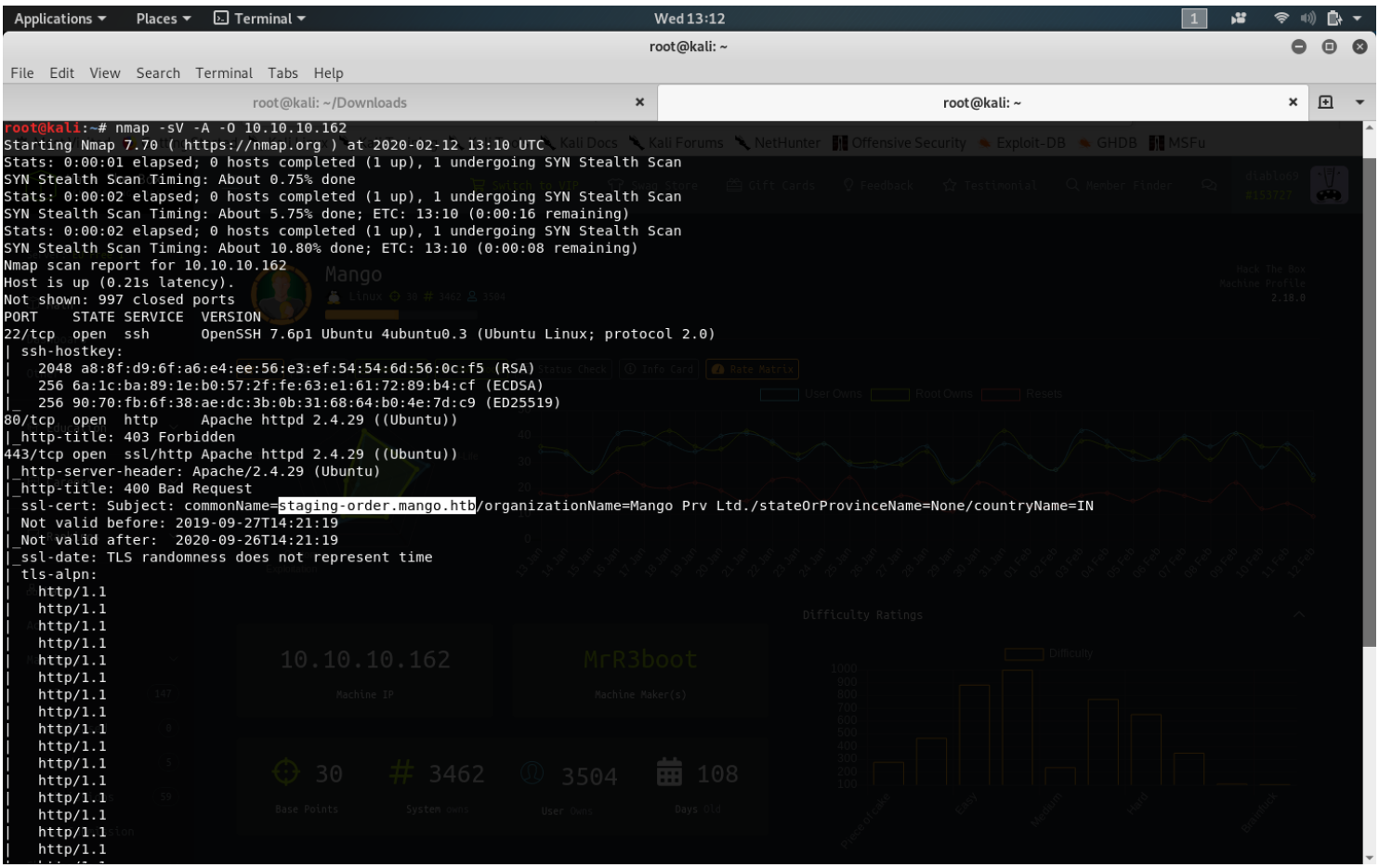
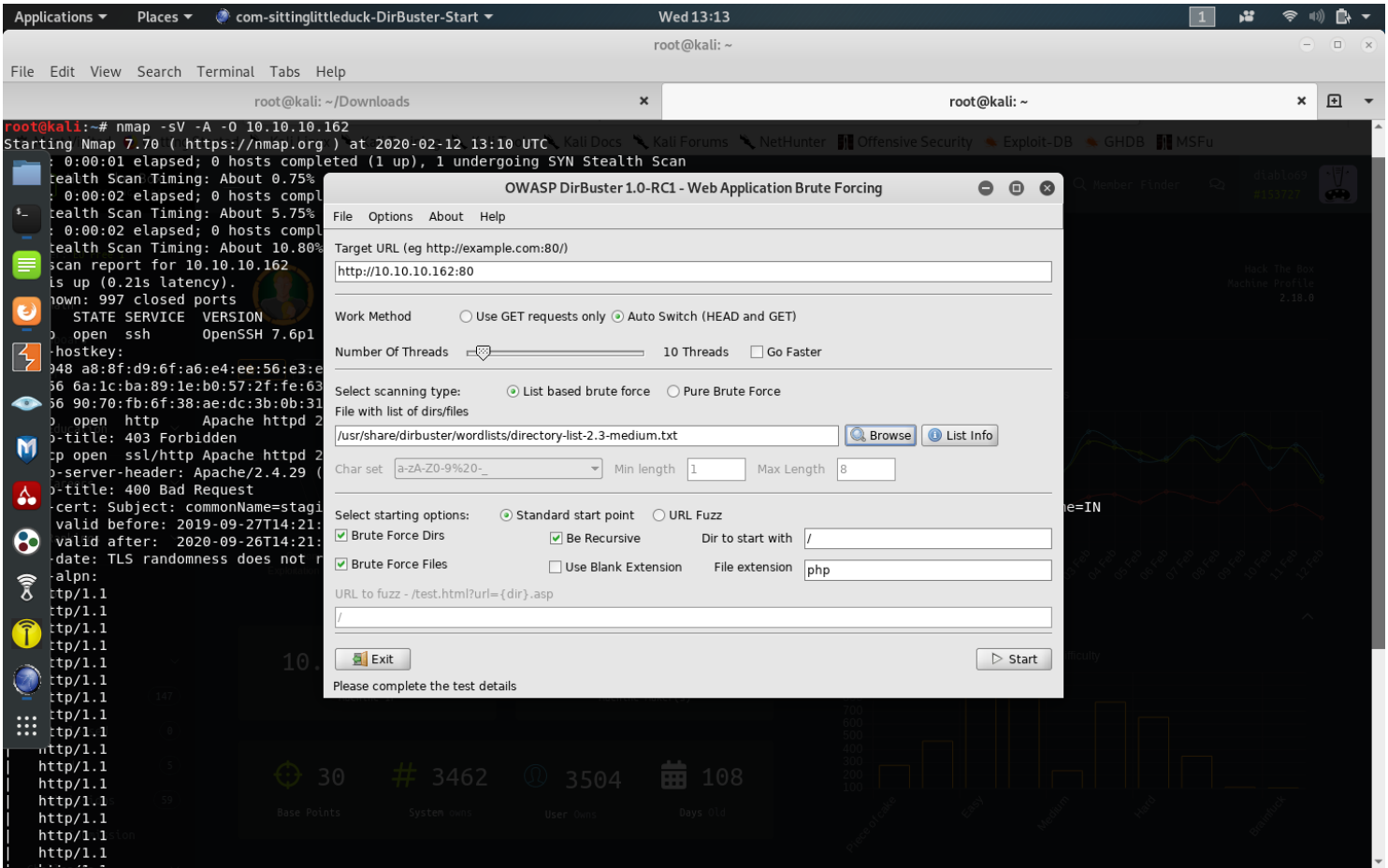
MANGO (10.10.10.162)

A Medium Rated Box in HTB CTF.

