会话劫持攻击

一【实验目的】

- 了解 Session 的概念。
- 了解会话劫持的攻击方式。

二【实验环境】

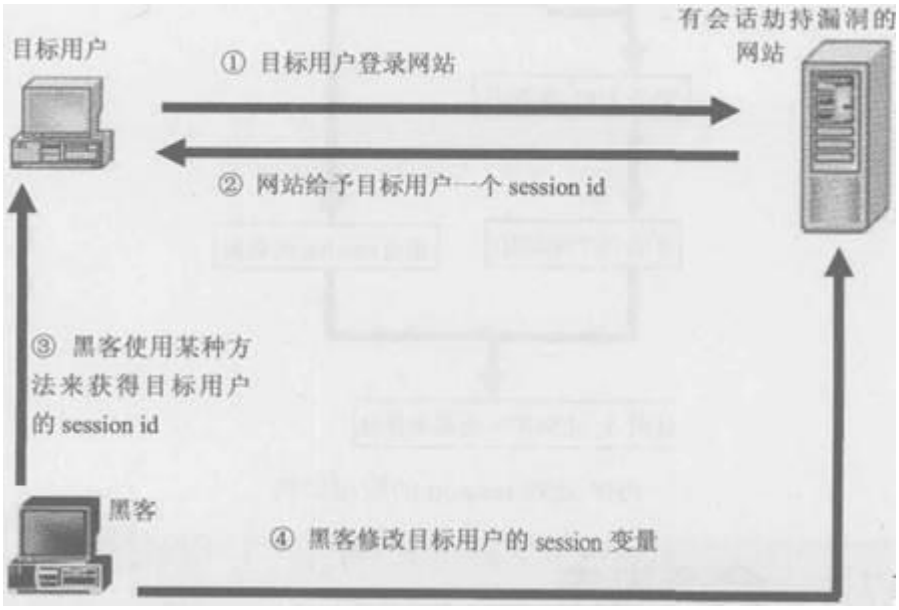
- 操作机和靶机：Windows 10 操作机，无靶机
- 网络拓扑结构：单一操作机
- 访问方式：本地访问操作机

三【实验原理】

会话劫持攻击实验原理如下：

会话劫持(Session Hijacking)攻击是指黑客利用各种手段来获取目标用户的 session id。session id 是 Web 应用程序用来识别用户的工具，如果黑客有了目标用户的 session id，他就可以存取目标用户在 Web 应用程序中的 session 变量值。这些 session 变量是相当重要的数据，如购物网站中用户所购买的商品名称、数量和付款方式等都是保存在 session 变量内。如果黑客使用目标用户的 session id 来登录网站，他就可以利用目标用户的身份来购买商品，当然最后的账还是算在目标用户身上。

会话劫持攻击步骤如下：



步骤 1：目标用户登录有会话劫持漏洞的网站。

步骤 2：网站给予目标用户一个 session id。

步骤 3：黑客使用某种方法来获得目标用户的 session id。

步骤 4：在目标用户的登录期间，黑客使用目标用户的 session id 来登录网站。黑客修改目标用户的 session 变量，来达到攻击的目的。

黑客获取目标用户的 session id 的方法有以下 3 种：

（1）暴力破解(Brute force)：黑客尝试许多的 session id 值，直到破解为止。

（2）计算：如果 session id 是使用非随机的方式产生，那么就有可能通过计算得出。

（3）窃取：使用网络截获、安装病毒或 XSS 攻击等方法来获得。

四【实验步骤】

（1）打开操作机，进入 phpStudy 所在安装文件夹【C:\tools\phpstudy】，双击【phpStudy.exe】启动 phpStudy。如下图 1 所示。

