使用 WAF 实时流量分析解决定制化业务安全问题

长亭科技　　李昌志

2019

安全+

自我介绍——李昌志

安全研究

- 腾讯安全平台部
- 安全研究员

研发

- 长亭科技
- 雷池 WAF 核心研发
- 雷池 WAF 产品负责人

产品

- 长亭科技
- 产品部总监

安全策略

- 长亭科技
- 安全策略部总监

目录

CONTENTS

01 理解业务的产品才是好产品

02 分析流量是理解业务的基础

03 如何提供人性化的流量分析

PART

1

理解业务的产品才是好产品

许多安全产品标榜自己可以理解业务

业务欺诈

盗刷、套现、薅羊毛、黄牛抢购、刷单、
短信轰炸、违反业务逻辑操作

数据泄露

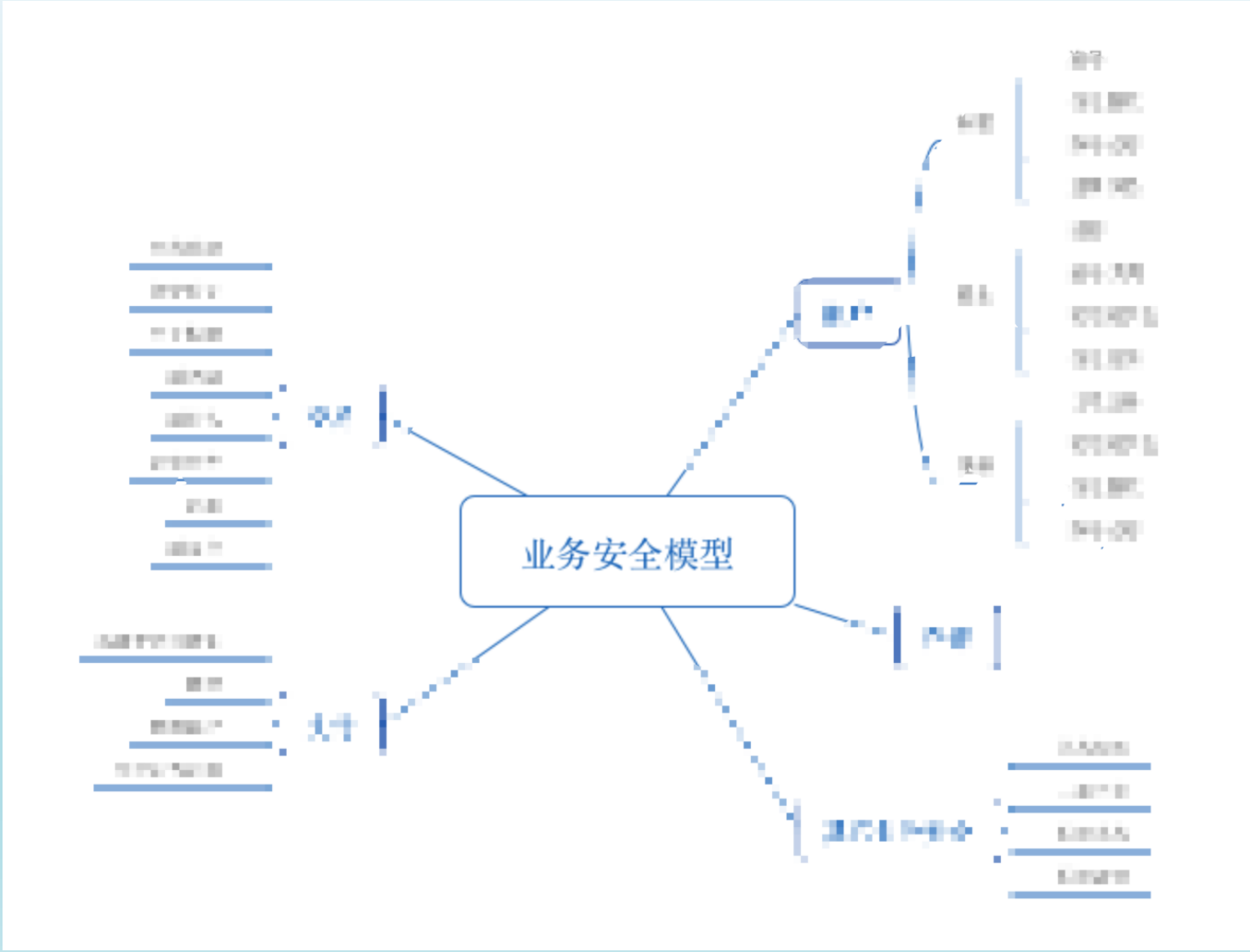
撞库、爬虫、敏感数据猜测、
内网窃密

许多安全产品标榜自己可以理解业务

1.1 产品介绍

业务安全风控是基于业务场景，[illegible]

