OWASP
Open Web Application
Security Project

平安金融安全研究院
PingAn Academy of Financial Security

OWASP自动威胁手册-WEB应用

邱菁萍 | 2018/09/17

OWASP
Open Web Application Security Project

平安金融安全研究院

PingAn Academy of Financial Security

业界**首家**综合性的**金融安全**研究及创新机构，以“聚焦金融、着力创新、引领行业、打造品牌”为指导方针，以倡导并共建**“科技+安全+生态”**的科技创新及应用体系为核心，着力整合**“政、产、学、研、金、介、用”**的业界优秀资源，与国家、行业、高校、研究院所等强强联合，“一手抓创新，一手抓落地”，创造一个良好的金融安全创新环境和生态，为平安集团、行业、国家提供强有力的金融安全技术支撑，为金融机构在互联网、人工智能时代下的信息安全建设、业务安全风控、金融科技安全保障和国家金融安全作出科技贡献，形成可持续发展的独特学术研究优势、产品和服务，推动和引领我国在金融安全方面上的科学技术进步，打造金融安全品牌。

引领信息安全，构建**“金融安全3.0”**大生态圈，打造金融安全品牌。

OWASP
Open Web Application Security Project

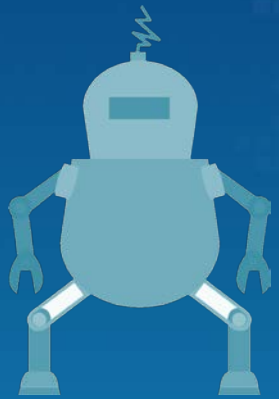
平安金融安全研究院
PingAn Academy of Financial Security

目录
CONTENTS

>> 项目介绍

- 大部分WEB应用随时面临威胁和攻击
- 应用程序漏洞类型/有效功能滥用?
- 什么才算是一个“事件”？/单个事件的影响?
- 攻击者实际在做什么?

