CWASP

IAST交互式应用安全测试技术

徐瑞祝

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

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。

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

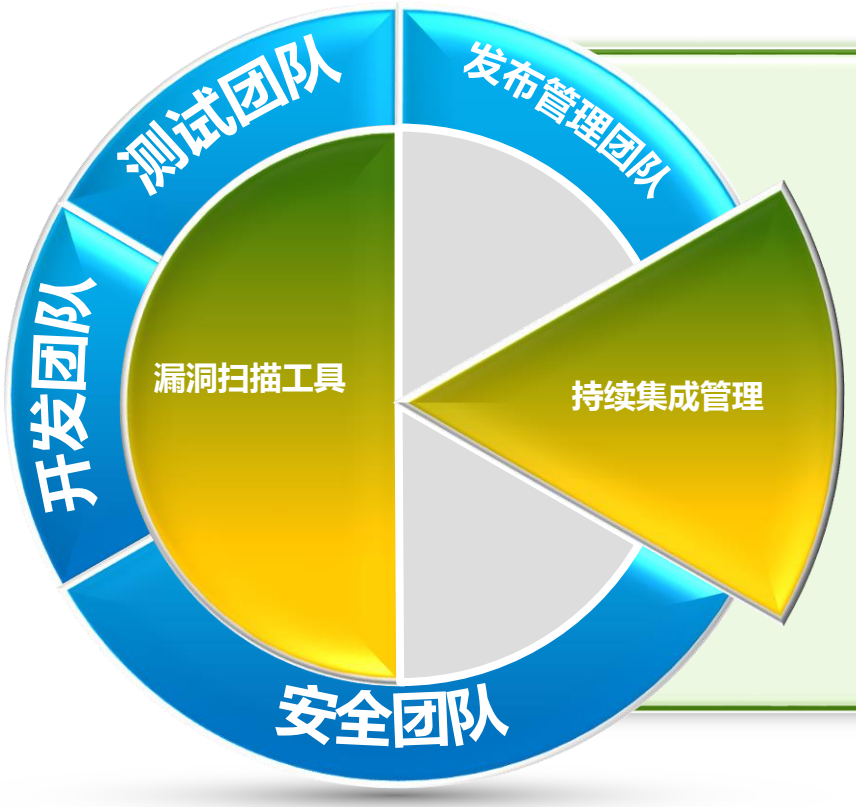
- 定义漏洞基线可以对应到标准S-SDLC威胁建模中定义威胁的部分。通过把项目可能有的威胁对应到漏洞扫描基线中，可以通过工具快速的检测项目应对威胁的安全措施有无实现。精确扫描基线的建立可以大量减少后期排查漏洞时间。

