

培训教育
Training Services



中间件安全

主讲: Gnosis

4.1.2 IIS

IIS 服务器的安全设置

IIS 服务器常见漏洞

IIS 服务器的安全设置

IIs是Internet Information Services的缩写，意为互联网信息服务，它的功能是提供信息服务，如架设 http、ftp 服务器等，是由微软公司提供的基于运行 Microsoft Windows的互联网基本服务



IIS 服务器的安全设置

了解身份验证功能，能够对访问用户进行控制

了解利用账号控制 web 目录的访问权限，防止跨目录访问

了解为每个站点设置单独的应用程序池和单独的用户的方法

了解取消上传目录的可执行脚本的权限的方法

IIS的身份验证概述

匿名身份验证

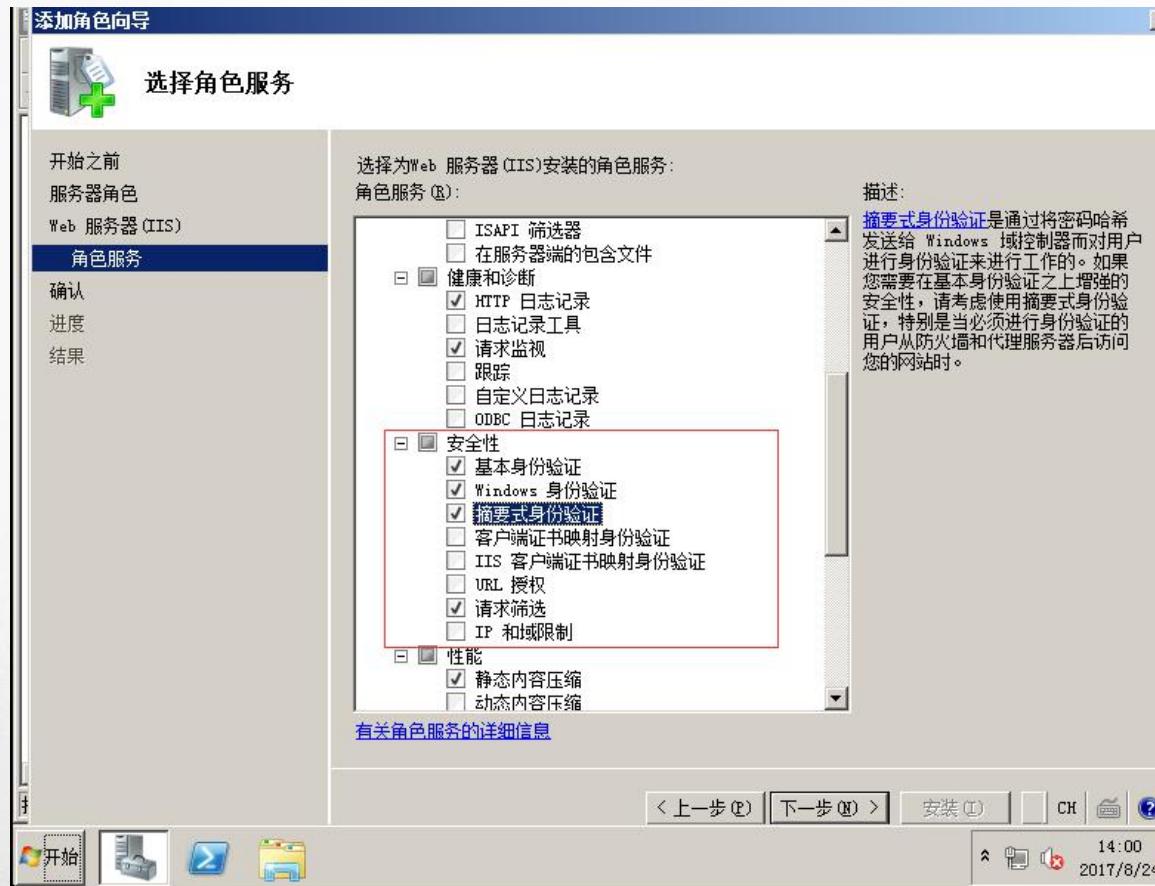
基本身份验证

摘要式身份验证

windows集成身份验证

IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

系统默认只启用了匿名身份验证，另外三种需要通过添加角色服务的方式来添加



另外身份验证的顺序为：

- 匿名身份验证>windows验证>摘要式身份验证>基本身份验证

- 可以这么理解，如果同时开启匿名身份验证和基本身份验证，客户端就会先利用匿名身份验证，所以基本身份验证即无效！

IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

➤ 匿名身份验证

➤ 即用户访问站点时，不需要提供身份认证信息，即可正常访问站点！

(服务端IIS设置允许匿名访问后，收到客户端的资源请求后，不需要经过身份验证，直接把请求的资源返回给客户端)

- GET /iisstart.htm HTTP/1.1
- Accept: */*
- Accept-Language: zh-cn
- UA-CPU: x86
- Accept-Encoding: gzip, deflate
- If-Modified-Since: Fri, 21 Feb 2003 12:15:52 GMT
- If-None-Match: "0ce1f9a2d9c21:d87"
- User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; InfoPath.1; .NET CLR 2.0.50727; MAXTHON 2.0)
- Host: 192.168.100.5
- Connection: Keep-Alive
-
- HTTP/1.1 200 OK
- Content-Length: 1193
- Content-Type: text/html
- Last-Modified: Fri, 21 Feb 2003 12:15:52 GMT