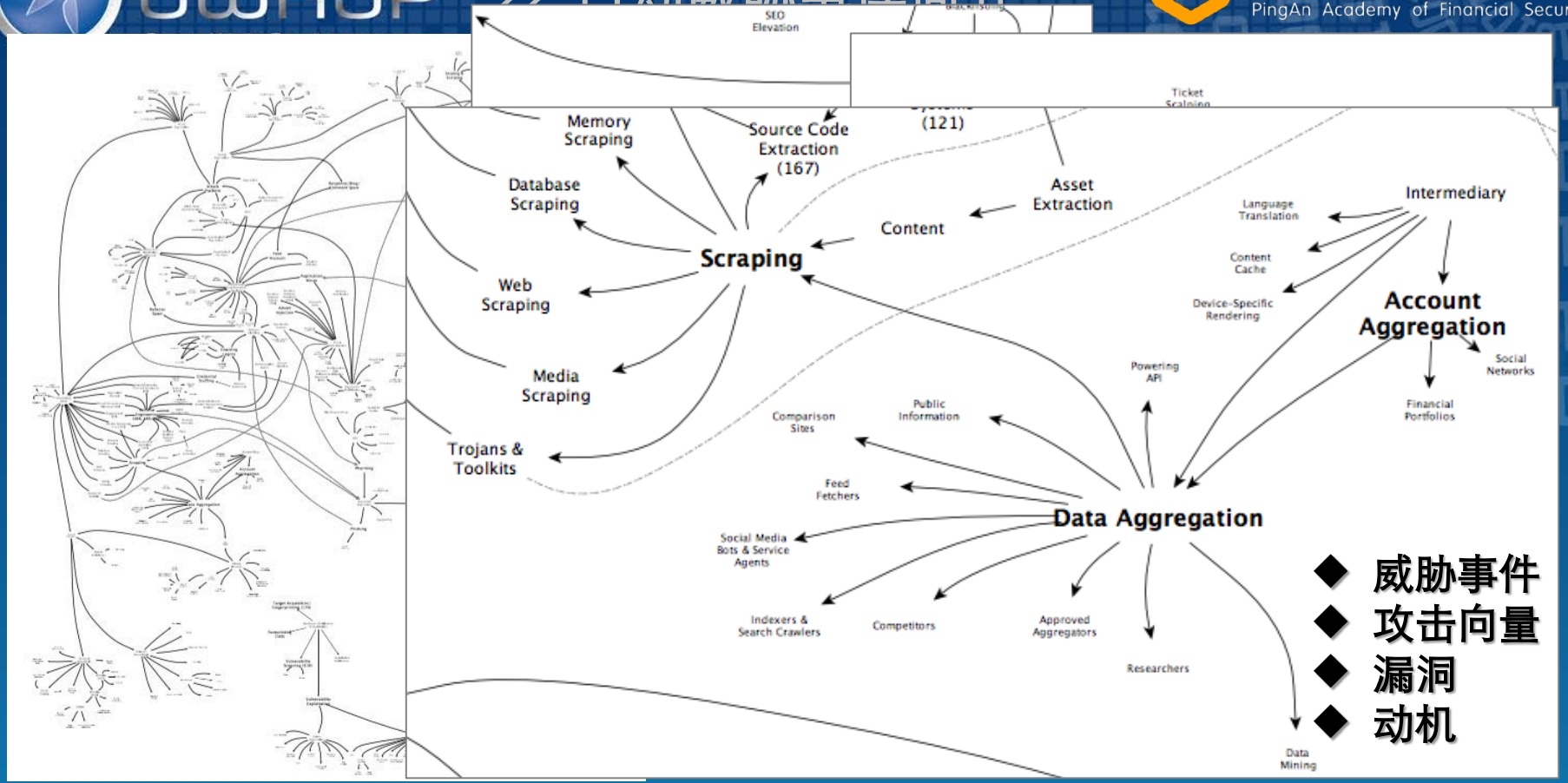
→ **“现在正在发生什么？”**



- 《OWASP Top 10（Web应用）》
- 《OWASP Top 10（Web应用）主动控制》
- 《OWASP WASC Web黑客事件数据库项目》
- ……

《OWASP自动威胁手册-WEB应用》
by Colin Watson，Tin Zaw

OWASP自动威胁手册从150余种信息来源中，读取并筛选出相关的威胁信息，最终总结出21个威胁事件，探究自动威胁的症状、缓解措施和控制方法。希望通过本项目为开发人员、架构师、运营商、企业主、安全工程师、采购商和供应商等提供一种通用语言，以促进沟通和解决实际问题。



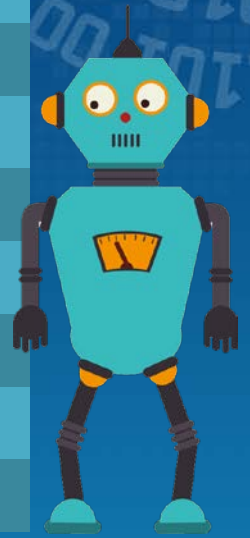
- 威胁事件
- 攻击向量
- 漏洞
- 动机

OWASP
Open Web Application Security Project

自动威胁事件简介

平安金融安全研究院
PingAn Academy of Financial Security

编号	名称
OAT-001 Carding	被盗卡确认
OAT-002 Token Cracking	凭据破解
OAT-003 Ad Fraud	广告欺诈
OAT-004 Fingerprinting	特征获取
OAT-005 Scalping	投机交易
OAT-006 Expediting	加速执行
OAT-007 Credential Cracking	凭证破解
OAT-008 Credential Stuffing	凭证收割确认
OAT-009 CAPTCHA Defeat	验证码破解
OAT-010 Card Cracking	支付卡破解
OAT-011 Scraping	信息搜刮
OAT-012 Cashing Out	盗用账户牟利
OAT-013 Sniping	交易狙击
OAT-014 Vulnerability Scanning	漏洞扫描
OAT-015 Denial of Service	拒绝服务
OAT-016 Skewing	重放
OAT-017 Spamming	垃圾信息
OAT-018 Footprinting	成分获取
OAT-019 Account Creation	账户创建滥用
OAT-020 Account Aggregation	恶意账户组合
OAT-021 Denial of Inventory	拒绝库存



OWASP
Open Web Application Security Project

自动威胁事件简介

平安金融安全研究院
PingAn Academy of Financial Security

◆ 与账户凭证相关的自动威胁事件

OAT-007 Credential Cracking	凭证破解
OAT-008 Credential Stuffing	凭证收割确认
OAT-019 Account Creation	账户创建滥用
OAT-020 Account Aggregation	恶意账户组合

