厦门大学
备案系统记录高校网站安全信用

利用漏洞全生命周期管理制度建立网站的安全信用记录体系，通过实施备案和漏洞管理，使得高校对校内网站有了更清晰的认识。基于备案和一系列第三方系统联动和技术检查措施，整体安全管理方法结合技术、管理和人工手段，可以极大提高高校在网站安全管理的能力，提高高校网站整体安全性。

文 / 郑海山 江晓莲 许卓斌 萧德洪

随着《中华人民共和国网络安全法》的出台，高校对网络安全也越来越重视，工业和信息化部的《互联网信息服务管理办法》，《非经营性互联网信息服务备案管理办法》和公安部的《计算机信息网络国际联网安全保护管理办法》都强调了备案的重要性[1]。备案是高校网站安全管理的基础，只有摸清了家底，才能对网站安全做好管理工作[2]。摸清家底除了确定网站的运维部门和使用部门等静态的管理信息外，还应当包括网站动态方面的一些信息，比如网站的 IP（Internet Protocol，网际协议）地址、DNS（Domain Name System，域名系统）、物理位置、连接的交换机、访问量和性能指标等等。由于高校域名一般为 .edu.cn 结尾，所以在工信部和公安部的备案只能对整个学校的三级域名进行备案，学校内部的四级域名自行备案，各个高校也都建立了自己的备案管理机制[2–4]，然而目前部分高校的网站管理还存在一些问题。

高校网站安全管理存在的问题和解决思路

站点分布情况复杂

高校网站是域名备案主体为学校的网站，校内备案主要的目的在于网站遇到安全事件后，第一时间可以联系到用户或者由信息与网络中心紧急处置。由于一个网站对外提供服务涉及到域名和 IP 地址两个基本条件，根据这两个条件的不同，处置相应会存在表 1 所列的几种情况。

目前大部分高校以上几种情况还处于并存的现状，甚至对哪些站点属于哪种情况还未调查清楚。建议做好备案工作，从技术手段识别出以上各种情况，并要求备案主体为学校的所有网站均应迁入校内，接受学校的统一安全防护和管控。

官方网站没有与信息系统分开

部分二级学院和部门的官方网站和信息系统紧密结合在一起。官方网站为宣传性质的网站，一般只有新闻发布功能，程序逻辑较为简单，访问受众大，可以生成静态页面增加安全性，而信息系统较为复杂，为动态网站，程序逻辑复杂，安全隐患多，访问者较少，在重大活动时期可限制校外访问。两者部署在同一台服务器会导致任何一个被攻击均可能影响另外一个。所以应当把官方网站和信息系统分开部署，使用不同的安全措施进行保护。或者将官方网站迁移到统一部署的网站群内提高安全性。

未采用信息系统支撑备案

备案过程使用线下的纸质流程、电子邮件上报、流程引擎，

表 1 高校网站分布和处置情况

域名注册提供商	IP 地址接入商	紧急处置方法	紧急处理时效性
学校	学校教育网	停止 DNS 解析、切断 IP 地址网络访问	快速
学校	互联网云服务	停止 DNS 解析	慢，DNS 解析有一定延迟
互联网域名提供商	学校教育网	切断 IP 地址网络访问	快速
互联网域名提供商	互联网云服务	无法直接处置	较慢

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

但是没有对数据做沉淀等手段，使得备案数据无法电子化，变更无法关联，统计查询困难。应当有功能较为完备的信息系统支撑备案工作。

网站安全信用记录缺失

网站过往有发生过何种安全漏洞无从得知，网站漏洞管理采用电话和邮件沟通，导致过程和处理结果跟踪效果较差，无法进行考核。未采用自动化工具，导致对有安全隐患的网站的保护性封禁不及时。在诸如通用软件漏洞出现时，无法根据历史漏洞情况对使用了特定通用软件的站点进行主动提醒，多个安全管理人员之间无法有效协作。应当利用系统建立网站的安全信用记录，对于多次出现安全漏洞的网站应主动要求整改。

