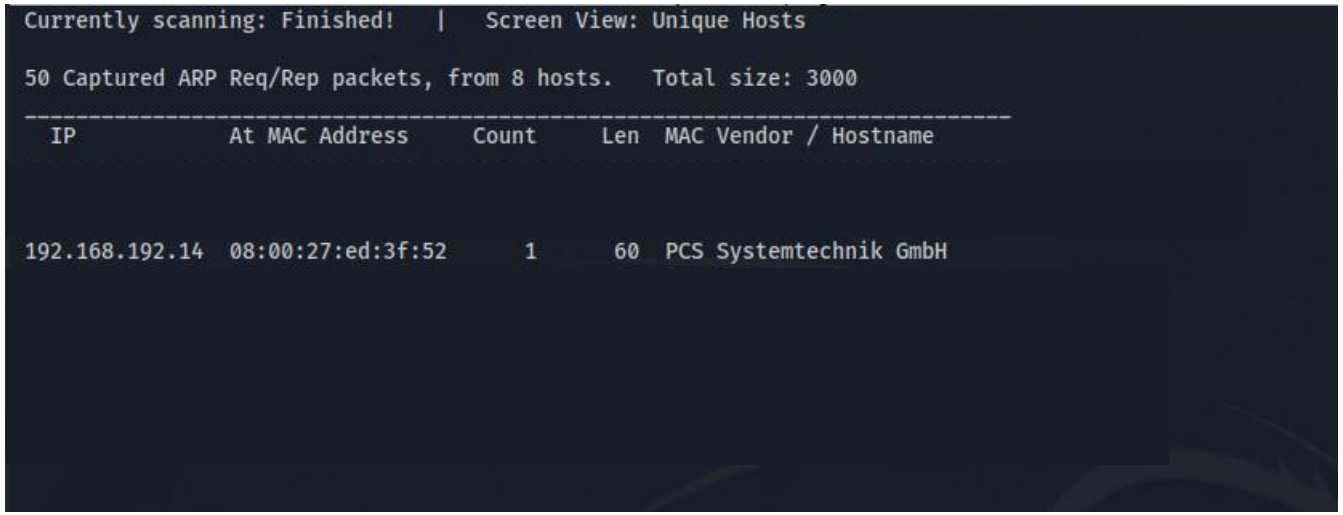
JANGOW 01

This is a box from vulnhub that is rated easy by the author but depending on your skill level it may also be considered as medium. The box had a web application that was running which was misconfigured and one end point allowed command execution. The box also teaches you to test for password re-use and that's how we managed to obtain the user flag.

