提高城镇化质量问题与对策研究

摘 要

在当今知识经济高速发展的社会，国家和地区的社会生产力随着科学技术的进步和产业结构的调整不断的进步，社会结构的调整，由以农业等第三产业为主的传统乡村型社会转变成以第一、二产业为主的现代城市型社会成为势在必行不可或缺的任务。

城镇化建设不仅可以降低农村地区人们的流动意愿，以此来实现控制大城市规模，合理发展中小城市的目的，减缓人们通过各种渠道进行的实际意义上向城市的迁移。还可以为创业者提供良好的发展创业环境，吸引外出打工者回乡创业，加速经济发展。城镇化的发展也有助于消除城乡二元经济结构，平衡东、中、西部经济发展，缓解城乡差异。

城镇化的必要性显而易见，但城镇化的转变不会是一蹴而就的,城镇化转变的过程中会带来环境、生态、人口、就业等各个方面的问题。因此，城镇化质量问题就成了关注的重点，本文主要是针对就如何提高城镇化质量，应对城镇化发展过程中遇到的问题及相应对策的研究。

关键词： 城镇化 城镇化质量 对策建议

Improve the Quality of Urbanization and Countermeasures

**ABSTRACT**

In the social productive forces of society, countries and regions, the rapid development of today's knowledge-based economy and with the progress of the adjustment of industrial structure of science and technology continues to progress, social structure is adjusted from agricultural and other tertiary industries traditionally dominated rural society transformation into the first and second industry mainly to the modern urban society has become an indispensable imperative mission.

Urbanization can not only reduce the flow of people in rural areas will to control the size of large cities in order to achieve rational development purposes small city, slowing migration to urban real sense of people through various channels. Entrepreneurs can also provide a good business environment for development, to attract migrant workers return home business, and accelerate economic development. Development of urbanization also helps eliminate the urban-rural dual economic structure, balanced economic development, the eastern, central, western, both differences between urban and rural.

The necessity of urbanization is obvious, but the urbanization transition will not be easy, environmental, ecology, population, employment and other aspects of the process of urbanization will bring a change in. Therefore, the focus of urbanization quality problems became concerned, this article is mainly aimed at how to improve the quality of urbanization, urbanization development to deal with problems encountered in the process of research and corresponding countermeasures.

**Key Words:** Urbanization Urbanization Quality Suggestion

**目 录**

[第一章 引言 1](#_Toc449383091)

[1.1 背景介绍 1](#_Toc449383092)

[1.2 线路的安全性分析 1](#_Toc449383093)

[1.2.1 电缆加压技术 1](#_Toc449383094)

[1.2.2 光纤通信线 1](#_Toc449383095)

[1.3 网络模型的安全性分析 1](#_Toc449383096)

[1.3.1 传输层安全性分析 1](#_Toc449383097)

[1.3.2 网络层安全性分析 2](#_Toc449383098)

[1.3.3 应用层安全性分析 2](#_Toc449383099)

[1.4 网络通信存在的安全威胁 2](#_Toc449383100)

[1.4.1 传输过程中的威胁 2](#_Toc449383101)

[1.4.2 TCP/IP协议的威胁 3](#_Toc449383102)

[1.4.3 路由器的威胁 3](#_Toc449383103)

[1.5 本章小结 3](#_Toc449383104)

[第二章 城镇化分析 4](#_Toc449383105)

[2.1 城镇化机理分析 4](#_Toc449383106)

[2.2 城镇化路径分析 4](#_Toc449383107)

[2.3 城镇化方法分析 4](#_Toc449383108)

[2.4 城镇化策略分析 5](#_Toc449383109)

[2.5 本章小结 5](#_Toc449383110)

[第三章 城镇化质量 6](#_Toc449383111)

[3.1 城镇化水平的测算方法 6](#_Toc449383112)

[3.2 SQL注入 9](#_Toc449383113)

[3.3 XSS攻击 10](#_Toc449383114)

[3.4 本章小结 10](#_Toc449383115)

[第四章 提高城镇化质量 11](#_Toc449383116)

[4.1 概述设计 11](#_Toc449383117)

[4.3 总体设计 11](#_Toc449383118)

[4.4 开发环境及工具 11](#_Toc449383119)

[4.5 系统模块开发 12](#_Toc449383120)

[4.5.1 综述 12](#_Toc449383121)

[4.5.2 登陆及用户操作模块 12](#_Toc449383122)

[4.5.3 前端展示模块 13](#_Toc449383123)

[4.5.4 攻击检测模块 13](#_Toc449383124)

[4.5.3 网络拓扑 14](#_Toc449383125)

[4.6 本章小结 14](#_Toc449383126)

[第五章 对策分析 15](#_Toc449383127)

[5.1 登陆测试 15](#_Toc449383128)

[5.2 性能模块测试 17](#_Toc449383129)

[5.3 攻击防护测试 21](#_Toc449383130)

[5.4 日至报表测试 22](#_Toc449383131)

[5.5 用户管理模块测试 23](#_Toc449383132)

[5.6 本章小结 24](#_Toc449383133)

[第六章 总结与展望 25](#_Toc449383134)

[6.1 总结 25](#_Toc449383135)

[6.2 展望 25](#_Toc449383136)

[参考文献 26](#_Toc449383137)

[致谢 27](#_Toc449383138)

# 第一章 引言

## 1.1 背景介绍

在当今知识经济高速发展的社会，国家和地区的社会生产力随着科学技术的进步和产业结构的调整不断的进步，社会结构的调整，由以农业等第三产业为主的传统乡村型社会转变成以第一、二产业为主的现代城市型社会成为势在必行不可或缺的任务[1]。

中央经济工作会议很早就已经提出了以推进城镇化的方式来调整经济结构、扩大内需实现经济的可持续发展。城镇化是基于中国国情和现阶段经济社会发展形势而做出的战略选择。城镇化创造国内需求的机理是：城镇化推动城镇建设从而创造投资需求；城镇化引发消费升级从而创造消费需求：城镇化推动产业升级从而扩充市场需求；城镇化促进郊区转型从而形成新的市场需求；城镇化促进新农村建设从而扩大农村需求。推进城镇化既要从中国的国情出发，也要遵循世界城镇化的一般规律，更要结合当前中国城镇化发展的新情况新趋势．实施新型的城镇化战略。更加注重提升城镇发展质量和水平。

## 1.2 线路的安全性分析

### 1.2.1 电缆加压技术

摒弃了之前在地下部署电缆的策略，改为将电缆架于空中，在整个楼中，所有的电缆都是可见的。当有人想要破坏电缆时，通过电缆电压检测会有实时警报，告知工作人员可能遭到破坏的位置。这样降低了电磁辐射的强度，所以一般需要大型设备才能进行电磁感应窃听，以此提高了电缆的安全性。

### 1.2.2 光纤通信线

之前的技术水平，认为光纤通信是完全安全的。因为当电缆发生变化如：断裂或者遭到破坏时，线路变化会被立刻察觉，并且拼接处的传输速度会受到影响。且光纤通讯线是没有电磁辐射的，所以电磁感应窃听就无法实施。

## 1.3 网络模型的安全性分析

### 1.3.1 传输层安全性分析

1. 对于端对端的应用服务来说，传输层能够提供很好的安全防护机制。我们也会为程序间提供可信任的数据传输协定。

2. 目前技术层面上，有两个协议提供了传输层的协议保障：安全传输层协议（TLS）和安全套接层协议（SSL）。而前者实际上是后者的一个IETF版本。这些协议为传输层提供了服务器验证与客户端验证，并且保证了数据的机密性、完整性。

### 1.3.2 网络层安全性分析

我们已经讨论了在传输层上的安全性。不过，在一些情况下，传输层上的安全协议是不够的。首先，应用层上所有的客户端和服务器端程序都能受到良好的保护。

### 1.3.3 应用层安全性分析

对于网络模型中，防御难度最大的一层就是应用层。TCP/IP程序没有太多的规则去限制它的运行，而且没有办法去保护所有应用层上的程序。但是应用层上的程序都会有一些共性。

通过对每个程序的网络防护来达到保护网络层肯定是不能实现的，但是只允许一些特定的程序通过网络进行通信，还是一个不错的办法。

1. 简单邮件传输协议（SMTP）本身有很小的风险。黑客可能利用的途径有[2]：
   1. 拒绝服务攻击
   2. 伪造邮件信息，通过社会工程学获取想要的隐私信息
   3. 直接在邮件中嵌入特洛伊木马或病毒并发送到准备攻击的用户邮箱
   4. 文件传输协议（FTP），当开启匿名登录后，不当的权限管理会造成任意用户上传或修改FTP服务器上的内容，形成安全盲点。
2. 超文本传输协议（HTTP）是现在互联网上应用最为广泛的一种通信协议。是一种无状态协议，它并不存储用户的连接状态。通常的过程是：
   1. 客户端发起一个连接请求
   2. 服务器端进行连接请求响应
   3. 客户端发起一个文档请求
   4. 服务器端响应客户端的文档请求
   5. 断开连接
3. 远程连接服务标准协议（Telnet）用于对远程终端进行访问。telnet的一个缺点就是发送用户名和密码时使用明文传输，攻击者可以借此进行信息劫持。所以，必须保证安全的网络环境下才能使用Telnet。主机（进程）间的数据传输可以通过网络层的安全协议来达到防护的效果。但究其本质，数据还是通过通信通道进行传输的。如果确实想要区分一个具体文件的不同安全需求，那就必须借助于应用层的安全性[3]。

## 1.4 网络通信存在的安全威胁

### 1.4.1 传输过程中的威胁

1. 截获：截获信息属于破坏正常传输过程的方式之一，它从正常的通信信道中直接将一部分信息捕获，并不再向后转发。
2. 窃听：窃听消息属于不破坏正常传输过程的方式之一，它在正常的通信信道中获取信息后，不进行截断，将传输继续传播下去。
3. 篡改：篡改信息属于破坏正常传输过程的方式之一，它从正常的通信信道中截取信息后加以修改，再进行向后发送，达到了修改原信息的目的。
4. 伪造：伪造信息属于破坏正常传输过程的方式之一，它从正常的通信信道中直接插入一段伪造的信息，并向下继续传输。

### 1.4.2 TCP/IP协议的威胁

为了能让各种不同的网路设备或者不同网络间传输数据，互联网通过技术手段将网络硬件的底层技术细节进行了封装。作为目前使用最广泛的互联网网络互联协议，TCP/IP在目前的网络通信中扮演着非常重要的角色。