管理办法无法得到有效的执行

信息与网络中心出台了各种网站安全管理办法，然而由于缺少技术手段，导致管理办法成为一纸空文。没有系统的支撑，开启和封禁有安全隐患的网站较为随意，易受用户影响。

虚拟主机生命周期管理缺失

信息与网络中心一般会为二级学院提供诸如虚拟主机或虚拟机的建站平台支持，然而这些资源往往只有申请，没有退出机制，导致变成僵尸站点。部分网站由学生开发，等学生毕业后无人维护。某些会议网站，申请了虚拟主机空间后，会议承办结束后不再使用，但是不会通知信息与网络中心。统一部署的网站群安全性能较高，然而也存在管理员账户密码泄露等问题。

针对以上问题，厦门大学建立了备案系统[5]，使用技术手段结合管理政策和人工操作，实现了对网站安全较为清晰的管理。本文将介绍备案系统和备案系统使用到的部分技术手段，和厦门大学在首次备案梳理、日常管理、基于备案数据和其他系统对接中的网站安全管理实践。

备案系统功能介绍和执行

备案系统主要功能为登记所有网站的运维负责人和分管领导，并对内部自查或互联网发现的网站漏洞，在备案系统内实现漏洞通知、认领、讨论、修复、确认等一系列全生命周期管理流程[5]。并基于备案基础数据，对接了近十个第三方系统，对整个学校网站进行分析和检查。同时引入年审、常态化检查等管理机制，建立网站安全信用记录，以此信用记录决定网站在重大时期的开放。

和第三方系统对接方法

备案系统需要和各个系统对接，有些系统使用了可远程访问的数据库，比如 MySQL，这些可以通过直接数据库连接获取信息。有些系统提供 API（Application Program Interface，应用程序接口），可通过 Python 的 suds 或者 urllib 模块获取信息。有些系统只有网页页面，可以使用类似 PhantomJS、Selenium 等网页自动化工具模拟登陆并获取信息。有些系统可以导出结果到 Excel 等格式，可通过定时手工方法导入到系统获取信息。如果以上方法都没有，可先手工操作，等条件成熟后再自动化获取信息。

管理员控制台

梳理出备案数据后，基于备案基础数据，结合第三方系统，展示管理员驾驶舱，通过图表展示校内备案总数、备案人员总数，站点总数、校外域名总数等各种统计信息，方便管理员对校园网内所有网站进行安全态势分析。厦门大学做了以下识别：

(1) 备案人高危识别：列出备案数较多的人，重点关注。备案数目较多，有可能该用户确实负责很多网站或系统，也可能说明该部门统一由某个人负责备案，真正各个网站的负责人可能还有其他人，这种情况会导致漏洞无法及时传达到具体负责人。所以，出现这种情况应督促具体负责人备案。

(2) 服务器高危识别：列出架设较多网站的服务器。一个服务器开设了太多网站，多个站点安全隐患会互相影响。应督促管理员对网站根据安全级别进行分离。

(3) 识别过往漏洞最多的站点和管理员。

(4) 域名注册商和接入服务商识别。识别出接入在校外、校内、数据中心外的服务器，督促尽快托管到信息与网络中心机房。

(5) 网站首页变化量识别。识别一段时间内首页变化量少于某个阈值的网站，督促管理员更新站点或者关闭站点。

(6) 识别非标准部署的网站。非标准部署的网站包括使用 IPv4 直接提供网站服务和 HTTP（Hypertext Transfer Protocol，超文本传输协议）端口开放在非 80 端口的网站。非标准部署网站记忆困难，搜索引擎优化程度较低，不支持 IPv6，今后也无法提供 HTTPS（Hypertext Transfer Protocol Secure）服务，应督促尽快申请域名。