- Accept-Ranges: bytes
- ETag: "0ce1f9a2d9c21:d8b"
- Server: Microsoft-IIS/6.0
- MicrosoftOfficeWebServer: 5.0_Pub
- X-Powered-By: ASP.NET
- Date: Mon, 12 Nov 2007 07:29:40 GMT

IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

➤ 基本身份验证

- 若网站启用了基本身份验证，访问站点时，会要求用户输入密码！在网站后台等目录常用
- 使用此身份验证，需先将匿名身份验证禁用！



IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

➤ 基本身份验证

- 先禁用匿名身份验证，然后再启用基本身份验证，我们可以然后在点右边的编辑！
- 默认域：可以添加域账户，或将其留空。将依据此域对登录到您的站点时未提供域的用户进行身份验证。
- 领域：随便输入，将被显示到登录界面上。



IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

➤ 基本身份验证

首页访问正常无需账户密码



打开后台地址，需要输入本地用户组账户



IIS 服务器的安全设置——了解身份验证功能，能够对访问用户进行控制

摘要式身份验证

- 摘要式身份验证如基本身份验证一样需要输入账户密码，但是比基本身份认证更安全，
- 基本身份验证在网络上传输不加密的 Base64 编码的密码，而摘要式身份验证用户密码使用 MD5 加密！
- 使用摘要式身份验证必须具备下面三个条件：
- 浏览器支持 HTTP 1.1 IE5 以上都支持
- IIS 服务器必须是 Windows 域控制器成员服务器或者域控制器
- 用户登录招呼必须是域控制器账户，而且是同 IIS 服务器用以域或者信任域！
- 所以说摘要式身份验证是使用 Windows 域控制器对请求访问 Web 服务器内容的用户进行身份验证。

Windows 集成身份验证

- 如果您希望客户端使用 NTLM 或 Kerberos 协议进行身份验证，则应使用 Windows 身份验证。
- Windows 身份验证同时包括 NTLM 和 Kerberos v5 身份验证，它最适用于 Intranet 环境，其原因如下：
- 客户端计算机和 Web 服务器位于同一个域中。
- 管理员可以确保所有客户端浏览器均为 Internet Explorer 2.0 或更高版本。
- 不需要不受 NTLM 支持的 HTTP 代理连接。
- Kerberos v5 需要连接到 Active Directory，这在 Internet 环境中不可行