可以究其根本，自身的安全性问题却给了骇客们有了很多攻击的机会。

### 1.4.3 路由器的威胁

1. 以路由器作为攻击平台，黑客通过路由器的漏洞，对其他的网站或站点进行扫描或者攻击；
2. 拒绝服务攻击，路由器拥有最大流量传输限制，通过转换思路，由攻击服务器改为攻击服务器所连接的路由器，当路由器传输的流量超过限定值时，即可造成等同于对服务器的拒绝服务攻击；
3. 明文传输配置信息，因为很多管理员未对设备进行密码更改，使用默认密码或者弱口令，黑客即可通过这些进行任意配置，造成之后的一系列威胁；
4. 新型的路由器都在自身防御功能上增加了很多保护，但是管理员的正确管理及物理隔离才是更重要的防护方式。

## 1.5 本章小结

本章主要说明了在现在的互联网环境下，哪些因素会引起网络安全事故，并分析了TCP/IP协议的安全隐患对整个网络传输的影响。这也是本系统采用对Web的入侵检测系统开发的理论基础。

# 第二章 城镇化分析

## 2.1 城镇化机理分析

Adenrson在 80年代早期使用了“威胁”这一概念术语，其定义与入侵含义相同。将入侵企图或威胁定义为未经授权蓄意尝试访问信息、窜改信息 ,使系统不可靠或不能使用。Heady给出另外的入侵定义，入侵是指有关试图破坏资源的完整性、机密性及可用性的活动集合。Smaha从分类角度指出入侵包括尝试性闯入、伪装攻击、安全控制系统渗透、泄漏、拒绝服务、恶意使用6种类型。

入侵检测技术主要分成两大类型：异常入侵检测和误用入侵检测。第1种是指能够根据异常行为和使用计算机资源情况检测出来的入侵[4]。异常入侵检测试图用定量方式描述可接受的行为特征，以区分非正常的、潜在的入侵性行为。Anderson做了如何通过识别“异常”行为来检测入侵的早期工作[4]。他提出了一个威胁模型，将威胁分为外部闯入、内部渗透和不当行为 3种类型，并使用这种分类方法开发了一个安全监视系统，可检测用户的异常行为。外部闯入是指未经授权计算机系统用户的入侵；内部突破是指已授权的计算机系统用户访问未经授权的数据；不当行为是指用户虽经授权，但对授权数据和资源的使用不合法或滥用授权。误用入侵检测是指利用已知系统和应用软件的弱点攻击模式来检测入侵[4]。例如，Internet蠕虫攻击使用了fingerd和sendmail错误，故可以归结到误用入侵这种类型。与异常入侵检测相反，误用入侵检测能直接检测不利的或不可接受的行为，而异常入侵检测是检查出与正常行为相违背的行为。

## 2.2 城镇化路径分析

入侵检测系统在近年来的发展中，各个方面都获得了长足的进步，但在包过学术理论研究，和实际应用中都还存在许多需要解决的问题：

很容易产生误报和漏报。主要原因是特征库的逻辑不够复杂。

防火墙系统的不同环境下，智能适应能力还比较差，自我学习能力不足，系统缺乏更高的机器学习能力和适应性。。

在科技飞速发展的今天，我们的网络速率提升异常明显，这也造成了入侵检测系统的Real-time检测效率值降低。

## 2.3 城镇化方法分析

对于入侵检测技术的未来，我们除了完善传统的技术，更应该开发出新的入侵检测技术来维护网络的安全。今后的入侵检测技术的发展方向集中在以下几个方面：[5]

面向IPv6的入侵检测。下一代互联网采用IPv6协议，目前世界正处于从IPv4向IPv6过渡时期。随着IPv6应用范围的扩展，入侵检测系统支持IPv6将是一大发展趋势，是入侵检测技术未来几年该领域研究的主流[5]。

1. 近年来，网络攻击的发展趋势是逐渐转向高层应用。根据Gartner的分析，目前对网络的攻击70%以上是集中在应用层，并且这一数字呈上升趋势。所以入侵检测系统对应用层的保护将成为未来研究的方向[5]。
2. 入侵检测系统的自身保护和易用性的提高。目前的入侵检测产品大多采用硬件结构，黑箱式接入，免除自身的安全问题。同时，大多数的使用者对易用性的要求也日益增强，这些都是优秀的入侵检测产品以后继续发展细化的趋势[5]。
3. 使用智能化的方法与手段来进行入侵检测。即现阶段常用的有神经网络、遗传算法、模糊技术、免疫原理等方法[5]。
4. 分布式、协作式入侵检测和通用式入侵检测体系结构的研究。随着网络系统的复杂化以及入侵方式的多样化，检测系统的体系结构也在发展[5]。
5. 基于云模型和支持向量机的入侵检测特征选择方法。解决了目前算法的缺陷[5]。

## 2.4 城镇化策略分析

对于入侵检测技术的未来，我们除了完善传统的技术，更应该开发出新的入侵检测技术来维护网络的安全。今后的入侵检测技术的发展方向集中在以下几个方面：[5]

面向IPv6的入侵检测。下一代互联网采用IPv6协议，目前世界正处于从IPv4向

## 2.5 本章小结

本章主要阐述了入侵检测的定义、分类，并分析了入侵检测系统的目前发展状况及存在的问题。最后是对入侵检测的未来发展做出一定的展望。

这就是本系统的设计依据，吸取现在系统的问题和缺点，根据现在的发展规划进行系统开发。

# 第三章 城镇化质量

## 3.1 城镇化水平的测算方法

衡量一个国家或者一个地区的城镇化质量有一个目前在国际上可以通行的重要指标，是居住在城镇的人口占总人口的比例，即通常意义上我们说的城镇化水平。抽象来说，城镇化过程可以被解释为城镇逐步成为致使国民经济与社会的发展的主导因素的过程。我们分析城镇化质量，评估城镇化水平的时候，不可避免的需要进行城镇化的测算，分析比较在不同的区域或不同的时期之间，城镇对于经济和社会发展的作用。但是，城镇化属于一种比较复杂的社会现象，所以，很难准确的测算城镇化。在此来归纳总结下近十几年来学者们探讨出的测算方法，一共三类：单一指标法，多项指标法以及其他指标法[2]。现在人们常用的测算城镇化水平的方法有：人口比重指标法、城镇土地利用比重指标法、调整系数法、农村城镇化指标体系、现代城市化指标体系等。

人口比重指标法，顾名思义是反映城镇化导致的人口变化情况，包括：城镇人口比重指标法和非农业人口比重指标法两种。这也是两种比较通用的方法。其中，城镇人口比重指标法是指用城镇人口占总人口数的比重来表示城镇化的水平。这种测量方式的优势在于简洁、易区分、统计便利。但是也有缺陷，在使用这种方法的时候，不仅要区分不同人口统计口径的标准，而且人口统计口径的适用性、可比性和局限性也是至关重要的。由于各个地区设镇标准各不相同，有时这种测量方法反馈出的数据不能准确的反映城镇化的程度，而且城镇人口也可能因为行政区划的变更而导致数据失真。非农业人口比重指标法是用非农业人口占总人口的比重来衡量城镇化水平。它的优势在于能够很好的反映贫富程度，体现人口在经济活动上的结构关系，也能够反映生产力水平及生活方式的情况。但是很难判断一个人的身份究竟是农民还是城市居民，无论是生活地点还是从事的职业隶属于农业还是非农业生产都是很难界定的。

城镇土地利用比重指标法是根据城区土地利用面积占区域总面积来反映城镇化水平。这种测量方式对于人口密度相对比较大的地区比较适合，但如果对于人口密度较小或者城区建设用地过多的地方则会测量失真。

比例关系调整系数法与其他单一的测量方法比如人口比重指标法、城镇土地利用比重指标法比较可能要更准确一些。但是调整系数法的理论依据不足，在不同的历史时期和制度环境，没有足够的理由来预期这些系数能够继续保持相对稳定的状态。由于城镇化进程并不是某一单一因素可以决定，而是要受多种因素制约，因而单靠某一调整数来反映城镇化水平是很难做到准确的。

农村城镇化指标体系法是根据25条农村城镇化指标来评判城镇化水平。根据农村城镇化的特征，指标涵盖了人口结构、经济发展状况、社会环境状况三个方面，结合了农村现代化的标准。这25项指标基本全面地反映了农村城镇化的总体概况。

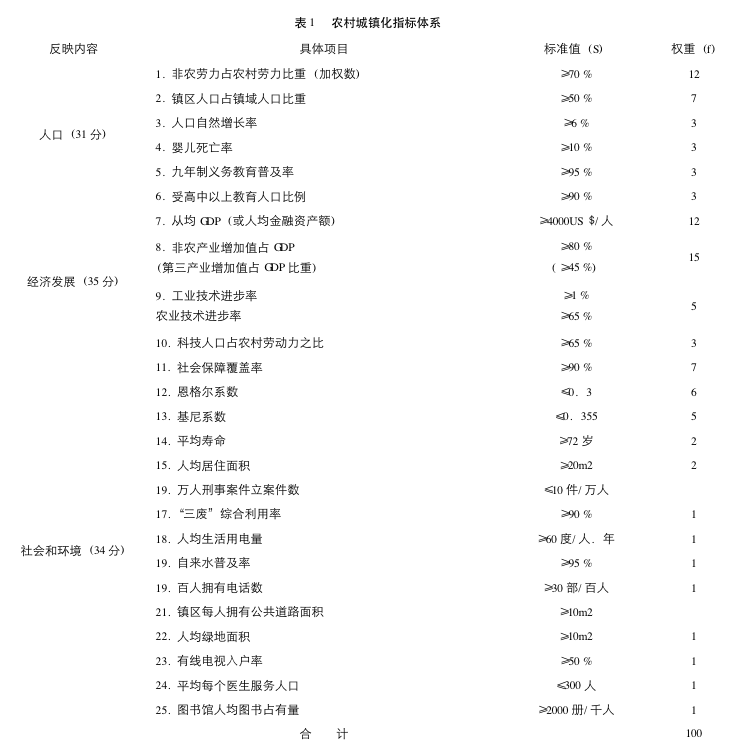


图3.1农村城镇化指标体系

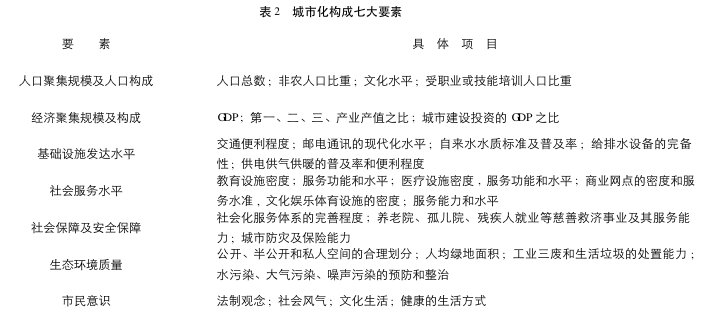
现代城市化指标体系与农村城镇化指标体系没有本质的差异，只是侧重点不同。现代城市化指标体系是根据七个城市化构成的要素，设置若干项指标来衡量现代城市化的程度。

