WAPH - Web Application Programming and Hacking

Instructor: Dr. Phu Phung

Student

Name: Vamshi Reddy Gummadi'
Email: gummadvy@mail.uc.edu

Figure 1: Headshot

Lab 1 Repository

Url for Lab 1: https://github.com/gummadvy-uc/vamshi-reddy-gummadi

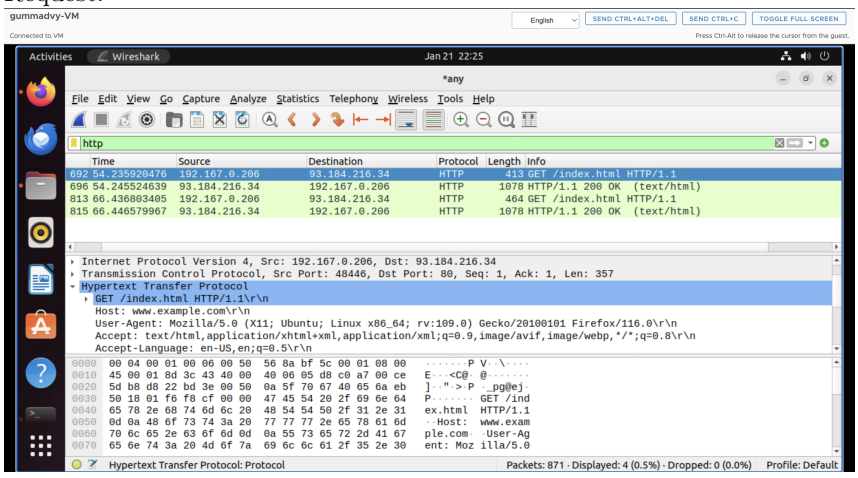
Lab 1 - Foundations of the Web

In this lab i familiar with wireshark tool and with the help of that tool i have i have captured the request and response in that tool.ALSO, applied http filter to check the request and response. With the help of telnet, I have checked the request and response. In the task2 i have learned some basic cgi application and also observed the output.Also, familiar with some php handson.

