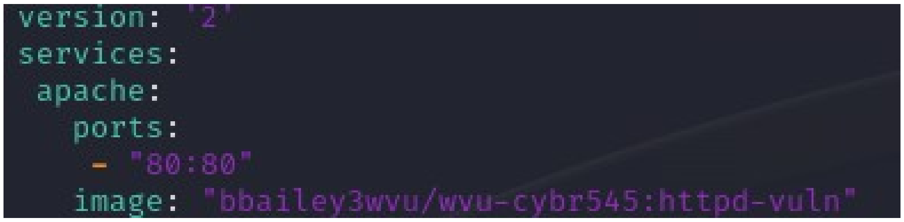
Kali Linux Exercise 2:

During week 2 you setup your docker environment on your Kali VM, now let's leverage the power of docker to spin up a vulnerable container and perform a web exploit. We will perform an attack on a system and retrieve a flag file. Upon retrieving the flag file, the goal is to find the special string within the file. You will be leveraging information from Chapter 6 and 8 from the Walker text as well as the videos that were from this week. If you are feeling adventurous, after finding the flag attempt to crack the passwords of the users on the local operating system. Cracking the passwords is not required for credit.

Create a docker-compose.yml file with the following contents:
(Note the tabs in the formatting)



```
version: '2'
services:
 apache:
   ports:
    - "80:80"
   image: "bbailey3wvu/wvu-cybr545:httpd-vuln"
```

Figure 1: Contents for docker-compose.yml file

The above docker file will pull a container that I created for this Kali exercise.

Please submit screenshot of docker container bbailey3wvu/wvu-cybr545:httpd-vuln running by issuing command

docker-compose up

Once the container is running open a web browser on your Kali machine and go to http://localhost and submit a screenshot of the resulting page.

This web server has a specific type of vulnerability. Typically, in a Capture The Flag or training course one would request you discover the vulnerability yourself, given you all are new to this the following hint will be provided.

Append the following text to the URL/URI to start your exploitation in your hunt for the flag.

/icons/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/

The goal of this lab is to exploit the vulnerability and retrieve the **flag file** and then find the string within the flag file.

- Hints: The /tmp directory sometimes has some juicy information.
- Lookup the meaning of .%%32%65/

If you elect to attempt to crack the passwords for the local users, then John the Ripper and the RockYou wordlist (usr/share/wordlists/rockyou.txt in Kali) will be your friend this week.

Please submit your answers by submitting the worksheet associated with this lab.