

# 一起走过的电商安全坑

【六年辛酸泪】



ID : Himan

京东商城-信息安全部

京东安全第一人

安全攻防 威胁情报 移动安全 安全合规 反欺诈

# 李学庆

让购物变得简单、快乐！

# 电商的特质

落地

数据

电伤

泄漏

速效  
救心  
丸

诈骗

大促阅兵

帐号

2017

2016

2015

2014

2012

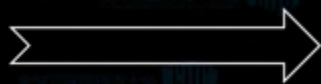
2013

2011



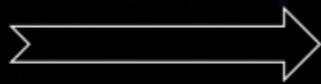
# 2011 年

✓ 订单泄漏问题



别人怎么可以查我的信息？

✓ 人员安全意识

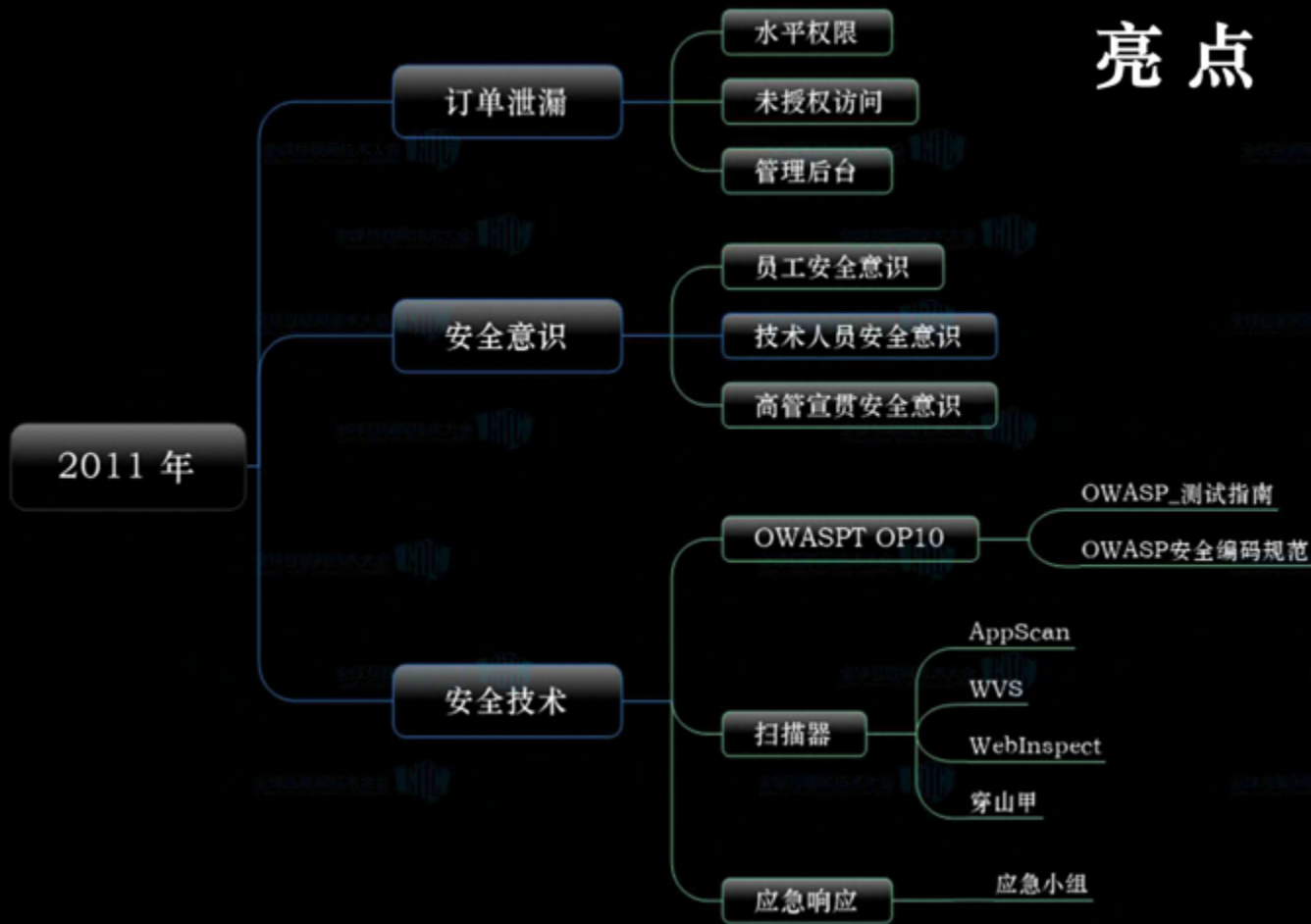


不知不觉敏感资料丢失！

✓ 安全技术萌芽



又是SQL注入…



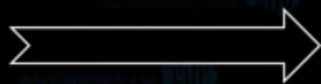
# 亮点

① 扫描器

② 全员培训

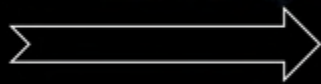
# 2012 年

✓ 数据泄漏问题



昨天XX被拖了，后天XX被拖了

✓ 框架漏洞



我的服务器被上传木马啦！

✓ 边界安全



在复杂的密码也怕万能钥匙！

# 亮点

2012 年

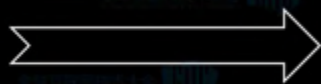


- ① 数据加盐
- ② WAF 拦截



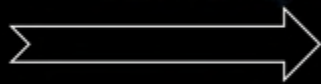
# 2013 年

✓ 帐号安全



我可以直接登陆数千账户！

✓ 漏洞回收



XX网站漏洞又被恶炒了一把！

✓ 调度系统



漏洞没有很好的渠道！

# 亮点

① JSRC平台

② 调度平台

2013 年

帐号安全

防撞裤

防黄牛

帐号体系加固

漏洞回收

JSRC发布

第三方安全平台

自主发现

调度平台

上线系统

重大漏洞排查

安全评估机制

扫描系统

黑盒扫描

后台、端口、管理页面