由于管理员态势分析必须经常打开各个不同的系统，所以厦门大学对管理员经常打开的系统链接做了聚合，方便管理员打开，常见链接包括 WAF（Web Application Firewall，Web 应用防火墙）、IPS（Intrusion Prevention System，入侵防御系统）、防火墙、堡垒机、校内各平台控制面板、互联网各种漏洞平台、监控平台等地址链接，使得备案系统成为安全人员的门户。

梳理备案过程

备案从无到有的过程，不能简单的一刀切，虽然不备案就禁止访问会加快备案进程，然而网络安全和信息化是相辅相成的。

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

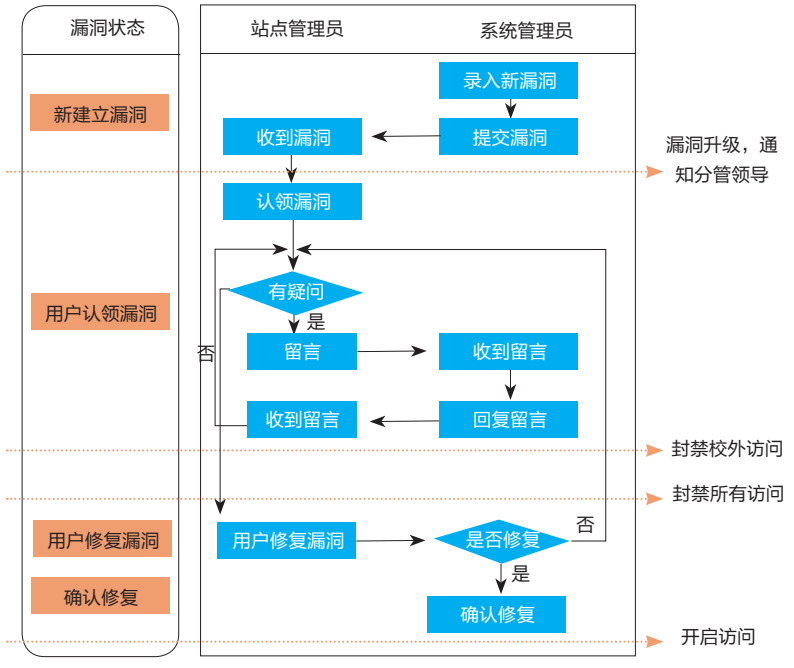

图 1 漏洞全生命周期管理和各个时间节点

安全是发展的前提，发展是安全的保障，安全和发展要同步推进[6]。为了最大限度不影响业务的正常开展，我们采用了以下较为柔性的备案推进过程：

(1) 多宣传。备案系统开发完成后，通过办公自动化发文和 QQ 群沟通，督促各个网站安全责任人在截止时间前备案。

(2) 减少对业务的影响。为防止在真正截断网络访问之后影响业务的开展，除了通知以外我们还通过查询 DNS 解析量、站点日志量、厂商的安全设备识别出来的站点信息防止重要域名被误删除。对于访问量较大的站点，额外通过电话提醒。

(3) 提供通知页面。截止时间到了对所有没有备案的域名直接解析到通知页面，在通知页面提示备案启动的时间点、目前进度和备案方法。减少用户投诉未收到通知和不知道网站无法访问的原因。

(4) 回收域名和虚拟主机空间。确定时间点，没有备案的站点，回收域名和虚拟主机空间。

漏洞全生命周期管理

漏洞全生命周期管理和各个时间节点如图 1 所示。一旦管理员从多个途径接收到漏洞信息后，判断为非误报，录入系统进入流程。红色虚线为各个重要时间点，如果未在一段时间内认领漏洞，漏洞会升级发送邮件给分管领导。在一段时间内未修复，则只允许校内访问。如果是高危漏洞在一段时间内未修复，则封禁校外访问或直接关闭网站。

漏洞来源有以下几种被动和主动来源：

(1) 互联网漏洞平台。在所有较大的互联网漏洞平台申请账户，登记邮件地址，做到白帽子录入漏洞后第一时间收到漏洞通知，并录入系统，做到有漏洞必确认必修复，无法修复的关闭站点。有些漏洞平台还提供了 API 数据开放接口，对于这种漏洞可直接预填信息减少管理员的工作量。

