基于网站建设中网页设计的安全缺陷及对策

程文彬*

(电子科技大学中山学院 广东 中山 528402)

【摘要】讨论了基于网站建设中网页设计的安全缺陷，指出服务器端动态网页技术本身存在安全缺陷。介绍了登陆验证漏洞、绕过验证直接进入设计页面漏洞、桌面数据库被下载漏洞、源代码泄露漏洞和文件上传漏洞，给出了相应解决漏洞的方法。

关 键 词 网址; 加密; 网络安全; 活动服务器页面; 服务器端网页设计

中图分类号 TP393 文献标识码 A

Security Defect and Countermeasure of Web Page Design on Building Website

Cheng Wenbing

(Zhongshan College, UEST of China Guangdong Zhongshan 528400)

Abstract The security defect of Web page design on building website is discussed in this paper, server-side dynamic Web page exists security defect are presented. Introducing the landing check lack-hole, and around checking the direct entering design page hole, and the table date-base loaded hole, and the source code expose hole and file up hole, and giving corresponding solving way.

Key words website; adding secret; network security; active server pages; server-side dynamic Web page

随着电子商务的兴起，许多企业都建立了自己的商务网站，在构建网站的时候，都会考虑网络安全问题，对于网络安全的投入较大，如使用防火墙、入侵检测、企业防病毒等安全产品，但网站还是有被攻击甚至完全被控制的可能。因为企业的网站一般都采用ASP、PHP或JSP等脚本语言来连接数据库，取得数据库里面的数据生成动态网页。当一个网站完全建立后，程序会很多，特别是网页设计的特殊性，服务器与用户的交互程序更多，所以，程序的漏洞也会增多，给网站带来不可估量的安全隐患，这些程序漏洞比网站服务器的漏洞更为严重[1~3]。

1 网页设计安全漏洞的形成

ASP、PHP或JSP等脚本语言作为典型的服务器端网页设计技术，为网站开发人员提供了简单高效的动态Web应用程序开发方法。在网站设计时，使用上述脚本语言编程可以更好地管理网站资源，增加网站与浏览者之间的交互，如新闻发布系统、产品管理系统、会员管理系统、论坛反馈系统、在线调查系统、在线订单系统和留言板系统等，其共同点是用户输入很多资料，与其他浏览者交流或者与网站管理者交流。而交互正是漏洞形成的一大原因，因为用户输入信息不可预测，如果程序没有考虑或者考虑不全面，用户输入就有可能成为攻击事件，且不管有意还是无意。网页编程直接和服务器打交道，与网站目录、网站数据

2003年9月1日收稿

* 男 38岁 大学 讲师 主要从事计算机及多媒体技术等方面的研究

库设置、系统设置相关，通过这些程序访问网站目录、设置等所有服务器内容，若程序设计有漏洞，即网站有漏洞。

2 网页设计的安全漏洞及对策

2.1 登陆验证漏洞

凡带有交互性的网站，包括论坛、聊天室、信息网会员区、网上影院等，登陆验证是必不可少的组成部分。虽然登陆的验证程序只是网站整体的一部分，但却是网站的安全关口。网站设计者容易疏忽这一点，没有处理好口令验证程序的关口，以至他人趁虚而进，甚至造成重大影响与经济损失。许多网站都存在一个登陆验证的漏洞，而这个漏洞是在编写程序验证账号密码时由于程序不严谨而造成。如在设计网站会员区时，都会将账号、密码放在一个叫“User”的数据表中，并设置“username”和“password”两个字段分别表示用户的登录名称和登录密码。当验证时，检查用户输入的两个参数是否存在于这个数据表，如果存在，证明这个用户合法；不存在，证明用户不合法，而漏洞就出现在这段验证代码上。

在登陆验证(以asp为例)中常会用SQL查询语句来判断该用户是否为站点的合法会员。

```
<!--连接数据库-->
<!--#include file=dbconn.asp -->
<%
Dim rs
Set rs=CreateObject("Adodb.Recordset")  '定义一个Ado数据集实例
rs.source="select * from user where username='" & username & "' and password='" & password & "'"  '连接登陆验证语句字串
rs.open rs.sourc,conn,1,1 '执行查询语句
...
%>
```

当根据以上的sql语句构造一组特殊的用户名和密码，例如用户名为该网站任意一个存在的用户名Admin，密码为a' or 'a'='a，则程序中sql变量的值将会变成sql="select * from username where username='a' and password='a' or 'a'='a'" 显然，该查询语句的逻辑原意已被彻底改变，一个逻辑运算符or使用整个逻辑条件为真，即这条SQL口令验证语句已经失去了效用，只要知道了任意一个存在的用户名就可以成功地进入到敏感区域。解决漏洞的方案如下：1）在生成SQL查询语句之前，对用户输入的参数(用户名和密码)进行过滤；2）先查询用户名再进行密码验证。

