

# 图书馆网站如何避免 SQL 注入攻击

陈天文

(潍坊市图书馆, 山东 潍坊 261041)

**[摘要]**通过分析公共图书馆建站技术,针对 ASP、PHP 技术构建动态网站存在的 SQL 注入漏洞易遭受攻击的问题,在开发及应用阶段提出了面向对象的网站代码编写规范、后台入口及数据库的保密、安装 SQL 防注入系统、限制登录方式、数据备份策略等 13 条建议和意见,从而有效避免 SQL 注入漏洞及其潜在危险,保证图书馆网站的安全、稳定运行,不间断为用户提供服务。

**[关键词]**图书馆 网站安全 SQL 注入

**[分类号]**JTP309

随着计算机和网络技术的日益发展,网络化、数字化成为图书馆发展的重要方向,图书馆网站建设成为其中不可缺少的重要组成部分。图书馆网站不但是图书馆实现对外交流的窗口,也是图书馆革新检索和服务方式、更好地为读者提供信息服务的桥梁和纽带。目前,图书馆网站已从早期提供简单信息服务转化为能根据用户需要提供动态的、具有交互功能的特定服务,如联合编目、网上流通、网上参考咨询、电子资源的管理与发布、视频点播等。在网站建设过程中,由于开发水平及管理经验参差不齐,部分网站开发人员在编写代码的时候,没有对用户输入数据的合法性进行判断,使应用程序存在安全隐患,网站容易遭受不同程度的 SQL 注入攻击。SQL 注入攻击由于其广泛性、易学性、难捕获性已经逐渐成为互联网上主流的黑客攻击方式,因此有必要结合图书馆网站自身特点,了解 SQL 注入攻击的原理,尽可能多地采取防范措施,并在遭受攻击后能采取行之有效的恢复措施,以保证网站的正常运行。

目前图书馆网络安全系统主要采用的是以防火墙为主的被动管理,即根据设定的规则,对流入网络中的流量进行过滤,从而防止非法行为的入侵。防火墙的作用只是对访问对象进行认证,而对于网站本身存在的软件问题,入侵者依然可以在遵守防火墙访问规则的前提下实施攻击,所以防火墙并不能解决所有的安全问题。

## 1 SQL 注入原理及其目的

### 1.1 什么是 SQL 注入

所谓 SQL 注入,就是在客户端通过把 SQL 命令插入到 Web 表单递交或页面请求的查询字符串,最终达到欺骗服务器执行恶意的 SQL 命令,即通过递交参数构造巧妙的 SQL 语句,从而成功获取想要的数据。

### 1.2 SQL 注入的目的

SQL 注入目的是获取管理员的账号和密码,后果轻则导致敏感信息的泄漏,重则整个服务器受他人控制。一旦网站服务器被注入成功,网站会出现以下几种后果:①重要信息被人窃取;②数据记录被篡改;③网站文件被插入“尾巴”,登录网站时转向其他网站或传播病毒;④网站服务器被挂“木马”程序;⑤网站服务器全面瘫痪。

## 2 图书馆网站类型

目前图书馆网站主要分为 4 类:①网站全部由静态页面组成,此类网站在功能上起到展示的作用,更新比较复杂,功能比较单一。②通过中间件产品,如 TRS、清华同方 WCCM 等内容管理系统进行二次开发或通过自主开发的中间件产品,在服务器端发布数据时自动生成静态网页,用户在客户端访问的全部是静态网页。③通过下载网站模板源代码进行修改

### 参考文献:

- [1] 王成栋.博客(blog)及其在图书馆中的应用研究[D].吉林大学,2006.
  - [2] 2007 年中国博客调查报告.http://www.sina.com.cn. 2007-12-26.
  - [3] 高海峰,任树怀.Web2.0 技术在高校图书馆学科建设中的应用——以上海大学图书馆学科馆员平台建设为例[J].图书情报工作,2007(4):115-118.
  - [4] 徐雁平.20 世纪 20 年代的国学推荐书目及其文化解读[J].学术研究,2000(10):100-106.
  - [5] 夏南强,张炯.当代社会需要的目录学[J].大学图书馆学报,2003(5):66-68.
  - [6] 葛剑雄.读书的“名堂”.文汇读书周报,1999-02-20.
- 杜玉玲 女,1977 年生。历史学硕士,馆员,已发表论文 1 篇。

(收稿日期:2009-09-16;责编:张欣。)

建站。④通过 ASP、PHP 等技术自主开发动态网站。

目前全国省级以上公共图书馆采用第一种、第三种方式建站的很少;采用第二种方式建站的有国家图书馆、首都图书馆、辽宁、福建、山西、湖北、河北、陕西、黑龙江、吉林、河南、青海、香港共 13 家;采用第四种方式建站的有甘肃、江西、云南、四川、海南、上海、内蒙古、新疆、西藏、广东、青岛、台湾、浙江、贵州、澳门共 15 家;其余图书馆采用 JSP 等其他技术。第二种方式是近年来比较流行的建站方式,安全性较高,该方式与 ASP、PHP 技术的区别在于所有数据在服务器发布处理完毕后生成静态网页,客户端访问时没有对数据库的操作,不像 ASP 等技术根据用户请求需要对数据库进行相应的操作,从而最大可能地减少了对数据库的攻击。目前,国内大型门户网站全部采用这种方式建站。ASP 技术由于灵活性、易用性,在图书馆网站的应用也比较广泛。ASP 技术是构建网站的主流技术,特别是 asp.net 技术的推出提供了更为广阔的空间,第二种建站方式的网站后台管理系统也较多采用 asp.net 等技术。

