CWASP

自动化安全开发与测试

徐瑞祝

ShenZhen 2016

SECZONE 互联网安全研究中心

SECZONE 互联网安全研究中心

1 源码审核方案介绍

2 IAST安全解决方案介绍

SECZONE
互联网安全研究中心

01 Part One

源码审核方案介绍

SECZONE 互联网安全研究中心

安全代码审核解决方案全貌

咨询、分析与规划

S-SDLC咨询

扫描工具咨询

漏洞基线咨询

扫描流程规范咨询

实现与定制化

L3使用与修复培训

工具使用培训

漏洞修复培训

L2安全代码审查规范

漏洞基线

规则自定义

流程优化

L1安全编码规范

交付与维护

技术支持

策略与规范文档

SECZONE 互联网安全研究中心

解决企业应用安全核心难题

缺乏安全管理体系

缺乏安全开发标准

安全工具效率过低

投入安全的人力与时间不足

安全设计需求的检查

- 输入验证
- 身份认证
- 授权
- 配置管理
- 敏感数据
- 会话管理
- 加密
- 参数操纵
- 例外管理
- 日志和审计

安全编码规范

- 开发阶段为引入漏洞最关键的阶段，超过50%的安全漏洞由错误的编码产生。究其原因是因为开发人员对所使用的语言与技术的安全特性不了解，写出的代码符合功能上的需求，但缺乏安全上的考虑。互联网安全研究中心基于OWASP国际开源WEB安全研究组织，联合国内外专家编写了各种主流语言的标准安全编码规范。根据不同的需求，能够为客户定制符合企业自身技术标准的安全编码规范。

代码审核规范

- 代码审核机制是确保编码质量的关键机制。由于工作量的缘故，采用静态扫描工具代替人工是当前的趋势。但静态扫描工具并非是全自动化的工具，如果企业没有相应的安全漏洞基线、扫描流程规范与安全负责人，那么工具并不能带来很大的作用，反而有可能带来额外的工作量。

漏洞基线

- 定义漏洞基线可以对应到标准S-SDLC威胁建模中定义威胁的部分。通过把项目可能有的威胁对应到漏洞扫描基线中，可以通过工具快速的检测项目应对威胁的安全措施有无实现。精确扫描基线的建立可以大量减少后期排查漏洞时间。

基线1

内存溢出

……

……

基线2

.跨站脚本攻击

……

……

基线3

隐私违背

……

……

基线4

OWASP TOP 10

……

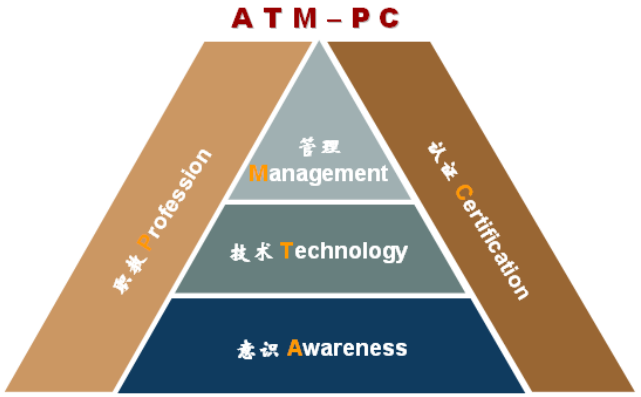
……

扫描流程规范

- 各部门之间的协作不畅往往是企业无法真正用好静态漏洞审核工具的原因之一。互联网安全研究中心通过汲取国内外成功案例的经验，具备能力为客户制定高效、合理的扫描流程规范。

SECZONE 互联网安全研究中心

培训内容



意识 Awareness
- 面向组织所有员工
- 提升组织普遍的安全意识和自我约束力

技术 Technology
- 面向对安全技能要求较高的人员
- 掌握必要的安全技术和操作技能

管理 Management
- 面向IT及信息安全管理人员
- 掌握风险管理分析决策和引导实施能力

职教 Profession
- 面向寻求信息安全职业发展的人员
- 具备理论基础和全面的素质技能

认证 Certification
- 面向对个人专业资质有诉求的人员
- 用国家最权威标准检验个人专业素质

意识 Awareness
- 安全意识培训
- 信息安全等级保护基础
- 信息安全法律和政策
- 信息安全标准介绍
- 信息安全等级保护定级指南
- 信息安全等级保护过程指南
- 信息安全等级保护建设规范