◆ 与支付卡持有人数据相关的自动威胁事件

OAT-001 Carding	被盗卡确认
OAT-010 Card Cracking	支付卡破解
OAT-012 Cashing Out	盗用账户牟利

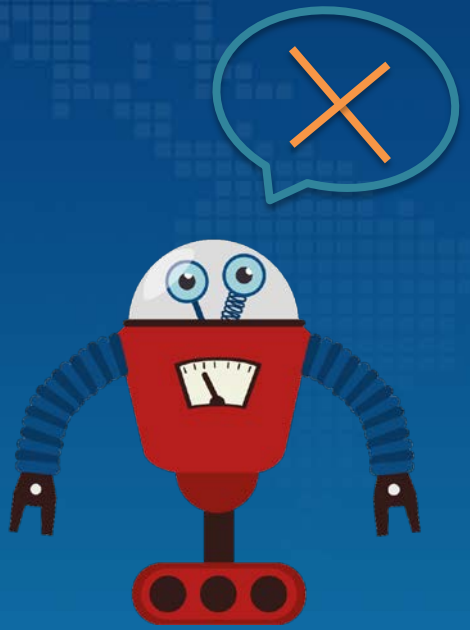
◆ 与漏洞识别相关的自动威胁事件

OAT-004 Fingerprinting	特征获取
OAT-014 Vulnerability Scanning	漏洞扫描
OAT-018 Footprinting	成分获取

◆ 与可分配存货相关的自动威胁事件

OAT-005 Scalping	投机交易
OAT-011 Scraping	信息搜刮
OAT-021 Denial of Inventory	拒绝库存

自动威胁事件简介

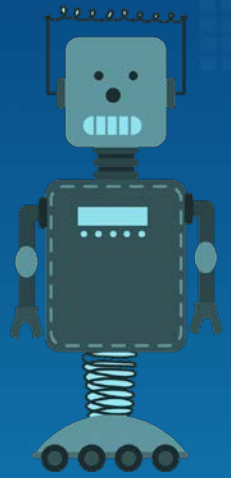


不包括：

应用程序消耗（Application Consumption）
应用程序蠕虫（Application Worms）
资产剥离（Asset Stripping）
攻击平台（Attack Platform）
代码修改（Code Modification）
表单劫持（Form Hijacking）
浏览器数据包截获（Man in the Browser，MitB）
逆向工程（Reverse Engineering）

>> 对策分析

对于所有程序来说，开发人员与安全人员的**构建-防御协作（builder-defender）**是控制和减轻自动化威胁的关键。



- 软件安全开发生命周期（S-SDLC）：构建；防御
- 对策是指三种减少已识别的自动威胁风险的控制措施：

预防——通过控制机制降低自动威胁造成的影响；

检测——通过控制机制识别用户是否为自动化程序或真正的人类用户，并/或识别自动化攻击是否正在发生，或曾经发生过；

恢复——通过控制机制协助响应自动威胁导致的事件，包括：减少攻击影响、帮助应用程序恢复正常。

对策分类		SDLC阶段		对策类型		
关键词	描述	构建	防御	预防	检测	恢复
值	禁止或限制应用程序访问资产，可以降低自动攻击带来的风险，包括确认数据和/或功能是否必要，是否可以被攻击者篡改。	Y		Y		

