面向安全漏洞管理的高校备案系统设计与实现

◆江晓莲　郑海山

（厦门大学　福建　361005）

摘要：随着高校网络安全的复杂化和校内站点类型的多样化，高校在网站管理方面面临更大的挑战。强化网站备案、提高备案信息的准确性，完善问题网站处置应急响应机制，成为一件刻不容缓的工作。为了方便校内站点的备案管理和对站点安全漏洞进行及时响应，厦门大学开发了新的备案系统。在传统备案系统的基础上，引入年审机制，及时更新备案信息；为各个备案网站建立漏洞库，以便能更好跟踪网站漏洞处理进度，建立长效机制。本文结合当前网络安全日益严峻的背景，对备案系统进行设计，并给出了具体实现细节。

关键词：备案系统；网络安全；信息化

0　引言

高校的网站类型可分为以下几种：门户网站、各部处学院网站、研究所和科研机构网站、会议网站、校内信息化应用、教师个人主页、学生社团网站、图书馆资源、新媒体平台等[2]。日益增长和种类繁多的校园网站，给网站的管理提出了更高的要求[3]。

此外，随着高校网络应用规模的扩大及复杂化，高校网络环境的开放特性，使得高校在网络安全方面面临着各种攻击和威胁，网络安全问题日益突出[3]。针对网络安全问题，除了从源头做好防范工作，更需要在发现问题的第一时间联系相关管理员进行及时处理。

根据中华人民共和国国务院令第 292 号《互联网信息服务管理办法》、中华人民共和国信息产业部令第 33 号《非经营性互联网信息服务备案管理办法 》、工信部发布的《互联网基础管理专项行动工作方案》等，强化网站备案、着力提高网站备案联系方式信息的准确性、完善违法违规网站处置应急响应机制，是一件刻不容缓的工作。备案系统的核心功能是进行网站信息和相应管理员信息的备案工作，备案信息的准确性至关重要。高校传统的备案系统主要是线上与线下结合的形式[3]，新增站点向高校备案管理部门履行登记备案手续。后期网站废弃或管理员更换，相关站点并不一定对备案管理部门报备。这种单向备案，不利于后期备案信息维护工作的开展。由于备案信息未能及时更新，当发生网站漏洞等紧急情况，无法及时联系到相关负责人。针对当前网站种类繁多，网络安全日益严峻的现状，为了更好地进行校内站点的管理工作，厦门大学信息与网络中心通过充分调研，在原有较为简陋的备案系统基础上开发了新的备案系统。基于原有备案功能，引入年审机制和漏洞管理机制，在备案的实施过程中取得了良好的效果。本论文将介绍本备案系统的功能模块和具体的实现细节。

1　备案系统设计

1.1　系统总体设计

厦门大学备案系统大量采用了开源软件。为方便和其它系统集成，操作系统基于 Linux 环境。开发语言采用 Python，使用 Django 框架。开发环境采用 Vagrant 和 VirtualBox 搭建，系统部署采用 Puppet 自动化部署工具。Web 服务器选择 Apache2，数据库使用 MySQL，缓存采用 Redis。

为兼容移动客户端，提供更好的用户体验，网站前端采用 Bootstrap 响应式布局，后台管理员界面使用 Gentelella 模板，JavaScript 框架使用 jQuery，文件上载采用 Dropzone 组件。从易用性及安全性考虑，系统对接学校统一身份认证，包括厦门大学教职员工、学生等在内的网站管理员无需注册即可使用统一身份认证登录备案系统。此外，新的备案系统使用 Chart.js、D3.js 展示备案信息的各种统计图表。

1.2　功能模块设计

新版备案系统的目标是对厦门大学各类站点进行网站备案，并结合年审机制督促管理员及时更新备案信息；对已通过备案的站点通过程序自动打开校外 IP 可访问权限；对接 DNS 系统，自动关闭未备案的僵尸和过期站点；为各个备案站点建立漏洞库，及时联系站点管理员处理相关漏洞，并对漏洞的生命周期进行跟踪；基于备案数据，生成校内站点数据的统计报表，为校内站点的管理决策提供数据支持[3]。

