SQL and XSS Exercises

Michele La Manna
Dept. of Information Engineering
University of Pisa
michele.lamanna@phd.unipi.it

Version: 2022-05-18

CYBERWISER.EU

What is CYBERWISER.eu

UNIVERSITÀ DI PISA

1. The CYBERWISER.eu cyber range platform has been developed in the scope of the CYBERWISER.eu European Project;

2. The purpose of the CYBERWISER.eu platform is **to form** multidisciplinary and highly skilled **experts** in the **cybersecurity** field;

3. Users can act both as **attacker** and **defender**, in different and highly configurable **scenarios;**

4. A **scenario** is composed by:
   a. A set of **virtual resources** simulating a real network;
   b. The **software** running on such resources.

5. **To each scenario it is possible to associate one or more cyber range exercise**. Users are asked to complete the exercise, by interacting with the virtualized environment, to acquire additional knowledge;

6. The CYBERWISER.eu platform is entirely **web-based.**

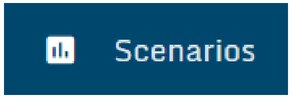
Reach CYBERWISER.eu

1. Power on your device;

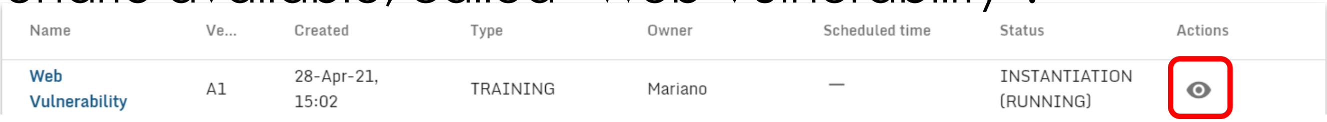
2. Open a browser (suggested: Chrome or FireFox or Safari) and go to the following address: https://cyberrange.unipi.it/

3. Login to the CYBERWISER.eu platform using the credentials which you should have received;

4. In the **left** menu, click on "*Scenarios*":

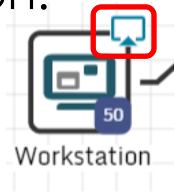


5. You should see a scenario available, called "Web Vulnerability". Click on the "eye":



Name	Ve...	Created	Type	Owner	Scheduled time	Status	Actions
Web Vulnerability	A1	28-Apr-21, 15:02	TRAINING	Mariano	–	INSTANTIATION (RUNNING)	👁

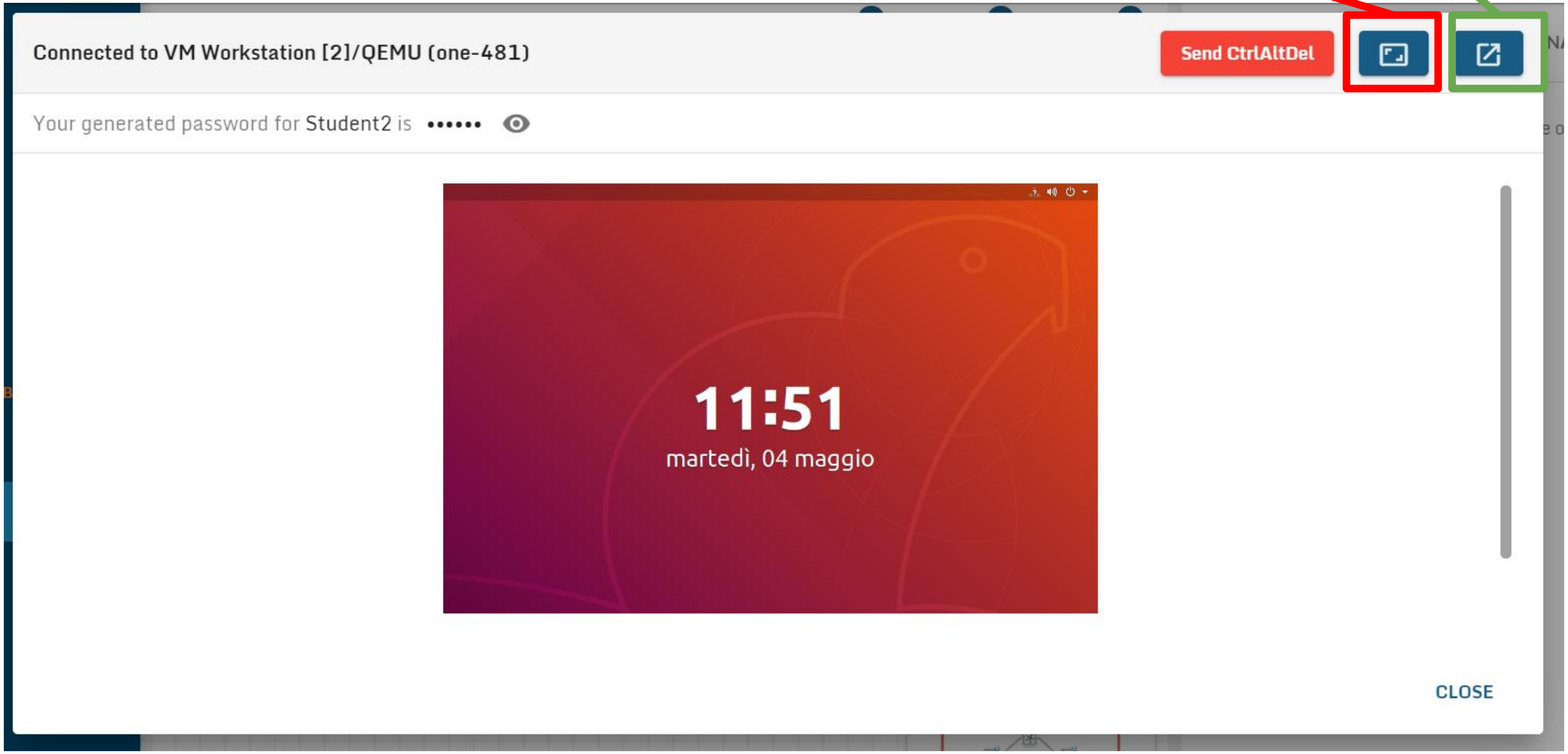
6. You have the right to access the VM called "**Workstation**". You can access it with the little screen icon on the top right the VM icon:



Control screen

Full screen

Open in a new Tab



Connected to VM Workstation [2]/QEMU (one-481)

Your generated password for Student2 is ••••••

BEE-BOX

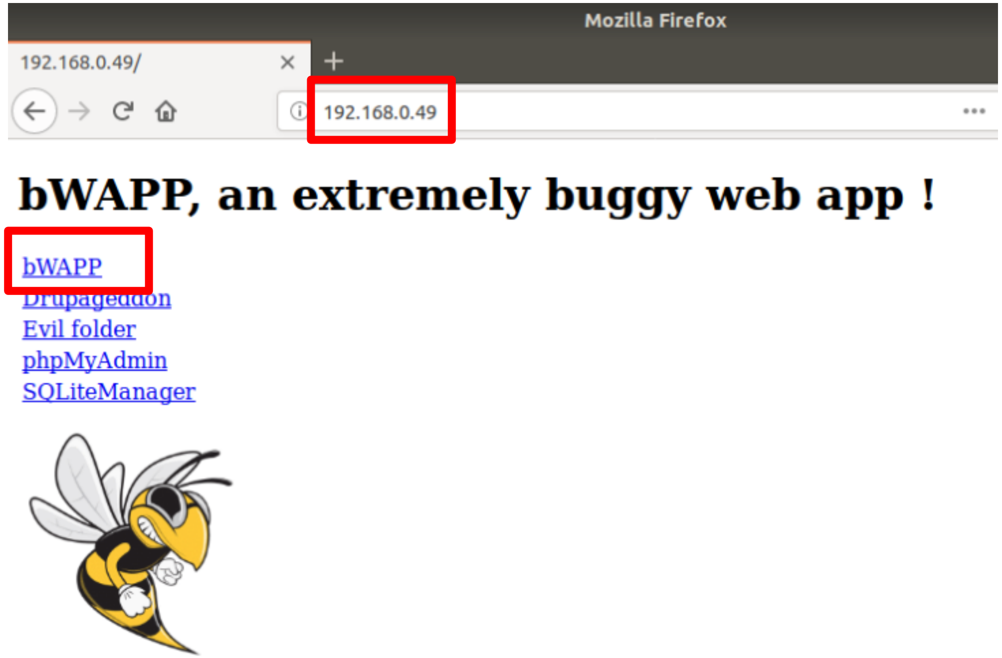
Workstation info

Workstation credentials:
User: student
Pwd: student

Open the browser mozilla, and enter the ip of the server_beebox assigned to you.

