Kali Linux Exercise 2

Web Exploitation and Flag Hunting

Group number:
Students names:

Refer to the Kali Exercise2.doc document to setup your Kali Linux for this lab and provide your answers below each of the questions below.

*Please provide each answer in **BOLD** below the corresponding question. Turn in one lab report per group. Write in all group member's names in the field above.

Setting Up Docker

1. Please provide a screenshot of the execution of your Docker container bbailey3wvu/wvu-cybr545:httpd-vuln as a result of your *docker-compose up* command. **[10 points]**

Confirming Web App is Running

2. 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.
[10 points]

Finding the Flag File

3. Please provide a description of the steps you used to discover the flag file. **[40 points]**

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/

Hint: The /tmp directory sometimes has some juicy information.

Finding the Key String in the Flag File

4. Please provide the key string from the flag file and a description of the steps you used to discover the string within the flag file. **[20 points]**

Type and Impact of Vulnerability

5. Please describe, in sentence form, the type of vulnerability and criticality level of this vulnerability and justify your criticality rating. For the sake of discussion, assume this vulnerability was discovered in a business setting and not in a lab environment. **[20 points]**

For the Fun of It (10% bonus)

Please provide the password(s) for the user that you were able to crack from the underlying operating system.

Hint: This might help you out *usr/share/wordlists/rockyou.txt*