网络应用程序的安全设计

Security Design of Network Application Program

贺立红　李 丹　吴建华　（东北大学信息科学与工程学院 辽宁 沈阳 110004）

摘要：对网络编程中涉及到的web服务器安全与ASP脚本安全作了较全面的分析，并针对各种漏洞提出了相应的防护措施。

关键词：网络 IIS ASP 安全防护

我们进行网络编程、开发交互性网站，是为了发展建设自身的站点，但是这些都应建立在安全基础之上，这里的安全包括对自己开发的ASP或其他网络应用程序代码的保护，网站服务器的安全正常运行，用户信息的安全及认证等等，因此熟悉系统的运作，及时了解系统漏洞，第一时间解决安全性问题就显得十分重要和必要。

1　网络应用程序的安全性分析

目前，用于web网站设计的开发工具很多，但大多数网站都采用目前比较流行的IIS＋ASP＋SQL Server方案来组建，但该解决方案在给我们带来便捷的同时，也存在不同程度的安全隐患。

1.1 IIS的安全性分析

IIS(Internet Information Server)是微软公司主推的服务器，因为具有适应性强，对系统资源消耗少，管理和配置简单的特点，所以获得了广泛的应用，但由于自身和外部的种种原因，其安全问题也很突出。

1.1.1 Index Server 漏洞

IIS服务器如果运行了Index Server，会导致如下的常见漏洞。

(1) Null.htw 漏洞。Null.htw 漏洞会使未授权的用户查看ASP脚本的源代码。如果网络入侵者提供特殊的URL请求给IIS，就可以跳出虚拟目录的限制，进行逻辑分区和Root目录的访问。这是由于Index Server中没有很好地规范各种类型文件的请求，所以导致入侵者可以访问服务器上的任意文件。Null.htw功能可以从用户输入中获得3个变量：CiWebhitsfile、CiRestriction和CiHiliteType，入侵者可通过下列方法传递变量来获得诸如examp.asp文件的源代码：

http://www.targethost.com/null.htw?CiWebhitsfile=/examp.asp

(2) Webhits.dll和htw漏洞。如果输入下面的命令：http://www.targethost.com/nosuchfile.htw，服务器返回format of the QUERY_STRING is invalid信息就表示用户的主机存在Webhits.dll和htw漏洞。此漏洞允许Web用户在文档上突出其原始搜索的条目。文档的名称通过变量CiWebhitsfile传递给htw文件，ISAPI应用程序Webhits.dll处理此请求，打开文件并返回结果。当入侵者控制了CiWebhitsfile参数并传递给htw时，就可以请求任意文件，导致非授权查看ASP源代码和其他脚本文件内容。如入侵者在系统中发现如下的htw程序：

/iissamples/issamples/oop/qfullhit.htw，就会通过如下的方法来访问系统中文件的内容(如win.ini文件)：http://www.targethost.com/iissamples/issamples/oop/qfullhit.htw?

CiWebhitsfile=/../../winnt/win.ini&cirestriction=none&cihilitetype=full

1.1.2 Unicode 解析错误漏洞

IIS4.0和IIS5.0在Unicode字符解码的实现过程会出现一个安全漏洞，导致用户可以远程通过IIS执行任意命令。当IIS打开文件时，如果该文件名包含Unicode字符，它会对其进行解码，如果用户提供一些特殊的编码，将导致IIS错误地打开或者执行某些web根目录以外的文件。网络入侵者往往利用下面的方法利用此漏洞。首先，如果系统包含某个可执行目录，就可能执行任意系统命令。下面的URL可以列出当前目录

的内容：

http://www.targethost.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir

其次，利用这个漏洞可以查看系统文件内容：

http://www.targethost.com/a.asp/..%c1%1c../..%c1%1c../winnt/win.ini

1.1.3 NT Site Server Adsamples 漏洞

网络入侵者若执行下面的命令：http://www.targethost.com/adsamples/config/site.csc 就可以获得数据库中的 DSN、UID 和 PASS 等重要信息。

1.1.4 "+.htr" 漏洞

如果对某些 ASP 站点追加"+.htr"的 URL，如 http://www.targethost.com/.com/global.asa +.htr 也会造成文件源代码的泄漏。

