

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

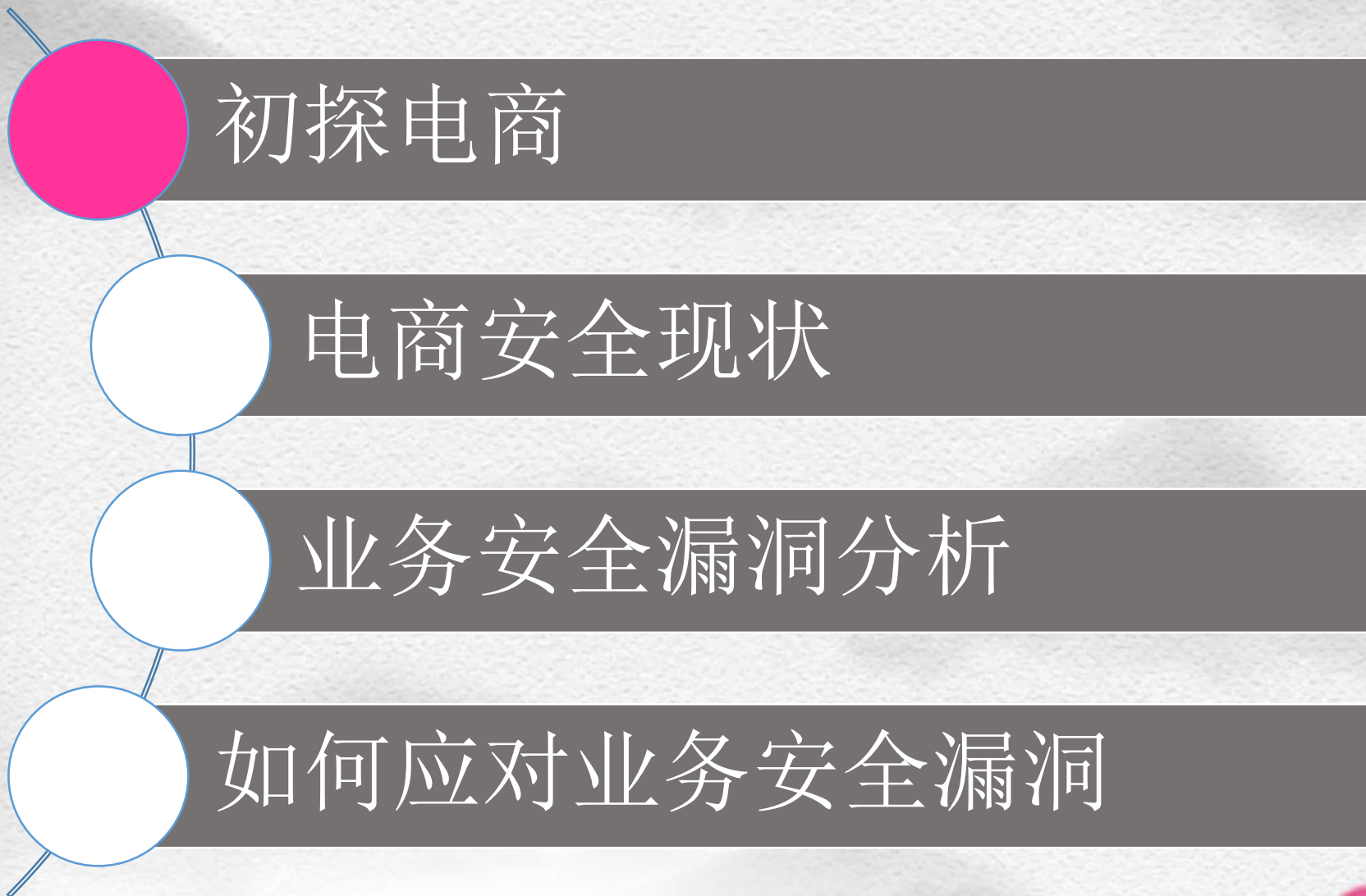
电商安全的闭环

电商安全体系建设的血与泪

探寻业务安全中的极(基)点

--江南天安猎户实验室.张洪骏







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。



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