Author: Kharim Mchatta

Date: 5/30/2023

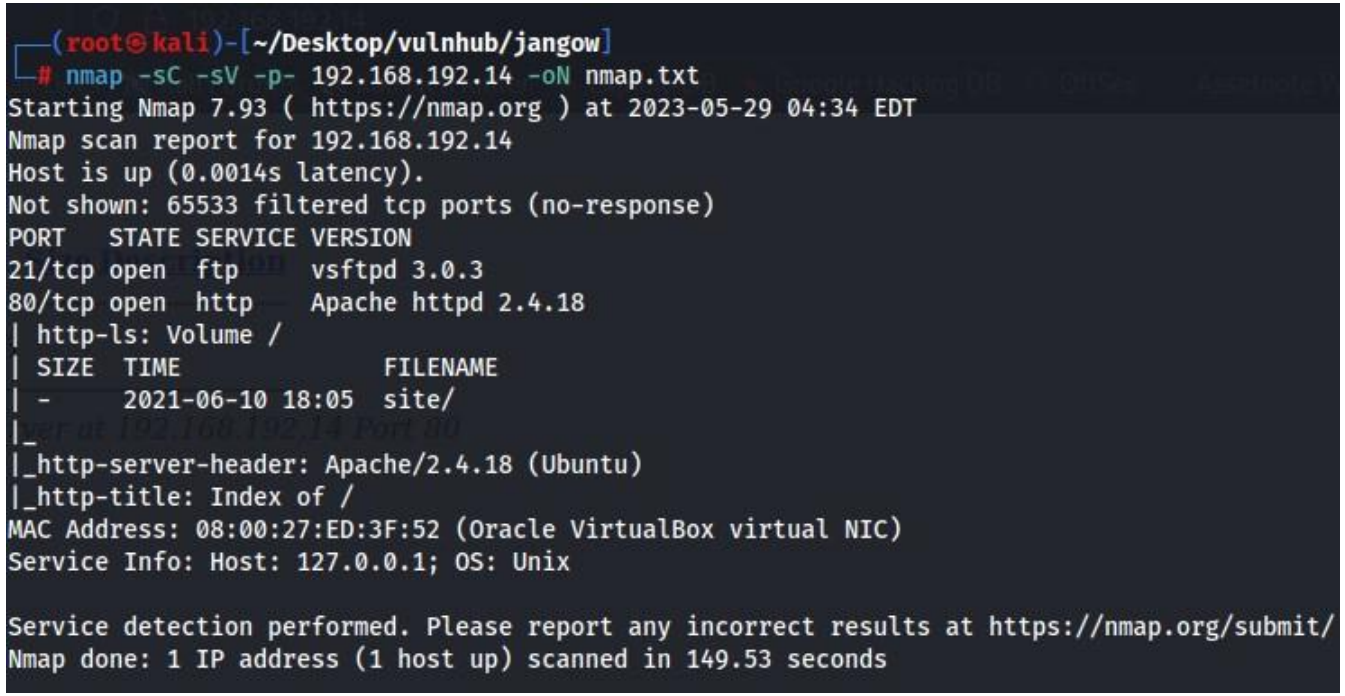


The first step is to get the IP address of our target machine where we used a tool called netdiscover, it is used to scan the network. To Scan the network, I used the following command

Netdiscover –r 192.168.192.10/24

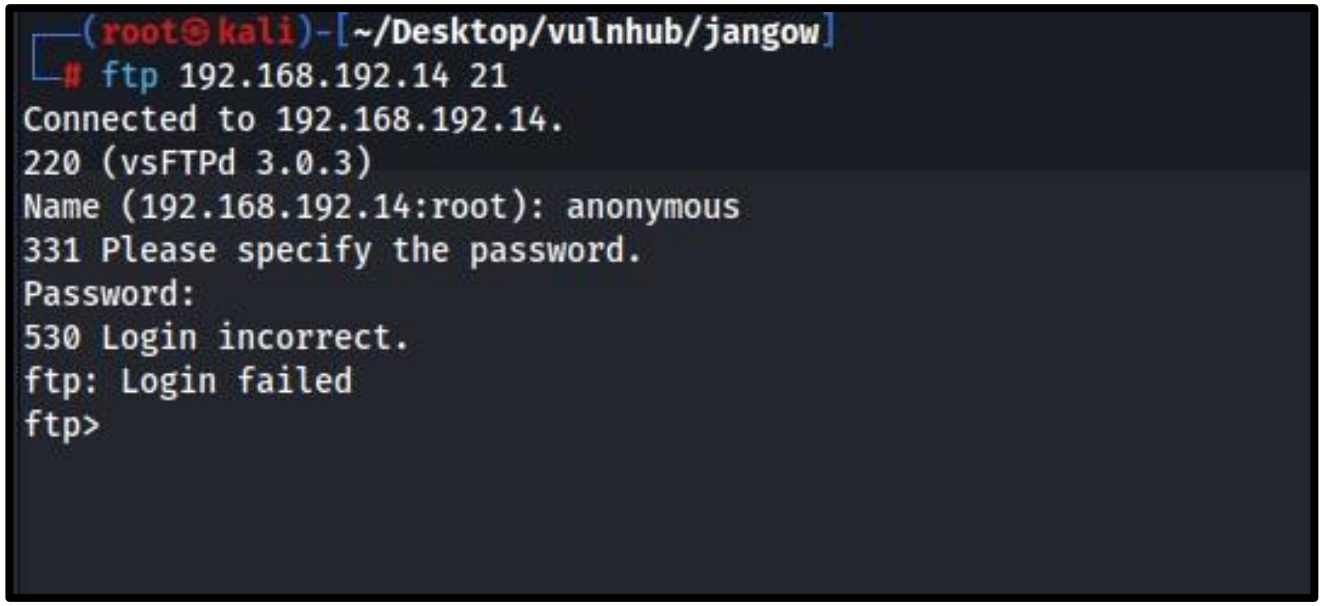
The target ip is the ip address that has the host name of pcs systemtechnik GmbH

Note: to scan for other devices on the network you need to first get your ip address by typing in if config then using your ip address you scan the whole subnet

