

i春秋:警惕您站上的“FCK编辑器”解析漏洞突破检测上传后

原创

喜欢散步  于 2015-06-01 04:17:27 发布  6632  收藏

文章标签: [初学](#) [安全](#) [渗透](#) [漏洞](#) [入侵](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/hopecsmile/article/details/46298641>

版权

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

本课程带领大家利用“FCK编辑器”解析漏洞突破检测上传后门, 进而帮助大家提高自身的漏洞防御能力。

实验思路

1. FCK2.6.6版本上传漏洞绕过测试
2. FCK2.4.2版本上传漏洞绕过测试
3. 防御方案

实验步骤

1

FCK2.6.6版本上传漏洞绕过测试

在浏览器地址栏中的测试网址后面输入: `/_whatsnew.html` 查看版本信息为**FCK2.6.6**。

现在打开FCK的编辑器的上传点页面, 在浏览器地址栏中的测试网址后面输入:

```
/editor/filemanager/connectors/test.html
```

在页面中点击”浏览”, 本地选择一个正常图片上传, 点击Upload进行上传。

上传正常则返回成功提示: `File uploaded with no errors`(文件上传, 没有错误), 如上传错误, 则返回失败提示: `Error on file upload Error number:102`(在文件上传错误编号错误:102)。

小提示:

- 如上传了一张图片(`tuping.jpg`), 返回上传成功提示, 即可判断出来FCK是可以正常使用的, 如果图片上传不成功则是FCK编辑器不可以利用。

点击Get Folders and Files(获取文件夹和文件)来查看当前文件信息。点击后,我们可以看到刚刚上传的图片信息: ,但是上传后, IIS是不会对jpg文件进行解析的,所以需要使用asp才可以执行asp一句话。于是我们需要上传asp文件, 如(图4)所示,但是在上传'yijuhua.asp'时,返回了错误信息: Invalid file(无效文件),服务器不允许直接上传后缀为asp, 由此可以推断服务器会对上传文件进行检测, 直接上传asp文件是无法通过验证的。所以我们要利用解析漏洞进行绕过检测。

小知识:

- IIS解析原理:Windows 2003 IIS6 存在着文件解析路径的漏洞, 当文件夹名为类似*.asp结尾的目录名的时候(即文件夹名看起来像一个ASP文件的文件名), 此时此文件夹下的任何类型的文件都可以在IIS中被当做ASP程序来执行。这样黑客即可上传扩展名为.jpg或.gif之类的看起来像是图片文件的木马文件, 通过访问这个文件即可运行木马。比如 1.asp/a.jpg

小提示:

- 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

首先点击Create Folder(创建文件夹)新建一个文件夹名为1.asp点击确定

然后在Current Folder(当前文件夹)里面输入刚刚建立的文件夹名字1.asp, 设置好文件保存路径,保存到1.asp文件夹里,把一句话(yijuhua.asp)的后缀换成.jpg,然后上传,从而绕过上传验证。

Current Folder(当前文件夹)把创建好的1.asp文件夹目录中, 再创建一个2.asp的文件夹(因为不创建2.asp的文件夹1.asp的文件夹是不能使用的, 所以要创建2.asp文件夹才可以使用)创建好后2.asp系统把1.asp文件夹自动生成出来然后1.asp的文件夹才可以使用, 在上传(yijuhua.jpg)木马。

Current Folder(当前文件夹)设置好目录保存文件路径1.asp上传(yijuhua.jpg)返回File uploaded with no errors(没有错误上传的文件)上传成功。

看到url="/userfiles/file/1.asp/"文件夹下的上传成功后,组合一个新的网址,先把文件夹路径给复制下来,然后复制上传后的一句话文件名, 然后组合文件夹路径: /userfiles/file/1.asp/上传后一句话文件名: yijuhua.jpg组合: /userfiles/file/1.asp/yijuhua.jpg组合好一个新网址后,打开目标站放入到目标站的网址后面最终地址: www.test.com/userfiles/file/1.asp/yijuhua.jpg然后使用菜刀连接最终组合好的地址称为webshell。

连接webshell地址: www.test.com/userfiles/file/1.asp/yijuhua.jpg成功连接到服务器。



2

FCK2.4.2版本上传漏洞绕过测试

打开FCK上传点在浏览器地址栏中的测试网址后面输入：

```
editor/filemanager/browser/default/connectors/test.html
```

首先要判断FCK是否能上传文件,上传一个正常图片,查看FCK是否能正常使用,正常使用才可以判断出能否使用解析漏洞拿到webshell,正常图片上传失败则FCK编辑器不能使用(正常图片无法上传,则FCK不能上传文件不能被利用)。



FCK2.4.2上传点在网址后面输入：

```
/editor/filemanager/browser/default/connectors/test.html
```

打开编辑器后,首先直接上传一个yijuhua.asp文件,返回Invalid file(无效文件)上传失败,被检测出来无法上传,现在使用解析漏洞进行绕过。



利用解析漏洞进行绕过检测,跟上面演示FCK2.6.6版本相似,点击(Create Folder)新建一个文件夹名字为2.asp, FCK2.4.2版本直接创建文件夹系统就会生成出来.所以2.6.6版本和2.4.2版本有小细节不一样,比如2.6.6要创建两次文件夹才可以生成出来一个文件夹,2.4.2直接创建一个文件夹系统就会生成出来。



创建好后的2.asp文件夹,在Current Folder(当前文件夹)设置好/2.asp/文件保存路径,保存2.asp文件夹里面。



将木马文件后缀改成.jpg正常图片类型进行上传,上传的是yijuhua.jpg点击上传返回File uploaded with no errors(没有错误上传的文件)上传成功,组合一个新的网址: /userfiles/file/2.asp/yijuhua.jpg组合上目标网站地址/userfiles/file/2.asp/`yijuhua.jpg`www.test.com/userfiles/file/2.asp/yijuhua.jpg使用菜刀连接webshell,成功连接到服务器。



3

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