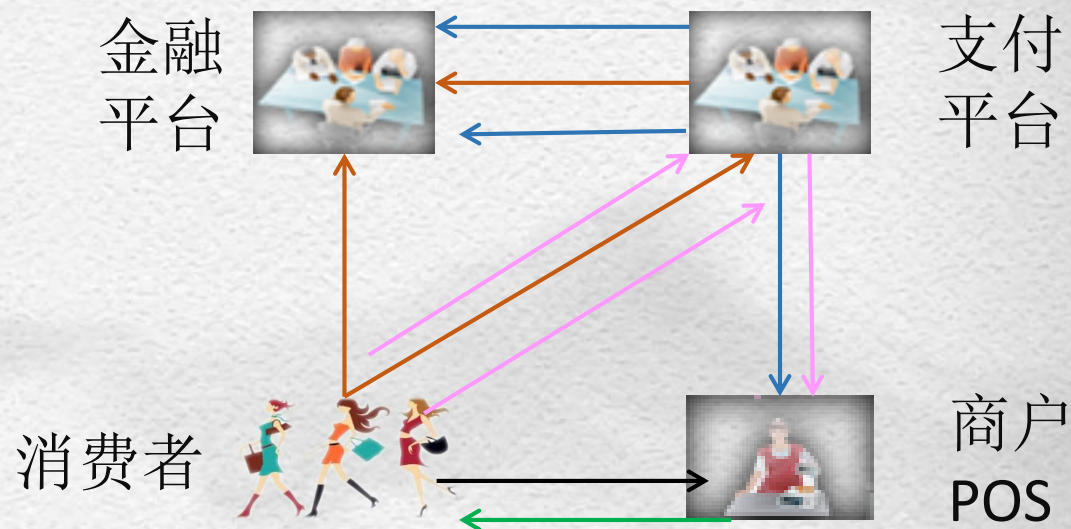
(7)预授权凭证

(8)提供商品或服务

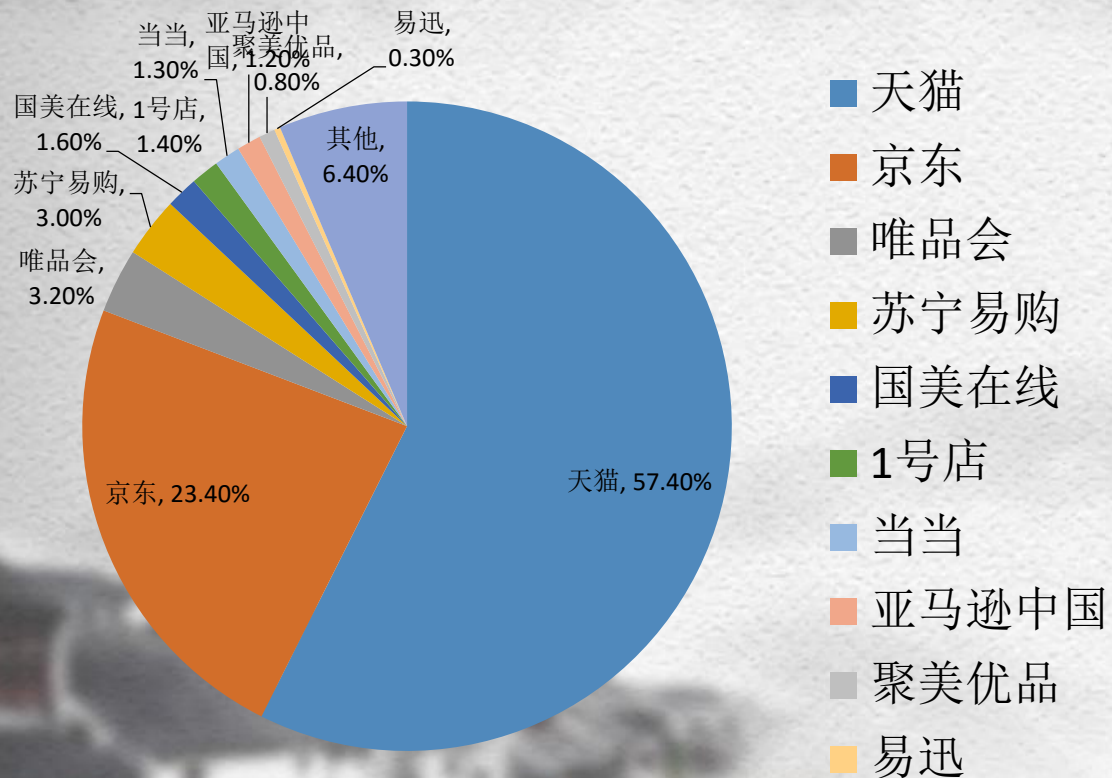
(9)支付请求

(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。 -

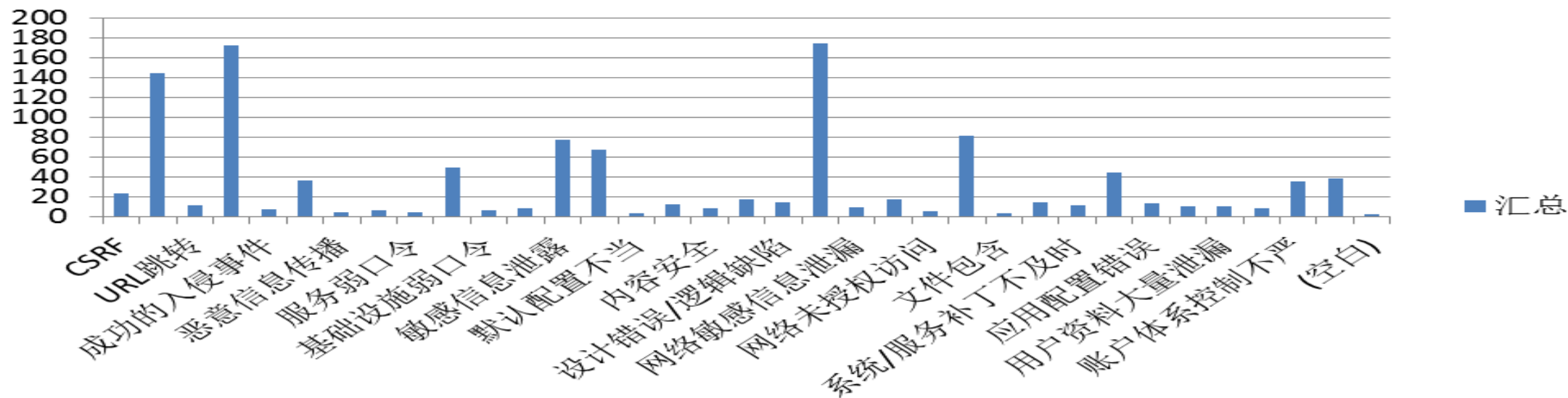