许多安全产品标榜自己可以理解业务



业务安全问题有哪些

刷单刷水

刷排名

刷评论

刷转发

刷点赞

刷使用

刷抽奖

垃圾账号注册

暴力破解

脱裤

撞库

爬虫

盗号

账号恶意登录

黄牛党

羊毛党

反欺诈

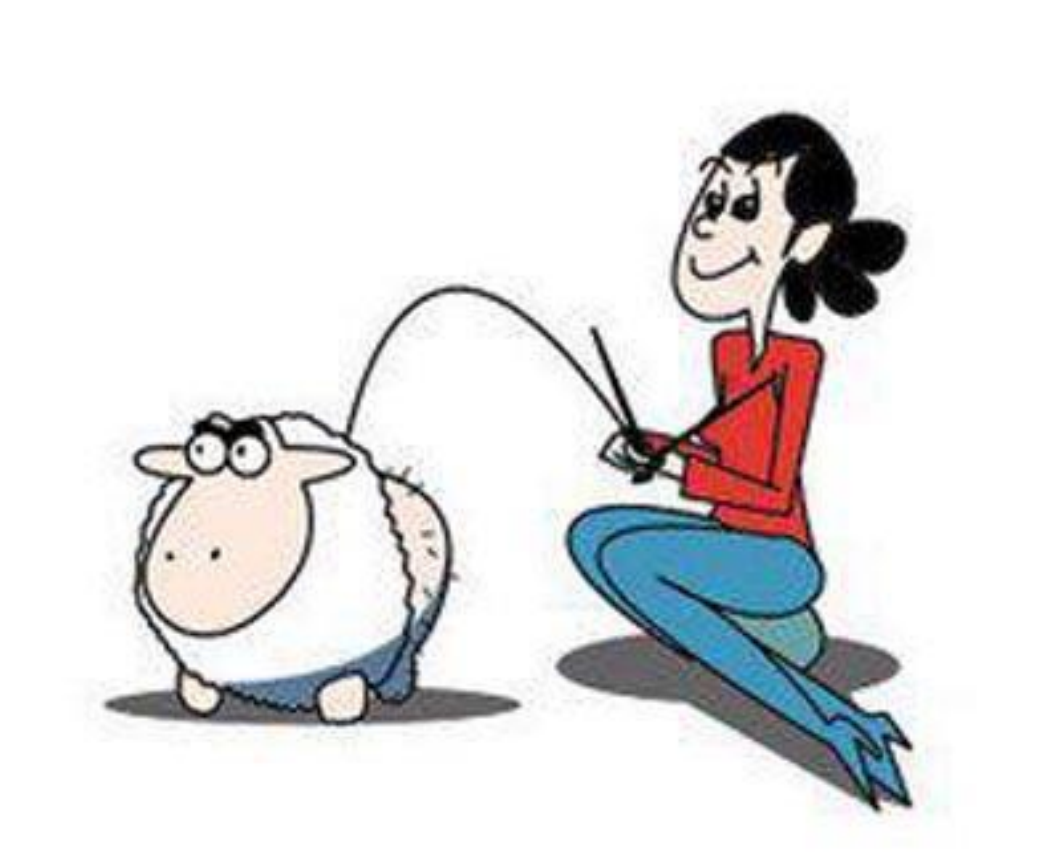
反作弊

恶意下单

短信轰炸

僵尸粉

不同的客户需求差别非常大



思考：

以“**薅羊毛**”为例

不同的业务遇到的薅羊毛问题是同一个问题么

不同的客户需求差别非常大

有哪些常见的“薅羊毛”问题

1. 利用不同的账号领取无门槛抵价券
2. 批量参与抽奖，提高中奖率
3. 虚假交易刷信用卡，使用积分换礼品
4. 。。。。。。

不同的客户需求差别非常大

对于此类“薅羊毛”问题，有通用解决方案么？

需要考虑几个问题：

1. 不同的业务账号体系一样么
2. 不同的业务领优惠券的流程一样么
3. 如何智能识别一个接口是否可以用来领优惠券
4. 。。。。。。

不同的客户需求差别非常大

