i春秋:警惕Apache站上的解析缺陷绕过上传漏洞

转载

喜欢散步 于 2015-06-01 04:09:51 发布 10918 收藏 1
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
本课程带领大家通过利用Apache解析漏洞绕过验证进行上传木马，从而使了解到上传木马并非难事，需要提高自身防御能力。

实验思路

1. 上传正常图片和WEBShell
2. 利用Apache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

打开浏览器, 在地址栏中输入目标的站点(IP地址)。进入到站点后,点击开始搜索图片。

搜索的图片的后缀名格式为`.jpg` 。

把搜索到的图片,复制粘贴到桌面,进行上传。

点击浏览选择桌面上的图片。

点击提交成功正常图片上传，(图片的后缀名类型在允许的上传后缀名类型范围内) 返回红色的成功信息和图片路径 在 `uploading/`文件夹下的文件名为 `tupian.jpg` 的图片文件。

尝试上传一句话文件

点击桌面的快捷方式(也就是访问tools工具文件夹下的caidao文件夹下的一句话.txt) 点击打开一句话`.txt` 文件复制一句话的 php 代码。

> **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

新建一个空文本文档，将php的一句话写入到文本中,修改文件名为`yijuhua.php`并保存到桌面

> **小i提示：**
>
> - 一句话中`$_POST['这里是密码']`，本例中我们以 `1` 为密码

点击浏览选择上传桌面的`yijuhua.php`文件。

点击提交 显示上传失败(鼠标下显示上传失败 文件名不是上传的类型)，说明服务器会对上传文件进行验证，我们需要绕过验证。

2

利用Apache解析缺陷绕过上传检测

进行绕过上传，将 yijuhua.php文件名加上后缀名为`.7z`。

> **小i提示：**
>
> - 也可以修改后缀名为`cab` `zip` `bmp`等,只要是允许的上传类型都可以上传成功

点击浏览,选择上传桌面上的`yijuhua.php.7z`文件名进行上传。

显示上传成功,将 `uploadimg/`上传路径和`yijuhua.php.7z` 复制下来。

3

获取WEBShell权限

把 `http:www.test.com/uploadimg/yijuhua.php.7z` 这个url 路径复制到菜刀工具进行连接。

打开桌面快捷方式(也就是在tools文件夹下的caodao文件夹)打开chopper.exe文件。

在空白处点击鼠标右键选择添加。

将上传的文件路径放到菜刀链接地址然后输入上传一句话里文件里设置的密码为1,选择相应的脚本类型,这里上传的是php脚本,最后点击添加。

双击点击打开地址,连接成功,可以成功看到 uploadimg文件夹下有一个 key文件。

右键key文件,点击编辑,可以看到字符串说明一句话上传成功。

4

防御方案

1.普通用户与系统管理员的权限要有严格的区分

2.强迫使用参数化语句

3.加强对用户输入的验证

4.多使用数据库自带的安全参数

5.使用专业的漏洞扫描工具来寻找可能被攻击的点