>> 对策分析

自动化威胁对策类型（1）

关键词	描述
值	禁止或限制应用程序访问资产，可以降低自动攻击带来的风险，包括确认数据和/或功能是否必要，是否可以被攻击者篡改。
要求	在安全风险评估时识别自动攻击威胁，并评估对策对功能可用性和可访问性的影响，进而确定应用开发和部署的要求。
测试	创建模拟自动化攻击的误用滥用的测试用例。
流量	创建足够大的访问带宽流量，当使得允许和潜在的自动化使用攻击发生时，不影响正常的使用/性能。
混淆	通过动态改变URL、字段名和内容、限制访问索引数据、或添加额外标头/范围，或转换数据为图片、或添加页和会话特定标识来防御自动化攻击。对策还包括减少数据泄露、对功能进行整合让应用程序不被外部访问、伪装或通过其他方式混淆，让自动化工具无法理解或映射程序及功能。
鉴定	考虑使用自动化攻击识别技术来区别和限制自动化访问案例。利用用户代理和/或HTTP请求（例如http头排序）、http头异常（例如http协议、标头不一致）、设备指纹来确认用户是否是人类。
信用	考虑通过信用数据库方法来识别和限制自动使用。通过分析用户身份（例如浏览器指纹、设备指纹、用户名、会话、IP地址/范围/地址位置），或用户行为（例如之前访问的站点、访问点、访问时间、请求率、新会话产生的数量、访问的路径），或访问资源的类型（例如静态或动态、隐藏的链接、robots.txt 文件、robots.txt 文件外的路径、蜜罐中的资源、缓存资源）、不能访问的资源（如js生成的链接）、或重复访问的资源类型。像指纹一样，信用数据库方法可以用于确认用户是否为人类,包括使用欺诈检测系统、第三方拒绝/阻止列表、信用和检查服务。

>> 对策分析

自动化威胁对策类型（2）

关键词	描述
认证	使用访问控制列表、要求用户进行认证，或二次认证、生物识别，或要求加强型的认证方法包括邮箱认证、拼图/验证码、复杂密码和时效要求、强验证、双因素认证、在操作/查询时再次验证、不允许账号并发访问、避免基于单因素密码的身份访问，不使用SSO（single sign on，单点登录），并且不支持虚拟货币。
限速	设置访问上限/下限/趋阈值，限制每个/组用户，每个IP/IP范围，每个设备ID/指纹等使用的数量和速率。限制每个交易事件的值，还包括使用排队系统、用户优先级功能和资产分配随机化。
监测	对错误、异常、功能使用/排序进行监测，提供告警和监视仪表板。通过自动化监控系统监控用户生成的内容。
方法	在应用程序内构建观测工具实时执行攻击检测和OWASP AppSensor中定义的自动化攻击，应用程序应和其他系统组件（如网关、网络防火墙或应用防火墙）对已经识别的自动攻击作出响应。响应可以包括增加监控、锁定用户、阻止/延迟/改变操作、改变流量/能力、增强身份认证、CAPTCHA验证码、设置禁区等等。
合同	通过合同、条款、指引、要求的方式约束用户不可以使用自动化方式对应用进行攻击。了解合同限制对应用其他方面的影响（比如服务级别、金融信用）。
响应	对各种自动化攻击场景定义应急处理操作，一旦检测到攻击，使用实际数据来反馈对策（比如需求、测试、监控）。
分享	与同行、贸易组织、国家CERTs分享自动化攻击的信息，例如IP地址、已知的违规设备指纹。

>> 用户案例场景

- 定义应用程序开发的安全性要求
- 在部门内分享情报
- 在不同CERTs之间交换威胁数据
- 提高应用程序渗透测试的发现结果
- 明确服务的获取需求
- 识别供应商服务的特征
- ……