图3.2 城市化构成七要素

## 3.2 城镇化与生态环境

城镇化的高速发展极大促进了农村经济的发展和繁荣，但是生态环境建设的速度远逊于城镇化发展的速度，所以在生态环境建设方面积累了很多问题亟待解决。

城镇化的发展中，以农业等第三产业为主的传统乡村型社会逐步转变成以第一、二产业为主的现代城市型社会。致使，一直制约我国农业发展的人地矛盾更加锐化。小城镇盲目跟风不考虑实际情况的建设城镇化，导致大量的农田被侵占。小城镇由于集约化程度和土地价格低，所以用地规模有很多并非产业拉动而是政府事先预订的。大量土地被圈占之后却缺乏实质性产业填充，造成浪费了大量的土地资源。

城镇化工程也导致了人口集中，生活废弃物、生活污水对环境的影响也逐渐严重。生活垃圾排放无序利用率极低，不仅占用大片土地，而且露天堆放导致病毒、细菌传播，渗透液污染地下水，加重生态环境的恶化，加之城市的生活垃圾也在向农村转移，更加剧了污染。

SQL注入主要有一下几个方面引起威胁：

1. 对表单提交的数据类型处理不恰当；
2. 使用的数据库配置不安全，不规范；
3. 对数据库的查询集执行不合理；
4. 对提交错误信息的容错机制不合理；
5. 对于转义字符的处理存在漏洞；

我们可以对以上的产生原因进行分析，并总结此类安全问题应该如何解决。当然，网络信息发达的现在，开发者也得出了一些在工程师开发应用时，应该给予关注的SQL注入防护。主要有以下几个点值得注意：

1. 永远不要信任用户的输入。对用户的输入进行校验，可以通过正则表达式，或限制长度；对单引号和双"-"进行转换等。
2. 永远不要使用动态拼装sql，可以使用参数化的sql或者直接使用存储过程进行数据查询存取。
3. 永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。
4. 不要把机密信息直接存放，加密或者hash掉密码和敏感的信息。
5. 应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装。

## 3.3 XSS攻击

XSS，翻译成中文叫做跨站脚本攻击。恶意攻击者往Web页面里插入恶意html代码，当用户浏览该页之时，嵌入其中Web里面的html代码会被执行，从而达到恶意攻击用户的特殊目的。XSS攻击分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，如：dvbbs的showerror.asp存在的跨站漏洞。

另一类则是来自外部的攻击，主要指的自己构造XSS跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。如当我们要渗透一个站点，我们自己构造一个有跨站漏洞的网页，然后构造跨站语句，通过结合其它技术，如社会工程学等，欺骗目标服务器的管理员打开。

## 3.4 本章小结

本章主要讲解了TCP/IP协议的基础知识，包括报文头格式、传输方式、传输规则等。让我们更深一步的了解这个协议。还分析了Web入侵的几种常见行为，如：XSS/SQL注入等。并分析了这几种行为的防护方法及攻击检测方法。

# 第四章 提高城镇化质量

## 4.1 概述设计

在该系统的准备工作进行知识，已经进行了了对系统各项技术需求及使用需求的准确分析，并制订了初步的主要系统功能模块，之后的工作就是针对需求分析的各项结果和需求分析的结果，着手开始对系统的各个模块进行开发。根据之前学到的软件工程专业课知识，一个软件的设计一般分为系统总体设计和单元模块详细设计两个部分。

当前阶段，我会将需求分析后的结果进行系统的安排和分解，把系统划分成几个模块，几个模块之间相互配合又互不影响，做种组成一个完整的系统。

综上所述，在详细设计之前，我们要先进行总体设计是有着一定的必要性：系统开发者将眼光放到整体上，从比较抽象的层次上分析对比出多种可行性高的的系统设计实现方案和系统的结构，从中选出最优方案，和软件结构，并开始正常开发。

## 4.3 总体设计

Web入侵监测系统是对服务器流量进行分析并发现其攻击特征，最根本的部分就是对Web行为的网络数据包获取，分析及举措。最基本的问题就是掌握数据包请求的获取和分析。目前对于网络数据包获取分为在线转发模式和离线复制流量模式。本系统将采用离线复制流量模式进行开发。

## 4.4 开发环境及工具

1. UNIX操作系统支持多用户、支持多任务的操作系统，支持多种处理器架构，按照操作系统的分类，属于分时操作系统，最早由KenThompson、DennisRitchie和DouglasMcIlroy于1969年在AT&T的贝尔实验室开发。

UNIX具有的特性：

* 1. UNIX系统是一个具有多用户，多任务支持的操作系统。
  2. UNIX由操作系统内核和系统的外壳两部分系统结构构成。
  3. UNIX系统大部分功能实现使用的是C语言，这为UNIX系统提高了更高的可读性和更好的复用性。
  4. UNIX系统使用了树状结构的文件系统模式，这样能更好的控制文件的权限，以此达到系统的安全防护的目的。
  5. UNIX系统的内存管理机制是采用了进程对换（Swapping）和请求调页的存储方式，实现了对内存管理的虚拟化，很大程度的提高了内存使用的比率。 UNIX系统提供了管道通信，软中断通信，消息通信，共享存储器通信，信号灯通信等多种通信通道。

1. PHP是Hypertext Preprocessor的缩写，中文翻译为超文本预处理器。是一们脚本语言，并且目前已经开源。PHP吸收了C语言、Java和Perl语言的各类特点。容易入门，学习曲线较低，一般作用于网页的数据传输及展示。以.php作为PHP文件的后缀名。
2. VMware是一个专注于虚拟机软件开发的公司，也是全球桌面到数据中心虚拟化解决方案的领导厂商。全球不同规模的客户依靠VMware来降低成本和运营费用、确保业务持续性、加强安全性并走向绿色。
3. Sublime Text是目前业界前端工程师使用率最好的编辑器。它支持各种模式的编辑，如VIM、BASH等。Sublime Text使用了用户体验很好的界面，并且提供了各类能大幅度提高效率的功能，例如代码缩略图，各语言的自动完成插件。还可绑定自定义键。Sublime Text的主要功能包括：代码标签、方法等的拼写自动检查，书签快速跳转，多窗口等等。Sublime Text也是一个全平台的编辑器，同时支持Windows、Linux、Mac OS X等操作系统。
4. FreeWaf是目前开源社区一个功能较为完善的Web应用安全产品，提供了较高的攻击行为检测准确度。一款开源的Web应用防火墙产品来防护Web应用的安全。

## 4.5 系统模块开发

### 4.5.1 综述

本系统使用MySQL来建立数据库，通过PHP进行数据库访问，并进行增删改查操作。子系统均采用模块化的方式构建，以达到高内聚低耦合的软件开发思想。

入侵规则检测使用目前网络最新的开源规则库作为默认的安全监控策略，并且可以通过Web管理界面进行自定义设计，包括停止原有防护规则；增加新的防护规则；以及修改当前防护规则的部分参数。

### 4.5.2 登陆及用户操作模块

用户权限采取平衡管理权限模式，所有用户除管理员外均具有相同的权限，管理员相较于用户权限还具有用户管理权限。

Web管理界面的浏览和管理在没有得到权限授权的前提下是无权进行的。PHP在用户登录模块开发过程中提供了有效的安全策略.该模块实现对身份认证、权限分配来实现用户的验证与登录。为安全起见，该系统对用户的所有操作，包括登陆，用户管理及网络安全防护的各项配置、操作等都进行了详细记录，并存入数据库。以此达到了对所有用户安全操作的全方面监控。

### 4.5.3 前端展示模块

本系统使用了将CSS全部抽离HTML页面，更加方便、统一的管理页面样式。并通过HACK等方式实现对各浏览器的地兼容。

数据通过底层方法对数据整理后存入数据库的数据进行调取，并通过前端JS代码进行实时动态展示。

### 4.5.4 攻击检测模块

本系统使用了freewaf网络最新的规则库文件进行网络安全防护。并对部分规则进行了修改，目前本系统支持XSS、SQL注入、CSRF等基本攻击的防护及预警。

1. SQL注入

对于基础防护,主要归纳一下，主要有以下几点：

* 1. 永远不要信任用户的输入。对用户的输入进行校验，可以通过正则表达式，或限制长度；对单引号和双"-"进行转换等。
  2. 永远不要使用动态拼装sql，可以使用参数化的sql或者直接使用存储过程进行数据查询存取。
  3. 永远不要使用管理员权限的数据库连接，为每个应用使用单独的权限有限的数据库连接。
  4. 不要把机密信息直接存放，加密或者hash掉密码和敏感的信息。
  5. 应用的异常信息应该给出尽可能少的提示，最好使用自定义的错误信息对原始错误信息进行包装

在分析了SQL注入的各类方法后，先做出如下总结和分析：

1. 输入验证：检查使用者提交表单输入的合法性，确人提交的内容全部是合法的安全数据。
2. 容错消息处理：为防止SQL注入，还要防止前台出现一些具体的的报错内容。
   1. 加密处理：将使用者的登录名、用户密码等高保密级别的数据进行加密处理。。
3. XSS攻击

XSS攻击防护所使用的正则代码如下：

function stripscript(s)

{

var pattern = new RegExp("[%--`~!@#$^&\*()=|{}':;',\\[\\].<>/?~！@#￥……&\*（）——|{}【】‘；：”“'。，、？]") //格式 RegExp("[在中间定义特殊过滤字符]")

var rs = "";

for (var i = 0; i < s.length; i++) {

rs = rs+s.substr(i, 1).replace(pattern, '');

}

return rs;

}

### 4.5.3 网络拓扑

本系统采用离线模式进行网络拓扑的部署，但是需要局域网环境的交换机需要支持端口镜像功能。离线模式虽然可以检测到各类攻击，但是不能达到真正防护的作用（因为虚拟机设备无法提供双网卡的服务器，所以不能搭建透明网桥或者是透明路由的模式进行网络拓扑的部署）。离线模式的网络拓扑图如下图所示：

