网站安全评估文档（一）

二十一世纪是网络的时代，网络已跟我们的生活息息相关。而网站通过网络这个枢纽密切的联系着人们的日常生活，人们也通过各种各样的网站获取所需要的信息。因此，网站的安全也越来越被人们所重视。然而网络存在着各种各样的安全隐患，比如：COOKIE 中毒，应用程序缓冲溢出，跨站脚本攻击，已知安全漏洞，强行浏览问题，参数篡改攻击等等，无时无刻不让使用者提心吊胆。

也许有的人说，我的系统是有防火墙保护的。防火墙是有访问过滤机制，但是还是无法应对许多恶意行为。虽然它可以设置访客名单，可以把恶意访问排除在外，但是如何鉴别恶意还是善意访问还是个问题。访问如果一旦被允许，后面的安全问题就不是防火墙能够解决的了。又比如，人们往往认为，网站使用了 SSL 加密就很安全了，网站起用 SSL 加密后，表明网站发送和接受的信息都经过了加密处理，但是 SSL 无法保障存储在网站里面的信息的安全。还有就是认为漏洞扫描工具没有发现任何问题网站就很安全。漏洞工具生成一些特殊的访问请求，发送给网站，在获取网站的响应信息后进行分析。但是它能够查找一些明显的网络安全漏洞，但是却没有办法对网站的应用程序进行检测，更别说查找程序中的漏洞了。因此，要使网站安全并不是只做表面的保护就可以高枕无忧了。国内的网站一般都采用 ASP+ACCESS 或者 SQL 的数据库后台，所以 SQL 注入就成了网站攻击最常见的一种方法。SQL 注入是从正常的 WWW 端口访问，表面上看和一般的 WEB 页面访问没什么区别，所以防火墙都不会对 SQL 注入发出警报，如果管理员没有看 IIS 日志的习惯，可能被入侵了还不会发觉。在判断出可以 SQL 注入后，就可以通过工具（比如啊 D SQLTOOLS）猜他的数据库名之类的信息了。当然，也可以用抓包的方法来获取网站的相关信息。

现在，，许多黑客甚至可以突破 SSL 加密和各种防火墙，攻入 WEB 网站的内部获取信息。他们可以仅借浏览器和几个技巧，既套取 WEB 网站的保密信息。一旦你的网站遭受了恶意攻击，那连哭都来不及了。

因此提高网站的安全性，已成为迫在眉睫的问题了。下面就从三个方面来分析相关的安全问题。

一、硬件环节。

从硬件的角度来提高网站的安全性有很多中办法，例如：不允许局域网内部私自介入外网，采用隔离网闸和放火墙，不允许接入层交换机直接连接到核心服务器等手段，都是从硬件的角度来提高网络的安全性的。在很长一段时间内，一提到网络安全人们所想到的都是软件漏洞。但随着技术和市场的发展，硬件安全正逐渐走入人们的视野。

以硬件为主的安全系统将比采用安全防护软件更不容易受到黑客入侵。若软件和硬件安全系统同使用，将使电脑使用者的资料获得更好的保护。在圈内，微软近日除了炫耀 Longhorn 操作系统之外，还首次展示了受到密切关注的新一代安全计算基准(NGSCB)的安全技术代码，这一技术先前被称为“Palladium”。NGSCB 是在一台 PC 内 部创建第二种操作环境的硬件和软件的总合，这一环境旨在保护系统免遭恶意代码入侵。作为这一

