i春秋:警惕IIS6.0站上的目录路径检测解析绕过上传漏洞

转载

喜欢散步 于 2015-06-01 04:08:59 发布 4710 收藏
文章标签： 初学 渗透 入侵 安全 漏洞
实验环境

- 实验环境
  - 操作机：`Windows XP`
  - 目标机：`Windows 2003`
- 目标网址：`www.test.com`
- 实验工具：中国菜刀 `BurpSuite`

实验目的
本课程带领大家利用IIS6.0目录路径检测解析漏洞，绕过上传检测，获取WEBShell。通过亲身实验，验证获取WEBShell的可行性，从而提高自身的安全防御意识。

实验思路

1. 上传正常图片和WEBShell
2. 利用IIS6解析缺陷绕过上传检测
3. 获取WEBShell权限
4. 防御方案

实验步骤
1

上传正常图片和WEBShell

准备一张普通的图片，使用`*.jpg`在电脑上进行搜索，可以看到很多图片，复制一张图片放到桌面上，改名为`tupian.jpg`。

打开上传地址，选取上传图片。

> **小i提示：**
>
> - 上传地址就是可以上传文件的地方
> - 本次实验用的测试网址`http://www.test.com`作为目标网站

上传成功后，观察返回的页面信息

小i提示：

- 观察红字部分（上传是否成功，成功为 **Upload Successful** ，失败这一行会显示失败信息）
- 观察蓝字部分（上传成功后文件的路径），它的名字是时间戳（通常是一个数字序列，唯一地标识某一刻的时间）加自己的尾缀

准备的是**ASP**环境,需要使用ASP的一句话，接着来制作一句话，新建一个空文本文档，将ASP的一句话写入到文本中,修改文件名为`yijuhua.ASP`并保存到桌面。

小i提示：

- 一句话是一种常见的网站后门，短小精悍,而且功能强大，隐蔽性非常好，在渗透测试过程中始终扮演着强大的作用。
- 不同的环境需要选取与环境匹配的一句话，一句话中`<%eval request[‘这里是密码’]%>`，本例中我们以 `1` 为密码。

上传ASP文件，发现提示错误信息：**White List Match Failed--asp** ,可能服务器端禁止了尾缀asp的文件上传。

2

利用IIS6解析缺陷绕过上传检测

首先打开**BurpLoader**，选择 `Proxy->Options` ，设置**BurpLoader代理地址**，默认为`127.0.0.1`、端口：`8080`。

接着修改**Firefox**的代理设置，修改代理地址以及端口（设置与在**BurpLoader**中设置的代理地址相同：`127.0.0.1`、端口：`8080`）。

小i提示：

- 不同浏览器设置代理的方法不相同， 但是设置位置基本类似，此处我们以火狐浏览器为例，首先点击右上角的工具->选项->网络->设置->手动配置代理，填入BurpLoader中设置的代理地址。

设置好浏览器代理后，我们再打开**BurpLoader**抓包，暂时截获浏览器给服务器发送的数据包，Proxy->Intercept 点击 intercept off 改为intercept on，截获的数据包将在关闭抓包的时候发送给服务端。

查看数据包：其中Content-Disposition:form-data;name=”path”下面的一行为服务保存文件的相对路径，我们把原本的 uploading/ 改为 uploadimg/1.asp;。

> **小i知识点：**
>
> - 本例用了IIS6.0目录路径检测解析，文件的名字为“*.asp/xxx.jpg”，也同样会被 IIS 当作 ASP文件来解析并执行
> - 首先我们请求 /aaa.asp/xxxx.jpg
> - 从头部查找查找 "."号,获得 .asp/xxxx.jpg
> - 查找"/",如果有则内存截断，所以/aaa.asp/xxxx.jpg会当做/aaa.asp进行解析

修改完成后，关闭抓包（点击intercept on ->intercept off），上传数据,查看浏览器发现上传成功，复制File Name后面的信息（例如：1.asp;14127900008.asp ）；在前面添加上uploadimg/粘贴复制到网站地址后面，从而构造访问地址（例
如：http://www.test.com/uploadimg/1.asp;14127900008.asp ），并复制访问地址。

3

获取WEBShell权限

打开中国菜刀软件并填入复制的访问地址，填入你设定的密码,之前我们在“**一句话**”中设置的密码是1，选择脚本类型为ASP，单击添加按钮，就会看到菜刀上出现一行信息，最后我们双击这条信息后，就可以看到目标网站的目录，这样我们就成功获取到目标网站的**WEBShell**权限。

> **小i知识点：**
>
> - 中国菜刀，是一款专业的网站管理软件，用途广泛，使用方便，小巧实用。只要支持动态脚本的网站，都可以用中国菜刀与一句话协作来进行管理

这里可以看见我们刚刚上传的文件，其中有一个空文件夹1.asp;以及其它我们上传的文件。

4

防御方案

1.客户端检测，使用JS对上传图片检测，包括文件大小、文件扩展名、文件类型等

2.服务端检测，对文件大小、文件路径、文件扩展名、文件类型、文件内容检测，对文件重命名

3.其他限制，服务器端上传目录设置不可执行权限