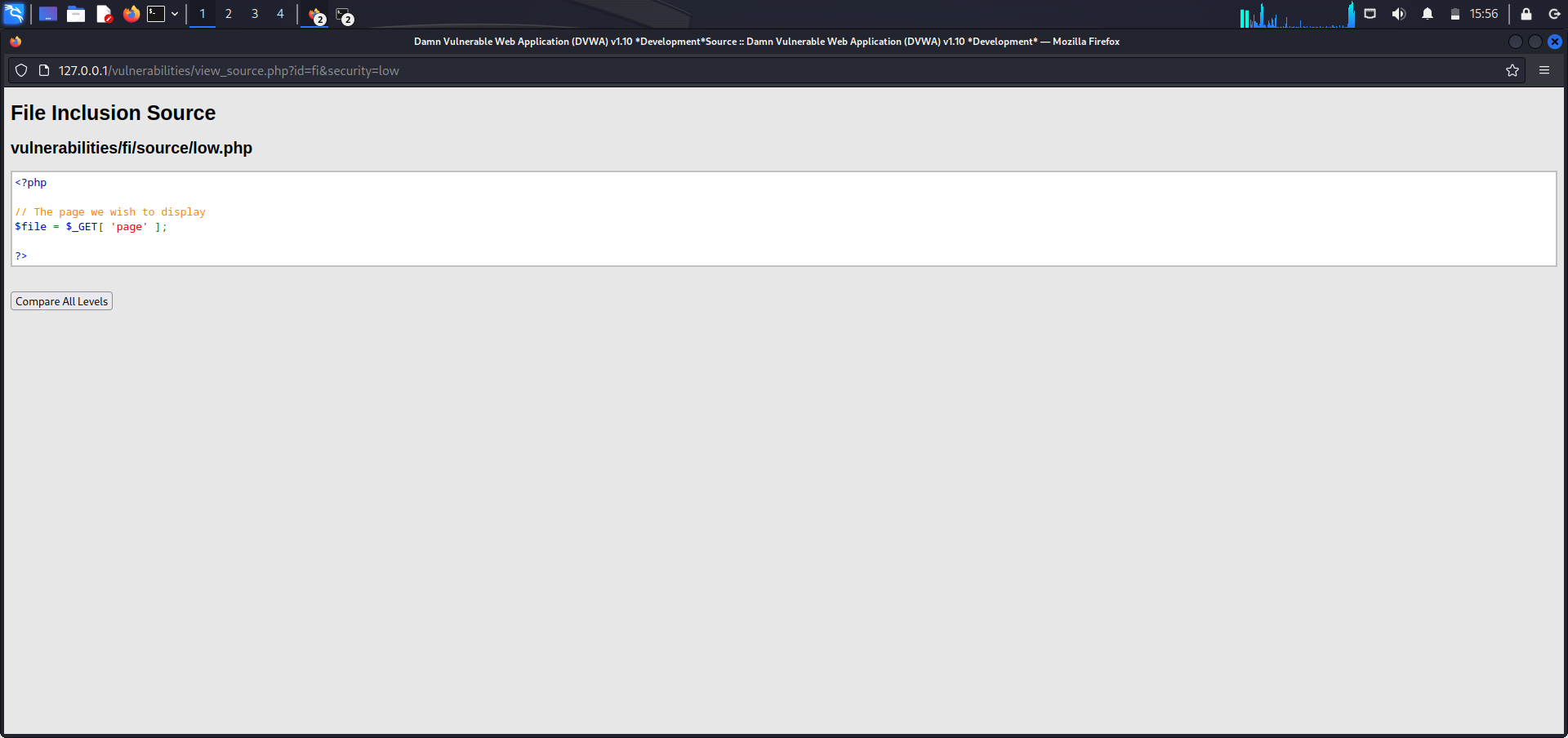
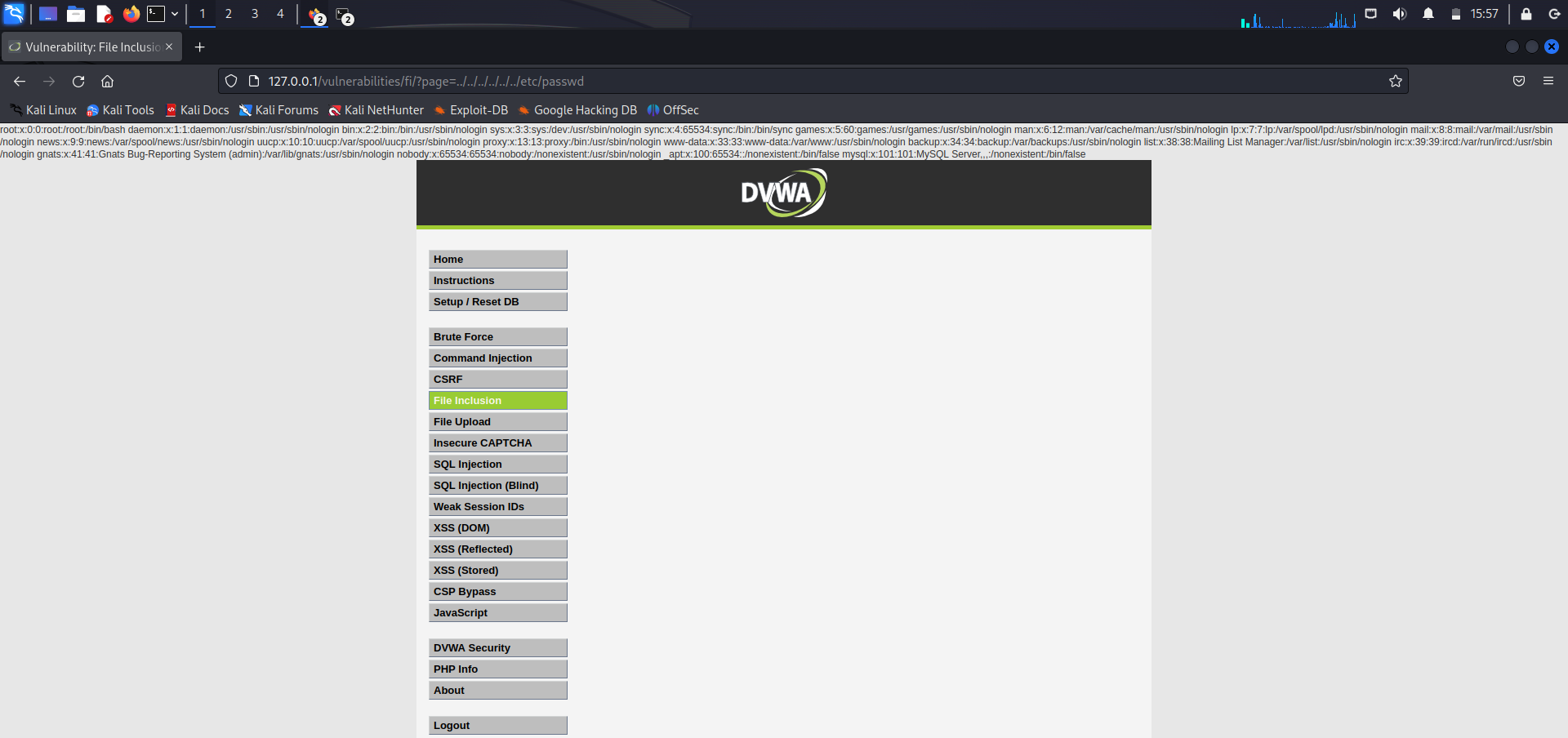
