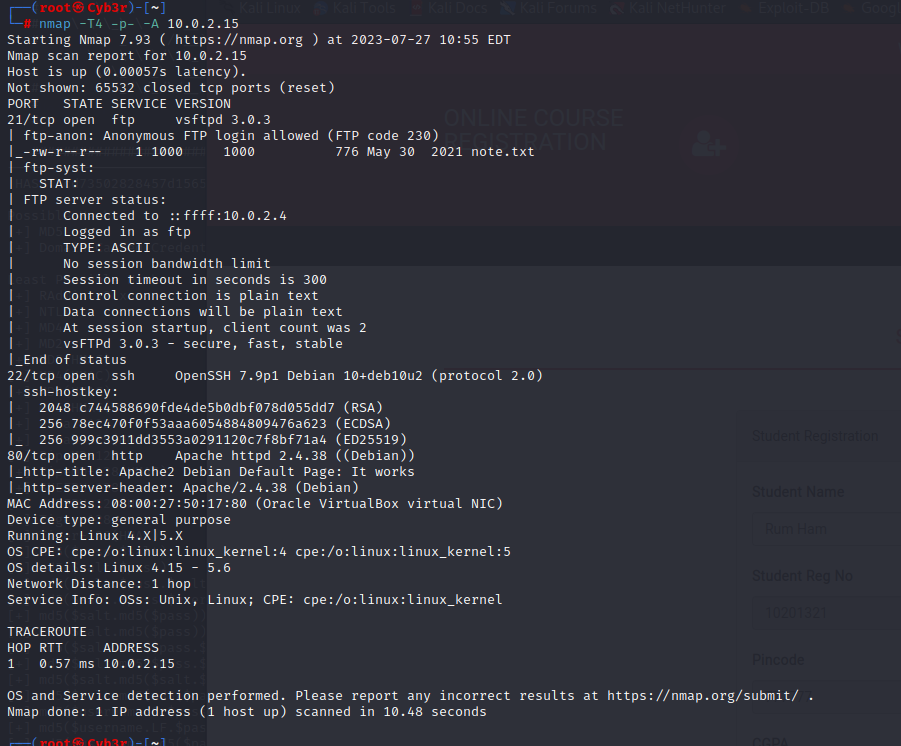
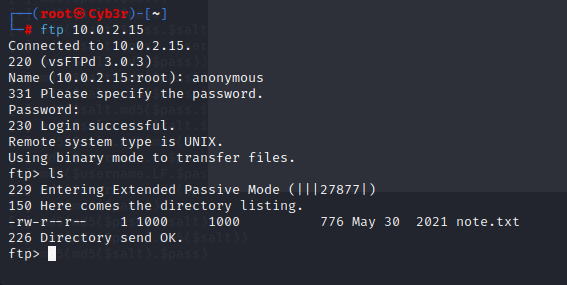