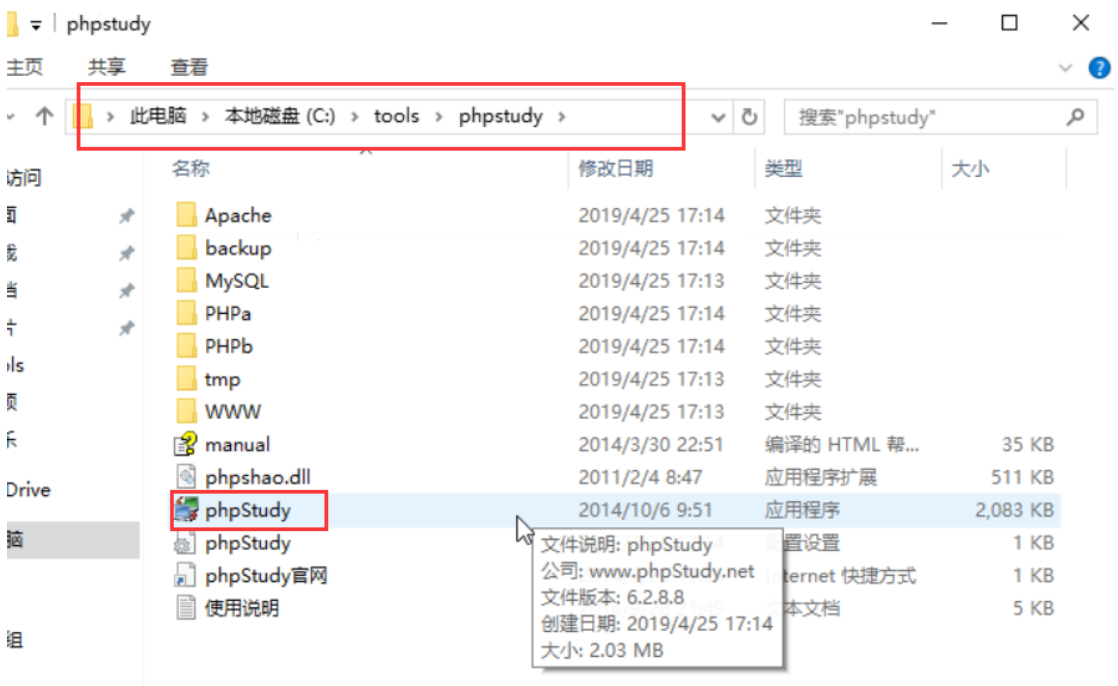


图 1

（2）在【phpStudy 启停】中点击【启动】。如下图 2 所示。

图 2

（3）将【C:\tools】中的【Session_Hijacking】复制到 phpStudy 根目录

【C:\tools\phpstudy\WWW】。如下图 3 和图 4 所示。

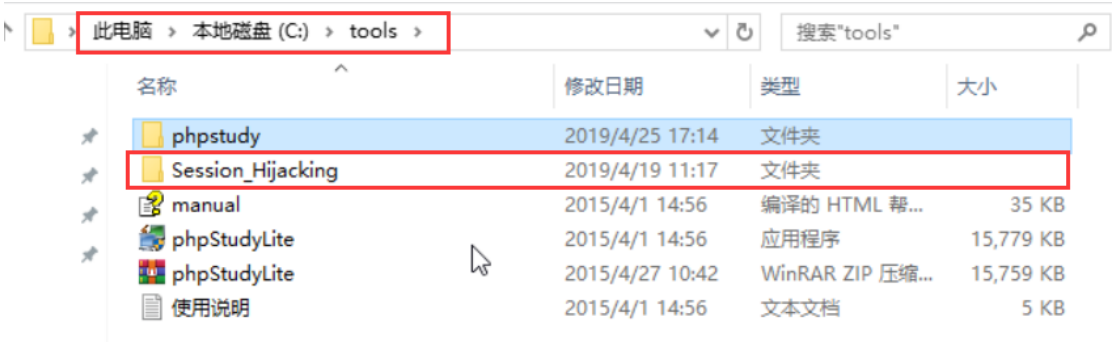


