



JD 京东
COM

京东业务安全架构

多·快·好·省



朱磊

- 熟悉国际信息安全标准BS7799、ISO27001、SOX 404
- 熟悉国内的等级保护标准和安全评估的方法，具有实际经验
- 熟悉TCP/IP协议
- 对系统漏洞、入侵检测、病毒防护、防火墙有深入的理论和实践经验
- 在企业信息安全架构方面有多年的经验





2004 – 2007	天融信
2007 – 2012	完美世界
2012 – 至今	京东

ISO 27001 foundation

京东账户安全问题

2012年11月01日 07:17

来源：解放牛网

0人参与 0条评论 分享到：    更多

原标题：京东账户安全问题

京东账户安全问题不是第一次曝光，今年以来，就有几起用户账号被盗事件见诸报端。

2012年7月31日，杨女士在登录京东商城时发现，自己输入密码时一直被提醒“密码不正确”；警觉的杨女士迅速意识到自己的密码可能被盗，随后，杨女士使用京东的“找回密码”功能试图挽回损失，但在输入注册邮箱时，系统却提示“注册邮箱与账号不一致”。就在此前，也有网友的账户被盗，买走了一部手机。

京东积分兑换大漏洞或亏2亿元

www.yongyao.net

2012-11-1 10:37:13

来源:

责任编辑: cq高川

[艳照门图](#)

[女性安全周期表](#)

[京东的安全](#)

[京东的安全](#)

[积分兑换](#)

[安全事件](#)

分享到:                                         

京东商城再现客户账号被盗事件

2012-07-09 18:59 北京晨报 Oo小孩儿

A⁺ A⁻

关键字：等待收货 京东 商城 应用安全 账号被盗



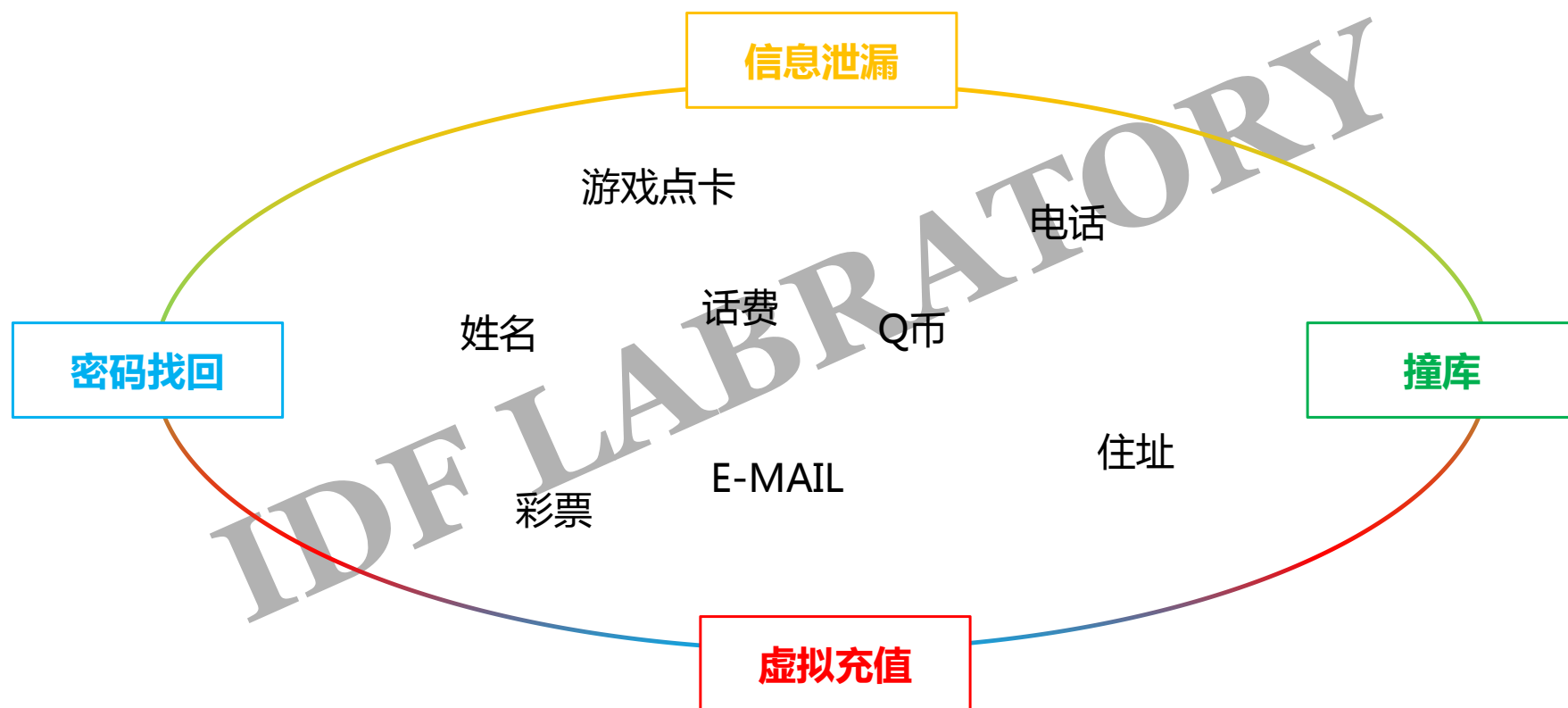
京东商城再现客户账号被盗事件。昨日，市民王先生反映，他在京东上的账户于7月6日被人盗用564元购买了一款手机。尽管客服表示会尽快拦截此快递，但截至昨日，王先生被盗账户上的订单仍显示为“等待收货”。

