Web应用安全风险防护分析与防护研究

窦 浩,武艳文,段升强

(西安建筑科技大学信息网络中心,陕西 西安 710055)

摘 要:分析了当前Web应用所面临的安全性问题以及重要性,同时分析了Web应用安全特性,给出了十大安全风险的描述并针对每一个安全风险给出了切实有效的防范措施与解决方案,包括注入式攻击、跨站点脚本攻击、错误的认证和会话管理、不安全的直接对象引用、跨站点伪造请求、不安全的配置管理、不安全的密码存储器、无法限制URL访问、薄弱的传输层保护、未验证的网址重定向.针对当前的各种Web应用安全的问题,给出了常见的安全技术及其描述.

关键词:安全性;Web应用;安全特性;安全风险;安全技术

中图分类号:TP393.08 **文献标志码**:A **文章编号**:1006-7930(2012)03-0446-06

互联网技术的日益成熟,使得人们越来越依赖于互联网,互联网已经发展成为人们生活中一个不可或缺的部分.虽然随着Web新技术的高速发展,Web应用在功能和性能上都得到了很大地提高和完善,但是在安全性上,由于Internet的开放性、交互性以及在Web应用设计时对信息的保密和系统安全性考虑不够完备,使得针对Web应用的攻击和破坏事件层出不穷,对人们的日常生活和经济社会造成了很大的麻烦:①2010年2月15日,中央电视台官方网站间歇性无法登陆,www.cctv.com主页变成一衣着暴露的欧美女子照片;②2010年1月12日,著名中文搜索引擎网站百度遭伊朗黑客组织入侵,导致用户无法正常访问百度;③2009年11月4日和2009年11月11日,少林寺官方网站两度被黑,导致网上出现"释永信悔过书"的假消息,在社会上造成恶劣影响.图1为2006－2010年中国被黑站点数量统计图[1].

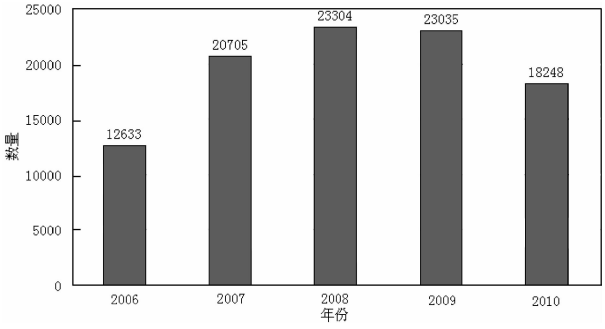

图1 2006－2010年中国被黑站点数量统计图

Fig. 1 2006－2010 the charts of sites were hacked in China

对于Web应用安全性的防护问题,已经成为了当前必须引起足够重视的问题.本文给出了Web应用安全特性,同时分析了常见的Web应用安全风险,并针对每个风险给出了详细的防范措施和解决方案,第三节详细的给出了针对Web应用安全的各种安全技术.

1 Web应用安全特性

由于Web应用一般采用分层体系结构,客户端与服务器端分离,使得Web应用的安全性与传统的应用程序的安全性有所不同,它更容易受到来自Web上的攻击与入侵,具体来说,Web应用的安全性具有如下几个方面的特性:

1.1 Web应用开放性

Web应用具有很强的开放性,导致了它在安全上易受攻击,这主要体现在三个方面:一是状态信息

收稿日期:2011-10-24 **修改稿日期**:2012-05-03

基金项目:国家2008年下一代互联网业务试商用及设备产业化专项(CNGI2008-060);国家科技支撑计划资助项目(2008BAH37B05060)

作者简介:窦 浩(1976-),男,陕西西安人,硕士,工程师,主要从事网络管理、网络安全工作.

的开放性,HTTP 协议是无状态的,Web 应用的开发人员需要自己记录程序运行的状态信息,并在客户端和服务器端进行保存和传输,这些信息对终端用户公开,容易被恶意更改和伪造. 二是源代码的开放性,Web 应用的客户端程序一般由 JavaScript 等脚本语言编写而成,其源代码对于用户而言是暴露在外可见的,此外还有些用 Java 编写的 Applet 程序,也可以通过反编译的方式得到其源代码,恶意用户可以通过修改源代码来进行攻击. 三是执行顺序的开放性,Web 应用的执行通过多次页面请求来实现,恶意用户很容易跳过某些程序执行步骤,而直接去执行后面的内容,从而造成安全问题.

1.2　信息流通双向性

传统信息发布一般为单向的,包括电子出版系统图文电视、语音应答、传真应答系统,而与此不同,Web 包含了文本、音频、图像、视频等多种媒介,这使得 Web 应用更容易受到来自 Internet 的攻击.

