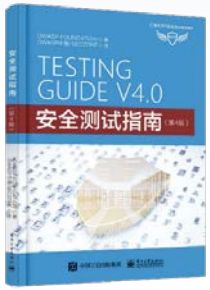
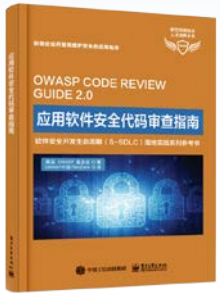
OWASP
Open Web Application Security Project

OWASP，以开源的方式支撑企业应用安全体系化建设

王颉

关于我





王颉 Ph.D（网络安全）

- 英国拉夫堡大学网络安全博士
- SecZone开源网安创始人之一
- 致力于应用安全与软件安全开发理念和技术的推广
- OWASP中国副主席
- OWASP中国成都区域负责人
- OWASP+OWASP China (2009-Now)
  - ✓ OWASP Top 10 2017, 2013, 2010
  - ✓ OWASP Secure Coding Practices - Quick Reference Guide
  - ✓ OWASP ASVS
  - ✓ OWASP Testing Guide
  - ✓ OWASP Code Review Guide
  - ✓ ……

OWASP
Open Web Application Security Project

https://www.owasp.org/index.php/User:Jie_Wang

Open Web Application Security Project

关于OWASP

O!WASP

About OWASP

Every vibrant technology marketplace needs an unbiased source of information on best practices as well as an active body advocating open standards. In the Application Security space, one of those groups is the Open Web Application Security Project (or OWASP for short).

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organizations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.

截止时间：2018年12月31日

OWASP全球企业会员

OWASP全球学术会员

截止时间：2018年12月27日

OWASP
Open Web Application Security Project

Pages in category "OWASP Project"

The following 200 pages are in this category, out of 388 total.

(previous page) (next page)

- OWASP in Action: Tools for the DISA ASD STIG

A

- OWASP Alchemist Project
- OWASP Anti-Malware Project
- AntiSamy Java 中文项目
- OWASP Application Security Program for Managers
- OWASP Application Security Skills Assessment
- AppSensor Summit
- OWASP Autumn of Code 2006 – Projects: Testing Guide

B

- Benchmark
- Best Practice: Projektierung der Sicherheitsprüfung von Webanwendungen
- Best Practices: Einsatz von Web Application Firewalls
- OWASP Bricks
- GPC Project Details/OWASP BWA Project
- OWASP Browser Security ACID Tests Project
- OWASP Web Browser Testing System Project

C

- Classic ASP Security Project
- GPC Project Details/OWASP Cloud - 10 Project
- GPC Project Details/OWASP Code Crawler
- Code review
- OWASP Codes of Conduct
- Collaborate

- OWASP iGoat Project
- Intelligent Security
- OWASP Internationalization

J

- OWASP Java HTML Sanitizer Project
- OWASP Java XML Templates Project
- JBroFuzz
- GPC Project Details/OWASP JBroFuzz
- GPC Project Details/OWASP JSReg Project

K

- Key Project Information:OWASP PCI Project

M

- OWASP Mantra – Security Framework
- Virtual Patching Best Practices
- Modsecurity crs 10 config.conf
- OWASP Myth Breakers Project

O

- O-Saft
- O-Saft/Documentation
- OWASP O2 Platform Project – Project Identification
- Octoms
- Opa
- Projects/Opa
- OWASP OVAL Content Project
- OWASP 1-Liner
- OWASP A&D Project
- OWASP Academy Portal Project

- OWASP Cyber Defense Matrix
- Owasp Cyber Security at the Board Level Project
- OWASP Damn Vulnerable Web Sockets (DVWS)
- OWASP DeepViolet TLS/SSL Scanner
- OWASP DefectDojo Project
- OWASP Dependency Check
- OWASP Dependency Track Project
- OWASP Desktop Goat and Top 5 Project
- OWASP DevSecOps Studio Project
- OWASP DevSlop Project
- OWASP Documentation Project Template
- OWASP Droid Fusion
- OWASP Droid10 Project
- OWASP DVSA
- OWASP Ecuador
- OWASP EJSF Project
- OWASP Embedded Application Security
- OWASP Encoder Comparison Reference Project
- OWASP Example Incubator
- OWASP Excess XSS Project
- OWASP Faux Bank Project
- OWASP File Hash Repository
- OWASP Financial Information Exchange Security Project
- OWASP Focus
- OWASP Framework Security Project
- OWASP Game Security Framework Project
- OWASP Global Chapter Meetings Project
- OWASP Glue Tool Project
- OWASP Good Component Practices Project
- OWASP Guide Project

- OWASP Common Numbering Project
- GPC Project Details/OWASP CBT Project
- Cornucopia – Ecommerce Website Edition – Wiki Deck
- OWASP Corporate Application Security Rating Guide
- OWASP Cross-Site Request Forgery Research Pool
- OWASP CSRFGuard Project/es
- CSRFProtector Project

D

- OWASP Data Exchange Format Project
- Diez Mayores 2004
- OWASP DVIA

E

- EDU
- Encrypted Token Pattern CSRF Defence Project
- OWASP Enterprise Application Security Project
- OWASP ESAPI C Project
- OWASP ESAPI C++ Project
- OWASP ESAPI Perl Project
- ESAPI Swingset
- OWASP ESOP Framework
- OWASP Exams Project

F

- OWASP Forward Exploit Tool Project

G

- OWASP German Language Project
- Germany/Projekte
- Germany/Projekte/Top 10
- Germany/Projekte/Top 10 fuer Entwickler
- GPC Project Details/OWASP Google Hacking Project
- OWASP Project Details Table 2

- OWASP AJAX Crawling Tool
- OWASP Amass Project
- OWASP Androick Project
- OWASP Anti-Ransomware Guide Project
- OWASP API Security Project
- OWASP APK DISSECTOR
- OWASP Application Fuzzing Framework Project
- OWASP Application Security Curriculum
- OWASP Application Security Guide For CISOs Project
- OWASP Application Security Guide For CISOs Project v2
- OWASP Application Security Program Quick Start Guide Project
- OWASP AppSec Designer Security Functional Requirements & Countermeasures Libraries
- OWASP AppSec Pipeline
- OWASP Appsec Tutorial Series
- OWASP AppSensor Handbook
- OWASP AppSensor Project
- OWASP ASP.NET MVC Boilerplate Project
- OWASP Assimilation Project
- OWASP ASVS Assessment tool
- OWASP Attack Surface Detector Project
- OWASP Auth
- OWASP Automated Threats to Web Applications
- OWASP Autosploit Project
- OWASP Barbarus
- OWASP Basic Expression & Lexicon Variation Algorithms (BELVA) Project
- OWASP Best Practices in Vulnerability Disclosure and Bug Bounty Programs
- OWASP Broken Web Applications Project
- OWASP Browser Security Project
- OWASP Bug Logging Tool