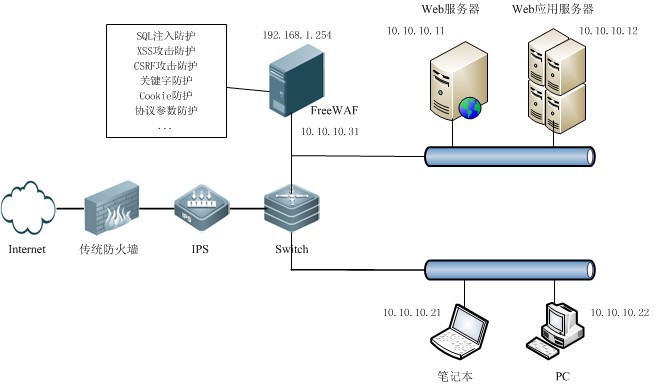


图4.1 离线模式网络拓扑

离线模式部署无需改变原有的网络拓扑结构，而只需将FreeWAF连接到支持端口镜像功能的交换机上即可，则这里可以使用其他任意一个接口接到交换机上。

## 本章小结

本章从综述、开发过程、开发环境、系统模块开发几个内容详细说明了系统开发的过程。并说明了大部分的设计思路。

# 第五章 对策分析

## 5.1 登陆测试

首先测试系统能否正常在Chrome浏览器下运行，截图如图5.1所示：



图5.1 系统登录界面

当密码输入错误是，无法正常登录。Web界面会进行提示，截图如图5.2所示：



图5.2 密码错误提示界面