### 3 SQL 注入攻击的主要对象及其方法

对于全部由静态网页组成的网站,主要用来发布图书馆简单信息,通过 FTP 实现更新操作,所以保管和设置好 FTP 密码即可。第二类网站,由于这类商品软件经过严格测试,技术比较成熟。其次,在前台呈现的大多是静态页面,遭受攻击的可能性较小,这类网站管理好后台登录系统的入口及密码是关键。第三四类网站是 SQL 注入的主要对象。

SQL 注入操作比较简单,特别是网上流行的啊 D 注入工具、HDSI 等能够自动分析网页是否存在注入漏洞及其数据库类型。在实际操作中,如果是针对 Access 数据库,可以对表名、字段名、字段值进行逐个猜测,接着用函数来计算数据并将它们还原;如果是 MSSQL 数据库,由于所有的列表都保存在特定的位置,可以直接通过暴库的方法来获取。图 1、图 2 分别为唐山图书馆 ACCESS 注入检测(图 1)和荆门图书馆 MYSQL 注入检测(图 2)界面及其结果。

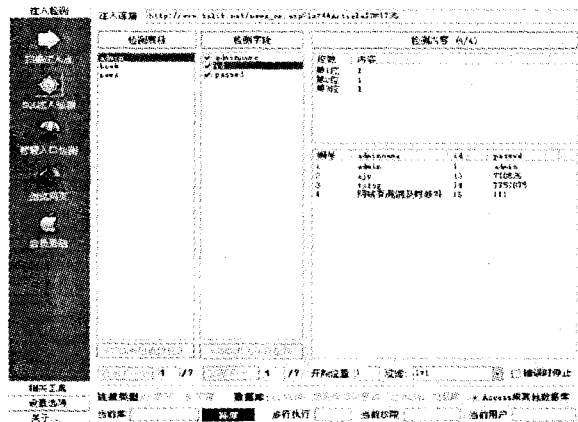


图 1 ACCESS 注入检测

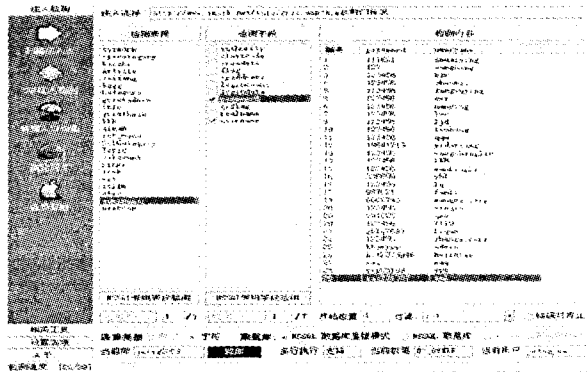


图 2 MYSQL 注入检测

### 4 避免 SQL 注入攻击的主要措施

4.1 在开发网站系统时使用类、存储过程等面向对象的概念实现数据库的访问可以有效防止 SQL 注入漏洞

面向对象的程序设计思想在一定程度上包含对输入的数据进行有效性检验及上下文的对比分析,并且能够重复调用,所以提高了代码效率,减少了由于多次重写代码而存在危险性的机率。

4.2 系统设计要严密,避免出现错误信息

入侵者根据错误提示很容易得到有关数据库的相关信息。如以下错误信息:

Microsoft OLE DB Provider for ODBC Drivers (0x80040E07)

[Microsoft][ODBC SQL Server Driver]

[SQL Server] 将 nvarchar 值 'sonybb' 转换为数据类型为 int 的列时发生语法错误。

/lawjia/show.asp, 第 47 行

根据这个出错信息,可以获得以下信息:该站使用 MS\_SQL 数据库,用 ODBC 连接,连接账号名为 sonybb。获得这些信息对下一步的 SQL 注入提供了重要数据,故始终通过测试类型、长度、格式和范围来验证用户输入,过滤用户输入的内容,防止出现系统错误提示,这是防止 SQL 注入式攻击的常见并且行之有效的措施,同时在客户端和服务端都执行验证,之所以要执行服务器端验证,是为了弥补客户端验证机制脆弱的安全性。

4.3 部署防注入系统

如网上流行的 SQL 通用防注入系统,能够自动封杀注入者 IP,使注入者不能再访问本站。同时可以查看入侵者提交数据记录,解除对注入者 IP 等。

该系统代码使用方法很简单,只要在需要防注入的页面头部插入<!--#Include File="Neeao\_SqlIn.asp"-->就可以做

到页面防注入;如果想整站防注入,就在目录的数据库连接文件中添加头部调用,如 conn.asp 中添加<! --#Include File="Neeao\_SqlIn.Asp"-->。