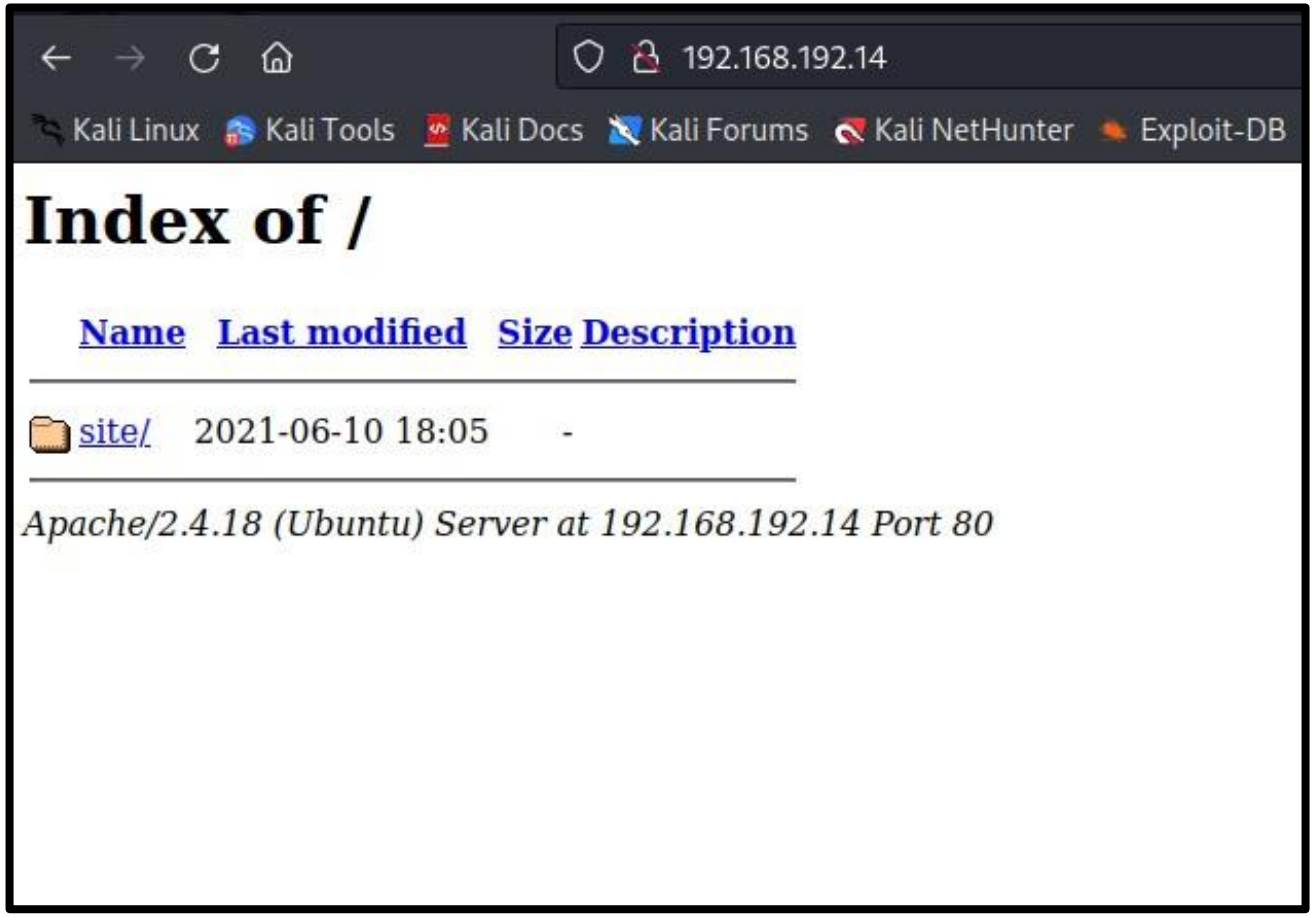


Next, I scanned the target ip 192.168.192.14 using nmap to see what ports are open and services are running on the target. From the results we can see that port 21, 80 are open. Port 21 is running the ftp service and port 80 is running http service.

