ByteDance 字节跳动 | Security 安全与风控

基于流量分析的API安全实践

邵凯强

字节跳动-安全与风控

字节跳动安全工程师，硕士毕业于复旦大学，加入字节跳动后参与流量安全分析、API安全检测方向能力建设，持续参与字节跳动产品安全风险发现与治理工作。

目录

1.背景

为什么关注API安全

为什么关注API安全

API数量众多，风险面更大

01

根据Akamai的一项统计，API请求已占所有应用请求的**83%**，预计2024年API请求命中数将达到**42万亿**次

API安全问题已经成为最主要安全问题之一

02

据Gartner在《 2022 年应用安全技术成熟度曲线》中描述，API将成为攻击者**最主要的攻击目标**

API导致的风险危害直接

03

API与业务关联最为紧密，直接承载业务数据，被攻击后导致的问题**更严重**

基于流量分析建设API安全的思路

流量分析

流量清洗

- 噪音流量过滤
- 流量筛选去重
- URL归一化

安全分析

- 资产识别发现
- 风险场景识别
- API安全检测
- API威胁感知
- 数据防止泄露

风险治理

- 安全风险治理，提升安全防护水位

清洗去重

非真实有效接口的请求，会给后续分析带来噪音数据

噪音流量去除

流量筛选

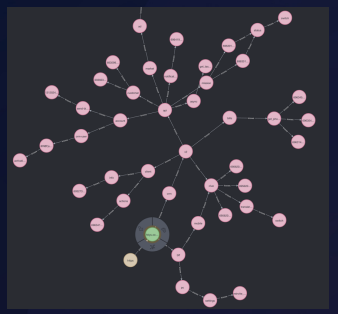
content-type: application/json, application/protobuf,…
content-type: text/html, application/javascript, …