IIS 服务器的安全设置——**了解身份验证功能，能够对访问用户进行控制**

身份验证总结

在一些需要身份验证的地方，Windows 集成身份验证和摘要式身份验证，因为使用条件限制，在个人网站中运用很少，所以我们更多的使用的是基本身份验证！

IIS 服务器的安全设置

了解身份验证功能，能够对访问用户进行控制

了解利用账号控制 web 目录的访问权限，防止跨目录访问

了解为每个站点设置单独的应用程序池和单独的用户的方法

了解取消上传目录的可执行脚本的权限的方法

IIS 服务器的安全设置——了解为每个站点设置单独的应用程序池和单独的用户的方法

要新建应用程序池，在IIS管理控制台中右击**应用程序池**文件夹，指向**新建**，选择**应用程序池**



IIS 服务器的安全设置——了解为每个站点设置单独的应用程序池和单独的用户的方法

然后在弹出的**添加新应用程序池**对话框，在**应用程序池ID**栏输入应用程序池名，然后选择使用默认设置还是继承现有的应用程序池设置，再点击**确定**即可；

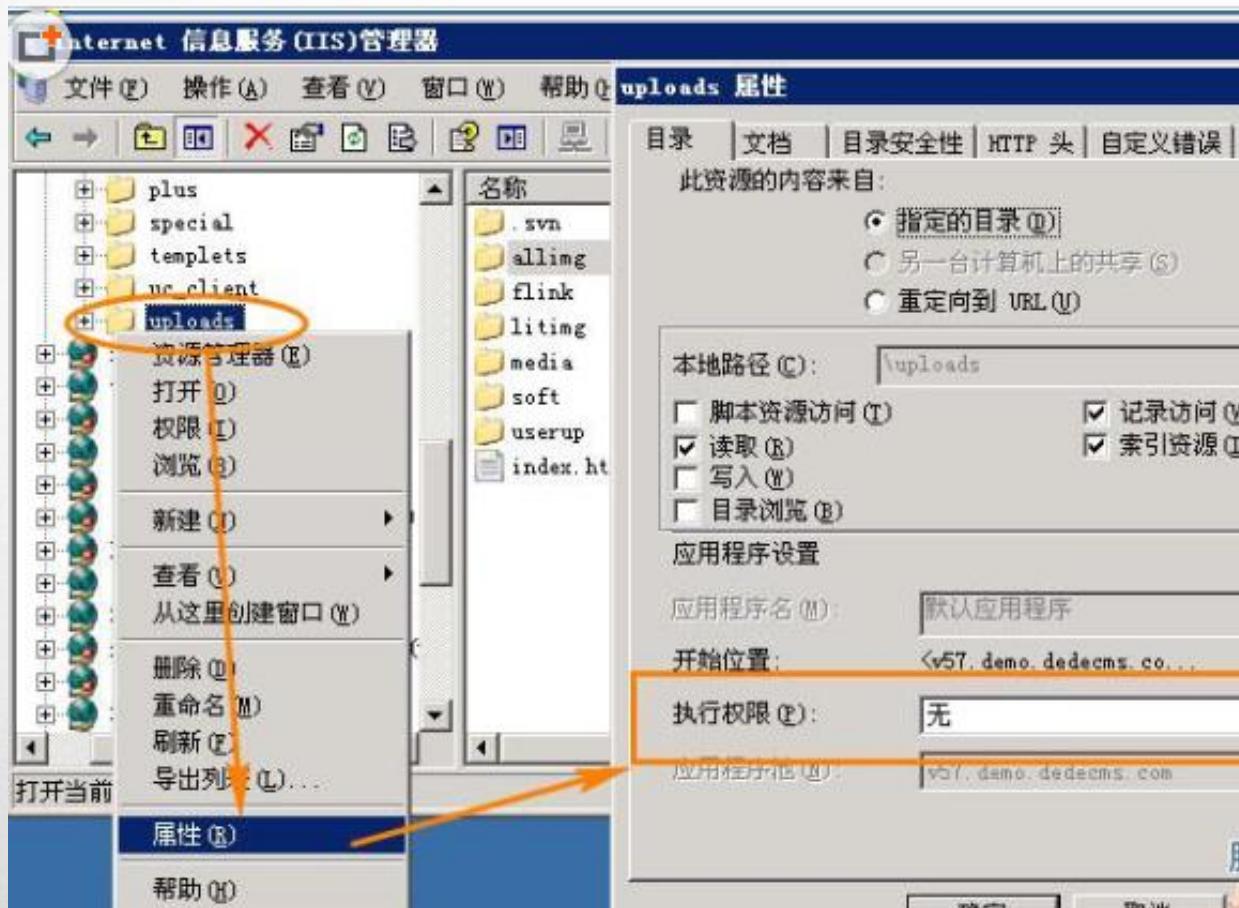
分配Web站点到应用程序池中

- 在IIS管理控制台中展开**网站**文件夹，右击对应的网站，然后选择**属性**，在弹出的**网站属性**对话框上，点击**主目录**标签，然后在**应用程序池**栏选择不同的应用程序池即可，默认情况下所有网站所使用的应用程序均名为**默认应用程序**，如果要想此网站使用不同的应用程序名，则在**应用程序名**栏修改即可，例如在此我就修改为**winsvr**，这主要是便于查看，然后点击**确定**即可

IIS 服务器的安全设置——了解取消上传目录的可执行脚本的权限的方法

Windows下的IIS6.0取消服务器主机空间目录脚本的执行权限

打开IIS中站点，在站点uploads目录、data目录以及静态html生成目录点击右键，菜单中选择“属性”，在目录属性面板选择执行权限为“无”即可



IIS 服务器的安全设置——了解取消上传目录的可执行脚本的权限的方法

IIS7取消服务器主机空间目录脚本的执行权限

- IIS7中的步骤
- 第一步呢，我们在IIS的左侧选中该目录，切换到功能视图
- 第二步呢，打开“处理程序映射”功能
