网站与信息系统安全

厦门大学
让二级学院也拥有漏洞扫描能力

厦门大学通过安全服务外包和采购漏洞扫描设备并开放给二级学院管理员使用的方法，探索全民参与网络安全的道路。

文 / 郑海山 屈斌 许卓斌

为提高高校网站和应用系统的安全性，高校会对已经存在和即将上线的网站和应用系统定期进行扫描，评估风险。常用的方法包括对源代码进行代码审计、对操作系统和数据库等运行环境进行配置核查、对网站和应用系统进行漏洞扫描和渗透测试等，并根据结果进行整改加固。由于代码审计需要有源代码，不是所有系统都可以提供，而渗透测试专业性和成本较高，所以使用漏洞扫描工具对高校网站和应用系统进行扫描是最常见和有效的方法。

开放漏洞扫描背景

漏洞扫描工具有开源和商业的产品，漏洞扫描工具会对服务器和网站进行扫描，与已知漏洞数据库进行比对，提示潜在的风险和提供修复建议。漏洞扫描工具的核心为漏洞数据库。漏洞数据库的覆盖率、更新速度和准确度是评估漏洞扫描工具最重要的指标。为提高覆盖率，一般会使用多个厂商多个类型的漏洞扫描工具。

高校购买了漏洞扫描设备，由信息中心集中扫描后分发给各个相关负责人要求整改。由于购买漏洞扫描设备一次性投入较高，而且需要专人维护，有些高校将扫描工作外包给安全厂商，定期请安全厂商对全校所有资产进行扫描。厦门大学通过两种模式结合的方式，对于暴露在校园网的服务器、网站和应用系统，通过购买漏洞扫描工具来进行批量扫描；对于新上线和重要的系统在扫描的基础上还通过购买渗透测试安全服务来提升安全性。

在实践中，我们尝试了向二级学院开放漏洞扫描能力。由于信息中心安全任务较重，人员配备不足，开放能力后二级学院大量计算机专业人员弥补了人员方面的短缺，扩大了扫描的范围，使学校网站和应用系统的安全性得到了整体提升。另外以往信息中心人员扫描完后，需要分发扫描报告给各个服务器、网站和应用系统的相关负责人，相关负责人再转发给具体的开发和运维人员，整改完还需要重新扫描验证，沟通成本和时间成本都很高。通过开放该能力，上述问题得到了很好的解决，极大地提高了各个服务器、网站和应用系统的自查、整改和验证效率。

市面上有些厂商的设备可以通过分析网络流量对高校内的所有对外网站资产进行探测，对发现的资产在系统内进行备案并关联负责人的邮箱等联系方式，将对资产的漏洞扫描结果通过系统自动分发给各个不同的负责人，也可以达到以上类似效果。

心得体会

在开放的过程中，我们通过前期评估风险、编写漏洞扫描工具使用文档、建立QQ群、寻找种子用户、过程中整理常见问答、最终扩大了开户面，达到了较好的

Web 应用上线安全评估方法

Web 应用程序安全漏洞可以分为两类，第一类为应用架构、逻辑方面的缺陷导致的安全漏洞，如失效的访问控制、失效的身份认证等，对于这类安全缺陷的发现，必须通过人工测试判断才能实现。第二类为应用编码不严谨导致的安全缺陷，如缓冲区溢出、非法输入等，这类缺陷既可以通过人工检查的方法实现，也可以通过自动化的测试工具，如黑盒扫描和白盒扫描的方法来实现。

一般来说，要真正实现对 Web 应用进行全面的安全评测，需要经过三个主要的步骤：

1. 审查 Web 应用的整体设计，找出由于设计上的不完善而导致的安全漏洞，比如敏感信息泄露、失效的访问控制、失效的身份认证等。这步工作只能通过人工的方法实现，主要依靠评测人员的经验。

2. 对 Web 站点的代码进行分析，找出由于编程的不完善而导致的安全漏洞，比如缓冲区溢出、SQL 注入等。此项评测可通过三类方法实现：第一类是黑盒测试方法，主要通过 HTTP 请求对 Web 应用进行漏洞扫描；第二类是白盒测试方法，主要通过扫描源代码发现其中存在的漏洞；第三类是通过人工静态代码分析实现。

3. 评估 Web 站点的部署，模拟网络用户对 Web 站点进行攻击，找出安全漏洞和弱点，比如认证不充分、信息泄漏等。此项评测可通过渗透测试的方法实现。采用上述的评测方法对应用进行上线前的安全评估，还需配置相应的准入规范。

效果，同时也积累了以下心得：

1.《中华人民共和国网络安全法》规定：任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。对于漏洞扫描工具的提供应当符合上述规定，所以我们要求用户使用强密码并只限本人使用，严格限制用户允许登录的 IP 地址和允许扫描的 IP 和 URL 列表。同时我们通过网络层限制漏洞扫描工具只能在校园网范围内进行扫描，并对用户普及《网络安全法》知识，禁止用户通过端口转发或代理去扫描他人的服务器、网站和应用系统。

2. 为减轻漏洞扫描工具压力，减少无谓的扫描，对于托管在信息中心虚拟主机上的网站，我们通知用户无需扫描服务器，只需扫描自己的网站即可。对于信息中心负责的虚拟主机和虚拟化宿主机的服务器扫描由信息中心统一负责。

3. 为防止扫描对网站正常的访问造成影响并防止多个任务同时启动影响漏洞扫描服务器性能，我们建议用户错峰启动任务，在网站访问量较低的时段进行扫描。比如使用漏洞扫描工具的预约扫描时间功能，在夜间及凌晨进行扫描。

4. 漏洞扫描有可能对数据造成破坏，我们建议用户在扫描之前备份自己服务器的数据。

5. 漏洞扫描可能被服务器的安全软件拦截，我们建议用户在安全软件的白名单设置内对漏洞扫描工具 IP 地址是否添加例外分别进行多次扫描和对比。我们也建议用户扩大扫描范围，对内网不对外提供服务的服务器也进行相应的扫描。

6. 漏洞扫描结果不一定完全准确，可能存在误报，也可能即使扫描结果为安全也不一定完全安全。所以我们推荐除了使用我们的漏洞扫描工具扫描外，还可使用开源的 OpenVAS、sqlmap、Nmap、Metasploit 和商业软件和互联网云服务进行扫描并多方比较。

7. 在种子用户的选择上，我们通过备案系统筛选出备案超过一定数量的管理员，沟通开户事宜，同时在备案系统内增加可导出管理员负责的所有服务器的 IP 地址和 URL 地址功能，方便管理员直接导入漏洞扫描任务内，极大地减轻了管理员的工作量。

8. 随着时间的推移，操作系统或中间件的版本更新和应用的更新可能会产生新的漏洞，同时漏洞扫描工具的漏洞数据库也会更新，所以我们建议管理员应当定期对服务器、网站和应用系统进行扫描。

9. 根据用户反馈不断丰富使用文档，结合 QQ 群的沟通，对用户遇到的问题给出建议。

10. 漏洞扫描工具对管理员的触动较大，很多管理员通过自行扫描看到扫描结果后才发现自己原先认为很安全的服务器、网站和应用系统实际上存在着较多漏洞，提高了管理员的安全意识，通过扫描结果的修复建议和修复后重新验证的过程，也让管理员的安全知识得到了提升。

11. 漏洞扫描工具内置了口令猜测和配置核查等模块，并有完善的修复建议，对于不存在漏洞的服务器的加固也很有帮助。

12. 漏洞扫描工具超级管理员应当密切关注漏洞扫描工具的使用情况，对所有用户扫描的结果进行观察，识别校内的风险点，并督促相关管理员及时进行整改。

厦门大学通过安全服务外包和采购漏洞扫描设备并开放给二级学院管理员使用的方法，对信息中心的日常安全运维工作形成了有效补充。开放漏洞扫描设备提高了设备的使用率和使用价值，提高了服务器、网站和应用系统从漏洞发现、分发、验证、到修复的效率。通过 QQ 群组建立了内部管理员安全交流群，探索全民参与网络安全的道路。CEN（责编：王左利）

（作者单位为厦门大学信息与网络中心）

锐捷网络 2018 产品及解决方案战略发布会召开

本刊讯 3 月 27 日，以“场景创新 精·进未来”为主题的锐捷网络 2018 年产品及解决方案战略发布会在北京召开。在本次发布会上，锐捷网络强调用匠人精神打造精品、用精准的解决方案直击用户痛点、用精耕行业的应用帮助用户数字化转型。

锐捷网络交换机产品事业部市场总监翟鹏远表示：“锐捷率先启动了 25G 数据中心架构产品和技术研发，投资数据中心实验室；同时锻造出 25G 数据中心架构下的全套产品以及 RDMA、可视化、去堆叠等领先技术，在全球范围内率先完成规模投产和商用。”

面对物联网、AR/VR、数字化转型等应用趋势变化，锐捷网络将在 2018 年全面启动智能无线网战略布局，通过人工智能分析、自动场景识别优化、网络现象可解释、全自动组网等科技创新，满足万物互联时代的需求升级，并通过全新的行业解决方案，满足高校、普教、医疗、企业等各个行业用户的升级需求，同时还会在智慧校园物联网等领域形成万物聚集、万物联动、万物感知的应用新格局。

云桌面是锐捷网络基于“场景创新”理念下诞生的又一创新领域。锐捷网络云桌面产品事业部市场总监肖广维谈到：“精致的场景细分，让我们有信心把云课堂标准版、增强版、考试专业版、3D 专业版在教育领域实现更大范围的应用覆盖。不论是传统的学生机房、还是英语听说考试、Pad 教室，云课堂将满足每间教室的定制化需求。”在此基础上，锐捷网络还推出“数字学习中心 1.0”、“智慧云课堂 1.0”，全新打造“云课堂 + 教室”的建设理念。