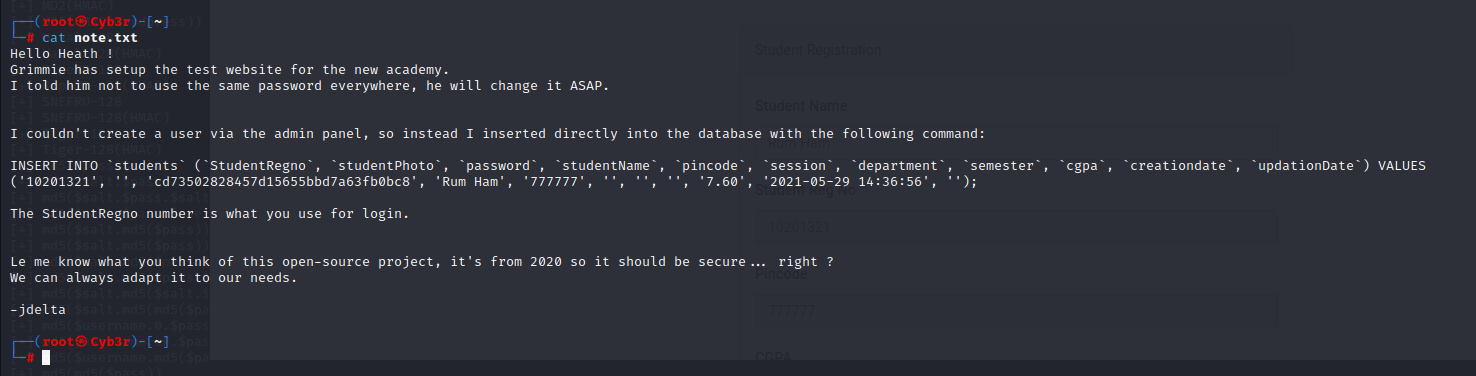
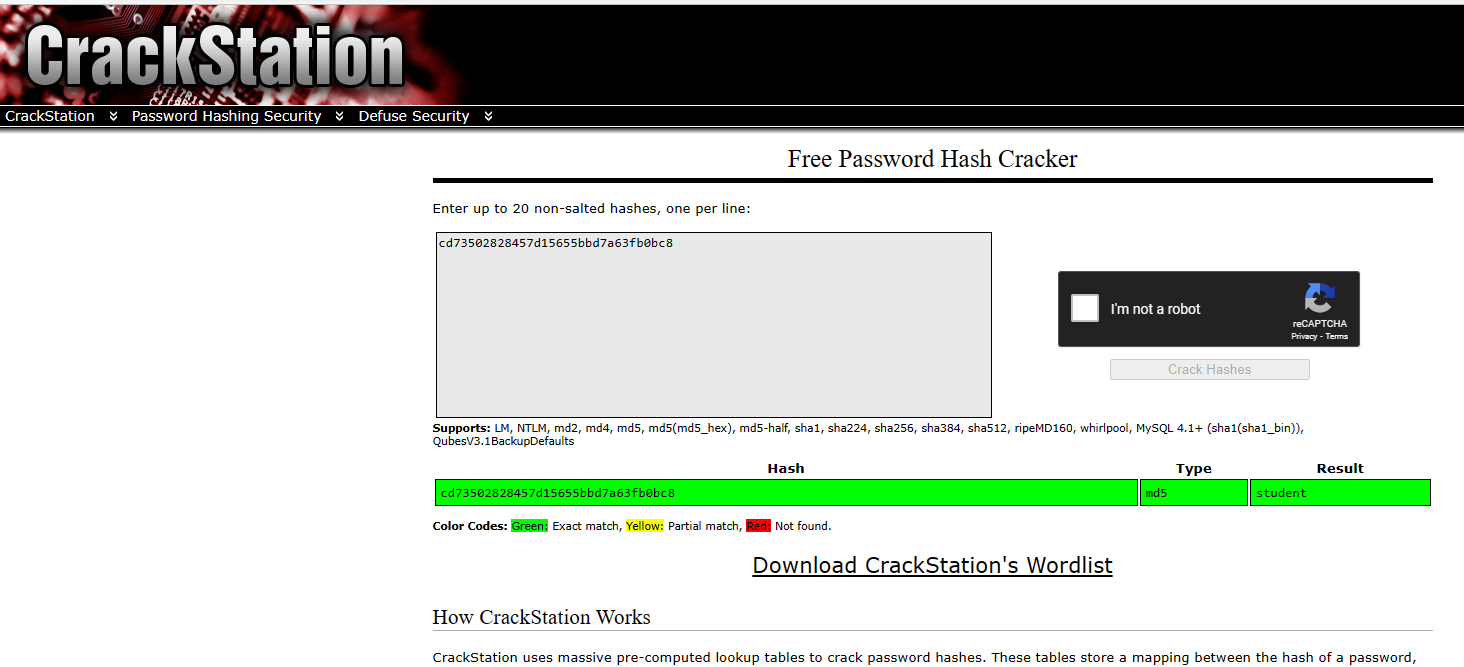