图 3

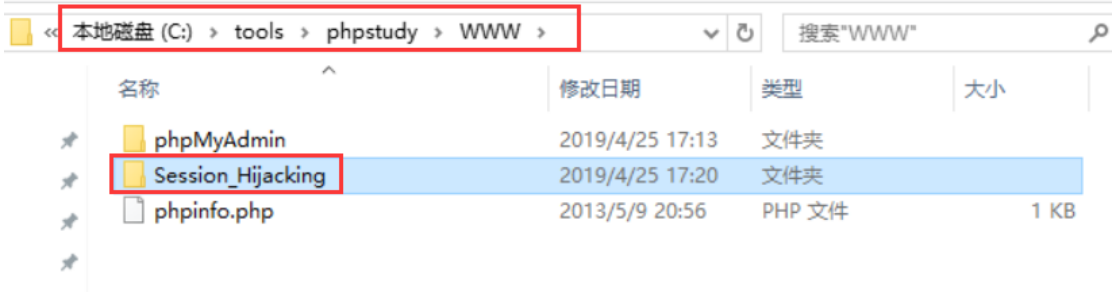


图 4

（4）在 phpStudy 主界面点击【其它选项菜单】-【MyHomePage】。如下图 5 所示。

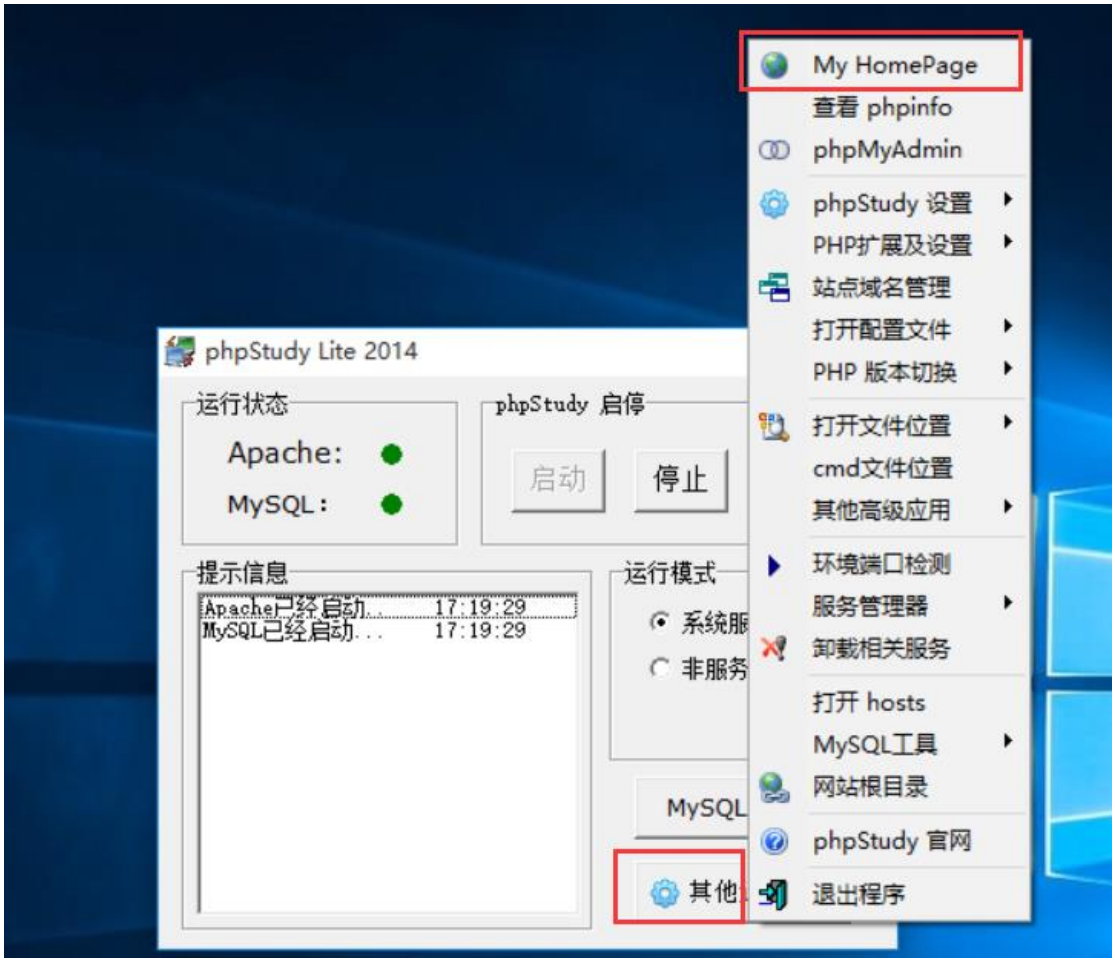


图 5

（5）点击【Session_Hijacking】。如下图 6 所示。