1.3　服务器容易受到攻击

安装有 Web 应用的服务器一般都挂接在 Internet 上,而计算机只要接入 Internet,服务器上的操作系统、系统配置都可能遭受到病毒、木马等恶意程序的入侵以及攻击者的非法攻击,由于任何操作系统都不可避免的会存在漏洞或是缺陷,所以攻击者可以利用这些缺陷进行攻击、盗号等非法活动.

1.4　开发人员的局限性

许多 Web 应用开发人员不知道如何开发安全的应用程序或是不太注重 Web 应用的安全性,在 Web 应用开发的过程中很容易忽略掉 Web 应用的安全性问题. 他们的经验也许是开发独立应用程序或 Web 应用,这些应用程序没有考虑到在安全缺陷被利用时可能会出现的灾难性后果,所以也很难及时地采取有效措施对这些安全风险进行降低消除.

1.5　底层应用软件漏洞众多

虽然 Web 浏览器非常易于使用,Web 服务器相对而言易于配置和管理,Web 内容也易于开发,但是其底层的软件却非常复杂,很难有软件能够做到不存在任何漏洞或缺陷,它们都隐藏潜在的安全漏洞.

1.6　用户错误操作

Web 应用的一般用户通常缺少足够的安全防范意识,没有经过系统训练,对 Web 应用的安全性重视不够,也不具备安全风险的概念,更没有采取有效措施以消除不安全因素的知识或工具.

Web 应用的这些安全特性,使得现今针对 Web 应用的安全问题层出不穷,已经极大的危害到了 Web 应用的发展.

2　Web 应用安全风险与防护

Web 应用安全不仅仅与系统服务及网络安全有很大关系,更重要是的 Web 应用自身的安全. Web 应用安全问题指的是攻击者可以通过 Web 应用本身使用很多不同的手段来对商业和组织进行破坏行为,而每一个这种手段都代表了一个安全问题.

2.1　十大安全风险与防范措施

据世界上最知名的 Web 安全与数据库安全研究组织 OWASP[2](Open Web Application Security Project)提供的报告显示,2010 年 Web 应用的十大安全风险是注入式攻击、跨站点脚本攻击、错误的认证和会话管理、不安全的直接对象引用、跨站点伪造请求、不安全的配置管理、不安全的密码存储器、无法限制 URL 访问、薄弱的传输层保护、未验证的网址重定向. 这些安全风险的存在极大地威胁着 Web 应用的安全,以下将重点分析这些风险并给出相应的防范措施.

2.1.1　注入式攻击

注入式攻击,典型的对操作系统的调用、使用 shell 命令来调用外部程序以及通过 SQL 诸如来调用后台数据库,会在不可信的数据作为命令或者查询语句的一部分被发送给处理程序的时候发生,攻击者发送的恶意数据可以欺骗处理程序,以执行计划外的命令或者访问未被授权的数据.

预防注入式攻击最核心的一点就是要把不可信数据与命令或者查询语句彻底分隔开. 具体而言,可以采取以下措施:①推荐使用安全的 API. 其中就包括使用带参数的存储过程. 需要注意的是,使用带参

数的存储过程依然有可能有注入式缺陷;②如果不能使用 API,那就手动的检测和过滤特殊字符,例如单引号等;③在验证输入数据的时候使用“白名单”的方式也可以有效防止注入式攻击.

2.1.2 跨站点脚本攻击

跨站点脚本攻击(Cross Site Script,XSS 或 CSS)是指攻击者向 Web 页面中插入恶意代码,当用户浏览该页面的时候,嵌入在该页面中的恶意代码会被执行,从而达到恶意攻击用户的目的. XSS 允许攻击者在受害者的浏览器上执行脚本,于是攻击者可以劫持用户会话,破坏 Web 站点或者将用户页面跳转至恶意站点. 图 2 为跨站点脚本攻击示意图.