保护的一部分，NGSCB 可以提供应用程序、附带硬件、内存以 及存储器之间安全的连接。在 Palladium 构想中，把用于认证和加密的密钥基本信息作为硬件预先嵌入个人电脑。购买支持 Palladium 的个人电脑 时，个人电脑独有的加密密钥就会被写入到这枚硬件芯片上。通过这个加密密钥，支持 Palladium 的 OS 可对运行于其上的程序进行认证，并加密保存机密 数据。具体而言，也就是说支持 Palladium 的 OS 将会设置一个只有已经得到认证的程序才可以访问的保护区域。而保存在保护区域中的数据都是经过加密 的，即使被拷贝到其他电脑上，也无法还原。据称微软 Palladium 的第一个版本将仅供编写特定的商务应用程序而非消费软件。从上面的分析可以看出，Palladium 的应用必须得到第三方的支持。在硬件方面，微软早于 2002 年 9 月份就开始分别与英特尔和 AMD 联合制定支持 Palladium 的硬件规格，此次 AMD 和英特尔推出支持 Palladium 的新产品正是合作的结果。预计，在今后的几年中，硬件安全的问题会越来越受到人们的重视。

二、操作系统漏洞来考虑

操作系统是计算机的灵魂，没有它的存在，我们现在可能还在不停的在烦人 0101 二进制编码中受苦。它给了我们友好的用户界面，让我们更容易的和计算机沟通。但是它也有很多缺陷。目前比较流行的操作系统，windows，linux，solaris 等，都或多或少的存在着安全问题。

网站是基于计算机网络的，而计算机运行又是少不了操作系统的。操作系统的漏洞会直接影响到网站的安全。我们就以比较有名的 IIS 漏洞来说明操作系统和网站安全的联系。早在 2004 年，微软公司检测到一种木马程序，该程序可利用微软ＩＩＳ服务器操作系统的 3 个安全漏洞攻击网站。微软公司说，该公司今年 4 月拥有了针对其中两个安全漏洞的补丁程序，但还没有设计出针对另一个安全漏洞的补丁。专家称，黑客用它攻破互联网站后，会对网站服务器操作程序做出修改，向访问网站的客户端计算机传输一段程序代码，用于记录客户端计算机的键盘输入情况，并把结果返回给攻击者。这种木马程序通常用于盗取计算机用户的信用卡号、银行账户和密码等资料。美国计算机紧急预备小 组已在互联网上发布警告要用户注意，“任何网站都可能受到影响……深受用户信任的网站也不例外。”

对于操作系统本身而言，文件的系统也应该采用安全级别较高的，比如 NTFS。NTFS 文件系统最大的特点就是安全性，在 NTFS 分区上，可以支持随机访问控制和拥有权，对共享文件可以指定权限，以免受到本地访问或远程访问的影响。NTFS 对于在计算机上存储文件夹或者耽搁文件，都可以指定相应的权限，使每个用户只能照系统给予的权限进行操作，充分保护系统和数据的安全性。同时，恰当的配置 WEB 服务器，只保留必要的服务的服务，删除和关闭没有用的或不需要的服务。因为启动不必要的服务可能使他人获得本机的系统信息，甚至获取密码文件。在对服务器进行管理时，应该避免使用 TELENT，FTP 等程序。因为这些程序是以明文形式传输密码，很容易被监听。

一个小小的系统漏洞可能就是让你系统瘫痪，经济承受毁灭性打击的导火索。我们应该经常关注一些有关操作系统漏洞的信息，及时给系统打上补丁。别让你的网站受到不该有的伤害。

三、软件代码的安全性

目前由于编程者的水平参次不齐。在应用系统中有许多都存在着大量的安全漏洞。就目前国内情况来看，由于软件代码安全性存在问题而导致网站被黑客攻击的情况屡屡发生。以基于 ASP 的网站为例，我们知道 ASP 的入门门槛比较低，大量的初学者在很快的时间内就可以编写出与经验丰富的程序员相匹敌的代码。但是这种匹敌往往仅仅是功能上的，在安全性方面就差的比较远了。比如说，有很多网站都没有对 SQL 注入进行屏蔽，给黑客留下了可乘之机。对他们来说只要耐心点就可能会拿到用户的相关信息，甚至会导致机密文件的外泄。也有的网站采用的数据库系统本身存在安全隐患，这就需要细心的程序员在自己的代码中来消除这些安全隐患。

