Am incercat sa dau ping la localhost sa vad ce se intampla.

Am observat ca pe pagina era fix output-ul de la comanda ping din bash, asa ca m-am gandit ca poate as putea cumva sa am acces la acest terminal si sa execut comenzi.

Cum input-ul pentru adresa ip era fix in fata mea, am incercat sa vad daca nu cumva e vulnerabil, asa ca am incercat sa scriu o comanda in continuarea comenzii ping:



N-am gasit ceva important prin fisiere, iar de printat index.php imi afisa iara site-ul, nu sursa in plain text.

Mi-am adus aminte ca pe home scria ca flag-urile se afla in /home/ctf/flag, asa ca am incercat sa caut acolo, iar dupa un cat am gasit:

