网站应用层安全防护体系①

徐竹冰

(中国移动通信集团 上海有限公司，上海 200233)

摘 要：针对网站面临的应用层安全问题，对应用层安全防护体系进行了研究。从事前 Web 应用漏洞扫描和测试、事中 Web 应用攻击主动防护、事后页面篡改检测及恢复三个层面建立了一个网站应用层安全防护体系。实践结果表明，该安全防护体系实现了网站的应用层安全，有效提高了网站安全性。

关键词：应用层；安全防护；漏洞扫描；攻击防御；页面防篡改

Security Protection Architecture of Application-Level in Portal

XU Zhu-Bing

(China Mobile Group Shanghai Co, Ltd, Shanghai 200233, China)

Abstract:Concerning the problem of application-level security in portal, this paper researched on security protection architecture of application-level. It built a security protection architecture of application-level which included vulnerability scanning and testing of Web application-level before the event, active protecting from Web application-level attacking during the event, detecting and recovering the modified page after the event. Application result showed that the security protection architecture achieved application-level security in portal, and enhanced portal security effectively.

Key words: application-level; security protection; vulnerability scan; attack defense; preventing page modification

1 引言

随着互联网技术的迅猛发展，相关行业的关键业务活动越来越多地依赖于 Web 应用，在向客户提供通过浏览器访问信息功能的同时，Web 应用系统所面临的风险不断增加，主要表现在两个层面：一是随着 Web 应用系统的增多，这些 Web 应用系统所带来的安全漏洞越来越多；二是随着互联网技术的发展，用来攻击 Web 应用系统的黑客工具越来越多、黑客活动越来越猖獗。据 CNCERT/CC 发布的中国大陆被篡改网页数量的统计显示，被篡改的网页数量每年都大幅增加。

目前大多数的网络攻击和互联网安全事件源于应用软件自身的脆弱性，而其根源来自程序开发者在网页程序编制过程中缺乏相关的安全意识和知识，并且开发完成后也缺乏相应的代码检测机制和手段。这些脆弱性在日后就成为了黑客用来发动攻击、进行页面篡改、以及布放和传播网页木马的最有效途径。一旦某些重要网页被篡改，被公众浏览到，将会对政府和企业形象造成巨大的负面影响，并且造成极其恶劣的社会影响。

然而，对于不断增加的安全风险，现阶段的安全解决方案无一例外的把重点放在网络安全层面，致使面临应用层攻击时（如：针对 Web 应用的 SQL 注入攻击、跨站脚本攻击等），传统的网络防火墙、IDS/IPS 等安全产品几乎不起作用。为确保网站应用层的安全，需要对网站应用实施主动评估、主动防御、被动保护等多方面安全措施[1]，形成网站应用层安全防护体系。