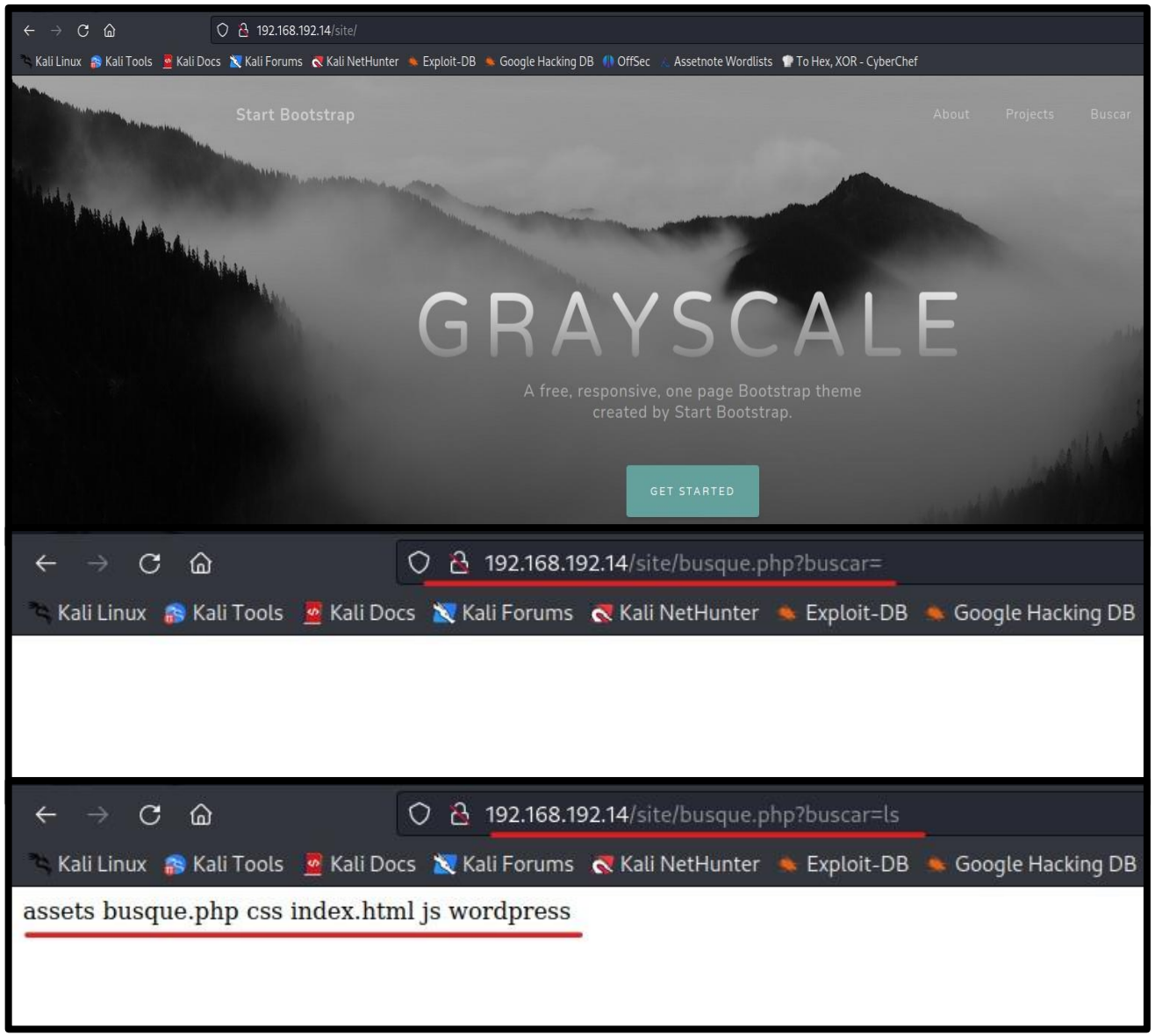
On the web application we can see that there is a file that is discovered called site which might be of interest to us.



The next step is to try to login the ftp service. Usually, it would require credentials to log you in but sometimes system administrators do tend to forget to remove the default credentials of ftp which is **anonymous:anonymous,** after attempting to login the ftp service I realized that the default credentials didn't work, so the next step would be to check the web application.

