文章编号：1005-8451（2016）06-0045-03

Web网站的安全问题及防护策略

李　尚
（国家新闻出版广电总局　机关服务局，北京　100866）

摘　要：本文针对Web网站的安全现状进行分析，介绍目前常见的对Web网站攻击的手段和危害，探讨如何采取相应的防护策略加固网站的安全。

关键词：计算机网络；网站安全；防护
中图分类号：TP393　　**文献标识码：**A

Security issues and protection strategies for Website

LI Shang
(Agency Service Administration, State Administration of Press, Publication, Radio, Film and Television, Beijing　100866, China)

Abstract: This article analyzed the security states to Website, introduced the common attack means and harm to the Website, discussed the corresponding protection strategy to strengthen the safety of Website.

Key words: computer network; Website security; protection

计算机网络技术被广泛应用在各行各业，改变了许多人的生活方式。网上购物，微信聊天，通过手机获取资讯等互联网应用已经融入到人们的生活。网络数据的安全问题成为了我们关注的焦点，在互联网及大数据快速发展的今天，如果网站存在安全漏洞，就会造成大量用户的数据泄密和不可估量的损失。解决 Web 网站的安全问题迫在眉睫。

1　Web网站安全现状分析

随着 Web 网站站点数量快速增长，人们不仅会访问境内的网站，也会连接到其他国家的网站，因此 Web 网站的安全问题变得更加严峻。Web 网站常见的安全隐患如下。

1.1　自然因素

计算机信息系统是智能机，由软件设施和硬件设施组成，机器设备容易受到自然因素的影响。例如，自然环境中的气温、火灾、空气湿度、化学物质的污染、声音污染等。由于计算机设备中没有防水、防潮、防震、防火等功能，所以没有防御自然灾害的能力。

1.2　网络系统因素

Internet 技术具有开放性，这是网络系统的优势，同样也是劣势。从网络安全角度来看，正是因为 Internet 技术的开放性，造成网络安全的巨大隐患。不法犯罪分子通过网络平台，恶意盗取计算机用户的信息，进行犯罪活动，造成用户的经济损失。

1.3　黑客恶意攻击

黑客的恶意攻击包含两方面：(1) 网络攻击，在用户使用网络的过程中进行数据破坏；(2) 不影响用户的正常使用，有目的性地进行信息窃取。

黑客攻击是对网络安全的重大威胁，不法分子利用非法的手段进行系统信息的盗取、窃听、修改、破坏等，导致系统数据的丢失和外泄，给国家的经济造成严重的损失。

1.4　用户因素

很多网站开发人员熟知网页的搭建和界面的美化，但网络安全的技能相对薄弱，从而导致网站在建成后存在很多常见的安全隐患。此外，网站在上线后，没有专职的安全维护人员对网站服务器进行安全补丁的更新，易被攻击者利用。

2　Web网站攻击手段和危害

2.1　SQL注入攻击

SQL 注入攻击利用服务器端代码自身存在的漏洞进行攻击，在 Web 客户端和服务器连接后，对数

收稿日期：2015-12-16
作者简介：李　尚，工程师。

据库后端进行攻击。这种攻击方式的优势在于，攻击者可以直接访问数据库，跳过了很多安全防护机制，进而使用非法获得的权限对非授权的数据进行访问。SQL 攻击存在大量的方法，十分灵活，攻击者可以根据 Web 应用程序中存在的各种漏洞，编写不同的脚本，选择最有效的攻击方法。最常见的 SQL 攻击分为以下 3 种：

（1）get 型注入，get 型 SQL 注入存在于带有参数的动态网页中。网站开发人员没有对参数进行过滤，攻击者可以使用 ID 所带的参数直接进入数据库中查询，轻易地得到网站数据库中的信息。

（2）post 型 SQL 注入，隐蔽性更强的攻击方式。post 方式传递数据应用于目前大多数网站后台登录框中，如果没有过滤，攻击者就能获取到管理员账号密码，提升权限，非法进入网站的后台管理系统。

（3）cookie 型 SQL 注入，在 ASP 语言中 request 对象获取客户端提交数据常用 get 和 post 两种方式。如果网站开发人员没有定义数据传递方式，通过 cookie 就可以获取客户端提交的数据，如果再对相应的数据过滤，cookie 注入就产生了。攻击者一般会在前两种方式失效后采取 cookie 型 SQL 注入的攻击方式。

SQL 注入攻击对网站的危害包括 4 个方面：

（1）网站数据库遭受攻击。数据库放置着所有用户信息等重要数据，一旦被窃取，导致网站用户的隐私信息落入攻击者手中，攻击者就可以从中获得非法利益。

（2）获得网站管理权限。数据库中存储着网站管理员的账户信息，管理员拥有网站管理系统的最高权限，一旦被非法获得，网站后台数据就会被篡改，网站页面也会直接被篡改。

（3）网站被植入木马。攻击者入侵网站后在系统内留下后门，网站服务器就变成了僵尸主机。

（4）直接破坏硬盘中的数据，致使系统遭到破坏。

2.2 XSS跨站脚本攻击

跨站脚本攻击（XSS）是由于 Web 开发者在编写应用程序时没有对用户提交的语句和变量中进行过滤或限制，攻击者通过 Web 页面向数据库或 HTML 页面中提交恶意的 html 代码，当用户打开有恶意代码的连接或页面时，恶意代码会自动执行，从而达到攻击的目的。