----- 《2014年中国网站安全报告》

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。

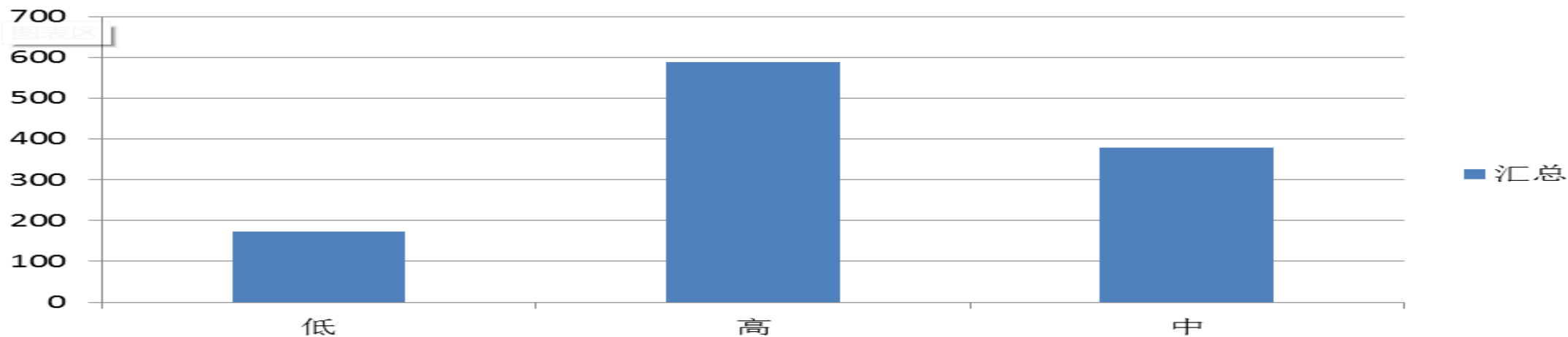
----- 《2013年中国电商行业网站安全检测报告》



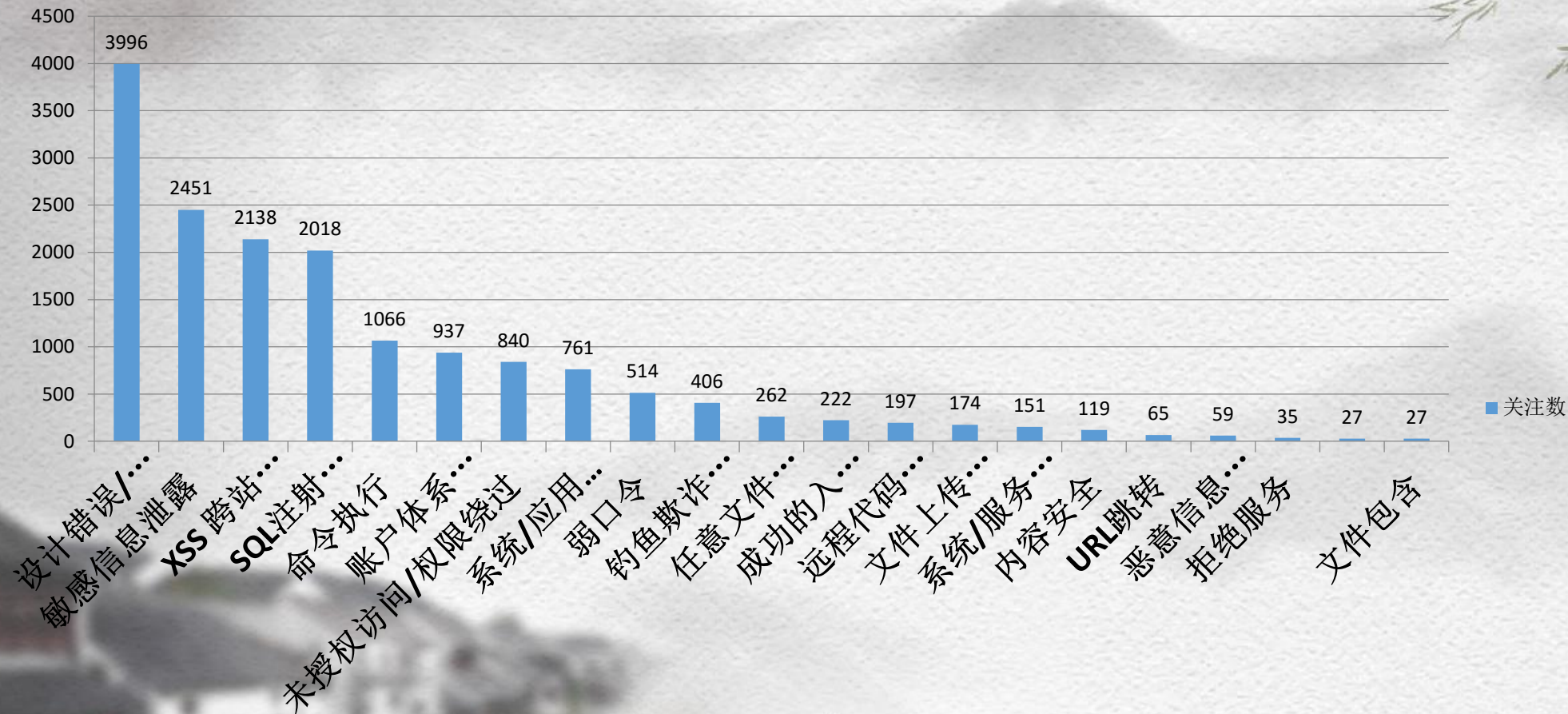
漏洞类型



漏洞等级

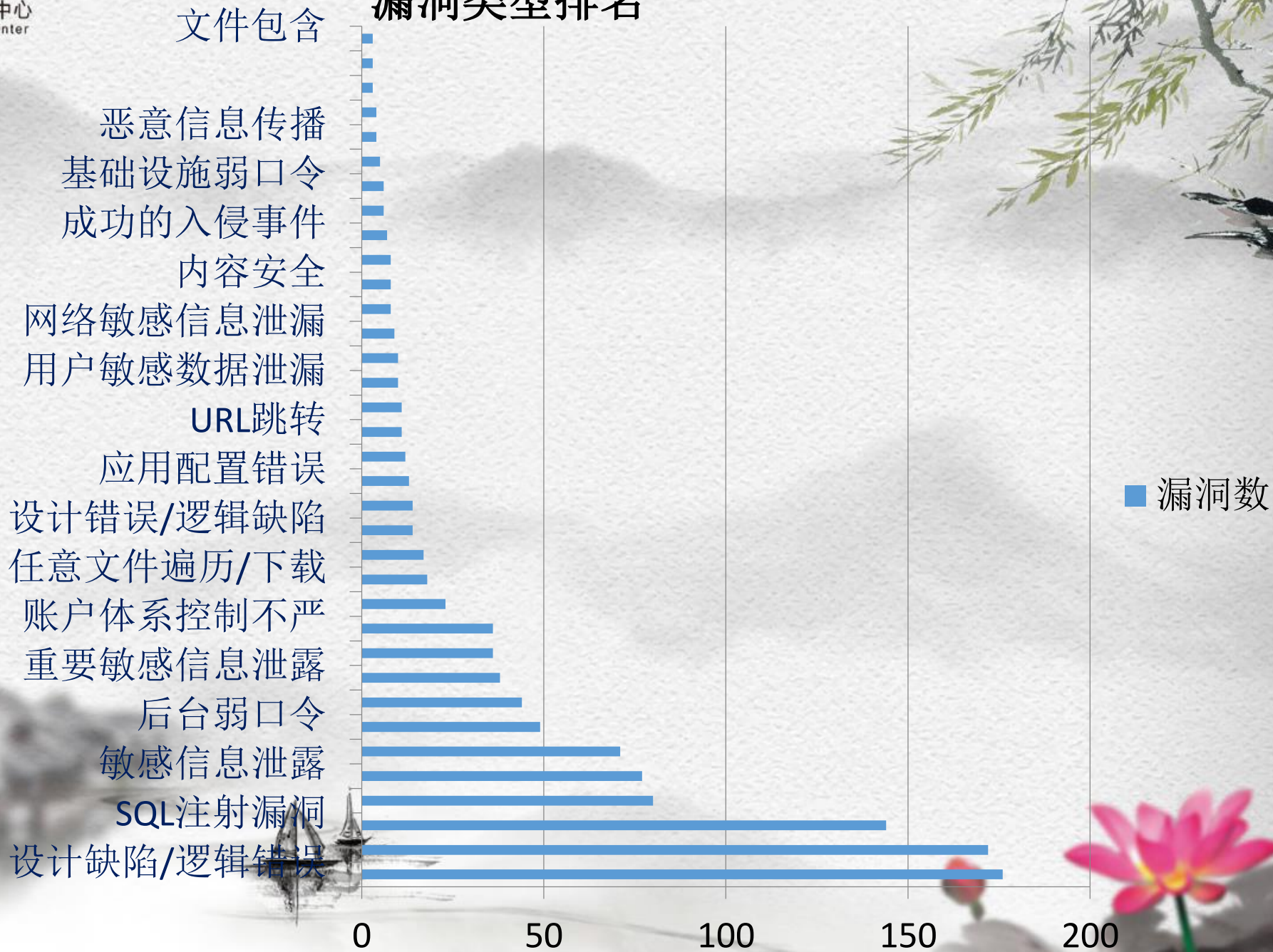


关注点