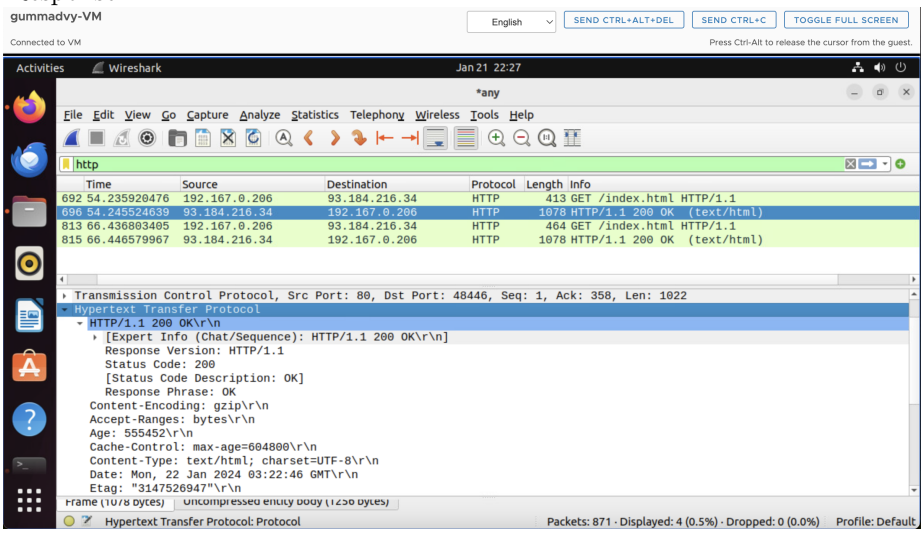
Part 1: The Web and HTTP protocol

TASK 1: Familiar with Wireshark tool and HTTP protocol

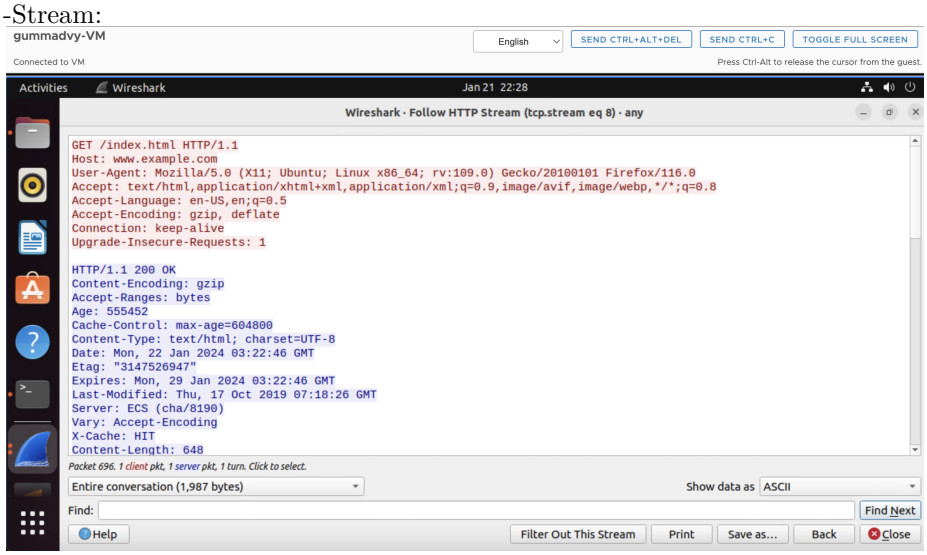
- I have installed Wireshark tool using the sudo apt installl Wireshark -qt command. And verified and run the application.
- I ran the Command sudo Wireshark & to open the Wireshark from the terminal.
- I clicked on the settings icon and selected any to capture all the interfaces, then clicked on start button.
- I opened a browser in a virtual machine and searched for the http://example.com/index.html , later returned to the Wireshark tool and stopped tracking.
- I applied a http in the filter bar to check the request and response of the example website. 6. clicked on the follow -> HTTP Stream to check the request and response.
- Request:



-Response:



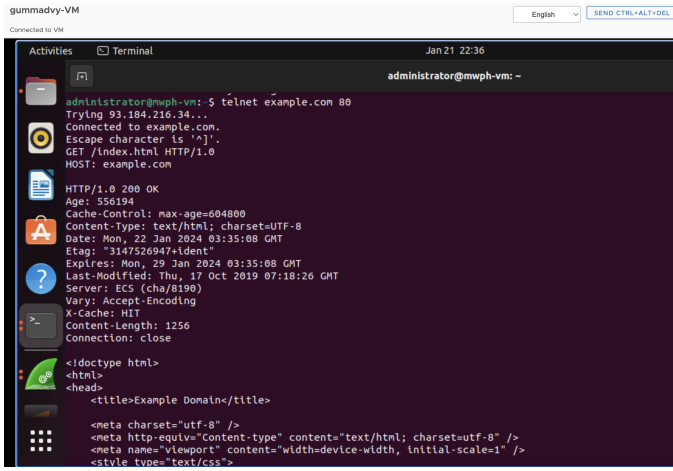
-Stream:



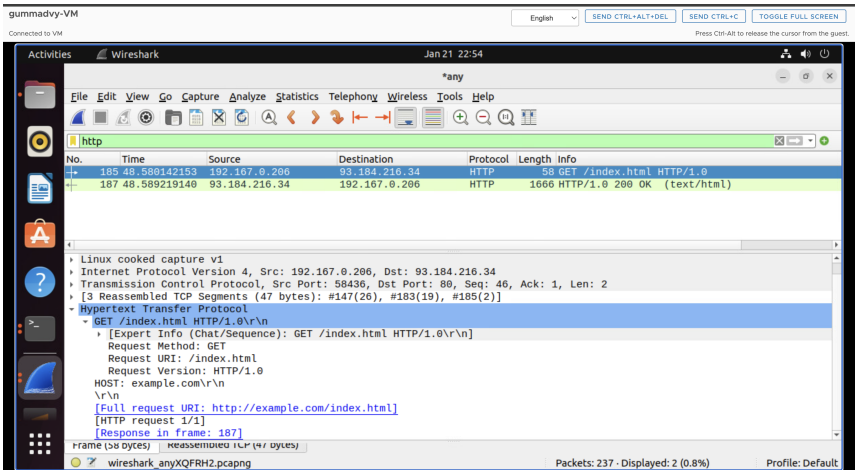
TASK 2: Understanding HTTP using telnet and Wireshark