2 网站应用层安全防护需求

对网站应用层的安全防护需要从事前、事中、事

① 收稿时间:2011-05-19;收到修改稿时间:2011-06-25

后三个阶段来考虑，如图 1 所示：

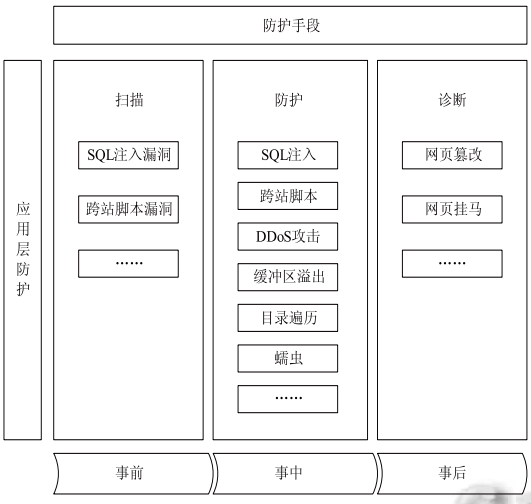

图 1　网站应用层安全防护需求

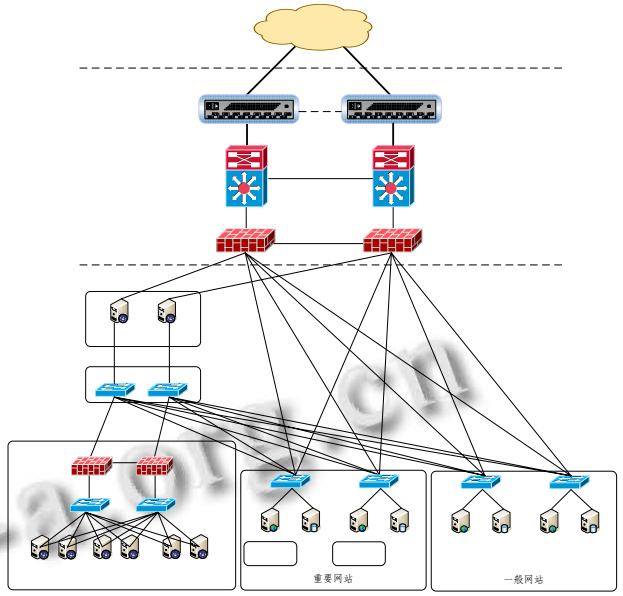

图 2　网站应用层安全防护架构

① 事前：在未发生各类攻击行为之前，需要有一个机制能对现有的各类网站应用系统及页面代码进行漏洞扫描，以发现可能被黑客利用的漏洞（如：SQL 注入漏洞、跨站脚本漏洞等）以及木马等，并以此作为依据供开发人员进行网站安全加固 [2,3]。

② 事中：在网站受到外部攻击（如：SQL 注入攻击、跨站脚本攻击、Web 应用拒绝服务攻击等）时，可以及时检测到，并能过滤攻击流量，以保护网站不受外部攻击的干扰，可以正常对外提供服务[4,5]。

③ 事后：在发生网站被入侵，页面被篡改的情况后，系统可以及时检测到，并能在最短的时间内将页面恢复，使外部用户无法访问到被篡改后的页面，并能通过声光告警等方式及时通知监控人员[6]。

3　网站应用层安全防护体系

3.1　整体架构

根据上述需求分析，整个网站应用层安全防护体系需要在事前、事中、事后三个环节分别部署安全防护措施：事前能实现 Web 应用漏洞扫描和测试；事中能实现 Web 应用攻击主动防护；事后能实现页面篡改检测及恢复。通过三位一体的防护手段实现网站的应用层安全。

网站应用层安全防护架构分为三个子系统：Web 应用漏洞扫描和测试系统、Web 应用攻击防御系统、页面防篡改系统。整个系统网络架构示意如图 2 所示：

根据实际的安全需求不同，可以将网站分为重要网站和一般网站：

① 重要网站指对所有客户提供业务信息浏览服务，且页面访问量大，页面内容经常变更，被攻击和篡改后对政府或企业形象会产生重大影响的网站。对这部分网站采用主动检测＋主动防御＋被动防御的部署方案，即采用：Web 应用漏洞扫描和测试系统＋Web 应用攻击防御系统＋Web 页面防篡改系统的模式。

② 一般网站指仅做内部业务管理使用，或者虽然对外部客户提供业务信息浏览服务，但页面访问量小，页面内容不经常变更，被攻击和篡改后对企业形象影响较小的网站。对这部分网站采用主动检测＋主动防御的部署方案，即采用：Web 应用漏洞扫描和测试系统＋Web 应用攻击防御系统的模式。

3.2　Web 应用漏洞扫描和测试系统

3.2.1 Web 应用漏洞扫描系统

Web 应用漏洞扫描系统用于对已知或未知的 Web 应用漏洞进行扫描。系统自带 Web 应用漏洞的规则库，并可以通过更新规则库的方式支持对新型 Web 应用漏洞的检测。Web 应用漏洞扫描系统可以采用软件或软硬集成的方式实现，能根据扫描结果提供详细的分析报告，为开发和维护人员提供安全加固所需的分析数据。