技术 Technology
- 物理安全测评
- 网络安全测评
- 数据库安全培训
- 主机安全测评
- 应用安全测评
- 渗透测评技术

管理 Management
- S-SDLC暨威胁建模
- 安全架构设计
- 灾难恢复计划
- 信息安全保障基本实践
- 信息安全管理体系
- 信息安全风险管理
- 重要安全管理过程
- 信息安全工程原理

职教 Profession
- 信息安全工程原理
- UNIX安全管理
- Windows系统安全
- 安全攻防
- 防火墙安全技术
- 网络与通信安全
- 密码技术基础

认证 Certification
- 国内认证
  - CISP
  - CISD、CISM
- 国际认证
  - CISSP
  - CISA
  - CSSLP
  - CISM
  - COBIT、ISO27001、CBCP、CWASP

SECZONE 互联网安全研究中心

02 Part Two

IAST安全解决方案介绍

安全漏洞查找与防御工具

- IAST安全测试平台是目前唯一即可以介入到软件开发生命早期，又不需要额外耗费人力的安全漏洞查找与安全攻击防御工具。

SECZONE 互联网安全研究中心

让功能测试人员完成安全测试！

- 无需专业培训
- 无需额外时间
- 无需排查漏洞

静态漏洞扫描工具使用流程

安全人员发起扫描

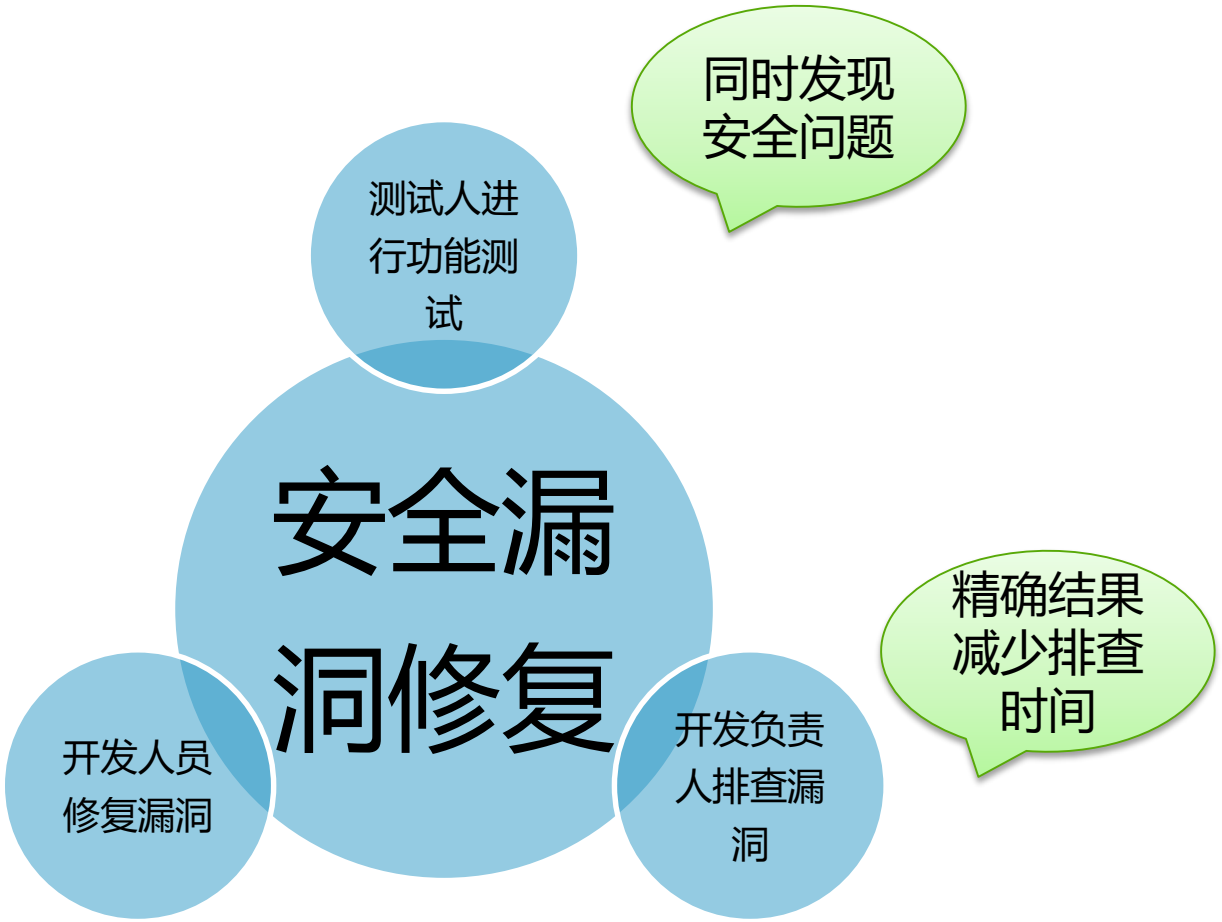
