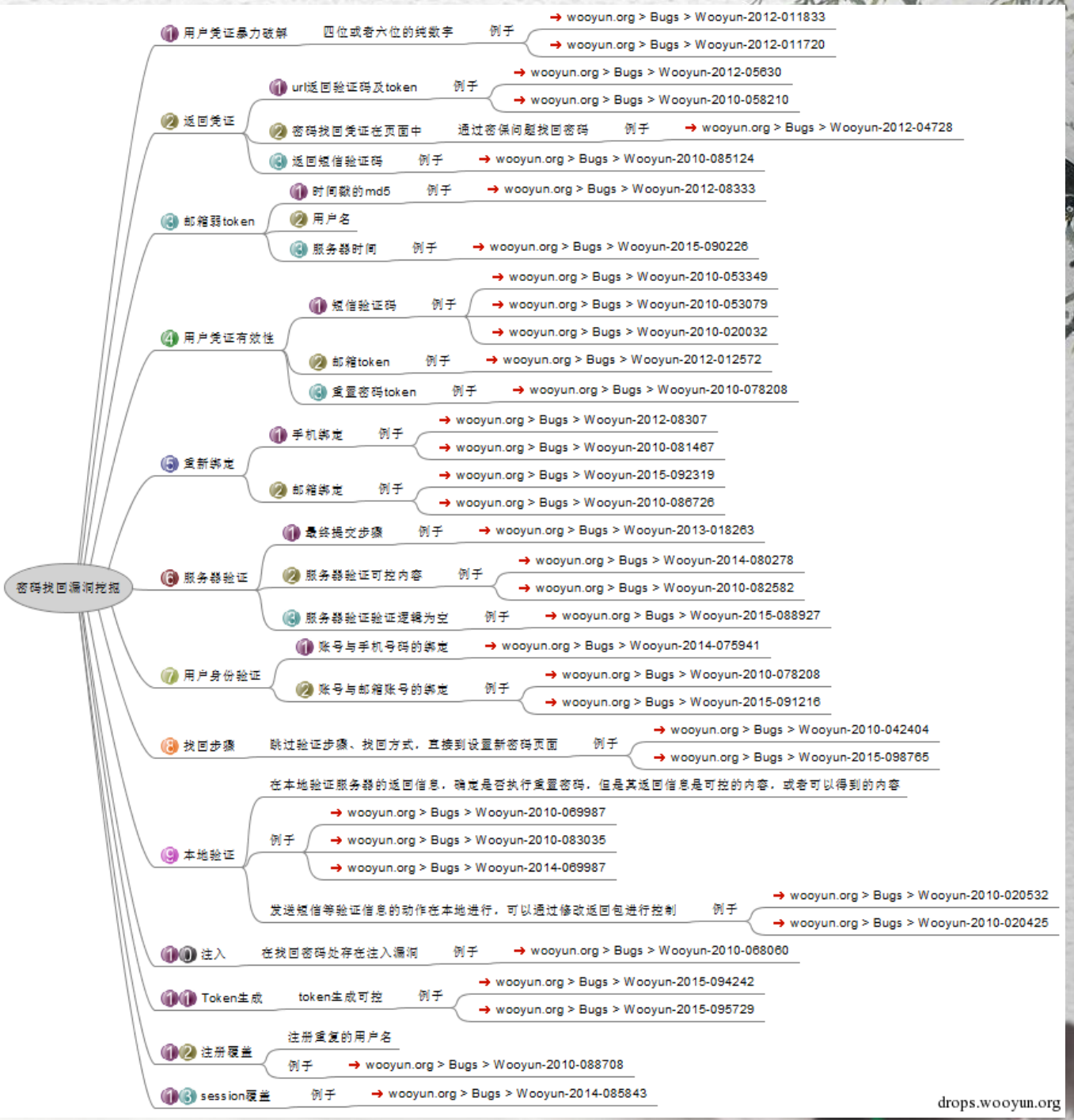
0X05密码找回漏洞

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



0x06 验证码突破

0x06 验证码突破

暴力破解

使用burp对特定的验证码进行暴力破解

客户端回显

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

重复提交、忽略次数

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

各种绕过

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

0x07业务授权安全

未授权访问

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

越权访问

- 垂直越权
- 水平越权

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

唯品会 vip.com | 唯品会安全应急响应中心 VIP Security Response Center

漏洞概要

缺陷编号： WooYun-2015-108184

漏洞标题： 淘美网逻辑漏洞美女QQ、手机号等信息免费任意看（1分钱都不给）

相关厂商： 淘美网

漏洞作者： 提莫

提交时间： 2015-04-15 19:11

公开时间： 2015-05-30 19:12

漏洞类型： 设计缺陷/逻辑错误

危害等级： 高

自评Rank： 20

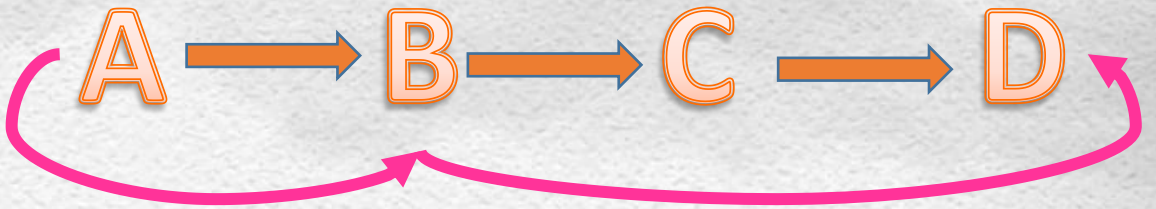
漏洞状态： 未联系到厂商或者厂商积极忽略

http://www.3need.com/index.php?controller=site&action=payok&out_trade_no=充值订单号

0x08业务流程乱序

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：