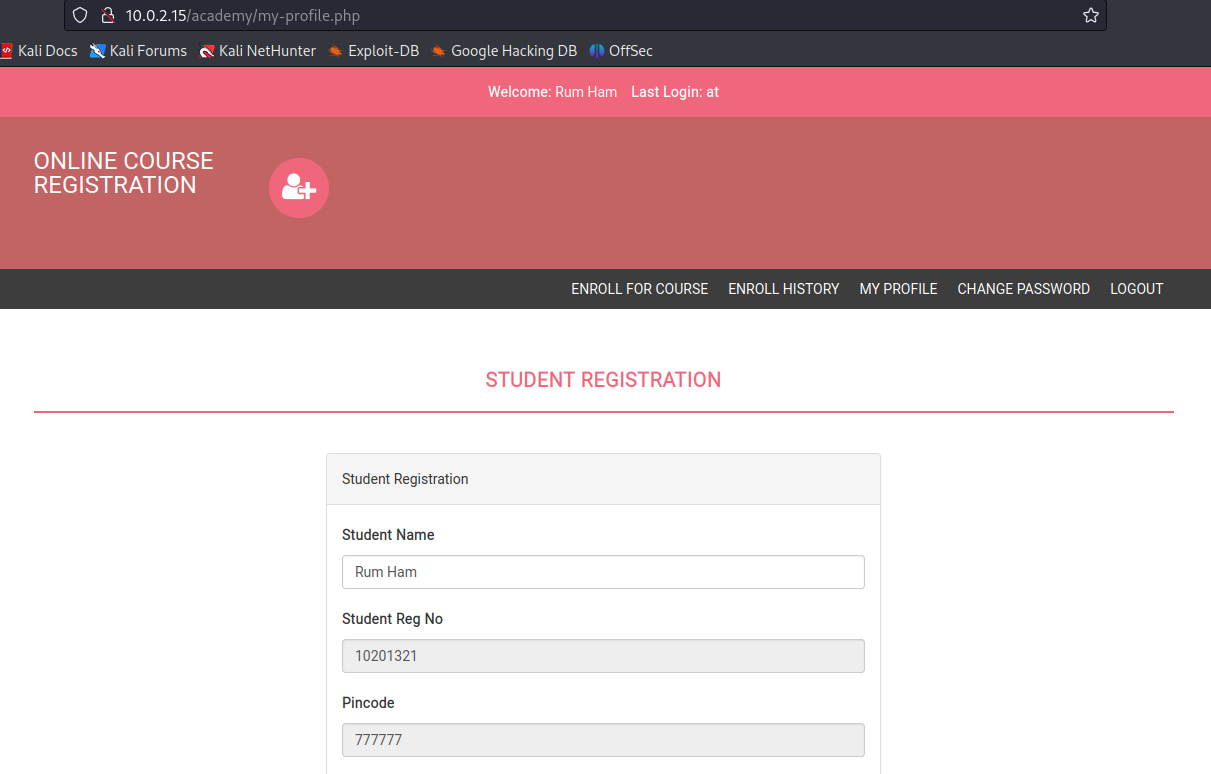
**Academy**