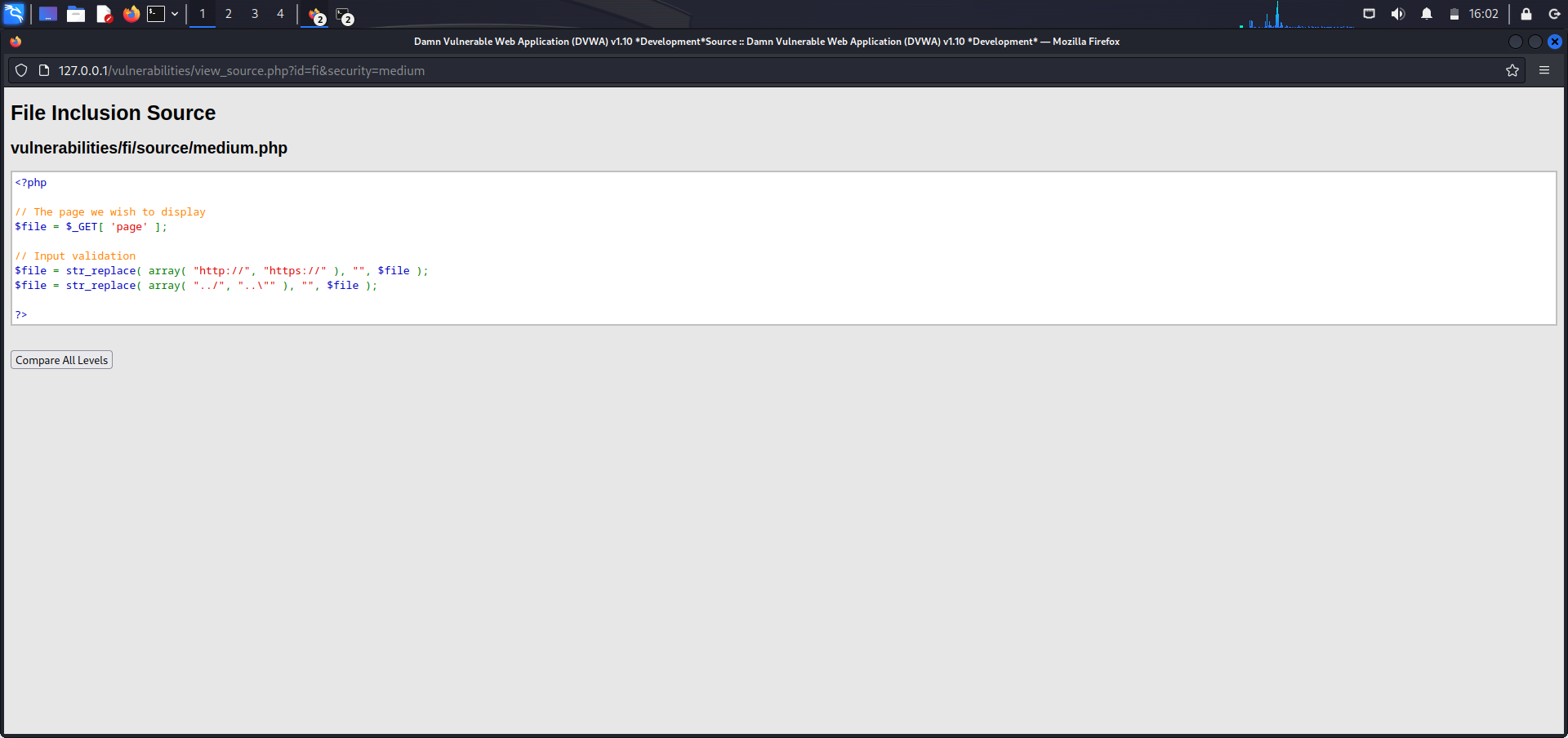
Lfi/rfi