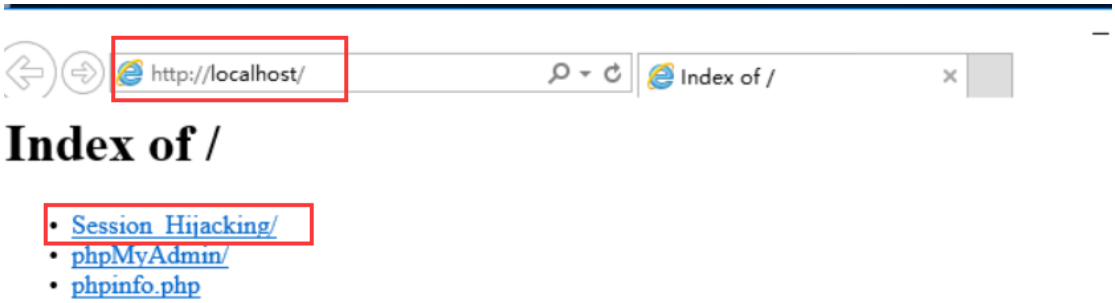


图 6

（6）在 PHP 应用架构中，执行 session start 函数后就会建立一个 session。Session ID 可以由用户自己来指定，也可以由服务器随机产生一个 32 个字符长度的字符串，Session ID 的字符串长度是由 php.ini 设置的。php.ini 在“phpStudy”的“PHPa”文件夹中。