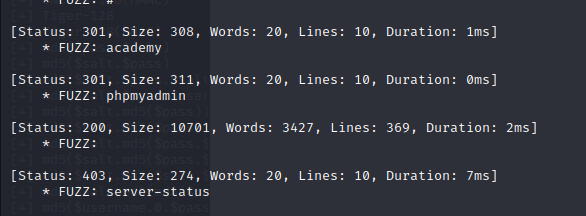


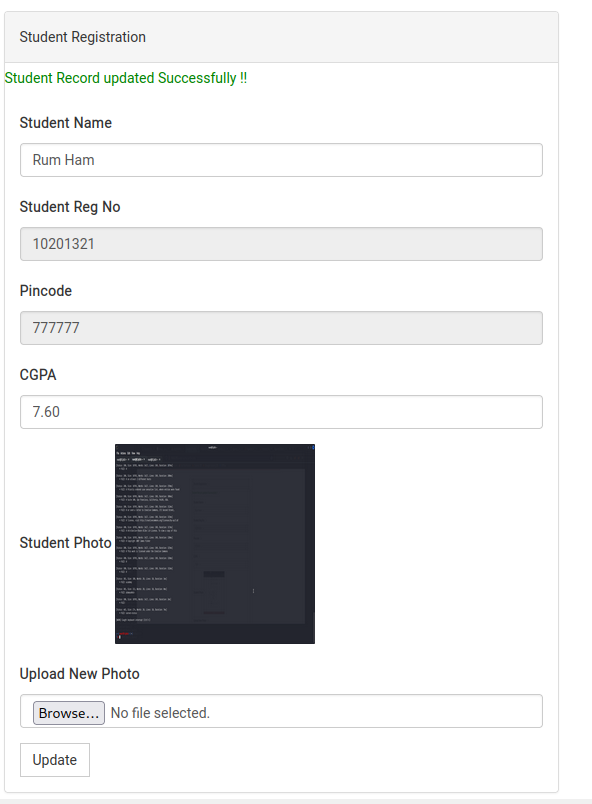




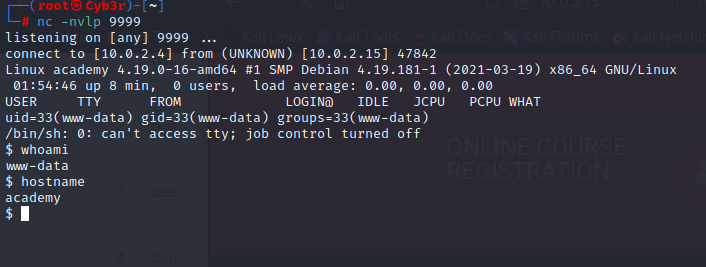




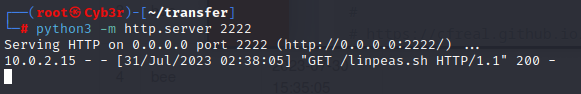




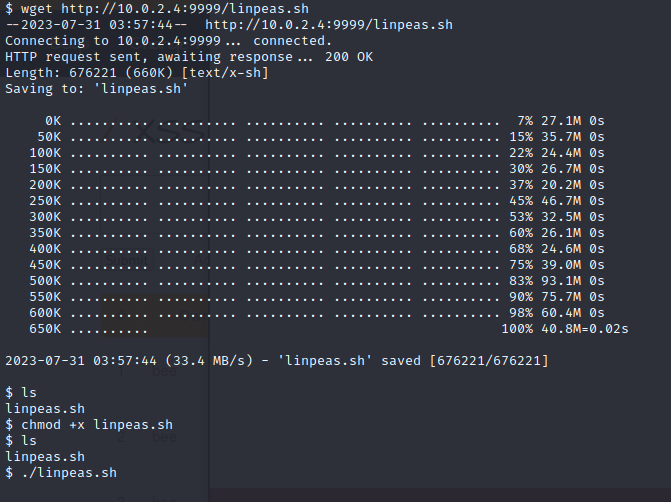
Using Pentestmonkey reverse shell git code, copy into a text file saved as .php and upload in place of images. Now run it. In this case, shell.php.



