**ASSIGNMENT 11**

**STEPS PERFORMED ON LAZY-ADMIN**

# **INDEX**

|  |  |  |
| --- | --- | --- |
| **SL NO** | **TOPIC** | **PAGE NO** |
| 1. | Summary report on different steps performed on lazy-admin | 2-8 |
|  |  |  |

# **Topic: STEPS PERFORMED ON LAZY-ADMIN (TRYHACK ME)**

ASSIGNMENT 11(DAY 13) Date:11-07-2022

1. **Summary report on different steps performed on lazy-admin**

**Step 1: Lazy admin room was solved today on tryhackme.**

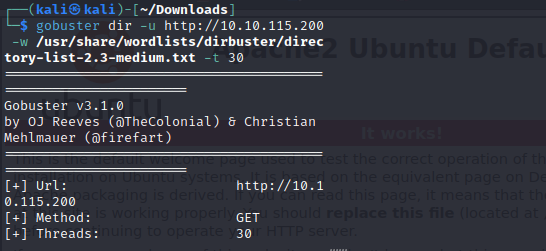
**Machine was started and we copied the IP address which was provided by tryhackme and then port scanning was done.**

**The first command did an aggressive scan on the IP Address to know version of the system.**

**Then the second command was used for a simple nmap open port scanning to know the ports which are open.**

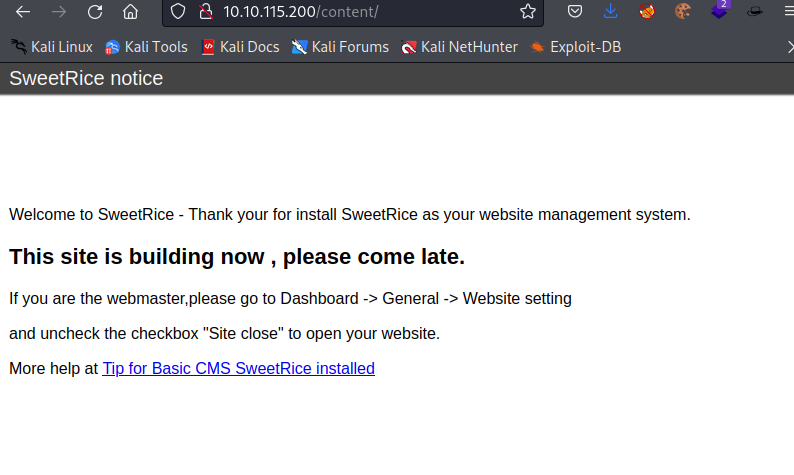
**Step 2: Now gobuster scan is done to know the hidden directories on the**

**particular website.**



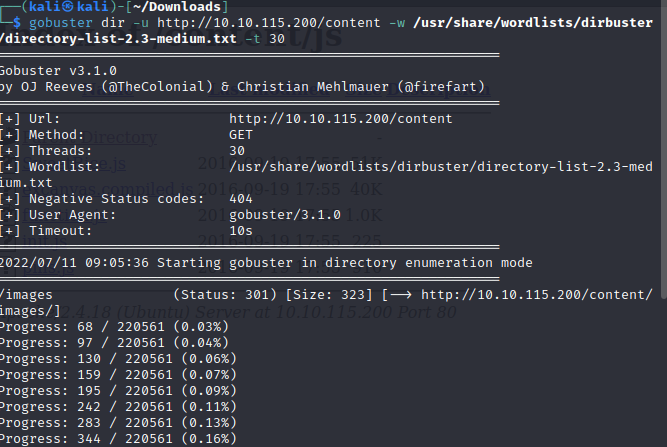
**Step 3: A directory named Content is found. The following page appeared when**