You can find the server's IP address inside the csv file containing the student's credentials.

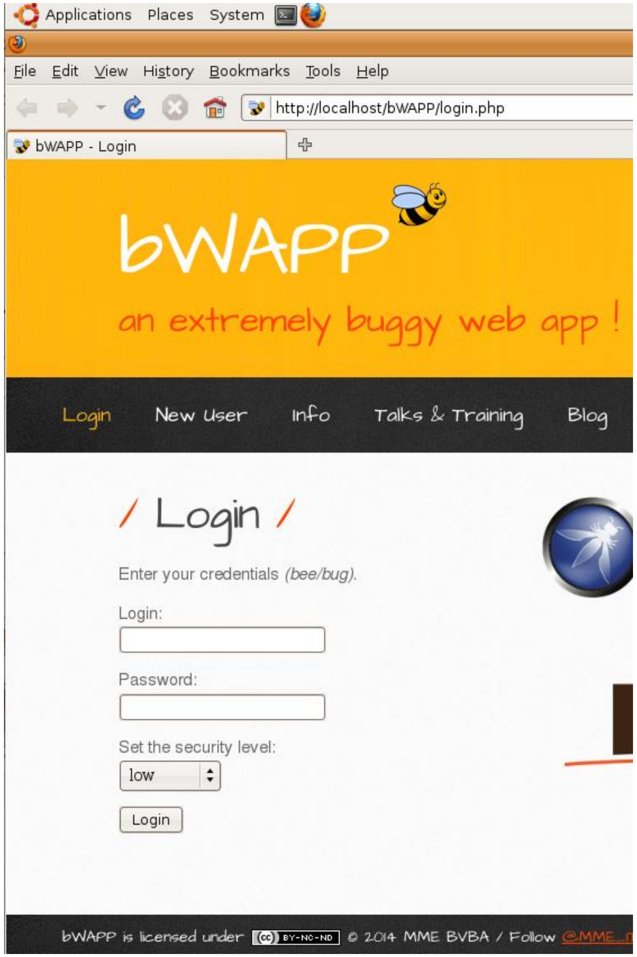
Then, click on bWAPP link.



bWAPP, an extremely buggy web app !

bWAPP
Drupageddon
Evil folder
phpMyAdmin
SQLiteManager

bWAPP homepage


Applications Places System
File Edit View History Bookmarks Tools Help
bWAPP - Login
bWAPP
an extremely buggy web app !
Login New User Info Talks & Training Blog

http://localhost/bWAPP/login.php

/ Login /

Enter your credentials *(bee/bug)*.

Login:

Password:

Set the security level:

low

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_

Server_beebox credentials

Login:

bee

Password:

bug

Press on «Login»

Exercises

UNIVERSITÀ DI PISA

You will be asked to «solve» 3 exercises from the list available on the page you have just logged-in.

To «solve» an exercise constitutes in 2 steps:

1) Successfully Hacking the web APP.
2) Successfully patching the php file behind the broken page.

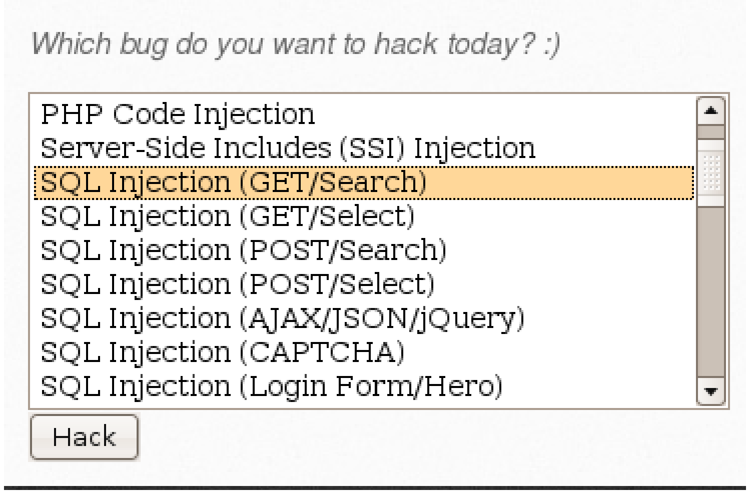
To do the step 2, you must retrieve from the server the «bugged» php file, patch them, upload the patched php on the server and finally restarting apache.

At the end of these slides, you will find some instructions for those tasks.

Once you have restarted apache, you simply test the effectiveness of your patch by trying the same attack that worked in step 1.

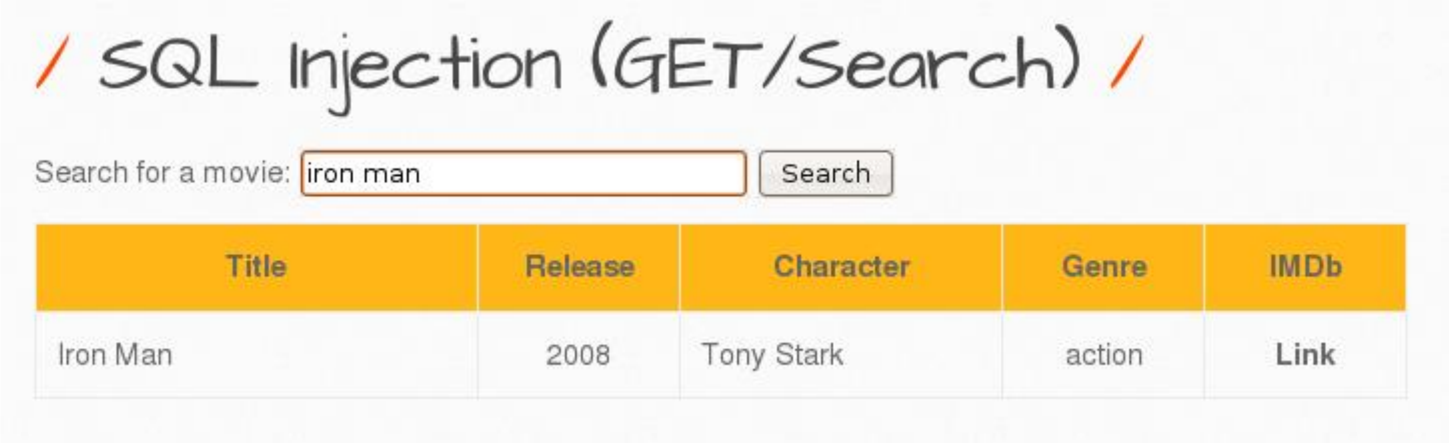
SQL INJECTION

SQL Injection (GET/Search)



Which bug do you want to hack today? :)
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)
SQL Injection (GET/Select)
SQL Injection (POST/Search)
SQL Injection (POST/Select)
SQL Injection (AJAX/JSON/jQuery)
SQL Injection (CAPTCHA)
SQL Injection (Login Form/Hero)
Hack

On the left-side of the page, scroll down a bit and select «SQL Injection (GET/Search)». Click on hack.
You will see a searchbar, try search for the film «iron man».



/ SQL Injection (GET/Search) /

Search for a movie: iron man

Title	Release	Character	Genre	IMDb
Iron Man	2008	Tony Stark	action	Link

SQL Injection (GET/Search)

Inject an SQL string that let you see all the film inside the DB.

Retrieve the server' file

```
sudo scp bee@<server_ip>:/var/www/bWAPP/sqli_1.php
/home/student/Scrivania/
```

Patch the vulnerability, then upload the patched file on the server.

