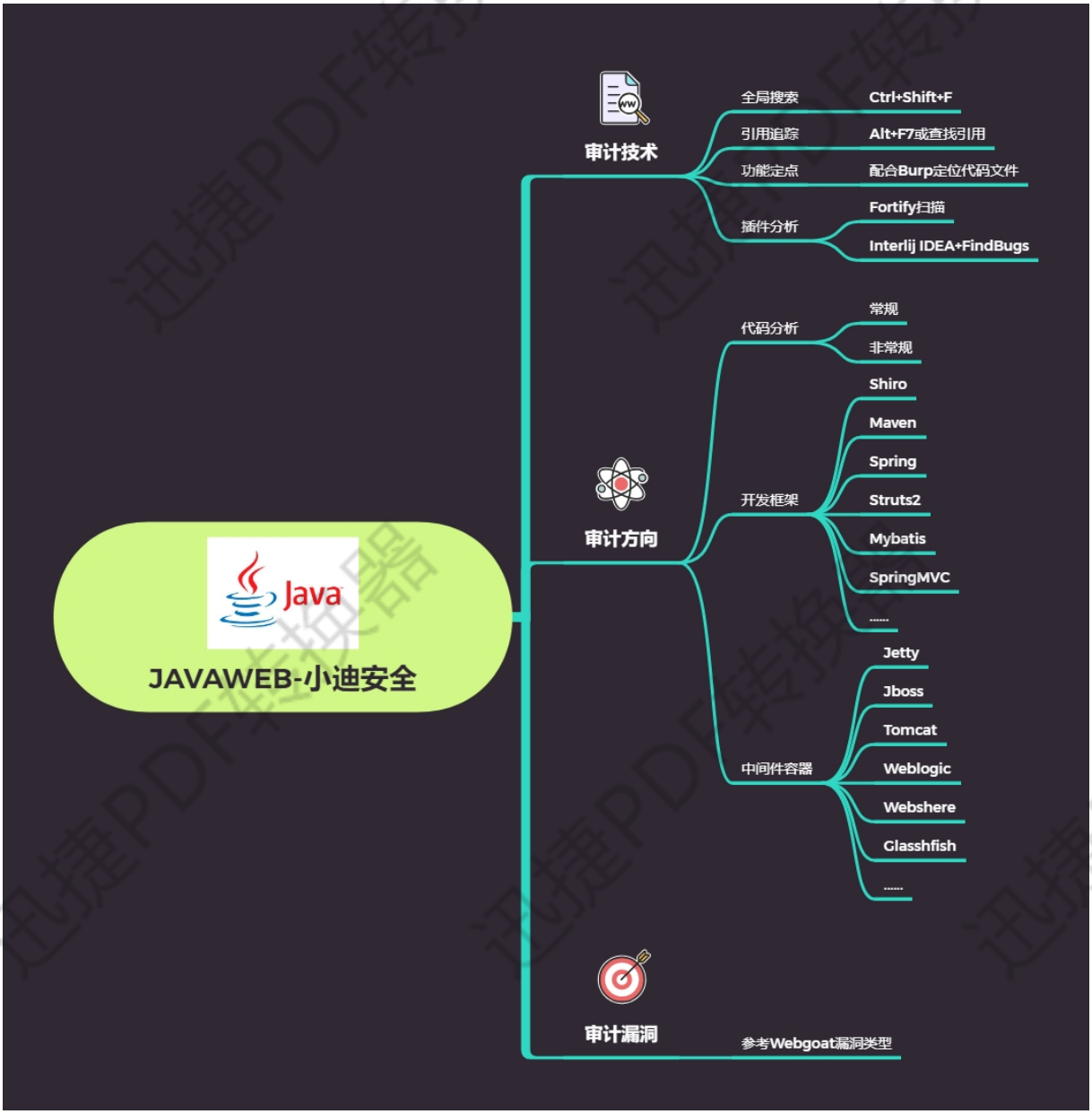
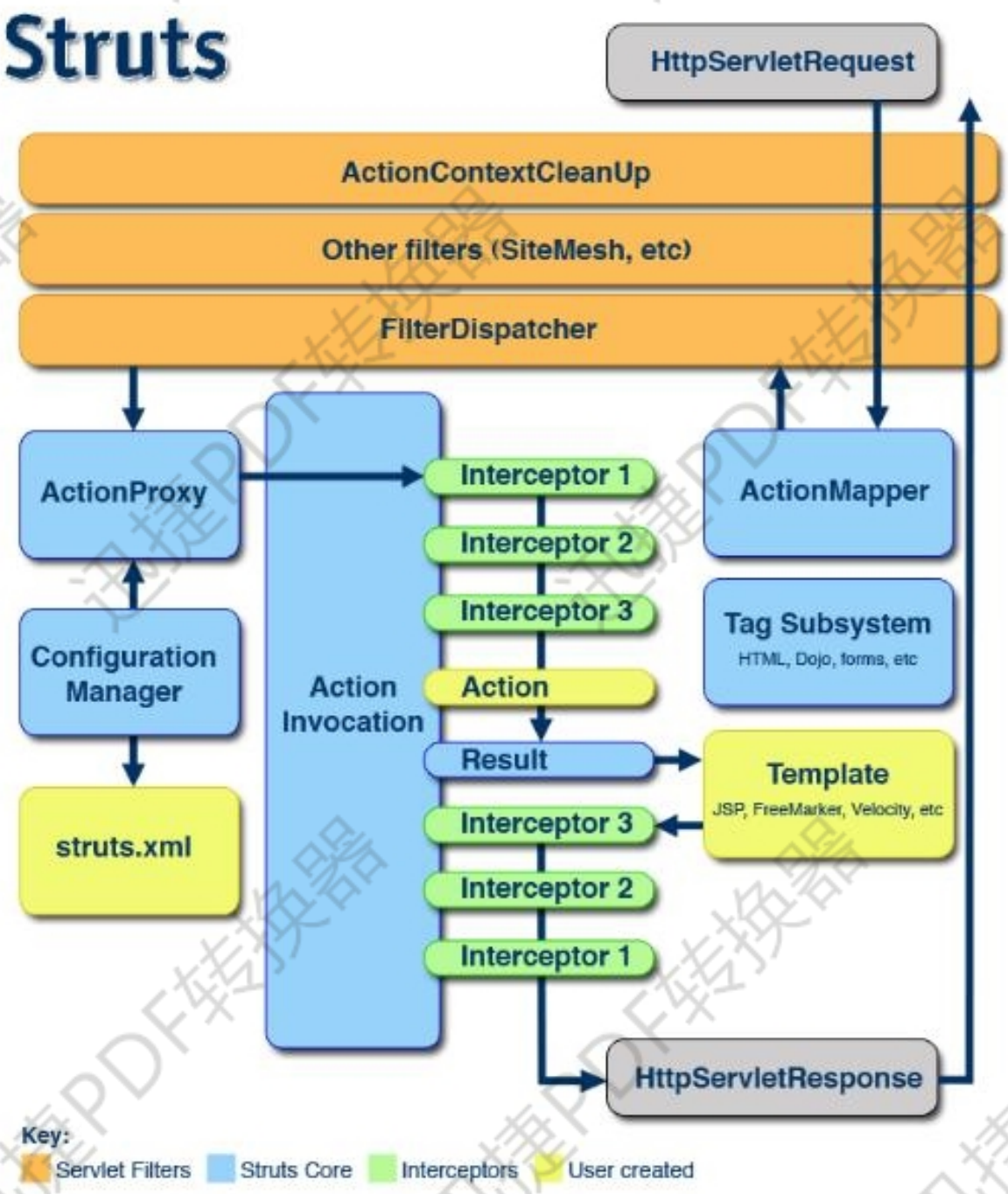
