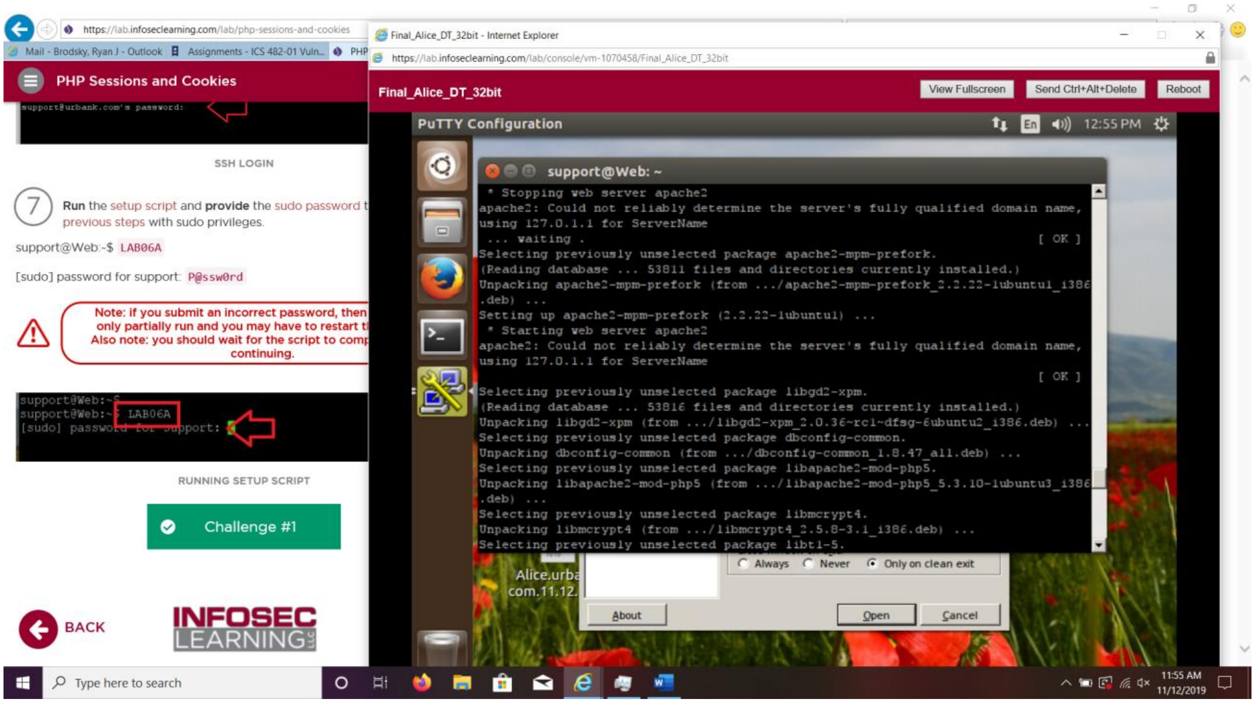
Ryan Brodsky

ICS 482

11/12/2019

InfoSec Lab: PHP Sessions and Cookies


https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions and Cookies
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reboot
PuTTY Configuration
12:55 PM
BACK
INFOSEC LEARNING
Type here to search
11:55 AM
11/12/2019

```
support@urbank.com's password:
```

SSH LOGIN

7 **Run** the setup script and **provide** the sudo password t
previous steps with sudo privileges.

support@Web:~$ `LAB06A`

[sudo] password for support: `P@ssw0rd`

Note: if you submit an incorrect password, then
only partially run and you may have to restart t
Also note: you should wait for the script to comp
continuing.

```
support@Web:~$
support@Web:~$ LAB06A
[sudo] password for support:
```