土豪甲方选择用定制化的方式搞定需求

甲方：你们这个产品不好用啊，都没有 **XX** 功能

乙方：**XX** 功能和我们产品的定位不符，其实不一定能解决问题

甲方：这个项目有 **1000** 万预算

乙方：爸爸，我们做，来，谈谈需求

土豪甲方选择用定制化的方式搞定需求

普遍的定制化需求

定制化业务安全需求

薅羊毛、拖库、撞库、反欺诈、
防勒索、防病毒。。。

定制化安全监控需求

监控业务的运行状态
监控敏感接口的访问情况
监控敏感用户的使用状态。。。

定制化统计存储需求

安全势态可视化
业务峰值预判
业务使用率分析。。。

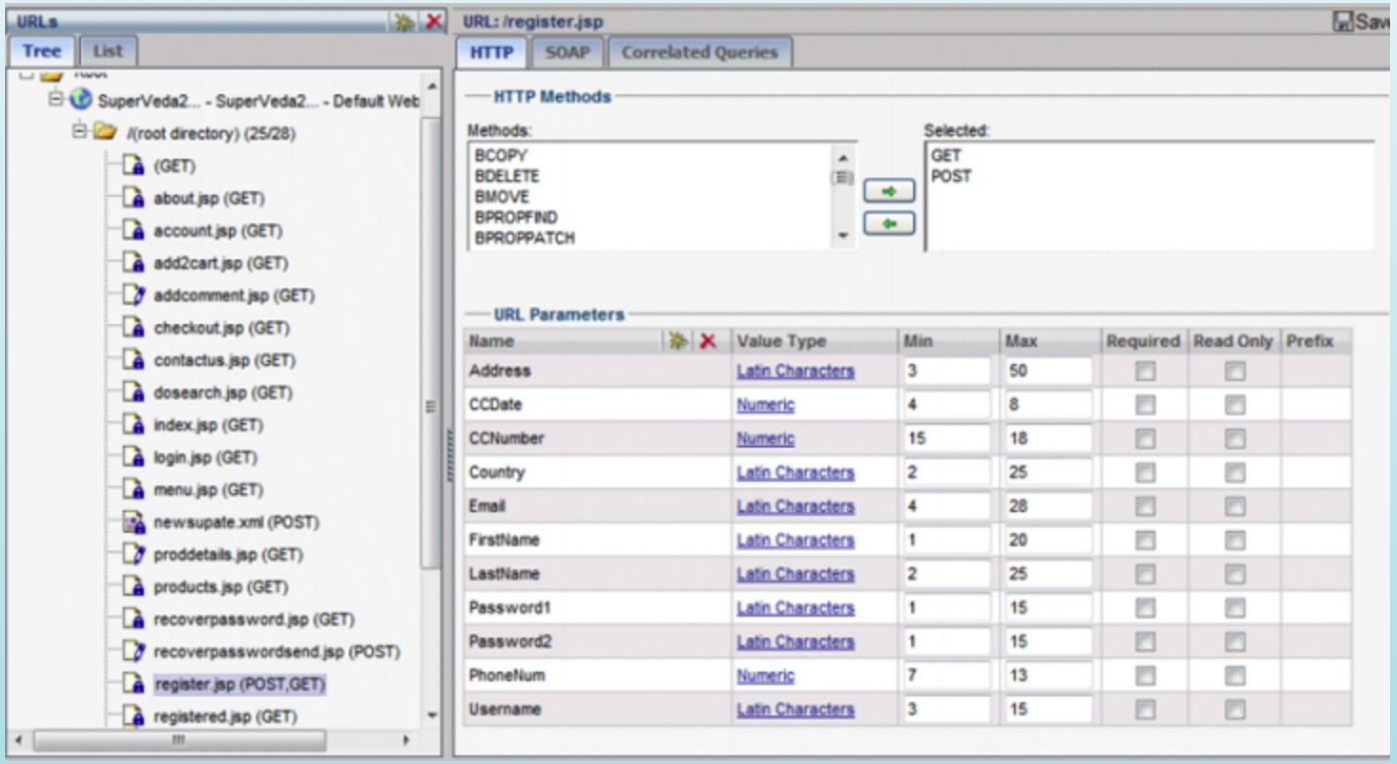
定制化对接需求

对接风控系统
对接威胁情报
对接 SOC
对接 SIEM。。。

PART 2

分析流量是理解业务的基础

现有安全产品是如何理解业务的



靠分析流量对网站建模

理解业务的内容包括：

- 业务有哪些页面
- 页面接受什么请求方式
- 页面有哪些参数
- 参数的类型是什么