**we typed the IP address with the content.**

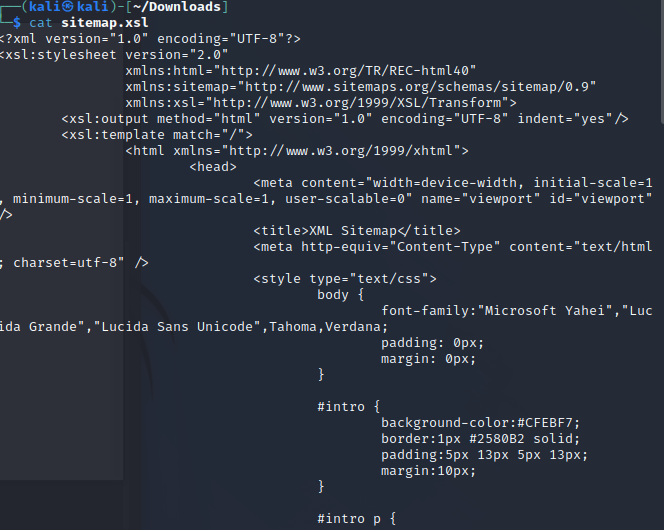


**Step 4: Now, gobuster scan is performed on the IP address with the content**

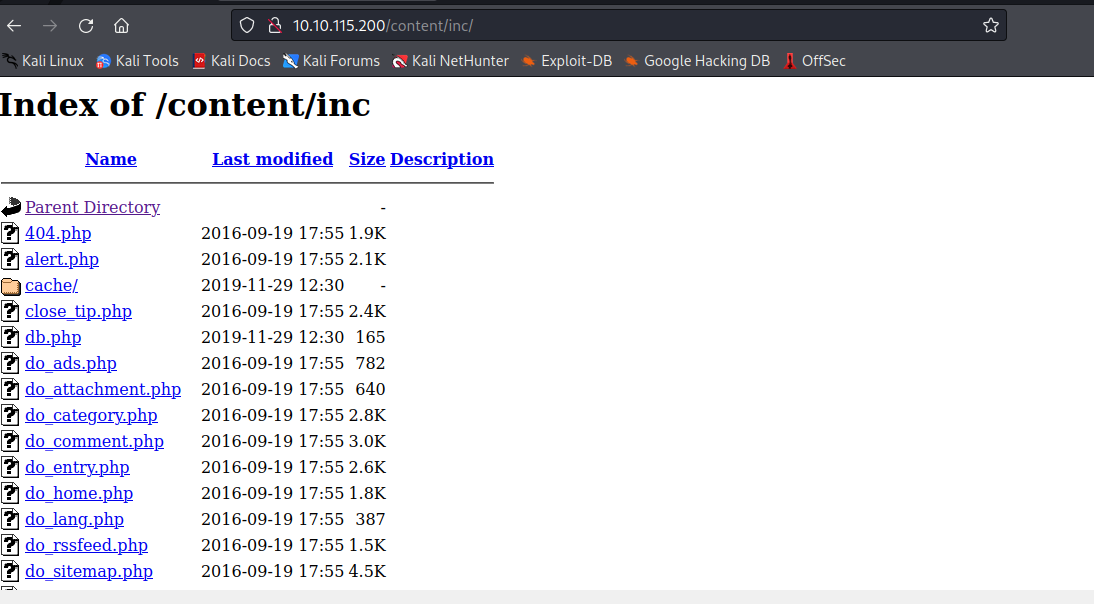
**Directory so we get more hidden directories under the content.**



**Step 5: Now we download the sitem app which is there in the content directory. With the help of CAT command we can see the contents of the file.**