(2) 上级部门通知。

(3) 使用漏洞扫描设备或者开源软件主动对所有备案系统的网站进行漏洞。根据扫描到的漏洞分发到各个站点。

(4) 主动恶意代码检测。对信息与网络中心有管理权限的虚拟主机或者虚拟机定期进行恶意代码检测。可使用杀毒软件查杀病毒，在虚拟化层面部署无代理模式的检测恶意代码软件检测。在校园网出口部署防恶意代码防火墙，定期检查拦截日志录入备案系统。

(5) 通用软件漏洞或蠕虫。一些站点使用了诸如 PHPCMS、WordPress、Drupal 等 CMS 系统或者 Struts2 等通用软件，在这些通用软件有漏洞时根据历史记录找出有可能使用了该通用软件的站点，通过 PoC（Proof Of Concepts，效果验证）检测后录入备案系统。

(6) 定期查看 WAF 和防火墙日志，找出被 WAF 拦截的地址，识别出可能存在漏洞的站点，录入备案系统。

技术实现细节

站点的识别

在备案梳理过程和日常管理中，有些 IP 地址通过了备案，开放了校外访问权限，于是管理员又在上面开设了其他没有备案的网站。有些站点以教学科研用途备案了，然而后期网站建设内容与备案用途不一致，这时需要识别出校内真实有多少网站在对外提供服务，需要识别出真实网站是否跟备案信息一致。对于这种情况我们采取多种方法识别：

(1) 对所有备案网站，自动获取 IP 地址，域名，Web 端口开放情况，网站首页标题，与备案系统内数据一并表格显示，方便管理员排查。

(2) 根据 DNS 权威服务器查询日志记录找出访问量较大但是没有备案的网站，人工通知。技术实现为：由于我们的 DNS 权威服务器查询日志记录保存在 Elasticsearch 数据库内，通过查询找出阈值超过一定数值的域名，检查备案情况，

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

列出。

(3)某厂商设备通过镜像校园网出口的Web流量到设备上，可以识别出流量中提供Web服务的服务器IP地址，Web链接地址等信息，通过手工导出导入到备案系统内，与备案系统内数据一并表格显示，可以发现一些直接通过IP地址提供Web服务和把校外域名解析到校内IP地址的网站。

内部IP地址的数据

厦门大学目前部分学院还有自有机房，部分网站使用虚拟主机或者网站群，通过维护校内IP地址段列表，根据备案地址通过DNS解析获取到的IP地址可以识别出网站是否在校外、是否在数据中心内、是否在学院自有机房、是否已经迁移到网站群、是何种类型虚拟主机等信息。任何一个备案网站的接入可清晰识别。

虚拟主机

厦门大学提供有多种类型的虚拟主机空间，有些网站由于更换空间或者已经下线，然而还保留在旧虚拟主机内。通过在虚拟主机服务器上运行VBScript或Python脚本，对IIS或Apache2，获取配置文件的所有开设的站点，查询wwwroot目录占用空间大小、DNS解析情况、查询访问日志，如果检查到可能已经不再使用，通知用户备份完删除网站。而对于网站群，则移动到归档网站，并禁止管理员登录。

出口防火墙封禁

厦门大学把服务器网段和用户网段分开，默认关闭校内所有IP地址段的校外HTTP访问，用户网段不能对外提供Web服务。服务器网段在备案后IP地址才开放对外访问。由于使用的防火墙设备无自动化接口对接，所以采用了半手工方式。技术实现为：为了开放和删除防火墙条目，在备案数据有变化时，通过解析所有备案网站的IP地址，和管理员导入的当前防火墙开放IP地址比对，邮件推送差异视图，让防火墙管理员做调整，调整后，管理员需要持续再导入目前的防火墙开放IP现状数据。