流量去重

Redis 设置TTL

URL归一化

/project/tt42066/invoke/
/project/tt32c31/invoke/
……



- 层级深度
- 上层宽度
- 下层宽度
- ……
- 文本特征

url转树状结构

特征工程

机器学习 → /project/{param}/invoke/

Flink
Spark
大数据
分布式计算

流量分析能力

安全治理

利用API清单、风险场景类型标签，开展安全治理

资产自动化发现

自动化发现API接口、域名

识别管理后台、三方系统及组件

防止数据泄露

构建请求链路全景，关注不安全的数据传输

风险场景识别

识别常见业务风险场景

评估安全现状

API威胁感知

发现API防御保护缺失

API安全检测

检测潜在的API安全漏洞

以及OWASP API Security Top10风险

资产自动发现

自动化发现API接口、域名

识别管理后台、三方系统及组件

API安全-资产自动发现

新增接口监控

- 第一时间发现新增接口，并进行风险评估，减少风险暴露时间

新增接口

- 发现非预期的接口，减少暴露风险面

识别隐藏、已弃用的API，以及临时测试使用的API，降低非预期接口带来的风险

/service/data/search/test/
/api/v1/project/debug/*

安全分析

- 形成API接口清单，提供资产全景，消除评估盲点
  - 更高效、全面的开展安全评估、测试

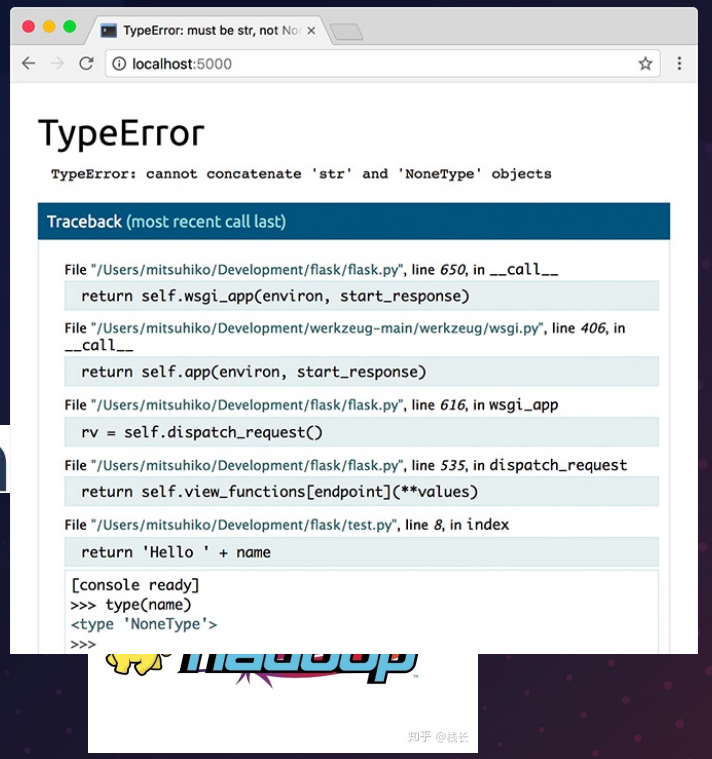
API接口清单

资产自动发现

管理后台发现

管理后台可能存在登录爆破、弱口令等安全风险

常用研发组件应用



部分组件可能存在未授权、调试模式暴露、N day攻击等安全风险

风险场景识别

识别常见业务风险场景，评估安全现状

API安全-风险场景识别

接口资产 → 功能场景分析

通用风险场景

- 文件上传场景
- 服务端发起URL请求场景
- SQL语句执行场景
- 后台登录
- ……

针对常见的伴随安全风险功能场景进行检测

业务风险场景

- 订单查询
- 短信发送
- OCR识别图片
- ……

针对30+种业务高风险功能场景进行识别，保持重点关注

API安全-风险场景识别

短信发送接口

/common/api/message/send/?

