Web 网页服务安全防护对策分析

石　慧　董俊磊

（河南职业技术学院　河南　450046）

【摘　要】由于网络普及率的快速提高，Web 成为互联网的热门概念，现今社会中，Web 不仅仅是信息发布，更是网络正常运作的一大保障。然而，随着网络环境的日益复杂，Web 服务的一些安全漏洞和缺陷也显露出来，因此，人们需要采用有效的安全防护对策，以保障 Web 服务的安全，继续为人类生产提供动力。本文即对 Web 服务的安全防护对策进行了相对详细的阐释和概述。

【关键词】Web 网页服务；安全；防护对策

中图分类号：TP393.08　　文献标识码：A　　文章编号：1009-6833（2014）11-098-02

Web services security protection countermeasure analysis

Shi Hui，Dong Junlei

Abstract：due to the rapid increase Internet penetration，the Web became the popular conceptions in the Internet，in the modern society，and the Web is not only a information release，network normal operation of a large security.However，with the increasingly complex network environment，some Web services security loopholes and defects also revealed，therefore，people need to adopt effective safety protection measures，to ensure the security of Web services，continue to provide power for the human production.In this paper，the Web services security protection countermeasures for the relatively detailed explanation and overview.

Keywords：Web services；Safety；Protective countermeasures

1　Web 网页服务的基本概念

Web 服务（Web Service）是根据 XML 和 HTTPS 衍生而出的一种新型服务，它的通信协议主要是依据 SOAP 制定的，它能使得运行在不同机器上的不同应用无须借助附加的、专门的第三方软件或硬件，就可相互交换数据或集成。同时，Web Service 是一种相对特别的网络模块，属于自描述、自包含的可用网络模块，能够有针对性的执行具体的工作，十分高效和可靠。

2　Web 网页服务面临的安全威胁

2.1　Web 安全受到威胁的原因

目前，很多类似于网上银行、网络购物等业务都依赖于计算机互联网进行交易，这就给许多恶意攻击者带来了巨大的诱惑，他们出于不良目的对 web 服务器进行攻击，通过各种非法手段获取他人的个人账户信息以谋求私利。正因如此，web 服务平台极易受到恶意攻击。

2.2　威胁 Web 网页服务安全的因素

威胁 Web 安全的因素可谓是林林总总，花样繁多，常见的有网页挂马、SQL 注入、缓冲区溢出、嗅探、利用 IIS 等针对 Webserver 漏洞进行攻击。下面，我们从中挑选几个威胁因素加以介绍。

2.2.1　网页挂马

网页挂马是指为达到破坏或控制用户电脑的目的，提前把木马下载到本地的做法，其主要过程和步骤如下：先是把一个木马程序上传到一个网站里面，然后利用木马生成器生一个网马，之后再将这个生成的网马上传到空间里面，再加代码使得木马在打开网页时运行。

2.2.2　SQL 注入

SQL 注入是黑客技术的一种，它能够欺骗服务器执行带有恶意破坏的 SQL 命令，它的运作原理是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串。之后，施放恶意的 SQL 命令，并欺骗服务器按其指示的命令去执行错误的业务。

2.2.3　跨站脚本攻击

跨站脚本攻击，也称为 XSS，简单来讲就是利用网站漏洞从用户那里恶意盗取信息。现如今，黑客的技术越来越强大，他们为了获取想要的机密信息，会采取很多非法手段，跨站脚本攻击就是其常用手段之一。他们善于抓住网站中存在的漏洞和缺陷，设置有陷阱的链接，例如被插入恶意代码的链接。用户在点击连接之后，信息就会被盗取。

3　Web 服务安全防护对策

Web 服务的诞生是科技发展的产物，极大地便利了人们的日常生产，但是 web 的安全并不是绝对的，他的安全威胁来自内外两方面，为了维护其正常运行，我们应该从内外两方面提出有效对策进行防护。

3.1　外部环境方面的防护——建立网络安全防护体系

网络安全防御体系可分为三个层次：安全评估、安全加固、网络安全部署。

首先，安全评估是指通过对网络的系统安全检测，Web 脚本安全检测，以检测报告的形式，及时地告知用户网站存在的安全问题。并针对具体项目，临时组建一个项目脚本代码安全审计小组来审核项目的安全度，为了提高安全度，在临时项目小组审核后，还会由资深网站程序员及网络安全工程师共通审核网站程序的安全性。找出存在安全隐患程序并准备相关补救程序。

第二，安全加固是指以网络安全评估的监测结果为依据，清除网站应用程序中存在的漏洞和安全隐患，并且在发现已经出现的问题时，及时应对，进行安全修复。安全加固作为一种积极主动地安全防护手段，在加强系统安全性方面，提供了有力的保障。