RUNNING SETUP SCRIPT

Challenge #1

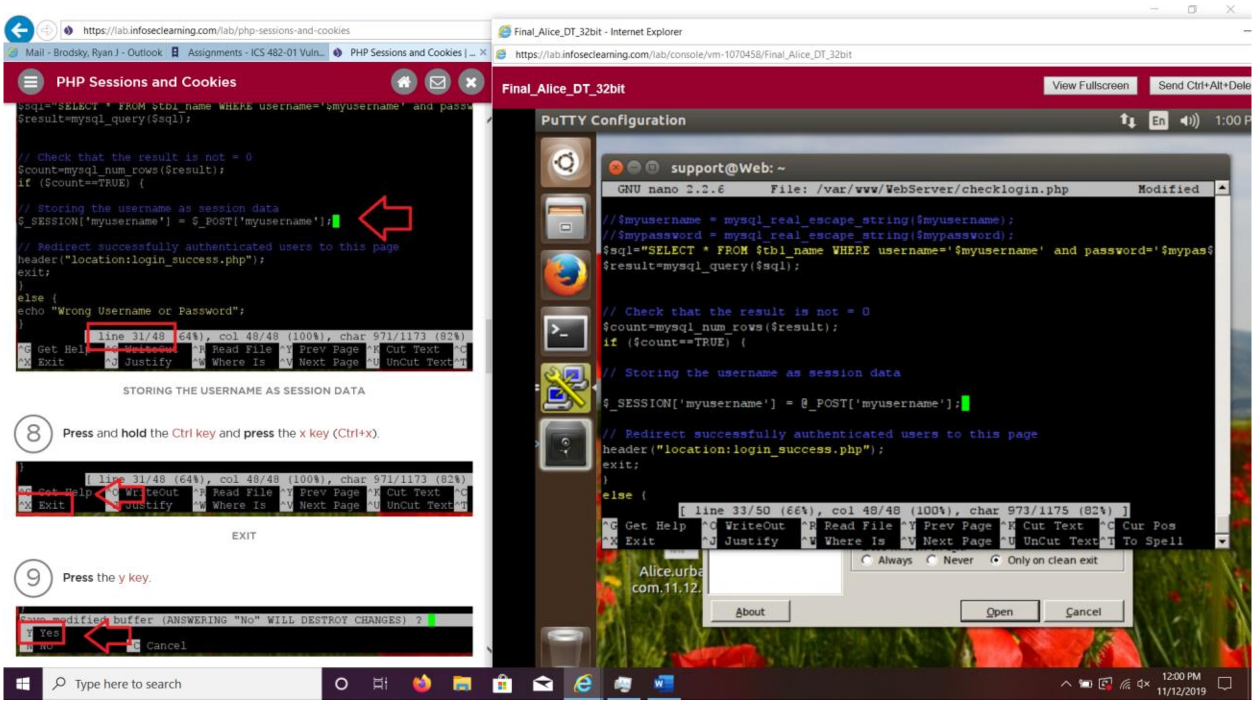
support@Web: ~

```
 * Stopping web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
 ... waiting .                                                           [ OK ]
Selecting previously unselected package apache2-mpm-prefork.
(Reading database ... 53811 files and directories currently installed.)
Unpacking apache2-mpm-prefork (from .../apache2-mpm-prefork_2.2.22-1ubuntu1_i386
.deb) ...
Setting up apache2-mpm-prefork (2.2.22-1ubuntu1) ...
 * Starting web server apache2
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
                                                                         [ OK ]
Selecting previously unselected package libgd2-xpm.
(Reading database ... 53816 files and directories currently installed.)
Unpacking libgd2-xpm (from .../libgd2-xpm_2.0.36~rc1~dfsg-6ubuntu2_i386.deb) ...
Selecting previously unselected package dbconfig-common.
Unpacking dbconfig-common (from .../dbconfig-common_1.8.47_all.deb) ...
Selecting previously unselected package libapache2-mod-php5.
Unpacking libapache2-mod-php5 (from .../libapache2-mod-php5_5.3.10-1ubuntu3_i386
.deb) ...
Selecting previously unselected package libmcrypt4.
Unpacking libmcrypt4 (from .../libmcrypt4_2.5.8-3.1_i386.deb) ...
Selecting previously unselected package libt1-5.
```

○ Always ○ Never ● Only on clean exit

Alice.urba
com.11.12.

About Open Cancel


https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions and Cookies | ...
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Dele
PuTTY Configuration
1:00 P
Type here to search
12:00 PM
11/12/2019

PHP Sessions and Cookies

```
$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and passw
$result=mysql_query($sql);


// Check that the result is not = 0
$count=mysql_num_rows($result);
if ($count==TRUE) {

// Storing the username as session data
$_SESSION['myusername'] = $_POST['myusername'];

// Redirect successfully authenticated users to this page
header("location:login_success.php");
exit;
}
else {
echo "Wrong Username or Password";
}
            [ line 31/48 (64%), col 48/48 (100%), char 971/1173 (82%)
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T
```

STORING THE USERNAME AS SESSION DATA

8 **Press** and **hold** the Ctrl key and **press** the x key (Ctrl+x).

```
}
            [ line 31/48 (64%), col 48/48 (100%), char 971/1173 (82%)
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T
```

EXIT

9 **Press** the y key.