考虑到日常需对多个网站进行 Web 应用漏洞检测，每个网站可能包含几万个不同类型的页面，检测

量大、耗时长，需耗费扫描系统大量资源，且漏洞扫描可能会增加被扫描系统负荷，为避免对现网系统的影响，一般建议放在夜间业务量低或无业务量时进行扫描。

3.2.2 测试系统

由于各 Web 网站在正式进行大规模页面部署和更新前无法预知部署后的效果以及页面是否存在安全漏洞，所以需要在网络中部署 Web 测试系统。此系统虽然不能全面覆盖所有可能的操作系统和 Web Server 软件组合，但可以为常见的 Web 应用环境提供测试平台。例如，可以使用一台设备模拟 Windows +Apache/Tomcat 平台，使用另一台设备模拟 Linux+Apache/Tomcat 平台。在测试环境上模拟发布测试的同时，可以利用 Web 应用漏洞扫描系统对其进行全面的安全评估，及时对存在安全漏洞的页面进行安全加固。

3.3 Web 应用攻击防御系统

Web 应用攻击防御系统主要有两种实现方式：软件方式和硬件方式。

① 硬件方式即硬件应用防火墙，一般通过反向代理（Reverse Proxy）技术实现。反向代理（Reverse Proxy）技术是指以代理服务器来接受 internet 上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器上得到的结果返回给 internet 上请求连接的客户端，此时代理服务器对外就表现为一个 Web 服务器。外部网络可以简单把它当作一个标准的 Web 服务器而不需要特定的配置。不同之处在于，这个服务器没有保存任何网页的真实数据，所有的静态或动态网页都保存在内部的 Web 服务器上。因此对反向代理服务器的攻击并不会使得网页信息遭到破坏，这样就增强了 Web 服务器的安全性。

② 软件方式即软件应用防火墙，采用 Web 服务器核心内嵌技术实现。Web 服务器核心内嵌技术是指将安全模块内嵌在 Web 服务器软件中，这个模块针对不同的 Web 服务器软件使用相应的核心内嵌技术，例如：ISAPI、Apache-module、NSAPI、JAVA-filter 等。安全模块内嵌于 Web 服务器软件，与 Web 系统完全整合，其优点在于：不存在独立的安全模块运行进程，入侵者无法找到和中止模块运行；精准理解和分析 Web 服务请求数据，进行充分可靠的安全检查；完全与 Web 服务的进程融合，稳定性和兼容性强；与操作系统及硬件无关，全面控制 Web 系统软件和服务。

Web 应用防火墙能支持对 SQL 注入、可执行命令注入、缓冲区溢出攻击、参数篡改、Cookie 篡改、会话劫持、跨站脚本攻击、恶意编码、密码窃取、应用层拒绝服务攻击等的防护。

Web 应用防火墙能支持智能自学习，从真实流量中不断学习 Web 应用元素进行动态建模，以提供更精确的保护。

Web 应用防火墙能对每项探测到的攻击提供详细的分析信息（包括攻击时间、源 IP、攻击具体目标、攻击类型、利用了哪些漏洞等信息），并支持报告的导出，以便开发和维护人员可以根据这些信息进行安全防范。

3.4 页面防篡改系统

3.4.1 页面防篡改技术

页面防篡改防护通过数字水印技术来实现：即在页面发布时将经过 128 位以上的密钥计算，生成唯一的、不可逆转的和不可伪造的数字水印，用于检测页面文件是否被篡改。页面防篡改防护主要采用软件方式来实现，主要有三种实现方式：