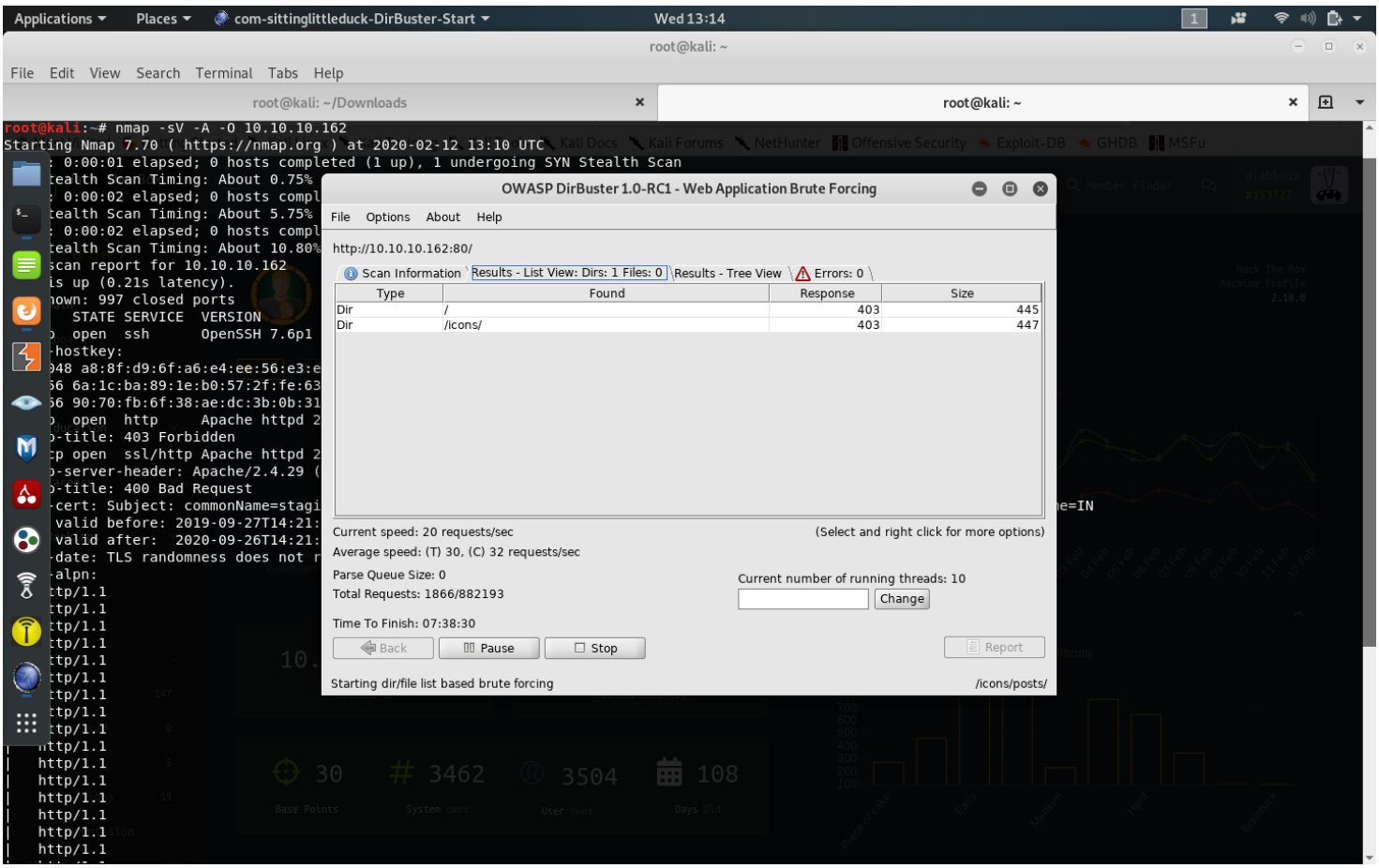
1. Port Scan and Enumeration:-
   We use nmap for the same.
   nmap -sV -O -A 10.10.10.10.162
   Found Ssh,Http and Ssl Port to be opened
2. Use Dirbuster for enumeration:-
   Nothing Juicy Found!
