58同城

2021

58同城 第2届 安全技术沙龙

业务风控建设 & 应用安全实践

58安全应急响应中心 Security Response Center | 58安全 58 CYBERSECURITY

DATE - 2021.12.17 线上直播

微博安全

业务漏洞挖掘
案例与思考分享

微博安全高级工程师　唐茂凡

01

现状

分类

常规

注入、XSS、XXE、CSRF、SSRF、文件包含、命令执行、URL重定向、点击劫持等

业务

登录认证、业务办理、业务数据、业务流程逻辑、业务授权访问、业务接口调用、验证码、输入\输出、回退、密码找回、密码重置、实名认证、设置个人信息、绑定银行卡、红包优惠券、订单CURD、充值、支付、提现.....

其他

网络层漏洞、系统层漏洞、组件套件中间件漏洞等

不同

01 现状 为什么业务安全越来越受重视？

1、业务是企业核心
2、业务越来越广泛
3、开发人员安全意识薄弱
4、开发代码频繁迭代，内部监管不严格
5、危害大隐藏深
6、传统的安全防护设备收效甚微
7、没有很好的解决方案

+

1、日趋成熟的防护产品和解决方案

2、安全渠道变多，通报及时，补丁打得快

3、攻击者的目的以经济利益为主，攻击者平衡攻击成本。

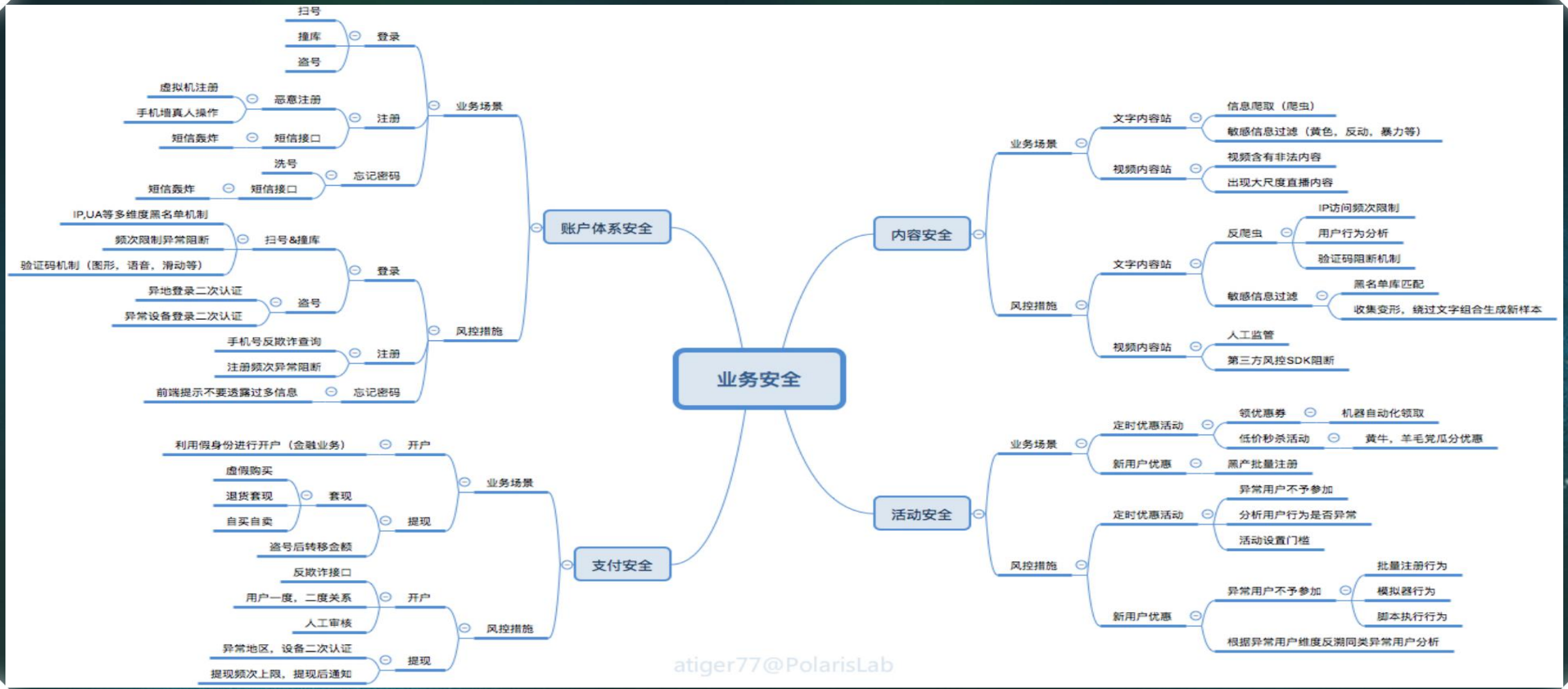
=

业务安全越来越被重视

02

风险

02 风险



03

怎么做

03 怎么做

微博安全

1、缺乏成熟的标准、工具、服务

2、信息不对称

3、外部力量有限

4、各种难：
难以接触业务环境
难以触发业务场景
难以理解业务原理和风险
……

03 怎么做 企业不同时期业务与安全的关系

微博安全

前期	中期	后期