- I have clicked the start button in Wireshark to capture the http request and response.
- I have ran the command telnet example.com 80 in the terminal to connect to the web server. After success, I have written GET/index.html HTTP/1.0 clicked enter, written Host: example.com, clicked enter for two times.
- After clicking on the enter twice, I have received the output of the example.com . Both the request and response.
- I have compared the request of both browser and telnet. I can see , when I run via browser there are some additional field are there such as user-agent, accept, connection.
- I have compared the response of both browser and telnet. The only difference is content encoding is present when I run via browser.

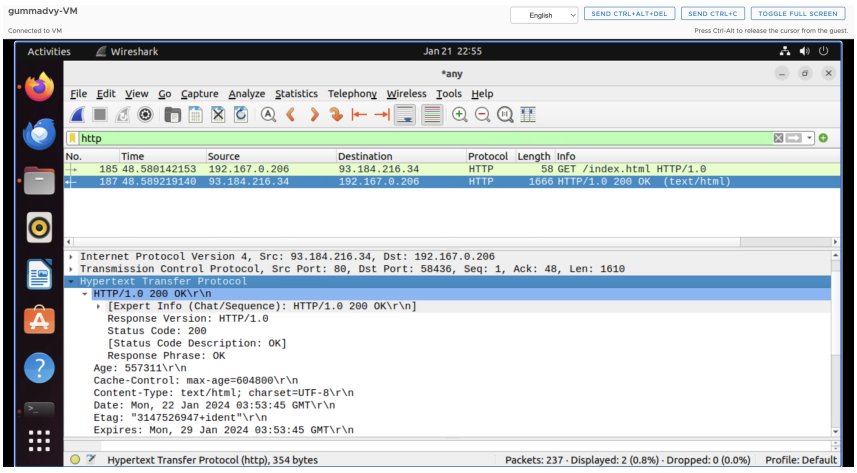
- Terminal showing HTTP Request and Response



- Request in Wireshark



- Response in Wireshark



Part 2:

Task1:

a)

- I have created a HelloWorld.c program in sublime and written the code which was given by the professor.
- By default CGI daemon is not enabled in Apache2, I have ran the command sudo a2enmod cgi and restarted apache server using the sudo systemctl restart apache2.
- I have installed the gcc by using the sudo apt install gcc command
- To compile the HelloWorld.c file I have used the command gcc HelloWorld.c -o HelloWorld.cgi clicked enter.
- I have copied the HelloWorld.cgi to /usr/lib/cgi-bin by using sudo cp HelloWorld.cgi /usr/lib/cgi-bin.
- I have run the link in the browser(http://localhost/cgi-bin/HelloWorld.cgi) and got the response as expected.