- OWASP H2H Tool Project
- OWASP HA Vulnerability Scanner Project
- OWASP Hackademic Challenges Project
- OWASP Hacking Lab
- OWASP Hacking-the Pentest Tutor Game
- OWASP Hive Project
- OWASP Honeypot Project
- OWASP ICS / SCADA Security Project
- OWASP iGoat Tool Project
- OWASP iMAS iOS Mobile Application Security Project
- OWASP Incident Response Project
- OWASP Information Security Metrics Bank
- OWASP Insecure Web Components Project
- OWASP Internet of Things Project
- OWASP iSABEL Proxy Server
- OWASP ISO IEC 27034 Application Security Controls Project
- OWASP ISO Project
- OWASP Java Encoder Project
- OWASP Java File I O Security Project
- OWASP Java J2EE Secure Development Curriculum
- OWASP Java Uncertain Form Submit Prevention
- OWASP JavaScript Sandboxes
- OWASP JAWS Project
- OWASP JOTP Project
- OWASP JSEC CVE Details
- OWASP JSON Sanitizer
- OWASP Juice Shop Project
- OWASP KALP Mobile Project
- OWASP Kates Project
- OWASP Knowledge Based Authentication Performance Metrics Project
- OWASP Knowledge Graph
- OWASP LAPSE Project

Webanwendungen
- OWASP Risk Rating Management
- OWASP Robot Security Project
- OWASP Ruby on Rails and friends Security Guide
- OWASP S.T.I.N.G Project
- OWASP SaaS Rest API Secure Guide
- OWASP SafeNuGet
- OWASP SafeNuGet Project
- OWASP SamuraiWTF Project
- OWASP Scada Security Project
- OWASP SE – Social Engineering
- OWASP SecLists Project
- OWASP Secu-RT Project
- OWASP Secure Application Design Project
- *OWASP Secure Application Lifecycle Management*
- OWASP Secure Configuration Guide
- OWASP Secure Development Training
- OWASP Secure Headers Project
- OWASP Secure Medical Device Deployment Standard
- OWASP Secure Software Contract Annex German
- OWASP Secure Software Contract Annex Italian
- OWASP Secure Software Development Lifecycle Project
- OWASP Secure TDD Project
- OWASP SecureTea Project
- OWASP Security Catalyst
- OWASP Security Controls in Web Application Development Lifecycle
- OWASP Security Frameworks Project
- OWASP Security JDIs Project
- OWASP Security Knowledge Framework
- OWASP Security Labeling System Project
- OWASP Security Logging Project
- OWASP Security Ninja Program Project
- OWASP Security Ninja Project
- OWASP Virtual Village Project
- OWASP Visual Crime Scene and Security Incident Education Project
- OWASP Vulnerability Management Guide
- OWASP Vulnerable Web Applications Directory Project
- OWASP WAF Project
- OWASP WAP–Web Application Protection
- OWASP WASC Distributed Web Honeypots Project
- OWASP WASC Web Hacking Incidents Database Project
- OWASP Watiqay
- OWASP Web Application Security Quick Reference Guide Project
- OWASP Web Malware Scanner Project
- OWASP Web Mapper Project
- OWASP WebSandBox Project
- OWASP WebSpa Project
- OWASP Windows Binary Executable Files Security Checks Project
- OWASP Wordpress Security Implementation Guideline
- OWASP Wordpress Vulnerability Scanner Project
- OWASP WS Amplification DoS Project
- OWASP XSecurity Project
- OWASP XSSER
- OWASP Zezengorri Code Project
- OWASP ZSC Tool Project
- OWASP中文项目

P

- OWASP Passw3rd Project
- OWASP Portuguese Language Project
- Project Information:template Vicnum Project
- Project Online Resources
- Project Reviews Guideline
- *Projects Reboot 2012*
- OWASP Spanish

T

- OWASP Testing Project
- OWASP Threat Modelling Project
- OWASP Tiger
- Top 10 2004
- GPC Project Details/OWASP Top10

U

- OWASP Uniform Reporting Guidelines

V

- OWASP VFW Project
- GPC Project Details/OWASP Vicnum Project

W

- WASC OWASP Web Application Firewall Evaluation Criteria Project
- OWASP Web Application Security Accessibility Project
- OWASP Web Service Attack Community Project
- WebGoatPHP
- OWASP WebScarab NG Project
- Proyecto WebScarab OWASP
- OWASP WhatTheFuzz Project
- OWASP Web Testing Environment Project

X

- OWASP Fiddler Addons for Security Testing Project
- OWASP Xenotix XSS Exploit Framework

Z

- OWASP SAMM Project
- OWASP Zed Attack Proxy Project

OWASP权威性

美、欧、日等多个国家的**32个**政府与行业组织机构引用了OWASP研究成果，形成**近百项**国际法规、标准、指南和行业行为准则。

目前，OWASP中国正致力于推进我国有关应用软件安全标准的建设。

https://www.owasp.org/index.php/Industry:Citations#National_.26_International_Legislation.2C_Standards.2C_Guidelines.2C_Committees_and_Industry_Codes_of_Practice

OWASP
Open Web Application Security Project

OWASP中国

播放视频

OWASP
Open Web Application
Security Project

OWASP中国区域分部

现有16个区域分部：

- 北京区域
- 上海区域
- 广东区域
- 广西区域
- 浙江区域
- 江苏区域
- 安徽区域
- 湖北区域
- 四川区域
- 山东区域
- 陕西区域
- 新疆区域
- 海南区域
- 辽宁区域
- 吉林区域
- 黑龙江区域

OWASP
Open Web Application Security Project

Open Web Application Security Project

关于“应用安全”

什么是应用安全？

OWASP
Open Web Application Security Project

行业认知中的应用安全

安全牛网络安全行业全景图（**2018年7月**）

OWASP
Open Web Application Security Project

什么是应用安全？（广义）

Wangjie8578sz Talk Sandbox Preferences Beta Watchlist Contributions Log out

Article Talk | Read Edit source View history | Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction

Help
About Wikipedia
Community portal

Application security

From Wikipedia, the free encyclopedia

This article **may be in need of reorganization to comply with Wikipedia's layout guidelines**. Please help by editing the article to make improvements to the overall structure. *(August 2016) (Learn how and when to remove this template message)*

Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle such design, development, deployment, upgrade, maintenance.