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

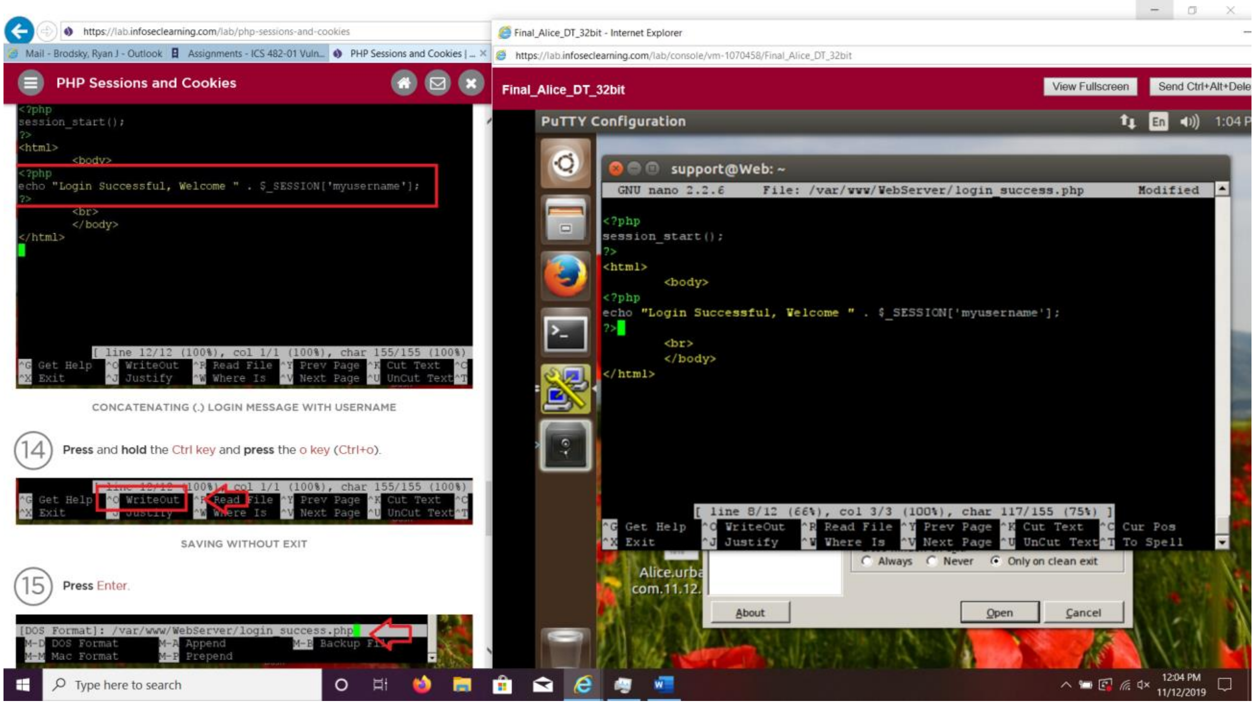
support@Web: ~

```
  GNU nano 2.2.6        File: /var/www/WebServer/checklogin.php          Modified

//$myusername = mysql_real_escape_string($myusername);
//$mypassword = mysql_real_escape_string($mypassword);
$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypas$
$result=mysql_query($sql);


// Check that the result is not = 0
$count=mysql_num_rows($result);
if ($count==TRUE) {

// Storing the username as session data

$_SESSION['myusername'] = @_POST['myusername'];

// Redirect successfully authenticated users to this page
header("location:login_success.php");
exit;
}
else {
          [ line 33/50 (66%), col 48/48 (100%), char 973/1175 (82%) ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```

○ Always ○ Never ● Only on clean exit

Alice.urba
com.11.12.

About Open Cancel



https://lab.infoseclearning.com/lab/php-sessions-and-cookies

Mail - Brodsky, Ryan J - Outlook | Assignments - ICS 482-01 Vuln... | PHP Sessions and Cookies | ...

PHP Sessions and Cookies

```
<?php
session_start();
?>
<html>
        <body>
<?php
echo "Login Successful, Welcome " . $_SESSION['myusername'];
?>
        <br>
        </body>
</html>

                    [ line 12/12 (100%), col 1/1 (100%), char 155/155 (100%) ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T
```

CONCATENATING (.) LOGIN MESSAGE WITH USERNAME

(14) **Press** and **hold** the Ctrl key and **press** the o key (Ctrl+o).

```
                    [ line 12/12 (100%), col 1/1 (100%), char 155/155 (100%) ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T
```

SAVING WITHOUT EXIT

(15) **Press** Enter.

```
[DOS Format]: /var/www/WebServer/login_success.php
 M-D DOS Format          M-A Append            M-B Backup Fi
 M-M Mac Format          M-P Prepend
```

Final_Alice_DT_32bit - Internet Explorer

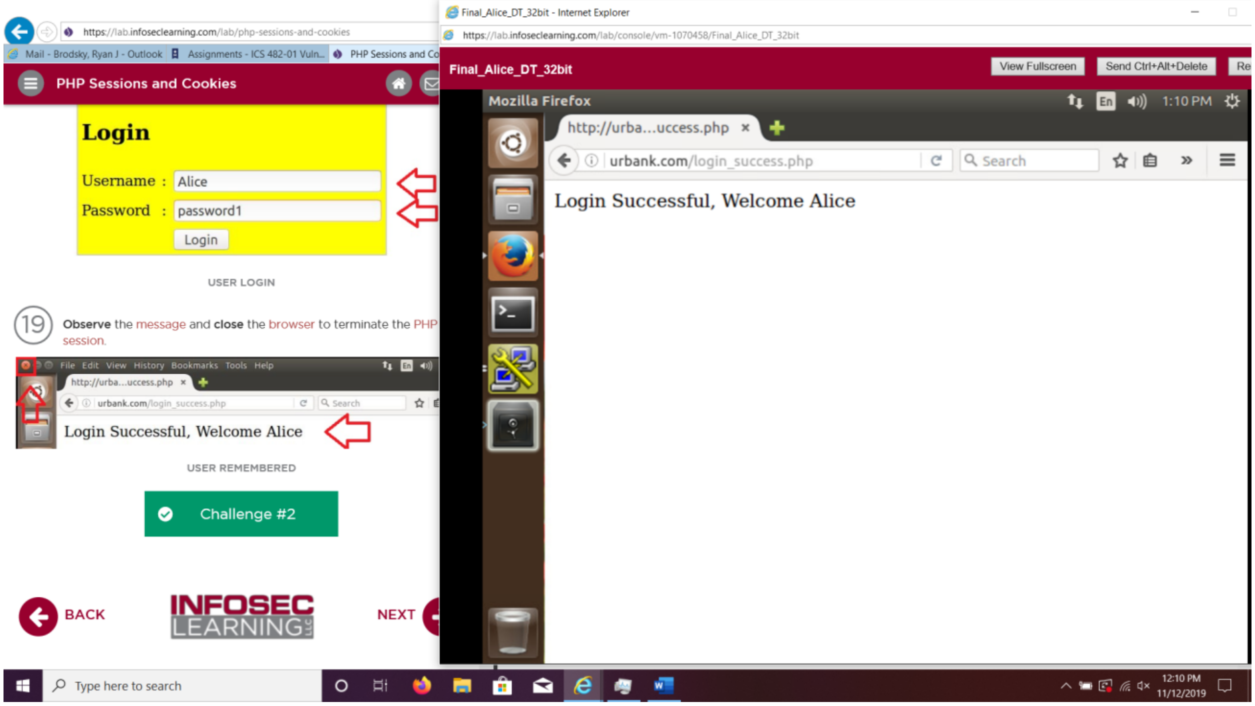
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit

Final_Alice_DT_32bit

PuTTY Configuration

support@Web: ~

