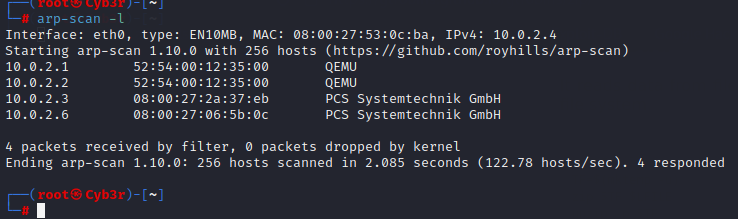
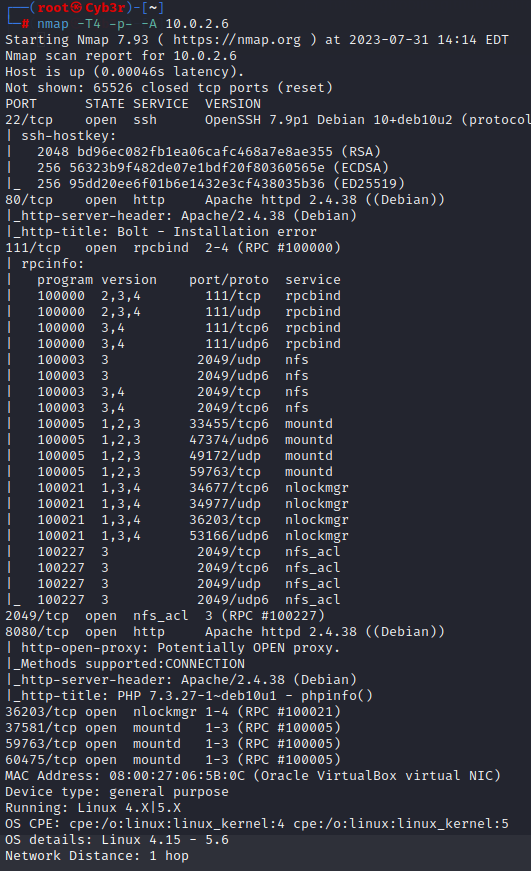
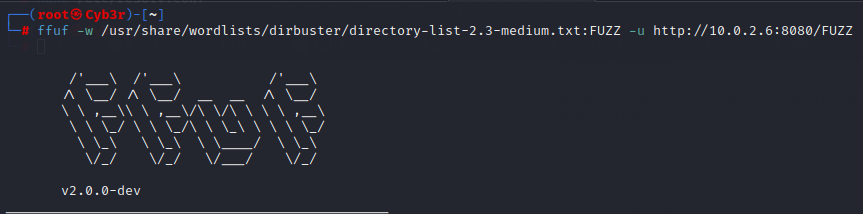
**DEV**

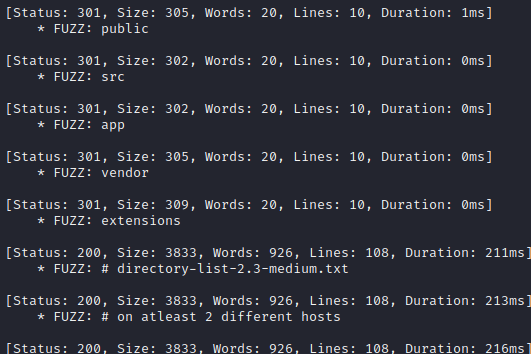


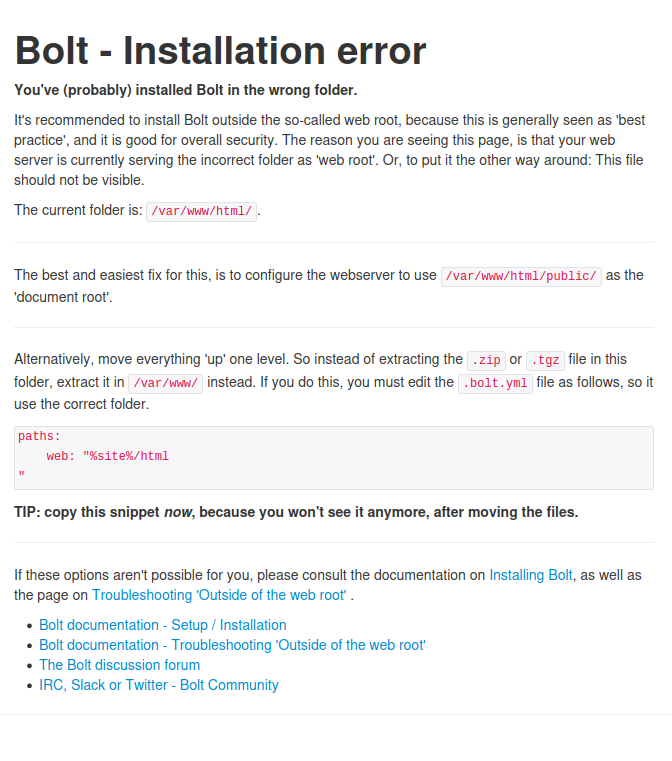


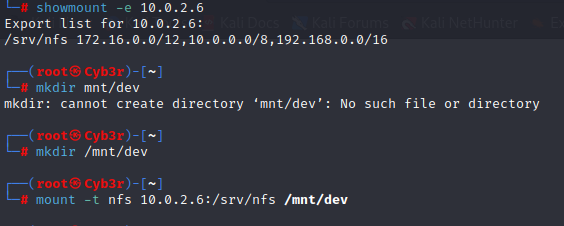


Fuzz the IP address and port 8080 because it is opened

Using the result from ffuf and the next image is the result of fuzzing port 8080 and adding the /app and others