点击【演示 1】。如下图 7 所示。

图 7

（7）session-id.php 文件会显示当前 session 的 id。如下图 8 所示。

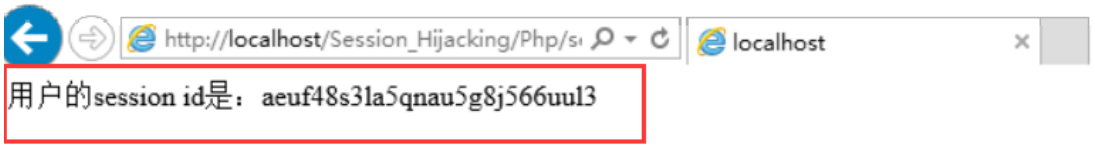


图 8

（8）返回演示页面，点击【攻击 1】。如下图 9 所示。

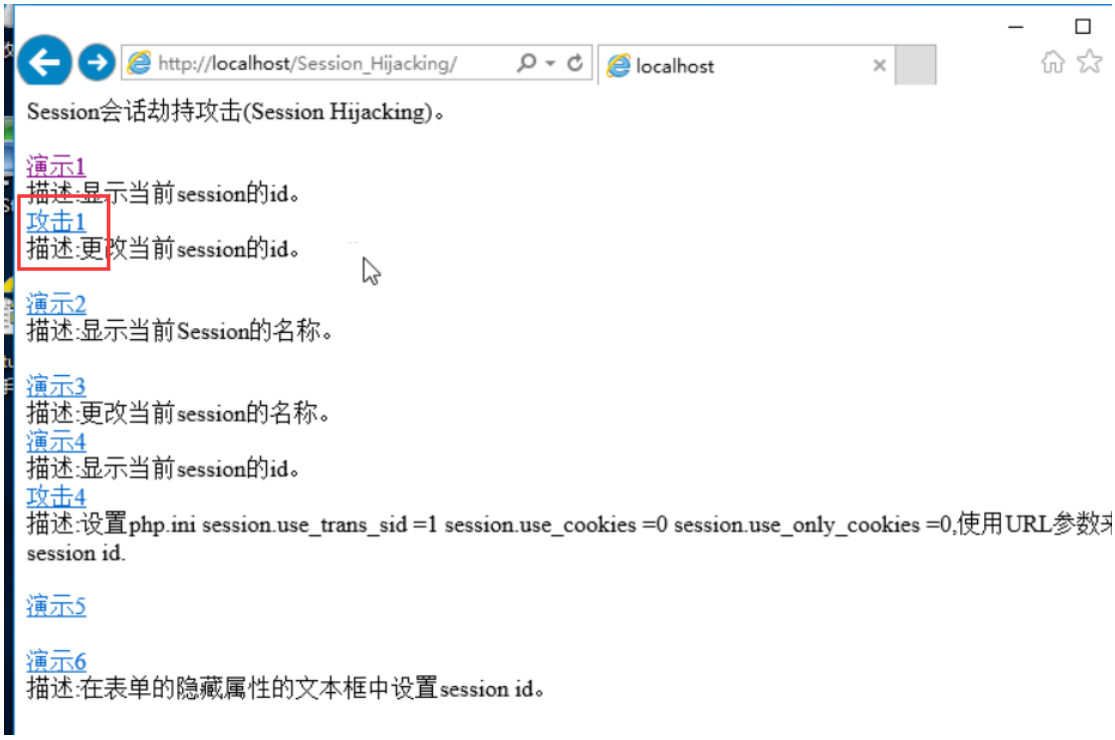


图 9

（9）能够看到当前会话的 ID 被修改。如下图 10 所示。

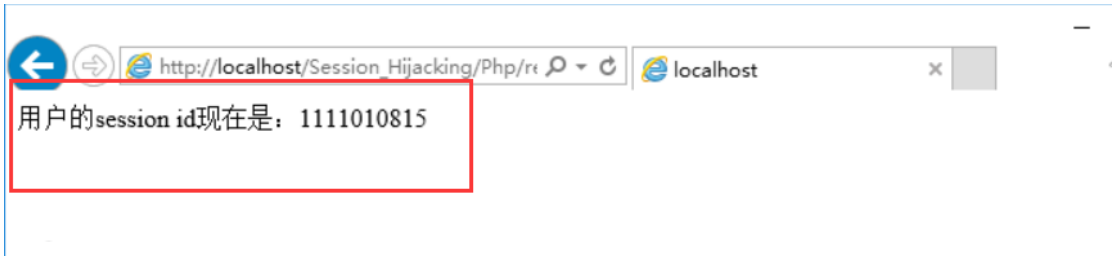


图 10

（10）Session 的名称在 php.ini 设置文件中，默认是 PHPSESSID。Session 的名称可以由用户自己来指定，亦可以不指定而使用默认值。