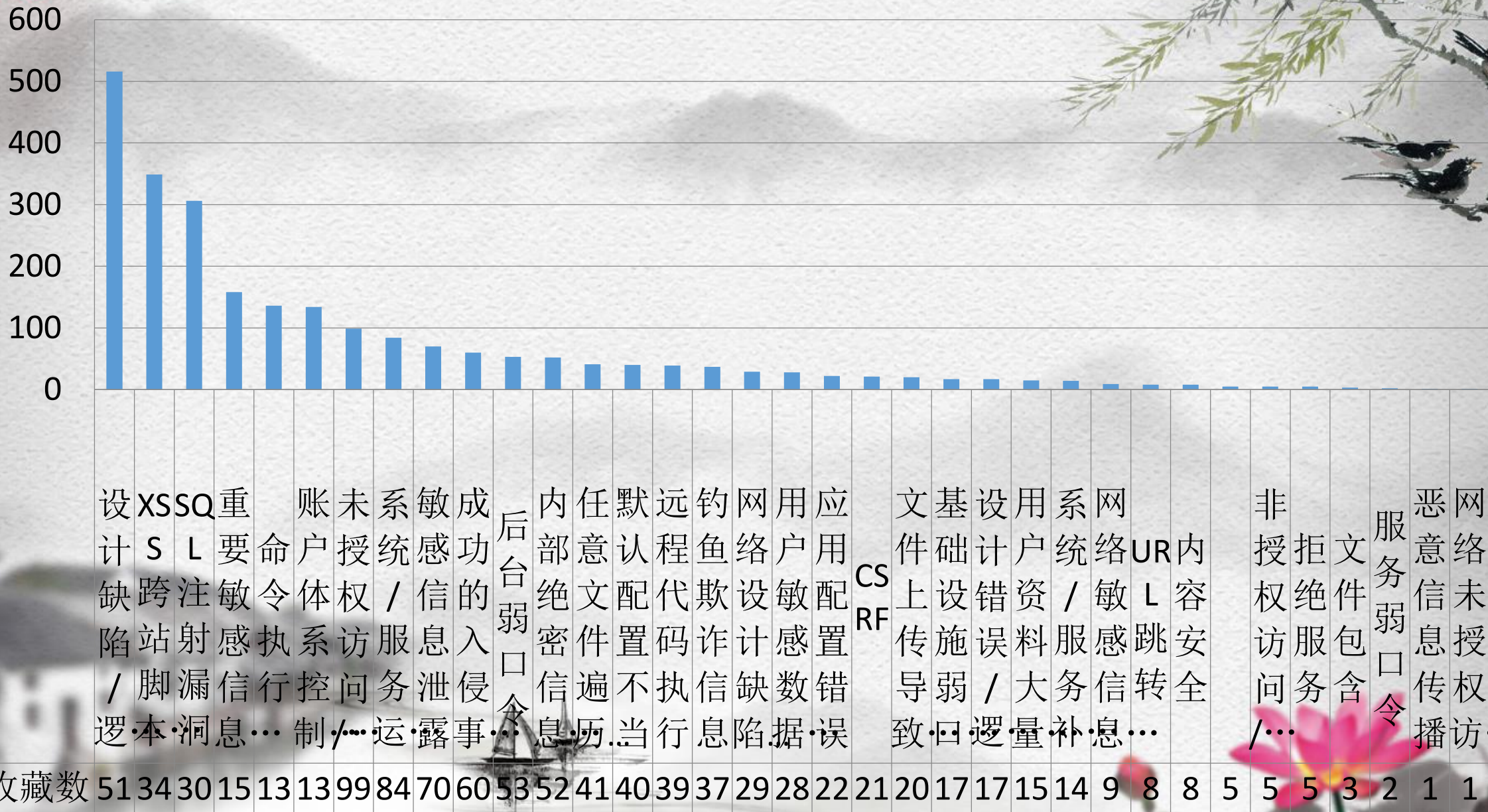


漏洞类型	关注数
	27
CSRF	101
SQL 注射漏洞	2018
URL 跳转	65
XSS 跨站脚本攻击	2037
成功的入侵事件	222
钓鱼欺诈信息	406
恶意信息传播	59
非授权访问/认证绕过	24
服务弱口令	25
后台弱口令	410
基础设施弱口令	79
拒绝服务	35
敏感信息泄露	639
命令执行	1066
默认配置不当	149
内部绝密信息泄漏	381
内容安全	119
任意文件读写	