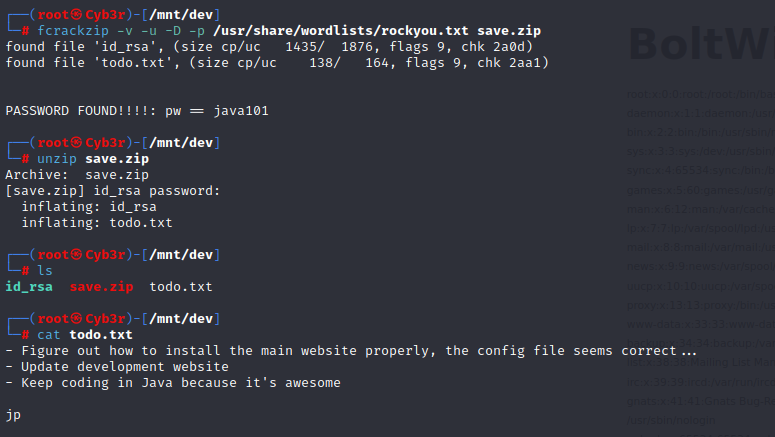






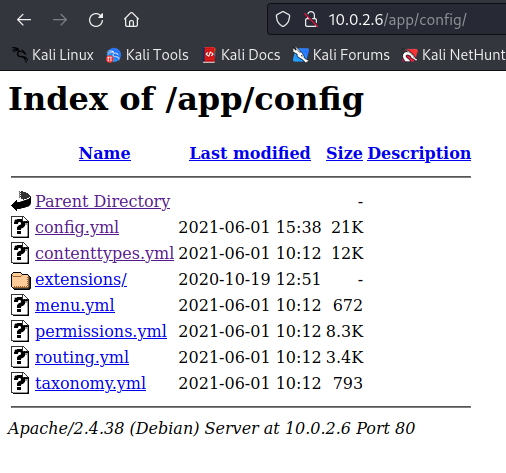
Mount command because the port for nfs is open. We create a folder and another called mnt/dev



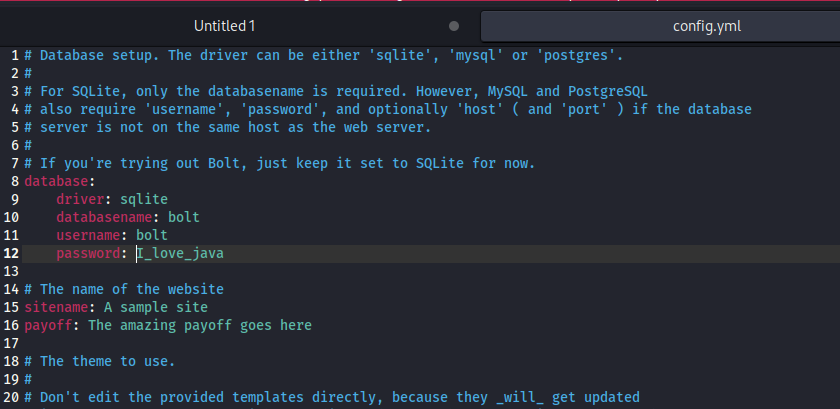


Id\_rsa file is used for ssh connection. Save.zip unzipped and the text file is catted.