⚠

- 短信发送场景，
  - 需要关注是否接入频控 -> 黑产短信轰炸
  - 是否存在内容可控 -> 钓鱼诈骗

查询订单物流

/shop/backend/order_manager/order_get/?orderId=

⚠

- 查询订单信息场景
  - 关注权限校验是否完善 -> 越权风险

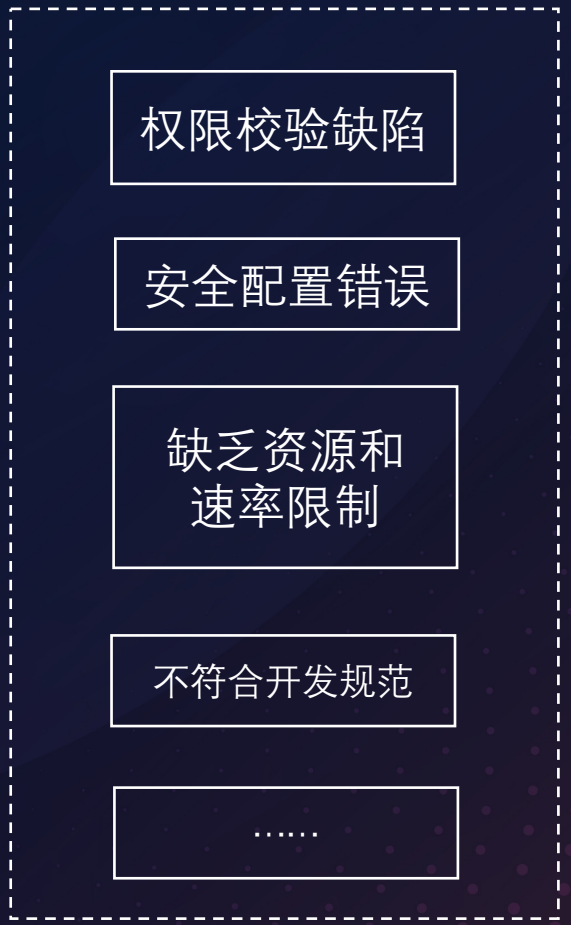
API安全检测

检测潜在的API安全漏洞

及OWASP API Security Top10风险

API安全检测

- 针对典型API安全问题进行检测，覆盖OWASP API Security Top 10 安全风险
- 拓宽关注视角，发现潜在缺陷风险



- 未授权访问风险
- 越权风险

- 返回详细报错信息

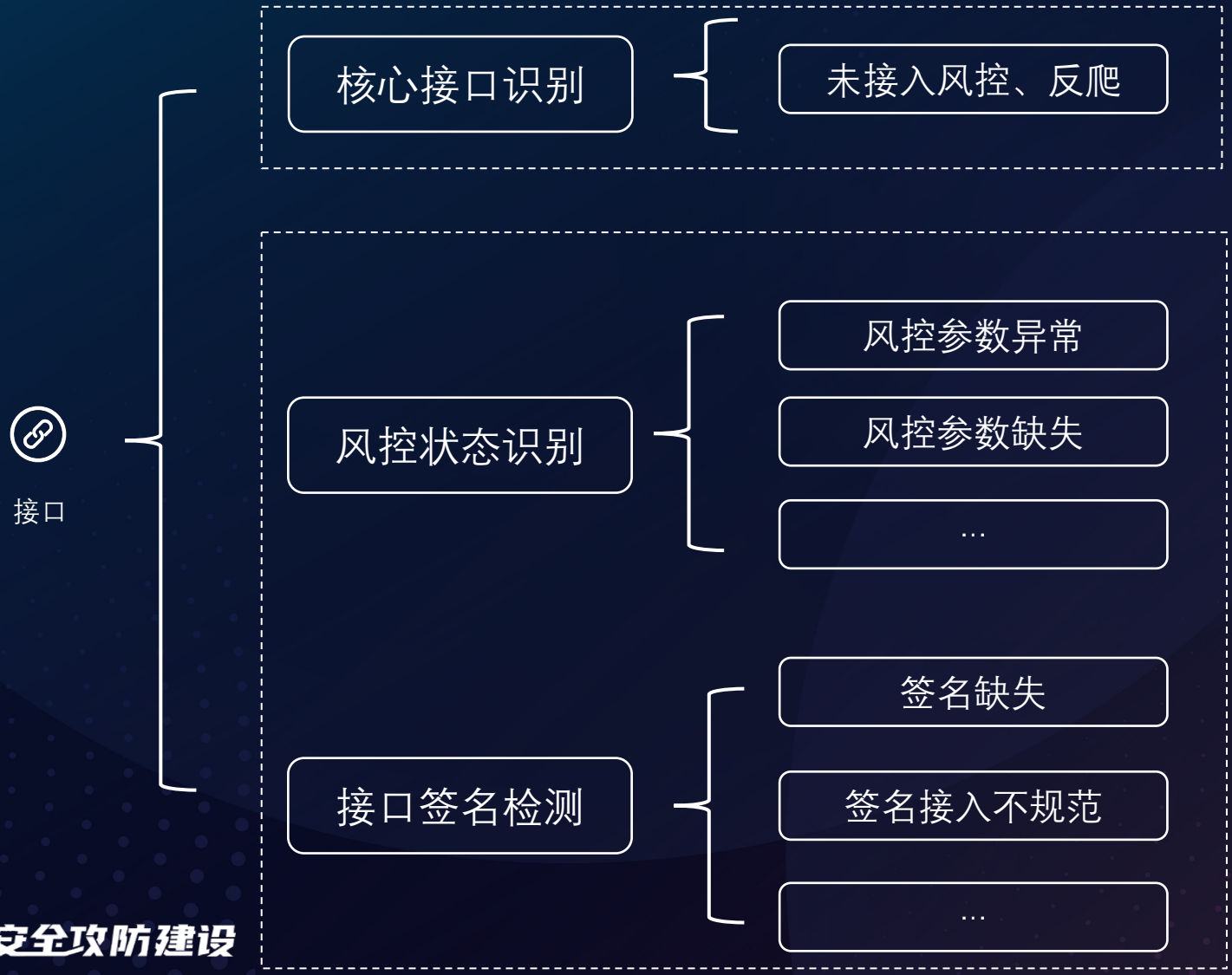