2.3 WebShell攻击

WebShell 是 Web 入侵的一种脚本工具，通常情况下，是一个 ASP、PHP 或者 JSP 程序页面，也叫做网站后门木马，在入侵一个网站后，常常将这些木马放置在服务器 Web 目录中，与正常网页混在一起。通过 WebShell，长期操纵和控制受害者网站。

2.4 目录遍历攻击

目录遍历攻击又称目录穿越、恶意浏览、文件泄露等，攻击者利用系统漏洞访问合法应用之外的数据或文件目录，导致数据泄露或被篡改。目录遍历攻击的危害在于，在攻击过程中，攻击者并不清楚网站的主目录位置，但是只要通过简单的测试就可以推断出结果。因而，通过目录遍历攻击，攻击者就可以突破网站主目录的限制，而去访问服务器上的敏感文件。

3 Web网站的防护手段

采取单一的手段无法解决当前的 Web 网站安全问题，需要针对不同的攻击方式采取不同的手段，再结合整体的构建，对 Web 网站实现多重加固。

3.1 SQL注入的防范

（1）对于 SQL 注入的防范关键是在源代码，要完善源代码，对每一个进入数据库查询的变量进行严格过滤。

（2）尽量设置复杂的 Web 网站后台目录，攻击者即使破解出用户名和口令，但是找不到后台路径就不可能上传恶意脚本。

（3）加强网站数据库的用户权限设置，Web 网站连接数据库的用户权限设置为最小，并以最小权限原则建立专门的账户，运行数据库服务。

3.2 XSS跨站脚本攻击的防范

（1）XSS 在用户输入处存在漏洞，必须对用户输入部分进行过滤。

（2）严格控制存储到服务器端的数据。

（3）使用 XSS 工具进行测试，一旦发现问题，马上处理。

3.3 WebShell攻击的防范

对于 WebShell 攻击的防范最关键是防止 ASP、PHP、JSP 等木马程序文件的植入。一般可以从以下几方面对安全性进行处理。

3.3.1 Web软件开发的安全

（1）程序中存在文件上载的漏洞，攻击者利用漏洞上载木马程序文件。

（2）防 SQL 注入、防暴库、防 COOKIES 欺骗、防跨站脚本攻击。

3.3.2 服务器的安全和Web服务器的安全

（1）服务器做好各项安全设置，病毒和木马检测软件的安装（WebShell 的木马程序不能被该类软件检测到），启动防火墙并关闭不需要的端口和服务。

（2）提升 Web 服务器的安全设置。

（3）对以下命令进行权限控制，以 Windows 为例：如 cmd.exe、net.exe、ping.exe、netstat.exe、ftp.exe、tftp.exe、telnet.exe 等。

3.3.3 ftp文件上载安全

设置好 ftp 服务器，防止攻击者直接使用 ftp 将木马程序文件上传到 Web 程序的目录中。

3.3.4 文件系统的存储权限

设置好 Web 程序目录及系统其它目录的权限，相关目录的写权限只赋予给超级用户，部分目录写权限赋予给系统用户。

3.3.5 不要使用超级用户运行Web服务

对于 apache、tomcat 等 Web 服务器，安装后要以系统用户或指定权限的用户运行，如果系统中被植入了 ASP、PHP、JSP 等木马程序文件，以超级用户身份运行，WebShell 提权后获得超级用户的权限进而控制整个系统和计算机。

4 使用Web应用防护系统加固网站安全

Web 应用防护系统（WAF，Web Application Firewall）是根据当今网络大环境应运而生的一类产品，WAF 用以解决诸如防火墙一类传统设备束手无策的 Web 应用安全问题，与传统防火墙相比，WAF 工作在应用层，能够针对应用层的攻击进行防范过滤。

通常情况下，WAF 放在企业对外提供网站服务的 DMZ 区域或者数据中心服务区域，Web 服务器是 WAF 所保护的对象，部署时要使 WAF 部署在 Web 服务器的前端，并尽量靠近 Web 服务器。WAF 设备一般设有 IPS 漏洞特征识别库、Web 应用防护识别库、实施漏洞分析识别库、数据泄密防护识别库、僵尸网络识别库，部署 WAF 后，可以对识别库内的各种攻击进行防护，并且设备厂家会提供识别库的更新，来应对最新的攻击手段。现在主流的 WAF 产品都能够对内网的网络安全状况进行评估，发现实时漏洞风险，记录安全事件，统计网络各端口或者 IP 的流量，并能从中识别出异常的流量。网络管理员可以清晰的掌握网络中各种安全问题，包括攻击的来源和攻击手段，进而采取相应的策略，来加固网站的安全。部署了 WAF 后，网站的安全得到了明显的加固。

5 结束语

通过对目前 Web 网站攻击手段的分析，采取相应的防范措施，可以使 Web 网站得到加固，然而，Web 网站没有绝对的安全，只有相对的完善，时刻都会有新的安全问题浮现出来。面对当前日益严峻的安全形势，网站安全防范必须从多角度、多层次入手，采取行之有效的技术手段和安全措施。

参考文献：

[1] 赵 真 . 浅析计算机网络的安全问题及防护策略 [J]. 上海工程技术大学教育研究，2010（3）：9-11.

[2] 冯永健 . 计算机网络的安全问题及防护策略 [J]. 计算机光盘软件与应用，2014（24）：203-205.

[3] 彭 珺，高 珺 . 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，2011，39（1）：121-124.

[4] 李 斯 . 校园网络安全问题及防护策略 [J]. 网络安全技术与应用，2009（9）：38-39.

[5] 黄顺华 . 军队计算机网络安全体系的研究 [D]. 重庆：重庆大学，2006.

责任编辑 陈 蓉