在本次的网络攻防比赛中，我们就有过利用程序漏洞，来骗过系统，达到非法操作目的的经验。

我们不能保证我们的系统是 100%安全的，但我们应该把我们能够做到的，作到最好。对网站的安全性要经常进行评估，尽量提高系统的安全性。为了自己，为了相信你的用户们。

网站安全评估文档（二）

简介：

随着互联网的盛行，WEB 服务的逐渐升温，在 INTERNET 上构架自己的站点愈来愈热，与此同时，网站的安全性也越来越受到重视评价一个网站安全与否，要涉及到很多方面。要构架一个整体上安全的网站，至少应该从如下几个方面加以考虑：

一：硬件方面

要构架一个网络，首先根据实际需求，采用合适的网络拓扑结构，仔细分析该网络拓扑结构，为以后网络的规划和管理提供资料，同时也能够清楚网络的优缺点和安全性，能够找出网络的安全缺陷和安全问题。

然后根据自己的情况，明白要向外提供怎样的服务，如：WEB 服务，电子邮件服务等。要使用防火墙，根据需求购买相应的硬件或软件防火墙，不允许局域网内部私自介入外网，也不允许交换机直接接到核心服务器的交换机上，所有内部和外网的连接均要通过防火墙。还要划分一个非军事区(DMZ)，把外网可以直接访问的系统（如：WEB 系统，电子邮件系统等）置于 DMZ 区，限制内部敏感信息被非法访问。

最后要设置备份系统，根据用户的网络情况，提供骨干交换机、路由器等核心网络设备的备份。备份设备可以在段时间内替代网络中实际使用的设备。这样，一旦核心设备出现故障，使用备件替换可以大大减少网络故障时间。通过备品备件，快速恢复网络硬件环境；通过备份文件的复原，尽快恢复网络的电子资源；由此可在最短的时间内恢复整个网络应用。

二：系统方面

目前市场上的操作系统以 Windows 为主，由于 Windows 的普及率和占有市场的比率特别高，因此 Windows 一直都是网上黑客的最爱。Windows 从发行到现在虽然在不断地升级，但出现的漏洞还是很多。以下简要介绍下几种常见漏洞及解决办法。

Unicode 漏洞

漏洞成因和危害

Unicode 漏洞从中文 IIS4.0＋SP6 开始，还影响到中文 Windows2000＋IIS5.0 和中文 Windows2000+IIS5.0+SP1。他们利用 Unicode 字符（如“..\”取代“/”和“\”）进行目录遍历而访问到 WEB 根目录以外的文件。

解决方法

（1）到微软官方网站及时下载补丁。

（2）限制网络用户访问和调用 CMD 命令的权限。

（3）若没有必要是用 Scripts 和 Msadc 目录，就将其删除或更名。

缓冲区溢出漏洞

漏洞成因和危害

服务器在安装 IIS 过程中，系统还会安装几个 ISAPI 扩展.dlls，其中 idq.dll 是 Index Server 的一个组件，对管理员脚本和 Internet 数据查询提供支持。但是，idq.dll 在一段处理 URL 输入的代码中存在一个未经检查的缓冲区，攻击者利用此漏洞能导致受影响服务器产生缓冲区溢出，从而执行自己提供的代码。更为严重的是，idq.dll 是以 System 身份运行的，攻击者可以利用此漏洞取得系统管理员权限。受影响平台有 Windows NT 4.0、Windows 2000、Windows XP beta；受影响的版本有 Microsoft Index Server 2.0、Indexing Service in Windows 2000。没安装 IIS 的无此漏洞。