邮件通知

定期群发推送安全资讯。根据备案网站的类型进行个性化推送，比如向部分未使用网站群的网站推送网站群的迁移通知、对还在校外的网站提醒迁移等，推送时间确定在上班时间。

重大活动时期校外访问申请

重大活动期间为减轻安全运维压力，可能采取对部分站点限制校外访问或者直接关闭等措施。如果部分网站确实因为业务需要开放，必须主动申请上报开放理由和应急措施，等待审核后开放，而以往发生过安全事件的网站通过系统限制无法提起开放申请。重大活动时期使用自动生成临时的规则，过后恢复以往规则。

漏洞扫描结果分发

一般厂商的漏洞扫描工具可批量扫描网站漏洞，然而报告无法全部直接程序化录入备案系统，因为有些报告为未扫描到漏洞的报告，同时如果一个个录入备案系统工作量较大，所以我们采取一般性漏洞只单独邮件通知，高危漏洞录入备案系统。邮件群发的方法为：从漏洞扫描工具下载打包的报告，使用Python程序解压，解析报告内容，根据域名找到备案系统内的联系人，放到邮件发送队列内发送。

监控

根据备案数据自动生成监控系统配置文件，并定期更新，把所有的备案站点全部加入监控，系统监控可用性和性能，可以识别出可能正在被攻击的站点和开设了虚拟主机但是很久都没有开始使用的站点。监控系统可采用Nagios或icinga等使用文本配置文件的监控软件。对于检测网站的更新频率直接使用Python的urllib模块定期抓取首页内容，并简单比较文本相似度。

厦门大学通过以上备案政策和系统的推进，在校园网站梳理方面取得了较好成果，关闭了100多个僵尸网站，清理了400多个过期域名。通过对漏洞的管理，录入了多个漏洞，并关闭了多个有安全漏洞的站点。通过结合技术、管理和人工手段，极大提高了厦门大学在网站安全管理的能力。下一步工作可基于备案数据生成校内网址导航，为展现高校文化特色做导航；也可参考Vul Tracker漏洞管理与自动化跟踪平台[7]实现对漏洞的自动化检测。CEN（责编：陶春）

（作者单位为厦门大学信息与网络中心）

基金项目：中国高等教育学会2016年度教育信息化专项课题（2016XXZD06）

参考文献：

[1] 张永强. 中山大学互联网网站管理经验分享[EB/OL]. 2017年高等教育信息化创新论坛.（2017-05-05）[2017-06-18]. http://free.eol.cn/edu_net/edudown/2017luntan/zyq.pdf.
[2] 姜开达. 开展网站普查是Web安全管理的基础[J/OL]. 中国教育网络，2017（05）：65-65.
[3] 梁艺军. 摸排校园网站 清理安全隐患[J/OL]. 中国教育网络，2017（05）：67-68.
[4] 吴海燕. 自动识别技术“倒逼”网站备案[J/OL]. 中国教育网络，2017（05）：66-66.
[5] 江晓莲，郑海山. 面向安全漏洞管理的高校备案系统设计与实现[J/OL]. 网络安全技术与应用，2017（04）：150-152.
JIANG Xiao-lian, ZHENG Hai-shan. Design and implementation of university website registering system for security vulnerability management[J/OL]. Net Security Technologies and Application, 2017(04): 150-152.
[6] 新华社. 习近平总书记在网络安全和信息化工作座谈会上的讲话[EB/OL]. 中共中央网络安全和信息化领导小组办公室.（2016-04-25）[2016-06-25]. http://www.cac.gov.cn/2016-04/25/c_1118731366.htm.
[7] 章思宇，姜开达. Vul Tracker漏洞管理与自动化跟踪平台[J]. 华中科技大学学报（自然科学版），2016（11）：7-10.
ZHANG Sai-yu, JIANG Kai-da. VUL tracker platform for vulnerability management and automatic tracking[J]. Journal of Huazhong University of Science and Technology(Nature Science Edition), 2016(11): 7-10.

?1994-2018 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net