广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(4):353~356
Vol. 25,No. 4 November 2009

Web 应用安全防护措施及应急预案
Web Application Platform for Security and Contingency Plans

唐承华,韦皓元
TANG Cheng-hua,WEI Hao-yuan

(广西经济信息中心,广西南宁 530022)
(Guangxi Economic Information Center,Nanning,Guangxi,530022,China)

摘要:分析 Web 应用安全现状及常见的 Web 应用攻击技术,提出 Web 应用的安全防护措施和安全应急预案,以确保 Web 应用安全。Web 应用的安全防护措施包括操作系统和应用程序两个层面,Web 应用的安全应急预案包括安全事故应急处理和安全事故事后处理两个部分。

关键词:Web 应用 安全 防护 应急 研究
中图法分类号:TP393.08 **文献标识码**:A **文章编号**:1002-7378(2009)04-0353-04

Abstract: This thesis analyzes the present security situation in Web application. The protective measures and the emergency plan to ensure the security of the Web application are proposed. The protective measures were composed of two gradations-operating system and application program. The emergency plan should contain the emergency treatments as the security accidents happening and post process.

Key words: Web application,security,protection,emergency,research

随着全球信息化时代的到来,Web 技术以及基于互联网平台的 Web 应用得到了迅速发展,为互联网的发展增添了不少活力。然而,随之而来的信息安全问题也日益突出,根据 Gartner 的最新调查,信息安全攻击有75%都是发生在 Web 应用而非网络层面上[1]。同时,数据也显示,三分之二的 Web 站点都相当脆弱,容易受到攻击。在绝大多数的网络安全措施中,人们将大量的投资都花费在网络和服务器的硬件安全上,而没有从真正意义上保证 Web 应用本身的安全。如何在推动社会信息化进程中加强 Web 应用的安全,已经成为信息安全研究领域必须要认真对待的一个问题。本文在分析 Web 应用安全现状的基础上,提出 Web 应用的安全防护措施和安全应急预案,以确保 Web 应用安全。

收稿日期:2009-10-10
作者简介:唐承华(1981-),男,助理工程师,主要从事 Web 应用开发及安全研究工作。

1 Web 应用安全现状及常见攻击技术分析

1.1 Web 应用的安全认识误区

为了保障 Web 应用的安全,人们通常会在各个工作层面部署自己的安全策略,比如在客户端机器安装防病毒软件来保护计算机的安全,使用 SSL(安全套接层)技术对传输数据进行加密,搭建防火墙和 IDS(入侵诊断系统)/IPS(入侵防御系统)来过滤一些非法的访问等等。这些防护措施虽然可以关闭不必要暴露的端口,过滤一些非法的访问,但是远远不能保障 Web 应用的安全。Web 服务所依赖的80和443端口是必须开放的,防火墙很难辨别出通过这两个端口传输的数据是恶意的还是善意的,只要访问可以顺利通过防护措施,Web 应用就毫无保留的呈现在用户面前,针对应用层面的攻击也就可以轻松的突破防火墙保护的网站。例如:最为常见的 SQL 注入攻击表现层面完全是正常的数据交互查询,对于防火墙或者入侵检测系统而言,这是最为正常的访问连接,没有任何特征能够说明此种访问连接存在恶意攻击。所以,安装杀毒软件、搭建防火墙、

IDS、通过 SSL 加密等并不能完全确保 Web 应用的安全。

1.2 Web 应用的安全现状

根据国内信息安全厂商瑞星数据中心最新统计数据，2009年上半年，仅中国大陆，瑞星“云安全”系统拦截到的挂马网页数累计达2.9亿个，共有11.2亿人次网民遭木马攻击，平均每天有622万余人次网民访问挂马网站；其中大型网站、流行软件被挂马的有35万个(以域名计算)，比去年同期有大幅度增长[2]。从这些统计数据可以看出，目前的互联网非常脆弱，90%以上的木马病毒通过“挂马”方式传播，这些几乎都源于 Web 安全领域上的问题，如 Web 应用服务器的系统漏洞、后台服务器存在不安全设置、Web 应用程序实现代码缺陷(如 SQL 注入、跨站脚本等)、IIS 漏洞、Apache 漏洞等隐患，给黑客可乘之机。而这些隐患发起攻击的有75%出现在 Web 应用程序本身，这是防火墙、SSL、入侵检测系统无法预防、解决和应对的。