3. Heading to 10.10.10.162:80
   Nothing Found
4. Heading to https://10.10.10.143
   Adding Security Exception
5. Adding staging-order.mango.htb at etc/hosts
6. Continued Later.

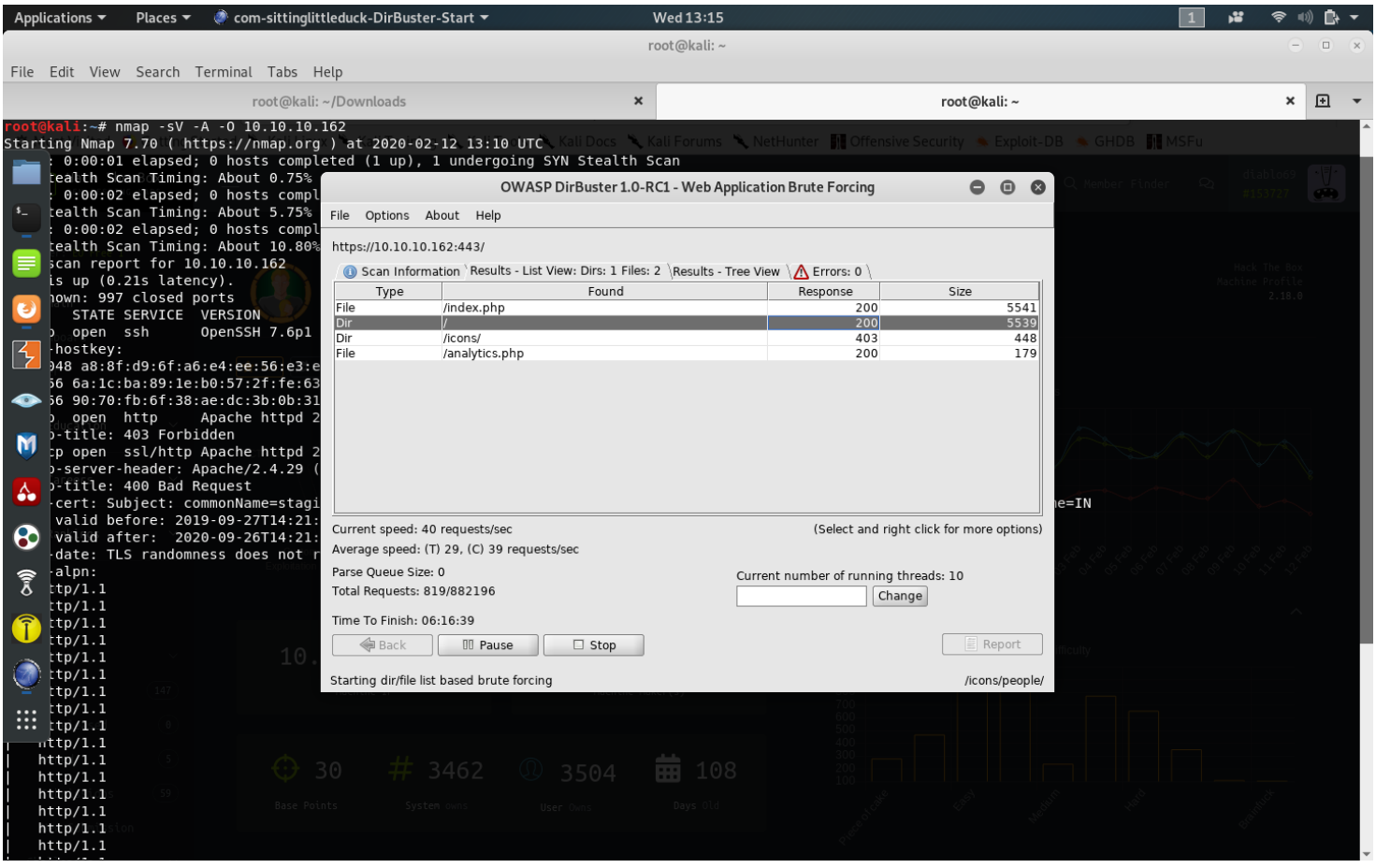
