设计研究与应用

基于 SSM+ZD 的漏洞管理平台设计与实现

唐菁敏，王红彬，王朝阳，张 伟，周 旋

（昆明理工大学，云南 昆明 650500）

摘 要：针对互联网信息安全事件频频发生，安全漏洞爆出频繁，用户难以管理平台漏洞问题进行分析研究，通过对国内外的漏洞管理平台的进行整理收集，后台采用了 SSM 框架，并集合了 Zookeeper+Dubbo 分布式模块，开发并设计了漏洞管理平台。漏管平台可以实时监测各主机状态，统计分析主机的漏洞分布情况，并对漏洞扫描结果进行图表展示，并提供相应处理办法。平台主要包括基础管理，漏洞管理和数据中心三大模块，实验结果表明漏洞查询具有高效的检测效率及正确率，系统运行稳定、效果良好，并具有良好的扩展性和维护性。

关键词：漏洞管理；漏洞扫描；SSM；zookeeper；Dubbo

中图分类号：TP393.08 文献标识码：A **DOI**：10.3969/j.issn.1003-6970.2018.02.026

本文著录格式：唐菁敏，王红彬，王朝阳，等. 基于 SSM+ZD 的漏洞管理平台设计与实现[J]. 软件，2018，39（2）：139-142

Design and Implementation of Vulnerability Management Platform Based on SSM + ZD

TANG Jing-min, WANG Hong-bin, WANG Zhao-yang, ZHANG Wei, ZHOU Xuan

(*Kunming University Of Science And Technology YunNan KunMing*)

【Abstract】: In view of the frequent occurrence of Internet information security incidents, the frequent loopholes in security breaches and the difficulty of users in managing platform vulnerabilities, the SSM framework is adopted in the background and the Zookeeper + Dubbo Distributed module, developed and designed a vulnerability management platform. The leaky pipe platform can monitor the status of each host in real time, statistically analyze the distribution of vulnerabilities of the host, display the result of the vulnerability scanning and provide corresponding solutions. The platform mainly includes three modules: basic management, vulnerability management and data center. The experimental results show that the vulnerability detection has high detection efficiency and correctness. The system runs stably with good effect and has good scalability and maintainability.

【Key words】: Vulnerability management; Vulnerability scanning; SSM zookeeper; Dubbo

0 引言

随着社会全面进入互联网时代，用户在享用高质量网络服务的同时，在复杂的网络环境中，存在着大量钓鱼网站、木马、软件本身缺陷等危害用户安全的问题[1]。如 2017 年爆发的新型“蠕虫式”勒索软件就是由不法分子，利用漏洞“EternalBlue”（永恒之蓝）进行传播，使至少 150 个国家、30 万名用户中招，造成损失达 80 亿美元，影响到金融，能源，医疗等众多行业，引起世界范围内对漏洞安全的广泛关注。

目前处理漏洞主要途径是对拥有主机进行单独漏洞扫描，发现漏洞进行安装补丁[2-3]。但是该流程还有可以继续优化，如对漏洞进行跟踪，对漏洞数据整理，展示漏洞不同解决方案，漏洞库实时更新等。根据以上问题，根据漏洞检测工具 cvechecker 提供的漏洞扫描接口[4]，开发设计了基于 SSM-ZD[5-8] 的漏洞管理平台，可以使用户通过漏管平台，下发漏洞扫描任务，查看漏洞处理流程，便于更好的管理系统存在漏洞并及时处理。

1 平台模块介绍

漏洞管理平台由三个核心模块组合而成，分别

作者简介：唐菁敏，男，副教授，博士，硕士生导师，主要研究方向协同通信；王红彬，男，(1993–)，研究生，主要研究方向：主要研究方向协同通信；王朝阳，男，(1993–)，研究生，主要研究方向：主要研究方向协同通信；张伟，男，(1991–)，研究生，主要研究方向：主要研究方向协同通信；周旋，男，(1992–)，研究生，主要研究方向：主要研究方向协同通信。