Then restart apache (on the server) with the command

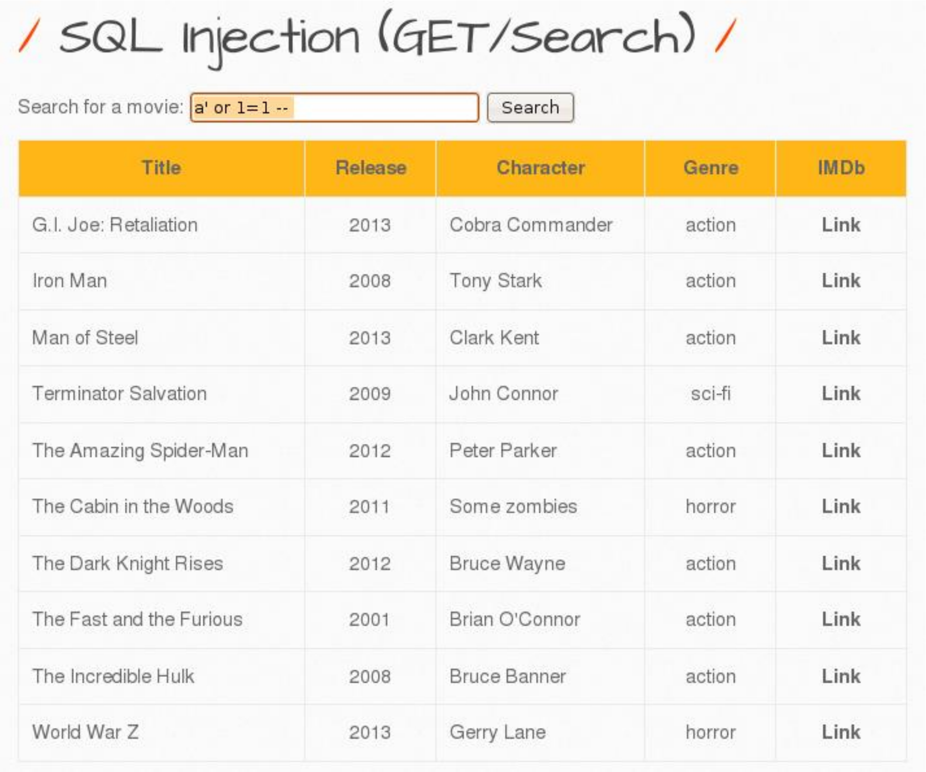
```
sudo /etc/init.d/apache2 restart
```

Try again the attack and test the efficacy of your patch.

Solution: Attack

The attack is a tautology, and we use a comment.

```
a' or 1=1 --
```

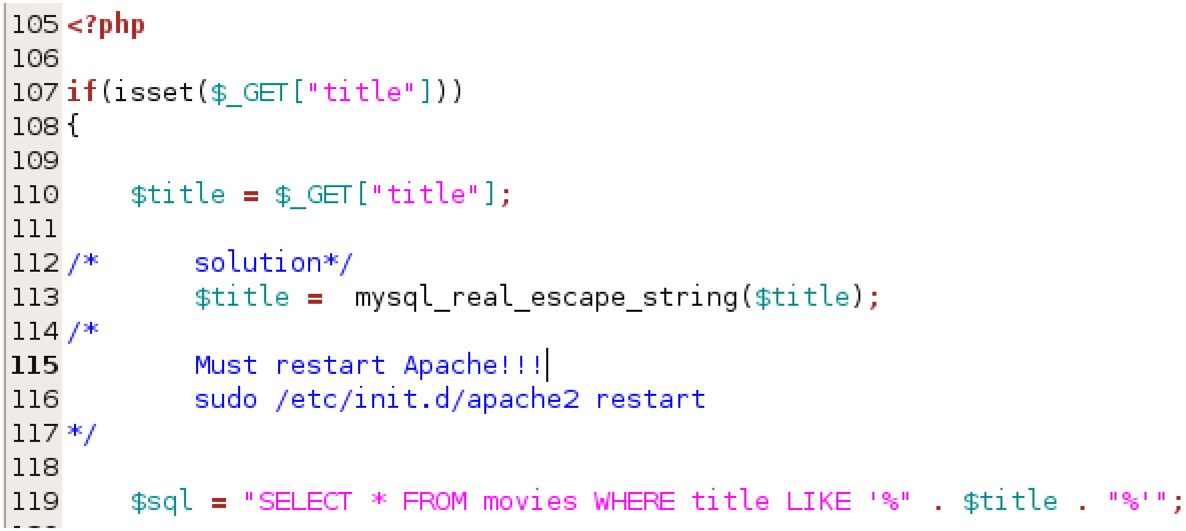


/ SQL Injection (GET/Search) /

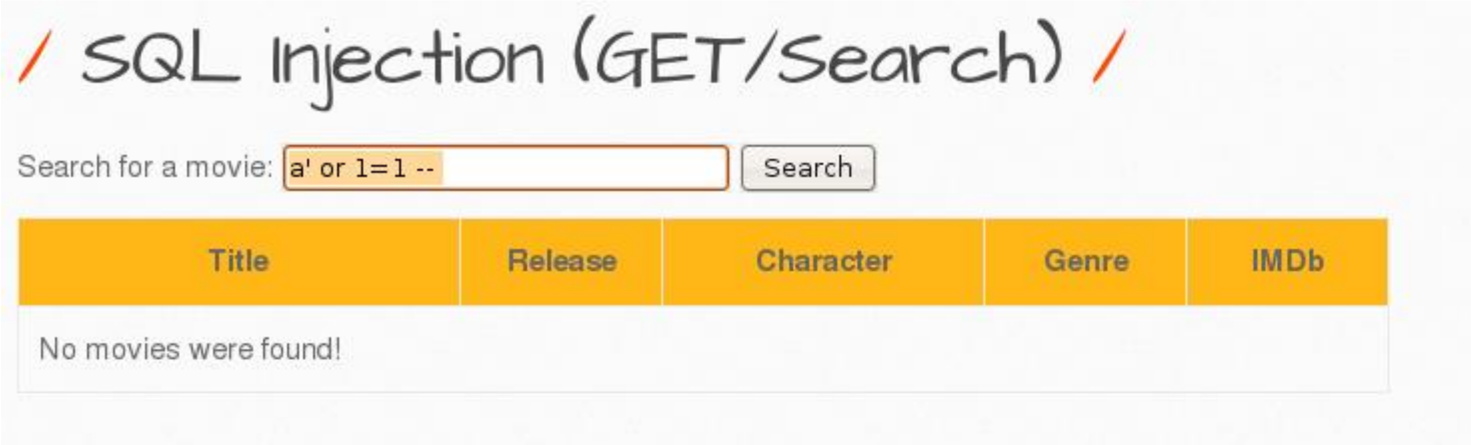
Search for a movie: a' or 1=1 --

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link

Solution: Patch



```
<?php

if(isset($_GET["title"]))
{

    $title = $_GET["title"];

/*      solution*/
        $title =  mysql_real_escape_string($title);
/*
        Must restart Apache!!!
        sudo /etc/init.d/apache2 restart
*/

    $sql = "SELECT * FROM movies WHERE title LIKE '%" . $title . "%'";
```



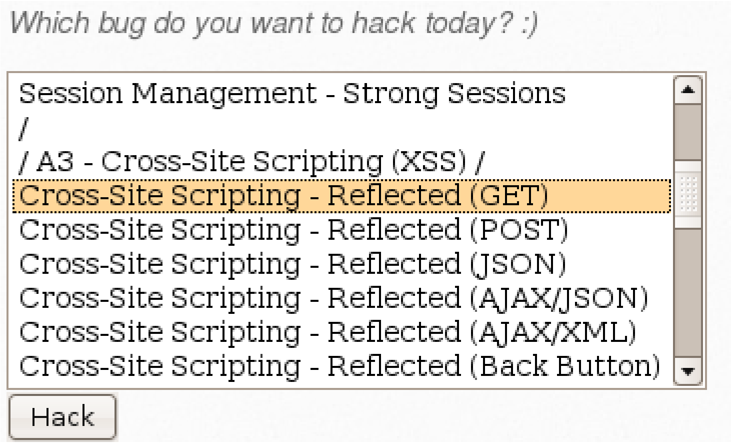
/ SQL Injection (GET/Search) /

Search for a movie: a' or 1=1 --

Title	Release	Character	Genre	IMDb
No movies were found!				