新备案系统用户分为三类：普通用户、院级管理员、系统管理员。

（1）普通用户功能

普通用户即各网站管理员，主要进行站点备案、站点相关设置、站点漏洞跟踪管理等工作。普通用户主要功能包括：

控制台：进行当前用户所有备案站点信息的汇总展示、站点所有安全漏洞汇总展示、待办事项提醒等。

我的个人信息：为防止备案站点联系人信息缺失，首次登录备案系统需要先进行个人联系信息的填写。个人信息填写的每一步均嵌入齐全的帮助信息。

备案：提交备案站点的相关信息及分管领导信息。备案过程嵌入齐全的帮助信息，提供当前可用域名查询，并进行是否开放校外 IP 可访问权限的设置；分管领导信息填写方面，用户可以直接选择之前已备案站点的分管领导信息，不需要重复填写，提高备案效率。备案成功后，普通用户会收到由系统自动发送的备案成功邮件。

备案项目列表：用户可查看所有备案条目，包括每条备案的当前认证状态、是否开放校外 IP 可访问权限、该备案的安全漏洞列表链接、查看该备案详情的链接等。

安全漏洞列表：通过安全漏洞列表，用户可以查看所维护站点的漏洞，包括每条漏洞的当前状态、漏洞等级、漏洞类别、漏洞来源、漏洞处理截止时间；点击相应的漏洞可进行漏洞详情查看及漏洞处理。这样，就为各个站点建立了漏洞库，实现网站安全漏洞的通知、确认和处理均在备案系统进行，方便站点漏洞的跟踪及历史信息的保存。此外，系统会将漏洞的进展对用户进行邮件推送，以提醒用户及时处理漏洞。

提交管理员权限移交申请。

（2）院级管理员功能

院级管理员除了拥有普通用户的功能外，还增加以下权限：

查看学院内所有站点备案列表。

查看学院内所有安全漏洞项目列表。

审核学院站点中管理员权限移交申请。

查看学院内所有备案站点统计报表：按月新增站点、活跃站点、学院站点开放校外访问权限的比例、漏洞类型分布、漏洞处

理情况统计等，且统计数据以图表形式进行直观展示。

（3）系统管理员功能

系统管理员通过备案系统对新增备案站点进行审核，对旧站点进行年审工作，并定期清理僵尸站点。

备案搜索管理和用户搜索管理：方便系统管理员进行相关站点或相关管理员信息的定位。

系统管理员使用备案系统进行漏洞录入、通知、跟踪、及修复验证。

检查 DNS 和备案系统数据，对备案站点进行梳理，发现已备案的僵尸站点，为备案站点的年审工作提供依据。

查看普通用户和院级管理员操作日志。

通过控制台查看全校备案站点的统计：包括校内已认证备案的站点数目、未认证备案的站点数目、需年审站点数目、按月新增站点统计、按学院网站个数分析、开放校外 IP 访问权限的站点统计等。查看全校站点漏洞数据统计、分析：根据漏洞类型、漏洞等级、漏洞状态等提供全校安全漏洞统计图表；按网站、学院统计漏洞数最多的网站。通过统计报表，使系统管理员对校内站点情况有更直观的了解，方便系统管理员更好地进行全校站点管理。

1.3 数据库设计

备案系统的主要数据表定义如表 1 和表 2。

表 1 备案站点信息表

字段名	字段类型	长度	说明
id	整形，自增长		关键字
creator	整形		关联备案者用户信息
license_name	字符型	200	备案站点名称
identity_type	枚举类型	200	网站性质
identity_name	字符型		所属单位
license_type	枚举类型	200	网站类型
url	字符型	200	URL 地址
ip	字符型	200	IP 地址
is_web_external	布尔型		是否开放校外 IP 可访问
add_date	时间		创建日期
annual_expired_date	时间		年审过期日
manager	整形		关联分管领导信息
status	枚举类型		备案状态

表 2 漏洞信息表

字段名	字段类型	长度	说明
id	整形，自增长		关键字
license	整形		关联备案站点 id
title	字符型		漏洞名称
priority	枚举类型		漏洞等级
issue_type	枚举类型		漏洞类型
source	字符型		漏洞来源
source_url	字符型		漏洞来源 URL
content	字符型		漏洞详情
suggest	字符型		修复建议
Filename	字符型		附件文件名
status	枚举类型		漏洞当前状态
add_user	整形		关联添加人
add_date	时间		添加时间