返回演示界面，点击【演示 2】。如下图 11 所示。

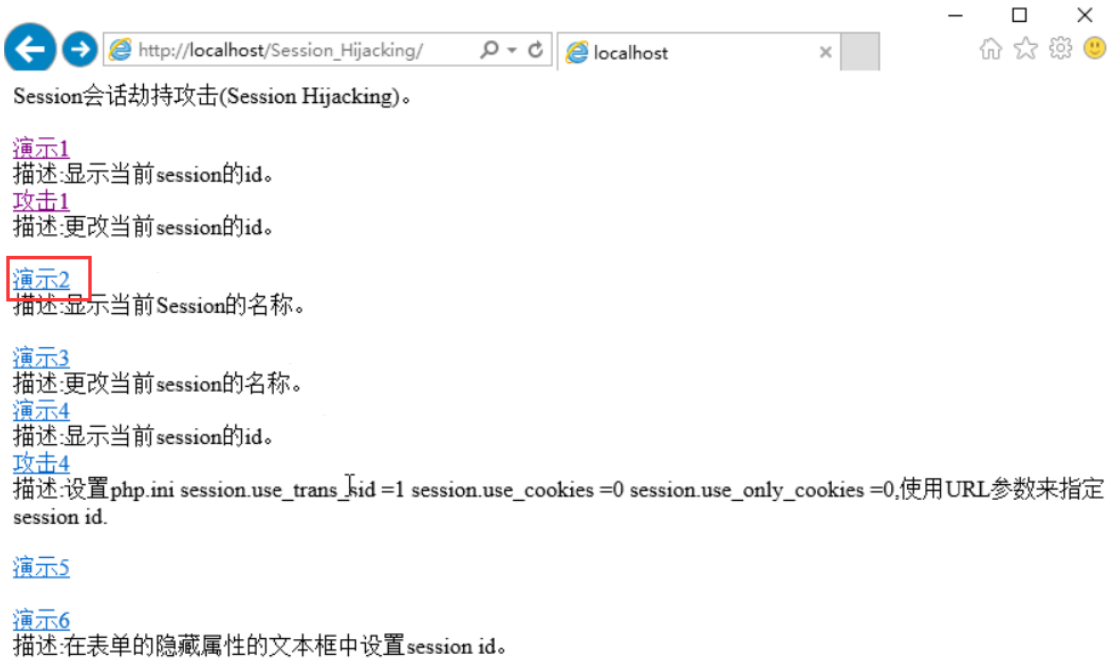


图 11

（11）页面会显示当前的 Session Name。如下图 12 所示。

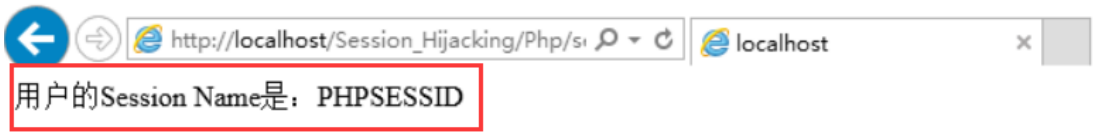


图 12

（12）Session 的名称只能由字母或数字组成，而且必须简短易懂。在每次送出 HTTP 请求时，session 的名称会重新设置为默认值 PHPSESSID。因此要更改 session 的名称时，必须在每次发送 HTTP 请求时都要调用 session_name 函数。返回演示界面，点击【演示 3】，观察结果。如下图 13 和图 14 所示。