1、以业务需求为主，注重功能实现 2、业务方安全意识薄弱 3、基础安全为主，不够重视业务安全 4、风险未集中暴露，不能有效止损 5、事前缺乏安全评审与安全测试 6、事中缺乏安全监控与风控运营 7、事后缺乏支持难以溯源	1、除功能、性能、稳定性，安全成为业务的一个属性 2、业务方安全意识提高 3、业务安全基础建设、业务安全价值体现，安全话语权提高 4、风险集中暴露，事件经验迅速积累 5、防护监控设备 6、网络层，系统层，组件套件层漏洞难以利用 7、攻击者目标更多转向业务逻辑层	1、业务安全标准化作业 2、业务安全决策影响 3、业务安全咨询，支持创新业务发展 4、基于业务安全体系建设，保障业务持续增长，从止损思维到盈利思维转化 5、业务安全能力对外输出
只对主要业务进行渗透测试、代码审计 被动事后响应	切入到业务需求评审、 业务设计	深入了解业务特点和安全需求，根据业务系统架构，从前/后视角、业务视角与支撑系统视角划分测试对象，结合所有信息获取和评估手段控制风险。
缺乏必要的安全评估与测试	基于漏洞类型的自动化扫描检测，辅以人工测试（传统类型的漏洞为主）	基于业务场景的安全测试，以业务场景、流程为重心，人工测试主导+自动化漏洞发现

03 怎么做 重视业务漏洞+较为完善的漏洞发现能力

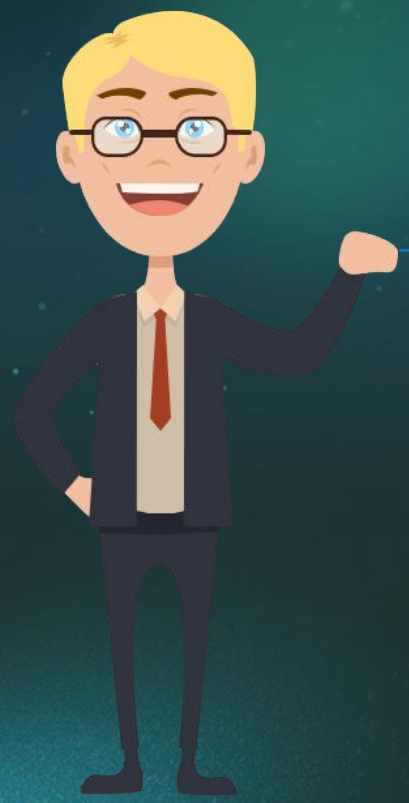
03 怎么做 不同的业务场景

注意：

1、注册登录接口收紧和统一
2、账号一对一绑定
3、优惠券发放
4、高并发
5、拉新传播风险
6、奖金支付方式
7、机器行为、刷单、薅羊毛
8、支付唯一性校验
9、安全漏洞评估
10、接口健壮性
11、降级策略
12、异常监控和发现
13、风控接入与应急预案
14、业务规则很重要
15、日志留存回溯