基线1	基线2
内存溢出 …… ……	.跨站脚本攻击 …… ……

基线3	基线4
隐私违背 …… ……	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。



◆如何嵌入现有项目发布流程？

◆扫描任务由谁创建？

◆漏洞缺陷由谁分发？

◆扫描漏洞由谁确认？

◆测试结果如果跟踪？

◆企业项目整体安全性如何管理？

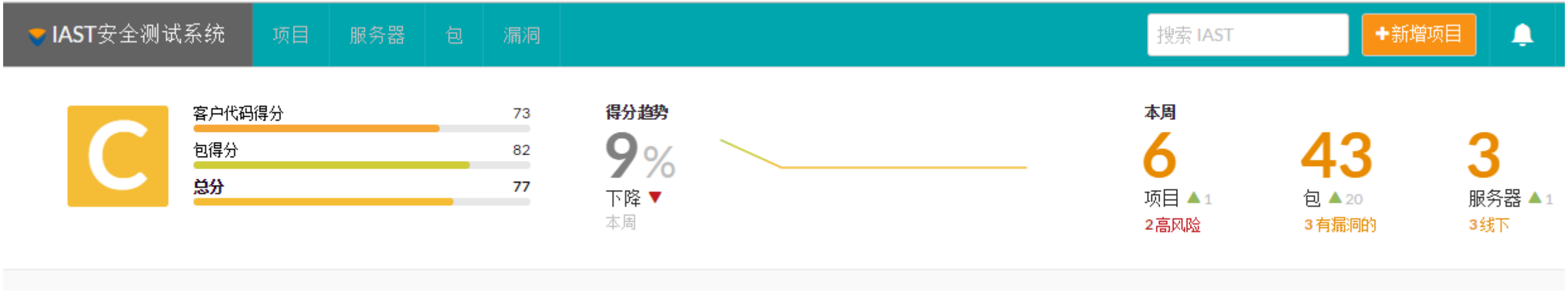
SECZONE 互联网安全研究中心

02 Part Two

IAST安全解决方案介绍

SECZONE 互联网安全研究中心

IAST安全测试系统

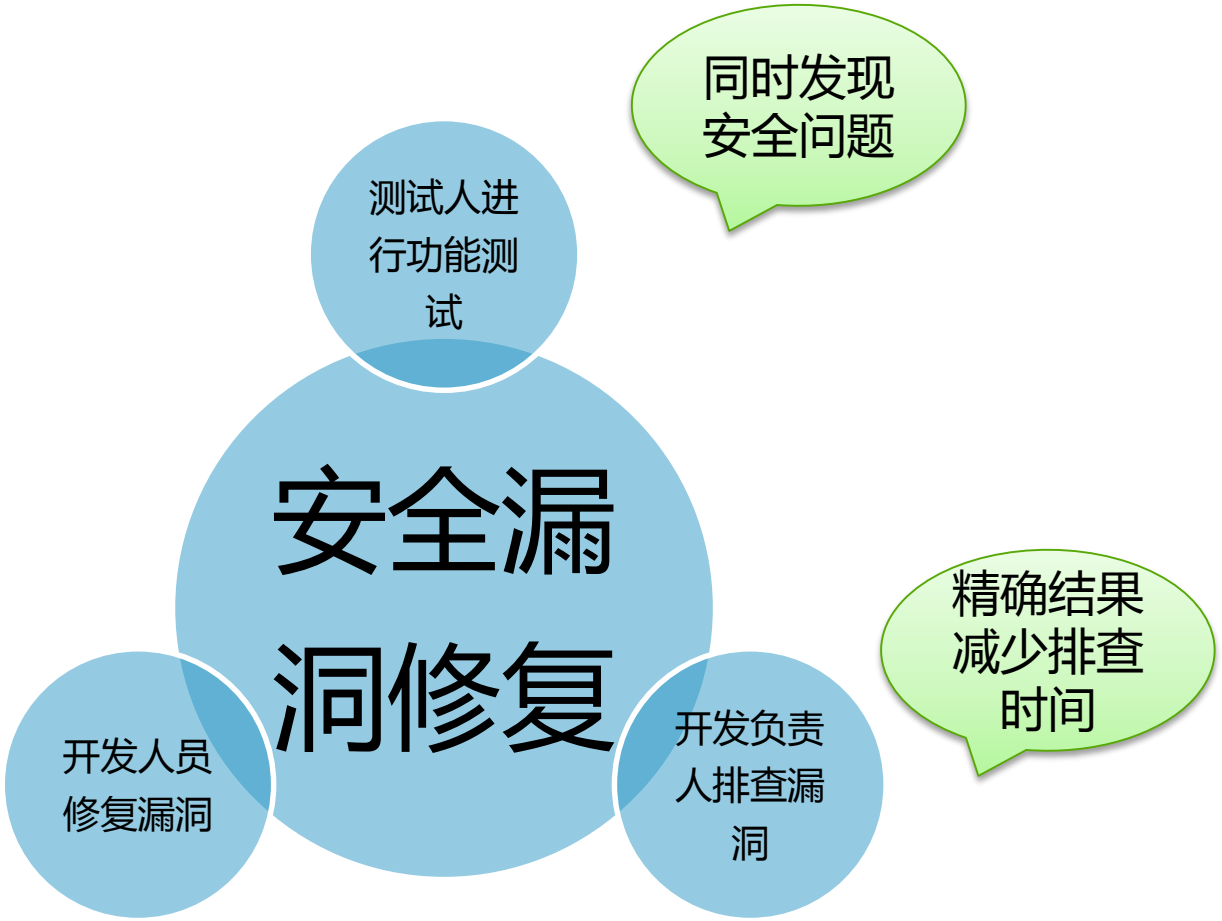