7月6日，王先生在外地出差时，手机上突然收到一条短信提示，告知京东账户余额发生了一笔564元的支付。“平时我的账户和爱人共用的，当时还以为是她买了东西”。王先生次日返京，无意间跟爱人聊起此事，却被告知没有用京东账户购物。王先生赶紧查看，不料在网站登录时竟连续显示输入密码错误。

漏洞列表:

提交日期	漏洞名称	状态	作者
2014-07-19	京东商城反射XSS#2	已忽略	kksky
2014-07-19	京东商城反射XSS#1	已忽略	kksky
2014-07-09	京东某站存在反射型XSS漏洞	已忽略	神经刀阿碍
2014-06-05	京东商城奇葩漏洞可随机进入他人账号(有操作权限、可泄露收货地址、手机号等)	已忽略	路人甲
2014-06-03	某第三方服务可能导致京东用户串号现象(随机登录陌生帐号)	已忽略	路人甲
2014-05-21	京东某开发人员意识不足泄露一些敏感信息(github)	已忽略	路人甲
2014-05-09	京东美胸大赛逻辑错误可刷票	已忽略	xiaoL
2014-04-25	京东某站点命令执行(发现已有大侠留下的shell了)	已忽略	PgHook
2014-04-14	京东云引擎逻辑设计不当可免费越权调用资源	已忽略	CplusHua
2014-04-08	京东某分站openssl漏洞导致敏感信息泄露及全站随机用户登录(证明可登录)	已公开	Knight
2014-04-07	京东商城某站命令执行(威胁内网)	已公开	if、so
2014-04-04	京东某后台弱口令(可进一步获得webshell但未证明)	已公开	猪猪侠
2014-04-04	京东商品任意额度享受免费送货	已公开	MBA
2014-04-03	一次成功的漫游京东内部网络的过程(由一个开发人员失误导致)	已公开	fate0
2014-03-31	京东商城商品抢购设计缺陷	已公开	H.Rui
2014-03-27	从细节问题看京东安全(设计缺陷可撞库)	已公开	bing
2014-03-17	京东晒单储存型XSS可以成功劫持他人账户	已忽略	px1624
2014-03-19	京东商城关注CSRF漏洞	已忽略	Levine
2014-03-02	京东订单拆分漏洞导致子订单任意减免	已忽略	医生
2014-02-27	京东JSRC各种漏洞泄露	已公开	bing

共 120 条记录, 6 页 [1](#) [2](#) [3](#) [4](#) [5](#)



舆论导向

黑色产业

京东安全应急响应中心
全新改版上线

全新界面、全新体验、更快的响应机制
还有幸运的礼品卡 满满全是惊喜

获奖记录
"bingsec"获得 iPhone5 16GB...