An always evolving but largely consistent set of common security flaws are seen across different applications, see common flaws

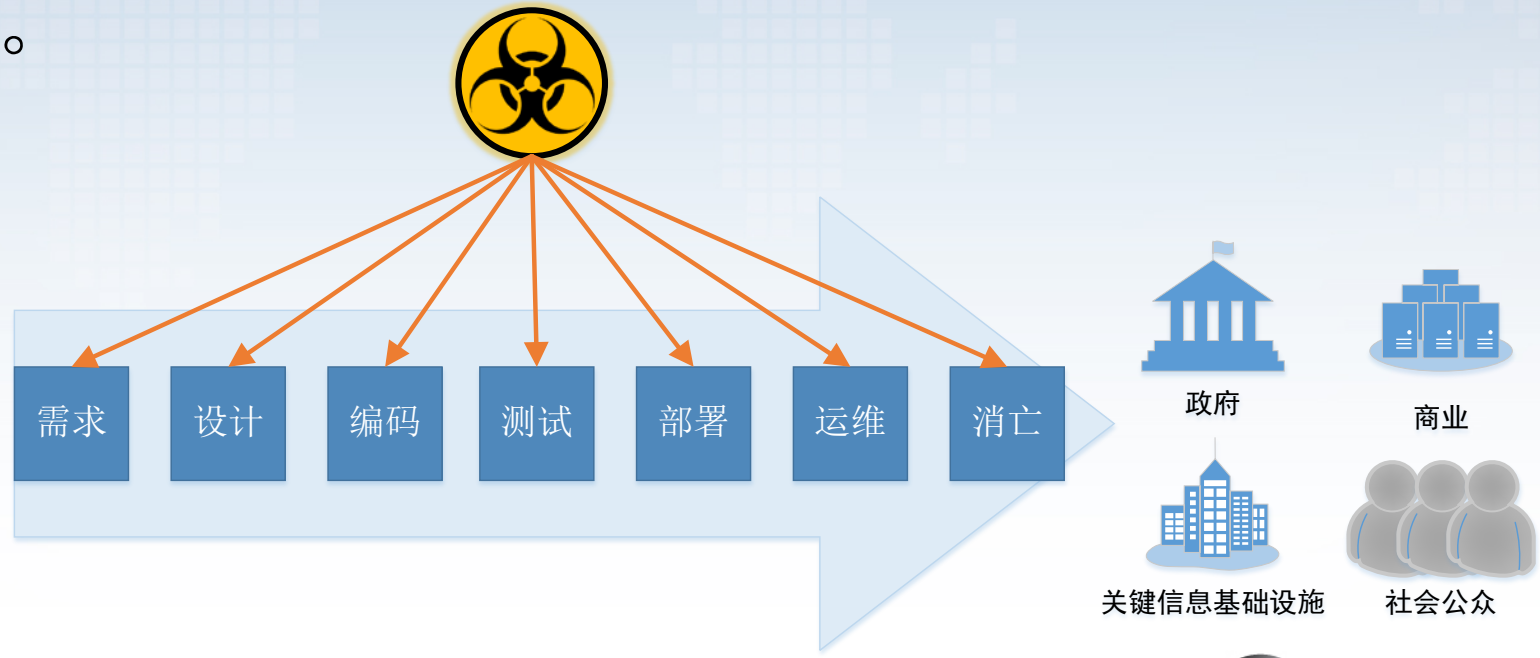
This article is part of a series on
Information security
Related security categories
- Internet security
- Cyberwarfare
- Computer security
- Mobile security
- Network security

- **Application security** encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.
- Different techniques are used to surface such security vulnerabilities at different stages of an applications lifecycle, such as: design, development, deployment, upgrade, maintenance.
- 软件开发安全

OWASP
Open Web Application Security Project

软件供应链安全/攻击

- 通过软件供应链上任何阶段对软件代码的恶意行为，影响或破坏最终用户的信息安全。



图片参考来源：NCSC: Software Supply Chain Attacks

开源软件（源代码）安全

开源软件源代码安全缺陷分析报告

原创：CNCERT软件安全 CNCERT风险评估 前天

开源软件源代码安全缺陷分析报告

——物联网软件专题

1、概述

随着软件技术飞速发展，开源软件已在全球范围内得到了广泛应用。数据显示，99%的组织在其IT系统中使用了开源软件。开源软件的代码一旦存在安全问题，必将造成广泛、严重的影响。为了解开源软件的安全情况，CNCERT持续对广泛使用的知名开源软件进行源代码安全缺陷分析，并发布季度安全缺陷分析报告。

自2005年国际电信联盟（ITU）正式提出"物联网（IoT）"这一概念以来，物联网在全球范围内迅速获得认可。随着物联网技术的发展创新，大量智能家居和可穿戴设备进入了人们的生活，"万物互联"成为全球网络未来发展的重要方向。根据Gartner报告预测，2020年全球物联网设备数量将高达260亿个。然而，由于安全标准滞后，以及智能设备制造商缺乏安全意识和投入，物联网已经埋下极大隐患，为个人隐私、企业信息安全甚至国家关键基础设施带来严重的安全威胁。

本期报告选取全球20款知名物联网软件进行源代码安全缺陷分析，结合缺陷分析工具和人工审计的结果，评估项目的安全性。从测评结果来看，与往期其他领域开源软件相比，物联网类软件的安全缺陷较多，潜在的安全问题不容忽视。同时，技术人员随机地取安全缺陷进行人工利用，发现存在能够被证实的