解决方法

及时到微软官方网站下载补丁更新即可。

IIS CGI 文件名错误解码漏洞

漏洞成因和危害

IIS 在加载可执行 CGI 程序时，会进行两次解码。第一次解码是对 CGI 文件名进行 Http 解码，然后判断此文件名是否为可执行文件，如检查后缀名是否为“.exe”或“.com”等。在文件名检查通过之后，IIS 会进行第二次解码。正常情况下，应该只对该 CGI 的参数进行解码，然而，当漏洞被攻击后，IIS 会错误地将已经解过码的 CGI 文件名和 CGI 参数一起进行解码。这样，CGI 文件名就被错误地解码两次。通过精心构造 CGI 文件名，攻击者可以绕过 IIS 对文件名所做的安全检查。在某些条件下，攻击者可以执行任意系统命令。影响平台：IIS 4.0/5.0(SP6/SP6a 没有安装)

解决方法

到微软官网下载补丁更新。

FrontPage 服务器扩展漏洞

漏洞成因和危害

对于安装 Frontpage 服务器的网站，通常会在 Web 目录(缺省)下有若干个以字母"_vti"开头的目录，正是这些目录隐藏了潜在的攻击性。当用户在任何常用的搜索引擎上搜索默认的 Frontpage 目录时，会得到大量从引擎上返回的信息，这时，给入侵者一可乘之机，使他们得以对服务器进行简单而又反复的攻击。此漏洞可使他们获得被攻击方的 Frontpage 口令文件、通过 Frontpage 扩展名执行任意二进制文件，以及通过用_vti_cnf 替换 index.html，即入侵者能看到该目录下的所有文件，并有可能获得访问权限等。

解决方法

对目录定义许可、移去某些目录、设置用户密码或不安装 Frontpage 扩展服务器。

Printer 漏洞

漏洞成因和危害

该漏洞只存在于运行 IIS 5.0 的 Windows 2000 服务器中。由于 IIS 5 的打印 ISAPI 扩展接口建立了.printer 扩展名到 Msw3prt.dll 的映射关系(缺省情况下该映射也存在)，当远程用户提交对.printer 的 URL 请求时，IIS 5.0 会调用 Msw3prt.dll 解释该请求，加之 Msw3prt.dll 缺乏足够的缓冲区边界检查，远程用户可以提交一个精心构造的针对.printer 的 URL 请求，其"Host:"域包含大约 420B 的数据，此时在 Msw3prt.dll 中发生典型的缓冲区溢出，潜在地允许执行任意代码。在溢出发生后，Web 服务会停止用户响应，而 Windows 2000 将接着自动重启它，进而使得系统管理员很难检查到已发生的攻击。

解决方法

可通过安装微软相应漏洞补丁来解决此安全问题。

总之，操作系统的大多数漏洞都可以通过及时下载补丁，做相应的更新即可完成。做好操作系统基本的安全措施后，还需要队相应的权限做适当的配置，否则再新的系统也是白搭。下面简要说下权限的设置：

权限设置的原理

WINDOWS 用户，在 WINNT 系统中大多数时候把权限按用户（组）来划分。在 控制面板→管理工具→计算机管理→本地用户和组 管理系统用户和用户组。

NTFS 权限设置，在分区的时候把所有的硬盘都分为 NTFS 分区，然后确定每个分区对每个用户开放的权限。文件（夹）上右键→属性→安全在这里管理 NTFS 文件（夹）权限。

IIS 匿名用户，每个 IIS 站点或者虚拟目录，都可以设置一个匿名访问用户（现在暂且把它叫“IIS 匿名用户”），当用户访问你的网站的.ASP 文件的时候，这个.ASP 文件所具有的权限，就是这个“IIS 匿名用户”所具有的权限。

权限设置的思路

要为每个独立的要保护的个体（比如一个网站或者一个虚拟目录）创建一个系统用户，让这个站点在系统中具有惟一的可以设置权限的身份。

在 IIS 的 站点属性或者虚拟目录属性→目录安全性→匿名访问和验证控制→编辑→匿名访问→编辑 填写刚刚创建的那个用户名。

设置所有的分区禁止这个用户访问，而刚才这个站点的主目录对应的那个文件夹设置允许这个用户访问（要去掉继承父权限，并且要加上超管组和 SYSTEM 组）。

设置方法

先创建一个用户组，以后所有的站点的用户都建在这个組里，然后设置这个组在各个分区没有权限或者完全拒绝。然后再设置各个 IIS 用户在各自文件夹中的权限。这样，各 IIS 用户就只能有相应的权限访问相应的文件夹，最多也只有 IIS 用户组的最大权限。

