从BSRC看互联网企业安全漏洞及威胁趋势

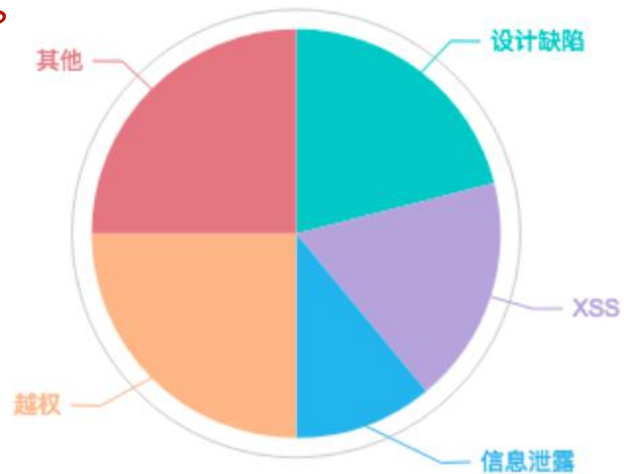
百度安全应急响应中心

Baidu Security Response Center

目录

互联网企业漏洞分布

- 安全设计缺陷（逻辑漏洞）20%
- XSS 18%
- 信息泄露 12%
- 越权 25%
- 其他 25%



逻辑漏洞（业务强相关性漏洞）

- 通常是对业务的威胁，而非对资产的威胁
- 产品在设计、实现阶段没有考虑到的问题
- 比如：帐号操作、支付逻辑

越权（未授权访问）

- 水平、垂直权限跨越
- 接口、页面的未授权访问
- 信息泄露

信息泄露

- 云存储：AWS S3
- 代码托管：github
- 文档：博客

漏洞趋势

- 传统高危漏洞占比小，但仍然存在
- 难以自动化发现的问题威胁凸显

技术因素

- 传统漏洞自动化检测方案成熟
- 开源、商业、自研产品成本低
- 现代web开发框架安全性提升
- 开发者安全意识提升

黑产

- 薅羊毛：关注各类营销活动
- 虚假刷量刷单：作弊欺骗平台获取收益
- 窃取用户隐私：用于诈骗
- 流量劫持：运营商劫持投放广告、捆绑恶意软件
- 诈骗：骗取用户钱财、各类帐号信息

挖漏洞的方式

权衡时间与收益

- 自动化：更深的路径、更广的范围
- 深入业务：边缘业务、深挖业务逻辑
- 新思路：奇技淫巧

坚持一定的时间投入

（互联网）企业关注什么

- 资产
- 法规
- 数据（隐私）「一个SQL注入多少分？」
- 声誉

未来的关注点

- API
- 业务逻辑漏洞
- 黑产情报
- 新基础环境（容器化、云化）

- 泄露用户隐私、执行敏感操作
- 被上下游系统滥用
- 无人维护

业务逻辑漏洞

- 结合相关业务特征
- 内容建模识别

黑产情报

- 能获取到的往往只是用户反馈的现象（线索）
- 难收到确切可靠的高价值情报

容器化：docker、kubernates、自研COS

- 漏洞定位
- 安全隔离
- 安全能力滞后

云化

- 没有自有IDC
- 依赖外部安全产品
- 原有安全基础设施需迁移、适配
- 系统边界模糊

谢谢