开发负责人排查漏洞

开发人员修复漏洞

测试人员进行功能测试

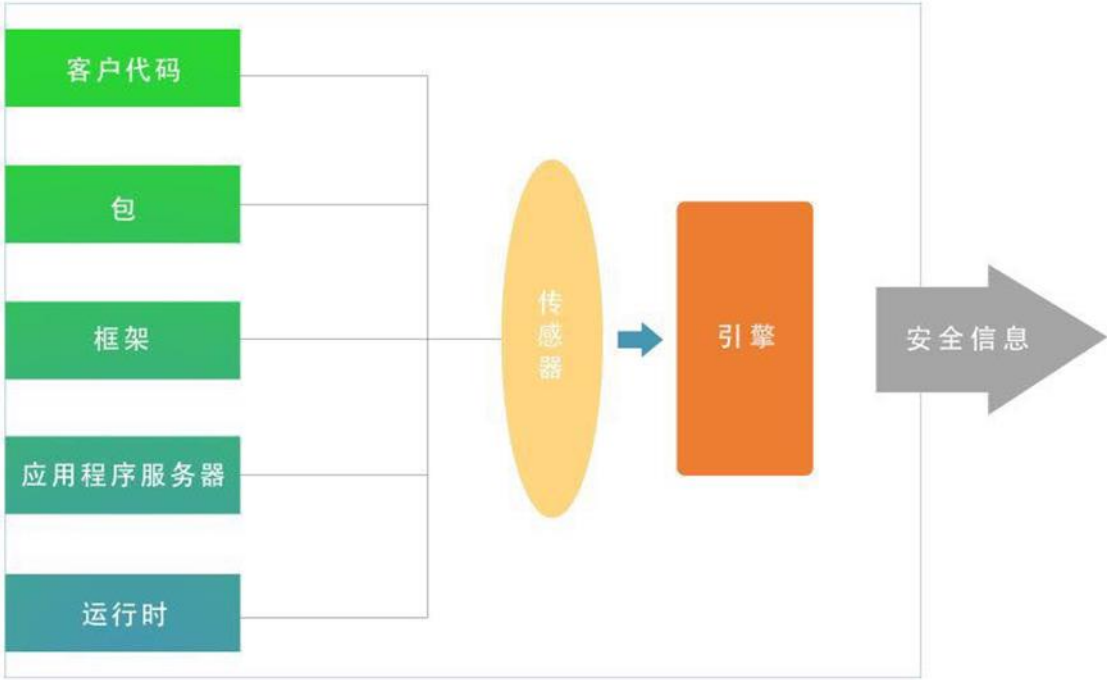
安全人员重复扫描

IAST使用过程


同时发现安全问题
测试人进行功能测试
安全漏洞修复
精确结果减少排查时间
开发人员修复漏洞
开发负责人排查漏洞

技术原理

- IAST安全测试平台内核核心技术是交互式应用程序安全测试技术。交互式应用程序安全测试技术在应用程序内部执行，当程序运行时，能够持续地监视与查找漏洞。面向方面的编程技术使得安全测试平台可以在程序运行时嵌入安全分析。分析内容包括提取上下文内容、数据流、和控制流，访问程序运行时传递的值。通过这些有价值的信息，安全测试平台可以达到其它工具所不能企及的精确度。



工具组件

Server

- 向开发人员或安全运维人员提供可视化的界面，显示实时的安全信息；
- 获取来自Agent传输过来的数据，并进行智能化漏洞分析及显示；
- 采用保护规则阻止所有的攻击，诸如Sql注入、XSS，防止0day溢出；
- 提供漏洞的解决方案；
- 检测攻击并提供防护；
- 对共享库和第三方组件进行安全性检查；
- 导出漏洞报告。

Agent

- 代理所有用户浏览器到应用程序之间的流量，并传输到Server；
- 获取服务器后端源代码，并传输到Server；
- 获取来自Server端发送的指令，并进行执行。