① 外挂轮询

外挂轮询技术是利用一个网页读取和检测程序，以轮询方式读出要监控的网页，与真实网页相比较，来判断网页内容的完整性，对被篡改的网页进行告警和恢复。

② 事件触发

事件触发技术是利用操作系统的文件系统接口，在网页文件被修改时进行合法性检查，对非法操作进行告警和恢复。

③ 核心内嵌

核心内嵌技术是将篡改检测模块内嵌在 Web 服务器软件中，它在每一个网页流出时都进行完整性检查，对被篡改的网页进行实时阻断，并予以告警和恢复。

核心内嵌技术与事件触发技术相对于外挂轮询技术在各方面都较为优越。核心内嵌技术与事件触发技术采用不同的防护措施对系统进行保护，两者技术各有所长。在实际应用中，考虑使用基于核心内嵌技术以及事件触发技术相结合的产品。

3.4.2 页面防篡改系统模块

页面防篡改防护系统分为三个模块：

① 集中管理和监控模块

部署管理和监控服务器，负责管理和监测页面统

一发布服务器运行状态、管理和监测各防篡改模块/同步模块的运行状态、页面被篡改后的自动恢复控制、记录和展现各类告警和日志。

② 统一页面发布模块

部署防篡改系统发布服务器。发布服务器上具有与受保护 Web 服务器上的网页文件完全相同的目录结构。发布服务器上的任何文件/目录的变化都会自动和立即反映到受保护 Web 服务器的相应位置上。

采用统一页面发布功能，各网站内容管理系统将内容传送到发布服务器的相应目录下，再由发布服务器向 Web 服务器进行发布。当页面由发布服务器发布时将经过 128 位以上的高强度密钥的计算，生成数字水印。

③ 应用防护/防篡改检测模块和同步模块

在各网站的 Web 服务器上安装部署应用防护/防篡改检测模块和同步模块，模块支持所有主流的操作系统：Windows 平台（2000、2003、2008 等）、Linux 平台（Redhat、SUSE 等）、UNIX 平台（Solaris、HP-UX、AIX 等）、FreeBSD 等；支持常用的 Web 服务器软件：BEA WebLogic、Tomcat、Apache、Sun Application Server、IIS、SunONE、iPlanet、WebSphere、resin、HP-AS 等；兼容所有常用的数据库系统：SQL Server、Oracle、MySQL、Access 等；兼容所有常用的安全防护软件：Symantec Norton、趋势等。

应用防护模块可以对外部访问行为进行安全性检查。如果正常则发送给 Web 服务器软件；如果发现有攻击特征码，即刻中止此次请求并进行告警。

防篡改检测模块利用数字水印对每个发送的网页进行即时的完整性检查。如果网页正常则对外发送；如果发现被篡改则阻断对外发送，并依照一定策略进行告警和恢复。

同步模块负责接收发布服务器发布的网页，在接收到网页和水印后，将网页存放在文件系统中，将水印存放在安全数据库里。

4 防护效果评估

根据上述应用层安全防护体系，我们对现有的网站进行了安全改造，部署了应用层安全防护系统。在实际使用中，安全防护能力和效果有了显著提升：

① Web 应用漏洞扫描系统能够扫描发现一般扫描器无法发现的应用层漏洞，给开发和维护人员提供了应用层安全加固的依据。在 Web 应用漏洞扫描系统部署上线后对上海移动某门户网站的首次扫描中，共发现 Web 应用安全漏洞 23 个（如表 1 所示），其中包括跨站脚本、框架注入、链接注入等 3 个高危漏洞。维护人员根据发现的漏洞对该网站进行了安全加固，降低了系统的潜在风险。

表 1　上海移动某门户网站 Web 应用漏洞

漏洞名称	漏洞级别	漏洞数量
跨站脚本	高危	1
框架注入	高危	1
链接注入	高危	1
跨站伪造用户请求	中危	3
web 应用程序错误	低危	13
敏感目录	低危	1
测试目录	低危	2
测试文件	低危	1