```
  GNU nano 2.2.6        File: /var/www/WebServer/login_success.php          Modified

<?php
session_start();
?>
<html>
        <body>
<?php
echo "Login Successful, Welcome " . $_SESSION['myusername'];
?>
        <br>
        </body>
</html>

                  [ line 8/12 (66%), col 3/3 (100%), char 117/155 (75%) ]
^G Get Help   ^O WriteOut   ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit       ^J Justify    ^W Where Is   ^V Next Page  ^U UnCut Text ^T To Spell
```



https://lab.infoseclearning.com/lab/php-sessions-and-cookies

Mail - Brodsky, Ryan J - Outlook | Assignments - ICS 482-01 Vuln... | PHP Sessions and Co

PHP Sessions and Cookies

Login

Username : Alice

Password : password1

Login

USER LOGIN

(19) **Observe** the message and **close** the browser to terminate the PHP session.

http://urba...uccess.php

urbank.com/login_success.php

Login Successful, Welcome Alice

USER REMEMBERED

✓ Challenge #2

BACK

NEXT

Final_Alice_DT_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit

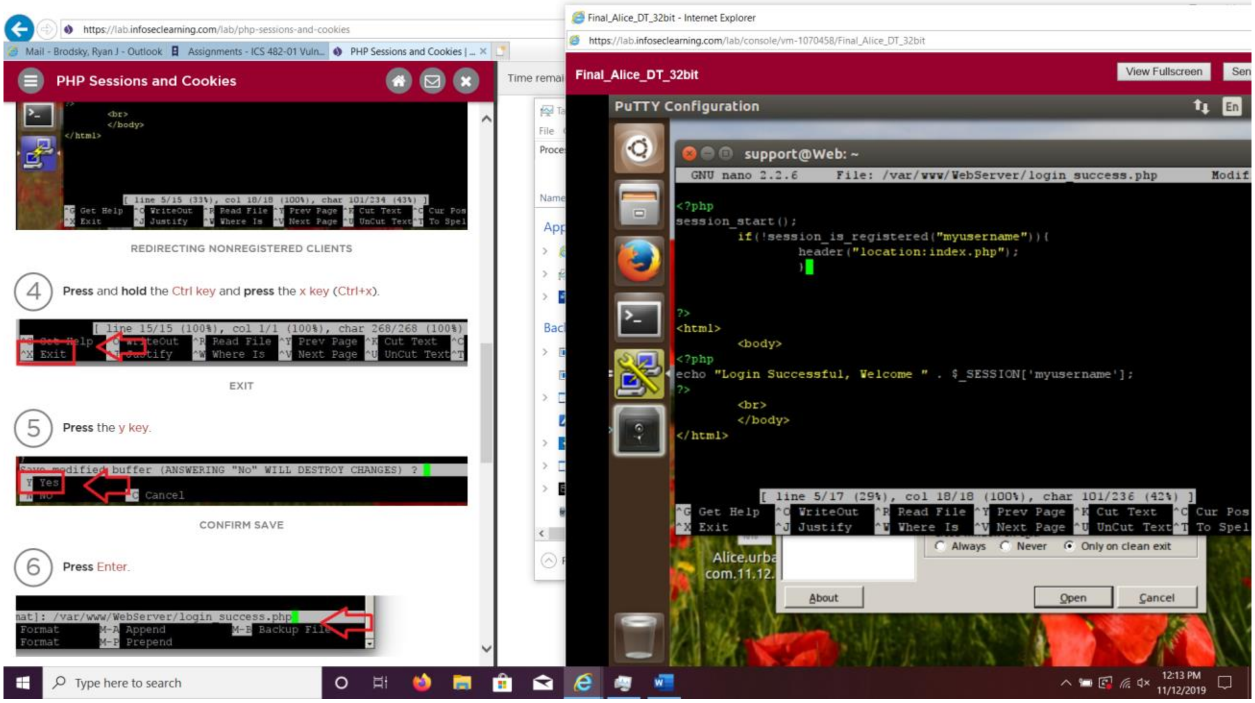
Final_Alice_DT_32bit

Mozilla Firefox

http://urba...uccess.php

urbank.com/login_success.php

Login Successful, Welcome Alice


https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions and Cookies | ...
PHP Sessions and Cookies
Time remai
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
PuTTY Configuration
support@Web: ~
Type here to search
12:13 PM
11/12/2019

```
               <br>
        </body>
</html>

                [ line 5/15 (33%), col 18/18 (100%), char 101/234 (43%) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spel
```

REDIRECTING NONREGISTERED CLIENTS

4 Press and hold the Ctrl key and press the x key (Ctrl+x).