1.4 网站流程设计

（1）备案流程如图 1 所示。

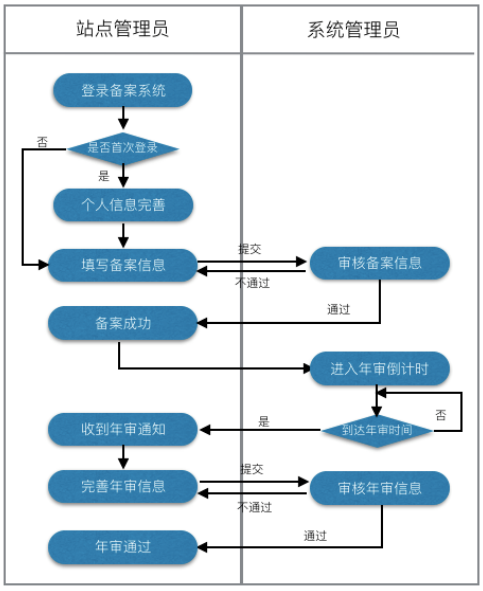

图 1 备案流程

（2）安全漏洞生命周期管理流程如图 2 所示。

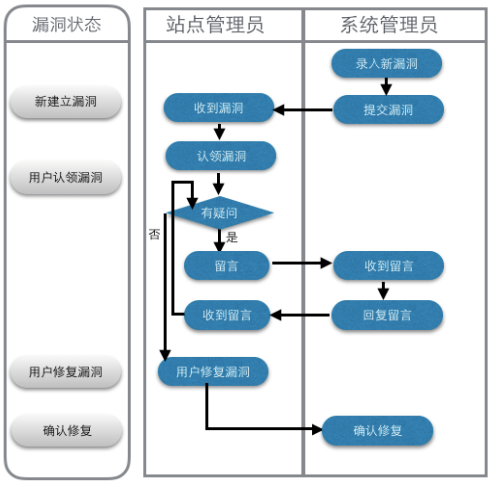

图 2 安全漏洞生命周期管理流程

2 部分技术实现细节

2.1 PDF 文档下载

为方便用户打印出备案信息交由领导盖章和单位签字，备案系统提供给用户预览打印效果和下载 PDF 打印功能。为了方便开发人员修改打印样式和重用代码，通过 Django 的模板机制，把需要预览的 HTML 和 PDF 统一成一个模板文件，在模板内编辑样式，通过模板引擎替换字符串，并渲染为 HTML 文本，最终根据用户是预览或者下载输出不同的格式。

```
# 构建 HTML 和 PDF 统一的样式
beian_detail_content = render_to_string('licenses/detail.html', {'license': license})
# 如果不是下载 PDF，则直接输出 HTML
if not download:
return HttpResponse(beian_detail_content)
# 如果是下载 PDF，通过 weasyprint 模块把 HTML 输出成 PDF
response = HttpResponse(content_type='application/pdf')
response['Content-Disposition'] = 'attachment; filename="xmu_beian.pdf"'
```

```
from weasyprint import HTML
response.write(HTML(string=beian_detail_content).write_pdf()
)
return response
```

2.2 与 DNS、防火墙联动

为了使得全校尽快地实现所有站点的备案，我们在实践中通过宣传、邮件群发、技术处理等多种手段促进备案进程。在一定时间过后，通过跟 DNS 和防火墙系统联动，自动封禁未备案站点。任何人访问未备案站点任何页面均会得到该站点未备案的通知，并引导用户到备案页面进行备案。具体实现为修改 DNS BIND9 系统的配置文件。BIND9 的配置文件为文本文件，每一行对应一条 DNS 记录。对每一条 DNS 记录，均查询是否通过备案，如果通过备案，则写入已备案配置文件，否则写入未备案配置文件。通过修改 DNS 配置，不再引用原先的记录文件而是引用新的拆封过的 2 个文件，达到封禁未备案站点的目的。同时继续保留原先记录文件，每天定时更新解封新备案站点。具体 Python 代码为：

```
with open('db.xmu.edu.cn.all_sites') as f:
content = f.readlines()
for l in content:
rec = l.rstrip(' \t\n ').split()
if is_beianed(rec[0]):
write_to_file(‘db.xmu.edu.cn.beianed’, rec[0])
else:
write_to_file(‘db.xmu.edu.cn.not_beian’, ‘%-20s CNAME ban_server' % rec[0])
```

