漏洞治理角度下的SRC漏洞高效挖掘

杨俊才

无恒实验室安全工程师

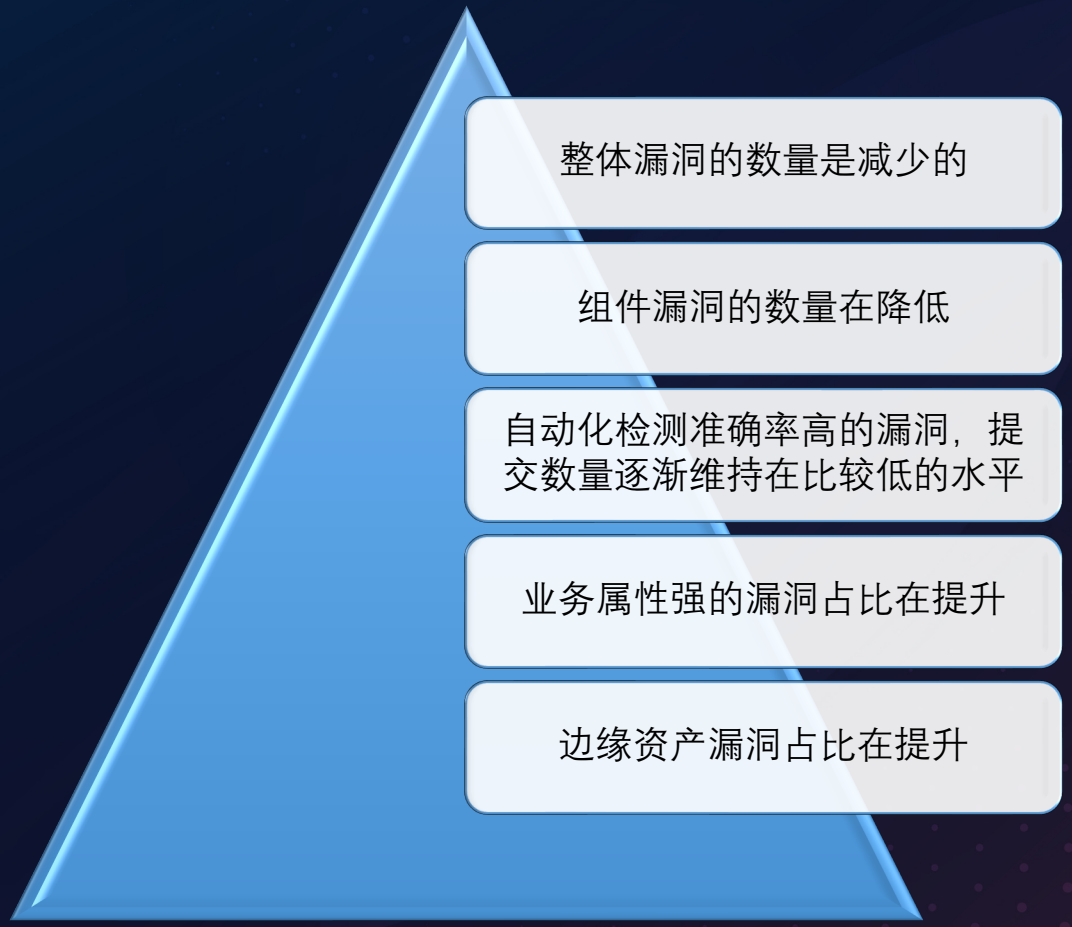
杨俊才

字节跳动 无恒实验室安全工程师

目录

近几年漏洞提交数据分析-SRC提交

近几年漏洞有哪些变化


整体漏洞的数量是减少的
组件漏洞的数量在降低
自动化检测准确率高的漏洞，提交数量逐渐维持在比较低的水平
业务属性强的漏洞占比在提升
边缘资产漏洞占比在提升

TOP3漏洞

- 逻辑漏洞
  - 跳过审核流程
  - 免费/低价使用资源/支付漏洞
  - …
- 权限绕过
  - 水平越权
  - 垂直越权
  - 隐私资源越权
  - …
- 潜在信息泄露
  - 前端脱敏
  - js文件泄漏
  - …

白帽子吐槽：现在洞越来越难挖了

漏洞挖掘治理

为什么会这样？

01

自动化工具检测越来越多样，越来越全面

- 黑盒、白盒、灰盒、流量…

02

企业在安全上投入的人力、精力越来越多

- sdl在企业的落地程度提高

03

业务关注度也越来越高

- 业务开始自发排查自己其他站点有无同样问题

为什么会这样?

