i春秋:通过案例学安全—“FCK编辑器”版本识别及信息收集技

转载

喜欢散步 于 2015-06-01 04:16:02 发布 3500 收藏
文章标签： 初学 安全 渗透 漏洞 入侵
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`

实验目的
本课程带领大家学习如何查看“FCK编辑器”的版本并且收集信息，为之后章节利用“FCK编辑器”解析漏洞打下基础。

实验思路

查看FCKeditor版本信息

了解FCKeditor不同版本上传地址

防御方案

实验步骤
1

查看FCKeditor版本信息

> - 本次实验使用测试网址`http://www.test.com`作为目标网站
> - 本节课程我们将查看FCK的两个不同的版本,由此来了解FCK不同版本的上传地址。

首先，在浏览器地址栏中的测试网址后面输入：`/_samples/default.html` 打开编辑器页面，点击“？”图标(鼠标放在问号图标上面点击问号图片)可以在关于中查看到编辑器的版本信息为`2.4.2。

在浏览器地址栏中的测试网址后面把`_samples/default.html`改为`/_whatsnew.html`访问这个地址可以查看FCK当前版本和历史版本，第一个显示的是当前版本`Version 2.4.2`下面是**FCK 2.4.2的历史版本**。

接下来,我们在浏览器地址栏中的测试网址后面输入:`/_samples/default.html`打开编辑器页面，点击”？”(问号图标)可以查看编辑器的版本信息为`2.6.6`，与刚才的`2.4.2`的查看方法是相同的。

在浏览器地址栏中的测试网址后面把`/_samples/default.html`改为`/_whatsnew.html`访问这个地址可以查看FCK当前版本和历史版本，第一个显示的是当前版本’Version 2.6.6’下面是FCK2.6.6的历史版本。

2

了解FCKeditor不同版本上传地址

我们先来查看**FCK2.4.2版本**的上传点，首先打开FCK编辑器页面,在编辑框的上方，可以看到图片上传图标，图片上传这里就是一个上传点，点击上传图片图标出现图像域，然后点击'上传'标签页。接下来，浏览本地要上传的文件(如yijuhua.jpg)，选择文件后，点击'发送到服务器上'就可以进行上传了。

我们继续查看**FCK2.4.4版本**的其他上传点，在浏览器地址栏中的测试网址后面输入：`editor/filemanager/browser/default/connectors/test.html`打开另外一个上传点，这里有几个按钮，首先是`Get Folders and Files`(获取当前文件夹和文件)，点击后，可以看到当前的文件信息；其次是`Create Folder`(创建目录)，我们可以通过`Create Folder`来新建文件夹。点击"浏览",这里可以选择要上传的文件，例如上传木马(yijuhua.jpg)，然后点击Upload(上传)按钮，即可完成上传。

我们继续查看**FCK2.4.4版本**的另一个上传点，在浏览器地址栏中的测试网址后面输入：`/editor/filemanager/upload/test.html`即可打开第三个上传点页面，在这里点击浏览选择文件,然后点击`Send it to the Server`(发送到服务器上传)，即可上传，如果上传成功，则会自动显示地址在`Uploaded File URL`中(上传的文件URL)。

FCK2.6.6版本的上传点与**FCK2.4.2**的基本相同，在浏览器地址栏中的测试网址后面输入：`/editor/filemanager/connectors/test.html`打开后，可以看上传点，页面与`FCK2.4.2`版本是相同的。

接下来，我们查看**FCK2.6.6版本**的另一个上传点，在浏览器地址栏中的测试网址后面输入：`/editor/filemanager/connectors/uploadtest.html`，打开后，可以看见，与**FCK2.4.2版本**的第二个上传点页面也是相同的。

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