为基础管理模块、漏洞管理模块和数据中心模块，平台以这些模块进行功能实现并扩展，如图 1 所示为漏洞管理平台功能模块。

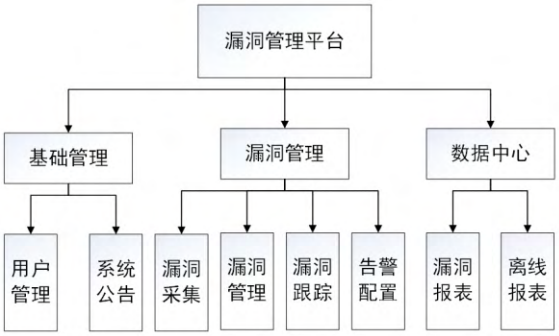

图 1　漏管平台功能模块

Fig.1　Leakage tube platform function module

1.1　基础管理模块

基础管理模块下包括了用户管理、系统公告。平台管理员通过用户管理添加用户并设置相应权限来新增访问账号，为保护用户安全，平台设置多种登录方式以供挑选，如若用户仅需要简单保护措施，可使用静态密码登录方式。如若平台安全级别需要提升，也可使用其他登录认证方式如：短信+密码认证、证书认证、Radius 认证和密码+令牌认证的方式[9]，为用户提供安全可靠的保证。

管理员可将最新的漏洞补丁情况以公告信息通知平台用户，便于各个用户能即使获取相关信息。公告会以弹窗形式来通知所有在线用户，并在平台首页实时动态显示。

1.2　漏洞管理模块

漏洞管理模块包括漏洞采集、漏洞管理、漏洞跟踪和告警配置。用漏洞采集配置包括数据类型、接口地址、账号密码、厂商。配置完成即可运行漏洞采集任务，并进入漏洞管理界面。

漏洞管理页面展示平台下发扫描任务，所有漏洞信息可在该界面查看并进行处理，点击可查看漏洞详情及相关解决办法。漏洞跟踪界面可对漏洞进行处理，不同业务线管理人员可对自己负责主机进行漏洞整改，管理员可在该界面查询漏洞具体的解决方法。

告警配置可设置系统告警方式、告警级别、跟踪级别、漏洞延期及漏洞延期率等相关配置。通过上述配置，当系统超过阈值可以通过配置告警方式进行告警，通知相关人员及时处理，以免对系统照成影响。

1.3　数据中心模块

数据中心模块包括漏洞报表、系统报表和离线报表。该模块主要进行数据可视化处理，用图表方式展示漏洞数据背后的系统可靠性，使用户更加直观清楚地了解各管理下各个系统安全及漏洞情况。平台也可生成 word 或 pdf 离线报表格式供用户下载使用。

2　平台设计

2.1　平台框架设计

平台后台框架采用 SSM[10-12]（Spring、SpringMVC、MyBatis）框架整合而成，框架模型如图 2 所示。

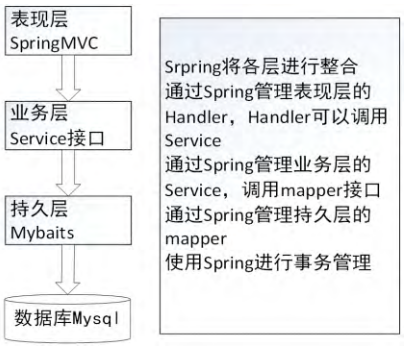

图 2　SSM 框架模型

Fig.2　SSM framework model

Spring：Spring 是整个项目中装配 bean 的工厂，根据设置的配置文件使用特定的参数去调用实体类的构造方法来实例化对象。其核心思想是 IoC（控制反转），可以不再繁琐的显式地`new`一个对象，而是让 Spring 框架解决并减少工作重复工作。

SpringMVC：主要进行页面的请求拦截与用户响应。组件有前端控制器，处理器映射器，处理器适配器，视图解析器，处理器 Handler，视图 View。SpringMVC 在项目中拦截用户请求，它的核心 Servlet 即 DispatcherServlet 承担中介或是前台这样的职责，将用户请求通过 HandlerMapping 去匹配 Controller，Controller 就是具体对应请求所执行的 操作。

Mybatis：主要进行 jdbc 的封装，它让数据库底层操作变的透明。操作使用 sqlSessionFactory 实例展开，通过 xml 配置文件关联到各实体类的 Mapper 文件，Mapper 文件中配置了每个类对数据库所需进行的 sql 语句映射。通过 sqlSessionFactory 拿到一个 sqlSession，执行 sql 命令与数据库交互返回给业务层[13]。