1.3 Web 应用常见攻击技术分析

当前，关于 Web 应用漏洞的攻击已经多达几百种。最近美国权威 Web 安全非赢利组织 OWASP 发布的10 大 Web 应用安全漏洞排名中，“跨站脚本攻击(CSS or XSS)、SQL 注入攻击”等10种攻击就是 Web 应用程序安全本身最典型的例子[1]。我们以常见的跨站脚本攻击和 SQL 注入攻击为例简要分析 Web 应用攻击技术。

1.3.1 跨站脚本攻击

跨站脚本攻击是用户向 Web 应用提交的数据未进行有效的过滤或转换，允许攻击者插入恶意 Web 代码，劫持用户会话、篡改网页信息甚至引入蠕虫病毒等。它通常是通过页面表单提交注入到 Web 应用中，然后在浏览器客户端执行。例如，我们在一个没有经过安全设计的留言板在正文输入这样的代码：<script>alert(document.cookie);</script>。而当用户打开这一个留言时 IE 便会弹出一个警告框，内容显示的是浏览者当前的 cookie 串。如果注入的不是以上代码，而是一段精心设计的恶意脚本，当用户浏览这个留言时，cookie 信息就可能被攻击者获取。此时用户的帐号就很容易被攻击者掌控。

1.3.2 SQL 注入攻击

SQL 注入的原理就是通过客户端提交非法字符，以达到修改页面、数据，在网页中添加恶意代码或网站挂马等操作。以下 SQL 代码是用户 Web 应用入口登录验证的查询语句：

```
SELECT count(*)
FROM users _ table
WHERE username='XXXX'
AND password='YYYY'
```

只要当用户输入用户名 XXXX 和密码 YYYY 正确时，这条语句的执行结果将为真(True)，否则为假(False)，为真时认证通过，为假时认证失败，即非法登录。如果我在输入用户名和密码的时候输入如下的内容：

用户名：a' or 'a'='a

密码：a' or 'a'='a

用代入法把用户名和密码输入值代入到上述的 SQL 语句，结果如下：

```
SELECT count(*)
FROM users _ table
WHERE username='a' or 'a'='a'
AND password='a' or 'a'='a'
```

通过这样的注入，这条语句的执行结果就永远是真。这个时候攻击者就能够通过认证，进入系统后台对系统进行破坏。

以上是 Web 应用安全隐患里最典型的例子，造成被攻击的原因主要是在程序开发的过程中，程序员没有注意控制脚本注入的语法要素，如没有对 javascript 语言中的“<”、“>”、“(”、“)”、“;”等一些非常字符进行过滤或转义处理。

2 Web 应用的安全防护措施

做好 Web 应用的基础防护对 Web 服务器安全来说至关重要，好的防护措施能够让服务器抵挡80%以上的漏洞攻击[3]。防护措施的实施包含操作系统层面和应用程序层面两部分，每部分都不可或缺，直接决定着整个 Web 系统的整体安全。

2.1 操作系统安全防护措施

操作系统是抵御 Web 非法攻击的第一道防线，保护操作系统的安全对 Web 的安全非常重要。操作系统安全防护措施主要包括以下几个方面：(1)实时更新系统补丁，避免恶意攻击者使用系统漏洞进行攻击。(2)关闭不必要的通讯端口。端口是攻击者的入侵大门，关闭不必要的通讯端口，可以减少入侵的通口。(3)规范的密码管理制度。服务器上各种登陆密码，应统一生成，集中管理。(4)谨慎安装系统组件和软件，关闭所有不必要的服务以减少安全隐患。(5)按最小权限原则对文件系统进行设置，这是避免提权操作和跨站脚本攻击的好办法。