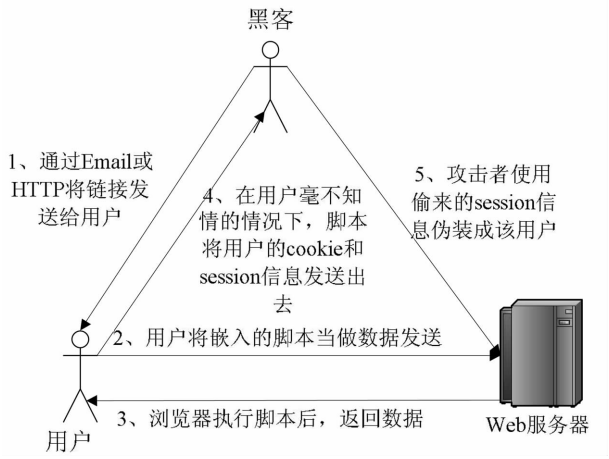

图 2 跨站点脚本攻击示意图

Fig. 2 Schematic of a cross-site scripting attacks

XSS 通常以嵌入式的 JavaScript 的形式出现,但其他的嵌入式内容也有可能存在危险,例如 ActiveX、VBScript 等,按照一定的规范来验证所有的头部、Cookie、查询串、表项和隐藏项是保护 Web 应用免受 XSS 攻击的有效方法,对用户提供的输出进行编码来防止被插入的脚本以可执行的形式传输到用户,如将一些特殊的字符转化成合适的 HTML 编码也可以有效地预防 XSS 攻击.

2.1.3 错误的认证和会话管理

通常 Web 应用的功能往往和权限管理、会话管理相关,但是却经常没有被正确的实现. 以至于让攻击者可以窃取到密码、密钥、会话 tokens 或者冒充其他用户身份.

合理的使用自定义的或者通用的认证和会话管理机制,需注意一些关键问题,主要表现为以下几个方面的内容[3]:①通过限制密码的长度和复杂度增加密码强度;②限制并记录使用密码进行错误登录的次数以及相关信息;③完善的密码修改控制;④以散列函数或加密的方式存储密码;⑤保护传输中的认证信息,使用 SSL 保护会话 ID;⑥不允许以假名的形式列出账号;⑦不用浏览器缓存认证和会话数据;⑧建立可靠的信任关系等.

2.1.4 不安全的直接对象引用

一个直接对象引用发生在当一个开发人员曝光一个引用给内部的实施对象时,例如一个文件、目录或一个数据库键码,由于 Web 应用没有对 URL 地址栏中输入的内容进行有效的访问控制检查或其它保护措施,致使攻击者可以在 URL 地址后加入特殊的字符,如“../”,来对 Web 应用中的实际对象,如文件、目录等进行查看,甚至可以对它们进行修改和删除.

预防这一安全风险需要选择一种方法来保护每一个用户可访问的对象,一般建议避免将私密文件直接暴露给用户,同时验证所有文件是否为正确文件或是使用 index/Hash 等方法,而非直接方式读取文件.

2.1.5 跨站点伪造请求

跨站点伪造请求(cross-site request forgery,CSRF)攻击的特点是强迫受害者的某个已进行登录操作的浏览器向安全保护薄弱的页面发送一条伪造的 HTTP 请求,包括受害者会话缓存内容及其他任何自动产生的包含认证信息的内容. 这就导致了攻击者可以通过强制受害者浏览器向具有漏洞的应用程序传递请求的方式,使相关的应用程序认定该请求是受害者本人所发出的合理请求.

图 3 为一个 CSRF[4] 攻击图示例,攻击站点导致该游浏览器发送一个请求到信任站点. 信任站点见是一个来自页面浏览器的已被认证的有效请求,就执行信任动作. 因为页面站点认证了该页面浏览器,而不是用户,这样 CSRF 攻击发生了.

防范 CSRF 攻击一般分为服务器端防范和客户端防范两个方面. 服务器端一般采用以下几个方面的防范措施:①对 Web 应用所有接受用户输入的内容进行严格的过滤;②Get 方法只用于从服务器端

读取数据,POST 方法用于向服务器端提交或者修改数据;③在所有 POST 方法提交的数据中设置一个类似于随机数的参数或是一个根据日期计算的 Hash 值,并且在 Cookie 中也保存这个参数;④利用 Cookie 安全策略的安全属性,只信任同源策略.

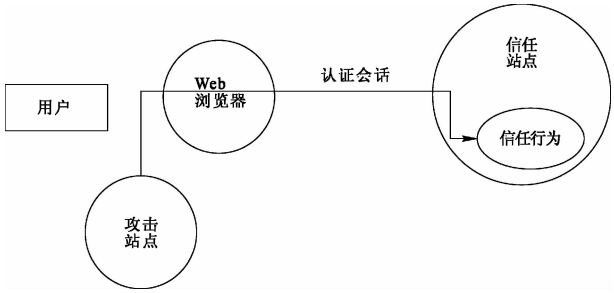

图 3　一个 CSRF 攻击示例

Fig. 3　Example of a CSRF attack

2.1.6　不安全的配置管理

好的安全需要有一个安全的配置和部署,包括对框架、应用服务器、Web 服务器、数据库服务器以及平台的设置必须正确,不能存在着安全问题,具体而言,配置管理主要需要注意以下问题:①服务器软件漏洞和错误配置允许列出目录和目录遍历攻击;②不必要的缺省、备份或例子文件,包括脚本、应用程序、配置文件和页面;③服务器软件安全更新;④不正确的文件和目录权限;⑤缺省密码和账号;⑥运行不必要的服务;⑦不正确的通过外部系统验证;⑧使用缺省证书;⑨提供太多信息的错误信息;⑩被激活的、能够被反问的管理和调试功能;⑪不正确的 SSL 证书和密码设定.