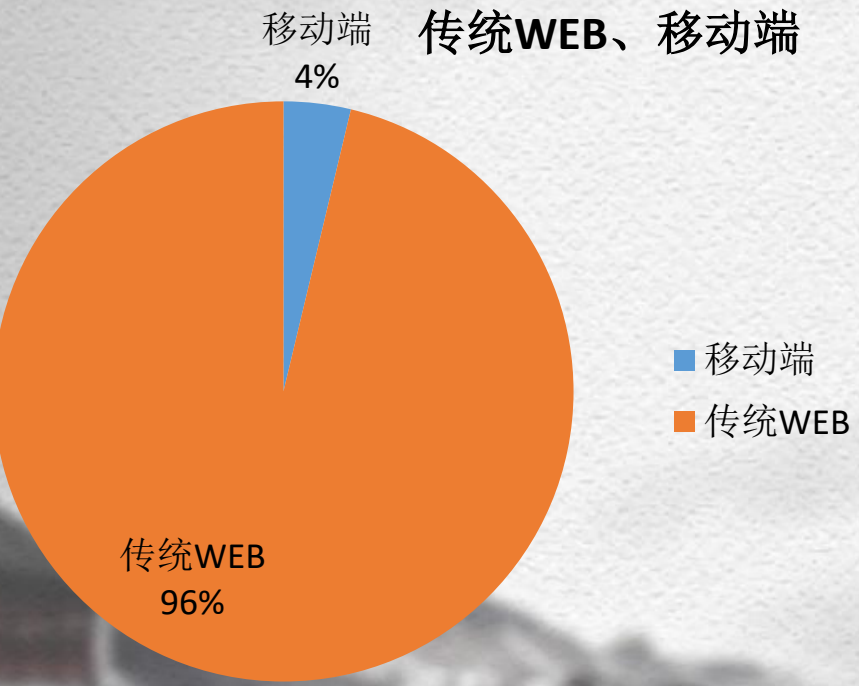
漏洞类型排名



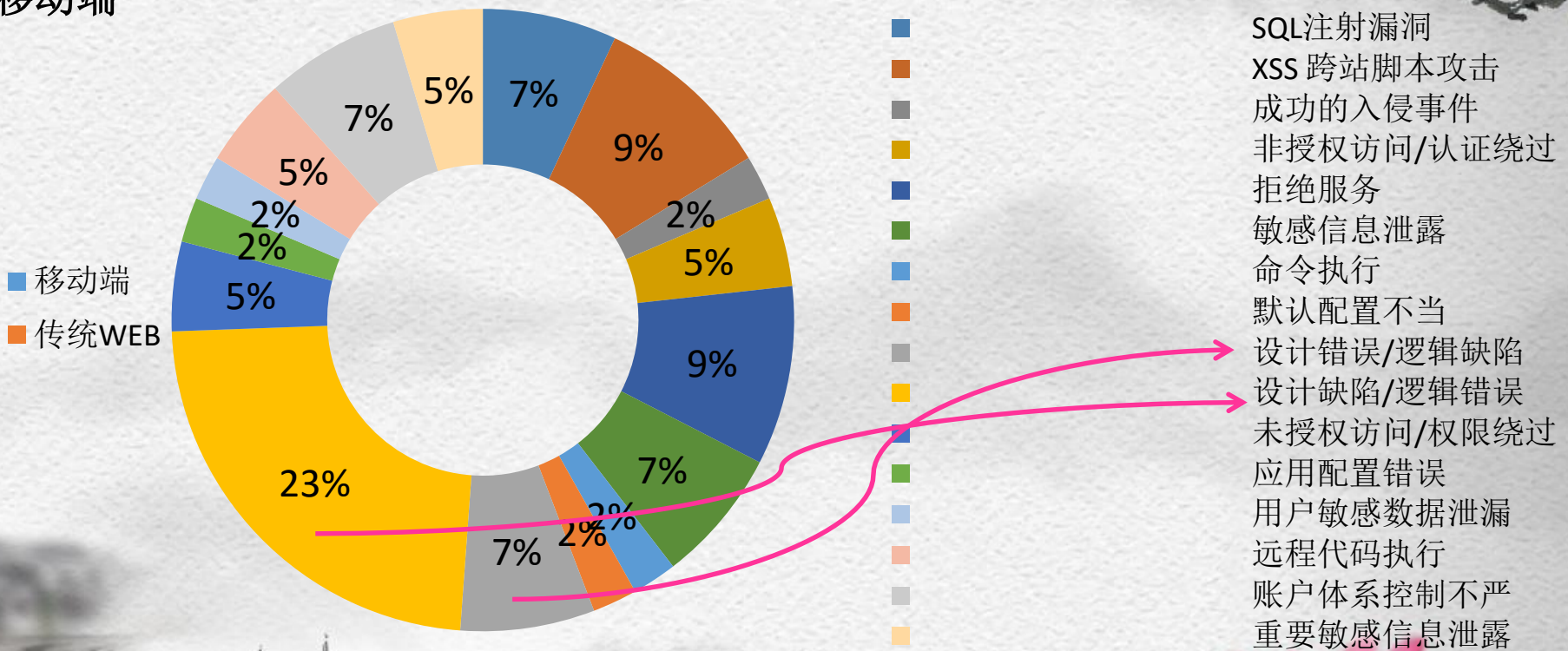
收藏数



传统WEB---移动端的兴起



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



电商系列安全漏洞挖掘

0X01安全认证

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:

The image shows a collage of security-related software interfaces. On the left, 'Intruder attack 15' displays a list of requests and payloads. In the center, a terminal window shows the usage and optional arguments for 'htpwdScan.py', an HTTP weak pass scanner. On the right, a '简单验证码识别工具' (Simple Captcha Recognition Tool) interface is visible, featuring tabs for image processing, segmentation, training, and testing, along with various configuration options for URL, status, threads, and captcha handling.

usage: htpwdScan.py [options]

* An HTTP weak pass scanner. By

optional arguments:

-h, --help show th

Target:

-u REQUESTURL Explici

-u="htt -u="htt

-f REQUESTFILE Load HT

-https Explici

SSL ena

Force m

HTTP Ba

e.g. -b

Dictionary:

-d Param=DictFile [Param=Dict

简单验证码识别工具 by Naih

图像细节处理 图像分割 图像识别训练 图像识别测试

灰度化: 二值化: 去除干扰项:

