链滴

行业交流 - 甲方代码审计系统建设 - 汽车之家

作者：nanolikeyou

原文链接：https://ld246.com/article/1531712972376

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

同汽车之家-赵乾交流

心得：总的来说有长有短，目前的代码审计系统类似于http://www.freebuf.com/sectool/176414.html，基于现有的sonar、checkmarx的api进行封装集成为系统。而foritify的SSC+Jenkins也可以实。

主要讨论以下问题：

1. coverity对百万行规则的低误报率模式只有宣称%20,fortify对j2ee支持更好,cobra采用的内部的规没有开源，对上亿行PHP找到上万个漏洞,误报数据还不还清楚。那么做源码审计关心几个关键数字，队人员投入，代码规模、覆盖率 编译扫描成功率，另外扫描失败的原因是什么？最重要的漏报率 误率。

答：系统大概一人投入一年时间业务时间开发，每天有安全人员每天看这个系统，分析发现的漏洞再工单。扫描成功率是百分之百成功，但是结果可能不如人意，有些项目扫不到漏洞。误报的话需要不加白名单的插件或规则来不断优化，目前我们知道的误报都可以根据白名单规则和插件100%消灭的自定义规则根据项目级别由安全人员和项目组制定。

2. 提高效果就三板斧，确保正式的扫描配置，新增规则，优化删改规则。代码审计对于xxe,反序列化反射xss，重定向这些还好，越来越突出的csrf,遍历，越权，信息泄露才是src的主流。那么是否对sona进行改造，对自定义规则有何心得。

答：买的版本问题checkmarx加不了规则，src暴的漏洞需要区分，比如逻辑这种就不行，如果定位代码吃层，这个是可以总结出规律的，比如dom xss这种innerhtml。

3. 还有涉及到对语言的支持程度nodejs,c swift，复杂的前端代码也要扫描domxss。

答：js和nodejs这种只能静态扫描+上线前的安全测试了。公司的sonar通过社区实现对各自语言的支。

4. 对二进制，第三方依赖，开源通用组件这样的供应链安全如何关注？

答：类似于OWASP_Dependency_Check。已经开源了https://github.com/MyKings/clocwalk。

5. 对待缺陷和漏洞的态度。找漏洞从来不是问题，如何运营才是问题。每个高中危的代码缺陷、包括量的，都修复还是只有漏洞才提工单？切入点的类似于是Google,error pone一样的编译，review阶，还是facebook的infer上线前扫描，迭代业务代码如何覆盖？

答：敏捷这种现在也不是强制策略，比如发现漏洞只告警不阻断，编译还是会通过。提漏洞只提高危洞。业务反馈的话，当然搞安全的一般都不太让人讨喜，其实这个就要和公司SDL相关了，代码审计该是多个纬度一起的建设:SDL，代码自动化扫描，上线前的安全测试来保证安全，单独一个纬度总会疏漏的，特别是需要多个部门合作，这就需要制定一个套流程规范出来，系统应该能够回溯和跟踪漏。

6. 你认为静态分析未来的趋势是如何，白盒是否会结合有和动态分析验证，看paper几乎都是模式匹，通过字节码进行语义语法，数据流分析，是否认同有机器学习进行判断的可能性。

答：通过调用一些sdk来实现吧，目前不是主要的问题。