关于用户数据库泄露的情况报告和反思

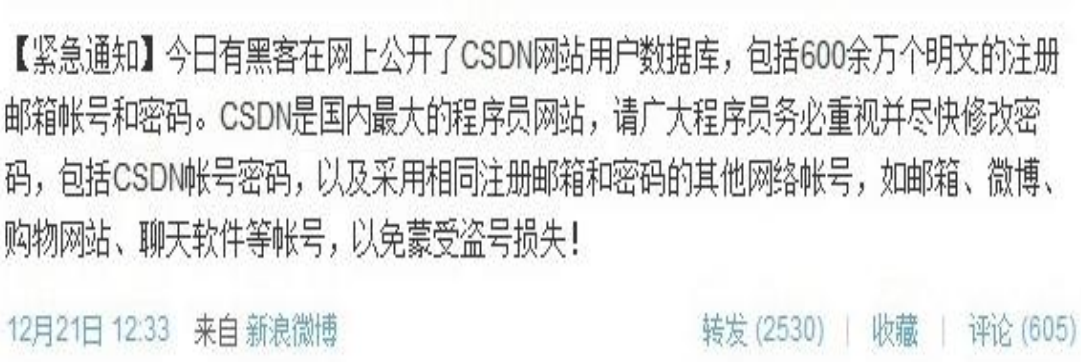
CSDN创始人 蒋涛
@蒋涛CSDN

主要内容

- 简介
- 分析
- 反思

事件简介

- 21号360微博



- 迅雷疯狂传播

当天应对措施

- 联系360微博 下载资料库比对
- 首页公告
- 重置相关用户密码 发送邮件通知
- 联系下载源（迅雷和QQ）
- 联系主要邮件服务商（网易和QQ）
- 报警

后续处理

- 22号邀请安全公司漏洞扫描和渗透测试
- 22-25号排查系统
- 24号下午遭受DDos攻击

数据分析

- 总会员库2010万 泄露库643万
- 625万数据用户id符合 18万不符
- 2010年9月后1.9万数据 92%邮件地址不符

安全审计（杭州安恒）

- 第三方系统漏洞
  开源CMS
- 应用程序漏洞
  存在跨站脚本漏洞
- 大量系统后台认证漏洞
  弱口令/暴露后台
- 已停用的老系统

反思

- 对安全系统的忽视
- 对网站运维的忽视

措施

- 信息系统等级保护
- 核心服务强化安全，非核心隔离
- 降低对黑客的价值
- 引入安全审核机制

建议

- 建立共享安全技术联盟
- 共享安全公共知识库
- 提升开发人员的安全技术技能