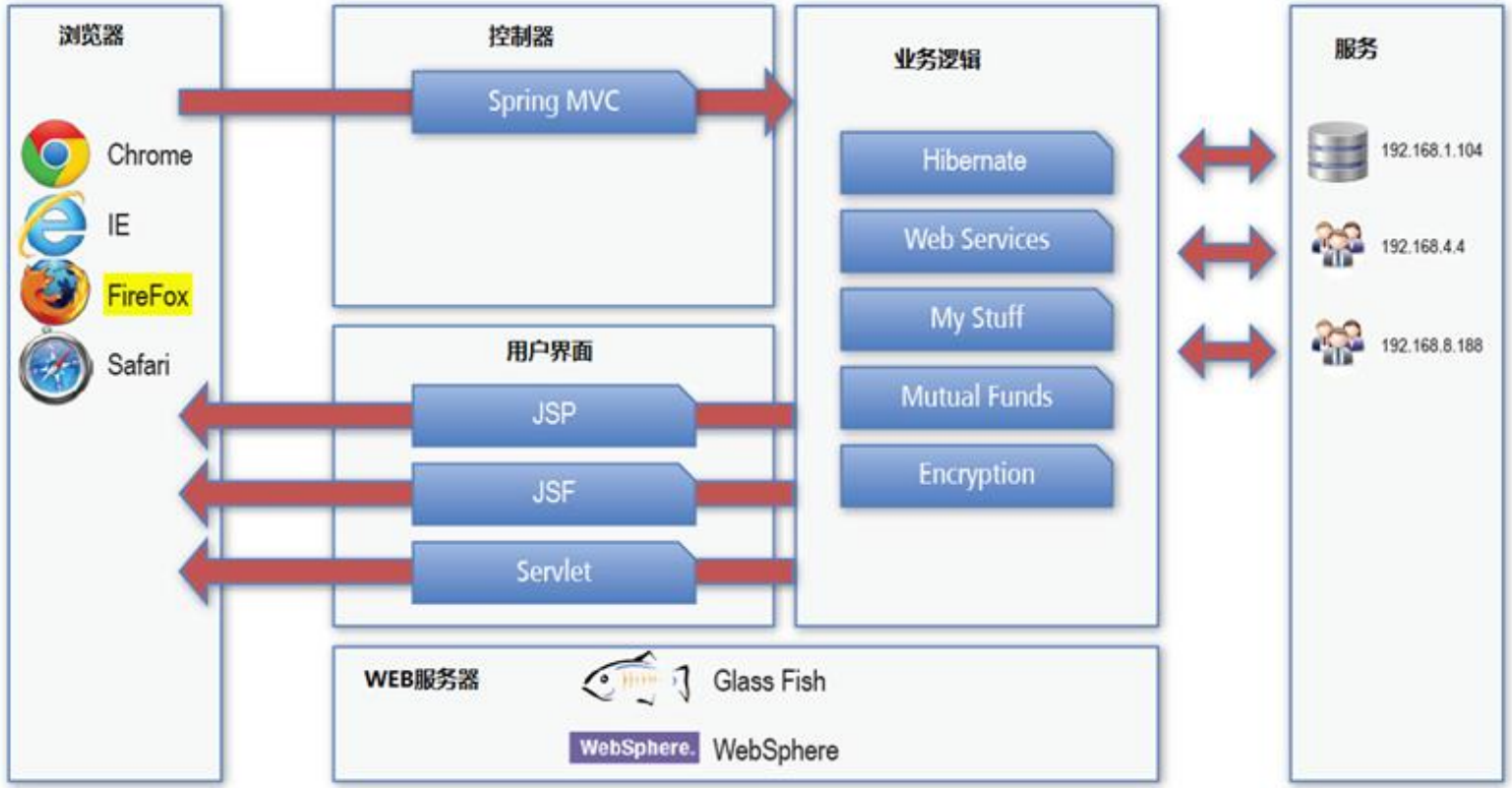
功能特点

- **企业级多应用处理能力**
  - 对于企业来说，获取单个应用程序的安全结果并不足够。要帮助用户实现安全目标，必须要考虑整个应用程序组合。安全测试平台可以实现同时对成百上千上项目进行实时分析。安全测试平台技术有点类似于New Relic或Google Analytics。
- **兼容敏捷型与瀑布型软件开发生合周期**
  - 安全测试平台采用的技术并不会破坏原始的软件开发生命周期。开发人员能够持续得到在他们开发环境中当前测试代码的反馈结果。测试人员能够在他们进行功能测试时找到安全Bug，而不需要有应用安全的相关经验。安全专家无需浪费时间去查找安全漏洞、排查误报。
- **第三方代码分析**
  - 现代的应用程序基本上80%的代码均像冰山一样埋于水下，如框架和其它组件。应用程序通常会有50个以上这样的包，组成上百万行代码。如果仅仅对自开发代码进行分析，往往会漏掉至关重要的安全漏洞。安全测试平台提供对第三方代码分析的能力。