2.1.7　不安全的密码存储器

很多 Web 应用都没有使用或使用较弱的加密或散列算法(例如 MD5/SHA1)来保护敏感数据,例如信用卡、SSNs 和认证证书,攻击者可能窃取或修改这样脆弱的数据来进行信用卡欺骗等犯罪行为.

最主要得方法是确保应当被加密的事物都确实已经被加密,然后确保加密机制正确的执行,有许多的加密方式是不适当的,以下建议可以纳入测试中以确保安全的加密处理:①使用比较安全的加密算法,例如 ASE、RSA public key cryptography 和 SHA-256 等;②不要使用强度较弱的算法,比如 MD5/SHA1 等,选择 SHA-256 算法或更安全的方案;③离线产生私钥并特别保存,不要在不安全的通信途径传送私钥;④确保硬件中存储的加密资料不容易被解密.

同时,在系统设计与分析阶段,可考虑将这些算法引入,以提升资料安全的等级.

2.1.8　无法限制 URL 访问

很多 Web 应用通过链接或按钮等方式来访问受保护页面之前如果没有检查 URL 访问权限,攻击者可以通过 URL 直接存取能够拥有权限进入的页面,例如修改个人资料页面、个人隐私页面、关页面等.

具体而言,/admin,/backup、/logs,/phpmyadmin,/phpinfo.php,/manage 这些都是常见的路径和档案,攻击者如果能够猜测到这些就可以比较容易地操作主机了.

针对这种安全风险,一般采用 HTTP Service 直接限制来源 IP、使用防火墙阻挡、密码授权加密页面等方式来进行防范.

2.1.9　薄弱的传输层访问

应用程序经常无法验证、加密、保护敏感网络通信的保密性和完整性,在执行时,它们有时可以支持弱算法,使用过期或无效的凭证,或者不能正确使用它们.例如,攻击者窃听无线网络,偷取用户 Cookie.

因此,为了保护网络通信中资料不被窃取,最简单的方式是对整个站点都采用 SSL,但是由于性能的原因,很多站点只在私有页面才使用 SSL,其他一些只对关键页面使用 SSL,但是这样可能会暴露会话 ID 和其他敏感数据.

2.1.10　未验证的网址重定向

Web 应用经常重定向和转发用户到其他页面和站点,并使用不受信任的数据来确定目标的页面.没有正确的验证,攻击者可以通过钓鱼或恶意软件的站点或者使用未经授权的访问转发页面重定向受害者.

检查所有要导向或前往的页面的值,而这些值是根据外来的参数作为其值,例如用 Get 方式传递参

数,但如果能避免使用 redirect 或 forward,就尽量不要使用. 如果一定要使用,则尽可能不要讲使用者输入的参数作为要导向或前往的页面的值. 如果无法避免此种情形,则必须验证使用者输入的参数.

除了常见的十大安全风险外,还有一些 Web 应用的安全风险需要特别注意包括:缓冲区溢出、分布式拒绝服务等.

2.2 常见的 Web 应用安全技术

由于 Web 应用安全是一个系统工程,所以针对 Web 应用的诸多安全性问题,论文在表 1 中给出了常见的针对 Web 应用安全的技术及其分析.

表 1 Web 应用安全技术

Tab. 1 A list of security technology on Web application

名称	描述
加密	对需要进行伪装的机密信息进行变换.
验证码	产生一组随机的数字或符号进行输入确认.
认证	确保用户和服务器不是假冒的.
访问控制	在身份认证的基础上针对越权使用资源进行防范控制.
网络隔离	把两个或两个以上可路由的网络通过不可路由的协议进行数据交换.
数据备份与恢复	将系统数据备份下来,以保证数据意外丢失时能尽快恢复.
VPN (虚拟专用网)	利用密码技术和访问控制技术在公共网络上建立专用通信网络,使数据通过安全的"加密管道"在公共网络中传播.
安全脆弱性扫描	指出系统存在或潜在的安全漏洞,以改进系统对网络入侵的防御能力.
防火墙	构建网络之间的网络屏障.
防病毒	对病毒进行检测、清除和对抗.
入侵检测	对企图入侵、正在进行或已经发生的入侵进行识别.
云安全[5,6]	通过网状的大量客户端对网络中软件行为的异常进行监测,获取互联网中木马、恶意程序的最新消息,推送到服务器端进行自动分析和处理,再把病毒和木马的解决方案分发到每一个客户端.