- 参数的长度范围
- 。。。。。。

想解决实际问题需要进一步理解产品

需要实现真正对业务内容的理解

当前站点上有什么业务

业务的支付逻辑是什么样的

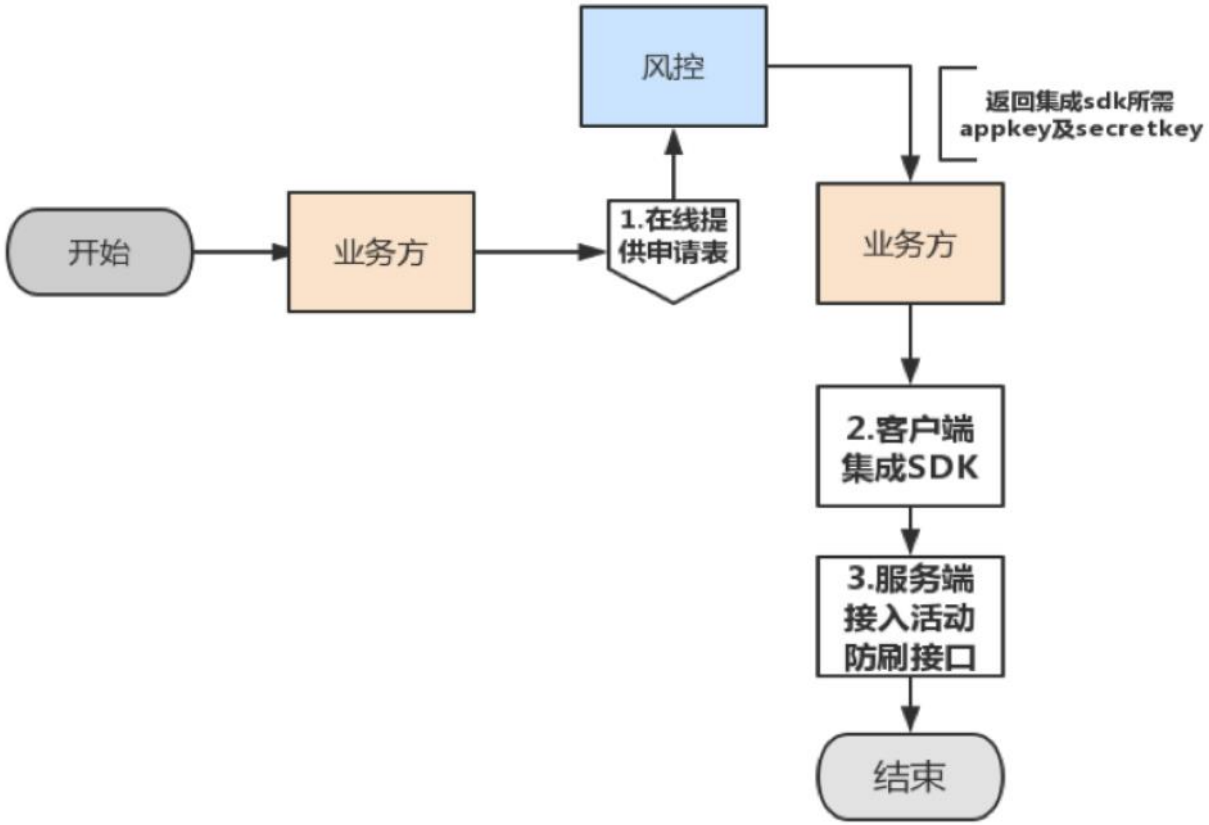
哪个页面有抽奖活动

哪个接口是登录接口

整个业务一共有多少个注册接口

。。。。。。

想解决实际问题需要进一步理解产品



业务风控 SDK

问题在于：

- 开发成本高
- 运维成本高
- 对业务变更的响应不及时
- 安全推动落地有难度
- 。。。。。。

安全产品理解业务的前提条件

- 需要从完整流量中分析
- 需要 **HTTP** 请求中分析
- 需要从请求日志中分析
- 需要手动配置 **API** 的类型
- 需要开发阶段介入

Web 网关——WAF

集群部署

超大规模集群

旁路镜像

透明串接

负载均衡

灵活代理

多种负载均衡算法

Web 攻击检测

传统 Web 攻击

爬虫、机器人风险

高可用

业务健康检查

主备方案

多活方案