② Web 应用攻击防御系统能够实时拦截公网上的各类应用层攻击和非法访问。根据 2011 年 5 月份的统计，Web 应用攻击防御系统在一个月内为上海移动某门户网站拦截的应用层攻击达 322 次，其中包括 SQL 注入攻击 4 次，跨站脚本攻击 6 次，以及大量 HTTP 特征码违规攻击，为网站提供了有效的安全防护。

③ 由于 Web 应用漏洞扫描系统和 Web 应用攻击防御系统有效降低了网站的安全风险，在实际使用中未发生过网站页面被篡改的情况。为了验证页面防篡改系统的有效性，我们在内网直接对上海移动某门户网站页面进行了篡改，结果发现页面防篡改系统对网站页面起到了很好的保护作用，当页面被篡改后，页面防篡改系统在 5 秒钟内将该页面恢复为正常页面。

5 结语

网站应用层安全防护体系包括事前 Web 应用漏洞扫描和测试、事中 Web 应用攻击主动防护、事后页面篡改检测及恢复三个层面的安全防护手段，解决了传统的网络防火墙、IDS/IPS 等安全产品对应用层攻击无法防御的问题，实现了网站的应用层安全。在实际应用中，通过与其他网络层安全技术手段及管理手段相结合[7]，将全面降低系统安全风险，提高安全防护能力，确保网站系统的安全运行。

(下转第 64 页)

以实现奇异点的精确定位，并且容易检测到虚假的奇异点。今后的工作应着重于改进这种奇异点的选取方法或者找到一种更精确的全新的方法。

参考文献

1 田启川,张润生.生物特征识别综述.计算机应用研究,2009,26(12):4401−4406.

2 方晨艳,杨凡.指纹图像质量评价方法.计算机系统应用,2008,17(11):62−65.

3 Addrew S. A Combination Fingerprint Classifier. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2001,23(10): 1165−1174.

4 Kawagoe M, Tojo A. Fingerprint pattern classification. Pattern Recognition, 1984,17(3):295−303.

5 Zhang Qin-zhi, Yan Hong. Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. Pattern Recognition,2004,37(11):2233−2243.

6 Li J, Yau WY, Wang H. Combining singular points and orientation image information for fingerprint classification. Pattern Recognition, 2008,41(1):353−356.

7 Lowe DG. Object recognition from local scale-invariant features. International Conference on Computer Vision, 1999: 1150−1157.

8 Aujol J, Aubert G, Feraudl. Wavelet-based level set evolution for classification of textured images. IEEE Trans. on Image Processing, 2003,12(12):1634−1641.

9 孟爱国,刘国彦,李峰.基于多层小波分解的虹膜识别算法.计算机工程与应用,2005,22:59−61.

10 任靖,李春平.最小距离分类器的改进算法—加权最小距离分类器.计算机应用,2005,25(5):92−95.

(上接第 84 页)

参考文献

1 白建坤.Web 服务安全架构研究.计算机应用,2005,25(11): 33−35.

2 沈寿忠,张玉清.基于爬虫的 XSS 漏洞检测工具设计与实现.计算机工程,2009,35(21):151−154.

3 Ismail O, Etoh M, Kadobayashi Y. A Proposal and Implementation of Automatic Detection/Collection System for Cross-site Scripting Vulnerability. Proc. of the 18th International Conference on Advanced Information Networking and Applications. Washington DC: IEEE Computer Society, 2004.

4 谢逸,余顺争.基于 Web 用户浏览行为的统计异常检测.软件学报,2007,18(4):967−977.

5 Kruege C, Vigna G, Robertson W. A multi-model approach to the detection of web-based attacks. Computer Networks, 2005,48(5):717−738.

6 张磊,王丽娜,王德军.一种网页防篡改的系统模型.武汉大学学报(理学版),2009,55(1):121−124.

7 互联网安全防护要求,YD/T 1736−2008,2008.