登陆后的正常界面，截图如图5.3所示：



图5.3 系统主界面

## 5.2 性能模块测试

首先进行CPU使用率测试，截图如图5.4所示：

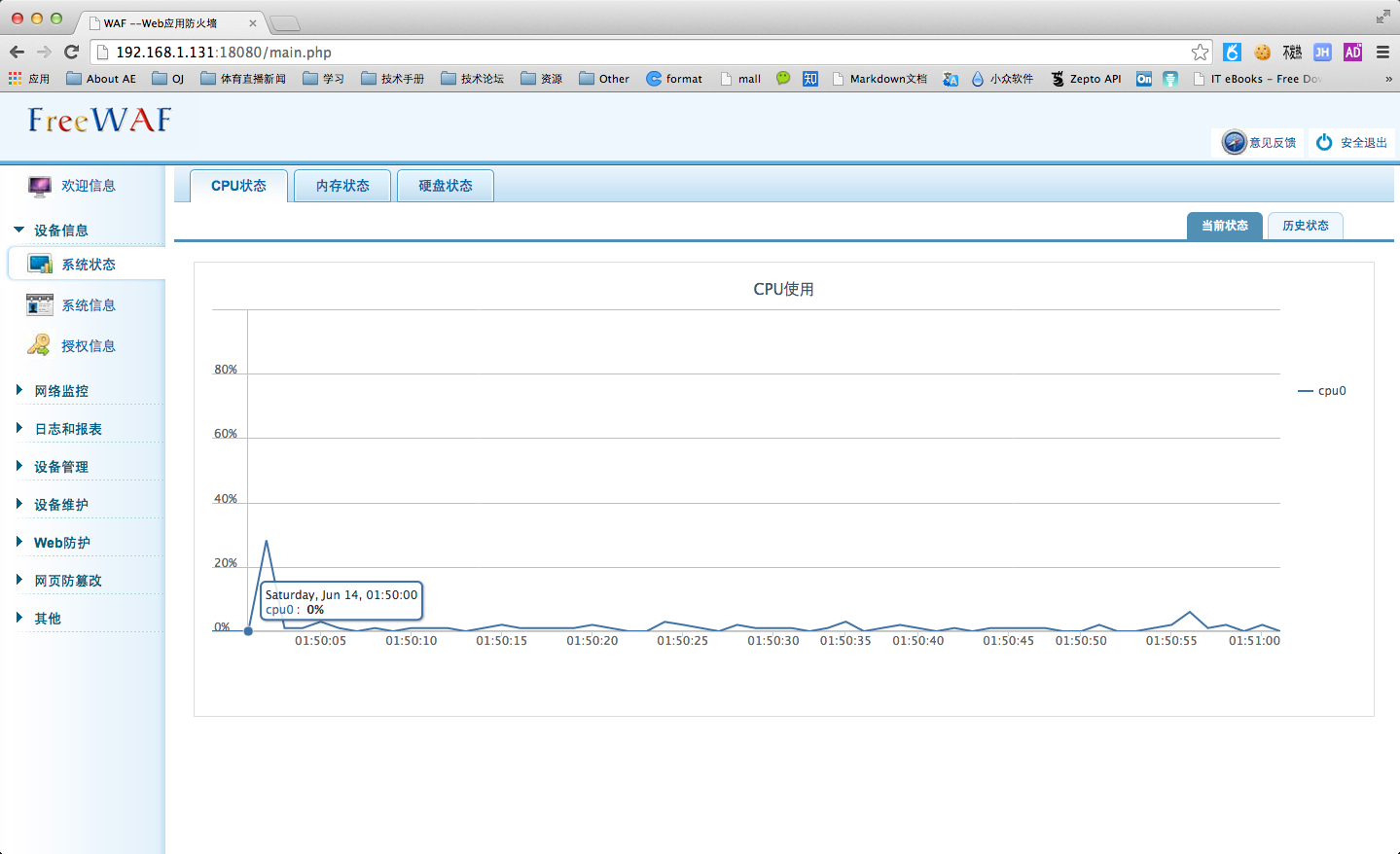


图5.4 CPU使用率功能

之后进行内存使用率测试，截图如图5.5所示：



图5.5 内存使用状态功能

之后进行硬盘使用率测试，截图如图5.6所示：

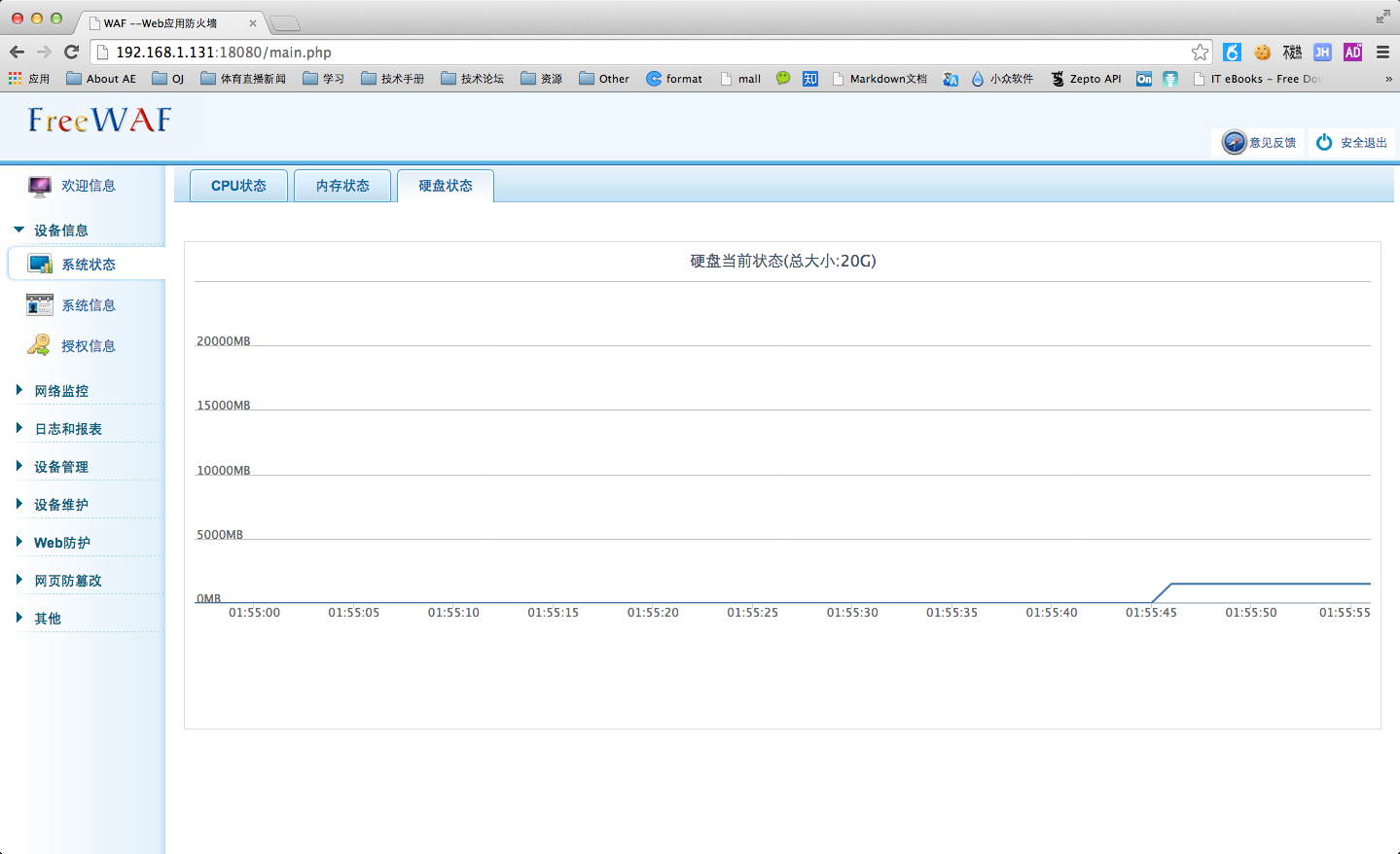


图5.6 服务器硬盘使用率功能

查看服务器综合信息的测试，截图如图5.7所示：



图5.7 服务器综合信息功能

服务器性能综合测试，截图如图5.8所示：