There is a shell after uploading the script instead of .img or jpg files

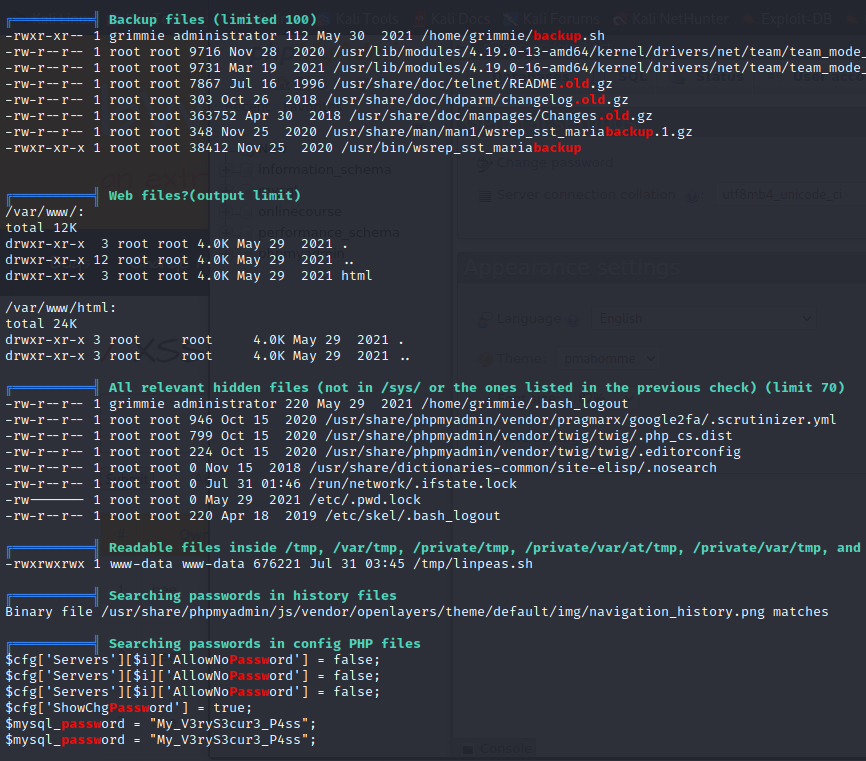


Above, host a python server then wget as shown below on same port

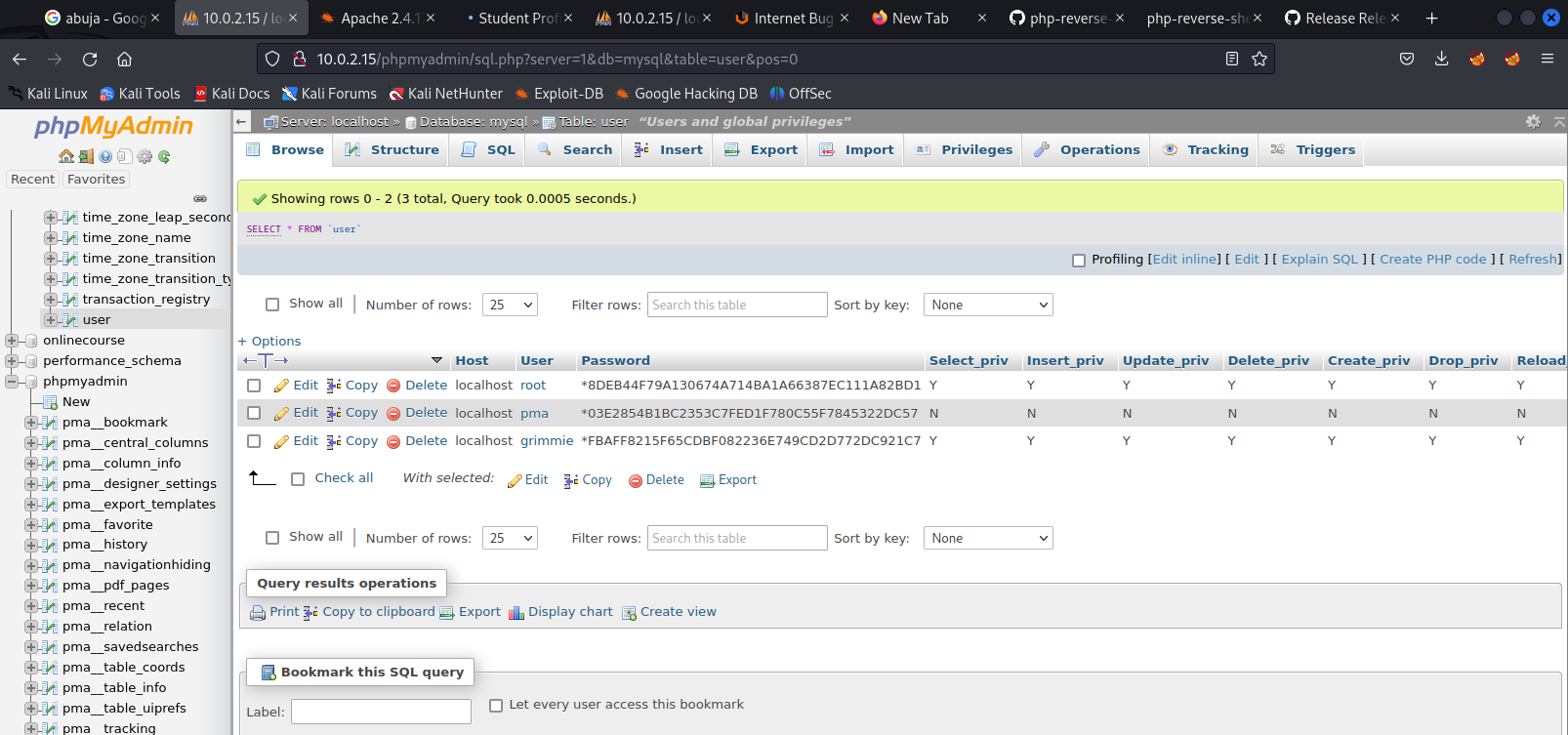


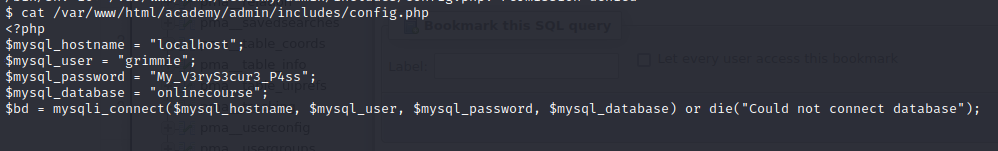
**Preferably download the file instead of copying**

**Ensure to host python server in same directory as linpeas**

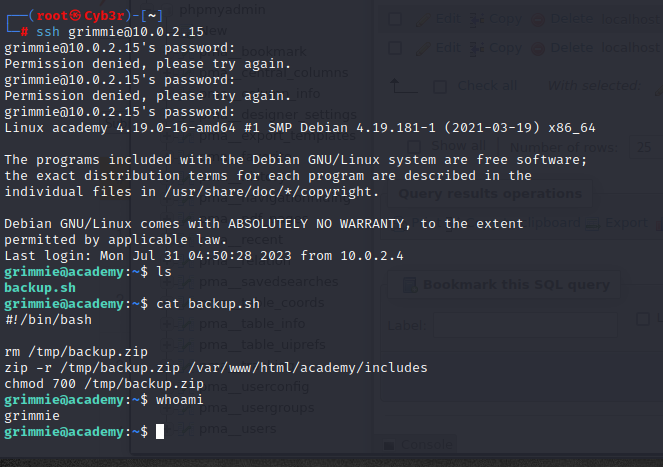


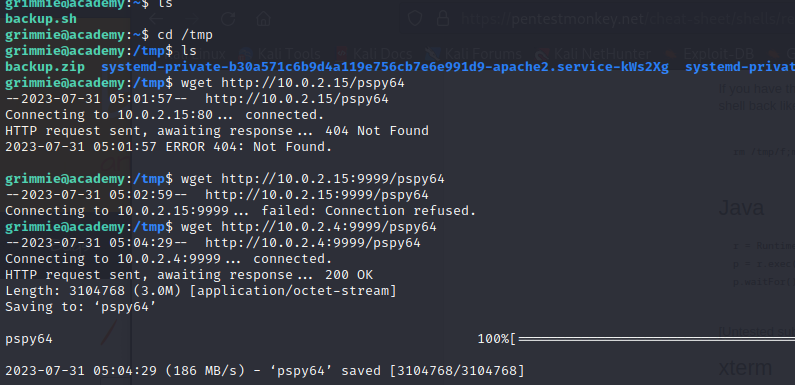
The name Grimme appeared a lot and I just guessed using the name and the password below and I got admin access to the Database as shown below

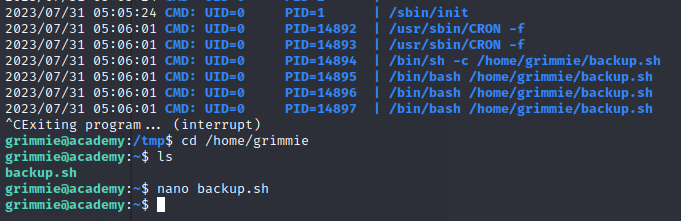




Found this file and it confirms the above



pspy is to ensure a process in particular is still running and in this case, grimmie’s backup.sh… download the static 64bit pspy



Also notice we opened backup.sh and we edited it with ‘bash reverse shell one liner and made few edits to the script’. Just save it but b4 then open a nc –nvlp on same port as b4 here 9999 and then update backup.sh and walla we have root