安全缺陷种类：

1、输入验证

2、API使用

3、安全特性

4、并行计算

5、错误和异常处理

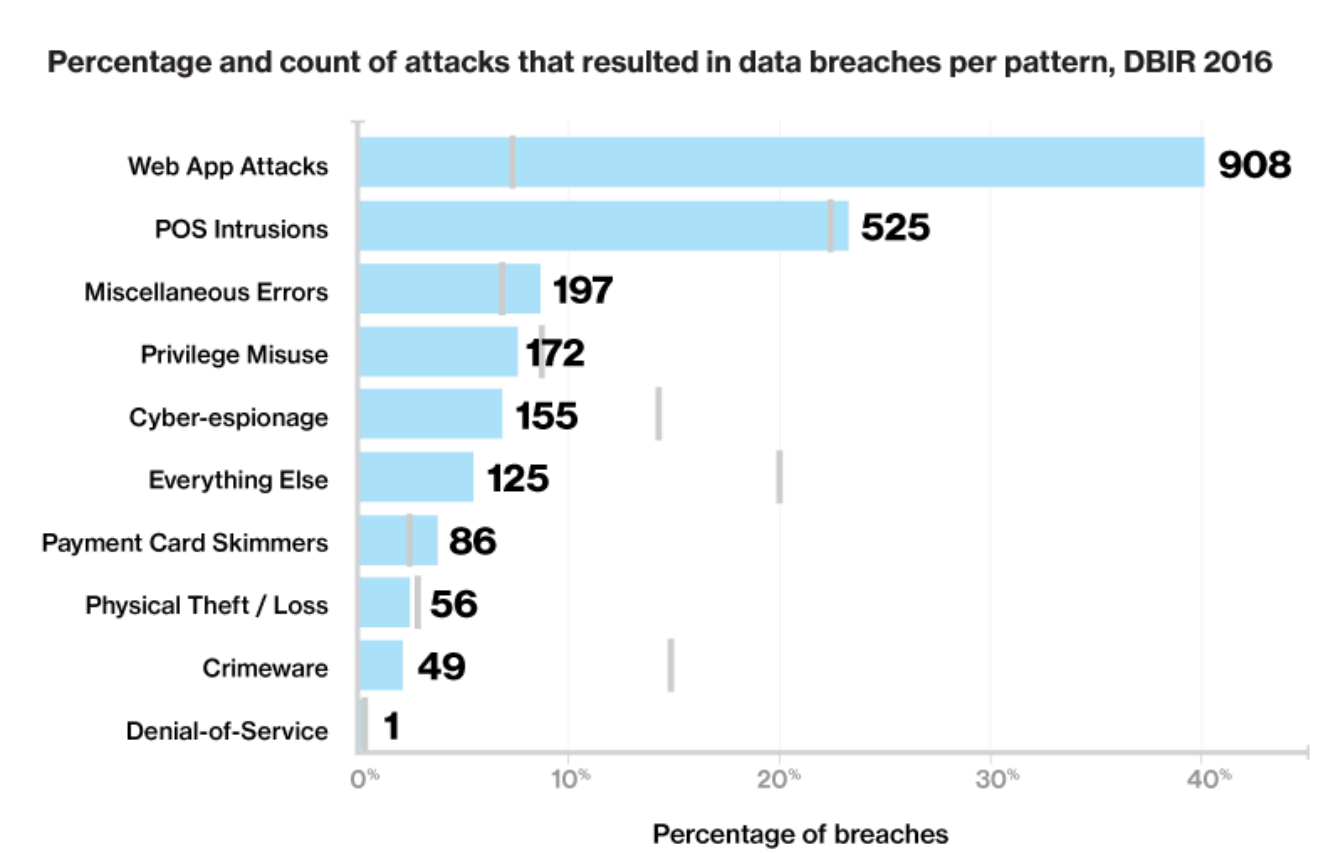
6、代码质量

7、封装和隐藏

8、代码运行环境

参考来源：CNCERT风险评估， 2019年1月10日，开源软件源代码安全缺陷分析报告——物联网软件专题

低劣的应用安全是个问题



29%—40%的数据泄露，是由应用安全问题引起的！

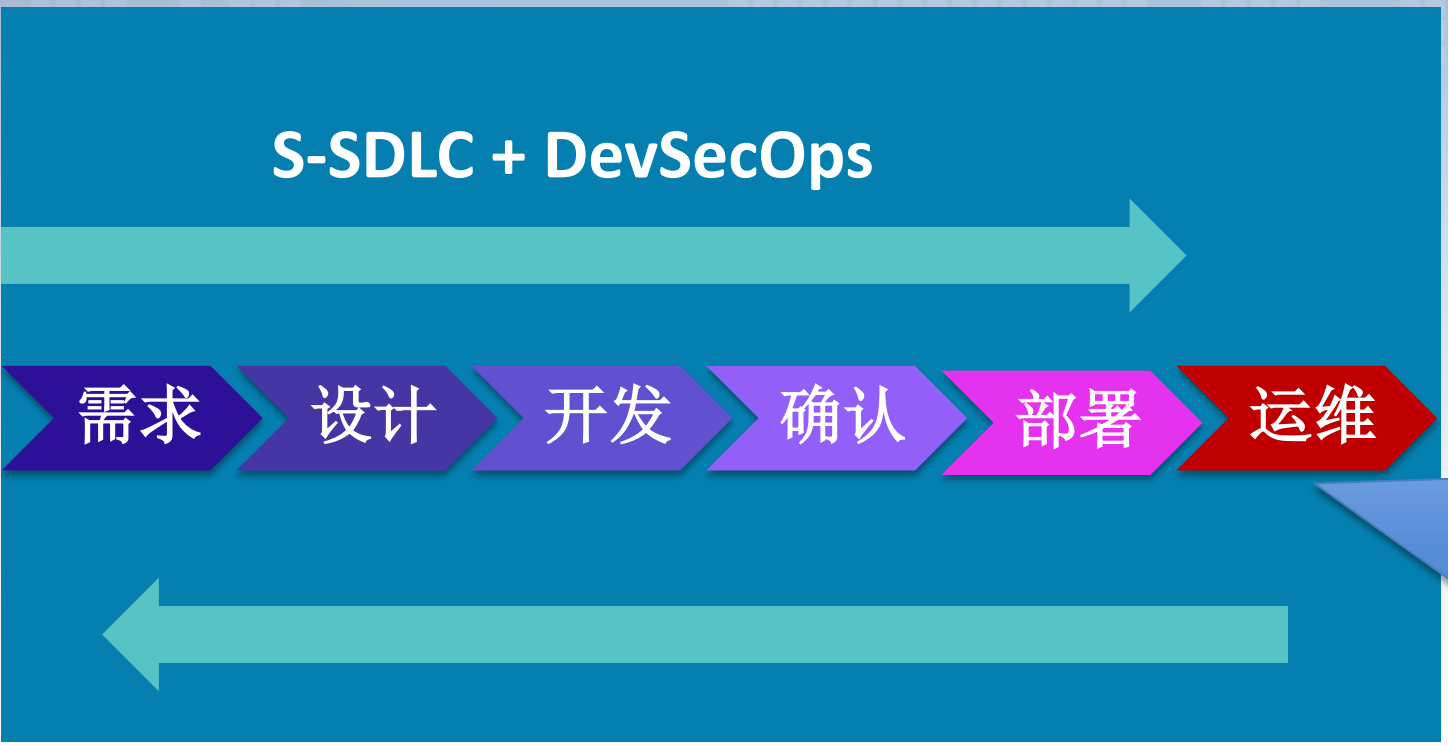
——2017年Verizon 数据泄露调查报告

企业面临的安全挑战

公司在网络安全保障方面高投入，安全设备、安全人才、SRC，要啥有啥，为啥还有那么多安全问题？

CEO

企业安全的本质原因



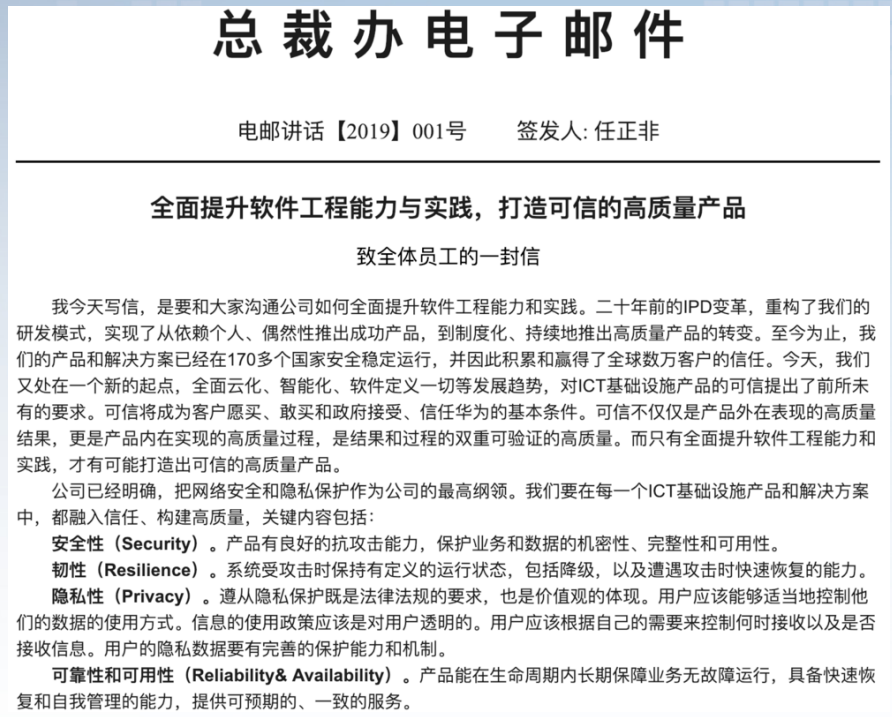
末端安全
（后端安全）

网络安全运维和网络安全管理

把安全左移，从软件系统诞生的源头出发！

OWASP
Open Web Application Security Project

华为2019年1号文件



总 裁 办 电 子 邮 件

电邮讲话【2019】001号　　签发人: 任正非

全面提升软件工程能力与实践，打造可信的高质量产品

致全体员工的一封信

我今天写信，是要和大家沟通公司如何全面提升软件工程能力和实践。二十年前的IPD变革，重构了我们的研发模式，实现了从依赖个人、偶然性推出成功产品，到制度化、持续地推出高质量产品的转变。至今为止，我们的产品和解决方案已经在170多个国家安全稳定运行，并因此积累和赢得了全球数万客户的信任。今天，我们又处在一个新的起点，全面云化、智能化、软件定义一切等发展趋势，对ICT基础设施产品的可信提出了前所未有的要求。可信将成为客户愿买、敢买和政府接受、信任华为的基本条件。可信不仅仅是产品外在表现的高质量结果，更是产品内在实现的高质量过程，是结果和过程的双重可验证的高质量。而只有全面提升软件工程能力和实践，才有可能打造出可信的高质量产品。

公司已经明确，把网络安全和隐私保护作为公司的最高纲领。我们要在每一个ICT基础设施产品和解决方案中，都融入信任、构建高质量，关键内容包括：

安全性（Security）。产品有良好的抗攻击能力，保护业务和数据的机密性、完整性和可用性。

韧性（Resilience）。系统受攻击时保持有定义的运行状态，包括降级，以及遭遇攻击时快速恢复的能力。

隐私性（Privacy）。遵从隐私保护既是法律法规的要求，也是价值观的体现。用户应该能够适当地控制他们的数据的使用方式。信息的使用政策应该是对用户透明的。用户应该根据自己的需要来控制何时接收以及是否接收信息。用户的隐私数据要有完善的保护能力和机制。

可靠性和可用性（Reliability& Availability）。产品能在生命周期内长期保障业务无故障运行，具备快速恢复和自我管理的能力，提供可预期的、一致的服务。

- 我们要转变观念，追求打造可信的高质量产品，不仅仅是功能、特性的高质量，也包括产品开发到交付过程的高质量。
- 我们要从最基础的编码质量做起，视高质量代码为尊严和个人声誉。
- 我们要深刻理解架构的核心要素，基于可信导向来进行架构与设计。
- 我们要重构腐化的架构及不符合软件工程规范和质量要求的历史代码。
- 我们要深入钻研软件技术，尤其是安全技术。
- 我们要遵守过程的一致性。
- 为此，我们要改变行为习惯，追求精品。我们要开放透明、积极和勇于揭示问题并主动推动改进。

做好应用安全的好处

- 在产品开发过程中，越早修复安全漏洞，成本投入越低。

源: Ponemon Institute Research

Open Web Application Security Project

如何开展应用安全体系建设？

如何开展应用安全体系建设？

体系化、工程化

人

流程

工具

安全团队/Security Champions

关于产品安全的指导

将产品安全和每一个产品团队融合

安全团队的目标

1. 降低部署代码中的漏洞数量；
2. 开发安全的软件；
3. 指导开发团队开发安全的软件；
4. 为企业内部的软件安全开发提供标准化的流程和工具；
5. 通过评估和度量，证明企业的软件安全能力成熟度。

意识、知识和教育：期望的效果

安全意识	安全知识	上手实操
• 基本理解有关应用安全领域中最重要的一些概念。	• 解决应用安全问题的参考信息； • 多种开发语言的安全编码样例； • 提供直接的安全需求。	• 帮助开发人员从安全漏洞利用（攻击）的维度理解和掌握安全意识和安全知识。