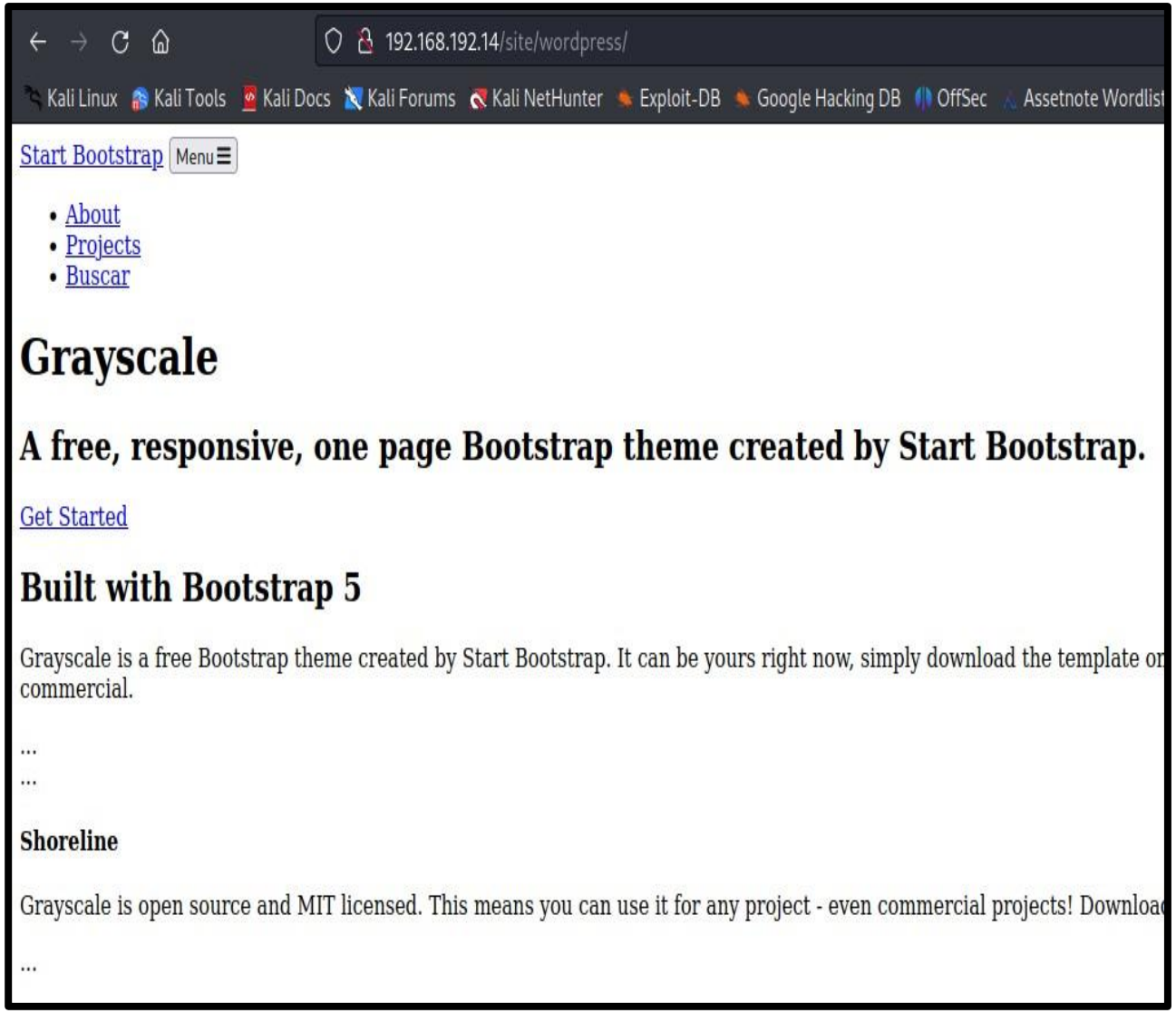


Opening the web application from the browser we can see that the web application was not configured properly since we can see the web server file called site as nmap had reported.