2.2 平台分布式设计

为了应对用户分布广泛，黑客攻击，数据量过大的问题，平台采用整合 Dubbo 和 zookeeper 来构建系分布式架构[14-15]。使用 Dubbo 来管理我们的服务的，以前我们都是自己调自己的服务，如果服务挂掉的话，那么整个系统就挂掉了，现在是我们把服务交给 dubbo 去统一管理，然后通过 zookeeper 来管理我们的 dubbo 的，具体模型图 3 所示。

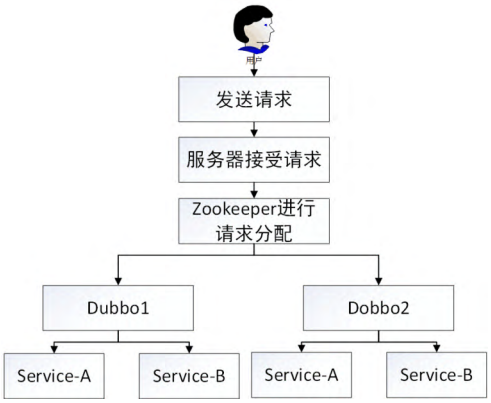

图 3 **Dubbo 整合 zookeeper 模式图**

Fig.3 Dubbo integration zookeeper mode diagram

ZooKeeper：Google 发布的开放源码的分布式协调服务，平台通过引入 ZooKeeper 作为存储媒介，实现负载均衡，因为单一服务器的承载能力是有限的，使用 ZooKeeper 群配合 Dubbo 服务框架完成分布式服务器，在流量达到一定程度的时候实现分流；使用 ZooKeeper 集群实现不同节点之间的数据和资源同步，让不同主机服务更多用户。

Dubbo：阿里巴巴公司开源的一个高性能优秀的服务框架，使用透明化的远程方法调用，实现负载均衡及容错机制，可在内网替代硬件负载均衡器，降低成本，减少单点。并且服务自动注册与发现，能够平滑添加或删除服务提供者，和 Zookeeper 整合可与 Spring 框架无缝集成。

在本平台中，通过 dubbo 的服务在 zookeeper 上面创建一个临时节点，表明自己的 ip 和端口，当用户需要提交请求时，会先在 zookeeper 上面查询[16]。根据 zookeeper 配置，做一些负载的选择（比如随机、轮流），找到服务相应的 dubbo 提供者，然后按照这些信息，为访问服务提供相应响应。通过添加分布式服务，可使平台成倍的增长服务能力，提供更可靠服务。

2.3 前端 WEB 设计

前端 WEB 主要为用户提供操作界面，平台前端页面采用 Freemark 模板引擎，前后端通过 JSON 来进行交互，解耦前后端的关联程度。在数据中心使用 Echarts 进行页面的数据可视化展示，并提供丰富的图表类型，使用 Bootstrap 技术简化前端页面维护难度及提高开发效率[17]。

3 漏洞管理实现细节

根据上述漏洞管理平台的功能模块分析及技术选型，完成对整体框架模型设计开发，因本文篇幅有限，现在仅对漏管平台核心模块漏洞管理模块进行详细介绍，漏洞管理使用流程如图 4 所示。

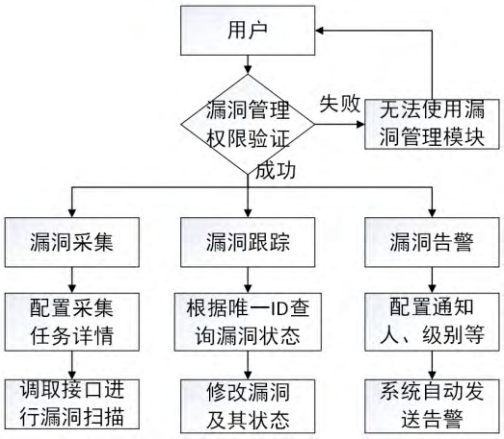

图 4 漏洞管理流程图

Fig.4 Vulnerability management flowchart

通过漏洞采集，将得到漏洞数据保存到 Mysql 数据库中，数据库按照漏洞 ID、发布日期、等级危害等关键字对保存数据进行分类排序，方便后续查询读取数据。扫描配置信息及漏洞详细描述会以 DES 加密算法处理[18]，秘钥通过 XML 配置文件保存在代码中，加密的工作主要保证平台的漏洞信息安全，防止安全信息泄露会被窃取。

漏洞告警主要负责及时通知平台安全状态，用户通过配置检测主机 ip、安全告警级别、通知方式、通知人等信息，平台可自动检测目标主机的漏洞安全状况，及时通知先关人员，避免问题处理不及时，造成不必要损失。