做了以上的配置和设置后，还应当对系统的事件进行审核，可以通过 Windows 系统中 本地安全策略→审核策略来完成，根据需要对系统的某些事件做审核，并配置系统日志，将系统中相应事件的操作写入日志。这样管理员可以通过查看系统日志了解最近系统的使用情况。同时，通过配置密码策略和密码锁定策略可以减小或消除攻击者对系统用户密码破解的威胁。具体实施可以打开本地安全策略，根据需要在里面做相关的设置。

三：应用软件方面

一个网络的安全与否，除了以上的操作外，别的安全产品也不能少，至少应使用一些安全产品，如防火墙、反病毒软件、入侵检测系统等。

防火墙

防火墙应安装在局域网与路由器之间或 Internet 服务器和托管机房之间。这里防火墙实现单向访问控制：允许局域网用户访问 Internet，但是严格限制 Internet 用户对局域网内部资源的访问。用防火墙将局域网划分为 Internet、DMZ 区和内部访问区三个逻辑上的区域，有利于对局域网的管理。同过配置防火墙的相应规则可以实现端口级的控制，对内部网络的安全起到了重要的作用。

反病毒软件

在服务器和各终端和工作站上应配网络反病毒软件，如果需要可专门设防病毒服务器。防病毒服务器通过 Internet 及时更新病毒库，并强制局域网中已开机的终端更新反病毒软件，记录局域网中各终端病毒库的升级情况以及终端上病毒出现的时间、类型以及处理措施。终端及工作站上的反病毒软件实时监控本机对内存、文件的读写，并根据预先定义好的处理方法处理新发现的病毒文件，同时还对邮件实施监控。

入侵检测系统

在 DMZ 区域和托管机房服务器区安装入侵检测系统(IDS)。入侵检测系统作为旁路设备，监控网络中的信息，统计并记录网络中异常主机和异常连接，并终端某些已定义好的异常连接，还可想防火墙关联，向防火墙发出指令，命其在限定的时间内，对某个特定的异常终止连接。

四：网站代码方面

外部工作做好后，网站源程序代码的安全也对整个网站的安全起到举足轻重的作用。若代码漏洞危害严重，攻击者通过相应的攻击很容易拿到系统的最高权限，那时整个网站也在其掌握之中，因此代码的安全性至关重要。目前由于代码编写的不严谨而引发的漏洞很多，最为流行的有：数据库注入漏洞、动网上传漏洞等。

数据库注入漏洞

原理

程序员在编写代码的时候没有对特殊字符作过滤，攻击者利用这一点，在客户端提交特殊的代码，从而收集程序及服务器的信息，获得他想要的资料，对网站进行攻击。

利用实例

实例 1：若某个站点的域名是 www.***.com，下面有一个连接，连接地址是 www.***.com/classes.asp?id=2，我们在提交的地址后面加上单引号"'"，服务器会返回以下错误信息：

```
            Microsoft JET Database Engine 错误 80040e14
字符串的语法错误 在查询表达式 ID=2 中。
/classes.asp，行 8
```

从上面的错误信息中，我们可以得到以下信息：

1：网站使用的是 ACCESS 数据库，并且通过 JET 连接数据库。

2：程序没有判断客户端提交的数据是否符合程序要求。

3：该 SQL 语句查询的表中有一名为 id 的字段。

有了上面的信息我们对网站和后台就有了一些了解。(注：要得到上面的错误信息，需做如下操作：打开 Internet 选项－高级，将显示友好的 HTTP 错误前面的勾去掉，否则服务器端发生错误 IE 值返回 HTTP500 错误，得不到更多信息)。

