

# 京东双十一大促背后的安全保障

Qing

# 关于我



ID : Himan

京东商城-信息安全部

京东安全方向第一人

# 李学庆

大促保障 | 安全攻防 | 威胁情报 | 安全人才 | 安全合规

## 让购物变得简单、快乐！

电商狂欢节

少约泡少搞基精力全放双十一

秒杀

1元购

同是低价 买一真的

\$\$

京东 11·11

真·正·低

11·1-12

200-100

1折

# 电商狂欢节安全隐患

漏洞

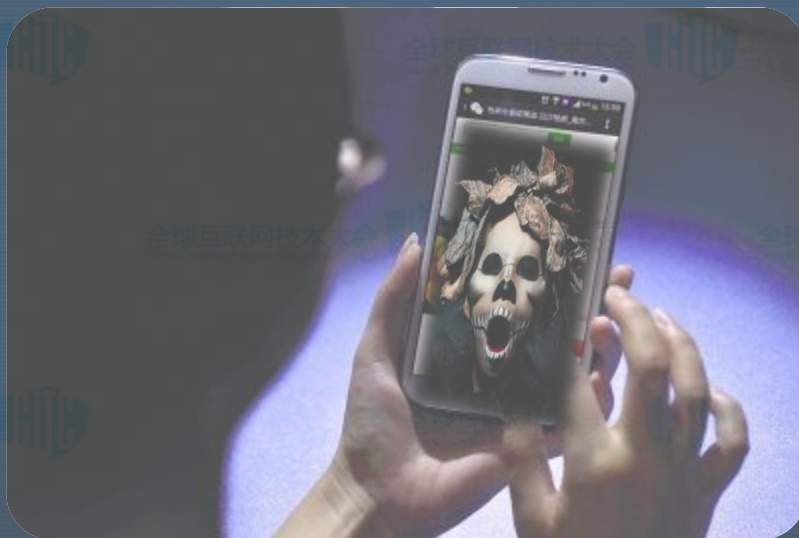
钓鱼

劫持

欺诈

攻击

公关







# 思考

风险→差距→解决

# 双十一 备战

## 备战

```
graph TD; A((备战)) --- B((引导发布)); A --- C((资产分析)); A --- D((隐患自查)); A --- E((响应演练)); A --- F((监控感知));
```

引导发布

资产分析

隐患自查

响应演练

监控感知

# 双十一 备战

## 引导发布

```
graph TD; A[引导发布] --- B[安全开发SDL]; A --- C[劫持处理流程]; A --- D[安全指引];
```

安全开发SDL

劫持处理流程

安全指引

# 双十一 备战

## 资产分析

统计域名

统计应用

统计类型



# 双十一 备战

隐患自查

自查漏洞

外部补充

JSRC

# 双十一 备战

## 响应演练

```
graph TD; A[响应演练] --- B[重大漏洞]; A --- C[信息泄露]; A --- D[DDOS]
```

重大漏洞

信息泄露

DDOS

# 双十一 备战

监控感知

哮天犬系统

威胁感知

外围风险

# 双十一 备战

## 备战

引导发布

安全开发SDL  
劫持处理流程  
APP应用生命周期管理

资产分析

统计域名  
统计应用  
统计类型

隐患自查

自查漏洞  
外部补充  
JSRC

响应演练

重大漏洞  
信息泄露  
DDOS

监控感知

哮天犬系统  
威胁感知



# 双 十 一 保障

保障

钓鱼网站

漏洞

反欺诈

劫持

DB审计

信息泄露

# 双 十 一 保障

## 保障

钓鱼网站

发现和关停XX个

漏洞

处置：XX个  
沟通：XX人

反欺诈

处置：X 起

劫持

处置：DNS劫持XX次  
链路劫持XX次

数据库审计

审计数据：XX 条

信息泄露

撞库：XX次（峰值）  
锁定IP：XX个

# 内外资源联动

## 京东安全

### 内部

法务部

公关部

云平台

客服中心

危机中心

金东金融

### 外部

# 双十一保障 5 原则





# 哮天犬监控系统



# 双十一保障团队



End | Q&A环节