4 系统测试

本平台部署在云服务器中，分 A、B 两个相同配置服务器同时运行，服务器为 CPU 核数：4 核，内存：3.74 GB，通过腾讯 WeTest 压测大师对平台进行压力测试[19-21]，主要测试了响应平均时间、事

务成功率、收发包率等关键参数。设置模拟 1000 人并发访问系统各项功能 1 小时，检测并记录关键数据如下表 1 所示。

表 1 服务器压力测试数据
Tab.1 Server stress test data

测试项	结果
平均响应时间	362.05 ms
事务成功率	99.90%
平均收包率	1728.12/s
平均发包率	1689.25/s

压力测试结果表明，在模拟一万人同时访问漏管平台时，系统性能稳定相应速度稳定在合理范围之内，事务基本全部成功执行，服务器可以稳定运行。

图 5，图 6 为部分关键页面的效果图。

图 5 漏洞管理主页
Fig.5 Vulnerability Management Homepage

图 6 漏洞下发界面
Fig.6 Vulnerability distribution interface

5 结语

平台针对互联网漏洞管理的问题进行分析研究，通过 SSM 框架并整合 Zookeeper 和 Dubbo 分布式服务，设计并开发了一个可提供高效稳定的的漏洞管理平台，平台可为用户提供一个简单快捷的漏洞管理工具。但是漏洞管理平台还有很多模块并未添加，目前所接触仅仅是系统的一部分，还有需要进一步集成并完善。随着互联网安全的发展及网络安全标准的建立，漏洞管理平台必然会成为未来网络安全的重要解决方案。

参考文献

[1] 石建国，周檬，石彦芳．计算机系统漏洞与安全防范技术探讨[J]．无线互联科技, 2014(11).

[2] 张蜻．计算机系统漏洞与安全防范技术探索[[J]．电子技术与软件工程, 2014(8).

[3] 刘西青．浅谈计算机网络安全问题[J]．软件，2013, 34(12): 239.

[4] 印杰，李千目．软件代码漏洞的电子取证技术综述[J]．软件, 2015, 36(12): 49-59.

[5] 姚成浪．基于ZooKeeper与dubbo的集群计算系统设计与实现[D]．哈尔滨：哈尔滨工程大学. 2007.

[6] 王杨．基于校园网的网络安全与开销研究[J]．软件，2014, 35(4): 189-192.

[7] 马立新，金月光．基于策略的网络安全管理系统设计与实现[J]．软件, 2013, 34(6): 25-26.

[8] 夏德友，陈艳华．探究微信技术架构及安全漏洞和防范技术[[J]．信息技术与信息化, 2015(9).

[9] 王倩宜，李润娥，李庭晏．统一用户管理和身份认证服务的设计与实现[J]．实验技术与管理, 2014.

[10] 吴黎明，陆晓辉，漏洞管理平台框架结构设计, 2013, 8.

[11] 张桂元、贾燕枫、姜波《征服Ajax Web 2.0快速入门与项目实践(Java)》人民邮电出版社, 2006.

[12] 高寅生《安全漏洞库设计与实现》，《微电子学与计算机》，2007年第24卷第3期.

[13] (美)威尔德，斯尼德等著，赵利通译. SpringFramework 2入门经典[M]．北京：清华大学出版社, 2015.

[14] 谭玉靖．基于ZooKeeper的分布式处理框架的研究与实现[J]．计算机工程, 2014, 29(22): 93-95.

[15] 王润华，任化敏，周艳芳分布式系统开发利器——ZooKeeper研究[J]．中国电子商情：通信市场, 2012(1): 64-67.

[16] 曹黎波．Web应用的漏洞检测与防范技术研究[[J]．中国矿业大学, 2015(6).

[17] 郑力明，李晓冬，罗建禄．服务器与集群系统节能技术研究[J]．软件, 2013, 34(4): 59-61.

[18] 龙著乾．流媒体服务器集群的负载均衡研究[J]．软件，2013, 34(4): 62-64.

[19] Charles P. Pfleeger, Shari Lawrence Pfleeger《信息安全原理与应用》(第4版).

[20] Ron Patton. 软件测试[M]．机械工业出版社, 2010.

[21] 涂华轲，邹华，林荣恒．增强的云化并行计算框架系统的设计与实现[J]．新型工业化, 2012, 2(12): 33-40.