红: 30 + - 自适应阈值: 去除背景色 自适应

黄: 59 + - 全局自适应: (Otsu) 降噪 中值滤波

简单验证码识别+登录暴力破解工具 --- by Naih

数据包 配置 结果

URL: Status 200 线程: 10 开始 Import Save

验证码地址 4

验证码接口

用户列表

密码列表

验证方式 一对一 一对多

验证码错误标识 失败后重新加入队列

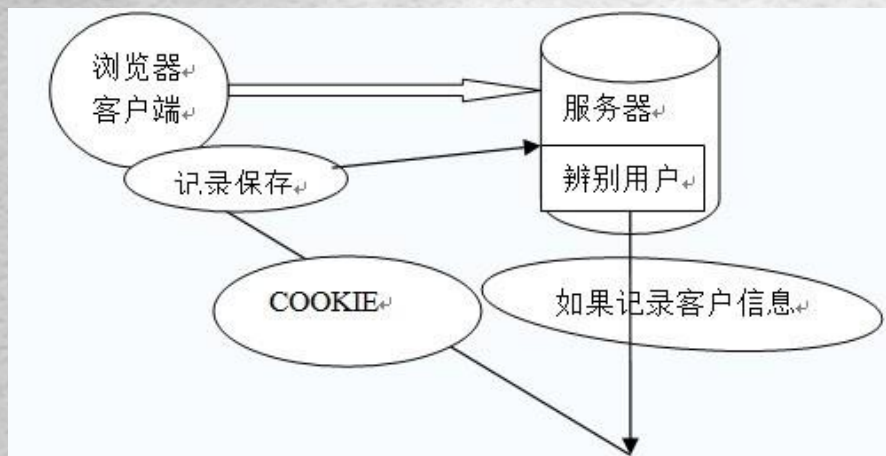
验证码成功标识 成功后进入下一个用户

爆破成功标示

关联参数

源	本包中的个数索引	目标	正则
---	----------	----	----

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。

0X02一致性校验

手机号篡改

订单号篡改

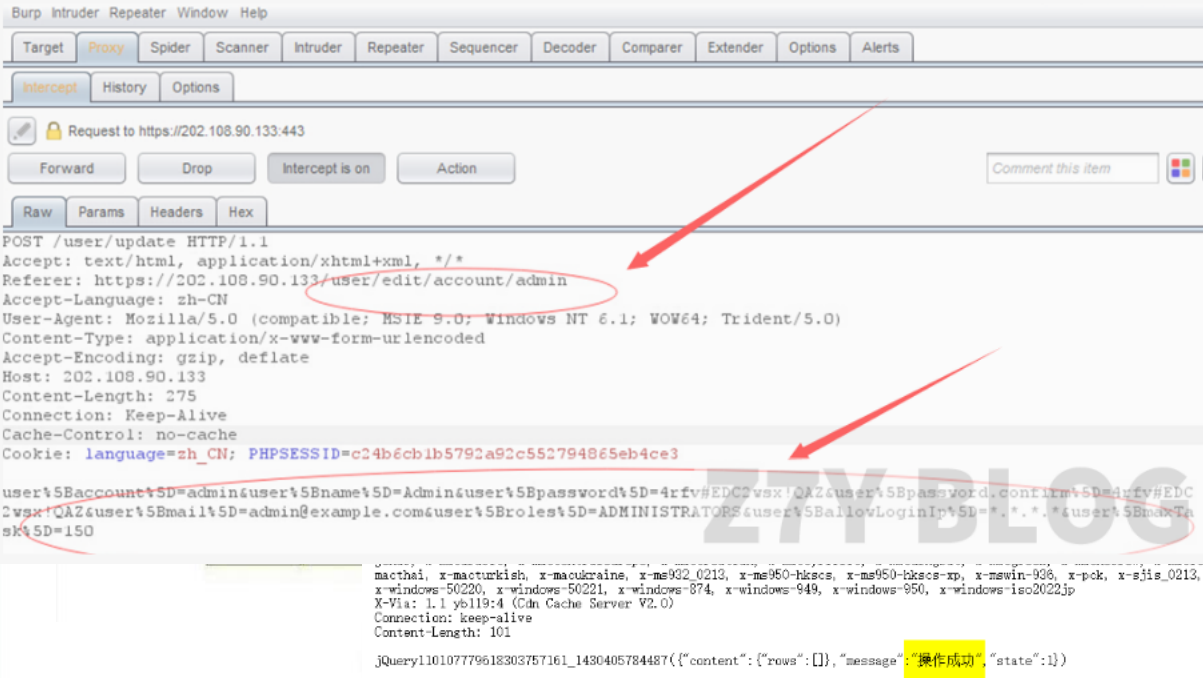
用户id篡改

商品编号篡改

其他业务篡改

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

然后修改审计员密码，抓包，将referer处的auditor和post的数据里面的auditor一律修改为admin，也就是管理员号，2处修改完后的数据包如下图：



> 我的帐户 > 登录管理

登录管理

验证手机号码和邮箱作为登录帐户

手机号码	13888888888
电子邮箱	

温馨提示：业务办理过程中

0X03敏感数据篡改

金额篡改

数量篡改

突破限制

漏洞概

缺陷编

漏洞标

相关厂

漏洞作

提交时


POST b

参数

参数

baidujs

源代码

商品信息：	商品	商品编号	单价	数量	总价
	16款哈弗H9背负式尊贵型_极地白外观_灰黑内饰内饰	103257	¥ 5800.00	1	¥ 5800.00

支付方式：

☒ 线上支付

结算信息：

共 1 件商品 商品金额： ¥ 5800.00
运费/服务费： ¥ 0.00
应付金额： ¥ 5800.00

购车人信息：

购车人：

请填写真实姓名

*

该姓名需要与最终购车发票上一致

手机号：

请填写正确的手机号

*

用于销售商与您联系，请确保准确

本次应付（整车订金）： ¥ 5000.00
(线上支付)

余款总金额： ¥ 800.00
(线下支付)