访问控制

会话跟踪

黑白名单

限频、限速

智能可视化

流量监控大屏

安全监控大屏

PART 3

如何提供人性化的流量分析

toB 产品如何提供更贴近用户场景的流量分析功能

- 定制化
- 官方插件
- 灵活但复杂的配置文件
- 开源
- 开放 API
- 开放扩展 SDK

什么样形式语言更容易被接受

- ASM
- C
- C++
- Java
- JavaScript
- Python
- SQL

如何提供更加人性化的逻辑定义方式

SQL

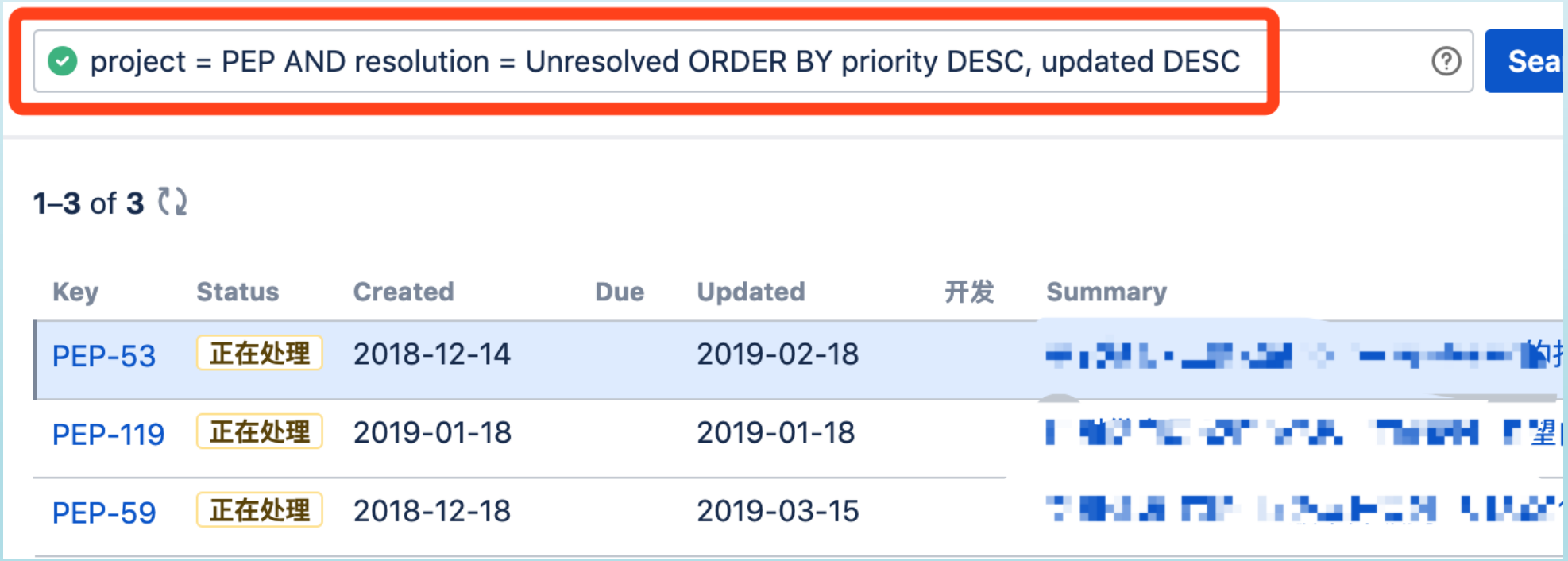
哪些场景下可以使用到 SQL

常见的关系型数据库

- MySQL
- MS SQL Server
- Oracle SQL
- PostgreSQL
- SQLite

哪些场景下可以使用到 SQL

用来筛选 JIRA ISSUE 的 JQL



哪些场景下可以使用到 SQL

用来操作 **WMI** 的 **WQL**

WQL (SQL for WMI)