集群接入上线

工单系统

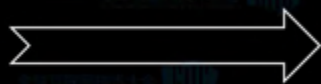
记录漏洞级别

推动漏洞SLA时间

分析安全报告

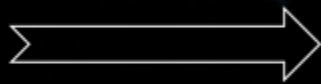
# 2014 年

✓ 业务安全



摇一摇无限刷积分！

✓ 合规安全



相关部门的合规检查！

✓ 数据安全



数据还是要给其他部门…

2014 年



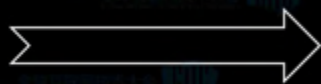
# 亮点

① 安全官

② 数据加密平台

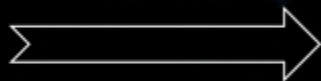
# 2015 年

✓ 反诈骗



我去，不小心被骗3个亿！

✓ DDOS



服务器又被D了…

✓ HTTPS



主站又被劫持了…

2015 年

反诈骗

数据脱密

上下游封堵泄漏

联合打击诈骗

虚拟号

DDOS

DDOS防御方案

DDOS测试平台

DDOS常态化

HTTPS

全站HTTPS

HTTPS降级方案

# 亮点

① 虚拟号

② DDOS常态化

③ HTTPS降级方案

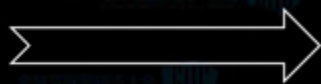
网络层、应用层

IDC流量控制

第三方

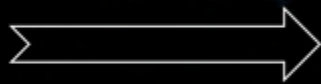
# 2016 年

✓ 安全资产



这个漏洞影响范围？

✓ 安全感知



漏洞来了吗，到哪啦？

✓ 数据泄密



哪个环节出问题了？

# 亮点

2016 年

安全资产

IP、域名

框架、组建

拓扑结构

网络设备规则

安全感知

网络日志

DNS日志

应用日志

办公网日志

数据泄密

数据链路画像

数据资产负责人

数据基线联动

① 资产关联

② 数据止损

③ 行为拦截



脉象平台

安全小  
课堂

SELIC

亮点

安全公益

IoT

安全法

安全委员  
会

威胁感  
知

安全月

APP



寻找

下一个

安全

亮

点