1.2 ASP 的安全性分析

1.2.1 源代码漏洞

由于 ASP 程序采用非编译性语言，大大降低了程序源代码的安全性，如果黑客入侵站点，就可以获得 ASP 源代码。

1.2.2 程序设计中的 SQL Injection 漏洞

SQL Injection 指入侵者利用数据库的外部接口将其数据插入到数据库操纵语句，从而达到入侵数据库乃至系统的目的。通常攻击者通过表单输入构造 SQL 语句来达到目的。对于下面的用户登录验证 ASP 程序：

```
username = request.form("username")
password = request.form("password")
strsql = "select * from login where username = '"
&username &"'and password = '" &password &"'"
set RS = conn.execute(strsql)
```

入侵者可输入任何内容来构造 SQL 语句，如提交"username：li'_ _， password：abc123"则查询字符串 strsql 将变为"select * from login where username = 'li'_ _'and password = 'abc123'"，因为符号"_ _"在 SQL 中表示注释，其后的内容为注释内容，所以将查询用户名为 li 的所有记录，而不管密码。

入侵者还可构造 SQL 语句删除表 login：提交"username：li'drop table login _ _， password：abc123"，则查询字符串 strsql 将变为"select * from login where username = 'li'drop table login _ _'and password = 'abc123'"。

总之表单输入内容中符号"'"后面的内容都可执行。

1.2.3 程序发布中的漏洞

有些 ASP 程序员在程序中加入调试量，如

```
Debug = true
Trace = on
Log = on
```

这样如果代码出错就会显示详细的错误信息，入侵者可以利用这些信息进一步探测 web 站点。

2 网络应用程序的安全防护技术

2.1 IIS 的安全防护

对 IIS 漏洞最有效的防护方法就是及时升级软件，及时安装最新的补丁程序，另外还要充分利用操作系统的安全机制来提高 IIS 的防范性能，在其自身的安全机制设置上，应做到以下几点。

2.1.1 IIS 的安全安装

为了避免给系统带来巨大的潜在危险和使非法用户侵入系统分区，安装 IIS 时应避免将其安装在主域控制器上和系统分区上。

2.1.2 登录认证的安全性

IIS 提供给用户身份认证的第一种形式为安全级别最低的匿名访问，应对其权限加以控制，若无匿名访问需要可取消此服务。第二种是安全性能一般的基本验证，在此方式下用户输入的用户名和口令以明文方式在网络上传输，没有任何加密，非法用户可以通过网络监听程序截获数据包，从中获取用户名和密码。第三种是安全性能比较高的 windows NT 请求/响应方式，在此方式下浏览器通过加密方式与 IIS 服务器进行交流，有效地防止了监听。第四种是安全性更高的认证—SSL 安全机制。SSL 位于 HTTP 层和 TCP 层之间，建立用户与服务器之间的加密通信，确保所传递信息的安全性。设置时可启动 ISM（Internet 服务器管理器）并打开 web 站点属性页，选择"目录安全性"选项卡，单击"密钥管理器"按钮，通过密钥管理器生成密钥对文件和请求文件，从身份认证权限中申请一个证书，通过密钥管理器在服务器上安装证书，激活 web 站点的 SSL 安全性。建立了 SSL 安全机制后，只有 SSL 允许的客户才能与 SSL 允许的 web 站点进行通信，并且在使用 URL 资源定位器时，应输入 https://。

2.1.3 IP 地址的安全控制

利用 ISM 的设置可以允许或拒绝从特定 IP 发来的

服务请求，有选择地允许特定节点的用户访问服务。

2.1.4 端口的安全性实现

对于 IIS 服务，无论是 web 站点、FTP 站点还是 NNTP、SMTP 服务都有各自监听和接收浏览器请求的 TCP 端口号，常用的端口号为：WWW 是 80，FTP 是 21，SMTP 是 25，编程时可以通过修改端口号来提高 IIS 服务器的安全性。可见，如果修改了端口设置，只有知道了端口号的用户才可以访问，当然在访问时需要指定新的端口号。

2.2 ASP 的安全防护

若要避免 ASP 应用程序遭到破坏，首先应把最新的安全补丁加入底层系统软件中，其次是尽量少的提供不必要的服务，因为多开启一个服务，就要多面对几个漏洞的威胁，还要时刻提访由这个服务所引起的未知漏洞，如关闭 IIS 的 Index Server 服务，即可避免 Webhits. dll 和 htw 漏洞。