```
             [ line 15/15 (100%), col 1/1 (100%), char 268/268 (100%)
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T
```

EXIT

5 Press the y key.

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

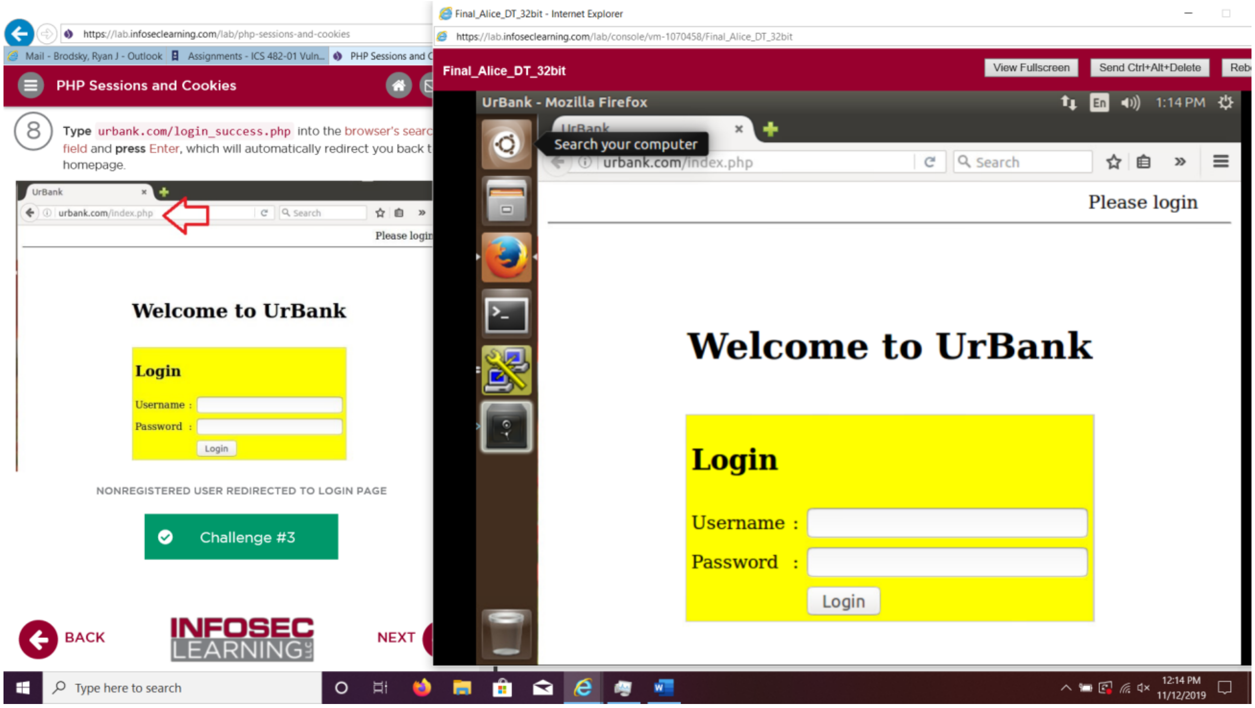
CONFIRM SAVE

6 Press Enter.

```
mat]: /var/www/WebServer/login_success.php
 Format          M-A Append         M-B Backup File
 Format          M-P Prepend
```

```
  GNU nano 2.2.6        File: /var/www/WebServer/login_success.php       Modif

<?php
session_start();
        if(!session_is_registered("myusername")){
                header("location:index.php");
                }


?>
<html>
        <body>
<?php
echo "Login Successful, Welcome " . $_SESSION['myusername'];
?>
        <br>
        </body>
</html>

            [ line 5/17 (29%), col 18/18 (100%), char 101/236 (42%) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spel
```

○ Always ○ Never ● Only on clean exit


https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions and C
PHP Sessions and Cookies
Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt+Delete
Reb
UrBank - Mozilla Firefox
1:14 PM
UrBank
Search your computer
urbank.com/index.php
Search
Type here to search
12:14 PM
11/12/2019

8 Type `urbank.com/login_success.php` into the browser's searc field and press Enter, which will automatically redirect you back t homepage.

Please login

Welcome to UrBank

Login

Username :

Password :

Login

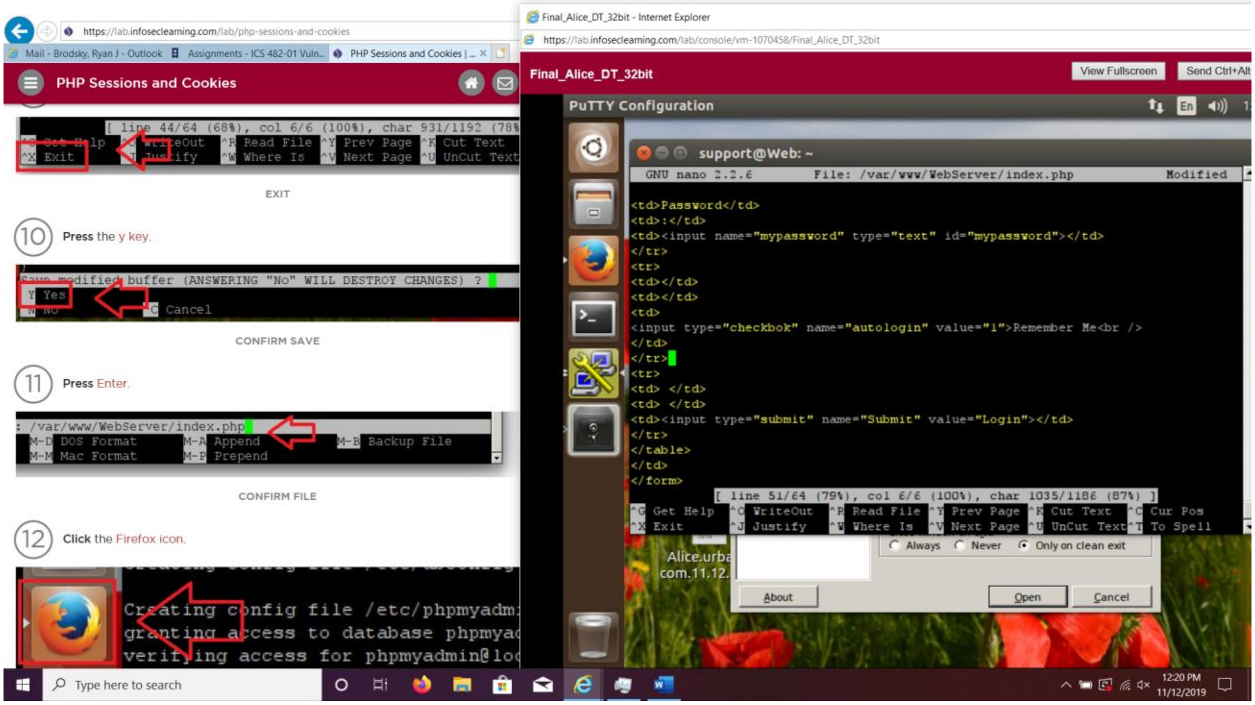
NONREGISTERED USER REDIRECTED TO LOGIN PAGE

Challenge #3

BACK

INFOSEC LEARNING

NEXT



https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions and Cookies | ...
PHP Sessions and Cookies