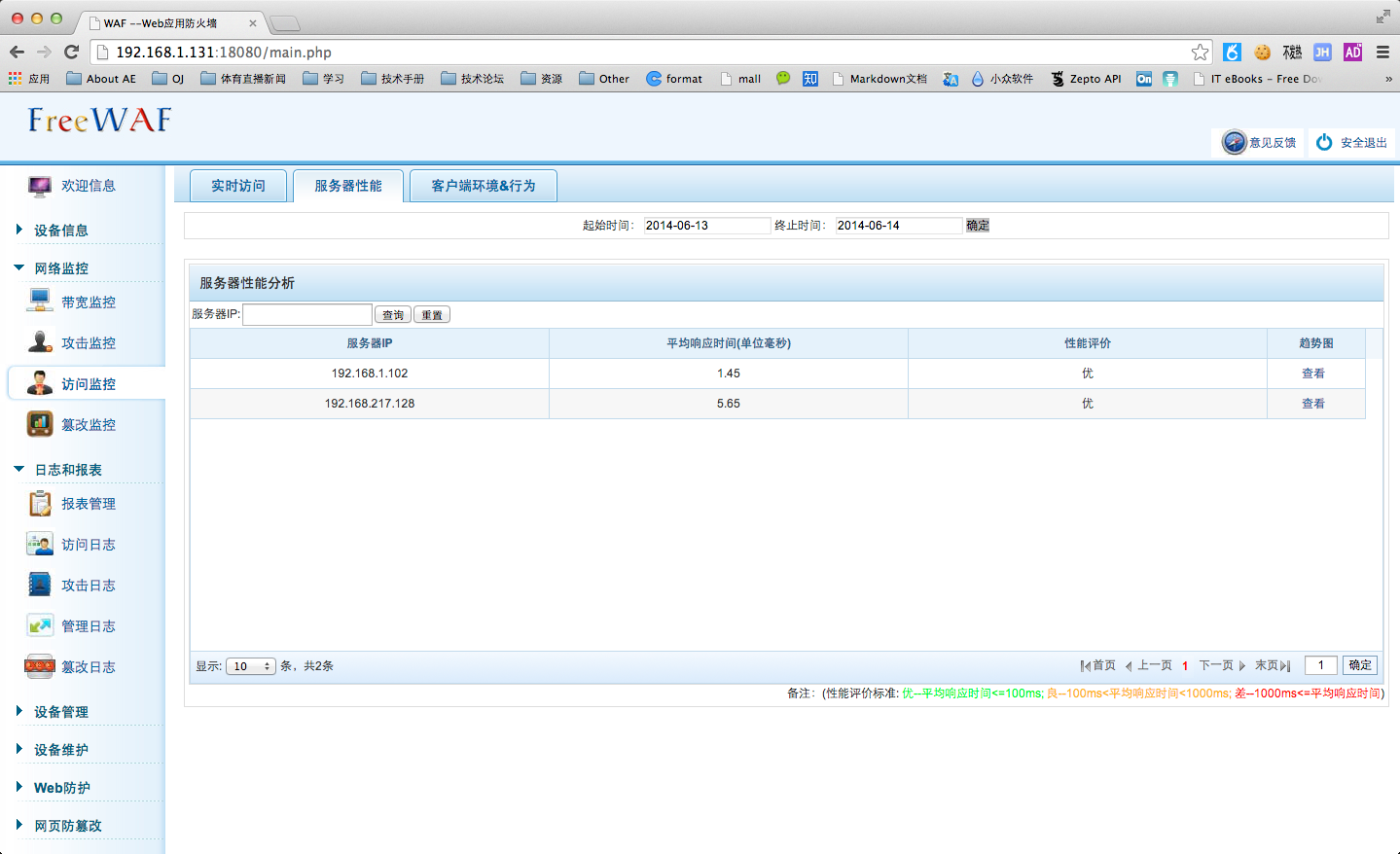


图5.8 服务器性能综合测试功能

客户端行为环境测试，截图如图5.9 / 5.10所示：

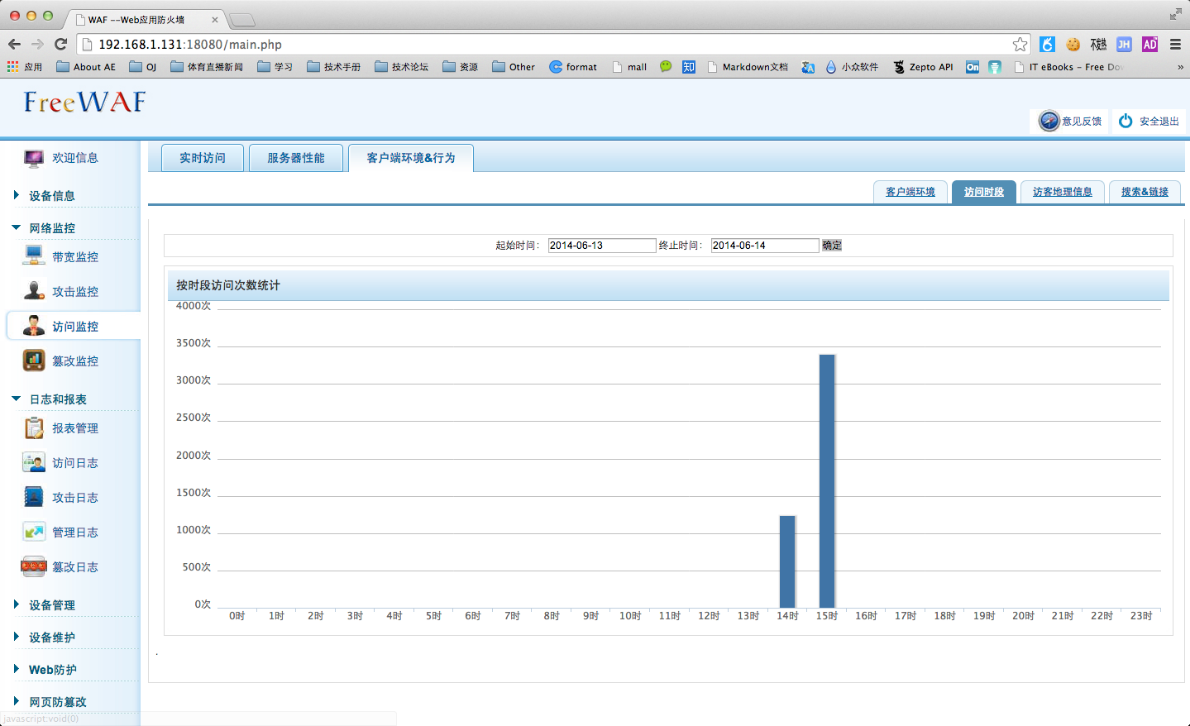


图5.9 客户端行为环境分析功能-统计

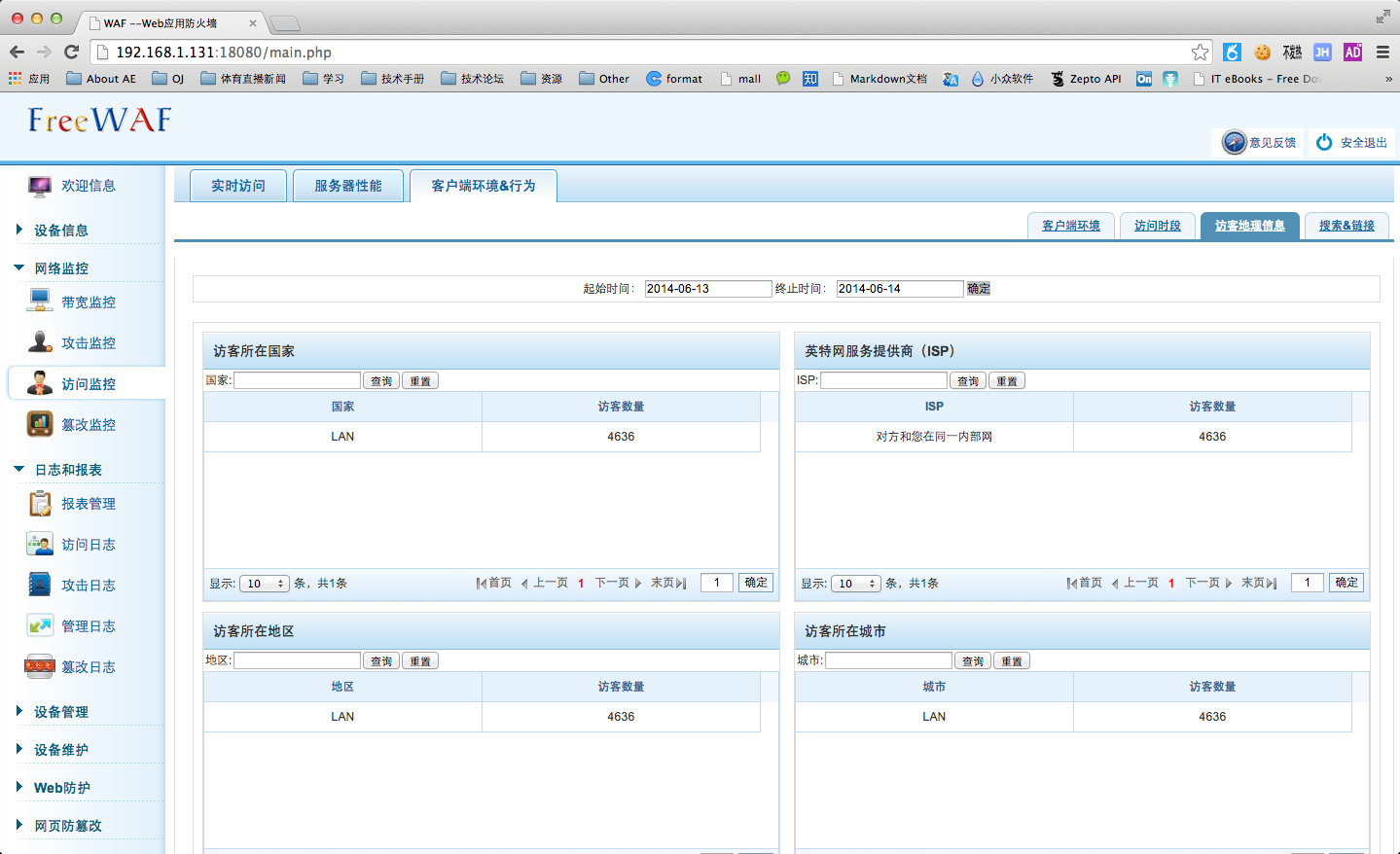


图5.10客户端行为环境分析功能-总结

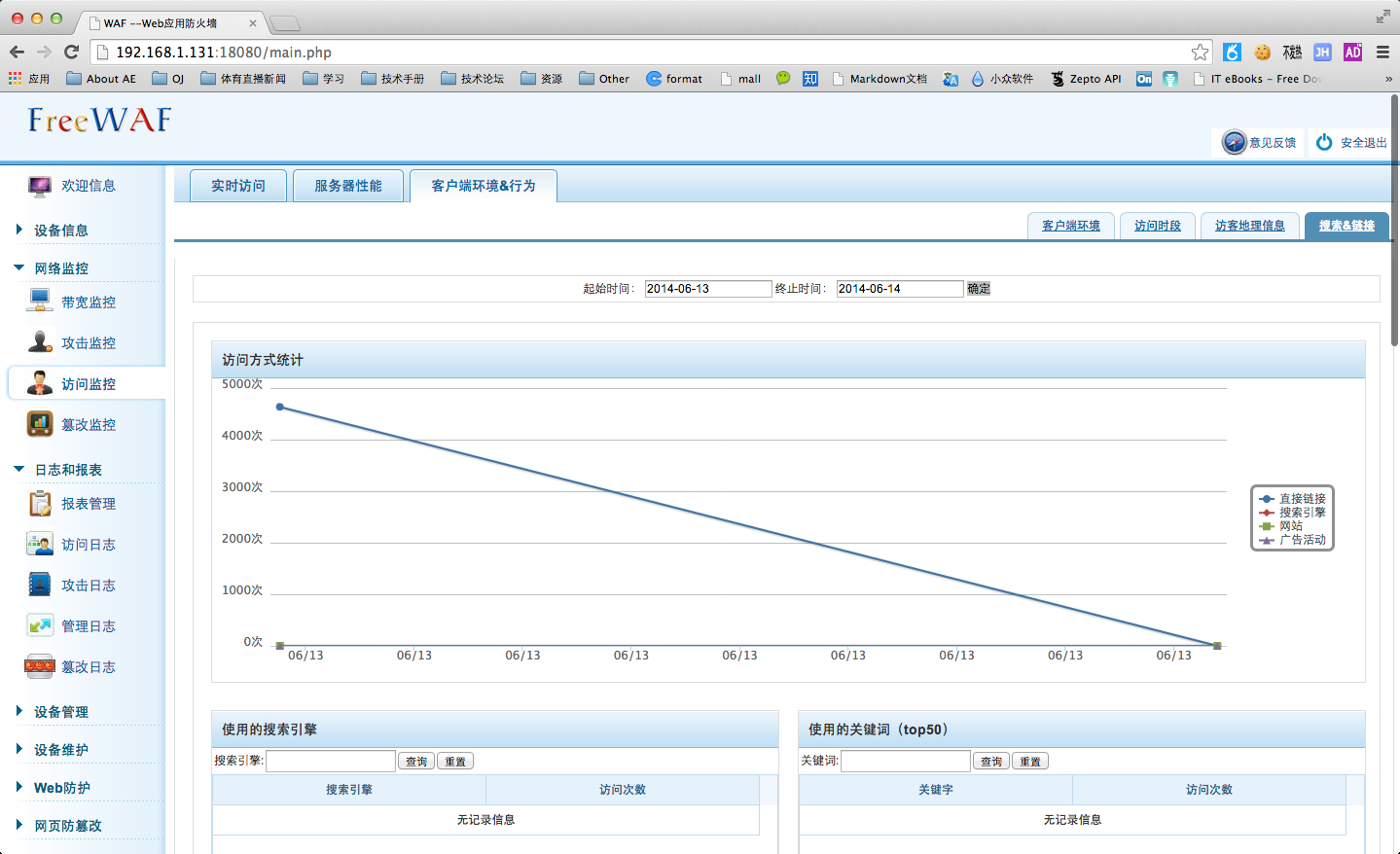


图5.11 服务器访问量统计图功能

## 5.3 攻击防护测试

流量带宽监控使用率测试，截图如图5.12所示：