This is the output of the IP on the web

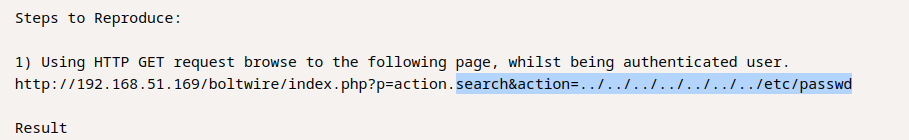


Download the config.yml file and then view it

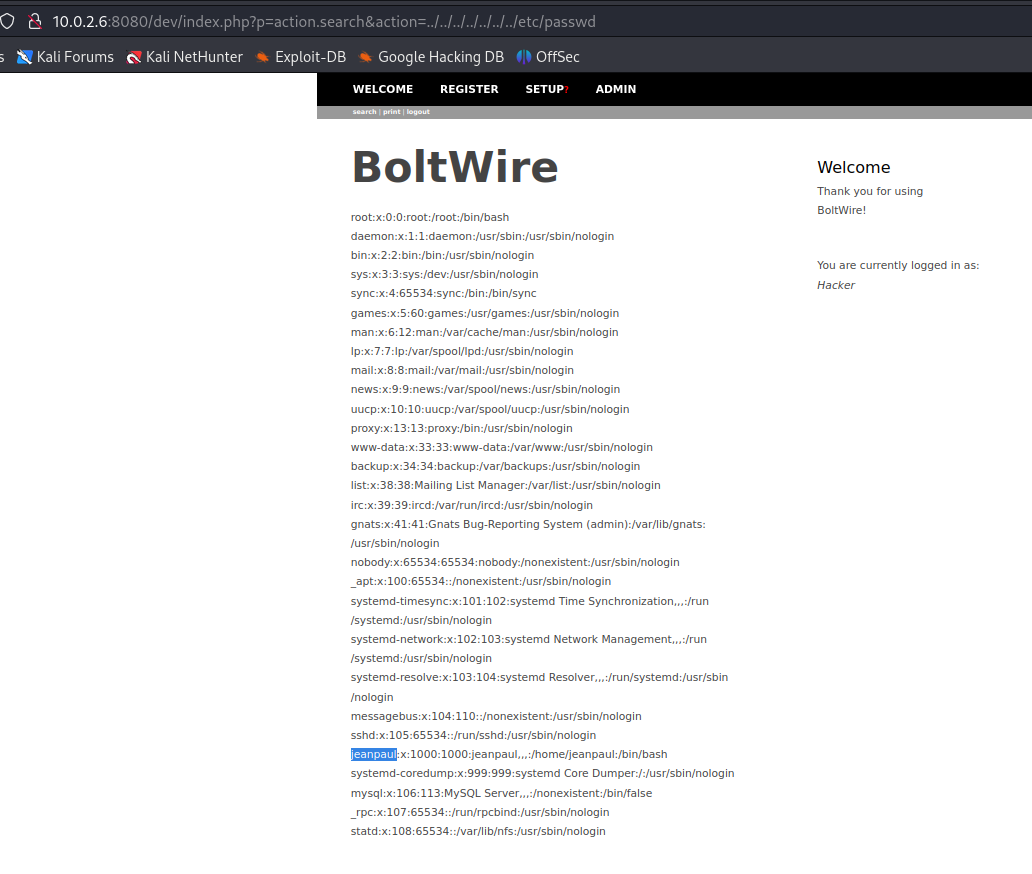




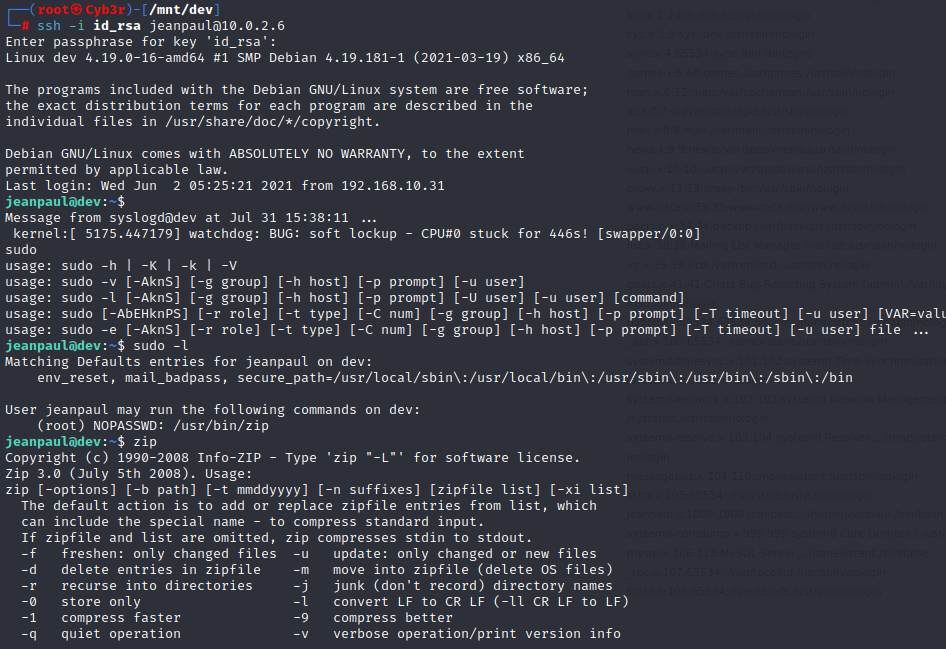
After confirming the exploit exists on Exploit DB, we go below to see how to reproduce it



Next we create an account on the site and then add it on the url. The ../../ takes us back to the very beginning of things. This is the result



The highlighted part is a username. Next we can try SSh to see if we are able to connect.



Sssh –I id\_rsa [jeanpaul@10.0.2.6](mailto:jeanpaul@10.0.2.6)... Jeanpaul is from the highlighted stuff above and the todo note, the password I love Java is from the config.yml file

Also, see that with sudo –l we see what we can do without root password, now we see we can do zip, so we go to GTFOBIN as shown below…. Click on sudo den scroll to zip and paste these commands one after the other on the same JP account and result is below