CROSS-SITE-SCRIPTING (XSS) REFLECTED

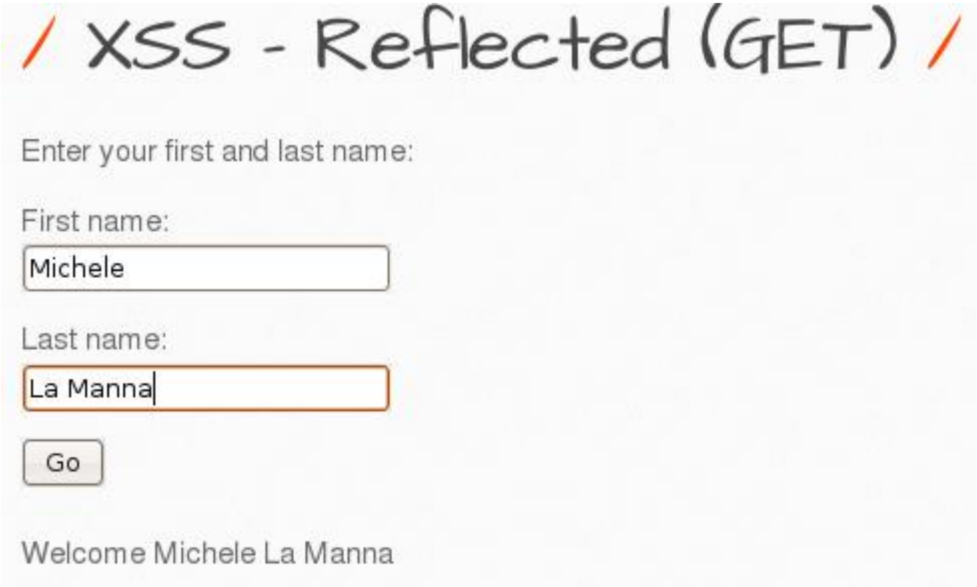
XSS - reflected (GET)



Which bug do you want to hack today? :)

Session Management - Strong Sessions
/
/ A3 - Cross-Site Scripting (XSS) /
Cross-Site Scripting - Reflected (GET)
Cross-Site Scripting - Reflected (POST)
Cross-Site Scripting - Reflected (JSON)
Cross-Site Scripting - Reflected (AJAX/JSON)
Cross-Site Scripting - Reflected (AJAX/XML)
Cross-Site Scripting - Reflected (Back Button)

This time, scroll down a little more and select «Cross-Site-Scripting – Reflected (GET)». Click on hack.
You will see two forms, try insert yours first and last names.



/ XSS - Reflected (GET) /

Enter your first and last name:

First name: Michele

Last name: La Manna

Welcome Michele La Manna

XSS - reflected (GET)

Inject a script that makes a pop-up appear.

Retrieve the server' file

```
sudo scp bee@<server_ip>:/var/www/bWAPP/xss_get.php
/home/student/Scrivania/
```

Patch the vulnerability, then upload the patched file on the server.

Then restart apache with the command

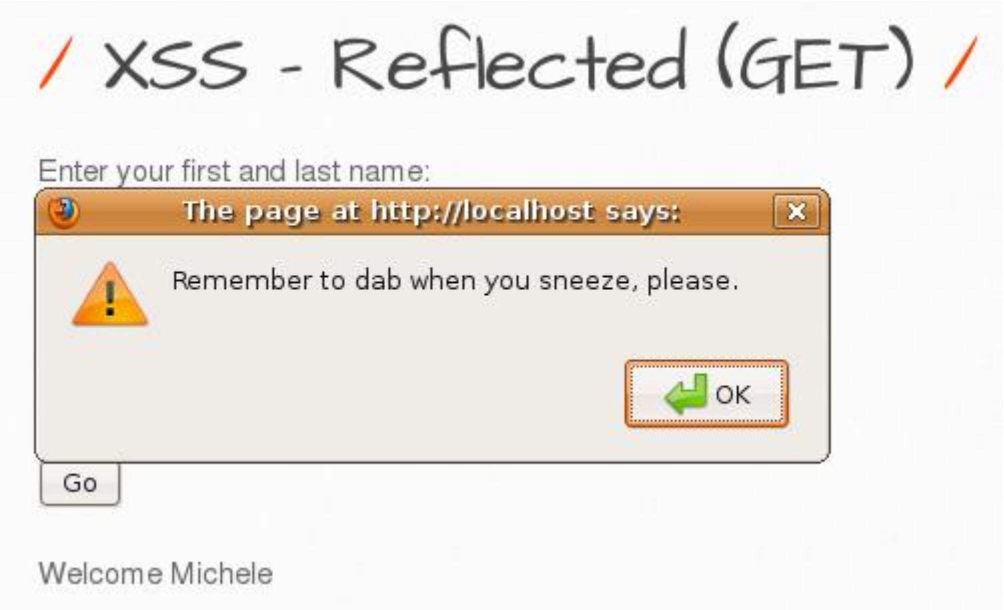
```
sudo /etc/init.d/apache2 restart
```

Try again the attack and test the efficacy of your patch.

Solution: Attack

A simple pop-up can appear using the “alert” instruction.

```
Michele<script>alert(“Remember to dab when you sneeze, please.”)</script>
```



/ XSS - Reflected (GET) /

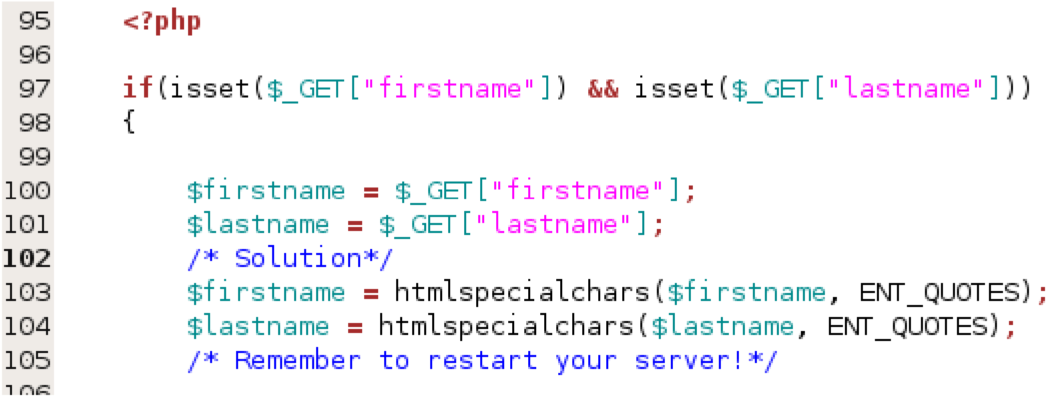
Enter your first and last name:

The page at http://localhost says:

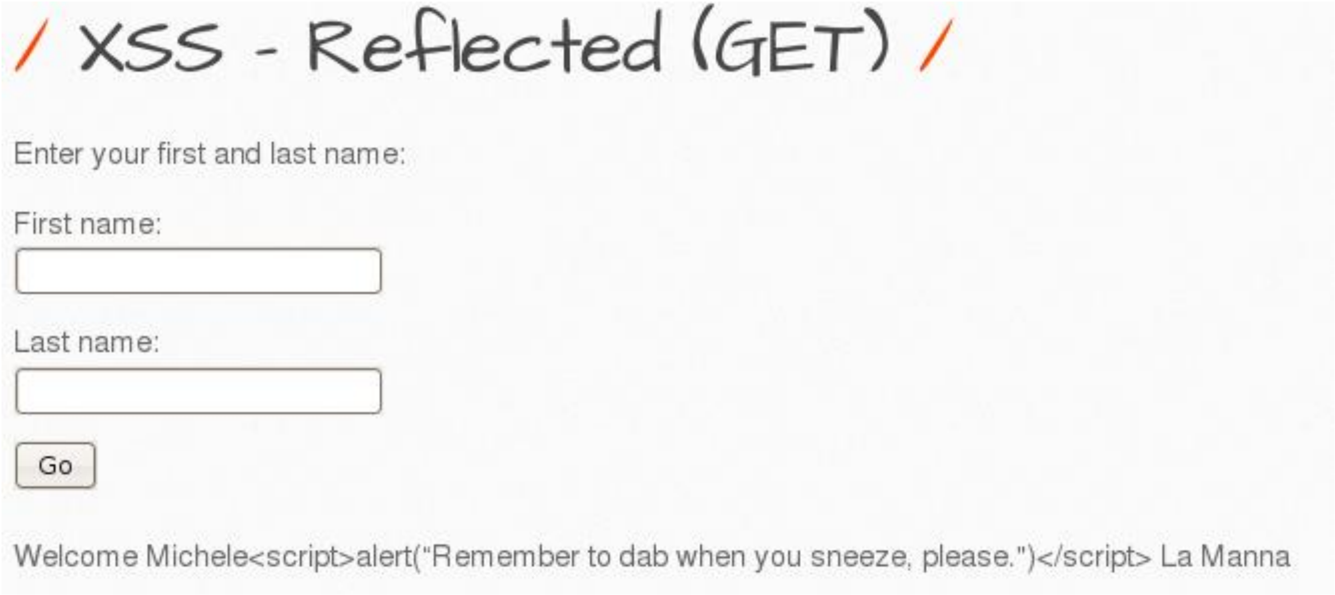
Remember to dab when you sneeze, please.