2.2 应用程序安全防护措施

应用程序安全包含 Web 服务软件的安全和在软件上运行着的业务系统代码安全。相对于操作系统的安全防护,做好应用程序安全的技术要求更高。应用程序安全防护措施主要包括以下内容:(1)部署安全可靠的 Web 应用程序。Web 应用程序安全设计的目的是消除漏洞,所以设计人员必须对 Web 应用的开发有一套详细、周密的思路,对 Web 页面进行有意识的验证和加密处理,而不是单单只为了实现某个功能。同时,部署安全的 Web 应用才能真正解决 Web 应用层面上的安全问题。(2)根据业务系统的需要,配置安全的 Web 服务。如关闭执行程序权限,控制业务系统读写磁盘权限等。(3)建立 Web 防御检测系统。采用 Web 防御检测系统实时监控 Web 应用的运行状况,第一时间掌握 Web 应用的安全动态,以便做出相关的应对措施,把安全风险降至最低。(4)安装防病毒软件。防病毒软件可以防止黑客通过漏洞上传病毒文件至服务器,同时也能对正常维护过程中可能感染病毒的操作进行监控,确保服务器上的文件是安全无毒的。(5)建立用户分级和审核制度,区分系统管理员和普通用户,设置健壮的密码。

3 Web 应用的安全应急预案

绝对的安全是没有的,当遇到攻击者入侵,正常工作被影响的时候,我们还需要有一套应急预案,以把损失降到最低,尽快恢复工作秩序,以保障 Web 应用的安全。我们提出一个 Web 应用的安全应急预案,该预案包括安全事故应急处理和安全事故事后处理两部分。

3.1 安全事故应急处理

3.1.1 不良信息事故紧急处理

(1)一旦发现不良信息(或者被黑客攻击修改了网页),立刻关闭 Web 应用,并备份不良信息出现的目录、一个星期内的 HTTP 连接日志及网络连接日志。隔离出现不良信息的目录,使其不能再被访问。

(2)删除不良信息,并清查整个网站所有内容,确保没有任何不良信息,重新开通网站服务,并测试网站运行。

(3)修改不良信息目录名,对该目录进行安全性检测,升级安全级别,升级程序,去除不安全隐患,关闭不安全栏目,重新开放该目录的网络连接,并进行测试,正常后,重新修改该目录的上级链接。

(4)全面查对 HTTP 日志,防火墙网络连接日志,确定该不良信息的源 IP 地址,并迅速向公安机关报案。

3.1.2 恶意攻击事故紧急处置

(1)发现出现网络恶意攻击,立刻确定攻击源在哪里,判断是否需要紧急切断 Web 服务器的网络连接,以保护重要数据及信息。

(2)查出对方 IP 地址并过滤,同时对防火墙设置针对此类攻击的过滤,并视情况严重程度决定是否报警。

(3)当有网页内容被篡改,或通过入侵检测系统发现有黑客正在进行攻击时,首先应将被攻击的服务器等设备从网络中隔离出来,技术人员立即进行被破坏系统的恢复与重建工作。

3.1.3 病毒安全紧急处置

当发现有计算机感染病毒后,应立即将该计算机从网络上隔离出来,对该设备的硬盘进行数据备份。启用反病毒软件对该计算机进行杀毒处理,同时使用病毒检测软件对其他机器进行病毒扫描和清除工作。

3.1.4 应用系统和数据库遭受破坏性攻击的紧急处置办法

重要的软件系统平时必须存有备份,与软件系统相对应的数据必须有多日备份,并将它们保存于安全处。一旦软件遭到破坏性攻击,应立即向技术人员、网络管理员报告,并将系统停止运行。网站维护员立即进行软件系统和数据的恢复。