礼品兑换
"bingsec"兑换 iPhone5 16GB...

新消息
"Evi1m0#FF0000"提交新漏洞...

提交漏洞



奇点云安全

知道创宇

君立华域

邪红色

济南安云

网络尖刀

ESST

XFAN

90SEC

大连安全联盟

KSSG

Binvul

以上组织排名不分前后

Beta Member

JD.COM 京东

I'm Robort J



Beta Member

JD.COM 京东



消息通知

任务调度



账号暴力破解

恶意订单

欺诈订单

虚假账户



评论



注册



订单

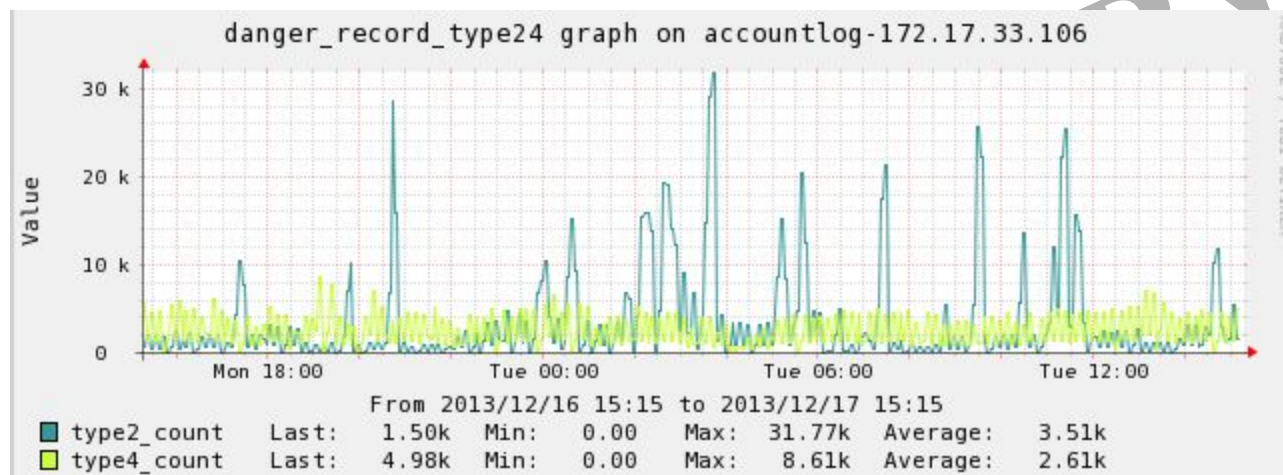


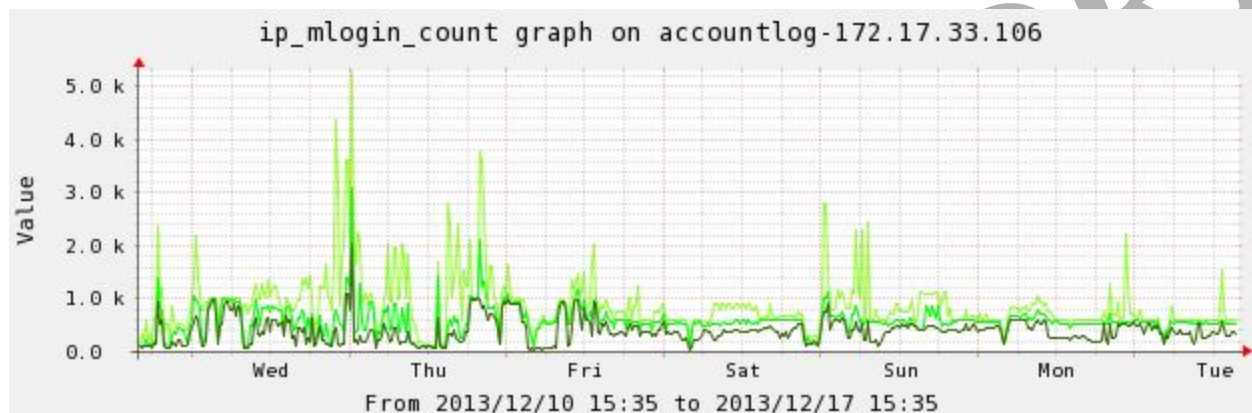
状态变更

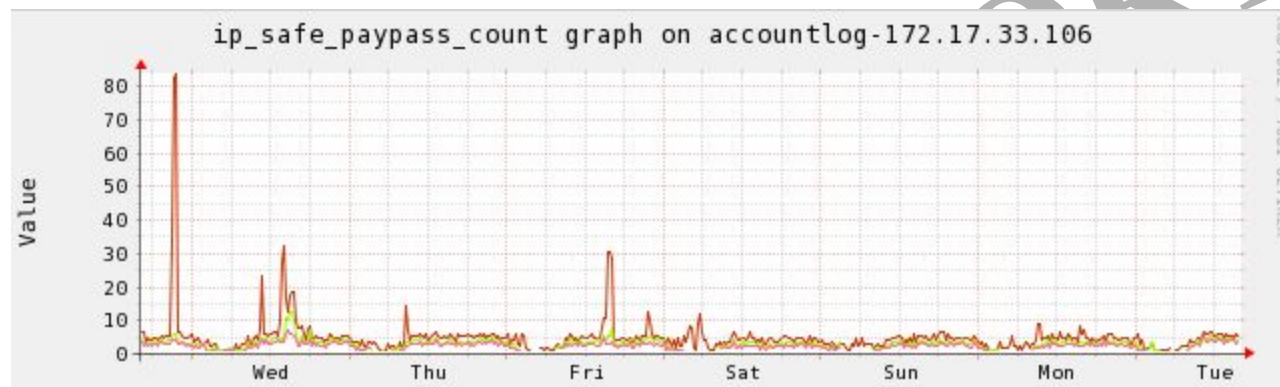


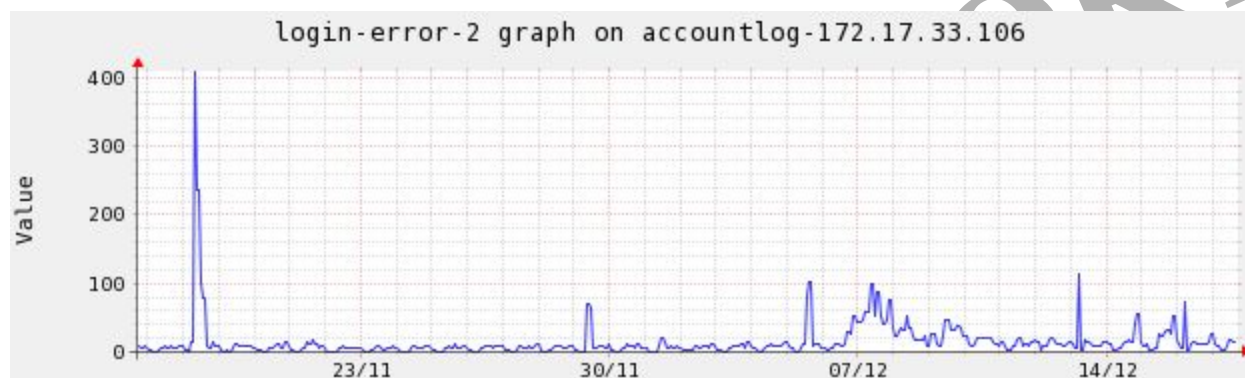
登录