- 第三步呢，打开右侧的“编辑功能权限”，将“脚本”这一项取消掉即可
- IIS7也类似于IIS6.0，选择站点对应的目录，data、uploads及静态html文件目录，双击功能视图面板中的“处理程序映射”



IIS 服务器的安全设置——了解取消上传目录的可执行脚本的权限的方法

IIS7取消服务器主机空间目录脚本的执行权限

- 在“编辑功能权限……”中，我们直接去除脚本的执行权限即可



IIS 服务器的安全设置——了解取消上传目录的可执行脚本的权限的方法

IIS7取消服务器主机空间目录脚本的执行权限

- 若想让指定目录只有读取权限，只要在目录中放置一个名为 “web.config”，内容为

- <?xml version="1.0" encoding="UTF-8"?>
- <configuration>
- <system.webServer>
- <handlers accessPolicy="Read" />
- </system.webServer>
- </configuration>
- 这样，在访问该目录下的 asp、php 等可执行文件时，IIS7 就会输出如下错误提示

HTTP 错误 401.3 - Unauthorized

由于 Web 服务器上此资源的访问控制列表(ACL)配置或加密设置，您无权查看此目录或页面

IIS 服务器的安全设置——启用或禁用日志记录，配置日志的记录选项

IIS启用日志功能安全基线要求项

- 1、参考配置操作
- 打开IIS管理工具，右击要管理的站点，选择“属性”。在“Web Site”选择“启用日志记录”，从下拉菜单中选择“Microsoft IIS日志文件格式”。“W3C”日志格式存在日志记录时间与服务器时间不统一的问题，所以应尽量采用IIS日志格式。



IIS记录安全事件安全基线要求项

1、参考配置操作

- (1) 进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核对象访问”、“审核目录服务器访问”、“审核系统事件”、“审核帐号管理”、“审核过程追踪”选项。
- (2) 运行IIS管理器->“Internet信息服务”->“应用相关站点”属性->“网站”->“属性”->启动日志记录“高级”，选择“时间”、“日期”、“扩展属性”