没有哪一种安全技术可以完美解决 Web 应用的所有安全性问题,各种安全技术必须相互关联,相互补充,形成一个完整的体系,才能构建出一个更加安全的 Web 应用.

3 结 语

本文分析了 Web 应用安全问题的现状,给出了 Web 应用安全的诸多特性,并根据 OWASP 给出了 Web 应用的十大安全风险,并针对这些安全风险给出了应该采取的安全措施与防护手段. 然后讲了一些 Web 应用安全的一些防护技术,Web 应用安全防护是一个系统工程,需要在整个 Web 应用开发过程中都引起足够的重视.

参考文献 References

[1] 2006－2010 中国被黑站点数量统计[EB/OL]. http://www.zone-h.com.cn/
2006－2010 the statistics of sites behacked in China[EB/OL]. http://www.zone-h.com.cn/.

[2] 2010 年 Web 应用的十大安全风险[EB/OL]. https://www.owasp.org/index.php/OWASPTop10-2010-PressRelease.
Top10 security risks of Web applications[EB/OL]. https://www.owasp.org/index.php/OWASPTop10-2010-PressRelease.

[3] 丁 妮. Web 应用安全研究[D]. 南京:南京信息工程大学,2007.
Ding Ni. Research on security of Web applications[D]. Nanjing: Nanjing University of Information Science&Technology, 2007.

[4] WILLIAM Z, EDWARD W F. Cross-Site Request Forgeries: Exploitation and Prevention[EB/OL]. http://www.

freedom-to-tmker. com/sites/default/files/csrf. pdf,2008-09-29.
[5] Cloud Computing Security from an Enterprise perspective[EB/OL]. http://cloudsecurity. org/.
[6] Security issues associated with the cloud, Dimensions of the cloud security, Security and Privacy, etc[EB/OL]. http://en. wikipedia. org/wiki/Cloud_computing_security.

Analysis and research on security risk of Web application

DOU Hao, WU Yan-wen, DUAN Sheng-qiang

(Information and Network Center, Xi′an University of Architecture and Technology, Xi′an 710055, China)

Abstract: The security problem of Web application and its importance are analyzed in this paper. At the same time, the security property of the Web application is also analyzed and the description of the ten security risks and the responsed precautionary measure and resolution are given including Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management, Insecure Direct Object References, Cross-Site Request Forgery (CSRF), Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Insufficient Transport Layer Protection, Invalidated Redirects and Forwards. For various security problems of Web application, the conventional security technique and its description are recommended.

Key words: *security*; *Web application*; *security property*; *security risk*; *security technique*

Biography: DOU Hao, Engineer, Xi′an 710055, P. R. China, Tel: 0086-13991916968, Email: douhao@xauat. edu. cn

(上接第 445 页)

[11] BUCY J S, SCHINDLER J, SCHOLOSSER S W, GANGER G R. The Disksim Simulation Environment Version 4. 0Reference Manual. May. 2008.
[12] RUEMMLER C, WILKES J. UNIX disk access patterns[C]// Proceeding of the Winter USENIX Technical Conference, San Diego, USA, January 1993: 25-29.

Study of massive data migration strategy on data evaluation

BIAN Gen-qing[1], *WANG Yan-yun*[1], *SHAO Bi-lin*[2], *YU Yong-hao*[3]

(1. School of Information and Control Engineering, Xi′an University of Architecture and Technology, Xi′an 710055, China;
2. School of Management, Xi′an University of Architecture and Technology, Xi′an 710055, China;
3. School of Information Management, Nanjing University, Nanjing 210046, China)

Abstract: According to the importance of data migration in hierarchical storage management(HSM), the paper proposes a data migration model based on data valuation. Calculated in proportion by the inherent properties and the expected value of data, exact expression of the data value can be acquired. Combined with the migration process control strategy, the corresponding value of the data will be assigned to compatible storage device. Simulation results show, compared to LRU and LFU, the migration algorithm can make the vast majority of access hit in the on-line storage devices. With the increase of the number of access, the accuracy of the algorithm can be improved gradually.

Key words: *HSM*; *Data MigrationTechnology*; *Inherent Property*; *Expected Value*

Biography: BIAN Gen-qing, Associate Professor, Xi′an 710055, P. R. China, Tel: 0086-13319273850, E-mail: bgq_00@163. com