SECZONE 互联网安全研究中心

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

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

当今应用程序安全瓶颈

应用程序组合

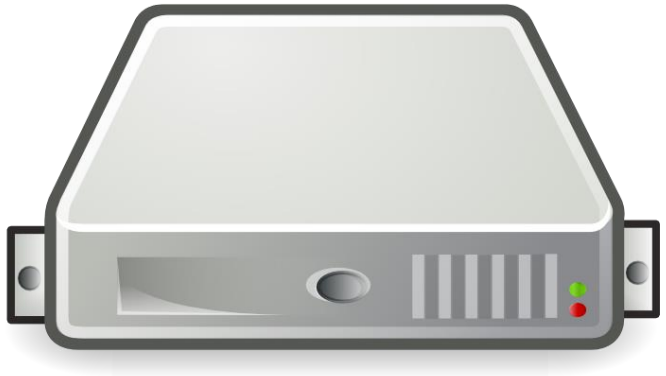
- 依赖人工
- 不准确
- 破坏性
- 滞后性

开发阶段 → 测试阶段 → 产品使用阶段

SAST (代码分析)　DAST (渗透测试)　WAF　IPS

SECZONE 互联网安全研究中心

源码审核工具效率瓶颈

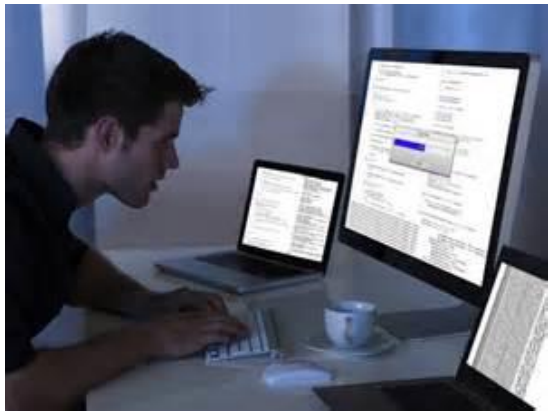