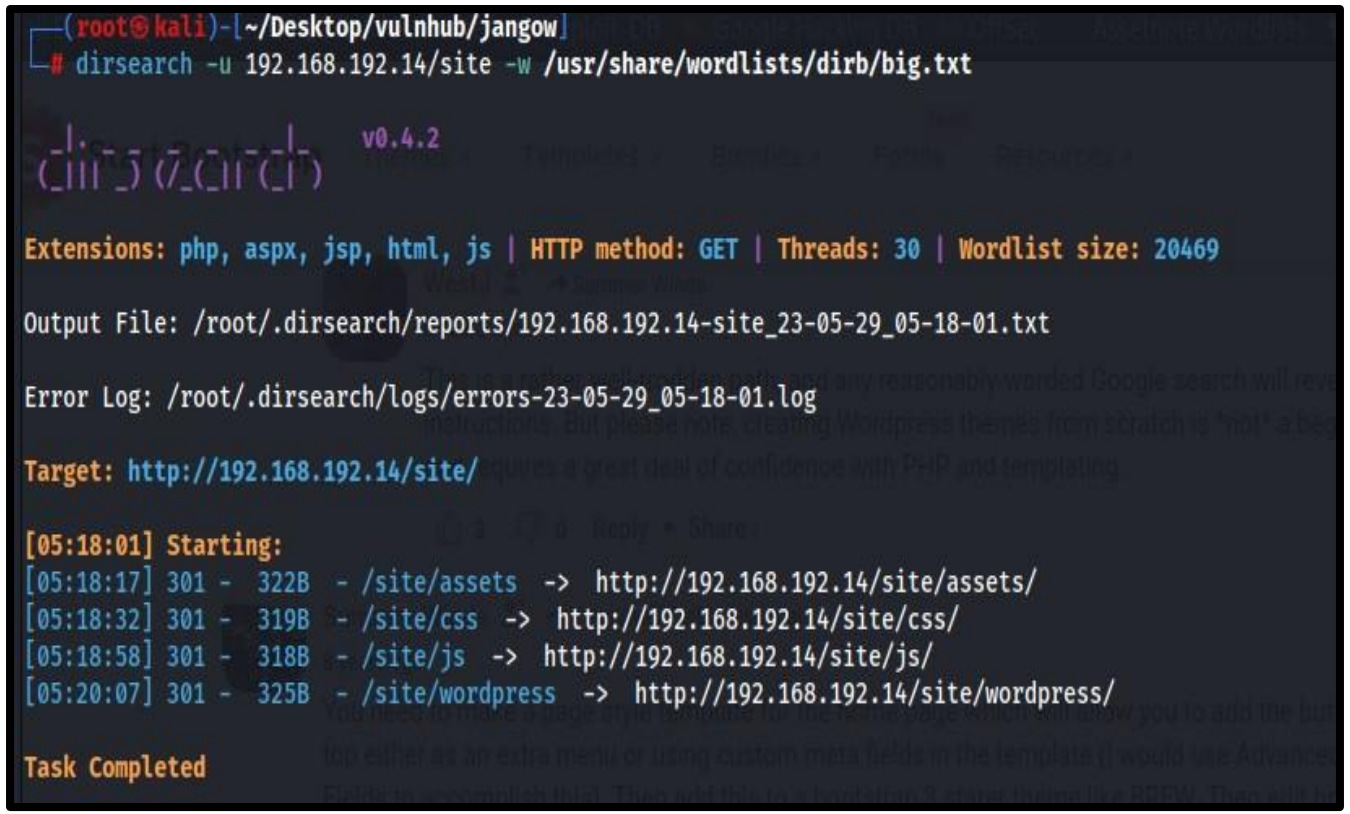


When I clicked the file site is when the web page was loaded onto the browser. I started navigating the website to see if I could get any useful information which would aid me in my attack but nothing useful was obtained. I then started checking where the tabs would take me and only buscar tab was the one that was interesting to us because of the url. Then I decided to tried if I could get command execution by typing ls and indeed it was vulnerable to command execution. There were different resources which were visible on the web application.

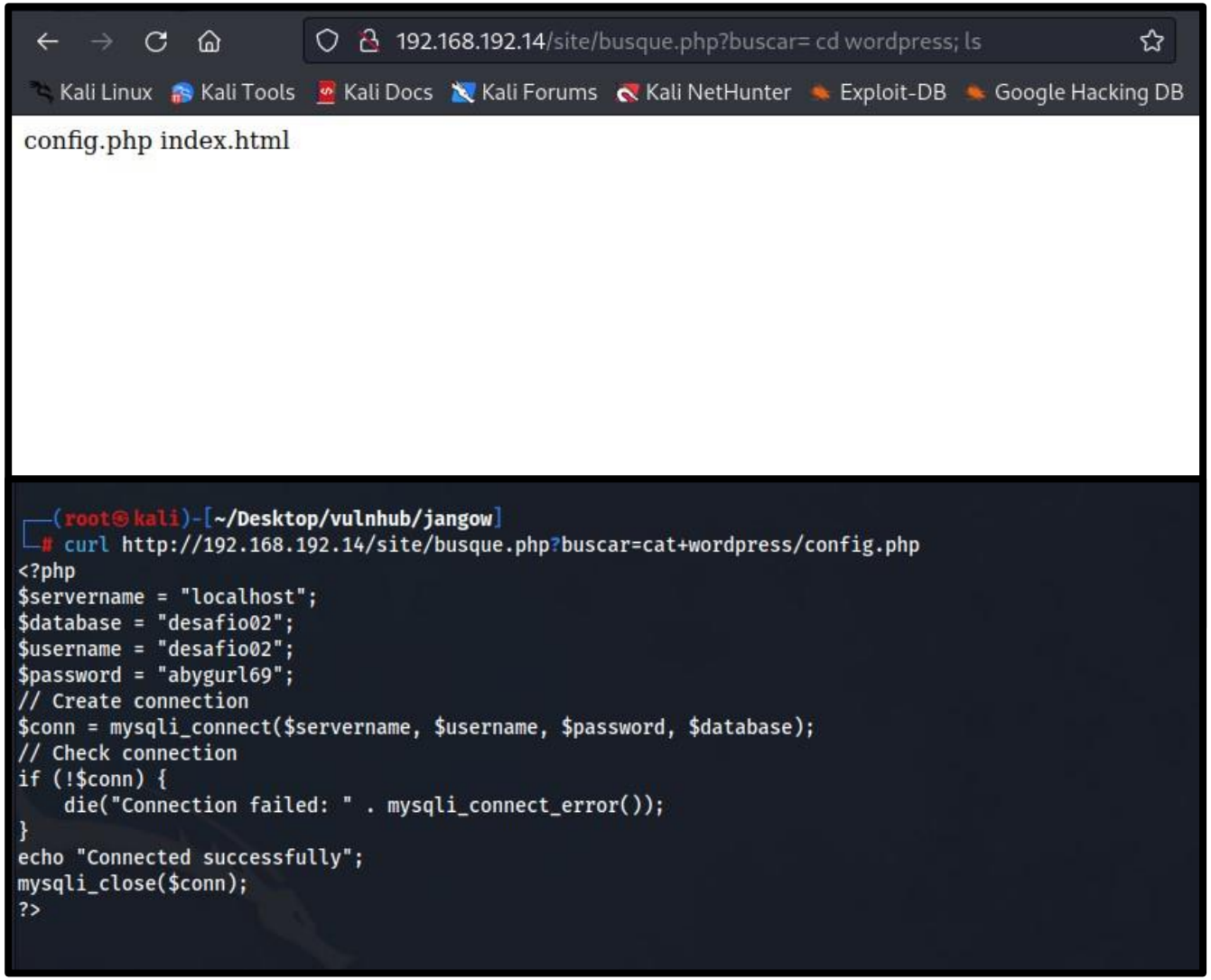
Author: Kharim Mchatta



I decide to look at each file and see if I could get any useful information but unfortunately there was nothing useful. Then, I decided to use Wpscan to scan the site perhaps I might get useful information but unfortunately Wpscan couldn't scan because it seemed the target ip address was not running WordPress, this could mean two things, either the web application is not really a WordPress site, or the system administrator had removed all WordPress signature from the web applications which made Wpscan to think that the target web application is not a WordPress site and not scan it.