以前的对手少:

- 上线前测试的安全人员

现在的对手多:

- 黑盒、灰盒、白盒、waf等防护工具、上线前测试的安全人员

如何才能更加有效的挖掘SRC呢

- 自动化工具弱点是什么
  - 在业务属性强的场景，规则很难完全覆盖
  - 准确率跟运营成本的平衡
  - 覆盖范围跟运营成本的平衡
  - 语义识别在自动化检测的落地有一定距离
  - …

如何才能更加有效的挖掘SRC呢

- 挖掘的侧重点是什么
  - 业务逻辑强的漏洞
    - 越权漏洞
    - 逻辑漏洞
  - 相对边缘的资产
  - 常见漏洞做到极致

越权漏洞的自动化检测与人工挖掘

越权漏洞的自动化检测

- 黑盒扫描
- 白盒检测
- 灰盒检测
- 流量探测
- 其他方式

黑盒/灰盒/流量检测流程


维持一个账号库并保持账号的登录状态
copy 流量
替换请求cookie
重放请求
对比response信息人工研判

黑盒/流量检测面临的挑战

脏数据	鉴权字段	公共接口/参数	账号的权限范围
• Post请求	• cookie • 网关	• 接口是公共接口 • 参数是公共参数	• 同组织 • 同权账号

白盒检测流程

研发梳理的鉴权函数

API函数名识别模块

- 统一网关API数据
- 子网关API数据
- 代码中API数据（定制化脚本提取）

白盒代码扫描

- API-鉴权函数关系表
- API-风险标签

告警识别引擎

告警

白盒越权检测面临的挑战

人工越权挖掘

- 确定场景/业务
  - 混合账号
    - 主、子账号场景
    - 组织/部门/公司/小组、子账号的场景
  - 跨产品资源访问的越权
  - …

SRC审核与白帽子协作

白帽子视角

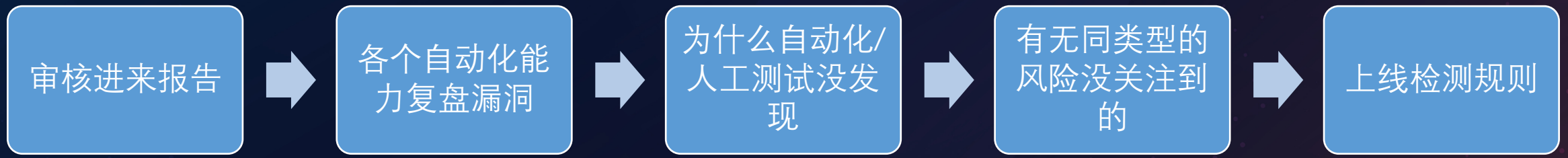
- 我提交了几个全被内部已知
- 边缘资产的收益不高
- 我x，我这个洞巨严重，你不得给我个特殊奖励？

审核视角

- 这种低级问题为什么没有发现
- 这个功能/站点都没几个用户，影响的确不大呀
- 业务都快要下线了你提个xss/csrf有啥用
- 大哥你这个报告写的我都看不懂

SRC审核与白帽子的协作

- 有效漏洞的复盘流程



希望看到的漏洞

- 重点功能测试（支付、点赞、评论、IM）、大批量敏感信息、突破网络权限
- 通用组件、配置的挖掘
- 安全策略的绕过、修复的绕过
- 已治理专项的遗漏
- 一份优秀的漏洞报告

发展趋势以及共同成长

THANK YOU FOR READING