意识、知识和教育


OWASP Top 10 - 2017
The Ten Most Critical Web Application Security Risks


OWASP
Automated Threat Handbook
Web Applications


OWASP
Cheat Sheets


WEBGOAT


DevSLOp


Security Knowledge Framework


JS


H


HACKING-LAB


OWASP
Open Web Application
Security Project

安全意识：OWASP Top 10-2017

A1:2017 – 注入
A2:2017 –失效的身份认证
A3:2017 –敏感信息泄漏
A4:2017 – XML外部实体（XXE） [新]
A5:2017 – 失效的访问控制 [合并]
A6:2017 – 安全配置错误
A7:2017 – 跨站脚本（XSS）
A8:2017 – 不安全的反序列化 [新，来自于社区]
A9:2017 –使用含有已知漏洞的组件
A10:2017 – 不足的日志记录和监控 [新，来自于社区]

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP
Open Web Application Security Project

安全意识： OWASP Automated Threat Handbook Web Applications

OWASP
Automated Threat Handbook
Web Applications

业务逻辑安全

#badbots

Account Aggregation 恶意账户组合	Account Creation 账户创建滥用	Ad Fraud 广告欺诈	CAPTCHA defeat 验证码破解	Carding 盗刷	Card Cracking 支付卡破解	Cashing Out 套利
Credential Cracking 凭证破解	Credential Stuffing 凭证收割确认	Denial of Inventory 拒绝存货	Denial of Service 拒绝服务	Expediting 超速执行	Fingerprinting 特征获取	Footprinting 成分获取
Scalping 投机交易	Scraping 信息搜刮	Skewing 重放	Sniping 交易狙击	Spamming 垃圾信息	Token Cracking 凭据破解	Vulnerability Scanning 漏洞扫描

https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

OWASP
Open Web Application Security Project

安全知识：OWASP ASVS

Requirement	
V1. Architecture, design and threat modelling	V11. HTTP security configuration
V2. Authentication	V13. Malicious controls
V3. Session management	V15. Business logic
V4. Access control	V16. File and resources
V5. Malicious input handling	V17. Mobile
V7. Cryptography at rest	V18. Web services
V8. Error handling and logging	V19. Configuration
V9. Data protection	V11. HTTP security configuration
V10. Communications	

Application Security Verification Standard

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP
Open Web Application Security Project

CTF平台： OWASP Juice Shop Tool

- 基于JavaScript开发；
- 故意包含大量安全漏洞；
- 包含大量攻击挑战；
- 适用于OWASP Top 10方面的教学；
- 可用作渗透测试和安全扫描工具。