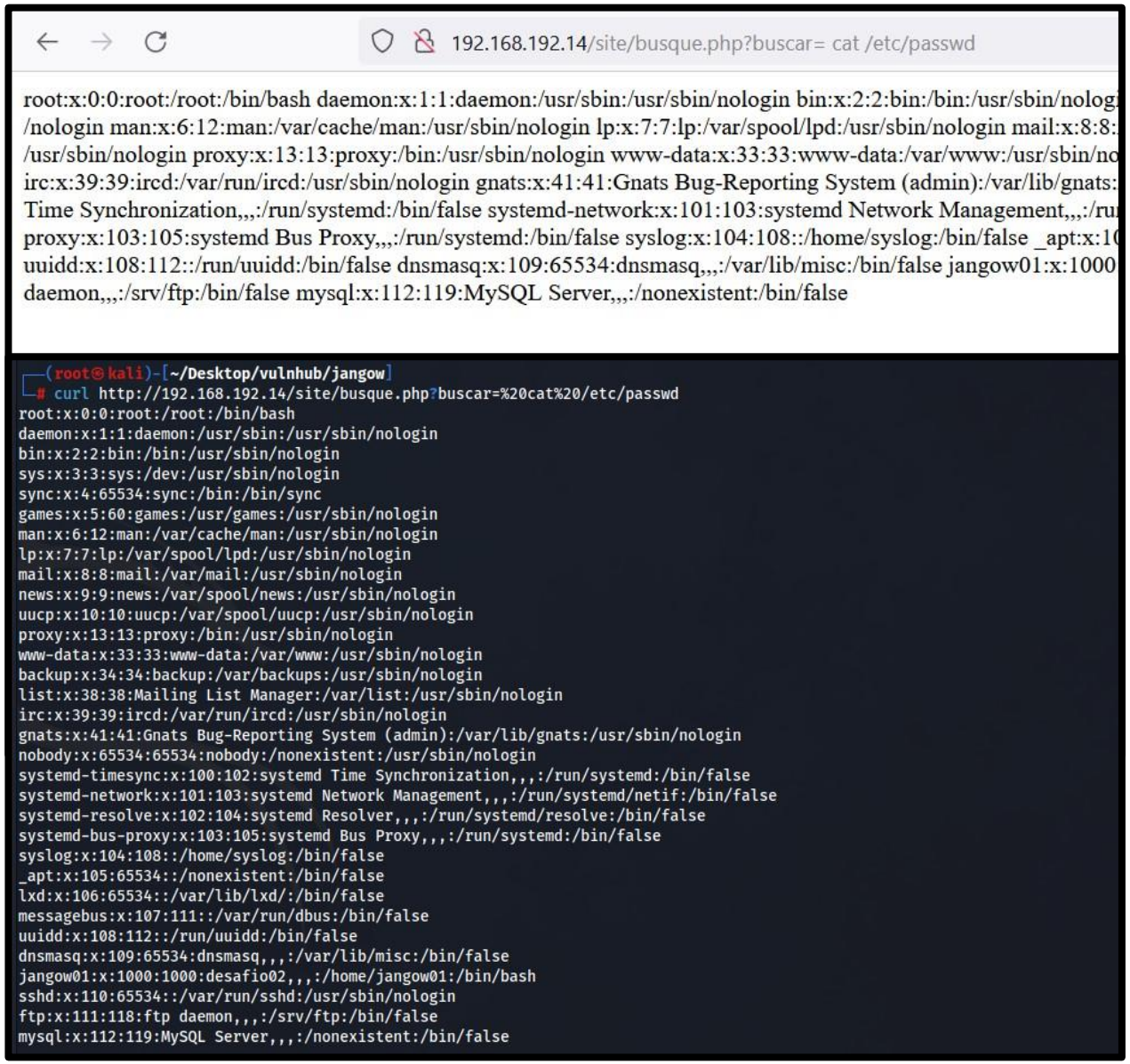


The next step I took was to try and do content discovery so that we can get hidden directory and to do this I used a tool called dirsearch. After running the tool, there was nothing interesting because all the results we see from dirsearch we had already discovered them manually from the web application by doing command execution, hence another dead end.