**Step 6: Now we find in c directory under the content.**

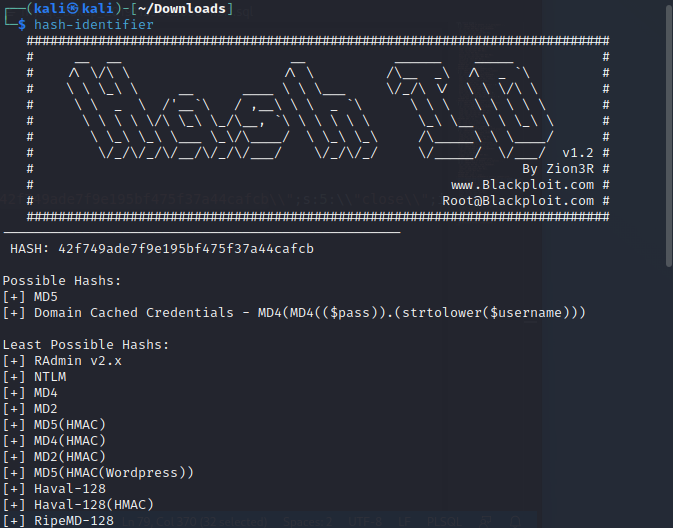


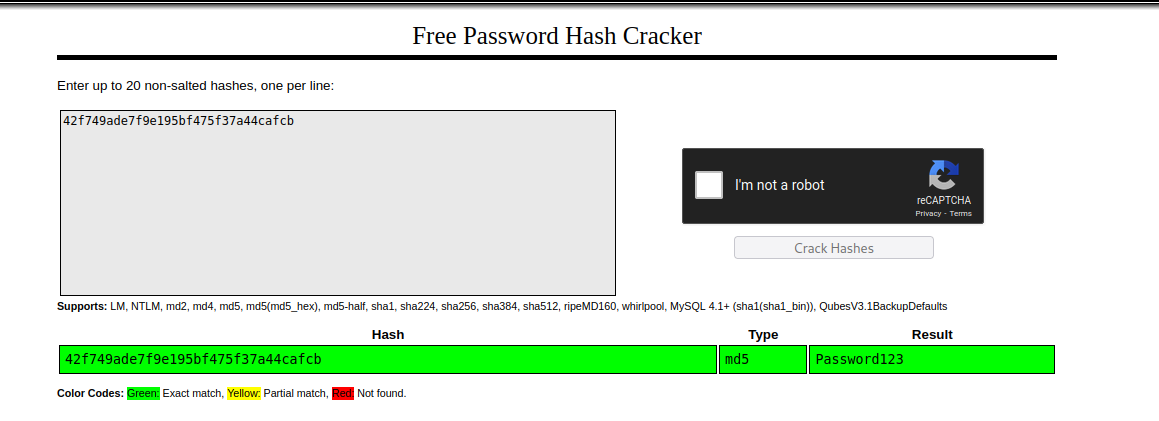
**Step 7: Now we save the file with mysql and then open it using VS Code editor.**

**After viewing the file, we find the username and password of the login site**

**‘SweetRice’. Ow we crack the password using hash identifier and by using**

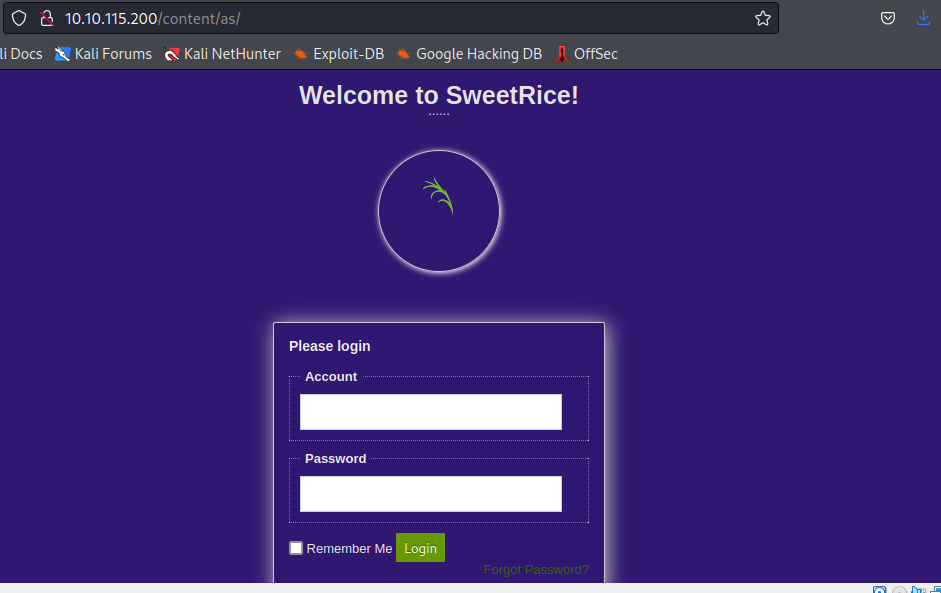
**Crackstation we decrypt the password and its type.**