实例 2：

在网站登陆页面，很多程序员会用如下代码：

select * from login where user='$user' and pass='$pass'

这样的代码极其危险，攻击者可以进行精心构造该语句，使气为真，达到攻击的目的。例如用 1' or 1='1 代替该语句中的$user 和$pass，代替后语句变成了：

select * from login where user='1' or 1='1' and pass='1' or 1='1'

显然该语句是成立的！对于网站的普通用户登陆界面若用此语句，攻击者很轻易的就成了网站会员，若管理员登陆页面用到此语句，而攻击者有同过别的手段得到了管理员登陆地址的话，攻击者轻易而举就拿到了网站的管理员权限，网站的一切都在其掌握之中！

解决方法

编码过程中，对可能出现的特殊字符做相应的处理或过滤，同时对用户提交的请求作出判断，判断它是否符合程序需要，若不符合则将其过滤掉。

动网上传漏洞

原理

程序编码不严谨，没有考虑到系统的很多特殊情况，攻击者通过构造特殊的上传路径或特殊

的文件名，绕过程序审核，使其接受程序规定以外的文件类型，达到攻击的目的。
利用实例
假设有台 www 主机域名是 www.***.com，论坛路径是/bbs/，漏洞源于动网 Upfile.asp 文件，upfile 是通过生成一个 form 表上传,如下

```
<form name="form" method="post" action="upfile.asp" ...>
<input type="hidden" name="filepath" value="uploadFace">
<input type="hidden" name="act" value="upload">
<input type="file" name="file1">
<input type="hidden" name="fname">
<input type="submit" name="Submit" value="上传" ...></form>
```

用到的变量:
filepath 默认值 uploadface 属性 hiden
act 默认值 upload 属性 hiden
file1 就是你要传的那个文件
关键是 filepath 这个变量!
默认情况下我们的文件上传到 www.***.com/bbs/uploadface/
文件是用你的上传时间命名的,就是 upfile 里的这一句

```
FileName=FormPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&FileExt
```

我们知道计算机中的字符串数据是以“\0”为标记结束的。我们构造的 Filepath 如下

Fielpath=’/newmm.asp\0’

我们在 2006.04.16.15.22 上传文件，
没有构造时，上传后为：http://www.***.com/bbs/uploadface/200604161522.jpg
用构造后的是，路径为：http://www.***.com/newmm.asp\0/200604161522.jpg
这样，当服务其接受到提交的 filepath 数据后，检测到 newmm.asp 后面的\0,就认为 filepath 的数据结束了，我们上传的文件就保存为 http://www.***.com/newmm.asp 了,现在的 ASP 木马多如牛毛，如存在类似漏洞，可以将 newmm.asp 换成相应的木马程序就 OK 了！
解决方法
(1) 将 Filepath 作为常量处理，怎样攻击者在怎么构造，程序还是用本身定义的常量。
(2) 加强对计算机特殊字符”\0”等特殊字符的处理。

五：管理方面

一个安全的网站，不但要有先进的技术支持，同时要配合并完善管理制度才能是网站的安全性更可靠。要对服务器机房制定相关的管理制度，以协助管理员管理机房，内容涉及限制进入机房人员的身份、进出机房作记录，设备进出机房做记录，设备配置做了修改也应记录等，有助于网络核心设备的监控和网络的正常运行。实行管理权限分散的原则，在不影响用户实施只能的前提下，给予其最小的权限。对于网络的最高权限，也可实行分散的原则，即要求多个拥有最高权限的用户同时才能完成最高权限功能。另外管理员密码要尽量复杂，不要有规律，经常更换密码，及时更新。网站的前后台密码不要一样或相似，尽量不要有任何联系。

小结：

管理是安全的核心，只有好的管理才能把现有资源最大程度地利用起来，先进的技术才能的到发挥。才能将网站的安全风险降到最低。