上线项目测试

TFS

筛选

信息收集

扫描系统

报告

上线

验证

修复

验证



例行检查

DNS列表

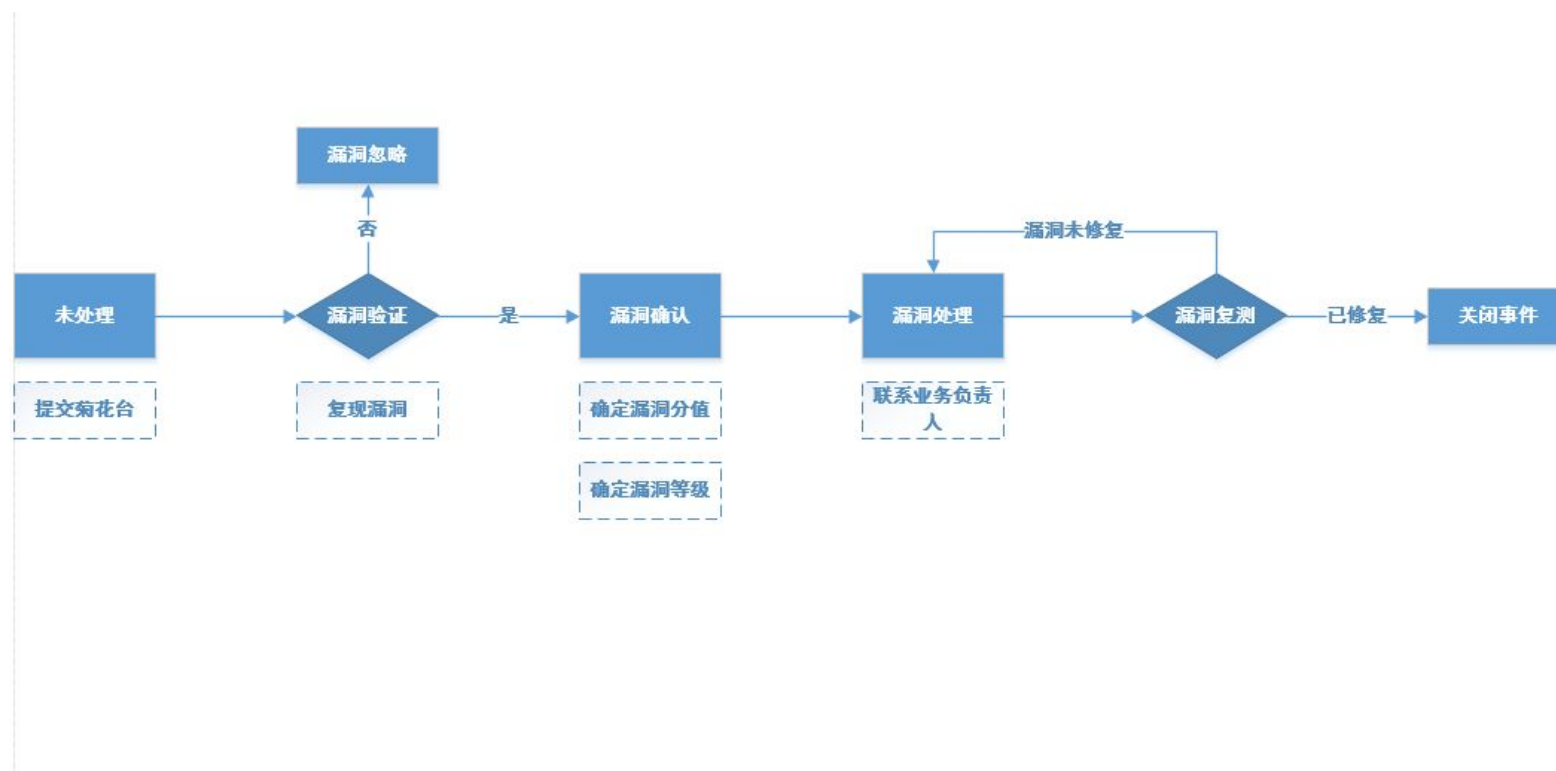
扫描系统

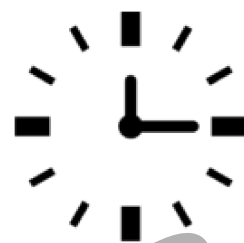
报告

验证

验证

修复





P1	1天
P2	3天
P3	7天
P4	14天

Frequently & Questions



Thanks — THE END