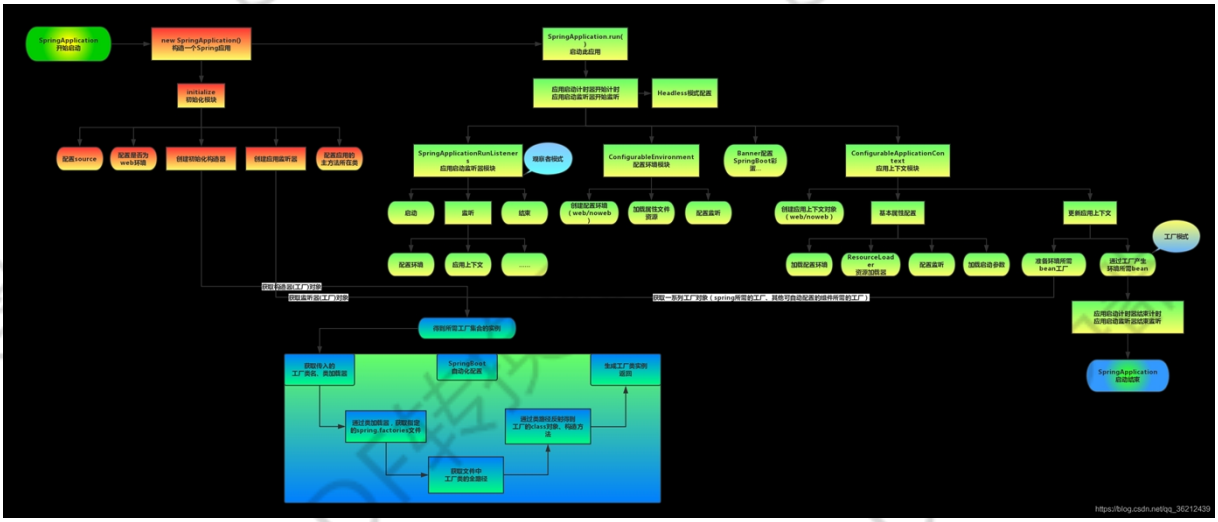
代码审计-JAVA 项目框架类漏洞分析报告