```
[ line 44/64 (68%), col 6/6 (100%), char 931/1192 (78%
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text
```

EXIT

10 **Press** the y key.

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

CONFIRM SAVE

11 **Press** Enter.

```
: /var/www/WebServer/index.php
M-D DOS Format          M-A Append          M-B Backup File
M-M Mac Format          M-P Prepend
```

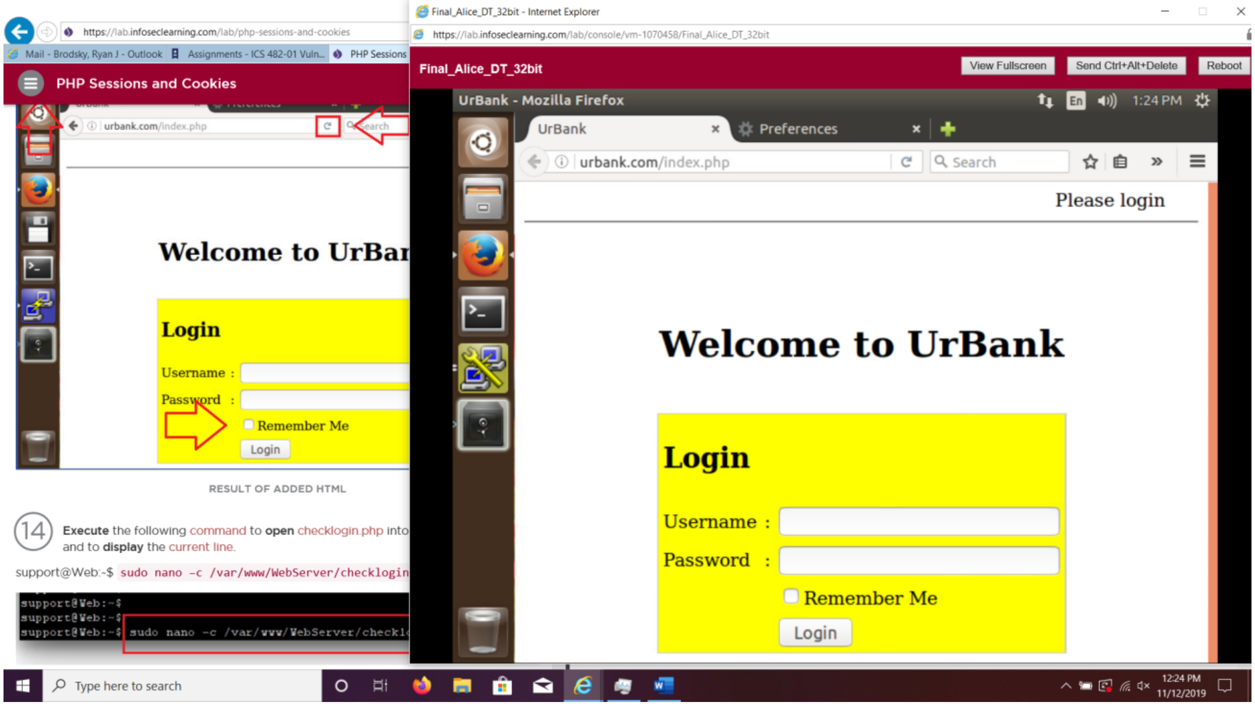
CONFIRM FILE

12 **Click** the Firefox icon.