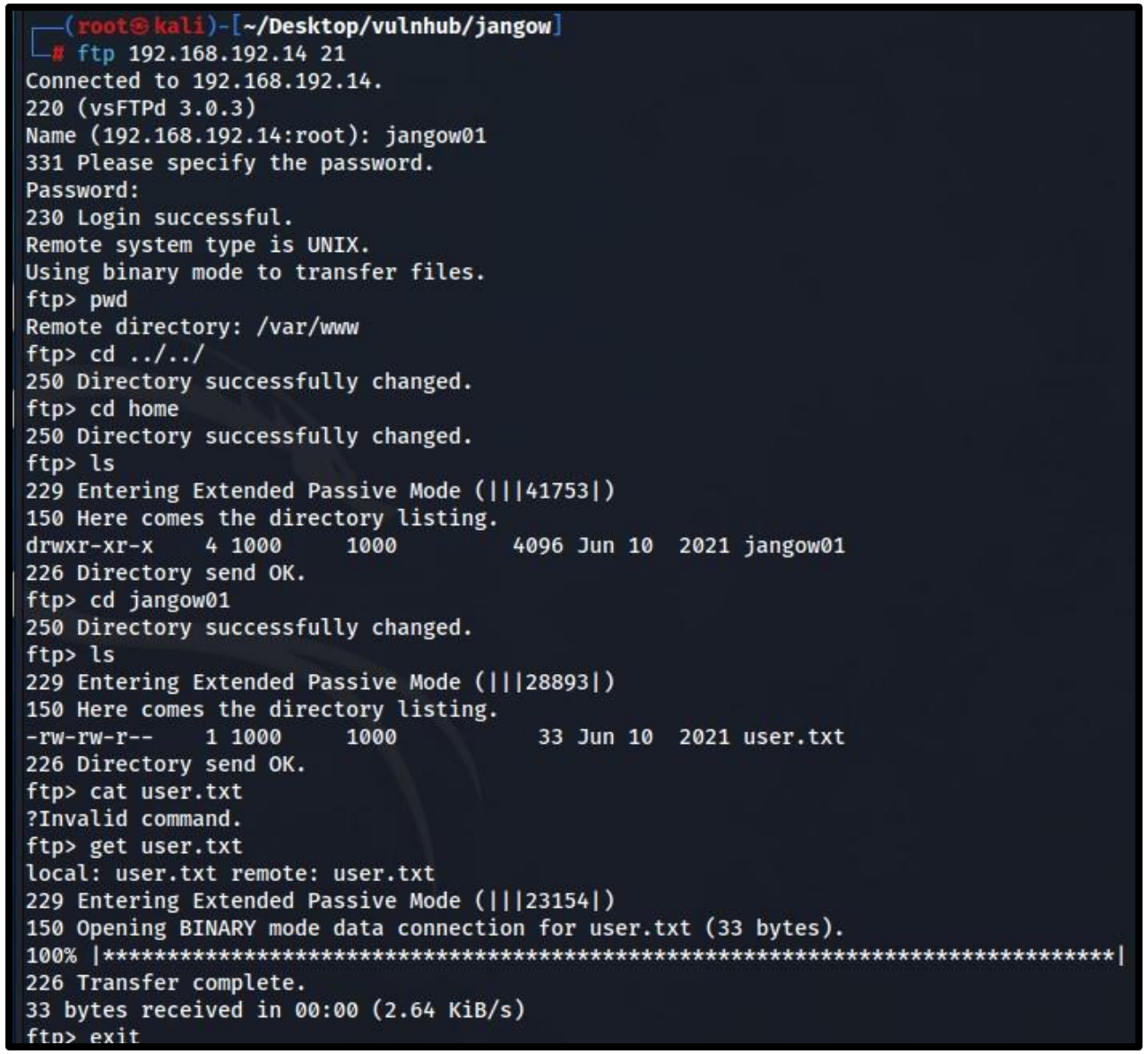
The next step was to get back to the place where we I initially found the command execution and tried to see if I can list the content of the WordPress directory by running the command **cd wordpress; ls** and there were two more files, config.php and index.html. The file of interest would be the config file which contains credentials to the database.

I tried reading the file from the browser but for some reason my browser was acting up or was it the box am not sure, but I decided to read the file using a command line tool called curl and I managed to get the credentials of the database



After retrieving the database credentials, I tried to test for credentials re-use and see if perhaps the administrator might have used the same credentials for the ftp service but that didn't work hence, I tried to read the /etc/passwd file to see what users are in the system by typing **cat /etc/passwd.** The reason why I used the terminal was for better view of the output compared from the browser. After looking at the content I saw that there was a used called jangow01 that had access to the ssh service but unfortunately port 22 was not opened.

Author: Kharim Mchatta



So, I tried to test for password reuse, I took the ssh username which was jangow01 and used the password that we had found on the WordPress configuration file abygurl69 and I managed to get access into the ftp services. Once I logged in I changed directory to home/jangow01 and there was the user.txt file and that marked the end of the journey.

Summary

---

1. Perform nmap
2. Access the web application
3. Find the vulnerable endpoint
4. Perform command execution
5. Get the configuration file
6. Retrieve the credentials
7. Check the /etc/password file
8. Get the username
9. Test for password re-use
10. Gain access to the ftp server and get the user flag

Author: Kharim Mchatta