**文件包含漏洞(本地包含配合文件上传)**

**预备知识**

程序开发人员通常会把可重复使用的函数写到单个文件中，在使用某些函数时，直接调用此文件，无须再次编写，这种调用文件的过程称为包含。

**实验目的**

学会本地包含配合文件上传

**实验工具**

火狐浏览器

**实验环境**

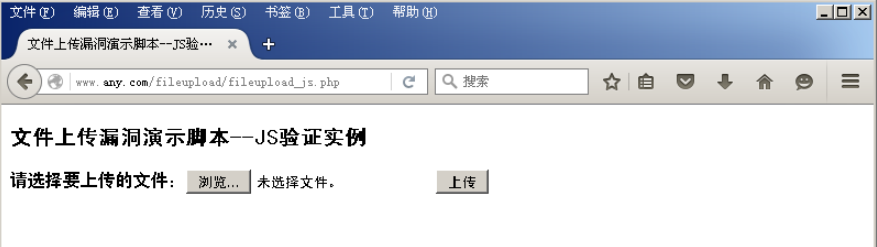
客户机一台（操作系统为Windows Server 2003）服务器一台（操作系统为Windows Server 2003）

**实验步骤**

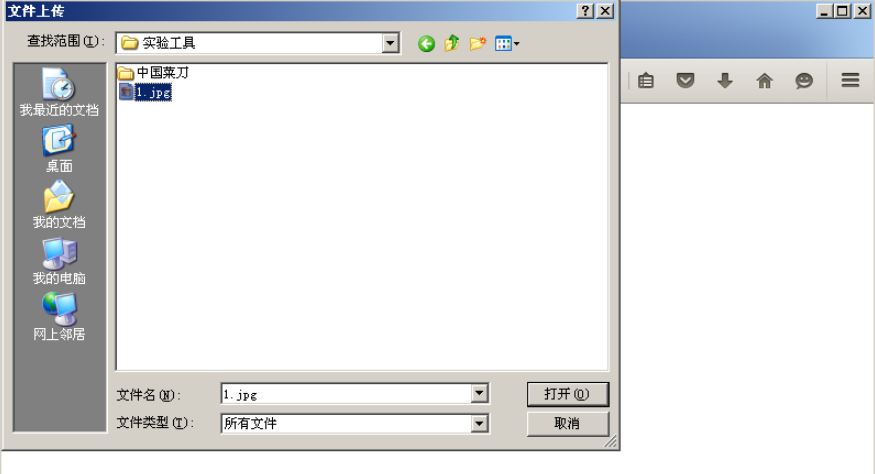
1、访问http://127.0.0.1/FI/PHP\_FI.php?filename=RFI.txt网页显示是远程文件包含漏洞。



2、浏览网址http://127.0.0.1/fileupload/fileupload\_js.php



点击【浏览】，选择【桌面】—【实验工具】—【1.jpg】，点击【打开】。



点击【上传】。结果如下图



文件1.jpg的内容如下图

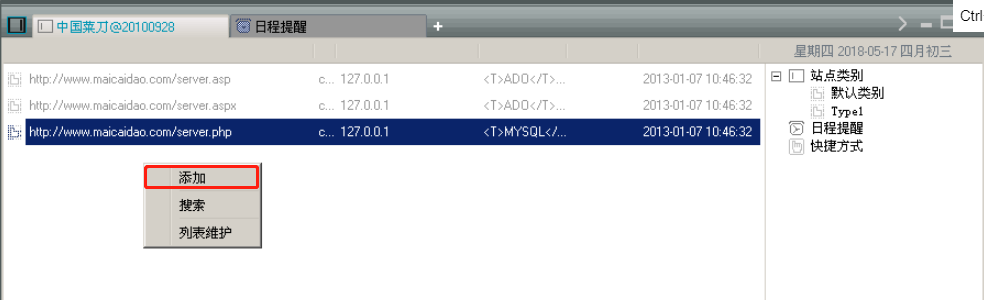
http://192.168.29.251/Public/course/584e1e345bacc.png

3、浏览器浏览网址http://127.0.0.1/FI/PHP\_FI.php?filename=../fileupload/uploads/1.jpg

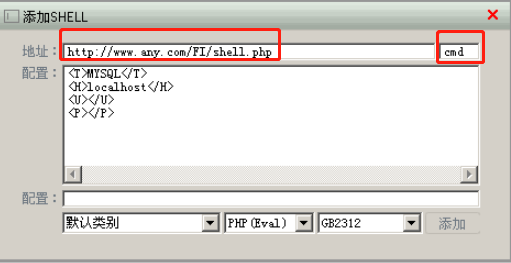


4、点击桌面的【实验工具】文件夹，打开【中国菜刀】文件夹。找到【中国菜刀.exe】并双击打开。

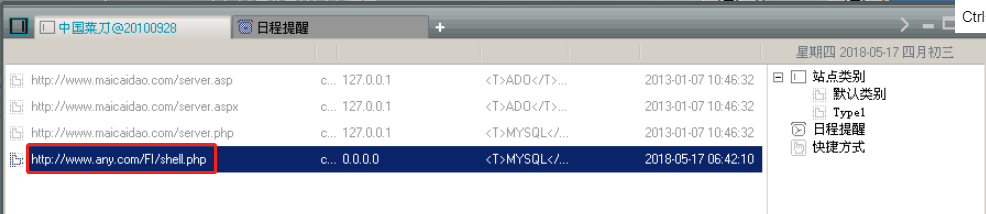
空白处单击，选择【添加】



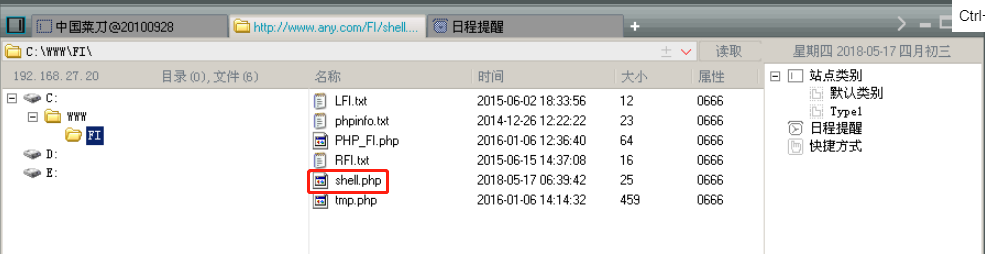
输入地址http://127.0.0.1/FI/shell.php，地址后的密码填写cmd。点击【添加】



双击下图红框内文本即可运行



实验结果如下



5、实验结束，关闭所有程序和虚拟机。