安全基线项目名称	IIS 日志访问权限安全基线要求项
安全基线编号	编号 QB-IIS-03-01-04 重要
安全基线项说明	设备应配置权限，控制对日志文件读取、修改和删除等操作。
检测操作步骤	<p>1、参考配置操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核策略更改”配置相应选项。</p>
基线符合性判定依据	<p>1、判定条件</p> <p>确定系统相关“审核策略”</p> <p>2、检测操作</p> <p>进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中配置相应“审核策略更改”选项选择状态。</p>



IIS 服务器的常见漏洞

掌握 IIS6, IIS7 的文件名解析漏洞

掌握 IIS6 写权限的利用

掌握 IIS6 存在的短文件名漏洞

IIS 服务器的常见漏洞 —— 掌握 IIS6, IIS7 的文件名解析漏洞

IIS 6.0解析利用方法有两种

1.目录解析

- /xx.asp/xx.jpg

在网站下建立文件夹的名字为 .asp、.asa 的文件夹，其目录内的任何扩展名的文件都被IIS当作asp文件来解析并执行。

例如创建目录 wooyun.asp，那么 /wooyun.asp/1.jpg 将被当作asp文件来执行。假设黑阔可以控制上传文件夹路径,就可以不管你上传后你的图片改不改名都能拿shell了。

2.文件解析

- wooyun.asp;.jpg

在IIS6.0下，分号后面的不被解析，也就是说 wooyun.asp;.jpg 会被服务器看成是wooyun.asp还有IIS6.0默认的可执行文件除了asp还包含这三种

/wooyun.asa
/wooyun.cer
/wooyun.cdx

IIS 服务器的常见漏洞 —— 掌握 IIS6 存在的短文件名漏洞

1)利用“~”字符猜解暴露短文件/文件夹名。

2).Net Framework的拒绝服务攻击。

Windows 还以 8.3 格式生成与 MS-DOS 兼容的（短）文件名，以允许基于 MS-DOS 或 16 位 Windows 的程序访问这些文件。在cmd下输入 “dir /x” 即可看到短文件名的效果。

通配符“*”和“?”发送一个请求到iis,当IIS接收到一个文件路径中包含“~”的请求时，它的反应是不同的。基于这个特点，可以根据http的响应区分一个可用或者不可用的文件。如下图所示不同IIS版本返回信息的不同

IIS Version	URL	Result/Error Message
IIS 6	/valid*~1*.aspx	HTTP 404 - File not found
IIS 6	/Invalid*~1*.aspx	HTTP 400 - Bad Request
IIS 5.x	/valid*~1*	HTTP 404 - File not found
IIS 5.x	/Invalid*~1*	HTTP 400 - Bad Request
IIS 7.x .Net.2	/valid*~1*/	Page contains: "Error Code 0x00000000"
No Error Handling		
IIS 7.x .Net.2	/Invalid*~1*/	Page contains: "Error Code 0x80070002"
No Error Handling		

IIS 服务器的常见漏洞 —— 掌握 IIS6 存在的短文件名漏洞

短文件名漏洞解决办法

- 1. 关闭NTFS 8.3文件格式的支持。该功能默认是开启的，对于大多数用户来说无需开启。
- 如果是虚拟主机空间用户，请联系空间提供商进行修复。
- 修改方法：
 - 1) 修改注册列表
HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation的值为1，或者，可以点击此下载，然后运行，再重启机器。(此修改只能禁止NTFS8.3格式文件名创建，已经存在的文件的短文件名无法移除)，
 - 2) 如果你的web环境不需要asp.net的支持你可以进入Internet 信息服务(IIS)管理器 --- Web 服务扩展 - ASP.NET 选择禁止此功能。
 - 3) 升级net framework 至4.0以上版本。
 - 攻击者可以利用“~”字符猜解或遍历服务器中的文件名，或对IIS服务器中的.Net Framework进行拒绝服务攻击

THANK YOU 感谢观看
FOR YOUR ATTENTION!

北京谷安天下科技有限公司

谷安天下公司主页：www.gooann.com

谷安培训教育网页：<http://px.gooann.com>

安全意识产品网页：<http://sectv.gooann.com>

产品解决方案网页：<http://product.gooann.com>

谷安信息安全商城：<http://gooannpx.taobao.com>