Welcome Michele

Solution: Patch



```
<?php

if(isset($_GET["firstname"]) && isset($_GET["lastname"]))
{

    $firstname = $_GET["firstname"];
    $lastname = $_GET["lastname"];
    /* Solution*/
    $firstname = htmlspecialchars($firstname, ENT_QUOTES);
    $lastname = htmlspecialchars($lastname, ENT_QUOTES);
    /* Remember to restart your server!*/
```



/ XSS - Reflected (GET) /

Enter your first and last name:

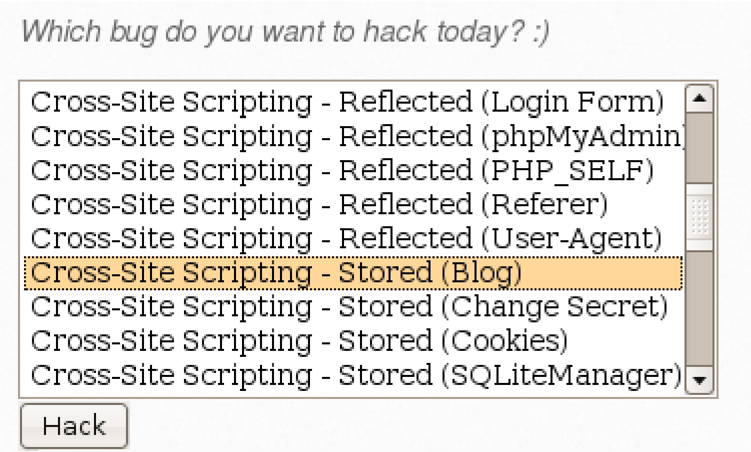
First name:

Last name:

Welcome Michele<script>alert("Remember to dab when you sneeze, please.")</script> La Manna

CROSS-SITE-SCRIPTING (XSS) STORED

XSS - stored (Blog)

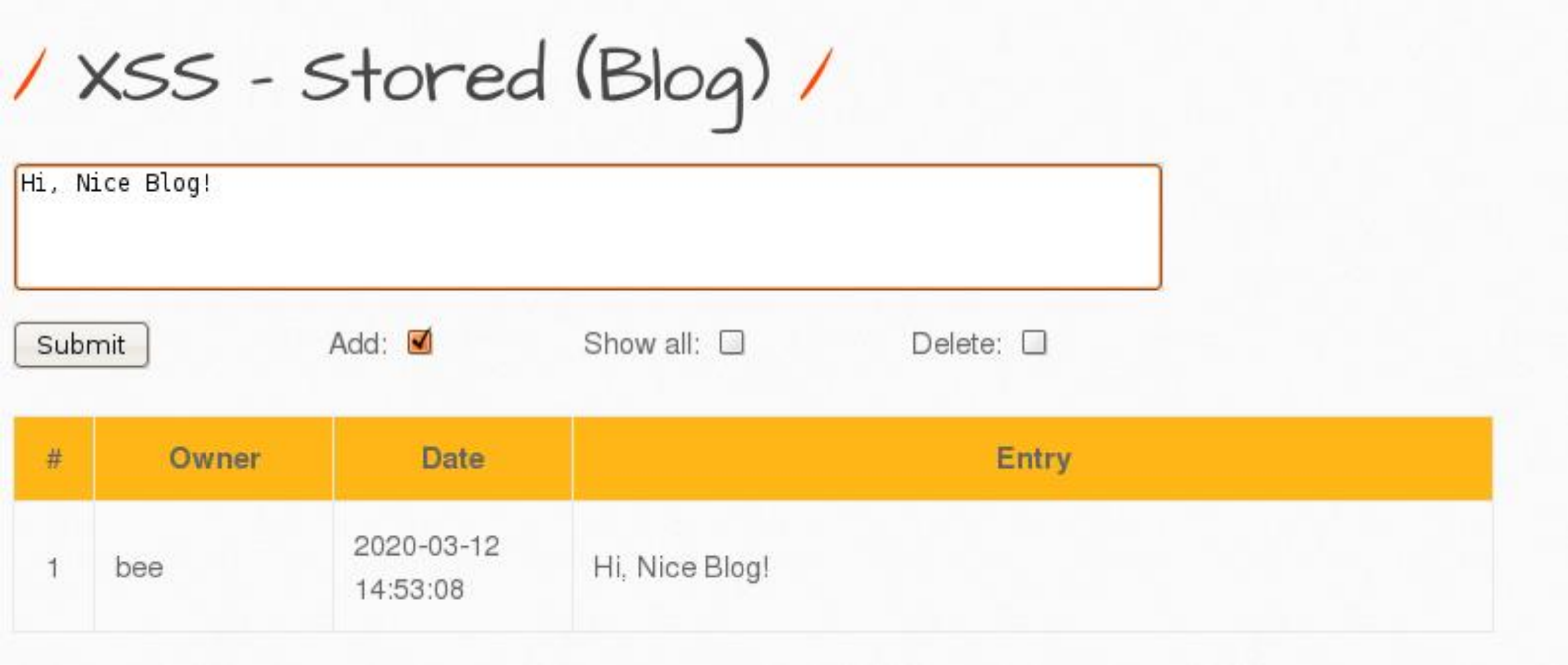


Which bug do you want to hack today? :)

- Cross-Site Scripting - Reflected (Login Form)
- Cross-Site Scripting - Reflected (phpMyAdmin)
- Cross-Site Scripting - Reflected (PHP_SELF)
- Cross-Site Scripting - Reflected (Referer)
- Cross-Site Scripting - Reflected (User-Agent)
- Cross-Site Scripting - Stored (Blog)
- Cross-Site Scripting - Stored (Change Secret)
- Cross-Site Scripting - Stored (Cookies)
- Cross-Site Scripting - Stored (SQLiteManager)

This time, scroll down a little more and select «Cross-Site-Scripting – Stored (Blog)». Click on hack.

You will see a form, try post a comment on this blog!



/ XSS - Stored (Blog) /

```
Hi, Nice Blog!
```

Add: ☑ Show all: □ Delete: □

#	Owner	Date	Entry
1	bee	2020-03-12 14:53:08	Hi, Nice Blog!

XSS - Store (Blog)

Inject a script that makes a pop-up appear.

Retrieve the server' file

```
sudo scp bee@<server_ip>:/var/www/bWAPP/xss_stored_1.php /home/student/Scrivania/
```

Patch the vulnerability, then upload the patched file on the server.