Spencer wise

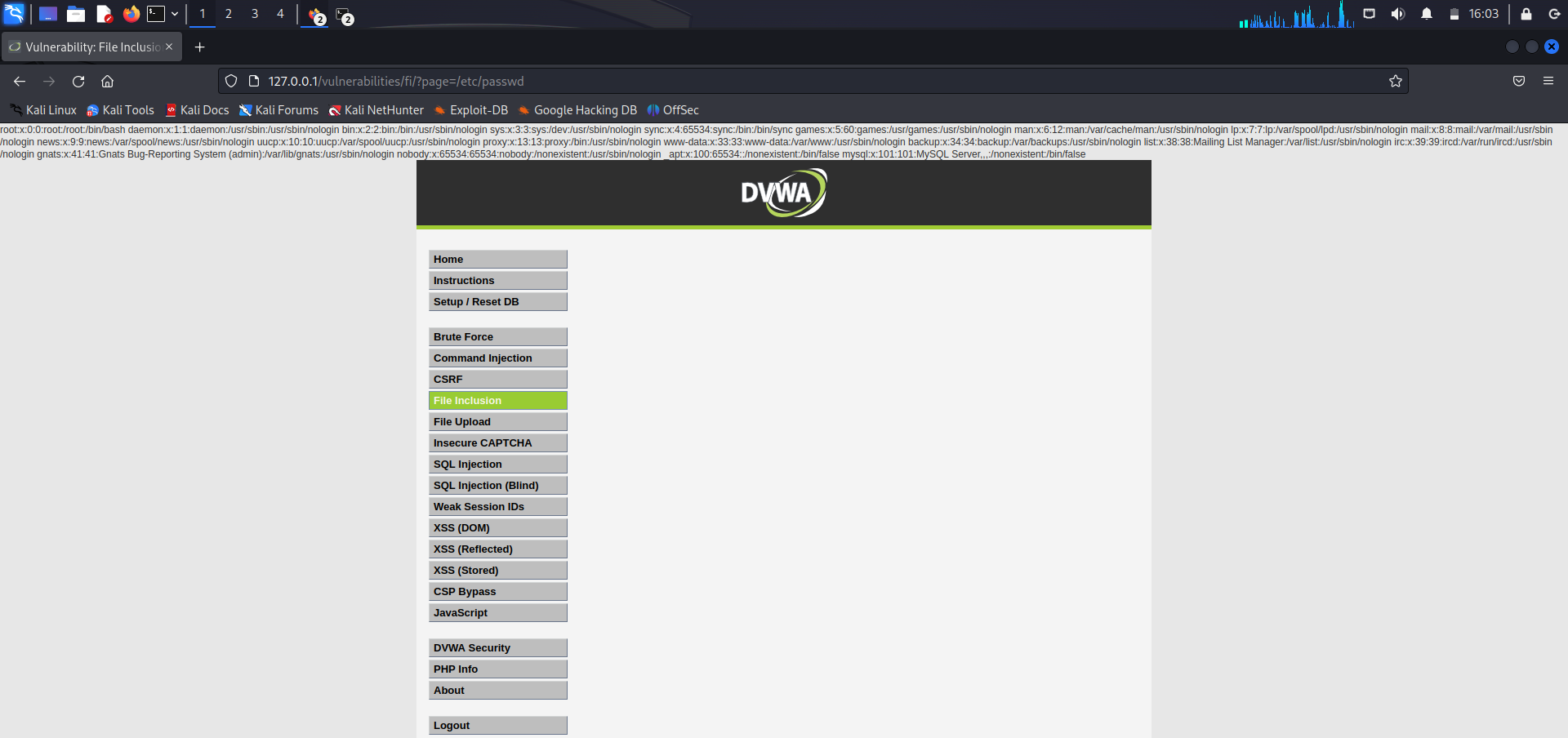


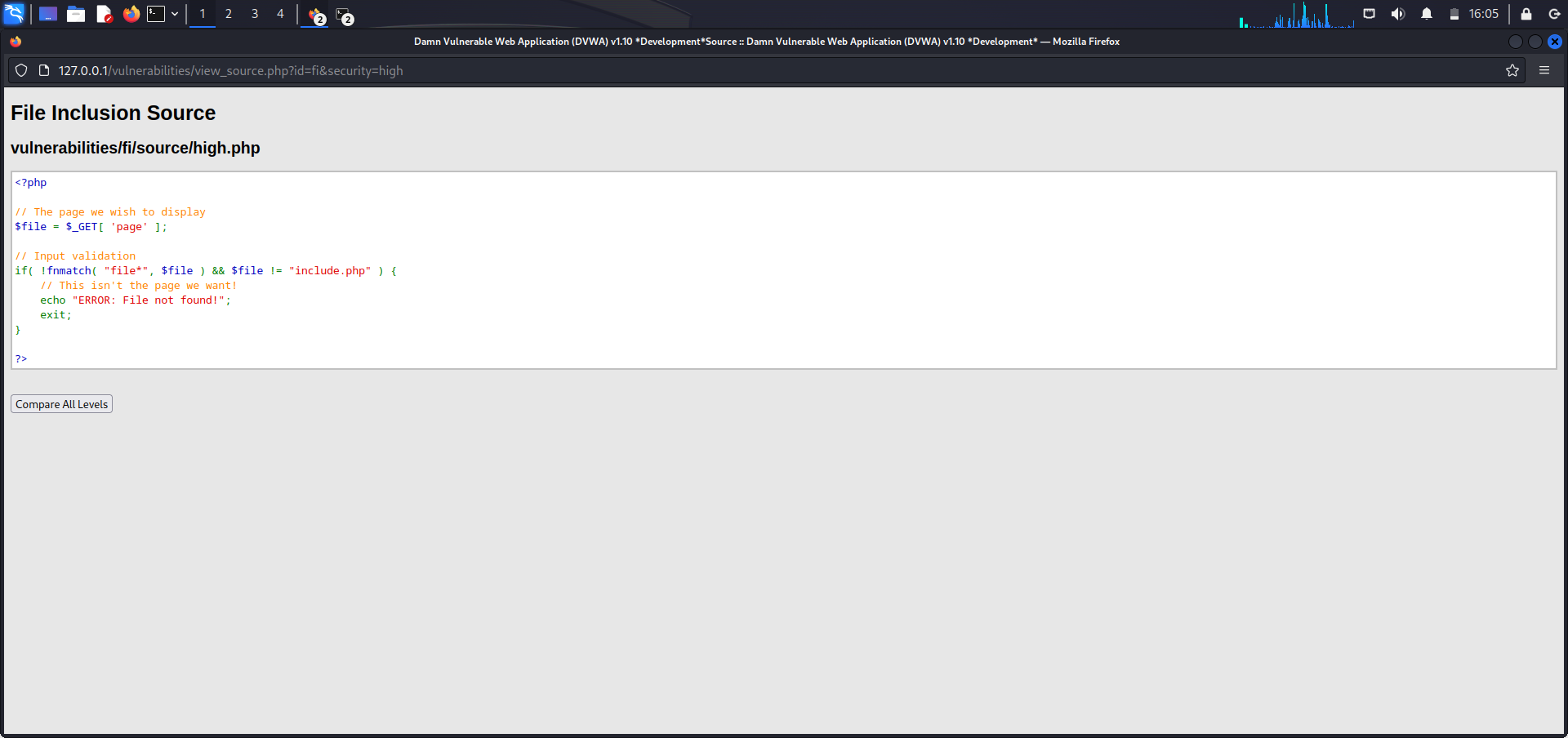
On low security there is no input validation to exploit the LFI vulnerability. I modified the url by adding ../../../../../../etc/passwd to reveal the sensitive information. Seen below.