源代码审核服务器

- 项目1开始扫描
- 项目2开始扫描
- 项目3排队
- 项目4排队

项目1　项目2　项目3　项目4　项目5　项目6　项目7　……　项目100

零人工干预全自动化安全测试



开发人员

1 编写一个功能的代码

2 测试自己写的代码

测试人员

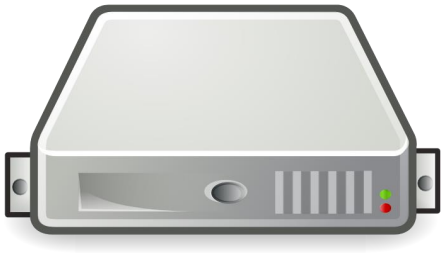
1 测试开发人员提交代码相关的功能

2 集成测试

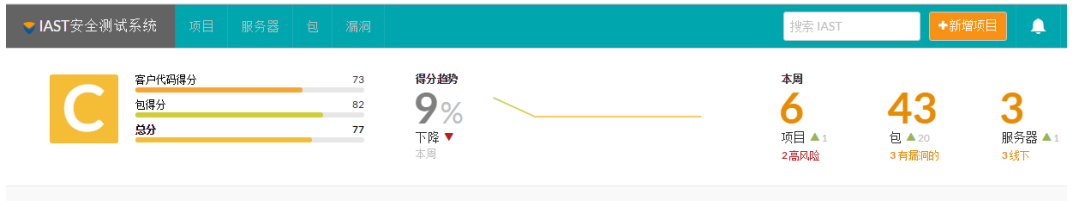
IAST自动实现安全测试

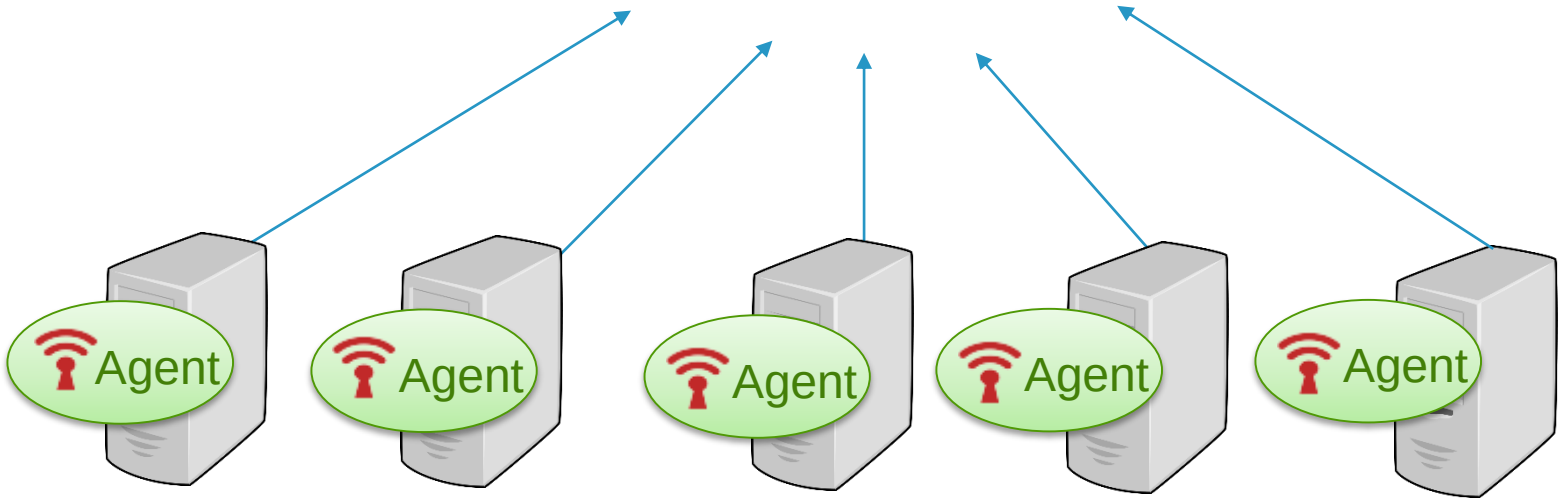
外包项目管理

- 实时监控项目安全质量
- 多项目同时管理