2.2 绕过验证直接进入设计页面漏洞

每个敏感的页面必须进行身份验证，如果用户知道了一个设计页面（如用ASP）的路径和文件名，而这个页面又没有验证的程序，则用户可直接输入这个设计页面的文件名，即绕过了登陆验证，直接进入了指定的页面。网站设计者除了登陆验证外还必须在有关页面进行身份验证，才能提高站点的安全指数。

2.3 桌面数据库被下载漏洞

在ASP＋Access应用系统中，如果获得Access数据库的存储路径和数据库名，则该数据库可以被下载到本地。如对于网上图书馆的Access数据库，一般命名为Library.mdb等，而存储的路径一般为“URL/database”或放在根目录（“URL/”）下。这样，只要在浏览器地址栏中输入地址 “URL/database/Library.mdb”，就可以轻易地把Library.mdb下载到本地的机器中。

在ASP程序设计中，应尽量使用ODBC数据源，不直把数据库名直接写在程序中，否则数据库名将随ASP源代码的失密而一同失密，例如：

```
DBPath = Server.MapPath("./akkjj16t/ kjhgb661/acd/avccx55/faq19jhsvzbal.mdb ")
conn.Open "driver={Microsoft Access Driver (*.mdb)};dbq=" & DBPath
```

可见，ASP源代码失密后，数据库也很容易被下载。如果使用ODBC数据源，则不会存在 conn.open “ODBC－DSN名”。

2.4 源代码泄露漏洞

为有效防止源代码泄露，可以对页面代码进行加密。一般有以下两种方法对ASP页面进行加密：1) 使用组件技术将编程逻辑封装入DLL中；2) 使用微软的Script Encoder对ASP页面进行加密。使用组件技术存在的主要问题是每段代码均需组件化，操作比较烦琐，工作量较大，而使用Script Encoder对ASP页面进行加密，操作简单、收效良好。Script Encoder方法具有以下优点：

(1) HTML具有很好的可编辑性，Script Encoder只加密在HTML页面中嵌入的ASP代码，其他部分仍保持不变，故仍可以使用FrontPage或Dreamweaver等常用网页编辑工具对HTML部分进行修改、完善，但不能对ASP加密部分进行修改，否则将导致文件失效；

(2) 操作较简单，只要掌握几个命令行参数即可，Script Encoder的运行程序是screnc.exe，其使用方法如下：

screnc [/s] [/f] [/xl] [/l defLanguage] [/e:defExtension] inputfile outputfile

其中 s为屏蔽屏幕输出；f为指定输出文件是否覆盖同名输入文件；xl指是否在.asp文件的顶部添加@Language指令；l为defLanguag指定缺省的脚本语言；e为defExtension 指定待加密文件的扩展名；

(3) 使用Script Encoder可以对当前目录中所有的ASP文件进行加密，并把加密后的文件统一输出到相应的目录中，例如：screnc ＊.asp c:\temp；

(4) Script Encoder是免费软件，该加密软件可以从微软网站http://msdn.microsoft.com/scripting/vbscript/download/x86/sce10en.exe下载，下载后，运行安装即可，利用Session对象进行注册验证。

2.5 文件上传漏洞

许多网站如论坛、同学录、邮件服务系统都提供了文件上传的功能，但设计者在设计用户提交参数缺少充分过滤，以至远程攻击者利用这个漏洞可以上传恶意文件，甚至造成系统数据库破坏或以Web权限在系统上执行任意命令。例如iXmail包含的\“ ixmail_attach.php\”脚本对用户提交的附件缺少充分过滤，攻击者可以通过操作URL参数上传恶意文件(如php文件)到服务器上，虽然文件放置在Web目录下的/tmp目录中，但可以远程访问，因此攻击者可能以Web进程权限在系统上执行任意命令，故在文件上传之前，加入文件类型判断模块，并进行过滤。如要求用户上传图片时，对上传的文件格式进行判断，如果是指定的图片文件格式(如JPG、GIF)允许上传，其他格式诸如*.EXE,*.PHP，*.ASP，*.JSP等可执行或可解释的程序文件就禁止上传。

3 结 束 语

本文介绍了网站建设中网页设计容易出现的漏洞和解决方法，其安全的概念贯穿在整个网页设计过程中，故必须随时考虑安全的问题，网站才会多一些安全性。

参 考 文 献

[1] 希利尔 S著. Active Server Pages编程指南[M]. 董启雄译. 北京: 宇航出版社, 1998

[2] 沈文智. Microsoft IIS 网页技术[M]. 北京: 人民邮电出版社, 1998

[3] 张小斌, 严望佳. 黑客分析与防范技术[M]. 北京: 清华大学出版社, 1999

编 辑 徐培红