- 拒绝服务攻击
- 黑灰产消耗资源

- 使用GET方法进行增删改
- 日志输出不合理等

API威胁感知

发现API防御保护缺失

API安全-威胁感知



推动重点接口提升安全防御能力

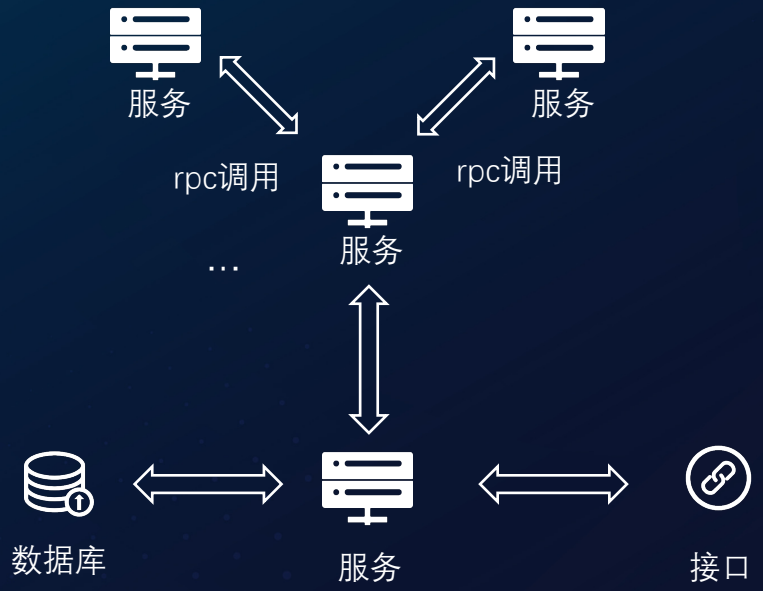
感知风控参数异常的情况，发现签名无效、不规范的情况，确认接口配置是否合理

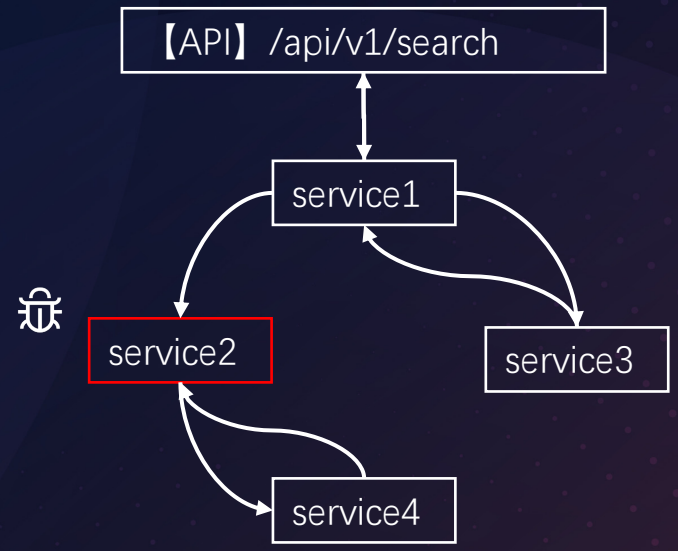
防止数据泄露

构建请求链路全景

关注不安全的数据传输

API安全-防止数据泄露





构建请求链路，了解数据流转情况

http://xxx.bytedance.com/api/v1/search?page=100&page_size=99999

⚠ 未开启https加密
存在泄露风险