- 发现第三外组件安全问题



IAST服务器端

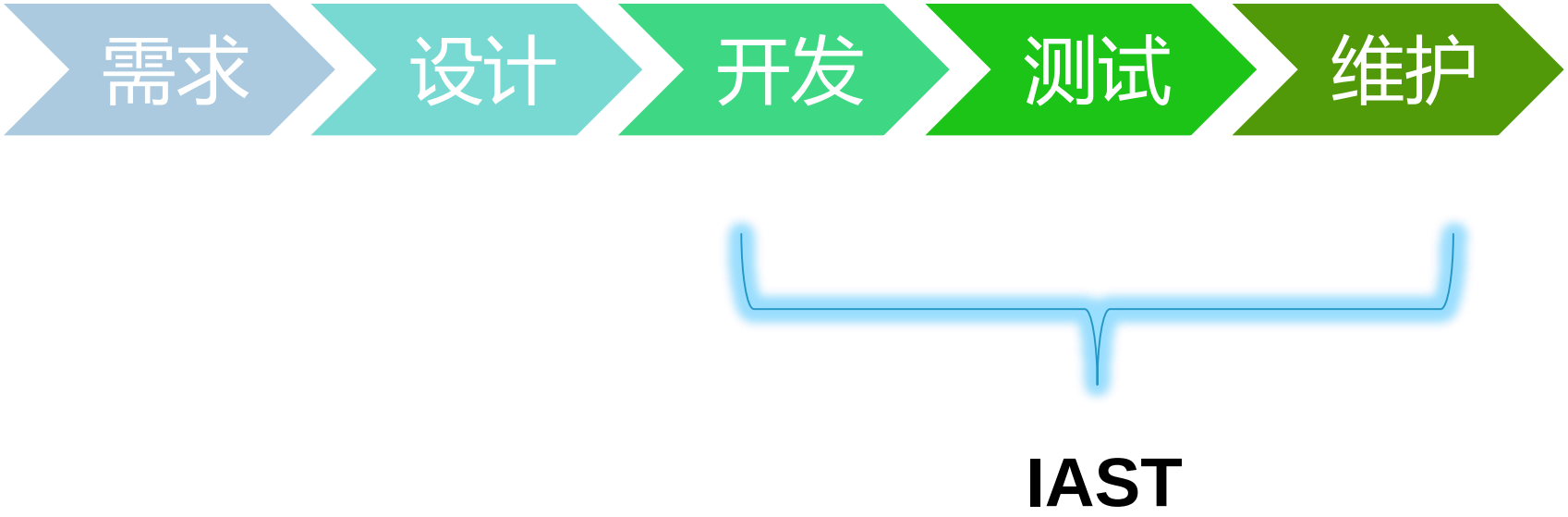




外包项目1　外包项目2　外包项目3　外包项目4　…… 外包项目100

嵌入安全软件开发生命周期

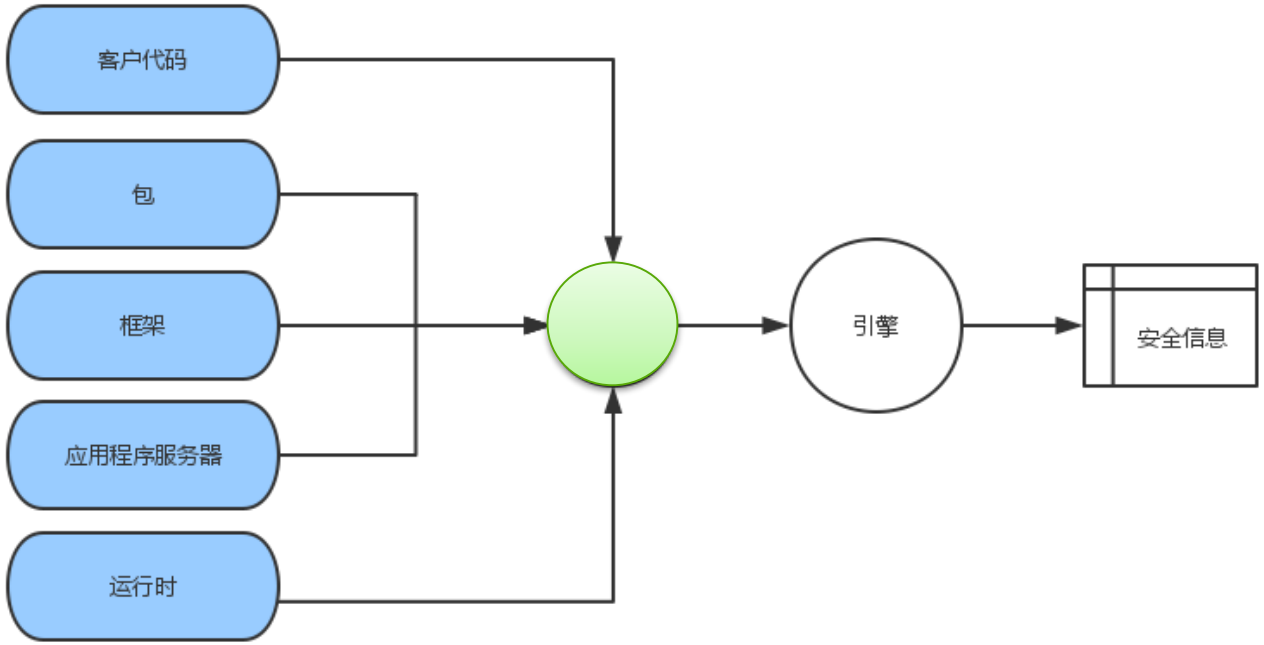
- IAST安全测试系统是目前唯一即可以介入到软件开发生命早期，又不需要额外耗费人力的安全漏洞查找与安全攻击防御工具。



技术原理

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。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。