```
Creating config file /etc/phpmyadm
granting access to database phpmyac
verifying access for phpmyadmin@loc
```

Final_Alice_DT_32bit - Internet Explorer
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit
Final_Alice_DT_32bit
View Fullscreen
Send Ctrl+Alt
PuTTY Configuration
support@Web: ~

```
  GNU nano 2.2.6         File: /var/www/WebServer/index.php              Modified

<td>Password</td>
<td>:</td>
<td><input name="mypassword" type="text" id="mypassword"></td>
</tr>
<tr>
<td></td>
<td></td>
<td>
<input type="checkbok" name="autologin" value="1">Remember Me<br />
</td>
</tr>
<tr>
<td> </td>
<td> </td>
<td><input type="submit" name="Submit" value="Login"></td>
</tr>
</table>
</td>
</form>
                    [ line 51/64 (79%), col 6/6 (100%), char 1035/1186 (87%) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```



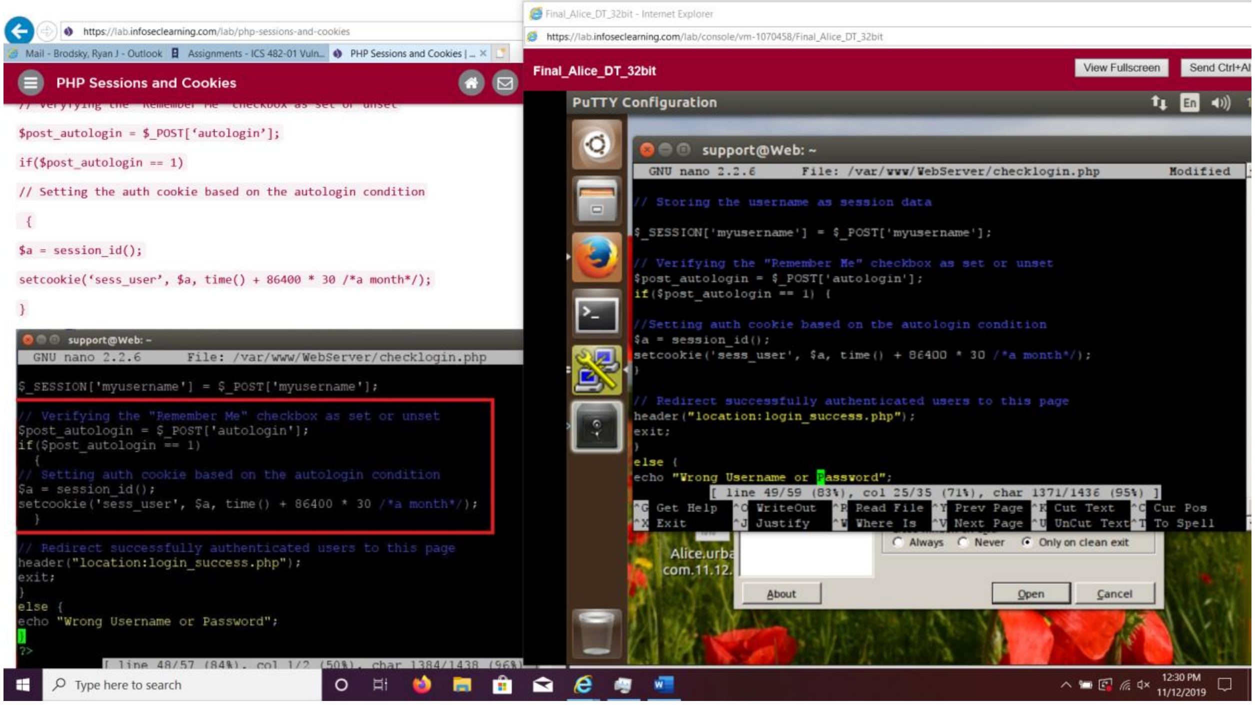
https://lab.infoseclearning.com/lab/php-sessions-and-cookies
Mail - Brodsky, Ryan J - Outlook
Assignments - ICS 482-01 Vuln...
PHP Sessions
PHP Sessions and Cookies
urbank.com/index.php
Search
Welcome to UrBar
Login
Username :
Password :
□ Remember Me
Login

RESULT OF ADDED HTML

14 **Execute** the following command to **open** checklogin.php into
and to **display** the current line.

support@Web:~$ `sudo nano -c /var/www/WebServer/checklogin`

```
support@Web:~$
support@Web:~$
support@Web:~$ sudo nano -c /var/www/WebServer/checkl
```



https://lab.infoseclearning.com/lab/php-sessions-and-cookies

Mail - Brodsky, Ryan J - Outlook | Assignments - ICS 482-01 Vuln... | PHP Sessions and Cookies | ...

PHP Sessions and Cookies

```
// Veryfying the "Remember Me" checkbox as set or unset
$post_autologin = $_POST[‘autologin’];
if($post_autologin == 1)
// Setting the auth cookie based on the autologin condition
 {
$a = session_id();
setcookie(‘sess_user’, $a, time() + 86400 * 30 /*a month*/);
}
```

```
support@Web: ~
  GNU nano 2.2.6        File: /var/www/WebServer/checklogin.php

$_SESSION['myusername'] = $_POST['myusername'];

// Verifying the "Remember Me" checkbox as set or unset
$post_autologin = $_POST['autologin'];
if($post_autologin == 1)
  {
// Setting auth cookie based on the autologin condition
$a = session_id();
setcookie('sess_user', $a, time() + 86400 * 30 /*a month*/);
  }

// Redirect successfully authenticated users to this page
header("location:login_success.php");
exit;
}
else {
echo "Wrong Username or Password";
}
?>
         [ line 48/57 (84%), col 1/2 (50%), char 1384/1438 (96%) ]
```