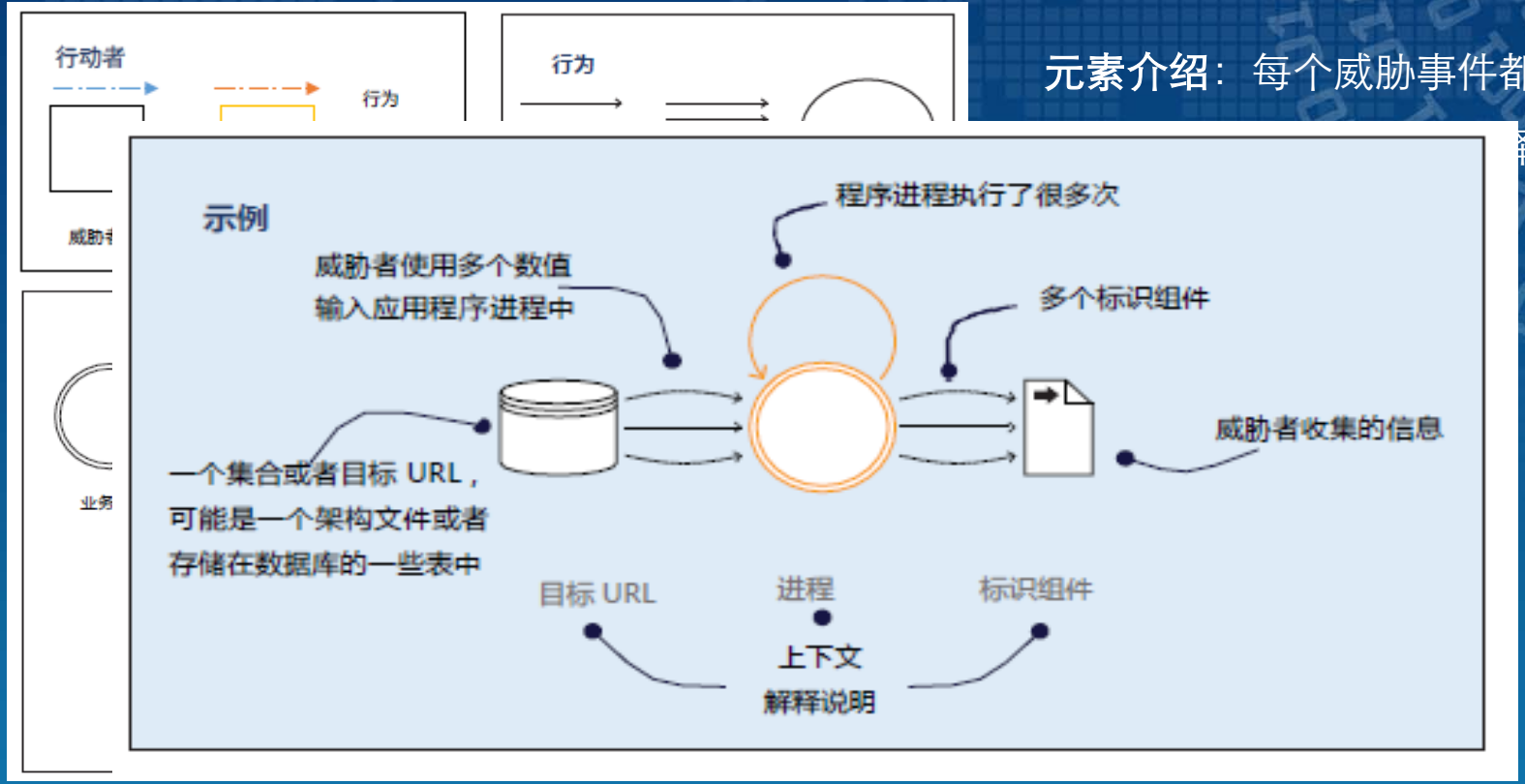
一些应用程序安全规范和安全需求是根据这些威胁事件确定的，而不是针对特定产品或服务类别。投标的应用程序开发公司可使用自动威胁手册来适当地重点关注对这些威胁事件的安全需求。

>> 用户案例场景

- 定义应用程序开发的安全性要求
- 在部门内分享情报
- 在不同CERTs之间交换威胁数据
- 提高应用程序渗透测试的发现结果
- 明确服务的获取需求
- 识别供应商服务的特征
- ……

国家计算机紧急响应小组（CERTs）意识到分享本地信息资源有助于全球网络攻击预防。CERT Zog和CERT Tarset同意根据OWASP自动威胁手册定义给威胁事件加标签，以便为它们之间的威胁数据交换增加更多解决方案场景。

自动威胁事件导引



元素介绍：每个威胁事件都包含一

释了所用

OWASP
Open Web Application Security Project

>> 自动威胁事件导引

平安金融安全研究院
PingAn Academy of Financial Security

自动威胁事件特征描述。

分类：对描述的威胁事件更具有普遍针对性的行业领域以琥珀色突出显示。

琥珀色突出显示的是此威胁事件影响最大的群体（个人，团体，应用程序用户和其他）。受影响群体判断的依据是应用程序和它的数据。

以琥珀色突出显示此威胁事件在特定应用中被滥用最多的数据。

文献中可供参考的威胁事件名称，特定领域名称和攻击示例。

指示图：
描述威胁行为者的主要威胁面。

威胁事件完整描述。

内部引用参考：
关联或相似的OAT编码和名称。

外部参考引用：
1.匹配最佳的常见攻击模式/枚举和分类（CAPEC）；
2.相关CWE分类ID（类ID和变体ID）；
3.匹配的最接近的OWSAP攻击子类和名称；
4.匹配最佳的Web应用WASC威胁分类/威胁分类ID。