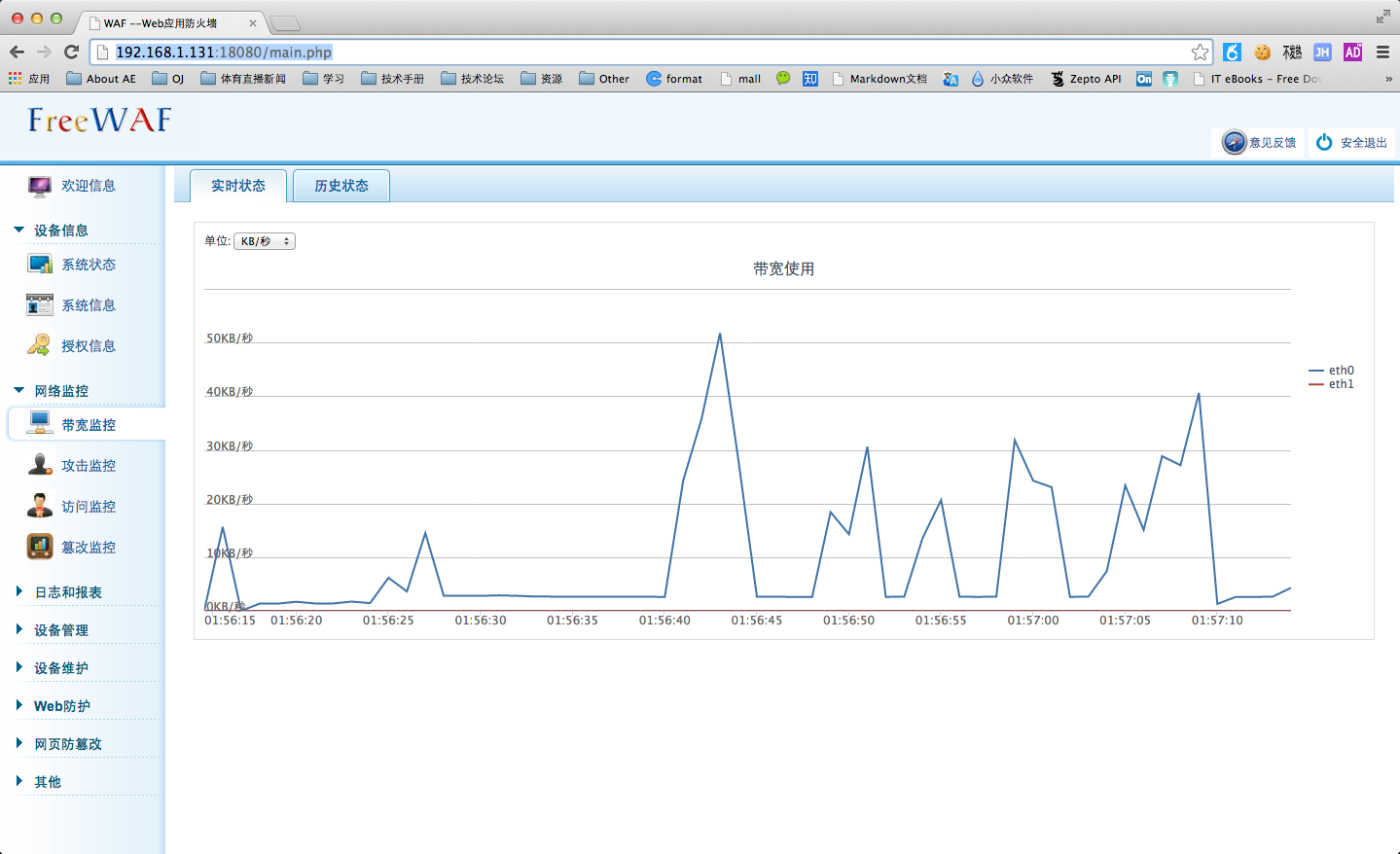


图5.12 服务器带宽使用实时监控

宽带历史状态查看测试，截图如5.13所示：

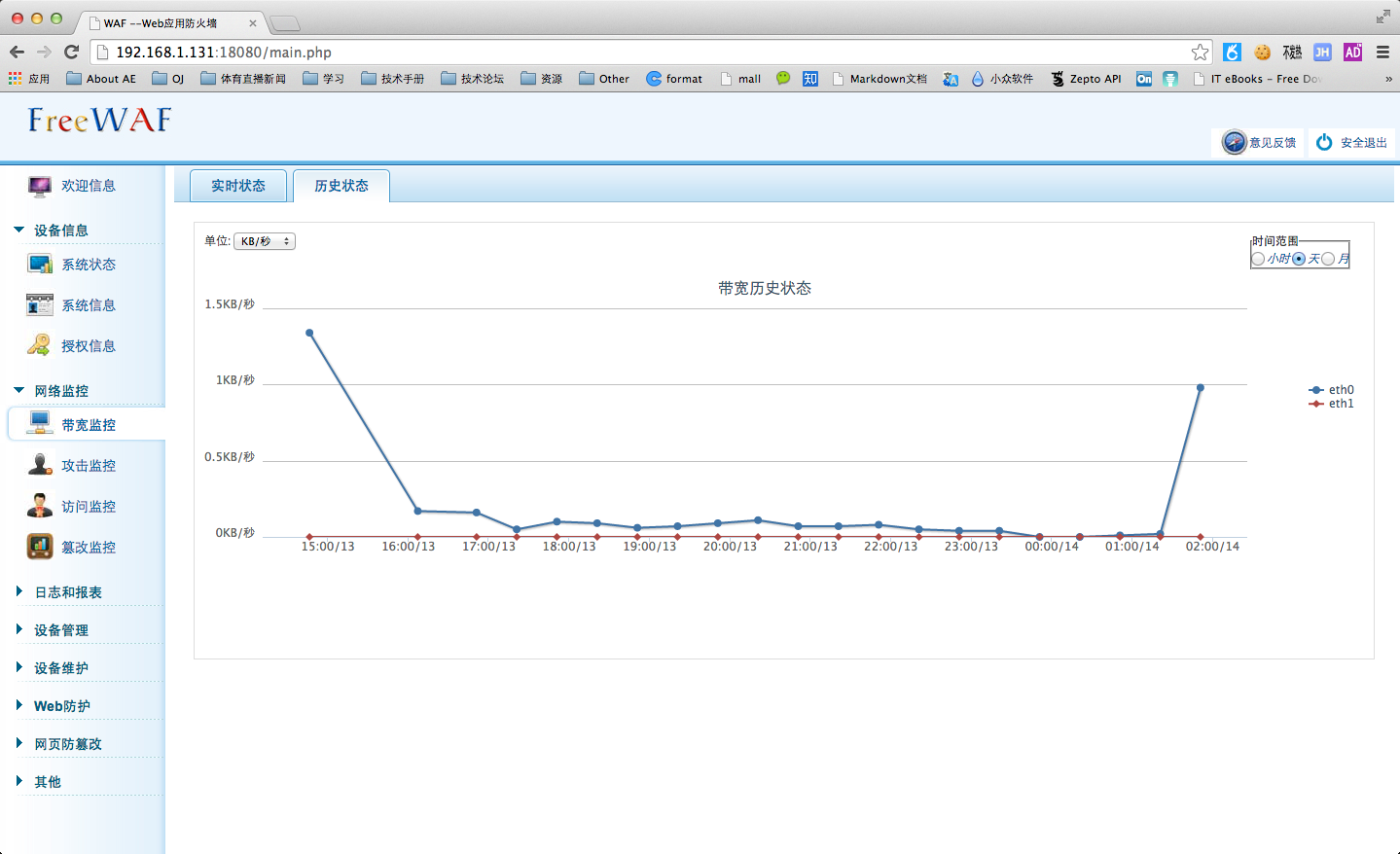


图5.13 带宽历史状态统计功能

攻击日志记录功能测试，截图如图5.14所示：

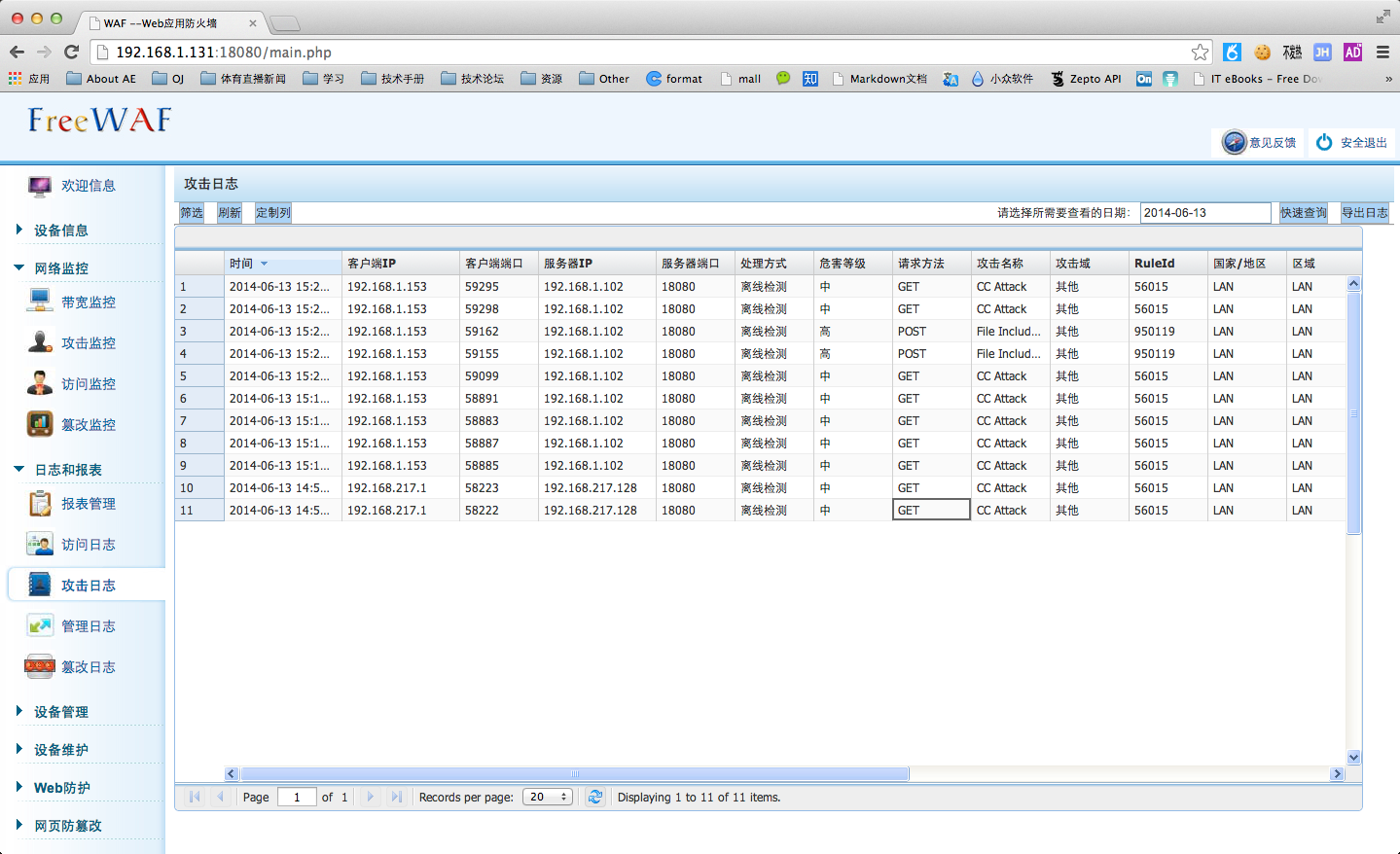


图5.14 攻击日志查看功能

## 5.4 日至报表测试

访问日志查看功能测试，截图如图5.15所示：

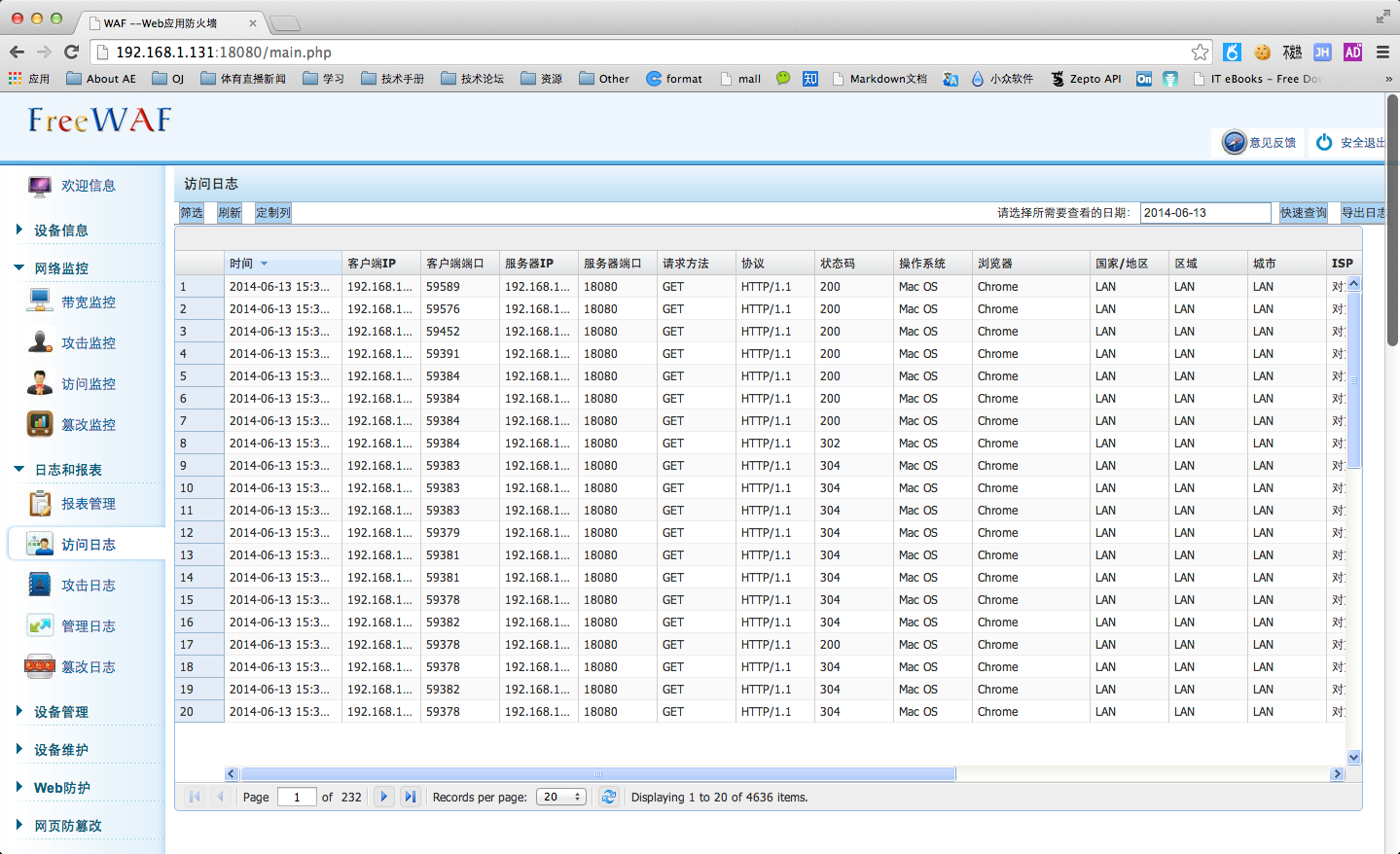
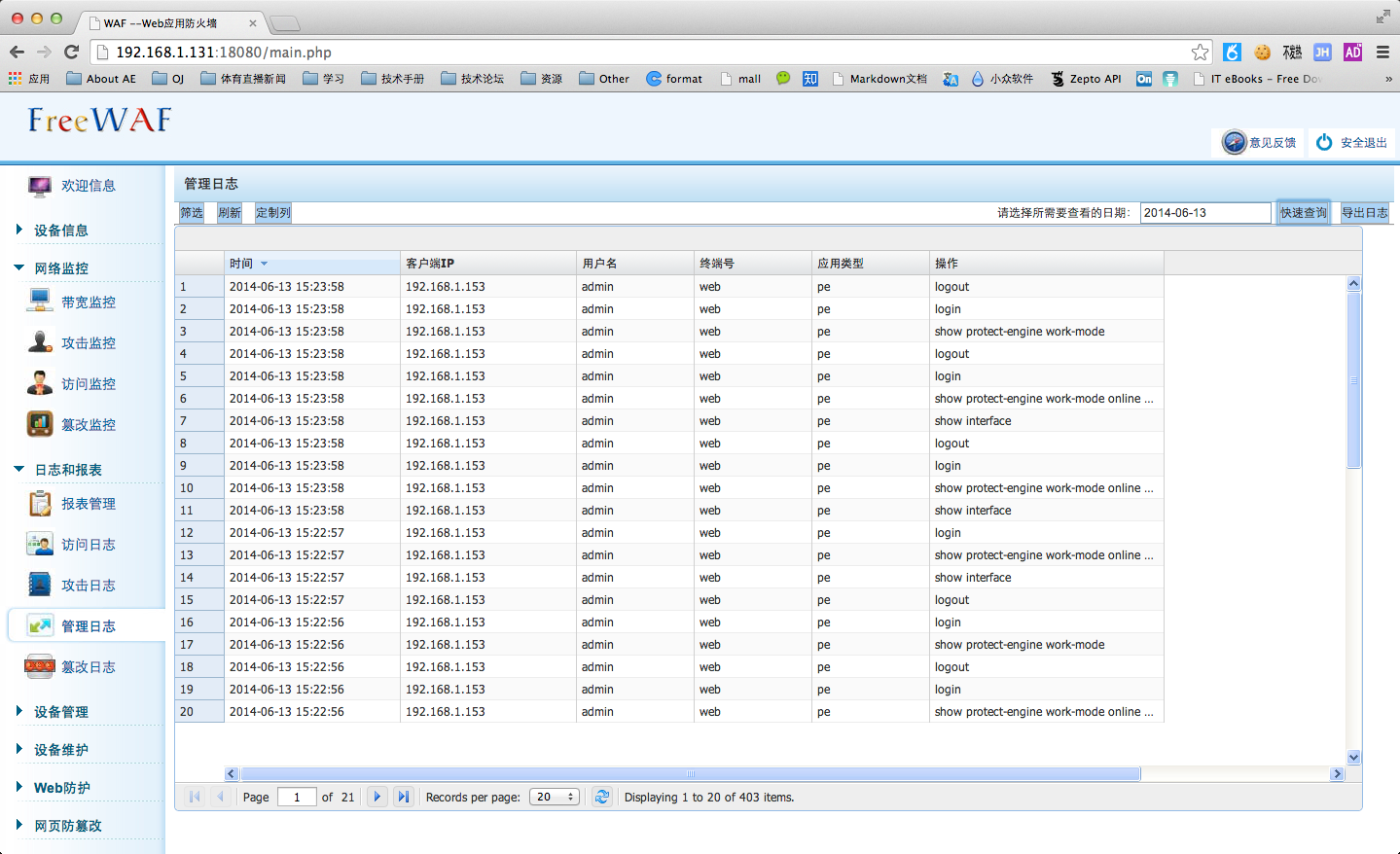