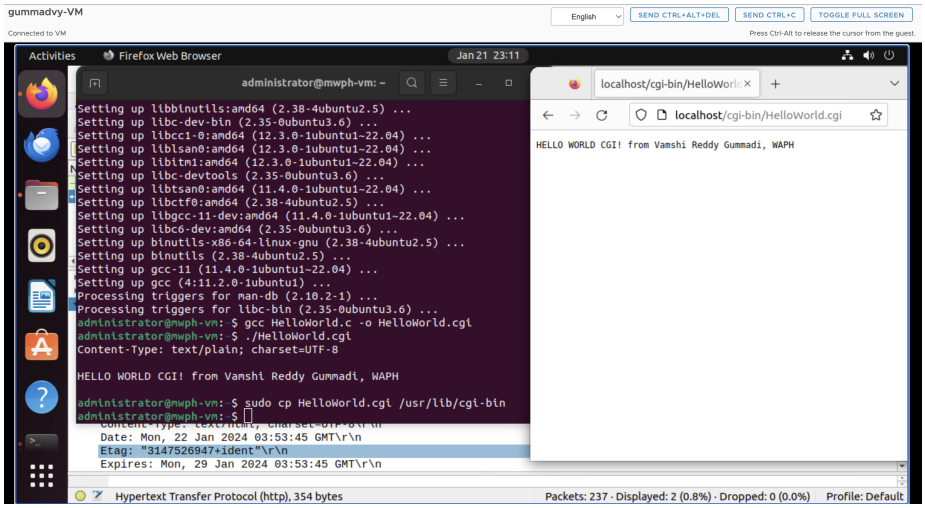


Figure 2: Screenshot7

b)

- Code for Index.c:

```
#include<stdio.h>
int main(void){

    printf("Content-Type: text/html; charset=UTF-8\n\n");
    printf("<!DOCTYPE html> \n <html>\n <head>\n <title> Vamshi Reddy Gummadi </title>\n </h
```

```
    return 0;
}
```

- I have used the same commands for the index.c as above and run the link http://localhost/cgi-bin/index.cgi

- Received the output as expected.

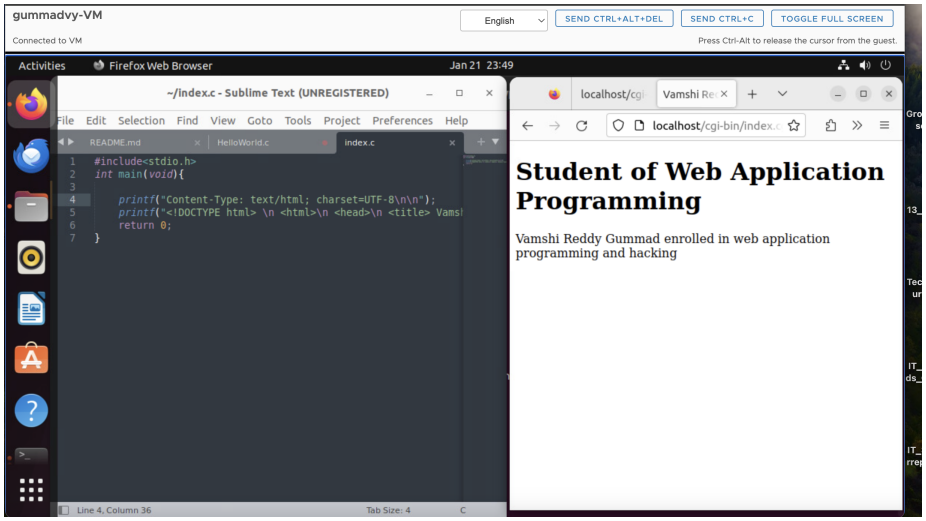


Figure 3: Screenshot8

Task 2:

a)

- I have installed PHP using the command sudo apt-get install php libapache2-mod-php -y.
- I have created the hello world.php in lab1 folder.
- Deployed the code to the web server by going into the directory of the file and run the command to copy that file into the server sudo cp hello world.php /var/www/html.
- I have used the localhost/helloworld.php to check if the output is coming.

b):

- I have created a echo.php file in lab1 folder.
- Source code:
- Copied the code into /var/www/html and run the http://localhost/echo.php?data=Hello