第三，网络安全部署是在网络信息系统中进行安全产品的部署，可以对网络系统起到更可靠的保护作用，提供更强的安全监测和防御能力。

3.2　Web 自身防护对策——具体的应对策略

Web 应用安全问题的产生追根究底是因为软件质量不过关。但 Web 应用与传统的软件相对比，有着其自身特有的性能特点。Web 应用往往是某个机构所独有的应用，对其存在的漏洞，已知的通用漏洞签名缺乏有效性；需要频繁地变更以满足业务要求，有序的开发周期很难得到维持和正常循环；客户端与服务端的交互场景十分的复杂，想要做到全面考虑各种复杂的情况并不容易，而且很多开发者并没有深入地理解业务流程，这就使难度更加深了一层；人们通常认为 Web 的开发是一件比较简单事情，即使是经验不足的开发人员也能够成功完成。这种现状，选择 Web 安全防护工具是十分合理的行为，WEB 应用防火墙，正是这类专业工具。针对这种现状，常见的 Web 服务安全防范策略有以下几种：

3.2.1　Web 服务器操作系统及发布软件的安全防范措施

一是在第一时间及时的更新所有升级，并为系统打好所有可能做好的补丁，可以将所有的更新下载到一个专门用来承载这些更新的服务器上，并在该服务器上以 Web 的形式将文件发

（下转第 100 页）

3.2 数据云端的备份

针对比较重要的云中数据，必须进行定期备份，然后把备份的有关数据传送到云端的存储区域，此种备份数据中仅仅有该分数据相关云用户能够进行访问，同时进行重新的获取与运用，针对备份的相关数据一定要选择对应的先进技术完成处理，例如选择比较机密的技术等，从而防止云端备份相关数据的黑客侵入等。另外，云中客户端的 Pn 和云中相关数据备份之间的关系如图 1 所示。

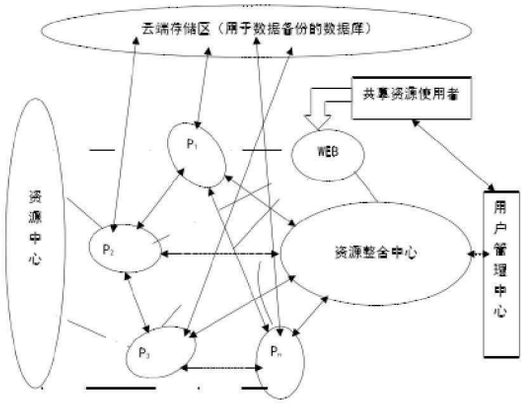

图 1 云中数据备份关系示意图

3.3 安装防护软件

网络防火墙技术作为一项强化网络间的访问控制，其可以有效避免外部网络用户通过非法的模式侵入内部网络，从而访问内部相关网络资源。网络防火墙可以对两个或者是许多个网络间的传输数据进行检查，进而明确网络间的数据通信是否安全，同时对网络的具体运行状态进行有效监测。依据防火墙选择的各种技术，能够把其分成包过滤形式和地址转换形式以及监测形式等多种。其中包过滤形式的防火墙主要利用网络中先进的分包传输技术，经过读取数据包中相关地址信息进行判断，如果发现来自于危险站点的有关数据包，这时防火墙就会把此种数据拒之门外。

3.4 定期完成补漏

漏洞是能够在攻击时主要运用的弱点，其可以为软件和硬件以及程序的缺点等。有关学者曾经给出一份如今比较流行的操作系统与运用程序的相关研究报告，明确指出软件中难以避免存在漏洞与缺陷[6]。现阶段，大部分的病毒与黑客主要运用系统存在的漏洞进行网络用户的攻击。为了可以纠正此种漏洞，软件的开发商必须及时发布补丁程序。客户一定要及时进行漏洞补丁程序的有效安装，从而科学处理漏洞造成的安全问题。比如客户可以运用 360 安全软件进行定期的系统扫描，在查找漏洞之后进行及时的修补等。

4 结束语

综上所述，在对如今网络安全技术有效结合运用的前提下，制定相对完善的基于云计算形式下的移动网络安全有效保护体制，并对存在的关键性安全隐患完成深入分析和研究。云计算凭借良好的网络资源共享体系，近些年来发展极为迅速。但是在共享数据的流动形式中数据安全与信息安全问题变得更加明显。因此，相关部门和研究人员一定要进一步研究基于云计算环境下的网络安全保护对策，从而推动计算机技术与互联网的安全、可靠发展。

参考文献：

[1]刘伯仁，张海波.浅析计算机网络安全的威胁及维护措施[J].中小企业管理与科技，2010（29）：11-12.