图5.15 访问日至查看功能

管理日志查看功能测试，截图如图5.16所示：



5.16 用户管理日志查看功能

## 5.5 用户管理模块测试

用户管理功能测试，截图如图5.17所示：

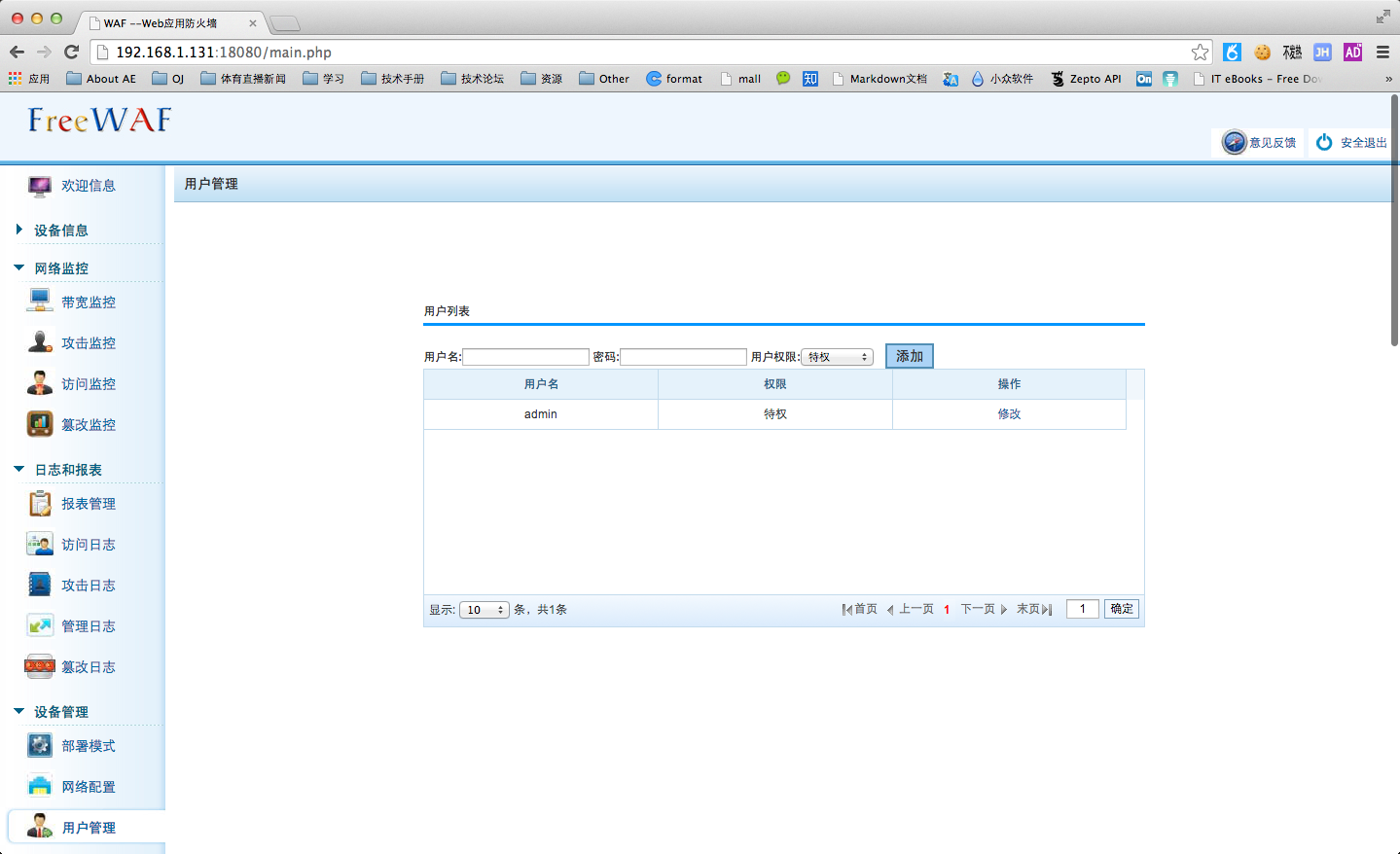


图5.17 用户管理功能

## 本章小结

本章对系统初步设计时设计的各项功能进行测试，并全部通过。美中不足的是在日至导出功能上还有导出不流畅的问题。在后期开发中修补该问题。

# 第六章 总结与展望

## 6.1 总结

本系统历时二个多月的时间开发出来，并准备在后期继续进行功能扩展的开发和系统的完善。后期投入实验室使用，为实验室的安全提供更大的高涨。

由于使用了依托开源系统的开发方式，相比独立开发等其它开发方式耗时较长。在开发本系统时，我提前对FREEWAF进行了深入的了解。包括在官网进行源码的深入分析，并且进行了大部分功能的修改，已达到本系统的需求。在源码学习期间又更加巩固了自己C语言底层命令的知识。后期在开源讨论组中也学到了很多对于开发的技能，包括部署系统，网络拓扑方面。

在系统开发这段期间，我又一次找到了自己的兴趣点，也将在今后的生活工作中给与更多的关注。体会到了在解决问题时，资源的不足和自己阅读英文文档的能力不足等主观和客观因素。

## 6.2 展望

由于时间非常仓促，防火墙系统中仍有存在着很多可以改进或者增加的功能，我将在以后的工作中不断的完善这个waf系统，为学生床戏实践中心提供一个更加完善的Web安全管理平台。

非常高兴能获得这样一个锻炼自己和学习知识的机会。在这次系统的开发过程中技术的各个方面都取得了很长足的进步。希望能在进口的发展中继续增强信息安全的基础知识学习，并在这个领域获得更多的技能。

# 参考文献

1. 王建庆. 网络安全技术教案(第1章). 豆丁网, www.docin.com.2011
2. 姜爱林. 城镇化水平的五种测算方法分析. 中央财经大学学报2002，（8）：76-80
3. 陈振宇, 宾艺. 论TCP/IP内有关层次的安全性及其提高方法. 广东水利水电, 2000
4. 冯登国,蒋建春. 网络环境下的信息对抗理论与技术,世界科技研究与发展. 2000
5. 刘孟勇,辛燕. 入侵检测技术的现状及未来,科技致富向导. 2014
6. 郭宁. IT项目管理[M]. 北京：清华大学出版社，2009
7. 王艳平,张越. Windows网络与通信程序设计[M]. 北京：人民邮电出版社, 2006
8. 王艳平. Windows程序设计[M]. 第二版. 北京：人民邮电出版社，2008
9. 郑阿奇. Visual C++实用教程[M]. 北京：电子工业出版社，2012
10. 谭浩强. VC++程序设计[M]. 北京: 清华大学出版社，2005
11. 尤文坚. 利用RAW SOCKET捕获网络底层数据包的方法[J]，广西轻工业，2007，（11）：56-57
12. 陈烽华，张代远. 基于Raw Socket技术的改进Sniffer[J]，计算机时代，2007，（5）：22-23
13. 宋漩, 张仲虎, 吕国宾. Windows2000网络封包的截获技术[J]. 计算机与现代化, 2003,(4) : 77-80
14. 谢希仁. 计算机网络[M]. 北京： 电子工业出版社, 2003
15. W.Richard Stevens[美]. TCP/IP详解 卷1：协议[M]. 北京：机械工业出版社，2000
16. 鲁斌. 网络程序开发实用安全教程[M]. 北京：清华大学出版社，2011
17. 张卫东，王伟，韩维桓. 网络流量测量与监控系统的设计与实现[J]，计算机工程与应用，2005，（32）：160-164
18. 赵英，黄九梅，董小国，刘莊. 网络流量监控系统的设计与实现[J]，计算机应用，2004，（24）：32-33
19. 王珊，萨师煊. 数据库系统概论[M]. 第四版. 北京：高等教育出版社，2006
20. Charles Petzold[美]. Windows程序设计[M]. 第五版. 北京：北京大学出版社，1999
21. 陈涛. IP网络流量监控数据图形化的实现方法[J]. 郑州轻工业学院学报，2009，（6）：62-65
22. 郑莉, 董渊. C++语言程序设计[M]. 北京：清华大学出版，2001
23. Wilton Richard[美]. Microsoft Windows软件开发环境与技术[M]. 北京：清华大学出版社，1993
24. 徐国爱, 张淼, 彭俊好. 网络安全[M]. 北京: 北京邮电大学出版社, 2007

# 致谢

在本论文最终截稿之时，首先要发自内心的，感谢我的指导老师王春东教授。王春东老师从开始选题，到前期开展需求分析和后期的系统修改中都提供了细心的指导和教育。并最终辅导我完成了这个系统的全部开发工作。

其次要感谢学院领导的指导和关怀，让我在大学四年能够学有所成，感谢常畅学长对我的毕业设计提出的宝贵建议，还要感谢家人朋友的支持和鼓励，尤其感谢在最后论文修改阶段给予我各种支持的方同学，帮我克服一个个困难。感谢理工大学图书馆给我提供了丰富的参考资料，让我为做毕业设计做了充分准备。在设计之中也参考学习了多位学者的研究文献，在各位学者的研究成果的启发之下，才能最终完成本次毕业设计。在此一并表示感谢。