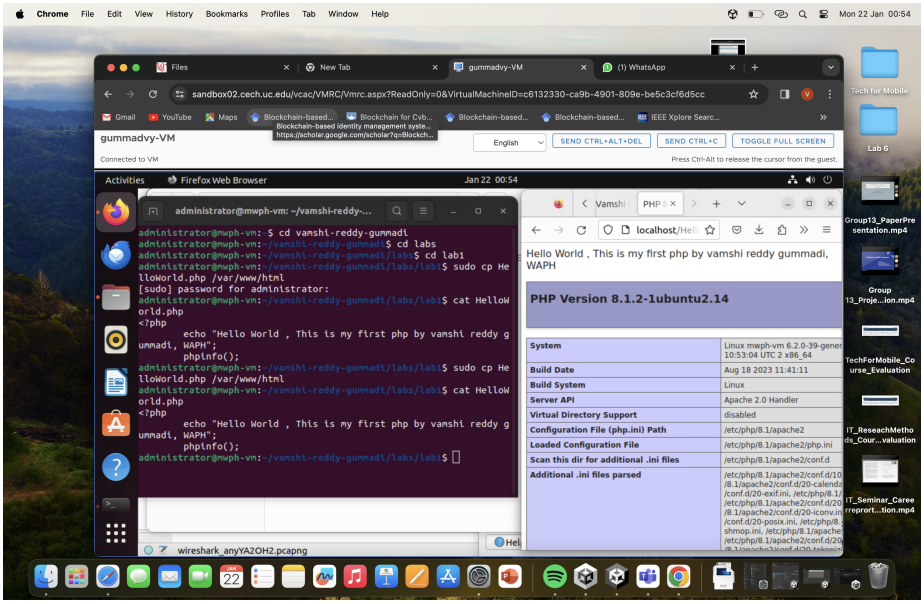
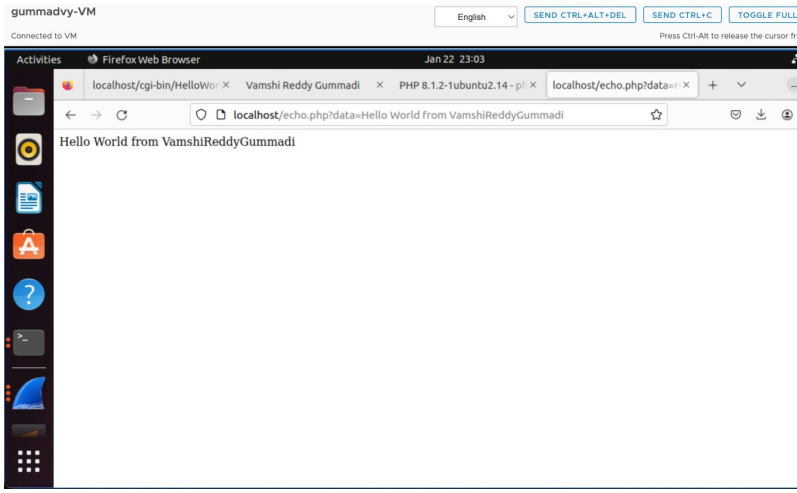