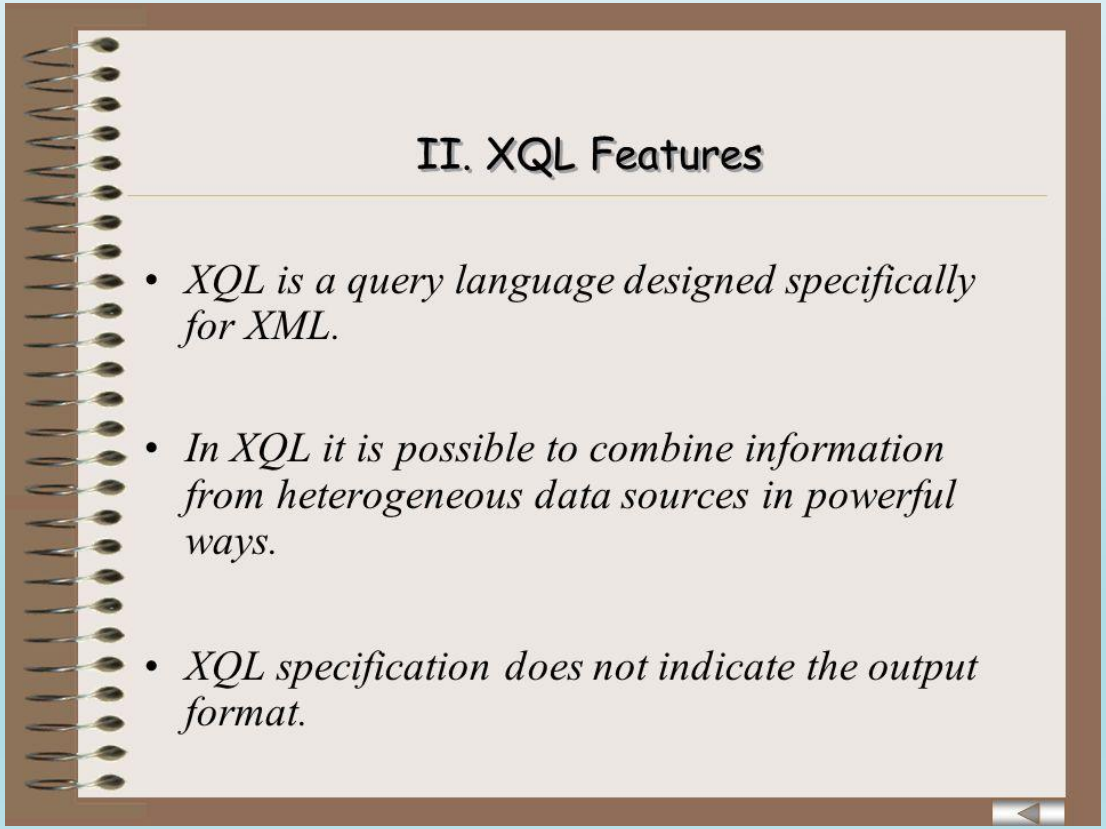
2018/05/31 • 2 分钟阅读时长 • 作者

The WMI Query Language (WQL) is a subset of the American National Standards Institute Structured Query Language (ANSI SQL) with minor semantic changes. The following table lists the WQL keywords.

WQL keyword	Meaning
AND	Combines two Boolean expressions, and returns **TRUE** when both expressions are **TRU**
ASSOCIATORS OF	Retrieves all instances that are associated with a source instance. Use this statement with schema queries and data queries.
__CLASS	References the class of the object in a query.
FROM	Specifies the class that contains the properties listed in a SELECT statement. Windows supports data queries from only one class at a time.
GROUP Clause	Causes WMI to generate one notification to represent a group of events. Use this clause with event queries.

哪些场景下可以使用到 SQL

用来处理 **XML** 的 **XQL**



哪些场景下可以使用到 SQL

用来执行实时流量分析统计的

SafeLine QL

Safeline QL 能干什么

看几个实际的问题

SafelineQL 能干什么

问题1：

某业务被 CC 攻击了，导致访问非常慢，甚至不可用

解决思路：