功能特点

架构分析

- 识别应用程序的架构对于执行安全分析时非常有用。安全测试平台可以在程序运行时收集关于应用程序架构与相关组件的信息，并提供一个简易的架构图表。这些信息能够帮助开发人员快速理解检测漏洞。

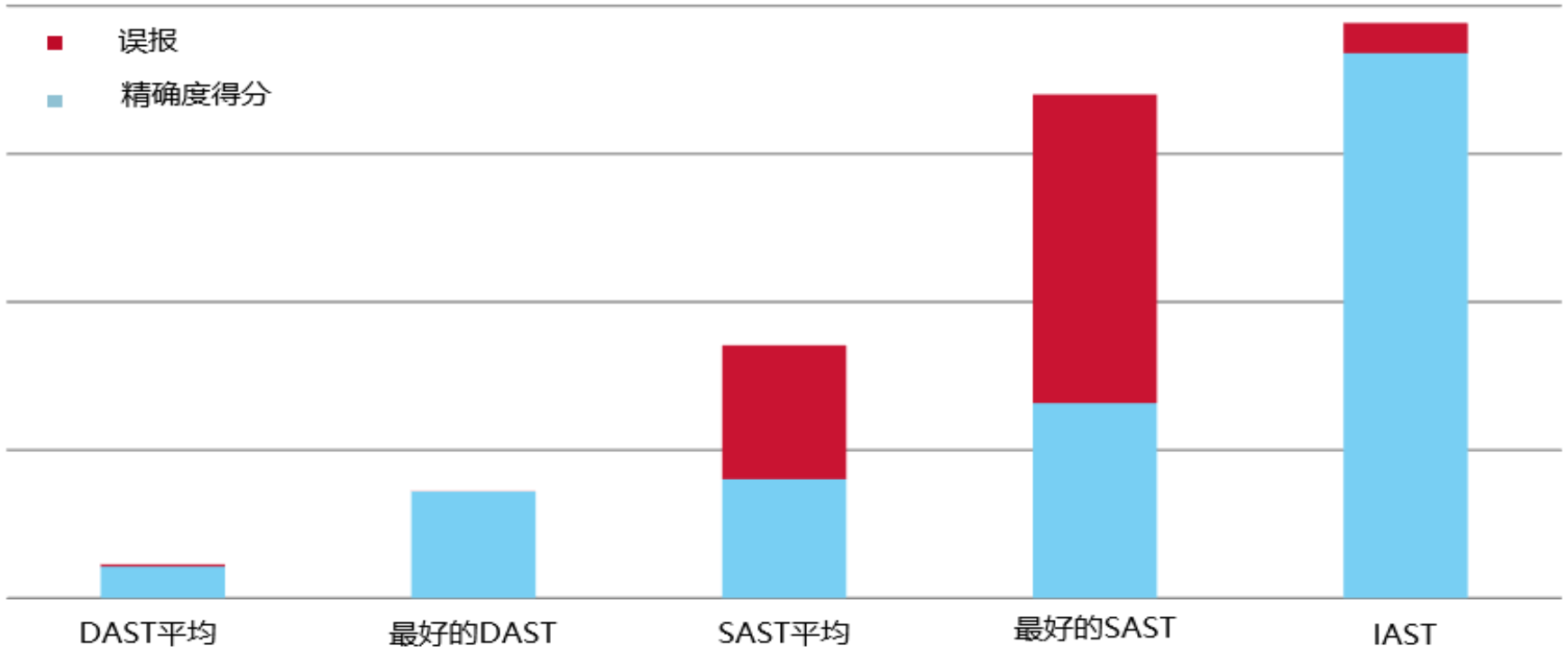


IAST安全测试平台VS御工静态源代码扫描工具

- **IAST安全测试平台**
  - 精确度
    - 工具在与运行时跟踪变量的传统过程
    - 审查框架与第三方库的安全性
    - 扫描结果精确度极高
  - 易用性
    - 漏洞扫描过程在功能测试的时候自动完成，不需要额外抽时间去做。
  - 速度
    - 实时监测漏洞，无需等待。
    - 可以同时对上千上项目进行监控。

- **静态源代码扫描工具**
  - 精确度
    - 无法看到第三方库与框架的代码
    - 扫描结果包含大量误报
    - 依赖安全专家排查漏洞
  - 易用性
    - 需要创建扫描基线
    - 需要创建扫描项目
    - 需要排查结果
  - 速度
    - 对于比较大的项目，单次扫描就需要等待几个小时、甚至几天。
    - 极度耗费硬件资源。

精确度比较



谢谢聆听

THANK YOU FOR YOUR ATTENTION

18611267718
xrz@seczone.org
http://www.seczone.org