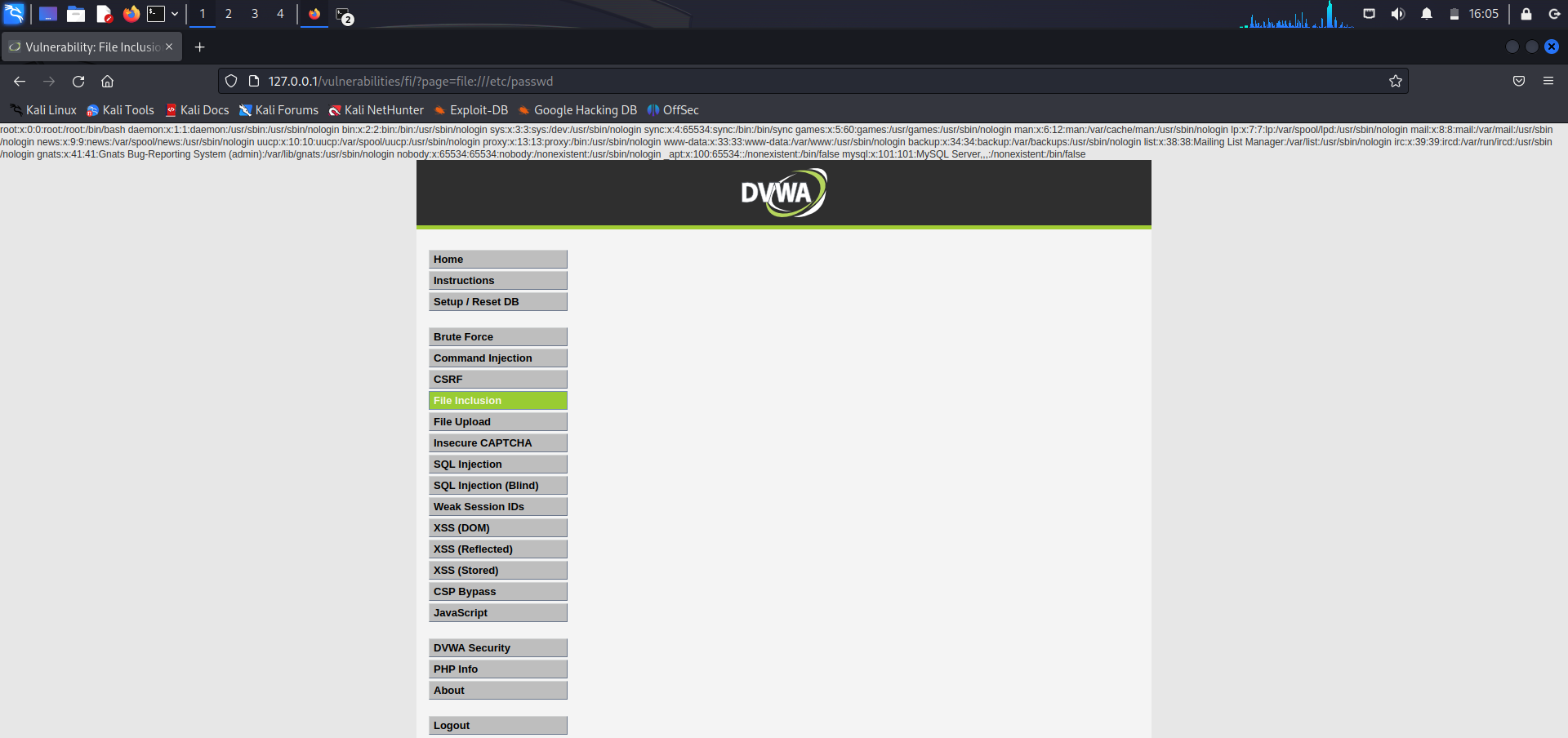


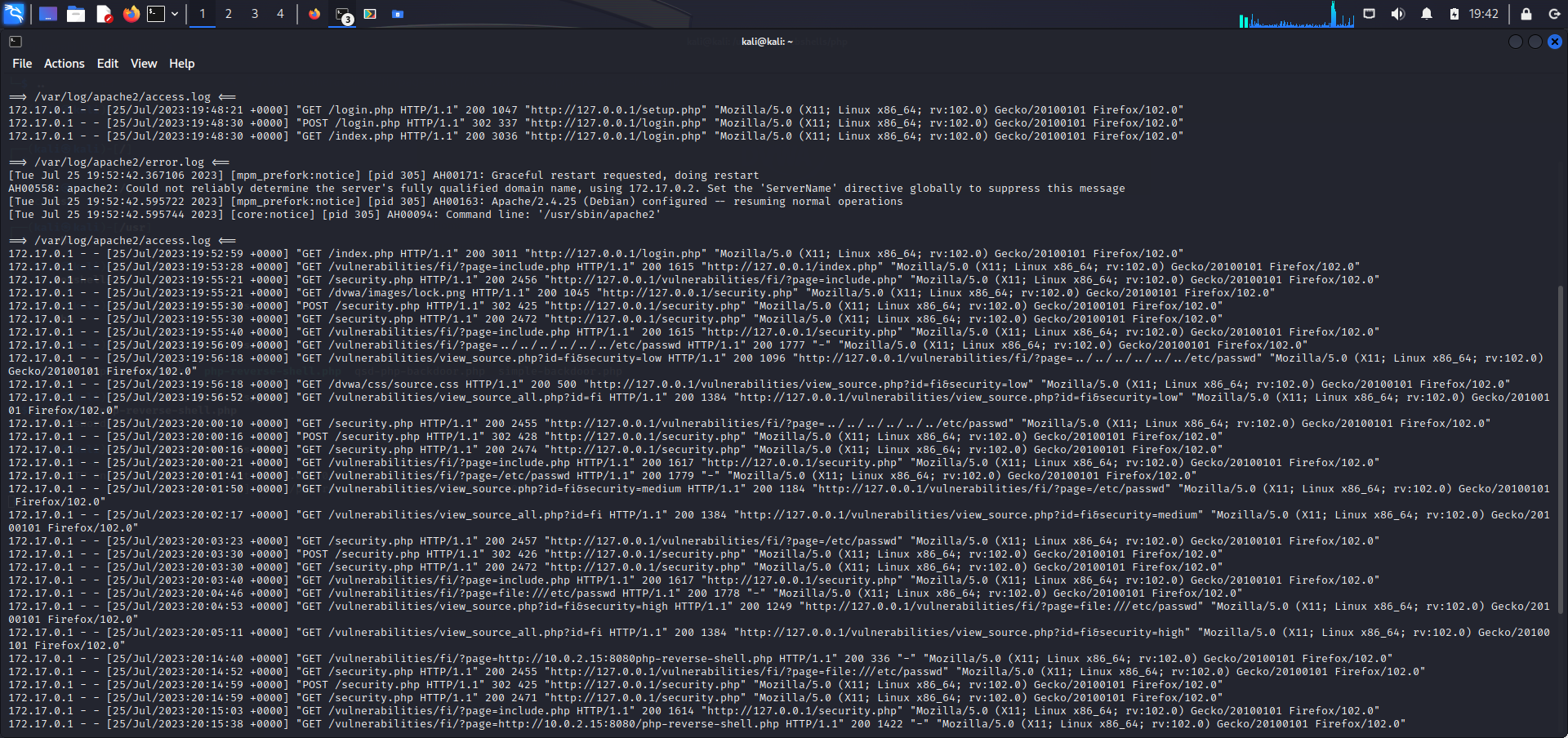
Medium security the server filters the pattern I used on low security (../ ..\) so I modify with /etc/passwd. As seen below.