#### 4.4 加强管理员入口路径的强壮度

即系统管理后台登录目录的保密,不要放在 admin、login 等常用目录下,文件名也不要使用这样的名字,最好使用不规则的没有通用意义的名字为好。可以说猜解后台管理员入口是 SQL 注入的第一步,所以做好管理员入口的保密工作极其重要,尤其不要在首页设置管理员入口,这样相当于给入侵者提供了一个入侵的窗口,即使管理员入口设置的是内网 IP 地址并不保险,很多情况下,公网地址(域名指向 IP)与内网地址是相互联系、相互映射的,把内网地址替换为域名或公网 IP 地址依然可以进入后台登录界面。

#### 4.5 隐藏数据库存储路径

按照常规来说,很多人习惯将数据库保存在网站的数据目录下,并且命名为 data.mdb、admin.mdb 等很容易被猜解的名字,这种做法是非常危险的,如果数据库文件被下载,就可以控制整个网站了。对此,我们可以创建一个没有任何含义的文件夹,并且将其隐藏一个较深的路径,从而减少被猜解的可能性。

#### 4.6 修改数据库名称

对于下载的网站模板,默认的文件名极易被猜到,因此在更改存储路径的同时应同时更改其文件名,而更改文件名不仅要更改主文件名,扩展名同样要更改,可以将扩展名更改为 ASP 和 ASA 等不影响数据库查询的名字,如 m337e0394 pjsdlkfjwet.asp。更改扩展名后是无法通过 IE 浏览器直接下载的,因为打开后看到的是一大片乱码,对窃取者来说毫无用处;同时数据库名字前带上“#”以防止被下载,因为 IE 遇到 # 就会忽略后面的字母。

#### 4.7 禁止设置默认账号和密码

不要误以为后台文件隐藏得很深,为方便起见,设置一个默认的账号和密码。否则一旦后台登录文件被猜解后就自动得到了进入网站的钥匙。

#### 4.8 限制管理员登录方式

①内网认证码方式。认证码只能在内网环境下才能显示,即管理员只能在内网登录,减少了被攻击的可能性。②设定专属 IP 登录后台系统,如设置为内网某台机器或某 IP 段进行登录,否则不予认证。

#### 4.9 使用漏洞扫描工具进行详细测试

网站建设完成后要使用漏洞扫描工具扫描 SQL 注入漏洞,尽早采取补救措施,避免各种损失。一个完善的漏洞扫描程序,它专门查找数据库中的 SQL 注入式漏洞,可以帮助管

理员发现 SQL 注入式漏洞,并提醒管理员采取积极的措施来预防 SQL 注入式攻击。

#### 4.10 规划完善的备份与冗余策略

当网站被 SQL 注入后造成数据库被修改、数据丢失,可以将备份的数据恢复到原始的数据,保证了网站在不可避免的条件下的相对安全性。图书馆网站重要的数据包括 Web 信息、书目数据信息、电子资源等。采用 SQLSERVER 数据库管理系统的,做好 SQL 数据库的备份,特别是异机备份。

#### 4.11 删除或隐藏后台管理程序的登录页面

由于 SQL 注入主要是通过漏洞获得管理员用户名和密码,然后检测管理员登录入口进入系统,所以为防止程序有未知漏洞,可以在完成维护后删除后台管理程序的登录页面,下次维护时再次上传,这样就有效阻死 SQL 注入攻击的入口。

#### 4.12 安装伪装后台登录系统及数据库

SQL 注入者在获得伪装的信息后会利用这些虚假的信息进行操作,经实验无效后一般会放弃攻击,从而有效保护真正的后台系统不被攻击。

#### 4.13 严格区分普通用户和系统管理员用户

在权限设计中,对于终端用户,禁止分配对数据库对象的建立、删除等权限。即使终端用户使用 SQL 语句中带有嵌入式的恶意代码,由于其用户权限的限制,这些代码也将无法被执行。故应用程序在设计时,把系统管理员用户与普通用户区分开来,可以最大限度地减少注入式攻击对数据库带来的危害。

综观全国范围内,省级以上图书馆由于在管理、技术、安全意识等方面比较完善,安全性较强。而市级图书馆大多采用 ASP、PHP 等动态技术建站,安全性问题较严重,所以在网站的建设及维护阶段必须加强 SQL 注入技术的检测,从而打造结构严谨、安全可靠的网站管理系统。

#### 参考文献:

- [1] 杨育均.高校图书馆网站的 SQL 注入防范及补救措施.广东电视大学学报,2008(4):105-108.
- [2] 俞小怡等.Web 应用中的攻击防御技术的研究与实现.计算机安全,2008(6):47-51.
- [3] 甘剑伟.基于 asp.net 技术的图书馆网站安全管理的隐患与对策.现代情报,2008(8):116-117.
- [4] 隆毅.浅谈图书馆网站防御 CC 攻击的方法.江西图书馆学刊,2008(2):101-103.

陈天文 男,1980年生.技术部主任,馆员.研究方向:图书馆自动化、网络化建设。

(收稿日期:2009-06-19;责编:徐向东。)