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

OWASP
Open Web Application Security Project

流程和度量：期望的效果

流程

- S-SDLC项目提供了企业落地实践的关注点；
- 威胁建模项通过样例展示了流程方法；
- 代码审核项目提供了如何执行代码审核及关注点；
- 测试指南项目提供了如何执行安全测试及有关安全漏洞利用的知识。

度量

- 了解企业当期的软件安全开发能力成熟度级别；
- 有助于明确企业未来软件安全开发能力成熟度发展的目标及提高方法。

流程与度量

CODE REVIEW GUIDE

OWASP Open Web Application Security Project | Testing Guide

Application Threat Modeling

流程：OWASP S-SDLC Project

- 由OWASP中国在全球发起和运营
- 一整套软件安全开发生命周期的方法论
- 工具：
  - VulHunter（SecZone开源网安）
  - OpenRASP（百度）
  - “INSIGHT” Platform（宜信）
- Top10：
  - S-SDLC落地实践Top 10
  - 安全意识Top 10

VulHunter

OpenRASP

宜信 CreditEase

https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project

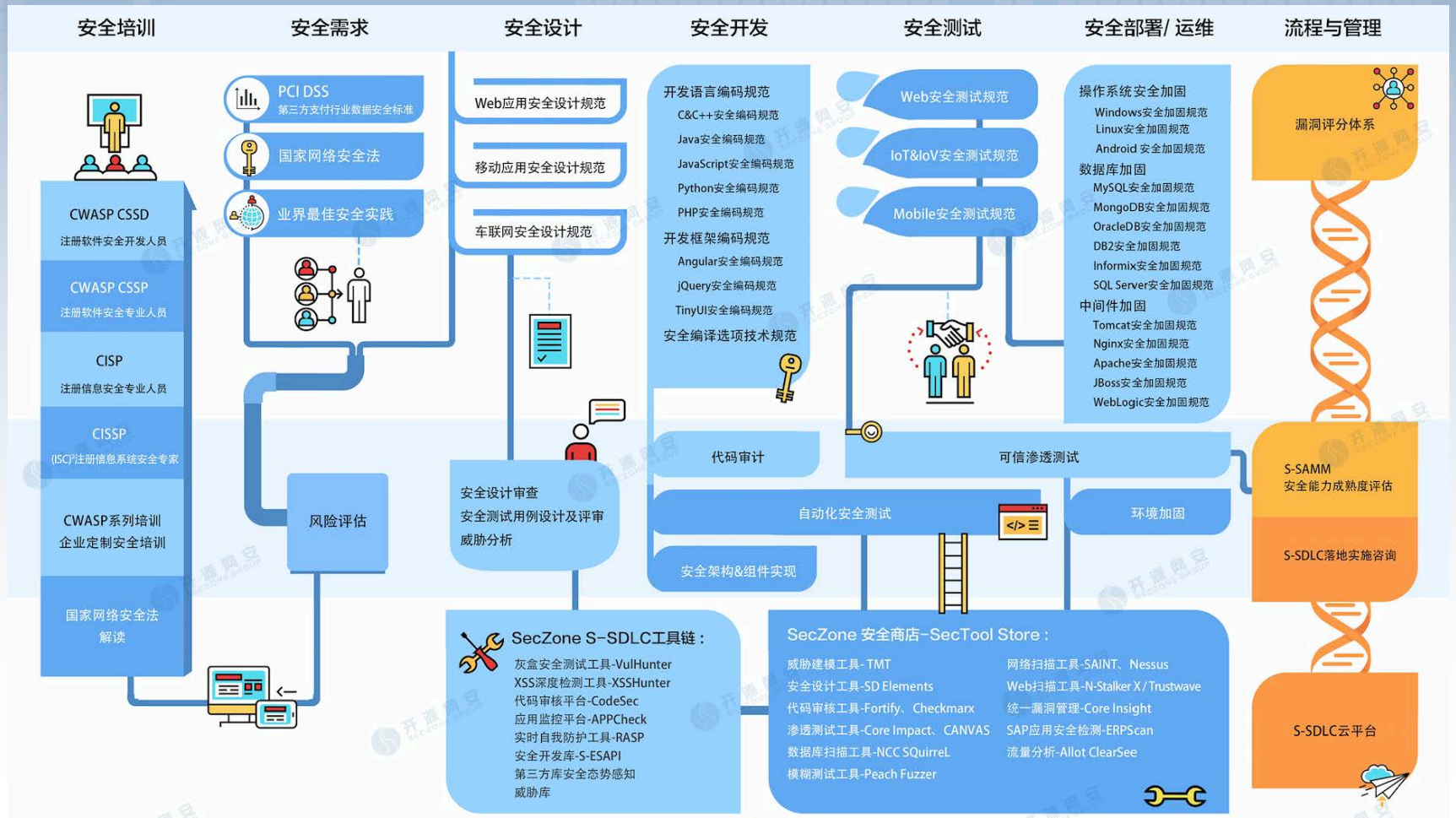
OWASP Open Web Application Security Project

OWASP S-SDLC落地实践Top 10

- 企业必须自上而下推行S-SDLC实施，且有相应的组织结构支撑
- S-SDLC要与企业的质量管理体系相结合
- 建立合适的人员培训体系
- 用度量体系将S-SDLC实施效果可视化
- 产品的安全目标决定S-SDLC的过程
- 威胁模型可以使产品避免大的设计风险
- 安全特性组件化可尽量避免编码漏洞
- 管理第三方软件的风险
- 安全服务化和自动化是实施DevSecOps的基础
- S-SDLC工具链

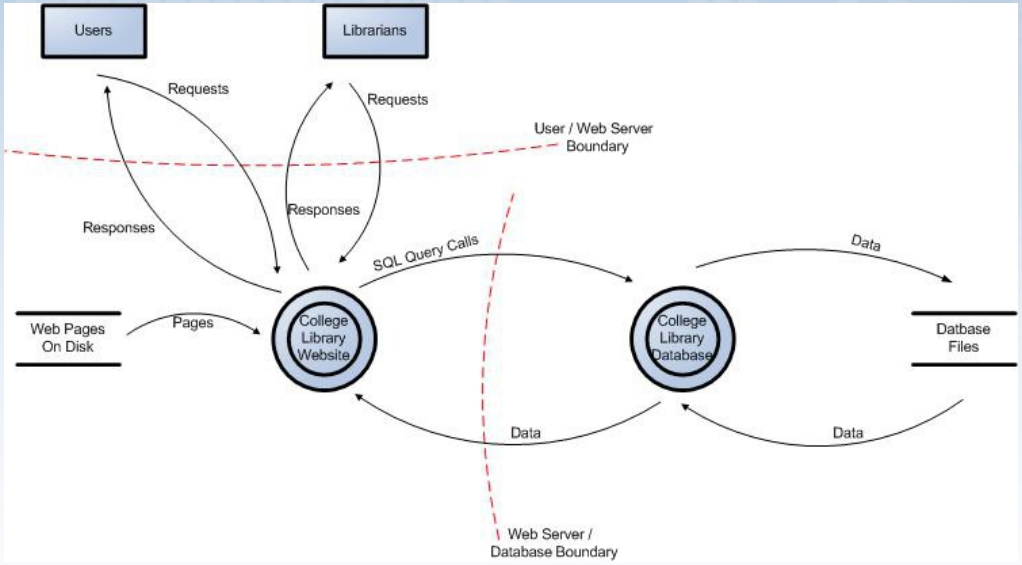
源: https://www.owasp.org/index.php/OWASP_Secure_Software_Development_Lifecycle_Project#tab=S-SDLC_Practices_Top_10