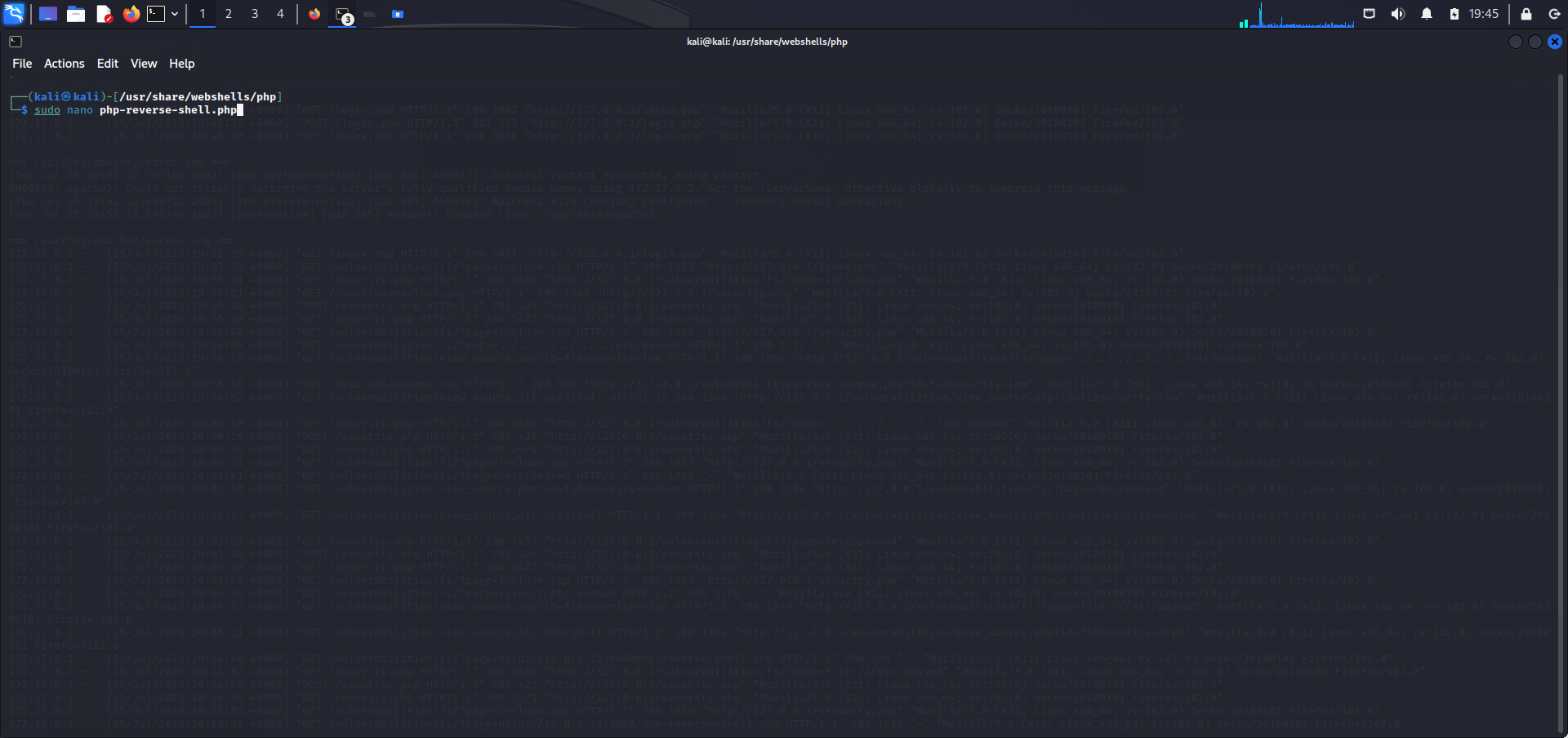


On high security, the server is only accepting “include.php” or inputs starting with the word “file”. So I modify the URL to ?page=file:///etc/passwd as seen below.