SECZONE 互联网安全研究中心

应用程序安全插桩转换对比

SAST

代码

DAST

HTTP 流量

WAF

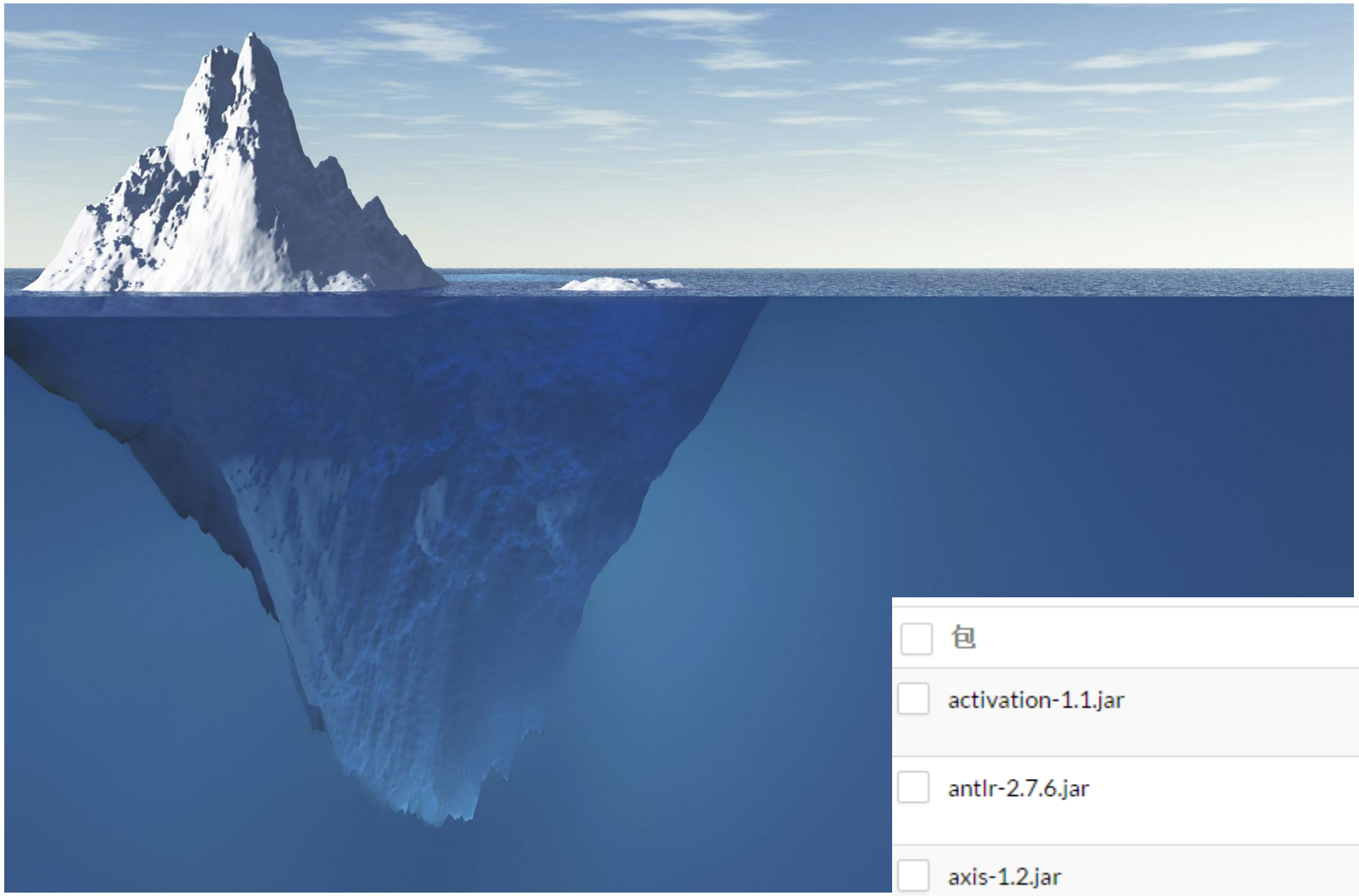
HTTP 流量

深度安全插桩

代码	包	数据流运行时间	软件结构
HTTP流量	架构	控制流量运行时间	服务器配置
Backend 连接	配置数据	平台运行时间	其他…

SECZONE 互联网安全研究中心

主要功能特点：第三方代码的检测



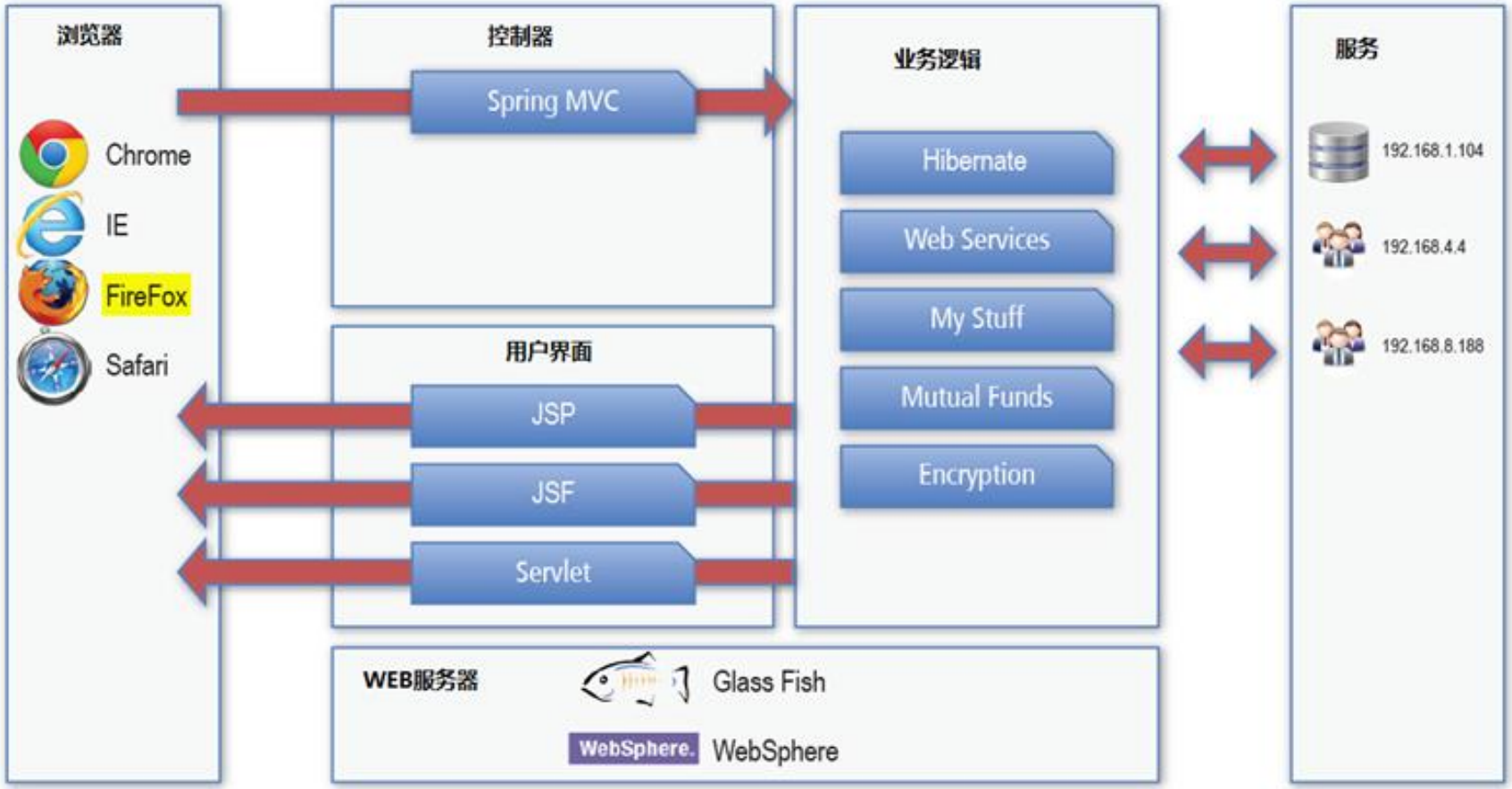
- 第三方代码的跟踪

```
string[] = facade.getParameterValues("File")
    在 getRawParameter() @ ParameterParser.java:615

sb = sb.append("CsrfTokenByPass.html")
    在 handleRequest() @ AbstractLesson.java:771

str = sb.toString()
    在 handleRequest() @ AbstractLesson.java:771

matcher = pattern.matcher("D:\apache-tomcat-7.0.40\w...lish\CsrfTokenByPass.html")
    在 createContent() @ PathBasedAccessControl.java:129
```

- 第三方代码库CVE漏洞
- 的检测。

包	等级	使用的项目	CVE
activation-1.1.jar	D	WebGoat	0
antlr-2.7.6.jar	A	SecurityAttackDemo	0
axis-1.2.jar	F	WebGoat	2