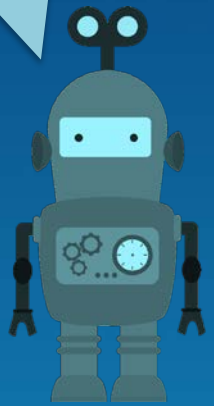
OWASP
Open Web Application Security Project

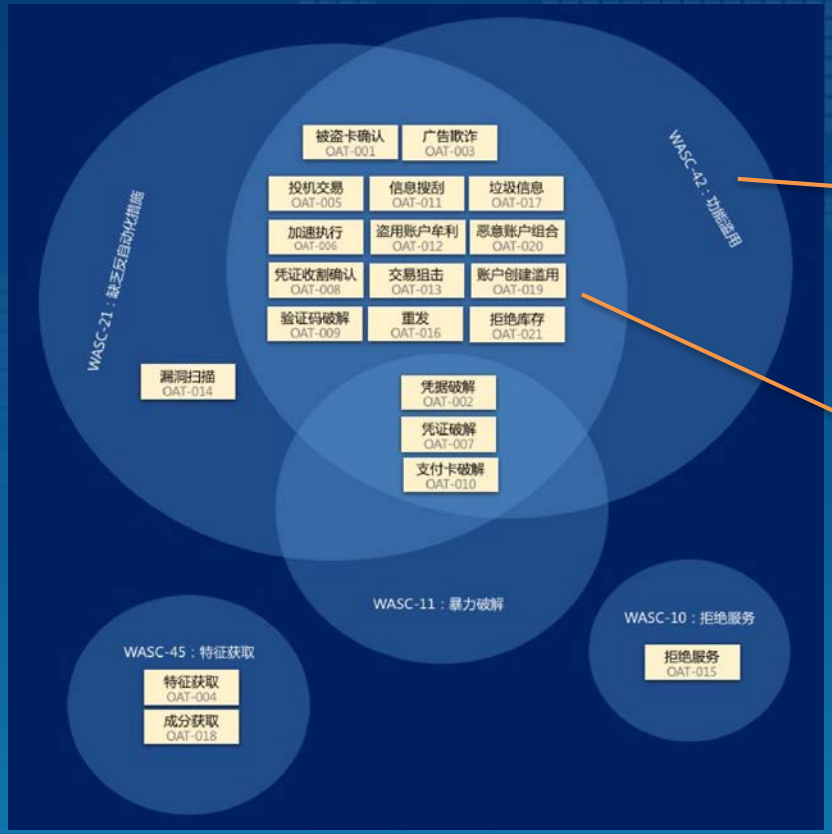
>> 自动威胁事件导引

平安金融安全研究院
PingAn Academy of Financial Security

例如: 与WASC自动威胁事件分类对比

外部参考引用:
1.Mitre CAPEC
2.相关CWE分类ID
3.OWSAP攻击子类
4. WASC威胁分类





WASC自动威胁事件分类

OWASP自动威胁事件分类

>> 结语

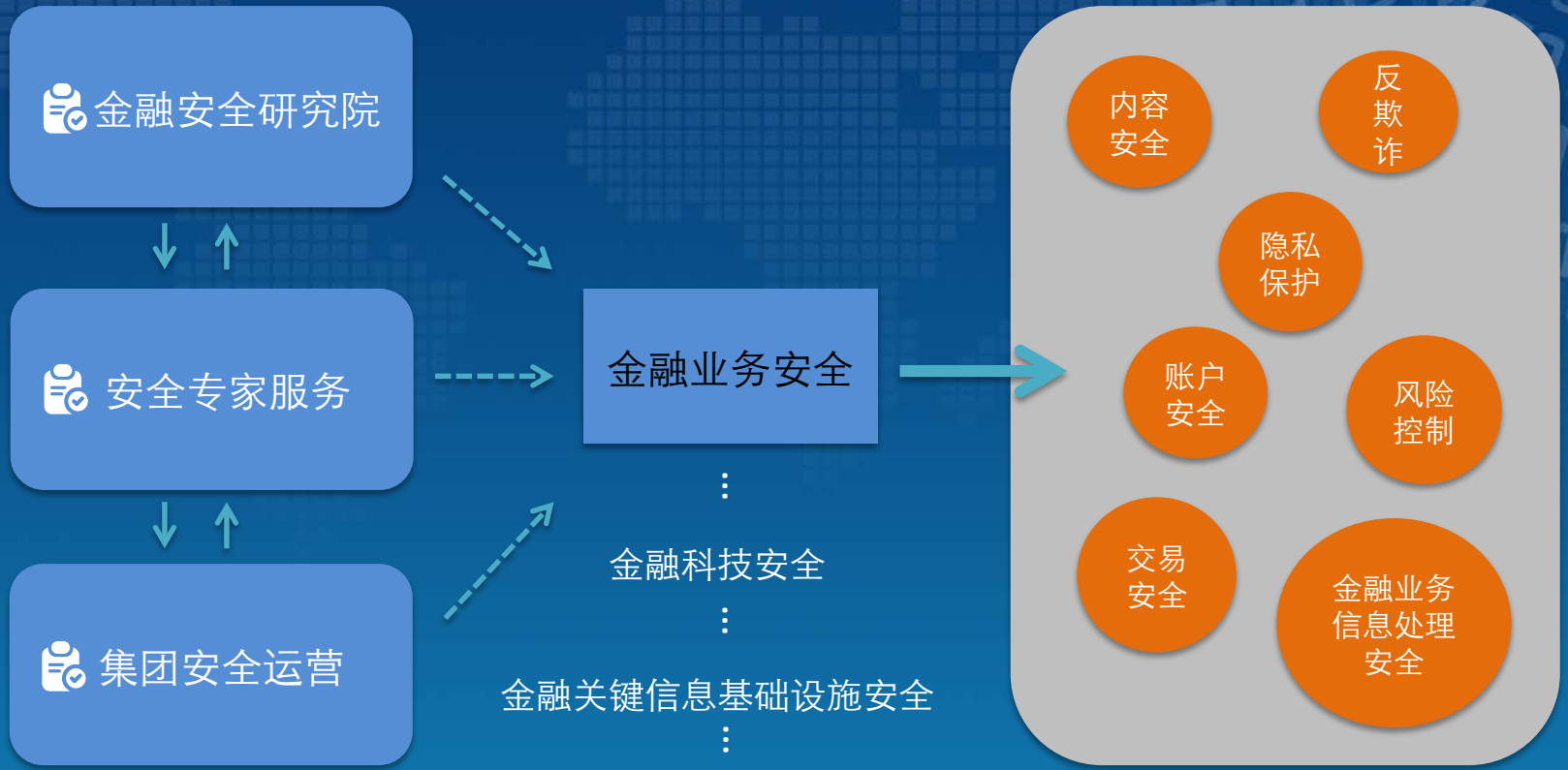
目标：

- 为“自动威胁”做定义
- 为自动威胁及其互相关系创建一个通用的词汇表
- 在检测和减轻恶意WEB自动威胁方面的行业标准
- 对整个软件安全开发生命周期中的系列活动是切实可行的

展望：

- 建立对策
- 分享信息
- 最佳实践

>> 结语


金融安全研究院
安全专家服务
集团安全运营
金融业务安全
金融科技安全
金融关键信息基础设施安全
内容安全
反欺诈
隐私保护
账户安全
风险控制
交易安全
金融业务信息处理安全

OWASP
Open Web Application Security Project

>> 参考资料

平安金融安全研究院
PingAn Academy of Financial Security

◆ OWASP Automated Threat Handbook Web Applications
https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf

◆ A New Ontology of Unwanted Automation (Colin Waston)
https://www.owasp.org/images/9/98/Colinwatson-a-new-ontology-of-unwanted-automation.pptx

◆ OWASP Automated Threats to Web Applications (Summary of research for ontology (threats and attacks, with some vulnerabilities and outcomes)
https://www.owasp.org/images/a/a2/Automated-threats.pdf

OWASP

Open Web Application Security Project

平安金融安全研究院

PingAn Academy of Financial Security

谢谢大家

平安金融安全研究院