0x09业务接口调用安全

重放攻击

恶意注册/评论

短信轰炸

其他

内容编辑

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

0x10 时效绕过测试

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

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

- 初探电商
- 电商安全现状
- 业务安全漏洞分析
- 如何应对业务安全漏洞

C **保密性（Confidentiality）——** 确保信息在存储、使用、传输过程中不会泄漏给非授权用户或实体。

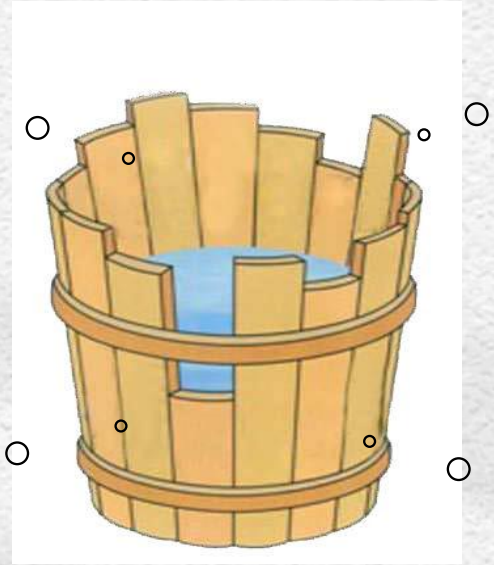
I **完整性（Integrity）——** 确保信息在存储、使用、传输过程中不会被非授权篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性。

A **可用性（Availability）——** 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。


用户输入合规性
可用性
验证码突破
业务授权安全
保密性
时效绕过测试
业务一致性安全
密码找回漏洞
完整性
身份认证安全
业务接口调用安全
业务数据篡改
业务流程乱序

组织

设备



制度

技术

业务

Mary的爸爸有5个女儿:
第1个女儿 Nana，
第2个女儿 Nene，
第3个女儿 Nini，
第4个女儿 Nono，
第5个女儿?????

Mary

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

不忽略任何可能出现风险或者歧义的细节

保障企业以及消费者安全最大化

建设一个更加安全、高效的电商环境

唯品会 vip.com 唯品会安全应急响应中心 VIP Security Response Center

感谢您的聆听！