Then restart apache with the command

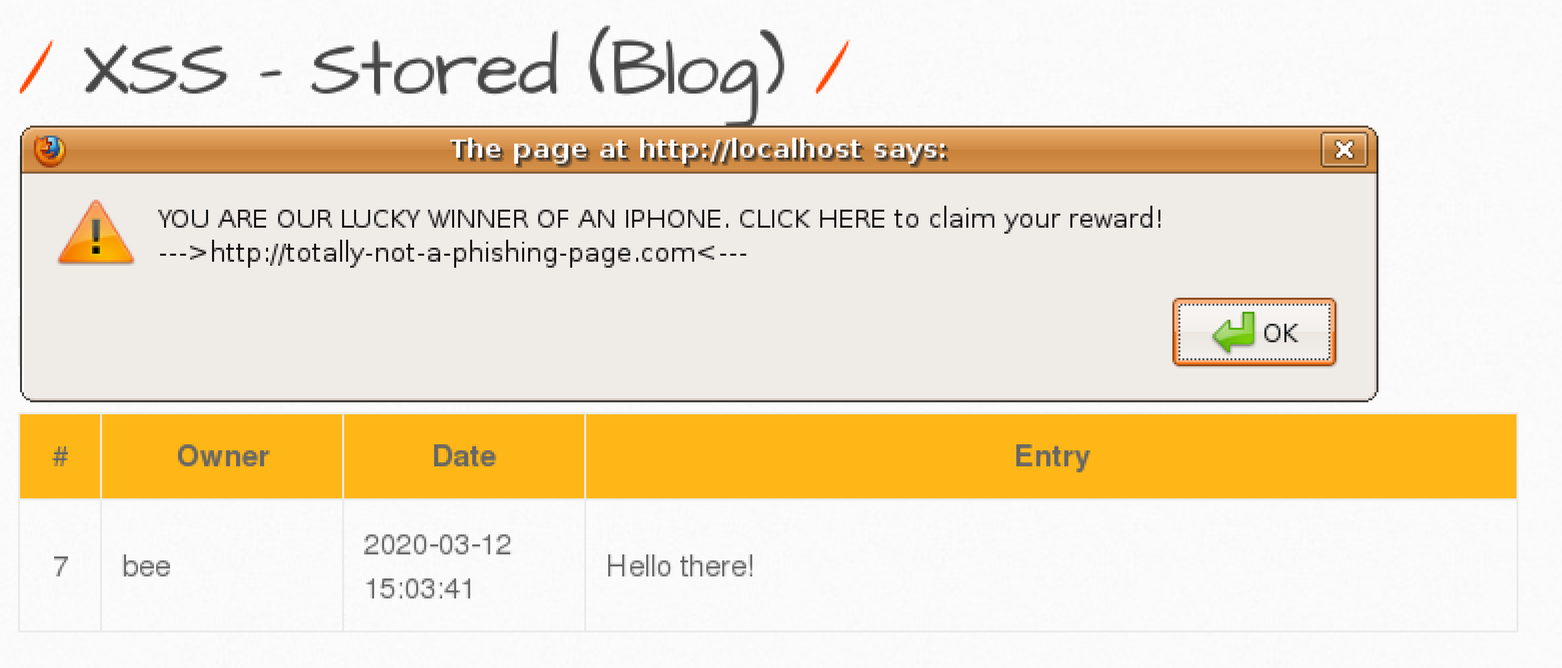
```
sudo /etc/init.d/apache2 restart
```

Try again the attack and test the efficacy of your patch.

Solution: Attack

A simple pop-up can appear using the “alert” instruction.

```
Hello there!<script>alert("YOU ARE OUR LUCKY WINNER OF AN IPHONE. CLICK HERE to claim your reward! --->http://totally-not-a-phishing-page.com<---")</script>
```



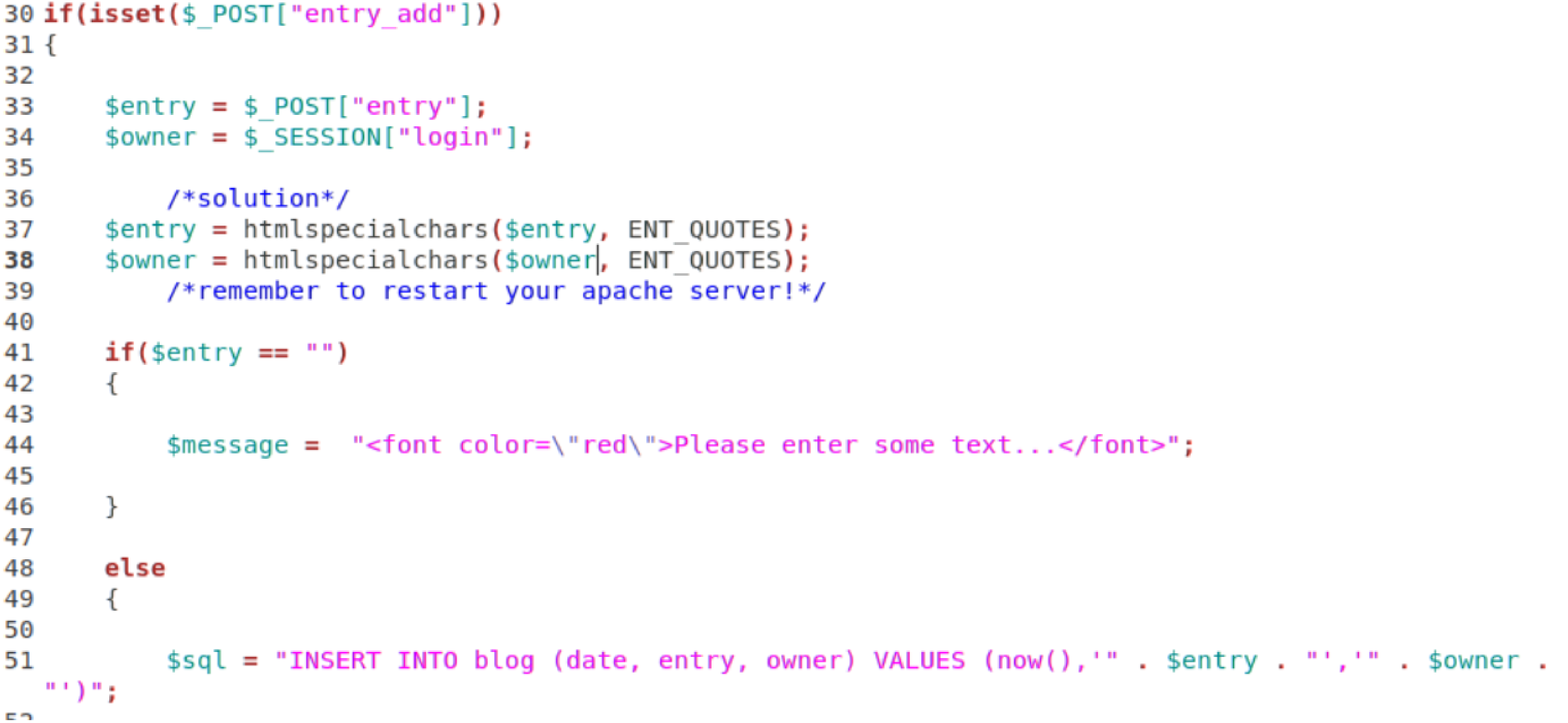
/ XSS - Stored (Blog) /

The page at http://localhost says:

YOU ARE OUR LUCKY WINNER OF AN IPHONE. CLICK HERE to claim your reward!
--->http://totally-not-a-phishing-page.com<---

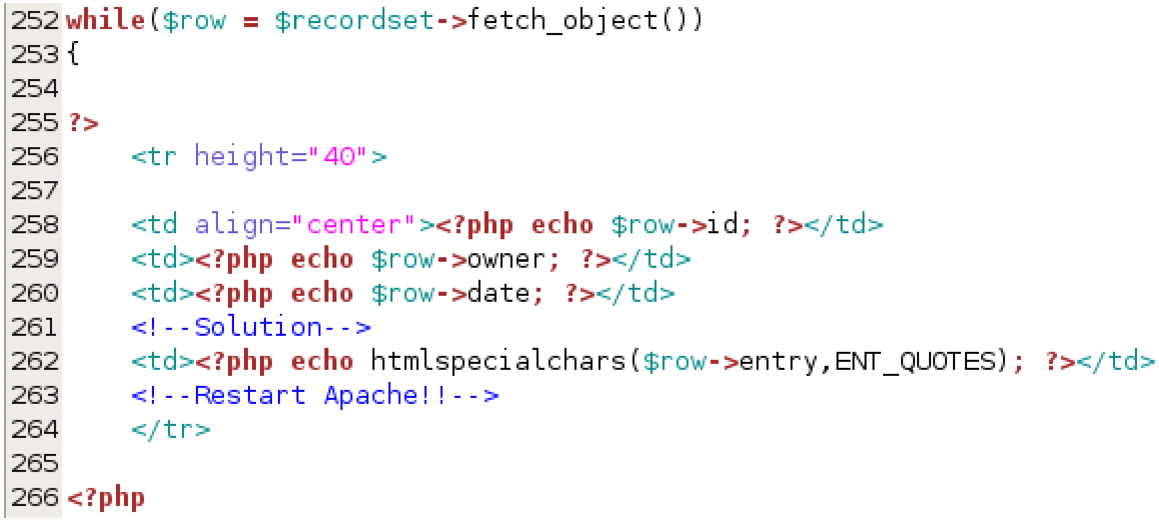
#	Owner	Date	Entry
7	bee	2020-03-12 15:03:41	Hello there!