**Step 8: Now we ‘as’ directory from gobuster scan .By using ip/content/as we**

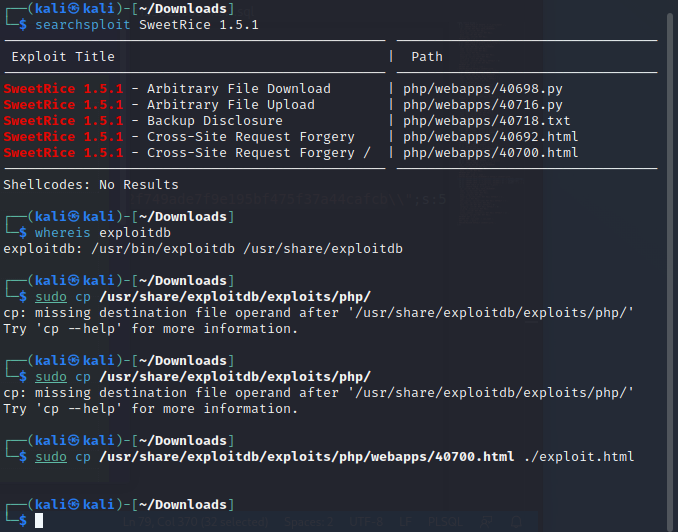
**retrieve the login page.**



**Step 9: After logging in, in order to exploit we need to update the exploit database**

**using sudo apt update exploitdb, after the updating searchploit tool is used**

**for Exploit DB, this takes a copy of exploit database.**



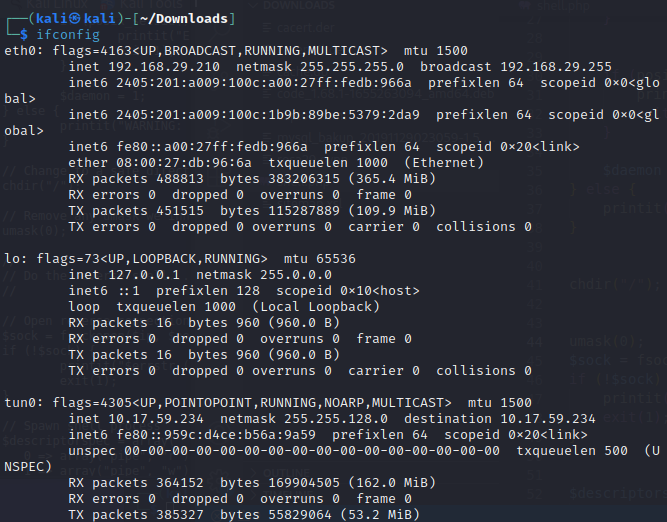
**Step 10: Now, viewing the exploit on VS Code Editor we change the IP address and**

**the port for the code and then upload file we click on ads option on the**

**SweetRice page. Now we name it and run the code. Now check the inc**

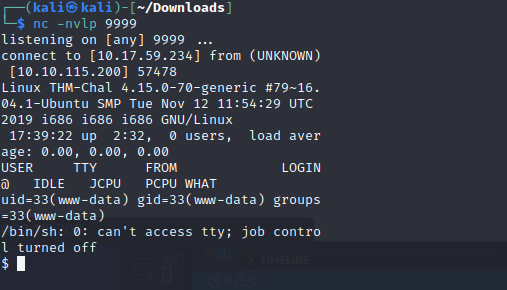
**folder and we can find that file is uploaded successfully. In order to find our**

**IP address we use ifconfig in the terminal.**

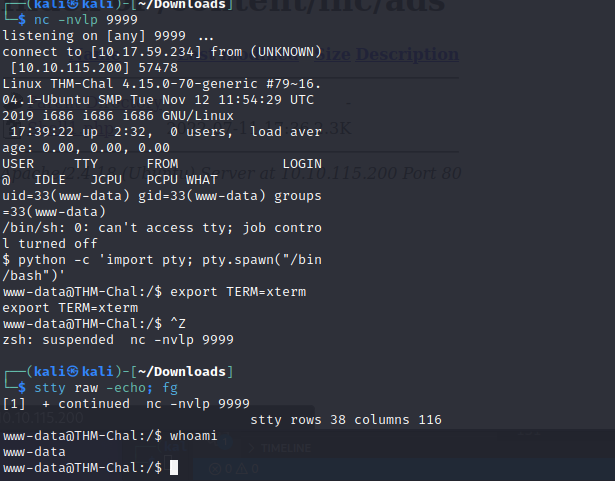


**Step 11: Now, nc -nvlp command is used because netcat nc runs a utility for**

**sending raw data over a network connection.**

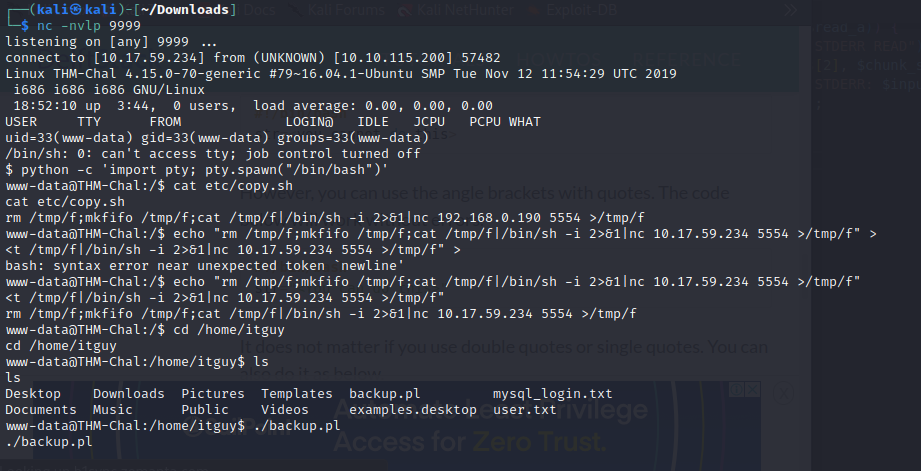


**Step 12: After connection is established we stabilize it using wappalyzer.**



**Step 13: Now, after the connection with the root www -data we retrive the contents**

**present in different files and directories.**



**Step 14: After solving the room, the machine is closed and exit.**

**NAME: I PRASANTI**

**SIC: 20BCEA56**

**BRANCH: CEN**