☒ 我已阅读，并同意购车协议

返回购物车修改

提交订单

www.wooyun.org

```
notify12Fsync12F20
bankInput=1&interf
mac=1cd00bd332c0
```

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

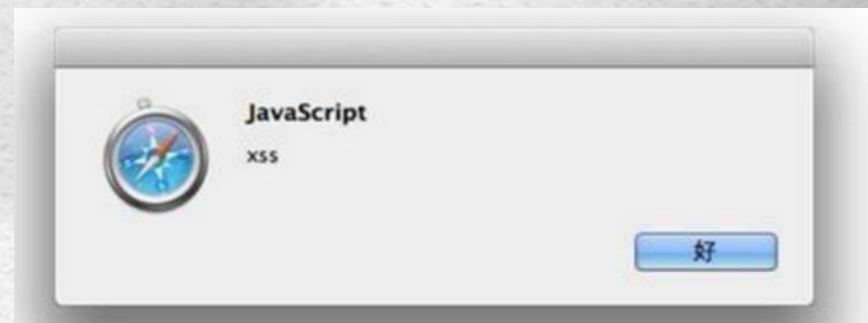
0X04交互输入



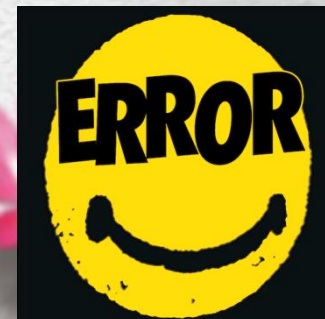
注入



跨站XSS



二次利用



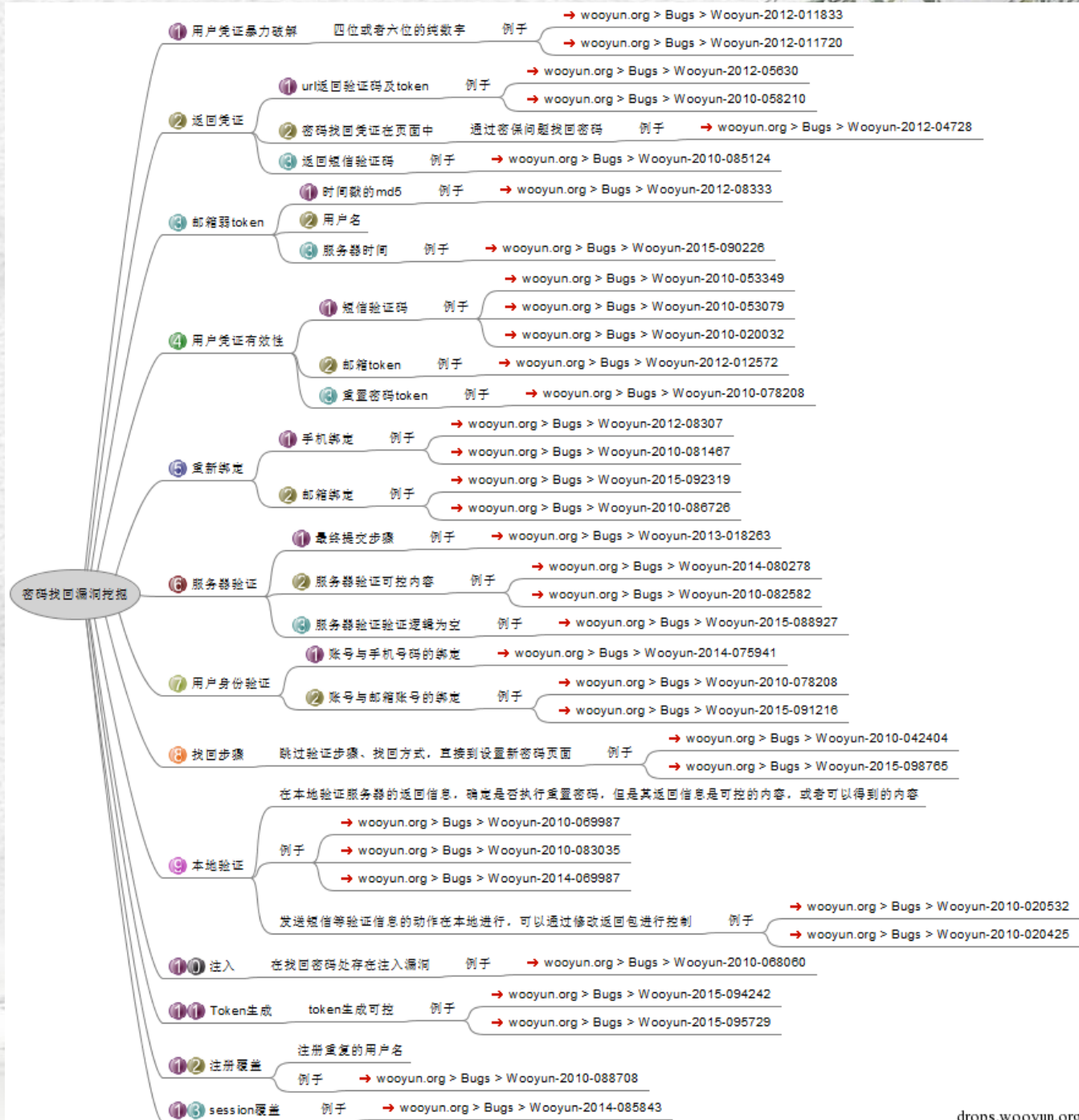
0X05认证找回

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越权测试

未授权访问



未授权勿入

No unauthorized access

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



开发人员在数据增、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

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



墨莼 V Q

昵称: 墨莼

编号: 12631

年龄: 24岁

地点:

查看资料 (每次花费0.1元)

给她送花 (每次花费0.1元)

给她写信 (每次花费0.1元)

查看联系方式 (每次花费1.0元)



念念, 年年 V Q

昵称: 念念, 年年

编号: 75

年龄: 25岁

地点: 湖北省

查看资料 (每次花费0.1元)