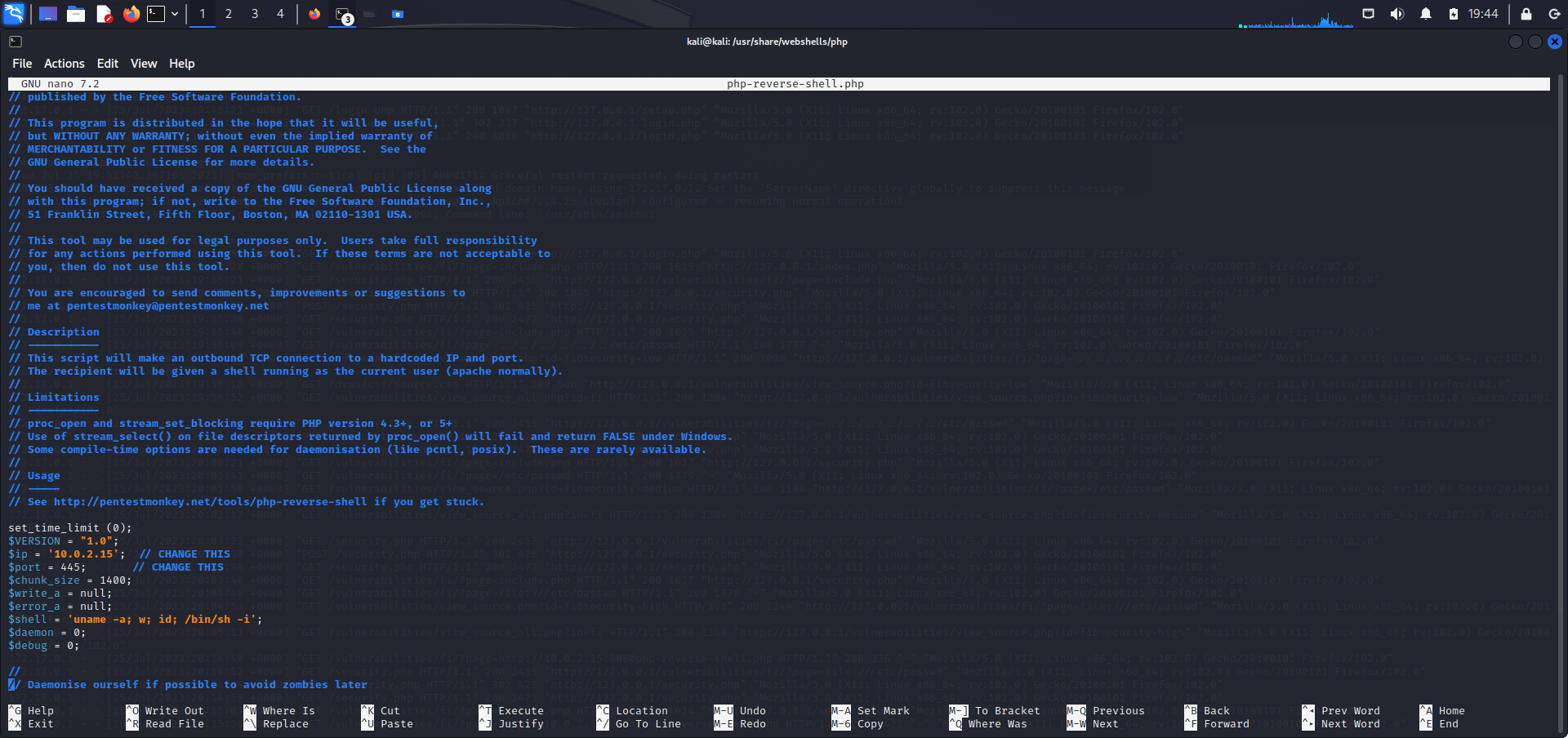




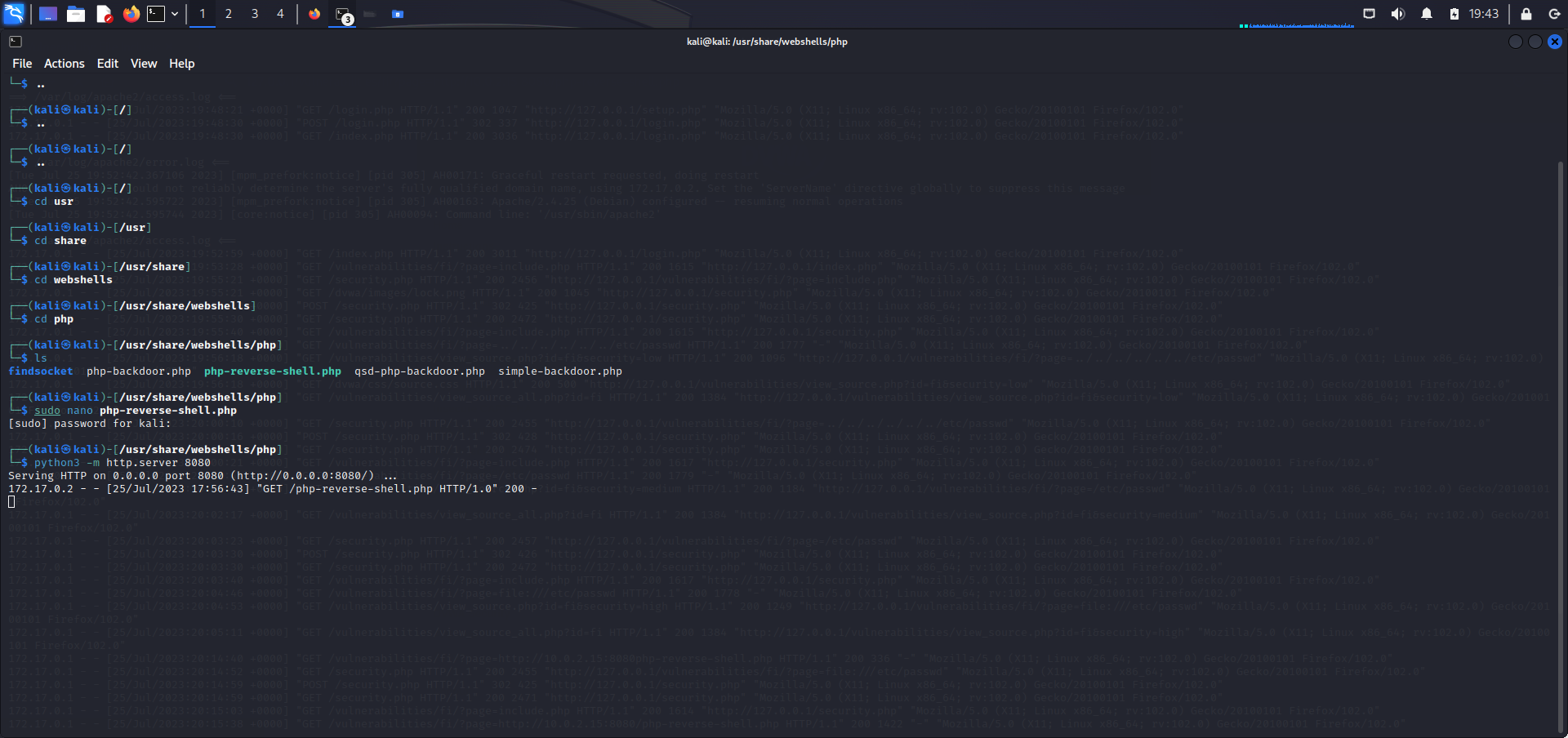
Everything done on DVWA site was logged on my Kali machine.



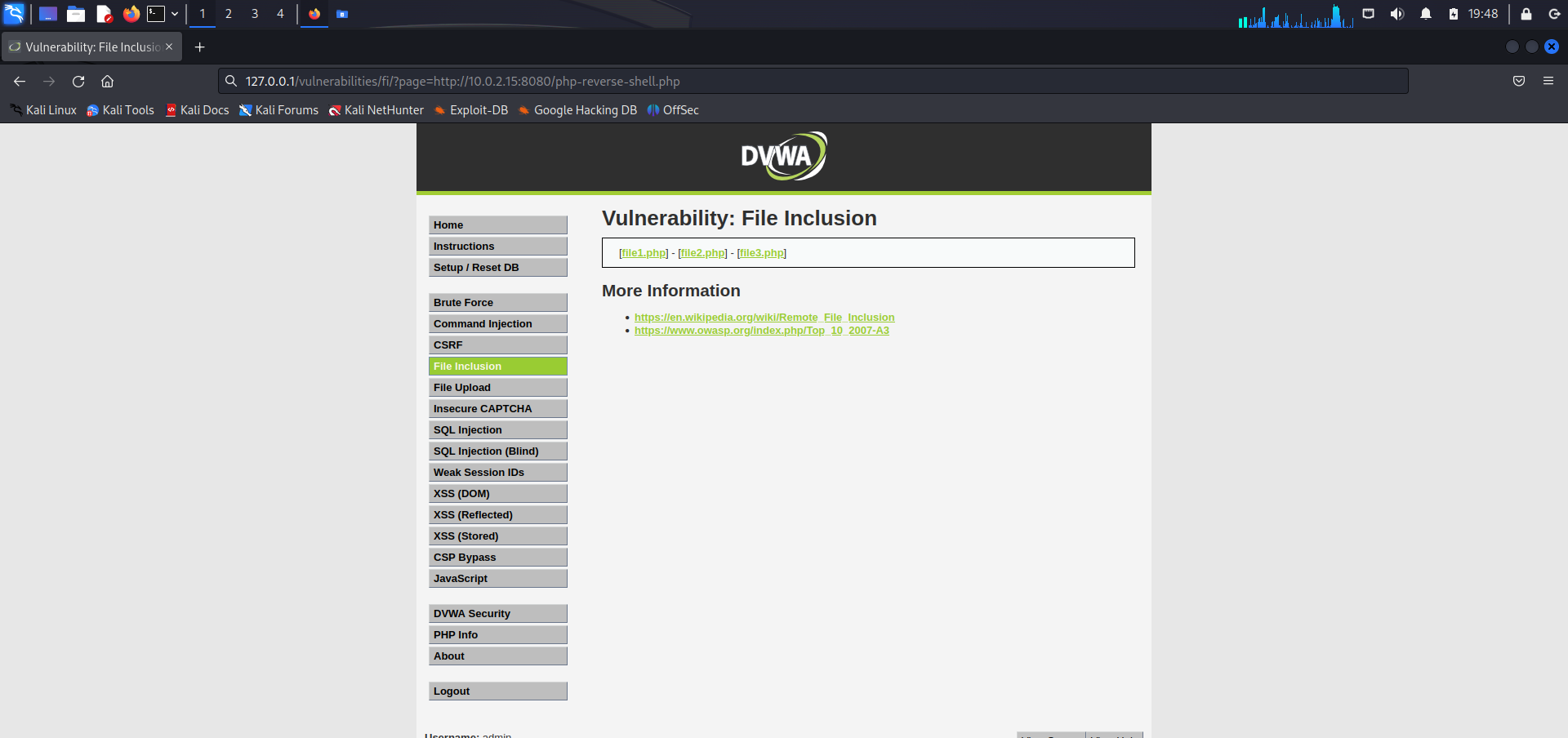
For RFI I navigate to webshells stored on my Kali machine. Then use the command sudo nano php-reverse-shell.php to open the shell I want to execute.