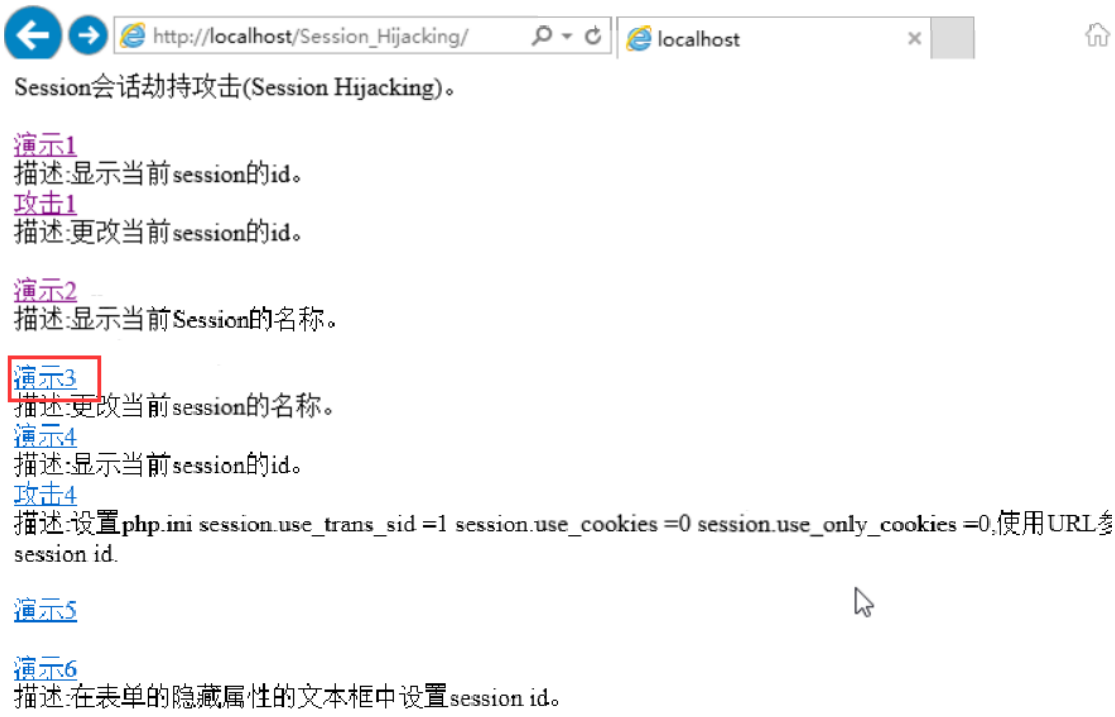


图 13

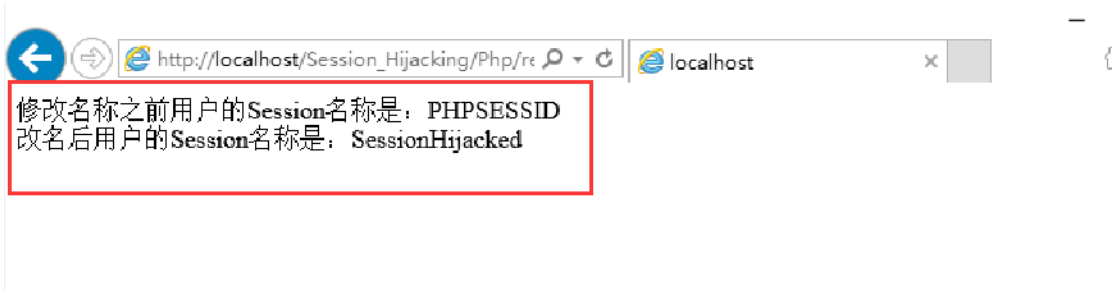


图 14

（13）实验完毕，关闭所有窗口和虚拟机。

五【实验总结】

通过本次实验，明白了 Session 的重要性，了解了会话劫持的原理、步骤以及攻击方式。

思考：

1、如何防范会话劫持攻击？

答：

1、更改 Session 名称。PHP 中 Session 的默认名称是 PHPSESSID，此变量会保存在 Cookie 中，如果攻击者不分析站点，就不能猜到 Session 名称，阻挡部分攻击。

2、关闭透明化 Session ID。透明化 Session ID 指当浏览器中的 Http 请求没有使用 Cookie 来存放 Session ID 时，Session ID 则使用 URL 来传递。

3、 设置 HttpOnly。通过设置 Cookie 的 HttpOnly 为 true，可以防止客户端脚本访问这个 Cookie，从而有效的防止 XSS 攻击。

4、 关闭所有 phpinfo 类 dump request 信息的页面。

5、验证 HTTP 头部信息