1. 攻击者的请求集中在运算量大的 API
2. 攻击者的请求频率较高

服务器响应时间超过 10s 的请求 IP 与 URL

```
SELECT ip, url_path
FROM access_log
WHERE TIME > 10
```

一分钟内访问次数最多的 10 个 IP

```
SELECT ip
FROM access_log
GROUP BY TUMBLE_WINDOW(TIMESTAMP, 60), ip
ORDER BY COUNT(ip) DESC
LIMIT 10
```

SafelineQL 能干什么

问题2：

某业务遭到了暴力破解 、撞库攻击

解决思路：

1. 攻击者的请求密集在登录接口
2. 登录失败的次数较高

统计 1 小时发生 1000 次以上登录事件的登录成功率

```
SELECT ip, status_code, count(status_code)
FROM access_log
WHERE url_path = "/login"
GROUP BY TUMBLE_WINDOW(TIMESTAMP, 60*60), ip, status_code
ORDER BY COUNT(ip) DESC
HAVING COUNT(ip) > 1000
```

SafelineQL 能干什么

问题2：

某投票业务，虽然一个账号只能投票一次，但是短时间内依然被刷了很多恶意票

解决思路：

1. 攻击者的请求密集在投票接口
2. 攻击者使用了批量账号来投票

统计 1 小时使用相同 IP 登录多个用户并投票的情况

```
SELECT
        ip, session
        COUNT(DICTINCT session) ,
FROM access_log
WHERE url_path = "/vote.php"
GROUP BY TUMBLE_WINDOW(TIMESTAMP, 60*60), ip, session
ORDER BY COUNT(DICTINCT session) DESC
HAVING COUNT(DICTINCT session) > 1000
```

总 结

01 流量分析对解决业务安全问题至关重要

02 WAF 占据流量关口，应该发挥更大的作用

03 SafelineQL 可以使流量分析更简单

Thanks