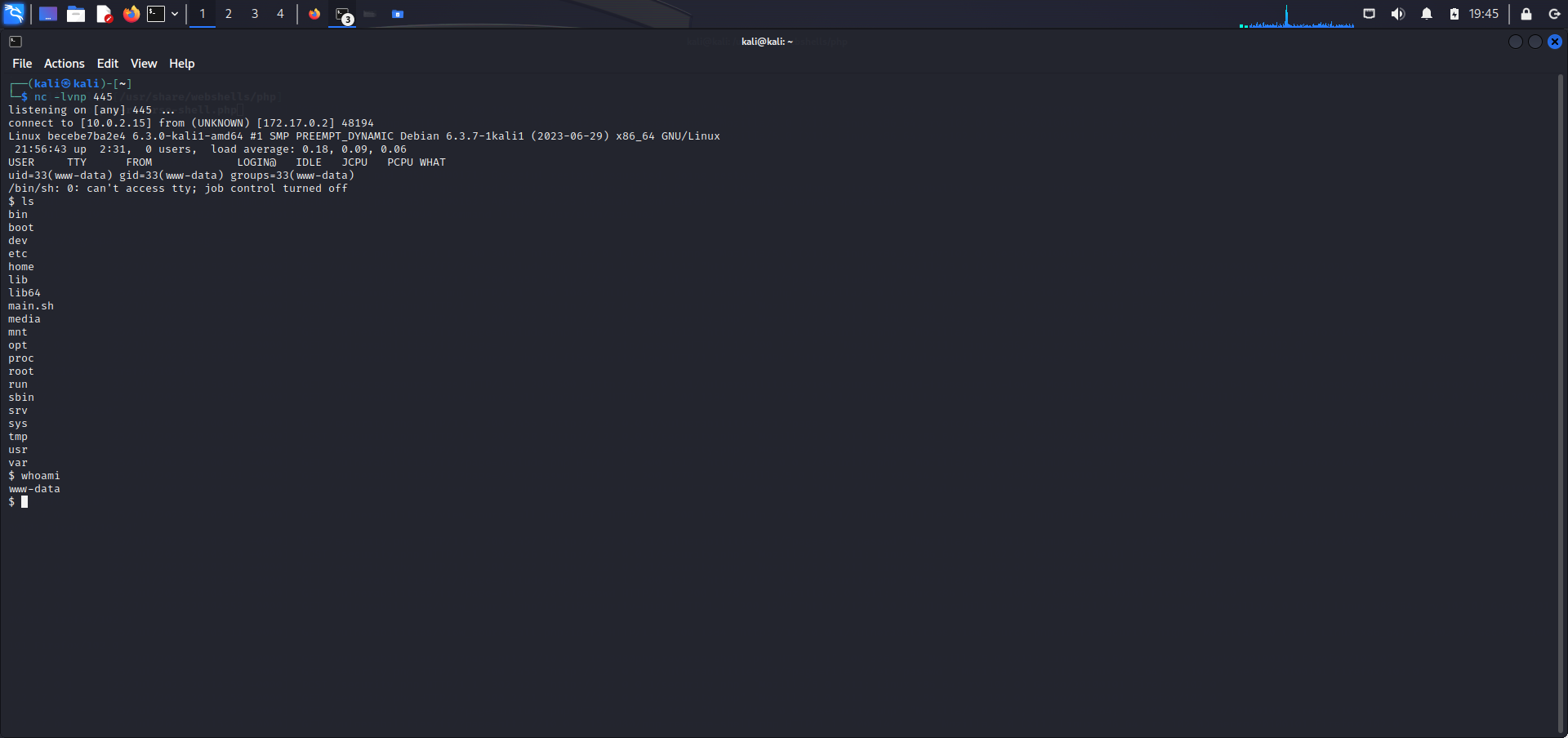
I modify the specifications of the shell to my IP 10.0.2.15 and the port I want it ran through.



Then I launch a python server under the same directory to get a 200 response or an accepted action for the webshell.



I launch a netcat on port 445 (same port I specified on the webshell) for the purpose of gaining access remotely. On the DVWA site I modify the URL with instructions to get the webshell from my Kali machine and which port to get it from, also the file name.



I ls to see the directory list and use the whoami command to see tge user I am logged on as.

I am www-data