MANGO (10.10.10.162)

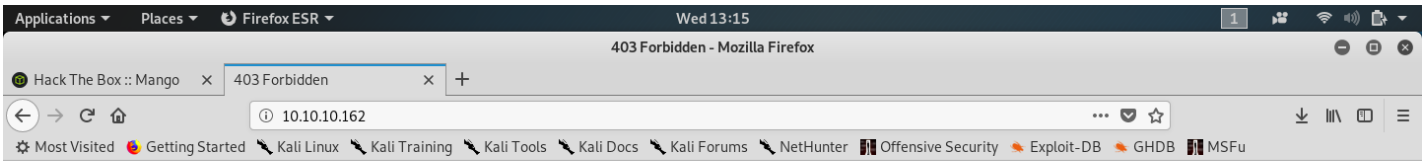




MANGO (10.10.10.162)



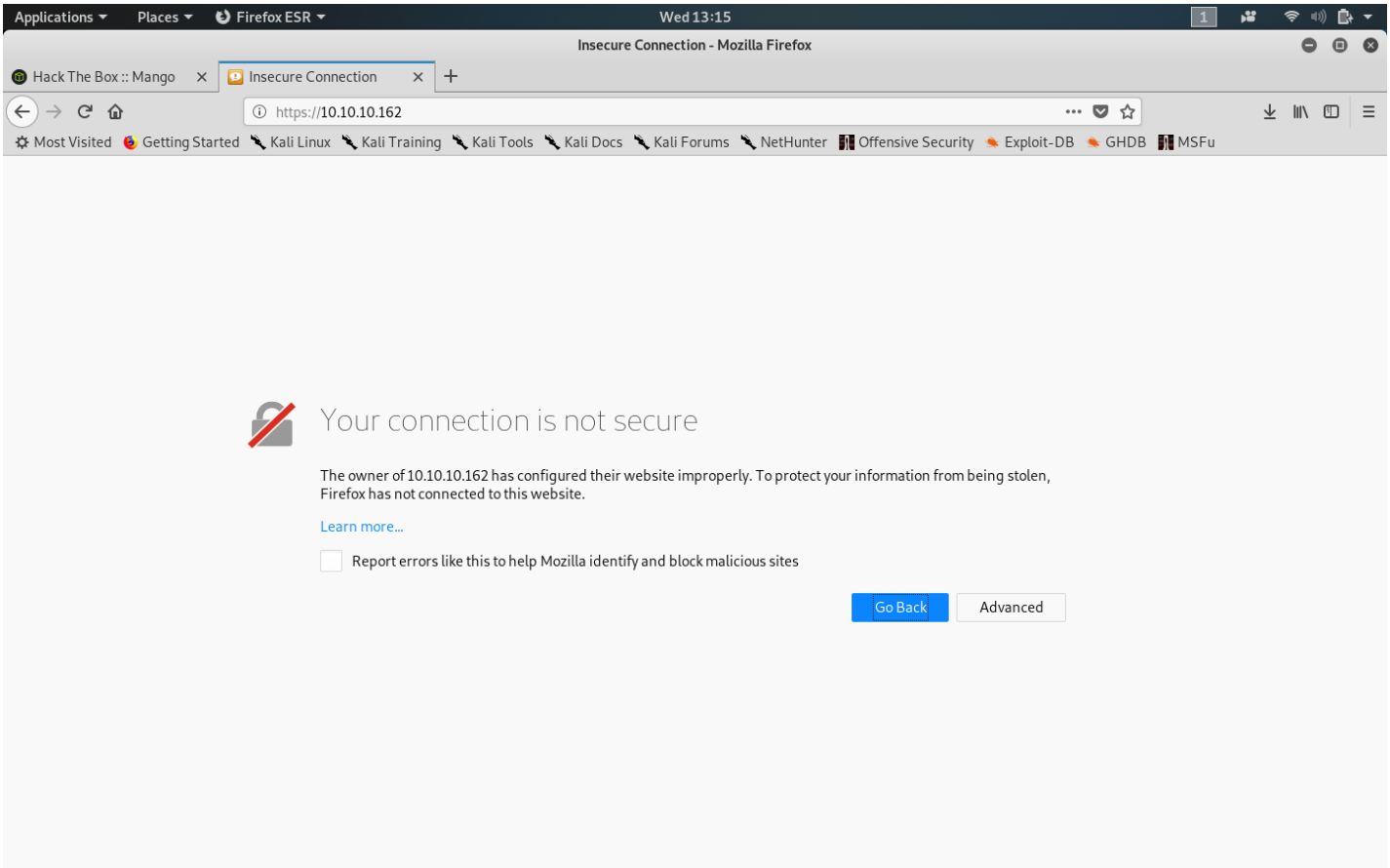