S-SDLC全景图



源: http://www.seczone.cn/2018/08/01/s-sdlc%E8%A7%A3%E5%86%B3%E6%96%B9%E6%A1%88v2-0/

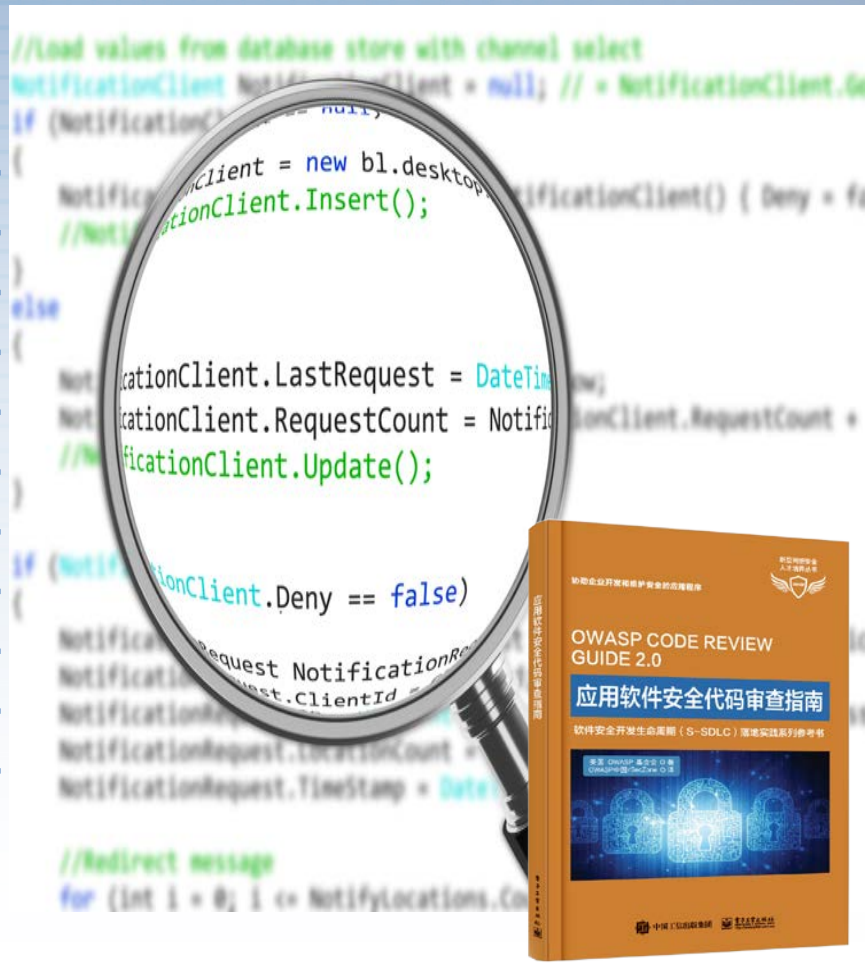
流程：Application Threat Modeling



https://www.owasp.org/index.php/Application_Threat_Modeling

流程：OWASP Code Review

- Secure code review methodology
- Technical reference for secure code review
- HTML5
- Same origin policy
- Reviewing logging code
- Error handling
- Buffer overruns
- Client side JavaScript
- Code review do's and don'ts
- Code review checklist
- Code crawling



https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

OWASP
Open Web Application Security Project

流程： OWASP Testing Guide

- Principles and techniques of testing
- Phases of a test
- Configuration and deployment
- Identity management testing
- Authentication testing
- Authorization testing
- Session management testing
- Input validation testing
- Testing for error handling
- Testing for weak crypto
- Business logic testing
- Client side testing
- Reporting

https://www.owasp.org/index.php/OWASP_Testing_Project

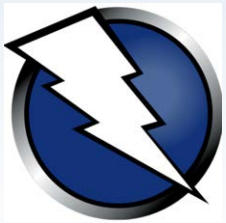
OWASP
Open Web Application Security Project

