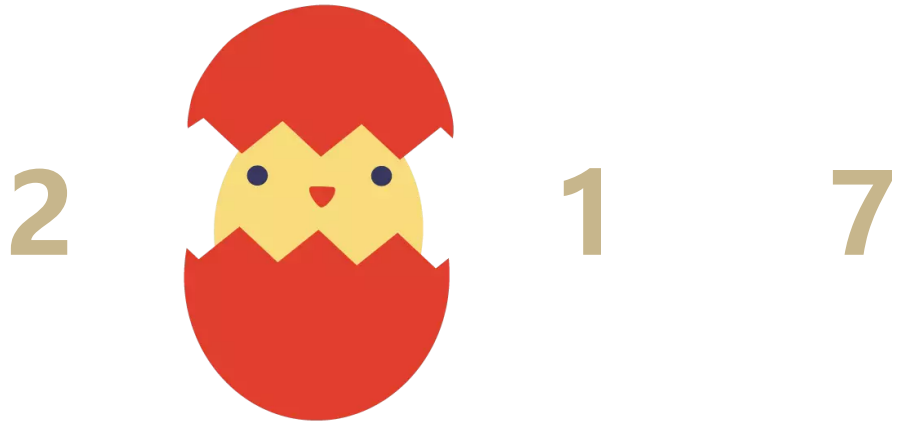
谈一谈java代码审计—安全小课堂第四十一期

京东安全应急响应中心 2017-01-06



安全小课堂第四十一期

Java因具有面向对象、平台独立与可移植性、多线程、动态性等诸多特点成为了主流的开发语言。但只要有代码的地方就有漏洞，PHP代码审计大家比较熟悉了，Java代码如何进行安全审计呢？本期邀请到孙爱萍小伙伴为大家分享Java代码审计。

关于分享者：
孙爱萍是京东高级安全工程师，有着多年的Java代码审计经验，参与京东代码安全审计平台建设。

图丨源自网络

> > > 1 < < <

豌豆妹

Java的漏洞出现的原因是什么？

小丸子

1、程序员编码不当，编码时未考虑安全性。例如，输入输出未做过滤&净化、权限控

制不完备、程序逻辑存在问题等。另外，对框架的使用不当造成的问题也不容忽视。例如，典型的使用MyBatis框架是未使用预编译模式。

2、第三方组件使用不当。例如，使用了存在漏洞的低版本组件，组件开发模式未关闭等。

豌豆妹

低版本的第三方组件能举一些例子么，还是说低版本的第三方组件都有问题？

小丸子 

典型的： Struts 2(远程命令执行)、Apache Commons Fileupload(远程DoS)、Apache Commons Collections(反序列化漏洞导致远程命令执行)。 Spring Boot(远程命令执行)。理论上只要有漏洞的都可被利用，上面提及的几个是比较容易被利用的。

> > > 2 < < <

豌豆妹

代码审计会遇到哪些问题？

小丸子 

Java代码审计中最大的一个难题就是效率问题。因为代码量大又不能完全依赖人工，而现在暂时没有发现开源的Java代码审计工具，商业的通用代码扫描器不能满足需求，而且还贵。

> > > 3 < < <

豌豆妹

Java代码审计能找出什么样的漏洞呢？

小丸子 

能找出的漏洞取决于产生漏洞的原因。Java代码审计可以发现的漏洞分为两类：
1、程序员由于编码不当产生的漏洞，典型包括后门、SQL注入、文件上传、任意文件下载、接口非授权访问、垂直越权。对于水平越权、XSS、CSRF、逻辑类漏洞也可以检测；
2、第三方组件使用不当产生的漏洞，从POM文件中可以找到使用了低版本的组件。从应用配置文件中可以找到配置不当问题。

豌豆妹

能否推荐一些Java Web代码审计的资源？

小丸子 

目前我也没有见过比较好的Java Web代码审计的资源，工具用过Fortify SCA和Checkmarx，规则都一般，因为太通用了。想要效果好需要定制化。

> > > 4 < < <

豌豆妹

Java代码审计主要关注什么样的漏洞？

小丸子

这个取决于有多少时间，如果时间足够充裕，理论上能找到的漏洞都可以通过自动化+人工的方式寻找。时间有限的情况下，重点关注以下类型漏洞：
1、SQL注入、文件上传、任意文件下载、接口非授权访问、垂直越权；
2、高危常用第三方组件漏洞，典型包括Struts 2（版本及配置问题）、Apache Commons Fileupload远程DoS问题。

豌豆妹

那如何高效率地发现尽可能多的严重漏洞呢？

小丸子

定制化的规则（但是仅对有固定模式的代码效果较好，如同一个公司、厂商的代码）。

> > > 5 < < <

豌豆妹

实现自动化的Java代码审计有哪些需要注意的点？

小丸子

目前的自动化只能是半自动化，还是需要人工的介入。

1、误报。只要扫描就肯定有误报，再怎么定制规则也一会有误报。
2、研发人员不懂安全，为了漏洞的修复效率，安全人员对审计结果进行筛查，最终提供准确的漏洞及修复方案给研发人员。

白帽子观点

1

关于工具我来说一点，如果有一个项目，让我们用一个星期做深入分析，这时其实用什么工具不重要，用notepad++当然也可以，但是大公司每天几百个业务上线请求，这时效率就变得非常重要，如何用最高的效率，把严重漏洞尽量多的发现，这才是最重要的。

2

关于如何高效率地发现尽可能多的严重漏洞，主要从三方面入手：
1、高效的引擎；
2、高效的规则；
3、高效的流程（比如如何切入公司的上线流程，代码库和研发人员是否直接可以对应。如不能，发现了漏洞，联系修复的流程就会效率很低），在业务量大的情况下，根据以往经验，流程往往比技术更重要。

3

扫描代码的工具常见的基于规则和静态语法树。

微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心