白皮书

beSOURCE 静态源代码扫描工具

企业级白盒源代码安全审计工具

为什么我们需要一款代码审计系统？

公司越来越大，开发人员也越来越多。每个研发人员的安全素质都不一样，虽然在公司核心项目上可以采取框架层安全防护，但各类新项目太多，无法做到每个项目都使用相同框架，都去集成安全组件。所以对于公司所有的项目都必须有一道防护来保障其基本安全，代码安全审计即可作为这一道安全防护手段。

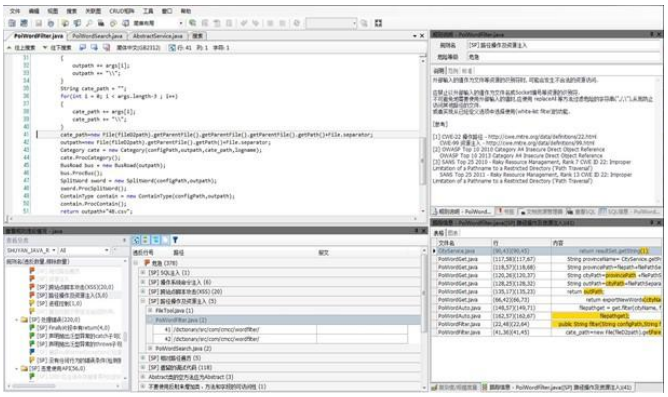
企业的白盒安全需求：

- 能够扫描多种开发语言（复杂的大型程序不止一种开发语言，这就涉及到需要支持多种语言）
- 能够自动扫描、自动报告（人工参与每个项目成本太大）
- 能够快速集成到软件开发生命流程中（项目频繁的迭代，自动化执行安全测试势在必行）
- 能够满足多种安全合规性报告（CWE/SANS，OWASP，CERT Secure Coding 等等）

产品概览

检测脆弱的源代码	使用语义分析算法，检测可能导致安全事故的源代码	SQL注入，命令注入，跨站脚本，缓冲区溢出等
灵活的规则管理	允许使用规则说明语言创建新的规则或修改现有的规则	中央化规则管理支持开发人员客户端自动更新规则
合规报告和安全编码指南	生成各类标准的国际安全合规性报告	提供代码修复编码指南，提高程序员安全编码水平
先进的分析技术	无需额外安装复杂的编译环境	采用如格式分析，流分析，类型分析，值分析等
精准的定位+增量分析	支持代码上下文联系比对，支持多次扫描结果快速对比	增量分析，自动识别并分析所有变更的代码，无需重头执行

支持编程语言及规范



支持的编程语言		
Python	PHP	JavaScript/Ajax
Objective C	HTML	JSP
Java	Android JAVA	JAVAWeb
ASP.NET	XML	PL/SQL
C#	C++	C99

支持国际标准安全编程指南:	
OWASP TOP 10	CWE/SANS TOP 25
Common Weakness Enumeration	CERT Secure Coding Guidelines

安全系统开发生命周期

1 代码上传阶段

- 使用Eclipse plugin本地扫描
- 发现并及时修复漏洞
- 保证提交前代码的安全性

2 代码变更阶段

- 触发远程代码静态扫描
- 增量扫描少量变更的代码
- 发现漏洞后利用邮件及时通知
- 责任人进行评审后修复

3 代码审计阶段

质量管理团队进行代码审计

- 质量管理人员针对新建 、变更的文件进行扫描。若存在规则违反，将Reject相应程序发布。

质量管理团队验收第三方开发代码质量

- 质量管理人员针对第三方开发的代码进行验收，查找不合规的代码，及不符合开发标准的程序。

品质部门定期质量抽查

- 品质部门定期(季度)抽取几个系统进行质量以及安全漏洞的扫描 ，对系统进行评估。

信息安全人员帮助制定与调整代码安全规则

- 安全安全小组人员定期协助开发部门调整代码安全规则，关闭产生误报的规则策略，调高严重问题的修复优先级别。

4 程序成功部署及发布

- 设置定时任务扫描来保证及时性和线上代码的覆盖率

5 产生合规性报告

报告仪表盘

诊断分析小结

— 通过多样的统计/图，迅速掌握品质现状

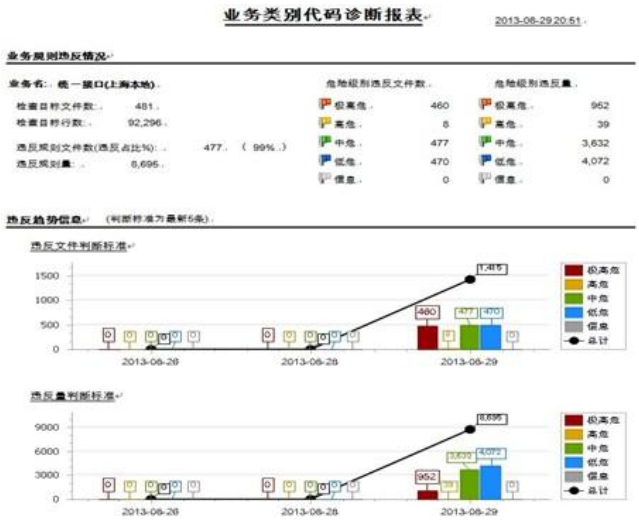
— 源代码扫描历史信息（按照扫描日期详细比较）

— 自动生成项目单位缺陷详细报表

— 支持多种格式（Excel，PDF，Word 等）

安全趋势分析

多次扫描结果对比，分析安全问题的发展势，定制安全策略



我们的客户

“使用beSOURCE安全解决方案能更快地扫描更多的应用程序，通过增量扫描的方式大大缩短了程序的上线时间，并快速的集成到整个软件开发生命周期。”— 客户评价

上海高仕达网络科技有限公司

软件安全解决方案系列产品

www.gosstal.com

Tel：021-50150593

Email：sales@gosstal.com