……

03 怎么做 安全测试人员需要哪些能力



- 安全能力
- 业务理解能力
- 了解黑灰产
- 信息获取与沟通能力

03 怎么做 真正理解业务

微博安全

01

业务场景建模

02

业务流程梳理

03

业务风险点识别

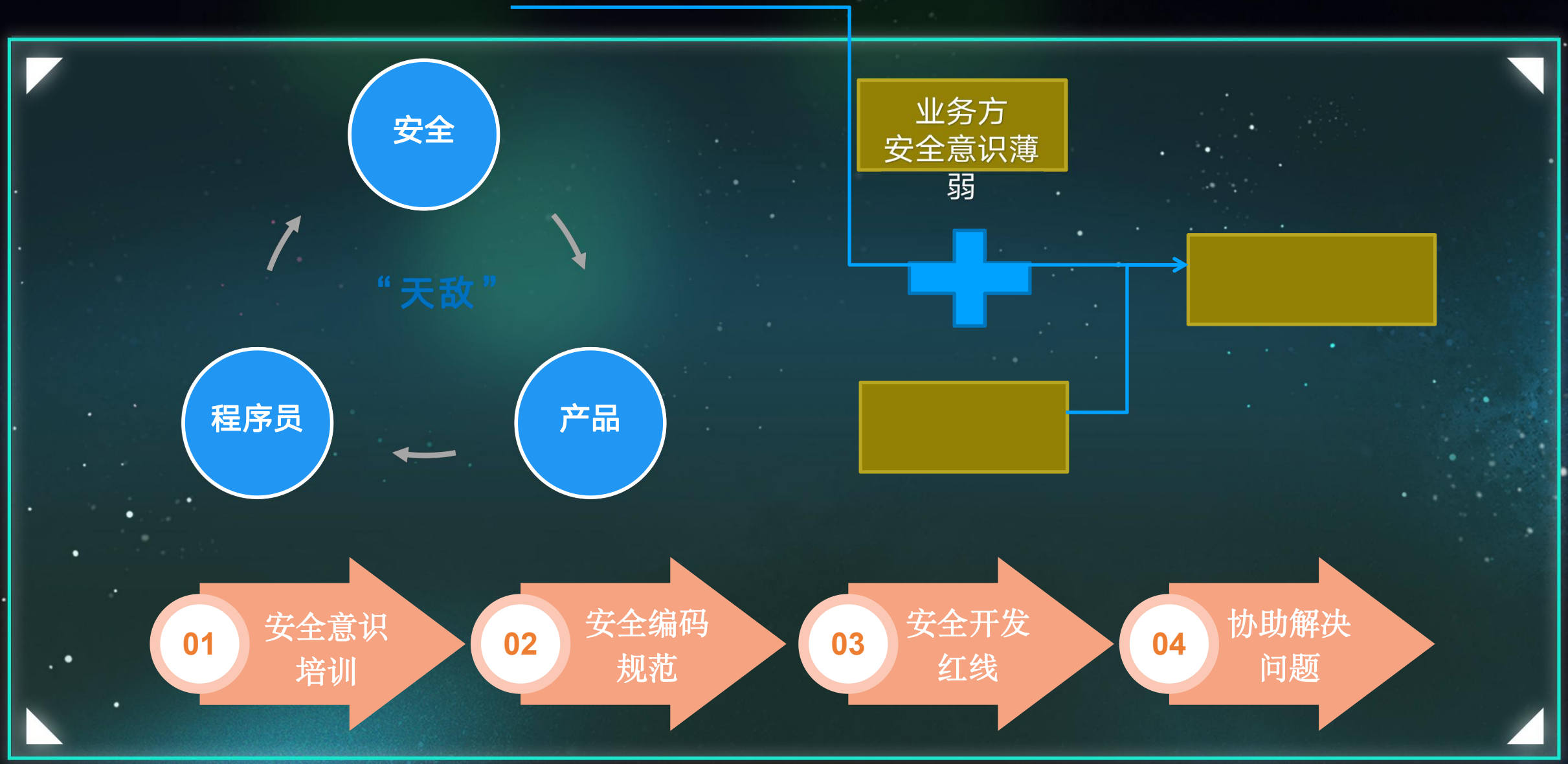
04

基于业务场景、流程、风险点进行安全测试

04

体会&经验&思考

04体会&经验&思考


安全
“天敌”
程序员
产品
业务方
安全意识薄
弱
01
安全意识
培训
02
安全编码
规范
03
安全开发
红线
04
协助解决
问题

定位

背锅侠or救火队or找茬的？