Web Security Assignment

This assignment includes two parts:

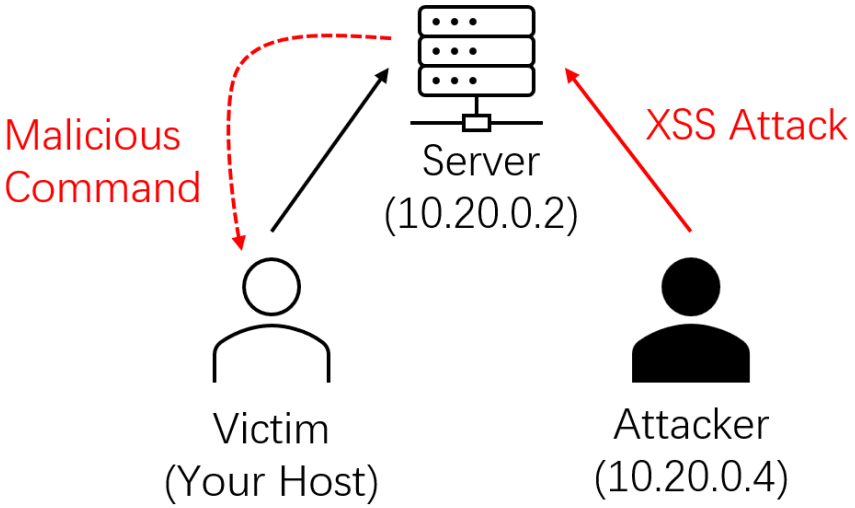
1. Message Board (50 pts)
2. Forum (50 pts)

In these two tasks, you are asked to conduct the corresponding attack in simulated network environment. As the virtual environment is built via Docker, you will need to install Docker. **Please use either Linux or MacOS to finish this assignment.**

Message Board (50 pts)

Description

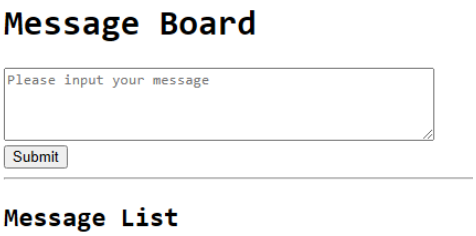
Consider the network environment as follows:



The server holds a message board service for the victim and attacker in the local net. However, the web application is vulnerable, and the attacker can launch XSS attack to execute malicious command in the victim machine.

Unzip **XSS_Attack.zip**, and run `docker compose up` under the decompressed directory. Before starting the assignment, please make sure the two containers are successfully deployed.

In this scenario, the attacker and the server are under the subnet (10.20.0.0/24), your host acts as the victim. In your host, you can visit the webpage via 127.0.0.1:5000 in the browser. **We strongly suggest using Chrome Browser to finish the task!** The webpage is a message board, all the users can upload their message in the input panel, and the message will be listed below.



Questions

Please answer the following questions and include them in your submitted report. You can attach to attacker's shell via `docker exec -it xss-attacker-1 bash`.

1. Is this XSS attack reflected, stored, or other types? Explain the reason and why this vulnerability exists. 5 pts
2. Write a script to launch an XSS attack in attacker's machine to pop out an alert box when you visit the webpage via browser. The alert content should be "hacked by <name> (<student number>)". Please explain the attack workflow along with your attack script. Please attach a screenshot to prove a successful attack. (Check Instruction-1) 15 pts
3. Write a script to launch an XSS attack in attacker's machine to send the cookie of this webpage in victims' machine (i.e. your host) to the attacker. Please explain the attack workflow along with the attack script and attach a screenshot to prove a successful attack. (Check Instruction-2) 20 pts
4. Try to launch an XSS attack to send a file from the victim's machine to the attacker (you can choose whatever files you want). Can this attack be launched successfully? If yes, please introduce the workflow along with the attack script. If not, please explain how the browser prevents this attack. 10 pts

Instructions

Instruction-1

You can send message to the webpage via "requests" library as an attacker. You can send the payload with the following code template.

```
import requests

payload = """
# Fill up your attack payload here
"""

# In attacker's machine, it need to use 10.20.0.2 to visit the webpage.
requests.post('http://10.20.0.2:5000/', data={'content': payload})
print("XSS payload submitted")
```

Instruction-2

As in this virtual network environment, you host cannot get access to the subnet we created for the two containers, we have implemented port mapping (attacker's port 7000 to host's port 7000) to enable the text transformation from the victim (host) to the attacker. Accessing 127.0.0.1:7000 in the host is equivalent to accessing port 7000 of the attacker machine.
One alternative way of the attacker to receive the message from the victim is to deploy a http server on attacker's machine using port 7000. You can refer to the following code template:

```
from flask import Flask, request

app = Flask(__name__)

@app.route('/receive', methods=['POST'])
def receive_cookie():
    # TODO
    # Implement this method according to your attack workflow

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=7000)
```

You can post message to attacker with URL 127.0.0.1:7000/receive in victim machine.

Forum (50 pts)

Description

In this task, you are provided with a forum website and are required to perform CSRF attacks on forum users. We will provide you with several accounts' usernames and passwords to log in to the forum to use its functionalities, such as adding friends, editing profiles, and posting blogs. To complete the task, you should use different accounts to act as both the attacker (to launch the attack) and the victim (to verify the effect of the attack). To complete a part of this task, we also provide another website for you to edit, which can simulate a malicious link for phishing victims to click.

Instruction

Unzip **CSRF_Attack.zip**, and run `docker compose up` under the decompressed directory. Make sure all containers are successfully deployed.

- If you intend to use docker in macOS, please follow https://docs.orbstack.dev/install to install OrbStack to run docker containers, instead of Docker Desktop on Mac. The network support by OrbStack is better so that you can visit the forum website directly. Otherwise, please use a Linux OS/VM for this task.

After running up the containers, please add these lines in your Mac or Linux's /etc/hosts:

```
10.9.0.5 www.seed-server.com
10.9.0.105 www.attacker32.com
```

And then, visit the forum website (http://www.seed-server.com) to start this task. Avoid conflicting addresses with your original /etc/hosts, which you can restore after finishing this task.

The accounts of this forum are:

Username | password:

```
alice   | seedalice
boby    | seedboby
charlie | seedcharlie
samy    | seedsamy
```

Please select any two of them to act as an attacker and a victim to finish the following questions.

Questions

Please include the code you wrote and screenshots step-by-step in your submitted report:

1. Browse the forum and collect the HTTP requests of different functionalities, including adding friends and editing profiles. Please search about the browser developer tools or other HTTP request inspection plugins to collect HTTP requests. 10 pts
2. Write malicious payloads on one user's (act as an attacker) profile, so that when a victim visits the attacker's profile, he/she is forced to send a forged GET request to add the attacker as a friend in the forum. You should log in as the victim user to verify the effect of the attack. 20 pts
3. Please edit the clickme.html and put the link in the attacker's profile, so that when a victim clicks the link, he/she is forced to send a POST request that changes his/her profile to some contents provided by the attacker. You should log in as the victim user to verify the effect of the attack. 20 pts