Figure 4: Screenshot9

World From VamshiReddyGummadi 

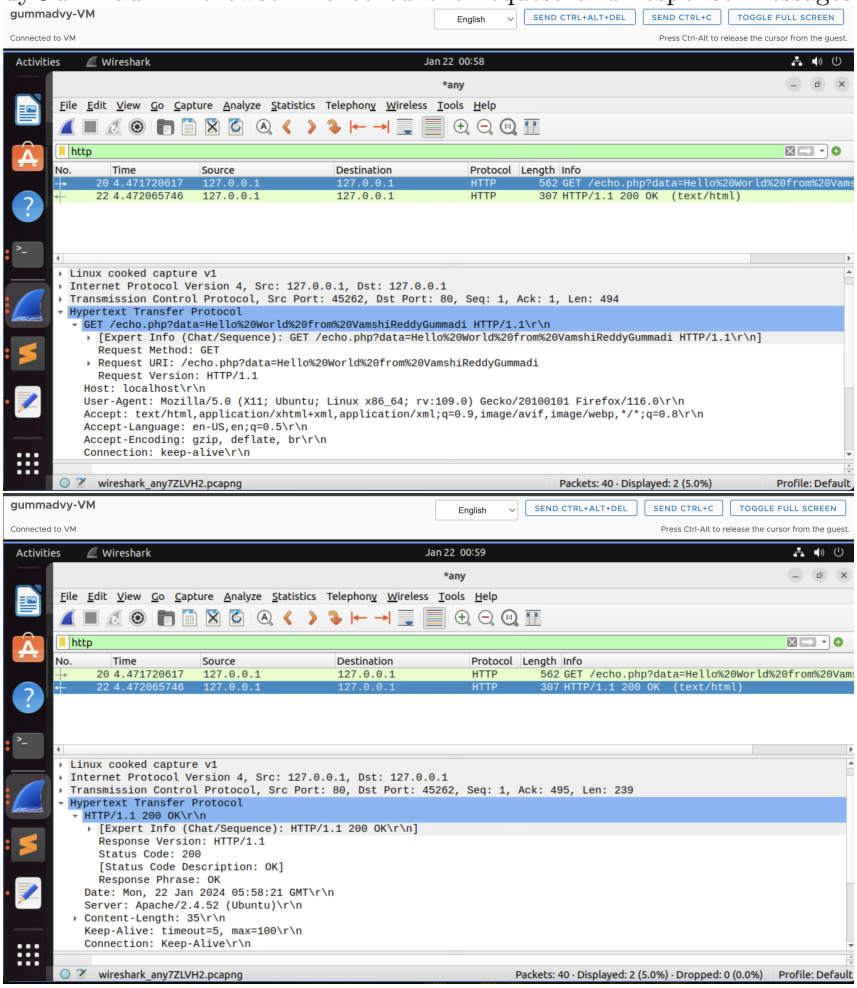
c:

- If the input for the request has not been properly checked then it could lead to some security issues.
- Always validate the data for request.
- If the data is not handled correctly, it may cause compromising the confidentiality like personal information.

Task 3:

a)

- I have started the Wireshark.
- Run the http://localhost/echo.php?data=Hello World From VamshiReddyGummadi in browser. checked the request and response messages



b):

- I have started the Wireshark.
- I have used the command to curl -X POST http://localhost/echo.php -d "Hello world, from VamshiReddy Gummadi" and opened http stream and observed the output.

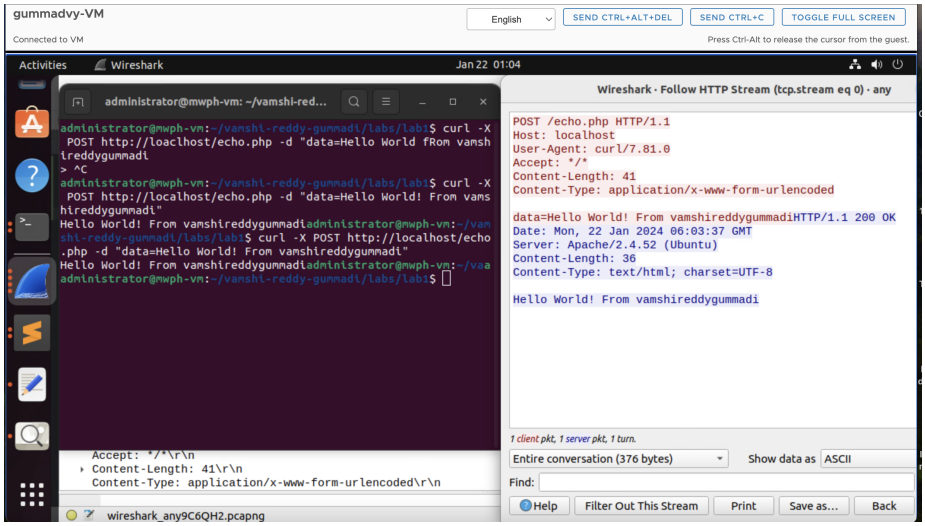


Figure 5: Screenshot12