JAVA框架-小迪安全
1 框架识别
2 利用已知漏洞
3 挖掘未知漏洞
引用配置获取
名称及版本号
过滤器
拦截器
框架特性
执行流程
分析核心：断点调试


Struts
HttpServletRequest
ActionContextCleanUp
Other filters (SiteMesh, etc)
FilterDispatcher
ActionProxy
Configuration Manager
struts.xml
Action Invocation
Interceptor 1
Interceptor 2
Interceptor 3
Action
Result
Interceptor 3
Interceptor 2
Interceptor 1
ActionMapper
Tag Subsystem
HTML, Dojo, forms, etc
Template
JSP, FreeMarker, Velocity, etc
HttpServletResponse
Key:
Servlet Filters
Struts Core
Interceptors
User created



#知识点

简称 OGNL，对象导航图语言（Object Graph Navigation Language），是应用于 Java 中的一个开源的表达式语言（Expression Language），它被集成在 Struts2 等框架中，作用是对数据进行访问，它拥有类型转换、访问对象方法、操作集合对象等功能。

Spring Expression Language（缩写为 SpEL）是一种强大的表达式语言。在 Spring 产品组合中，它是表达式计算的基础。它支持在运行时查询和操作对象图，它可以与基于 XML 和基于注解的 Spring 配置还有 bean 定义一起使用。由于它能够在运行时动态分配值，因此可以为我们节省大量 Java 代码。

1、HttpServeletRequest

请求信息。

2、ActionContextCleanUP

3、Other filters

2,3 不重要，貌似现在已经没用了。

4、Filter Dispatcher

过滤器，这个应该是最底层的过滤器。

5、ActionMapper

Struts2 中主要检测请求信息是否需要 Struts2 处理。

6、ActionProxy

一个中间层，就是可以调用其他类什么的。

7、ConfigurationManager

ConfigurationManager 则负责将 struts.xml 文件中配置文件映射到内存中去的

8、Struts.xml

Struts 配置文件需要程序员填写。

9、ActionInvocation

包含四个属性分别获取前端传递的值，action,struts.xml 信息，其他一些数据。

10、Interceptor

拦截器不是太理解应该是获取前端传递的属性值，然后封装到 action 的属性域中。

11、Tag Subsystem

Struts2 自带标签库没用

12、Templete

Struts2 的前端模版，没用吧，不清楚。

13、HttpServletResponse

响应用户的类。

Filter 是基于函数回调的，而 Interceptor 则是基于 Java 反射的。
Filter 依赖于 Servlet 容器，而 Interceptor 不依赖于 Servlet 容器。
Filter 对几乎所有的请求起作用，而 Interceptor 只能对 action 请求起作用。
Interceptor 可以访问 Action 的上下文，值栈里的对象，而 Filter 不能。
最重要的要记住他们的执行顺序： 先 filter 后 interceptor，
另外在不同框架中有的是自带有的是需要自写，具体可以查看开发资料。