给她送花 (每次花费0.1元)

给她写信 (每次花费0.1元)

查看联系方式 (每次花费1.0元)

com 国家真实美女资料库

明星图片集锦 人体艺术欣赏 两性生活话题 淘美专题资讯

l9@hotmail.com

1.联系方式

电话: 1858006257

QQ: 7452462

邮箱: 7452462@qq.com

支付宝



网银支付:



云贝牙切 · 回致云贝

个性: 冒险/疯狂、浪漫/脱俗、目田、认真/负责、自然/本能



充值成功!

1秒钟后自动跳转至个人中心,
如果不跳转, 请点击个人中心

查看详情

马上定购

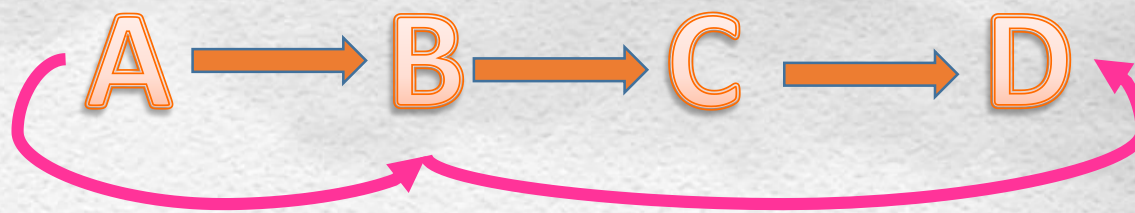


0x08条件竞争漏洞

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接口安全

重放攻击

内容编辑

API接口安全

0x10 敏感时效绕过

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](#)



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

身份认证安全

业务接口调用安全

时效绕过测试

业务一致性安全

密码找回漏洞

完整性

业务数据篡改

业务流程乱序

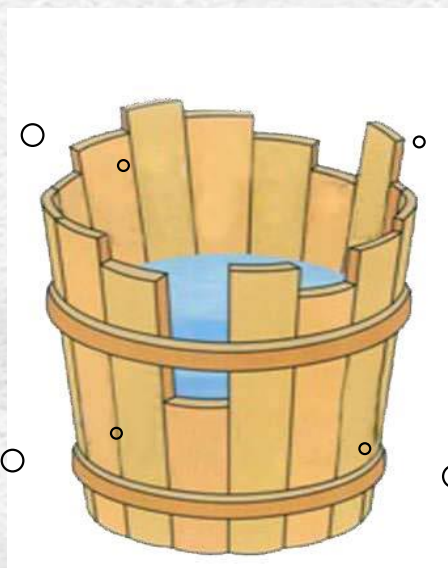
组织

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



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

感谢您的聆听!