Solution: Sanitize input

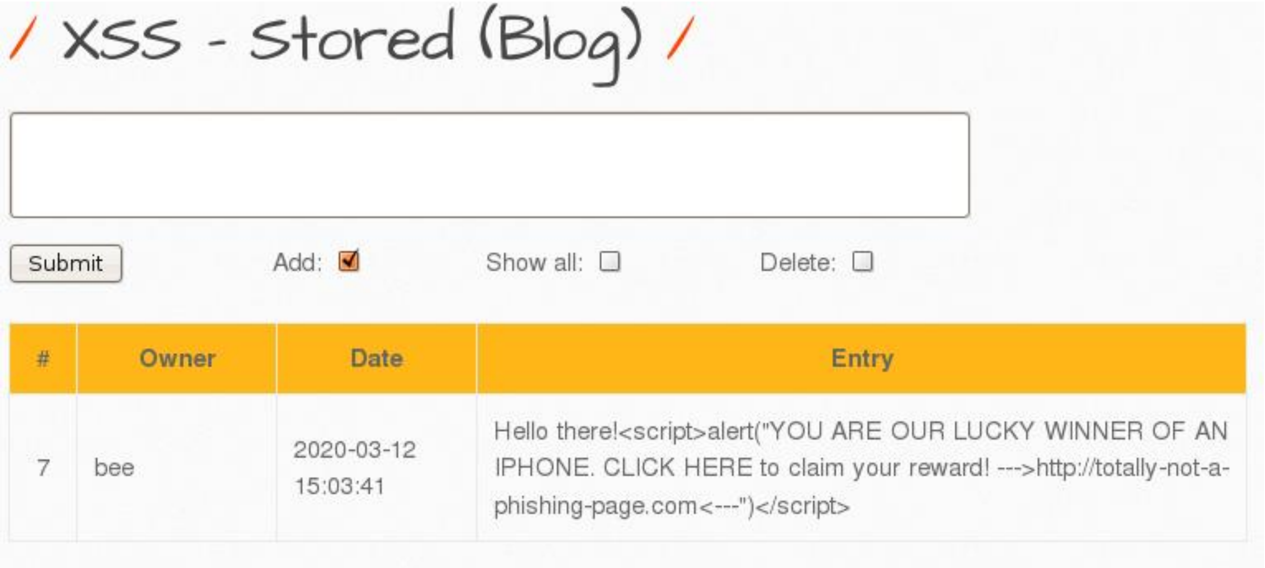


```php
if(isset($_POST["entry_add"]))
{

    $entry = $_POST["entry"];
    $owner = $_SESSION["login"];

        /*solution*/
    $entry = htmlspecialchars($entry, ENT_QUOTES);
    $owner = htmlspecialchars($owner, ENT_QUOTES);
        /*remember to restart your apache server!*/

    if($entry == "")
    {

        $message =  "<font color=\"red\">Please enter some text...</font>";

    }

    else
    {

        $sql = "INSERT INTO blog (date, entry, owner) VALUES (now(),'" . $entry . "','" . $owner . "')";
```

Solution: Sanitize output



```
while($row = $recordset->fetch_object())
{

?>
    <tr height="40">

    <td align="center"><?php echo $row->id; ?></td>
    <td><?php echo $row->owner; ?></td>
    <td><?php echo $row->date; ?></td>
    <!--Solution-->
    <td><?php echo htmlspecialchars($row->entry,ENT_QUOTES); ?></td>
    <!--Restart Apache!!-->
    </tr>

<?php
```



/ XSS - Stored (Blog) /

Add: ☑ Show all: ☐ Delete: ☐

#	Owner	Date	Entry
7	bee	2020-03-12 15:03:41	Hello there!<script>alert("YOU ARE OUR LUCKY WINNER OF AN IPHONE. CLICK HERE to claim your reward! --->http://totally-not-a-phishing-page.com<---")</script>

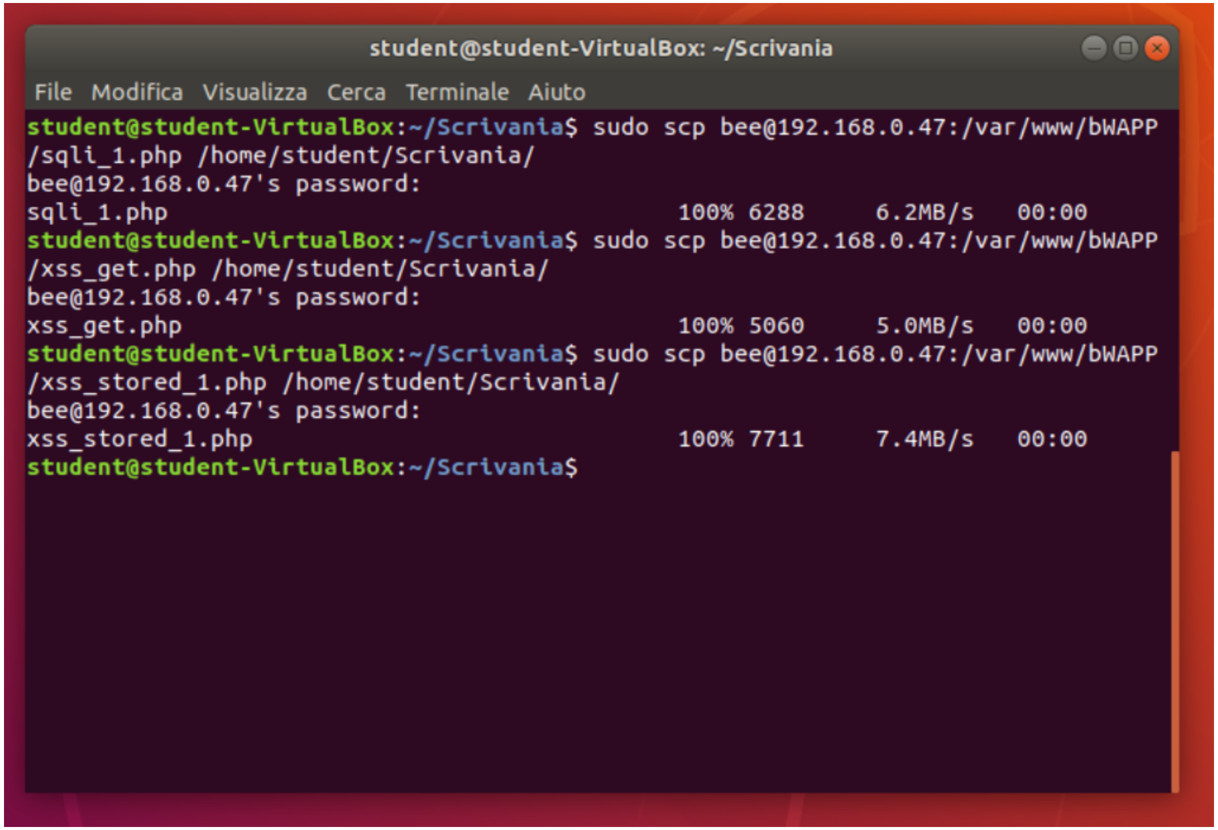
What should you do?

You need to sanitize the input because it is always good to store “safe” data in a DB.

You need to sanitize the output in case future users will be able to insert records into the DB from other pages (or even to prevent an insider’s attack).