2.2.1 利用 Session 对象进行注册验证

为防止未经注册的用户绕过注册界面直接进入应用系统，可以采用 Session 对象进行注册验证。Session 对象最大的优点是可以把某用户的信息保留下来，让后续的网页读取。

如程序设计要求用户注册成功后系统启动 hrmis. asp? page = 1 页面。若不采用 Session 对象进行注册验证，则用户在浏览器中敲入“URL/hrmis. asp? page = 1”即可绕过注册界面，直接进入系统。利用 Session 对象可以有效阻止这一情况的发生。相关的程序代码如下：

```
<%
'读取用户输入的账号和密码
UserID = Request("UserID")
Password = Request("Password")
'检查 UserID 及 Password 是否正确
If UserID < > "hrmis" Or Password < >
"password" Then
Response. Write "账号错误!"
Response. End
End If
'将 Session 对象设置为通过验证状态
Session("Passed") = True
%>
```

进入应用程序后，首先进行验证：

```
<%
'如果未通过验证，返回 Login 状态
If Not Session("Passed") Then
Response. Redirect "login. htm"
End If
%>
```

2.2.2 SQL Injection 防护技术

（1）过滤符号“'”：将“'”过滤为“''”可使用函数 replace（输入量，“'”，“''”）来实现。

（2）限制输入内容：只允许输入指定的内容，或者排除带有攻击性的内容。

（3）不要使用数据库超级管理员 sa 权限连接数据库 SQL Server。

2.2.3 磁盘文件使用 NTFS 格式

NTFS 不仅具有 FAT 和 FAT32 的所有基本功能，而且还具有更多的安全控制功能，可以对不同的文件夹设置不同的访问权限。如果 web 服务器已经安装运行，应确保服务器上所有的硬盘分区都是 NTFS 格式，可以用内置的实用工具 convert 将 FAT 格式的分区无损地转换成 NTFS 格式。在命令行方式下执行：convert volume / fs：ntfs（volume 表示驱动器）；也可用磁盘管理工具来转换文件系统格式，将 FAT 格式转换为 NTFS，根据需要修改权限。

2.2.4 目录属性的安全设置

程序设计中应对目录设置不同的属性，如：Read、Excute、Script 等。可以通过配置 web 服务器的权限来限制所有用户查看、运行和操作用户 ASP 网页的方式。在设置 web 服务器权限时应遵循下列原则：

（1）对包含 ASP 文件的虚拟目录允许。

（2）对 ASP 文件和其他包含脚本的文件（如 HTML 文件等）在的虚拟目录允许“读”或“脚本”权限。

（3）对包含 ASP 文件和其他需要执行“权限”才能运行的文件（如 EXE 和 DLL 文件等）的虚目录允许“读”和“执行”。

2.2.5 利用 COM / DCOM 组件封装脚本

在 ASP 文件中只编写尽可能少的源代码，针对需要保护和加密的重要脚本封装到一个 COM / DCOM 组件，并在 ASP 创建该组件，然后调用相应的方法实现。

2.2.6 对 ASP 脚本加密

由于 ASP 脚本是采用明文编写，所以一旦发布到

（下转第 48 页）

(上接第 91 页)

运行环境去后,就很难保证这些源代码不会被流传出去,通常采用加密的方法来保护 ASP 源代码。

从微软公司的网站可免费下载 Sce10chs. exe 加密程序,安装完毕后,将生成 Screnc. exe 文件,运行"screnc – 1vbscript source. asp destination. asp"命令可生成包含密文 ASP 脚本的新文件 Destination. asp,用记事本打开查看,凡是"<%"和"%>"之间的内容,不管是否注解,都变成不可阅读的密文。

3 结束语

网络应用程序由于其自身和外部的种种原因很容易遭到攻击和破坏,所以作为网络应用程序开发者应正视网络安全,时刻关注最新的系统安全知识和信息,及时更新和下载系统软件和安全补丁,确保设计出的网站安全实用。

参考文献

1 章立民,SQL Server 2000 中文版完全实战[M],北京 中国铁道出版社,2001。

2 消志刚,ASP 动态网站设计[M],北京 清华大学出版社,2004。

3 (美)JonesA, Ohlund J. Windows 网络编程技术[M],北京 机械工业出版社,2000。

4 李海泉、李健,计算机网络安全与加密技术[M],北京 科学技术出版社,2001。