i春秋:警惕您站上的文件扩展名绕过漏洞

转载

喜欢散步 于 2015-06-01 04:02:10 发布 1801 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

实验目的
本课程带领大家学习利用通过修改文件扩展名，绕过上传验证，获取WebShell。通过亲身实验，验证绕过上传验证的可行性，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. 修改文件扩展名绕过上传检测
3. 获取WebShell权限
4. 防御方案

实验步骤
1

上传正常图片和WebShell

上传正常的图片以及上传PHP一句话文件，查看区别，准备一个普通的图片，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，选取准备好的图片，上传图片。

> **小i提示：**
>
> 上传地址就是可以上传文件的地方
>
> 本次实验使用的是一个测试网址`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：

观察红字的部分（上传是否成功）

观察蓝字的部分（上传后文件的路径）

由于我们准备的是PHP环境,所以需要使用PHP的一句话，接着我们来制作一句话。

小i提示：

不同的环境需要选取与环境匹配的一句话

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。

新建一个空文本文档，将一句话写入到文本中。

修改文件名为`yijuhua.php`并保存到桌面。

上传PHP文件，这时如果提示上传失败，则证明服务器可能对上传文件的后缀做了判断。

2

修改文件扩展名绕过上传检测

小i知识点：

- php语言除了可以解析以`php`为后缀的文件，还可以解析`php2`、`php3`、`php4`、`php5`这些后缀的文件。

我们可以将文件名修改为如下的后缀`yijuhua.php2`，重新上传。

我们发现上传依旧失败，接着我们把文件名改为`yijuhua.php3`、`yijuhua.php4`、`yijuhua.php5`依次进行上传尝试，直到发现`yijuhua.php3`和`yijuhua.php4`是可以上传成功的。

小i提示：

- 不同的服务器，可以上传的文件类型也不同，所以需要进行逐个排除

当使用yijuhua.php3或yijuhua.php4上传成功后，我们需要访问文件，这时可直接复制文件路径（File Name后面的内容，即是一句话的路径），将复制的地址粘贴至网站地址后面，从而构造访问地址，并复制构造好的地址。例如:http://www.test.com/uploading/1412097218.php3。

3

获取WEBShell权限

使用中国菜刀软件打开webshell地址

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,这里设置的密码是1，选择脚本类型为PHP，单击添加按钮，最后我们双击指定条目后的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。

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