Final_Alice_DT_32bit - Internet Explorer

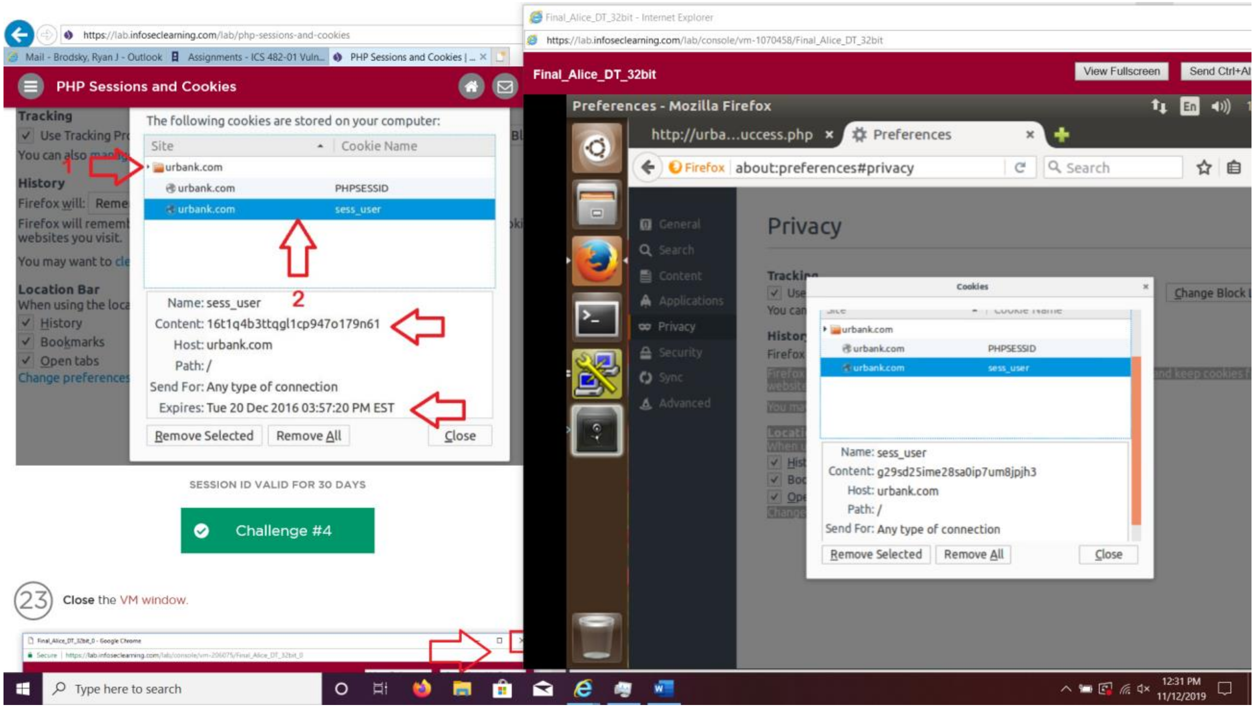
https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit

Final_Alice_DT_32bit

PuTTY Configuration

```
support@Web: ~
  GNU nano 2.2.6        File: /var/www/WebServer/checklogin.php        Modified

// Storing the username as session data

$_SESSION['myusername'] = $_POST['myusername'];

// Verifying the "Remember Me" checkbox as set or unset
$post_autologin = $_POST['autologin'];
if($post_autologin == 1) {

//Setting auth cookie based on the autologin condition
$a = session_id();
setcookie('sess_user', $a, time() + 86400 * 30 /*a month*/);
}

// Redirect successfully authenticated users to this page
header("location:login_success.php");
exit;
}
else {
echo "Wrong Username or Password";
                [ line 49/59 (83%), col 25/35 (71%), char 1371/1436 (95%) ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

○ Always ○ Never ● Only on clean exit



https://lab.infoseclearning.com/lab/php-sessions-and-cookies

Mail - Brodsky, Ryan J - Outlook | Assignments - ICS 482-01 Vuln... | PHP Sessions and Cookies | ...

PHP Sessions and Cookies

Tracking

☑ Use Tracking Pr

You can also mana

History

Firefox will: Reme

Firefox will rememb websites you visit.

You may want to cle

Location Bar

When using the loca

☑ History

☑ Bookmarks

☑ Open tabs

Change preferences

The following cookies are stored on your computer:

Site	Cookie Name
urbank.com	
urbank.com	PHPSESSID
urbank.com	sess_user

Name: sess_user

Content: 16t1q4b3ttqgl1cp947o179n61

Host: urbank.com

Path: /

Send For: Any type of connection

Expires: Tue 20 Dec 2016 03:57:20 PM EST

SESSION ID VALID FOR 30 DAYS

Challenge #4

23 **Close** the VM window.

Final_Alice_DT_32bit_0 - Google Chrome

Secure | https://lab.infoseclearning.com/lab/console/vm-206075/Final_Alice_DT_32bit_0

Final_Alice_DT_32bit - Internet Explorer

https://lab.infoseclearning.com/lab/console/vm-1070458/Final_Alice_DT_32bit

Final_Alice_DT_32bit

Preferences - Mozilla Firefox

http://urba...uccess.php | Preferences

about:preferences#privacy

Privacy

Cookies

Site	Cookie Name
urbank.com	
urbank.com	PHPSESSID
urbank.com	sess_user

Name: sess_user

Content: g29sd25ime28sa0ip7um8jpjh3

Host: urbank.com

Path: /

Send For: Any type of connection