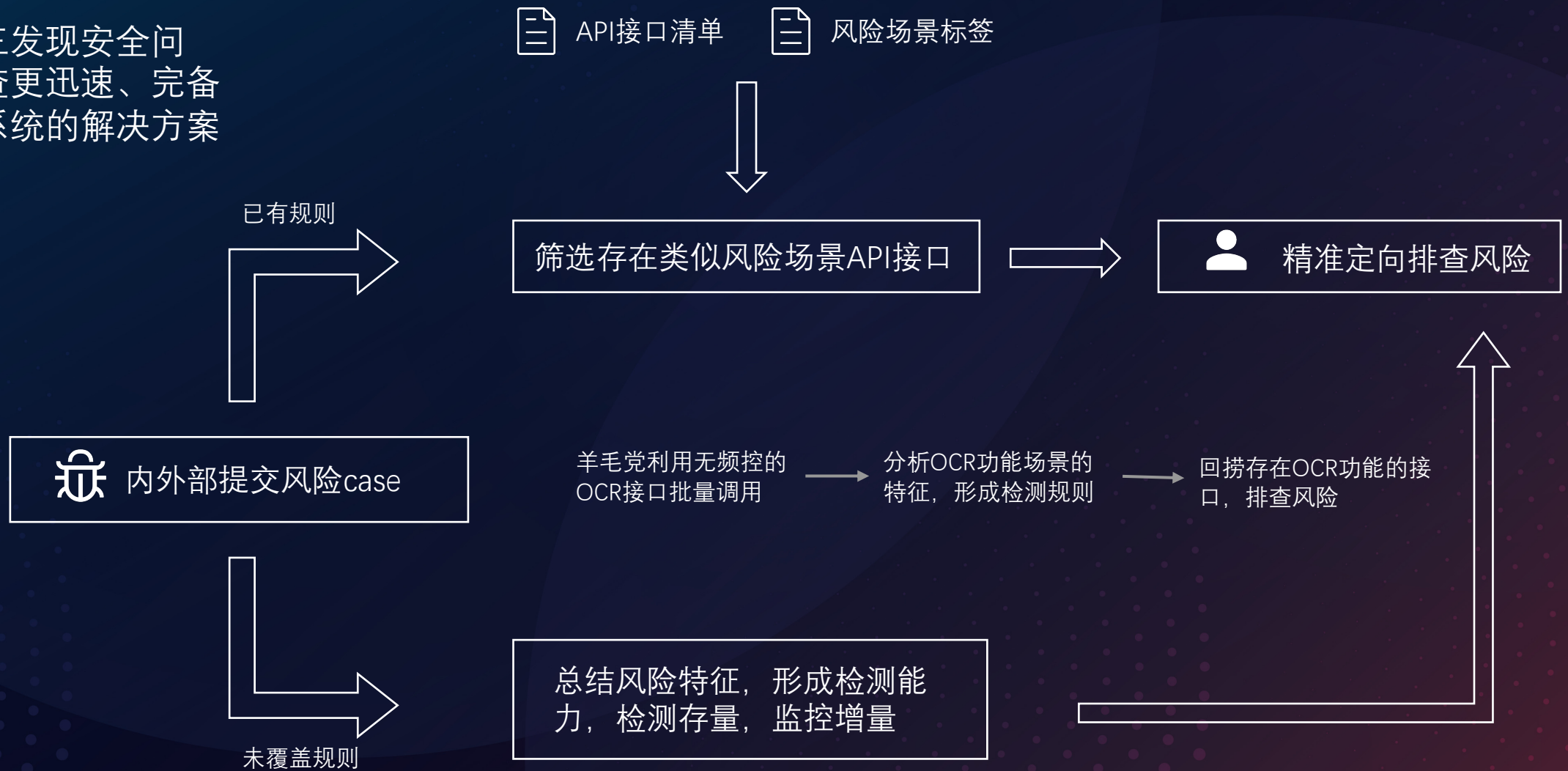
⚠ 数量未限制，
可能导致批量泄露

流量分析应用于风险治理

利用API清单、风险场景类型标签，开展安全治理

快速横向排查风险

- 举一反三发现安全问题，排查更迅速、完备
- 促成更系统的解决方案



系统平台安全治理

当前问题

- 应用众多，资产收录不完整
- 废弃系统未下线，增加了风险面
- 应用安全能力缺失，防御水位较低

遗漏系统补录 → 减少资产盲点

废弃系统下线 → 减少不必要的风险面

推进接入防护能力
- 安全的登录形式
- 完备的鉴权组件
- 水印、日志等溯源能力

THANK YOU FOR READING

字节跳动 安全中心 × 安全范儿 BYTEDANCE SECURITY

甲方安全攻防建设

ByteDance 字节跳动 | Security 安全与风控