工具

DEPENDENCY-CHECK

Code Pulse

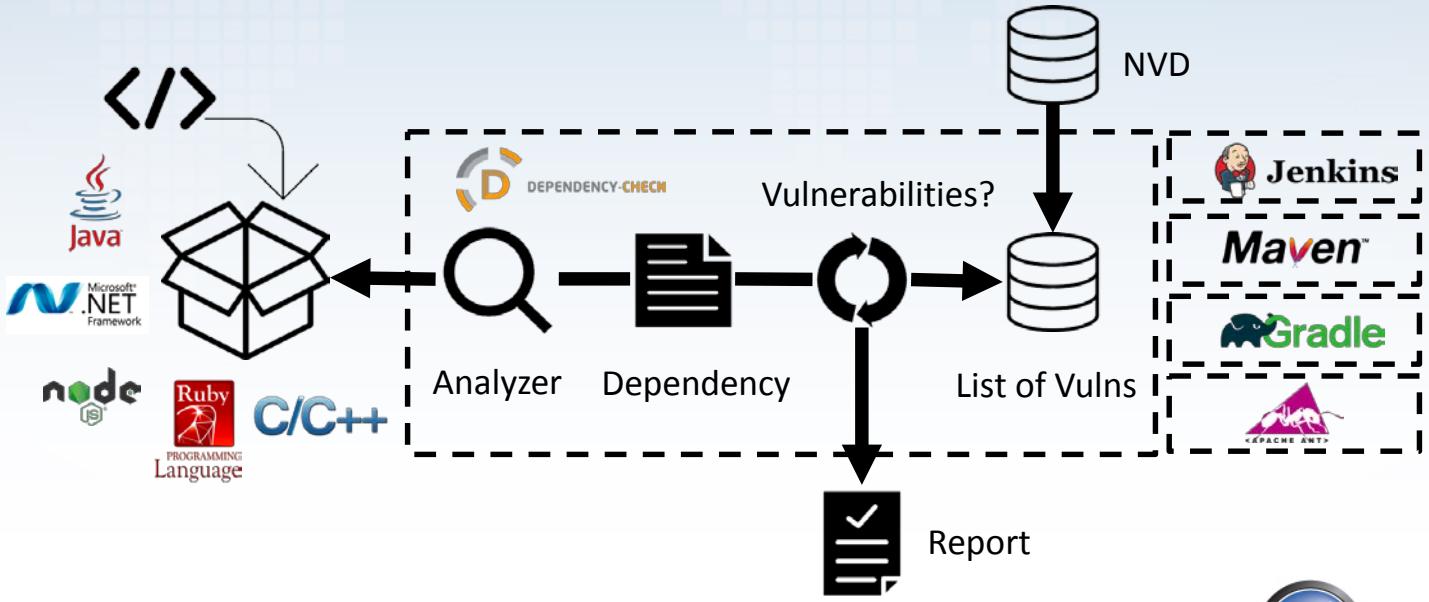
DEPENDENCY-TRACK



OWASP
Open Web Application
Security Project

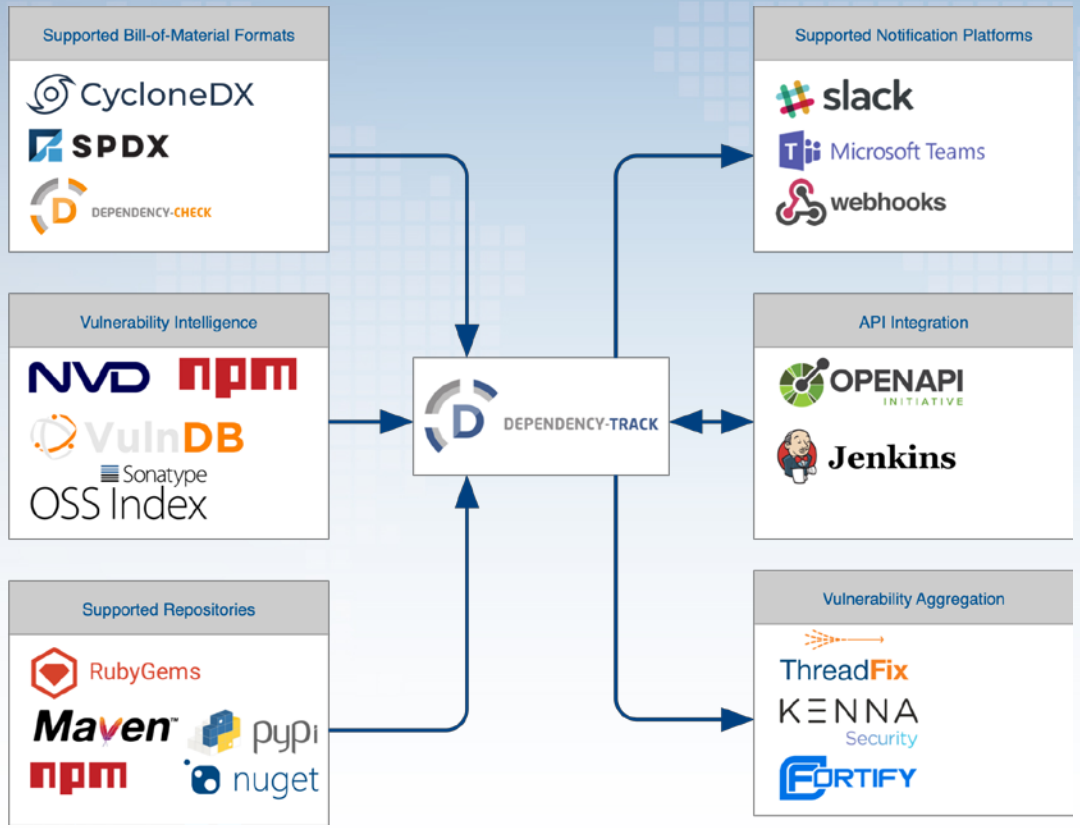
工具：第三方软件漏洞检测工具

- 识别软件研发项目中第三方软件的已知漏洞；
- 目前支持Java和.Net；
- 可作为OWASP Top 10 2017中“**A9:2017-使用含有已知漏洞的组件**”的解决方案。



https://www.owasp.org/index.php/OWASP_Dependency_Check

工具：第三方软件漏洞跟踪工具



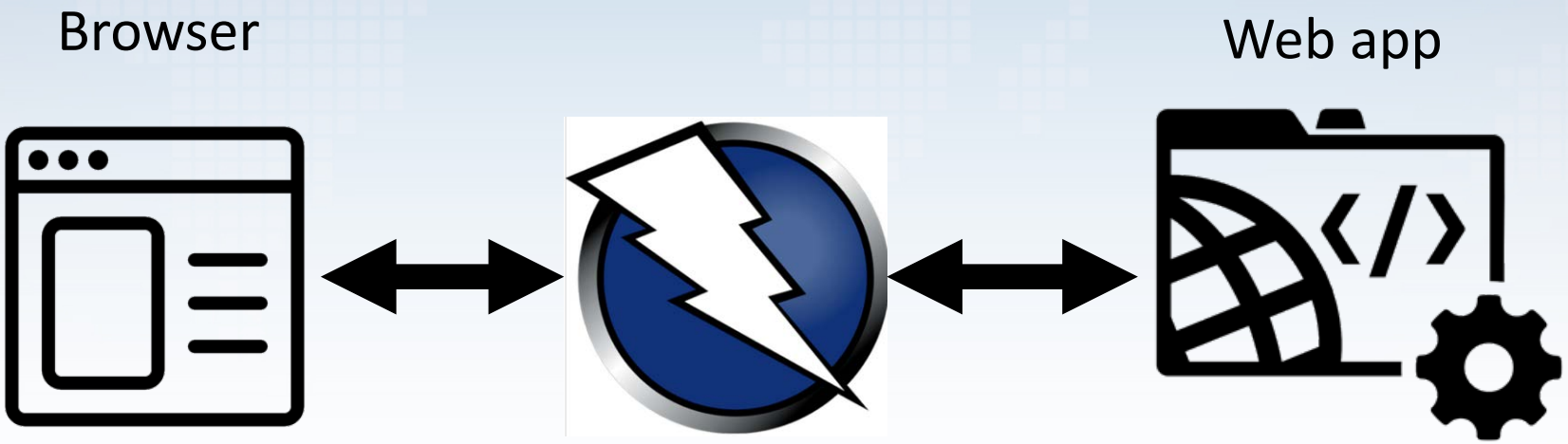
DEPENDENCY-TRACK

- 持续跟踪软件研发项目中第三方软件的漏洞更新情况；
- 集成了多个漏洞数据库，包括：NVD、NPM公众公告、Sonatype的OSS指数等。

OWASP
Open Web Application Security Project

工具：安全测试工具

- 全球最流行的免费DAST安全工具；
- 可用于渗透测试和手动安全测试。



https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

加入我们！

- 您是否想在AppSec应用安全领域有所成就或崭露头角呢？
- 您是否愿意为应用安全领域的发展贡献一点力量呢？
- 您是否有兴趣在参与、领导一个OWASP中国的研究项目呢？
- 您所在单位是否想成为OWASP中国的企业级会员单位？
- 您所在单位是否想成为OWASP中国的学术支持单位？

OWASP
Open Web Application Security Project

谢 谢

OWASP
Open Web Application Security Project