INSTRUCTIONS FOR RETRIEVING/UPLOADING FILES FROM/TO THE SERVER_BEEBOX

Retrieve files from Server

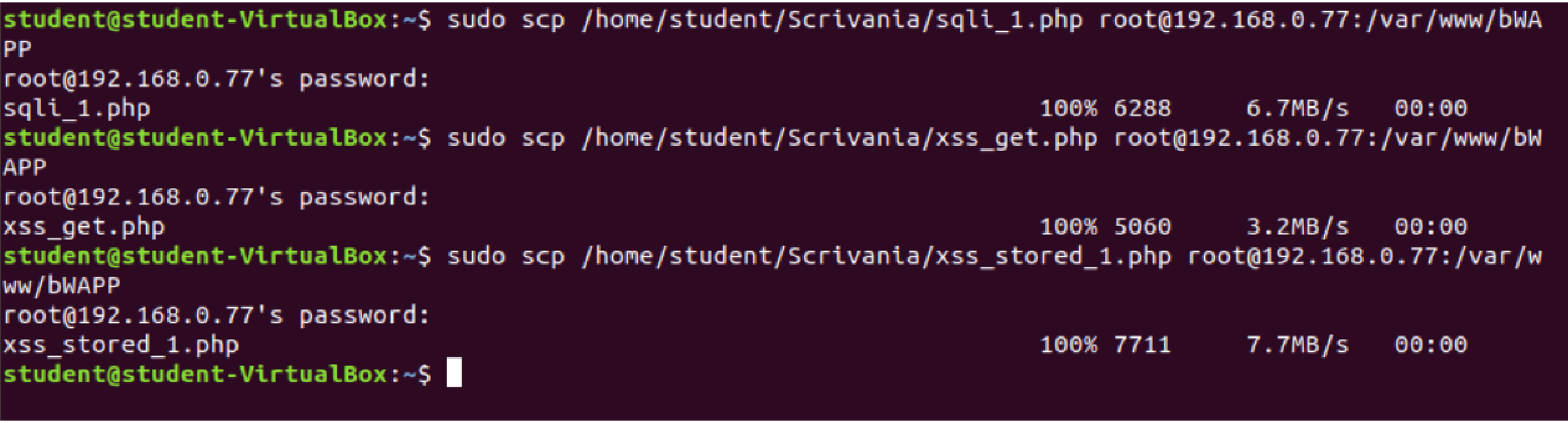


student@student-VirtualBox: ~/Scrivania
File Modifica Visualizza Cerca Terminale Aiuto

```
student@student-VirtualBox:~/Scrivania$ sudo scp bee@192.168.0.47:/var/www/bWAPP
/sqli_1.php /home/student/Scrivania/
bee@192.168.0.47's password:
sqli_1.php                                    100% 6288     6.2MB/s   00:00
student@student-VirtualBox:~/Scrivania$ sudo scp bee@192.168.0.47:/var/www/bWAPP
/xss_get.php /home/student/Scrivania/
bee@192.168.0.47's password:
xss_get.php                                   100% 5060     5.0MB/s   00:00
student@student-VirtualBox:~/Scrivania$ sudo scp bee@192.168.0.47:/var/www/bWAPP
/xss_stored_1.php /home/student/Scrivania/
bee@192.168.0.47's password:
xss_stored_1.php                              100% 7711     7.4MB/s   00:00
student@student-VirtualBox:~/Scrivania$
```

NOTE: You must use the server's IP address assigned to you. Please refer to the csv file containing the student's credentials. The server's credentials are **user:** bee (or «root») **pwd:** bug

Upload patched php files on the server

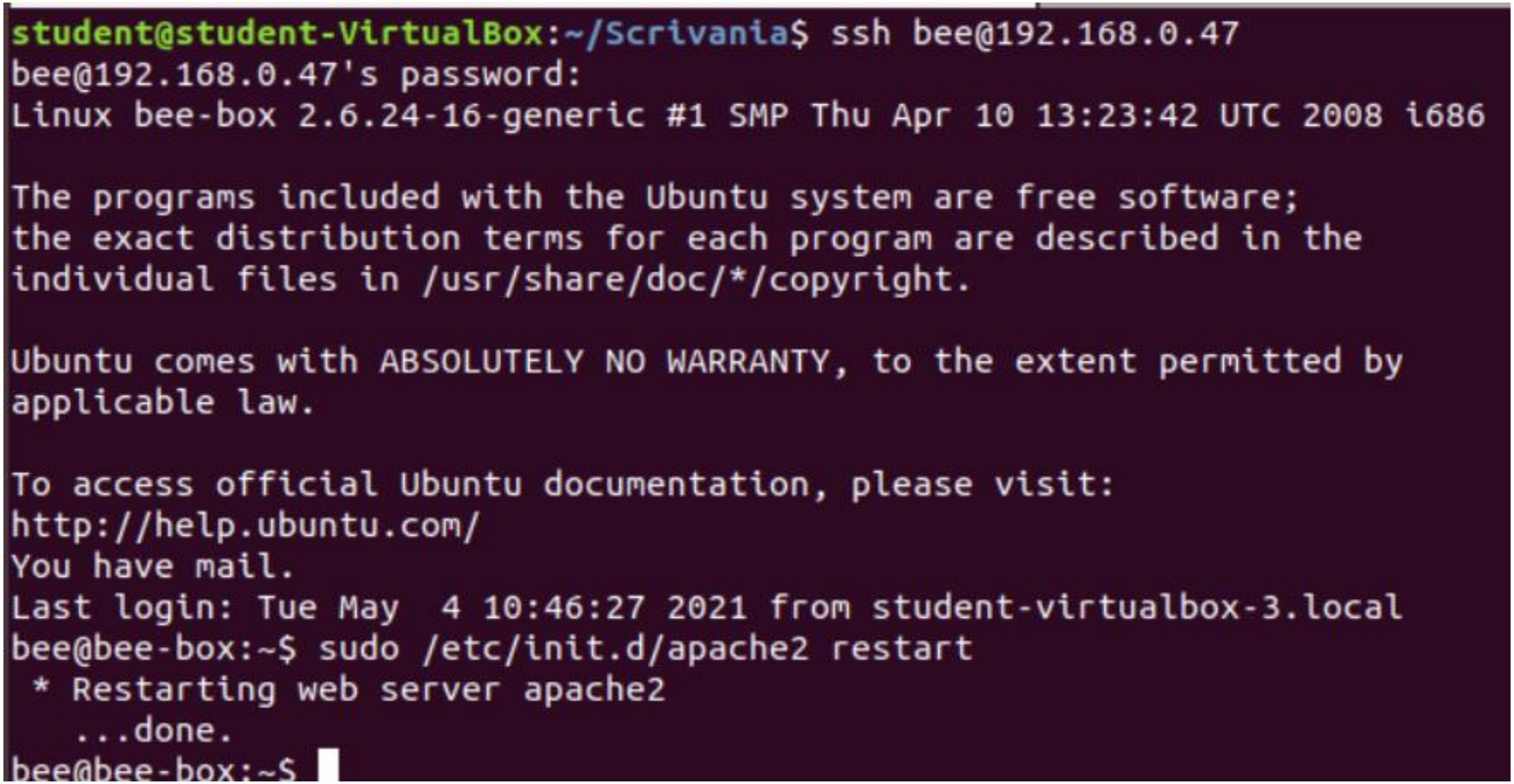


```
student@student-VirtualBox:~$ sudo scp /home/student/Scrivania/sqli_1.php root@192.168.0.77:/var/www/bWA
PP
root@192.168.0.77's password:
sqli_1.php                                                 100% 6288     6.7MB/s   00:00
student@student-VirtualBox:~$ sudo scp /home/student/Scrivania/xss_get.php root@192.168.0.77:/var/www/bW
APP
root@192.168.0.77's password:
xss_get.php                                                100% 5060     3.2MB/s   00:00
student@student-VirtualBox:~$ sudo scp /home/student/Scrivania/xss_stored_1.php root@192.168.0.77:/var/w
ww/bWAPP
root@192.168.0.77's password:
xss_stored_1.php                                           100% 7711     7.7MB/s   00:00
student@student-VirtualBox:~$ 
```

After you have patched the php files, you need to upload them on the server.

NOTE: to upload the files to the server you must log in as «root».
The user «bee» does not have the rights to write in the needed path.
User: root **pwd:** bug

Connect in ssh and restart apache



```
student@student-VirtualBox:~/Scrivania$ ssh bee@192.168.0.47
bee@192.168.0.47's password:
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
Last login: Tue May  4 10:46:27 2021 from student-virtualbox-3.local
bee@bee-box:~$ sudo /etc/init.d/apache2 restart
 * Restarting web server apache2
   ...done.
bee@bee-box:~$ 
```

PLEASE HELP US!

UNIVERSITÀ DI PISA

https://forms.gle/Cg9UZ5JfhEwZvZ1S9
Please take this questionnaire right after the session.
We need YOUR feedback to improve this platform!

The questionnaire is anonymous, so be completely honest: negative feedbacks are important too!

THANK YOU!