

i春秋:警惕您站上的htaccess文件上传解析漏洞

转载

喜欢散步  于 2015-06-01 04:14:27 发布  8119  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上传htaccess文件解析漏洞绕过验证进行上传WebShell,从而使了解到上传WebShell并非难事,需要提高自身漏洞防御能力。

实验思路

1. 上传正常图片和WEBSHELL
2. 利用.htaccess文件绕过上传检测
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。

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。

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。

点击提交成功上传图片,(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,图片路径为 uploading/文件夹下的文件名为 tupian.jpg 的图片文件。

尝试上传 一句话文件的木马。

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。

在桌面新建一个文本把刚才复制的php代码 粘贴到此文件下。

将密码改为1保存 后保存。

将新建的文本文档文件名改为yijuhua.php。

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.htaccess文件绕过上传检测

打开.htaccess文件。

.htaccess文件里的代码的含义是 将上传的文件后缀名为.jpg格式的文件以 php格式来解析文件。

将.htaccess文件进行上传,上传成功。

小提示:

- .htaccess是apache服务器中的一个配置文件,不是上传的文件的黑名单之内,所以.htaccess文件是可以上传成功。

把一句话文件的后缀名为yijuhua.php改为后缀名为jpg格式。

小提示:

- 上传成功到服务器的.htaccess文件里的代码可以让.jpg后缀名文件格式的文件名以php格式解析 所以我们要把yijuhua.php文件的后缀名改为.jpg格式,让.htaccess文件解析 yijuhua.jpg文件里的php代码,使木马上传成功。

3

获取WEBSHELL权限

上传成功之后,复制上传路径到菜刀链接中(地址为 `www.test.com/uploading/yijuhua.jpg`)。

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。

访问木马地址,复制链接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 点击添加。

双击点击打开地址,连接成功,可以成功看到 uploading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 说明一句话木马上传成功。

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