[2]彭珺等.计算机网络信息安全及防护策略研究[J].计算机与数字工程，2010，（1）：122-123

[3]钱葵东，常歌.云计算技术在信息系统中的应用[J].指挥信息系统与技术，2013，3（6）：51-54.

[4]杨健，汪海航，王剑，俞定国.云计算安全问题研究综述[J].小型微型计算机系统，2012，33（3）：472-479.

[5]杨斌，刘海涛.云计算对移动互联网发展的助推作用[J].电信工程技术与标准化，2013，（12）.

[6]房秉毅，张云勇，徐雷，蓝天-云计算应用模式下移动互联网安全分析[J].电信技术，2011，（10）.

作者简介：

马娟（1978—），女，山西永济，教育硕士，讲师，研究方向：计算机网络。

（上接第 98 页）

布出来，这样可以防止 Web 服务器接受直接的网络访问。二是设置服务器的管理账号和复杂的密码，加密的服务器会给入侵者的恶意入侵带来阻碍，越是复杂的密码，入侵者破解的可能性就越低，其入侵系统的可能性也同比下降，如此一来，入侵者获得 Web 服务器最高管理权限所造成的损失就可以避免了。三是关闭与 Web 服务无关的服务，尽量减少系统与外部通信的几率。

3.2.2 Web 应用程序安全防范措施

一是不管是数据的输入还是输出，都应该经过应用程序确认、检测和过滤。二是拒绝使用连续的可猜测的标识符，而是应用 UUID 全球通用的唯一标识符，使所有的管理员功能上都设定了相应的授权和访问控制，应用程序应该只在最小程度上提供所需的访问权限。三是管理界面应当放在单独的站点，设置用户的访问权限，使普通用户不能访问，用于应用程序通信的连接字符串应当被安全存放，并且设置为只能通过安全的方式传递，当传递方式存在安全隐患，操作即会被拦截或终止。四是经常访问相关的官方网站，关注程序安全漏洞和更新版本，及时的给自己的程序升级或打上补丁。五是经常备份自己的网站数据，黑客的存在是数据安全的一大隐患，难以预料何时会遭到黑客的袭击，为了防止黑客袭击后，可靠数据的丢失和损坏，要求我们做好日常的备份工作，这也是网络安全的第一要求。

3.2.3 选择适用的 Web 安全产品

（1）网页防篡改产品。网页防篡改产品运作的基本原理是对 Web 服务器上的页面文件进行监控，发现有更改的时候，能够及时反应，快速恢复，属于典型的被动防护技术。

（2）web 防火墙产品。之前所述的网页防篡改产品是被动的防护技术，为了更高效、更有力的防范威胁，还需要主动型的产品，例如防火墙产品，它能阻断入侵行为，主要对 Web 特有的入侵方式加强防护，例如 DDOS 防护、SQL 注入、XML 注入等。

（3）Web 数据库审计产品。安全保障一个十分重要理念就是安全恢复，动态网页维护的难点在于网页的数据是用数据库现场生成的，因此对数据库的修改以及怎样修改，就成为了一个必须关注的问题，而为了达到运营状态可以恢复这一目的，Web 数据库审计产品对重要数据库操作进行详细的审计活动，通过审计活动的详细审核，安全恢复得以实现。

（4）Web 木马检查工具。Web 安全不仅是维护网站自身的安全，通过网站入侵用户电脑的危害也十分具有威胁性，网页容易被挂上木马，进而对 Web 造成影响或破坏。为了解决这一问题，Web 提出了有效的解决措施，它按照一定的规则，将网站上的所有页面打开一遍，再对网页有关的事项进行详细的检查，重点查看网页上是否被挂有木马，或被 XSS 利用。

4 结束语

伴随网络技术的极速发展，Web 服务的技术种类和涉及范围越来越宽泛，Web 服务安全的防范工作也是越来越复杂。Web 服务的安全性的提高有赖于对所有相关环节的安全性的同步提高，要综合利用各种有效的手段和可能的资源对 Web 服务的安全进行防护，努力做到防患于未然，使 Web 更好的服务于人类生产。

参考文献：

[1]段江涛.王保保.基于 Web Service 的应用系统构架研究[J].计算机仿真.2005（5）.

[2]裴华.卿昱.基于 SOA 的 Web 安全通信模型研究[J].信息安全与通信保密.2008（8）.

[3]王明飞.Web 服务安全体系结构的研究 [J].电脑知识与技术.2010（23）.

作者简介：

石慧（1979—），女，河南周口，硕士，讲师，研究方向：计算机网络。