3.2 安全事故事后处理

在安全事故发生后,我们除了及时采取相应的应急处理外,还要做好以下几个方面的工作。(1)确保 Web 应用信息安全为首要任务。迅速发出紧急警报,所有相关安全成员集中进行事故分析,确定处理方案。(2)确保其它接入设备的信息安全。经过分析确认之后,可以迅速关闭、切断其他接入设备的所有网络连接,防止滋生其他接入设备的安全事故。(3)分析网络,确定事故源。使用各种网络管理工具,迅速确定事故源,按相关程序进行处理。(4)事故源处理完成后,逐步恢复网络运行,监控事故源是否仍然存在。(5)针对此次事故,进一步确定相关安全措施、总结经验,加强防范。(6)从事故一发生到处理的整个过程,必须及时向安全领导小组汇报,解释此次事故的发生情况、发生原因、处理过程听从安排,注意做好保密工作。

4 结束语

本文介绍了 Web 应用的安全现状,并对一些常

见的 Web 应用攻击技术进行分析，最后提出 Web 应用的防护措施及应急预案。但是在 Web 应用的安全领域中，本文所涉及的层面只是其中的一小部分，更多的问题还需要人们做更进一步探讨和研究。

参考文献：

[1] 斯卡姆布雷，施玛. 黑客大曝光：Web 应用安全机密与解决方案[M]. 北京：电子工业出版社，2008.

[2] 瑞星公司. 2009年上半年中国大陆地区互联网安全报告[EB/OL]. [2009-07-30]. http://www.rising.com.cn.

[3] 马恒太. Web 服务安全[M]. 北京：电子工业出版社，2007.

（责任编辑：韦廷宗）

（上接第349页）

的信心程度，立足在大制造环境信任的共性下，阐述目前网格环境下信任的研究现状，分析制造网格环境下信任的特殊需求及其特点，并提出制造网格环境下的信任管理新思路。本文仅是制造网格下基于域的信任管理模型的基础内容。该模型的信任关系建立、信任评估公式、信任更新公式、信任值存储策略以及具体的实现算法和实验将在下一步的工作中实现。

参考文献：

[1] 范玉顺. 制造网格的概念与系统体系结构[J]. 航空制造技术，2005(10)：42-45.

[2] 刘丽兰. 制造网格及其基于 QoS 的资源管理系统研究[D]. 上海：上海大学，2004：6-11.

[3] 蔡红霞，俞涛，方明伦. 制造网格中访问控制的研究[J]. 计算机集成制造系统，2007，4(13)：716-720.

[4] 胡业发，陶飞，周祖德. 制造网格资源服务 Trust-QoS 评估及其应用[J]. 机械工程学报，2007，43(12)：203-211.

[5] Farag Azzedin，Muthucumaru Maheswaran. Evolving and managing trust in grid computing systems[M]// Canadian Conference on Electrical andComputer Engineering. Available：IEEE ComputerSociety，2002：1424-1429.

[6] Beth T Borcherding M，Klein B. Valuation of trust in opennetwork[M]//GOLLMANN D. Proc of European Symposium on Research in Security(ESORICS). Brighton：Springer-Verlag，1994：3-18.

[7] Josang A，Knapskog S J. A metric for trusted systems [C]. Proceedings of the 21st National Security Conference，NSA，1998.

[8] Josang A，Grandison T. Research proposals on trust modelling[C]. Thursday，2002.

[9] Josang A，Hird S，Faccer E. Simulating the effect of reputation systems on e-markets[C]. In the Proceedings of the First International Conference on Trust Management，Creece，2003：179-194.

[10] 唐文，陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报，2003，14(8)：1401-1408.

[11] Azzedin F，Maheswaran M. A trust brokering system and its application to resource management in public-resource grids [C]. 18th International Parallel and Distributed Processing Symposium (IPDPS' 04)，2004：22-23.

[12] 张涛，何岩利，邓磊，等. 制造网格环境下的制造资源信誉度模型研究[J]. 计算机工程与应用，2009，45(1)：211-212.

[13] 徐锋，吕建，郑玮，等. 一个软件服务协同中信任评估模型的设计[J]. 软件学报，2003，14(6)：1043-1051.

（责任编辑：邓大玉）