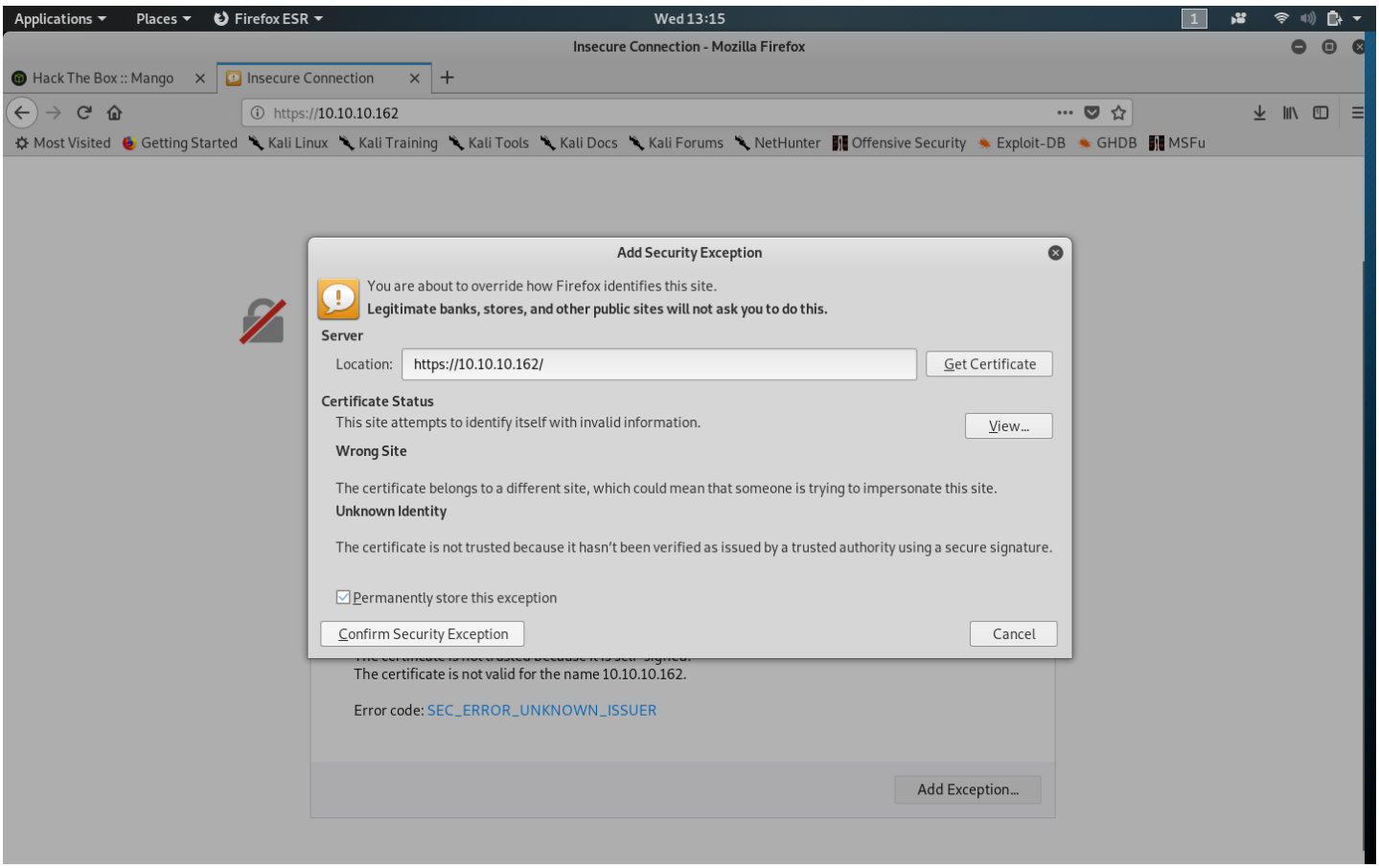
Forbidden

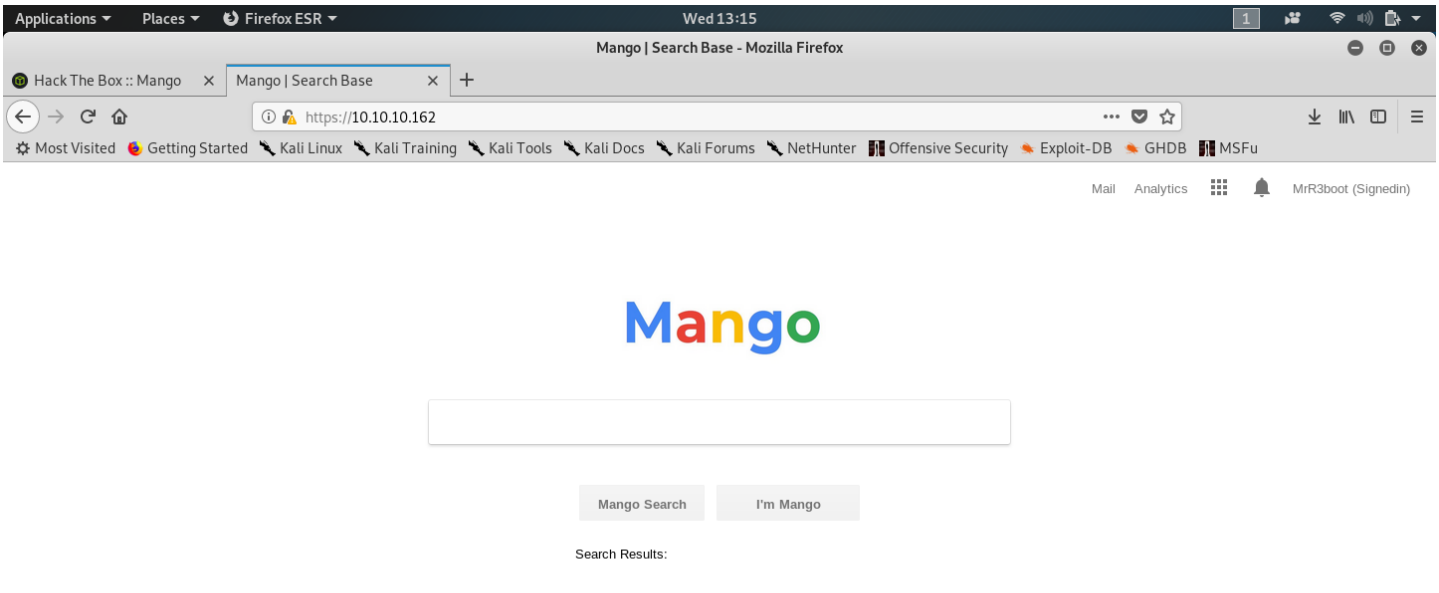
