**Webshell**

顾名思义，“web”的含义是显然需要服务器开放web服务，“shell”的含义是取得对服务器某种程度上操作权限。webshell常常被称为匿名用户（入侵者）通过网站端口对网站服务器的某种程度上操作的权限。由于webshell其大多是以动态[脚本](http://baike.baidu.com/view/54.htm" \t "_blank)的形式出现，也有人称之为网站的后门工具。

**作用**

　　一方面，webshell被站长常常用于网站管理、服务器管理等等，根据FSO权限的不同，作用有在线编辑网页[脚本](http://baike.baidu.com/view/54.htm" \t "_blank)、上传下载文件、查看数据库、执行任意程序命令等。

　　另一方面，被入侵者利用，从而达到控制网站服务器的目的。这些网页脚本常称为WEB

　　脚本木马，目前比较流行的asp或php[木马](http://baike.baidu.com/view/931.htm" \t "_blank)，也有基于.NET的脚本木马与JSP脚本木马。

[编辑本段](http://baike.baidu.com/view/53110.htm)**隐蔽性**

　　有些恶意网页脚本可以嵌套在正常网页中运行，且不容易被查杀。

　　webshell可以穿越服务器防火墙，由于与被[控制](http://baike.baidu.com/view/57913.htm" \t "_blank)的服务器或远程主机交换的数据都是通过80端口传递的，因此不会被防火墙拦截。并且使用webshell一般不会在[系统日志](http://baike.baidu.com/view/1270588.htm" \t "_blank)中留下记录，只会在网站的web日志中留下一些数据提交记录，没有经验的[管理员](http://baike.baidu.com/view/315045.htm" \t "_blank)是很难看出入侵痕迹的。

[编辑本段](http://baike.baidu.com/view/53110.htm)**防范**

　　从根本上解决动态[网页脚本](http://baike.baidu.com/view/543.htm" \t "_blank)的安全问题，要做到防注入、防暴库、防COOKIES欺骗、防跨站攻击等等，务必配置好服务器FSO权限。最小的权限=最大的安全。防范webshell的最有效方法就是：可写目录不给执行权限，有执行权限的目录不给写权限。希望看过本词条的人，[发表](http://baike.baidu.com/view/145286.htm" \t "_blank)一下你是如何防范恶意WEBSHELL后门的。

**防范方法：**

　　1、建议用户通过ftp来上传、维护网页，尽量不安装asp的上传程序。

　　2、对asp上传程序的调用一定要进行身份认证，并只允许信任的人使用上传程序。

　　3、asp程序管理员的用户名和密码要有一定复杂性，不能过于简单，还要注意定期更换。

　　4、到正规网站下载asp程序，下载后要对其数据库名称和存放路径进行修改，数据库文件名称也要有一定复杂性。

　　5、要尽量保持程序是最新版本。

　　6、不要在网页上加注后台管理程序登陆页面的链接。

　　7、为防止程序有未知漏洞，可以在维护后删除后台管理程序的登陆页面，下次维护时再通过ftp上传即可。

　　8、要时常备份数据库等重要文件。

　　9、日常要多维护，并注意空间中是否有来历不明的asp文件。

　　10、一旦发现被入侵，除非自己能识别出所有木马文件，否则要删除所有文件。

　　重新上传文件前，所有asp程序用户名和密码都要重置，并要重新修改程序数据库名称和存放路径以及后台管理程序的路径。

**常见webshell**

　　提到webshell，那就一定要提到“海阳顶端网asp后门”这应该是asp后门中最有名的了，后面还有“杀手十三”等功能丰富的后门出现！

　　一句话后门 <%eval request("value")%> 或者 <%execute request("value")%> 或者 <%execute(request("value"))%> 或者他们的加密变形！

　　当然webshell还有jsp，php等多种脚本形式的

**webshell概论**

　　webshell是web入侵的脚本攻击工具。简单的说来，webshell就是一个asp或php木马后门，黑客在入侵了一个网站后，常常在将这些asp或php木马后门文件放置在网站服务器的web目录中，与正常的网页文件混在一起。然后黑客就可以用web的方式，通过asp或php木马后门控制网站服务器，包括上传下载文件、查看数据库、执行任意程序命令等。

　　为了更好理解webshell我们学习两个概念：

**什么是“木马”？**

　　“木马”全称是“[特洛伊](http://baike.baidu.com/view/28818.htm)木马(Trojan Horse)”，原指古希腊士兵藏在木马内进入敌方城市从而占领敌方城市的故事。在Internet上，“特洛伊木马”指一些程序设计人员在其可从网络上下载(Download)的应用程序或游戏中，包含了可以控制用户的计算机系统的程序，可能造成用户的系统被破坏甚至瘫痪。

　　什么是后门？大家都知道，一台计算机上有65535个端口，那么如果把计算机看作是一间屋子，那么这65535个端口就可以它看做是计算机为了与外界连接所开的65535扇门。每个门的背后都是一个服务。有的门是主人特地打开迎接客人的（提供服务），有的门是主人为了出去访问客人而开设的（访问远程服务）——理论上，剩下的其他门都该是关闭着的，但偏偏由于各种原因，很多门都是开启的。于是就有好事者进入，主人的隐私被刺探，生活被打扰，甚至屋里的东西也被搞得一片狼藉。这扇悄然被开启的门——就是“后门”。

**如何寻找webshell**

　　1，脚本攻击SQL注入

　　2，使用注入工具

　　3，在[浏览器](http://baike.baidu.com/view/7718.htm" \t "_blank)里打开百度,输入搜索关键词"在本页操作不需要FSO支持&"或者"一次只能执行一个操作",然后点击搜索,很快就可以看到检索到了大量的查询结果.

**检测与清除**

**1、检测木马**

　　（1） 浏览网站，右键查看源代码，在源代码里搜索 iframe ,看看有没有被插入了一些不是自己网站的页面，如果有，一般就是恶意代码。

　　（2） 也是右键查看源代码，搜索 "script" 这个关键字，看看有没有被插入一些不是自己域名下的的脚本，如果有，并且不是自己放上去的，那很可能也有问题。

**2、手工删除木马的方法**

　　（1） 调出任务管理器，看看有没有一些不知名的程序在运行，如果有，用windows的文件查找功能找到这个文件，右键asp网站源码查看属性，如果这个可执行文件的摘要属性没有任何信息，而自己又不知道是什么东西，那很可能有问题，然后上google搜索一个这个文件的信息，看看网上的资料显示是不是就是木马病毒，如果是就先将其改名。

　　（2） 打开注册表编辑器，查看一下 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run有没有一可疑的启动项，有的话就删除.

　　（3） 查看本地机器的 windows 控制面板，看看“任务计划”那里有没有一些不是自己定义的任务，如果有查看属性，找到这个任务所执行的可执行文件是哪个，重复前面步骤1方法进行查杀。

**其他**

　　为了更好理解webshell我们学习两个概念：

　　问：什么是“木马”？

　　答：“木马”全称是“[特洛伊木马](http://baike.baidu.com/view/2611.htm)（Trojan Horse）”。原指[古希腊](http://baike.baidu.com/view/64778.htm" \t "_blank)士兵藏在木马内进入敌方城市从而占领敌方城市的故事。

　　在互联网上，“特洛伊木马”指一些程序设计人员在其可从[网络](http://baike.baidu.com/view/3487.htm" \t "_blank)上下载（Download）的[应用程序](http://baike.baidu.com/view/330120.htm" \t "_blank)或[游戏](http://baike.baidu.com/view/2468.htm)中，包含了可以控制用户的[计算机系统](http://baike.baidu.com/view/1130583.htm)的程序，可能造成用户的系统被破坏甚至瘫痪。

　　问：什么是后门？

　　答：大家都知道，一台计算机上有65535个端口，那么如果把计算机看作是一间屋子，那么这65535个端口就可以它看做是计算机为了与外界连接所开的65535扇门。每个门的背后都是一个服务。有的门是主人特地打开迎接客人的（提供服务），有的门是主人为了出去访问客人而开设的（访问远程服务）。

　　理论上，剩下的其他门都该是关闭着的，但偏偏由于各种原因，很多门都是开启的。

　　于是就有好事者进入，主人的[隐私](http://baike.baidu.com/view/350273.htm" \t "_blank)被刺探，生活被打扰，甚至屋里的东西也被搞得一片狼迹。

　　这扇悄然被开启的门就是“[后门](http://baike.baidu.com/view/20922.htm)”。

**推荐：webshell的优点**

　　webshell 最大的优点就是可以穿越防火墙，由于与被控制的服务器或远程主机交换的数据都是通过80端口传递的，因此不会被[防火墙](http://baike.baidu.com/view/3067.htm" \t "_blank)拦截。

　　并且使用webshell一般不会在系统日志中留下记录，只会在网站服务器的日志中留下一些数据提交记录，没有经验的管理员是很难看出入侵痕迹的。

　　问：什么是网站提权？

　　答：所谓网站提权，是入侵者惯用做法，通过注入，及服务器及[软件](http://baike.baidu.com/view/37.htm)的本身漏洞提权，使其得到webshell，从而掌握服务器的最高管理权限。

　　问：如何寻找webshell？

　　答：关注您所留意的各种程序的漏洞，进行深入了解、脚本攻击SQL注入、使用注入工具。