功能特点：架构分析


浏览器
Chrome
IE
FireFox
Safari
控制器
Spring MVC
用户界面
JSP
JSF
Servlet
业务逻辑
Hibernate
Web Services
My Stuff
Mutual Funds
Encryption
服务
192.168.1.104
192.168.4.4
192.168.8.188
WEB服务器
Glass Fish
WebSphere.
WebSphere

SECZONE 互联网安全研究中心

同类产品比较

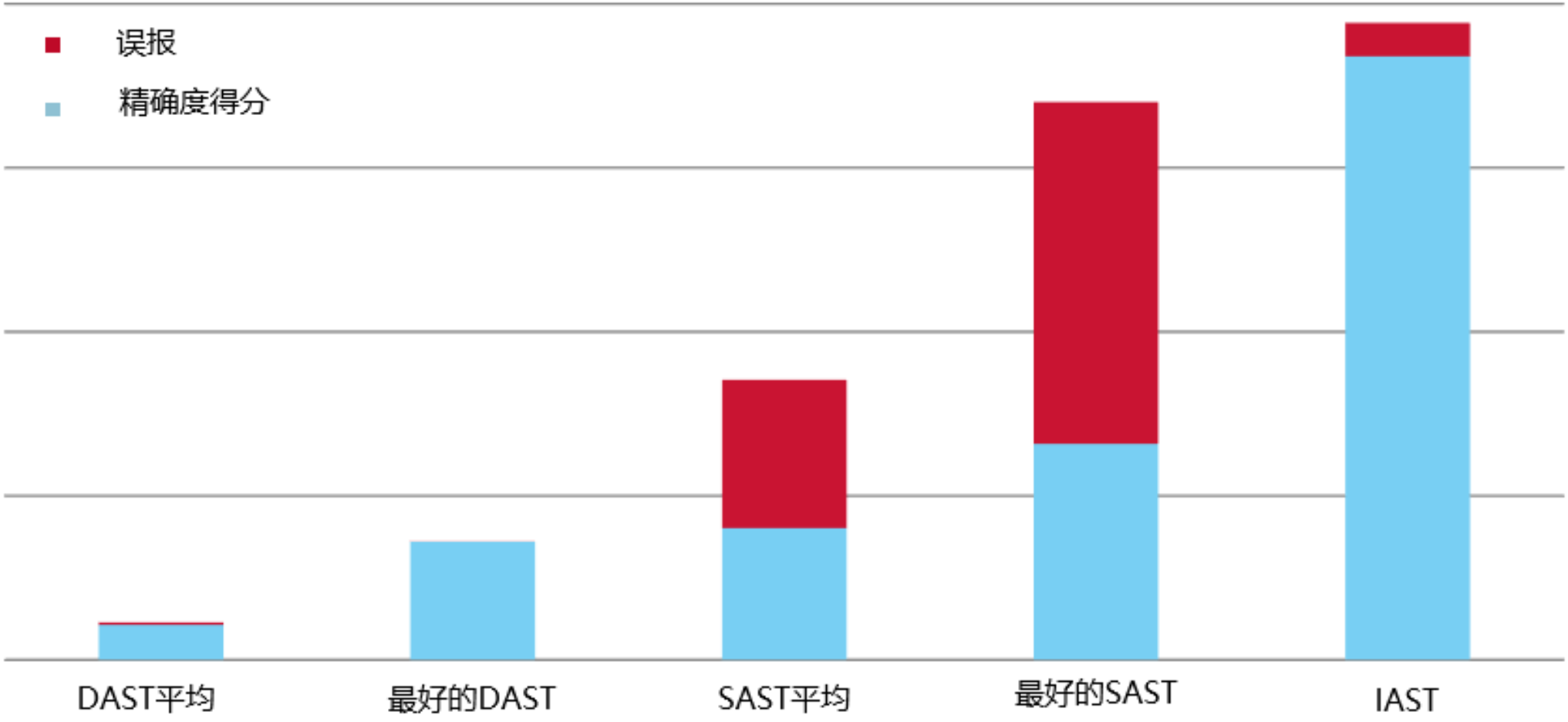
• IAST安全测试平台

- 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。

Owasp 项目测试结果比较



谢谢聆听

THANK YOU FOR YOUR ATTENTION

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