BIND 配置文件修改为：

```
;注释掉原先记录文件，更改为引入新的拆封过的文件
;$INCLUDE /etc/bind/db.xmu.edu.cn.all_sites
$INCLUDE /etc/bind/db.xmu.edu.cn.beianed
$INCLUDE /etc/bind/db.xmu.edu.cn.not_beian
```

经过以上修改，极大加快了全校备案的进程。

3 结束语

厦门大学新备案系统在传统备案功能的基础上，引入年审机制，着力提高备案站点信息的准确性，为及时应对站点安全问题提供基础；建立备案站点漏洞库，有效对站点安全漏洞进行跟踪、处理，建立长效机制。通过在全校开展备案工作，截止到 2017 年 2 月，厦门大学新备案系统通过和 DNS、防火墙系统联动，封禁未备案站点的域名解析，实现短时间内将 500 多个站点登记了管理员和分管领导信息，识别出 100 多个僵尸和过期域名，为下一步的网站漏洞扫描和安全管理提供了坚实的基础。通过引入的新的漏洞管理功能，使得漏洞整改过程清晰可查，漏洞响应时间加快，漏洞平均处理时长也较以往有所减少。今后备案系统的开发方向可整合更多安全设备信息，例如与漏洞扫描设备和 WAF、IPS 等安全设备联动，为站点管理员和学校提供各个站点和全校更加清晰的安全态势分析。

参考文献：

[1]JEFF FORCIER. DJANGO WEB 开发指南[M].机械工业出版社, 2009.

[2]郑海山.高校校内网址导航站的研究与实现[J].中国教育信息化, 2014.

[3]简思远. 基于 SSH 架构的高校校园网站备案系统的构建[J]. 福建电脑, 2010.

[4]刘兰娟.高校网络系统的安全管理策略[J].计算机工程, 2003.

[5]李宗峰.校园网络安全问题及对策研究[J].网络安全技术与应用, 2009.

[6]马文海.高校网络存在的安全隐患与应对措施研究[J].中国教育信息化, 2016.

[7]徐涛.深入理解 Bootstrap[M].机械工业出版社, 2014.

[8]陈晨,邵叶秦.数字化校园基础平台信息安全问题及对策[J].网络安全技术与应用, 2016.

（上接第 147 页）

服务器备用策略。一台服务器出现故障可以快速的启动另外一台服务器服务，提高系统可靠性；（4）要做好软件以及系统的备份问题，如采用冻结网络恢复软件进行数据保护，无需购买其他设备，就可以还原，进行数据的安全使用；（5）加强硬件管理工作。要保持机房打扫工作。同时要重视防火、 防水、 防盗等安全工作，平日需要做好例行检查，以便能及时发现问题及时处理；（6）机房线路接入定期更新处理，对一些老化的以及接触不良的线路及时进行处理，同时在日常使用中对学生进行引导，避免破坏性的操作。

4 结论

现代技工院校教学向信息化发展，传统的机房管理和维护工作变得愈加繁重，本文探讨了基于云计算的技工院校计算机机房管理和维护模式，通过对现存的机房管理的问题进行总结，研究云计算技术的特点，将云计算技术引入到技工院校计算机机房管理和维护中，其优点有：

（1）节约成本。其一是现有机房的一些淘汰的计算机可以重新得到使用，提高其应用率。其二是减少了系统以及相应软件的购买成本，只需购买主服务器的系统以及软件即可。其三是减少了硬件设备的购买成本，无需购买高性能的服务器和存储设备。其四是无需配备更多的管理人员，降低了人力成本。

（2）提高运行效率以及可靠性。其一是系统以及软件不需要每台电脑都安装，只需安装到服务器上即可。其二是可以实时监控病毒以及非法程序，能够及时的对计算机运行时遇到的状况进行处理。其三是使用云计算可以提高资源共享利用率，让资源更加高效的互相交流。

参考文献：

[1]洪伟珍.技工学校云计算实验室的建设研究[J].科技风, 2016 .

[2]贾艳玲.技工学校计算机教学现状分析及应对策略探讨[J]. 亚太教育, 2015.

[3]罗国玮,兰瑞乐.基于云计算的高校科研实验平台构建研究[J].实验技术与管理, 2012.

[4]叶栋.技工院校计算机教学中一体化教学的运用浅谈[J].中国教育技术装备, 2015.

[5]肖吉英, 陈凤美, 赖宏图.基于云计算的高校公共计算资源整合应用研究[J].中国科教创新导刊, 2014.