You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.10.10.162 Port 80

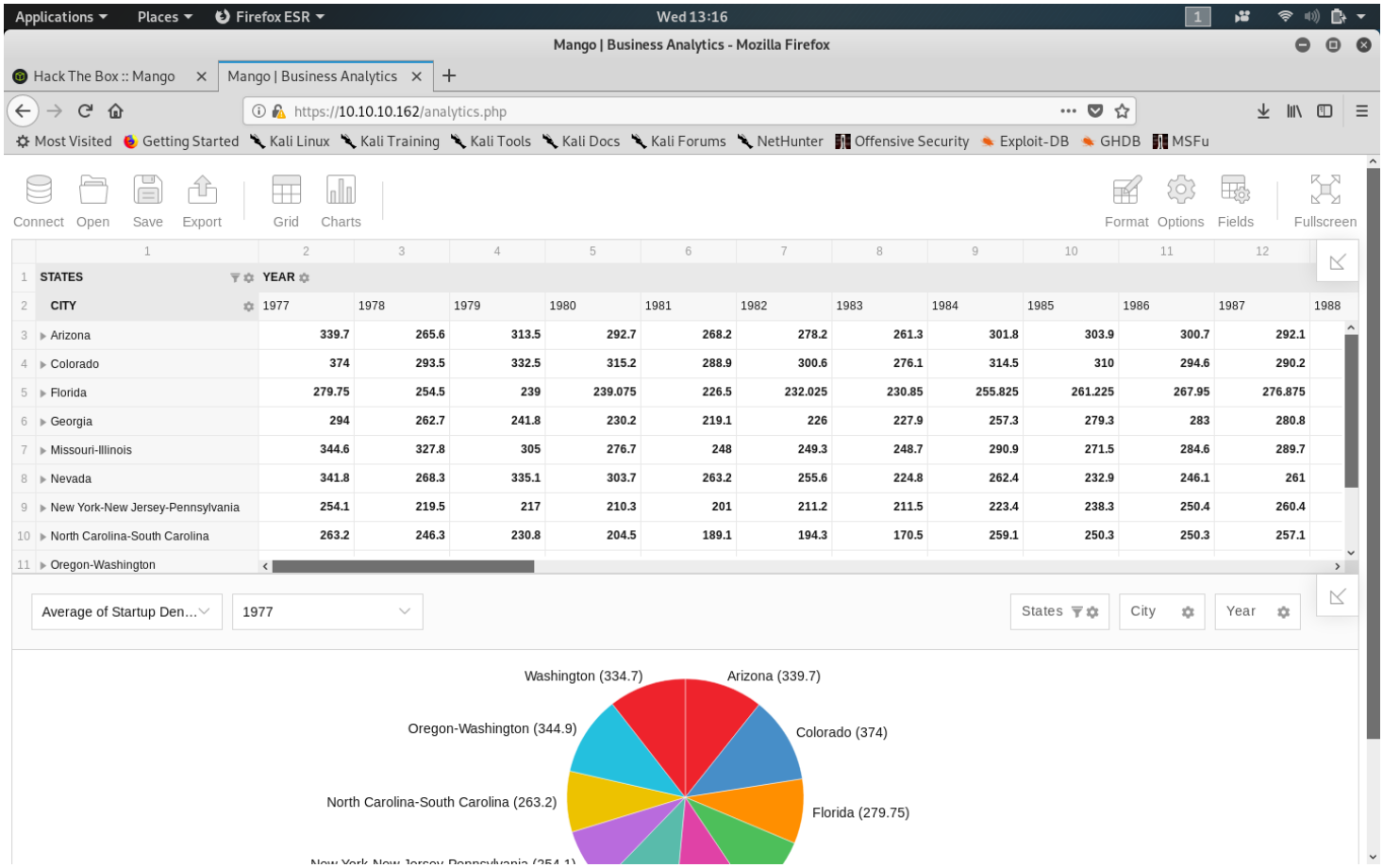


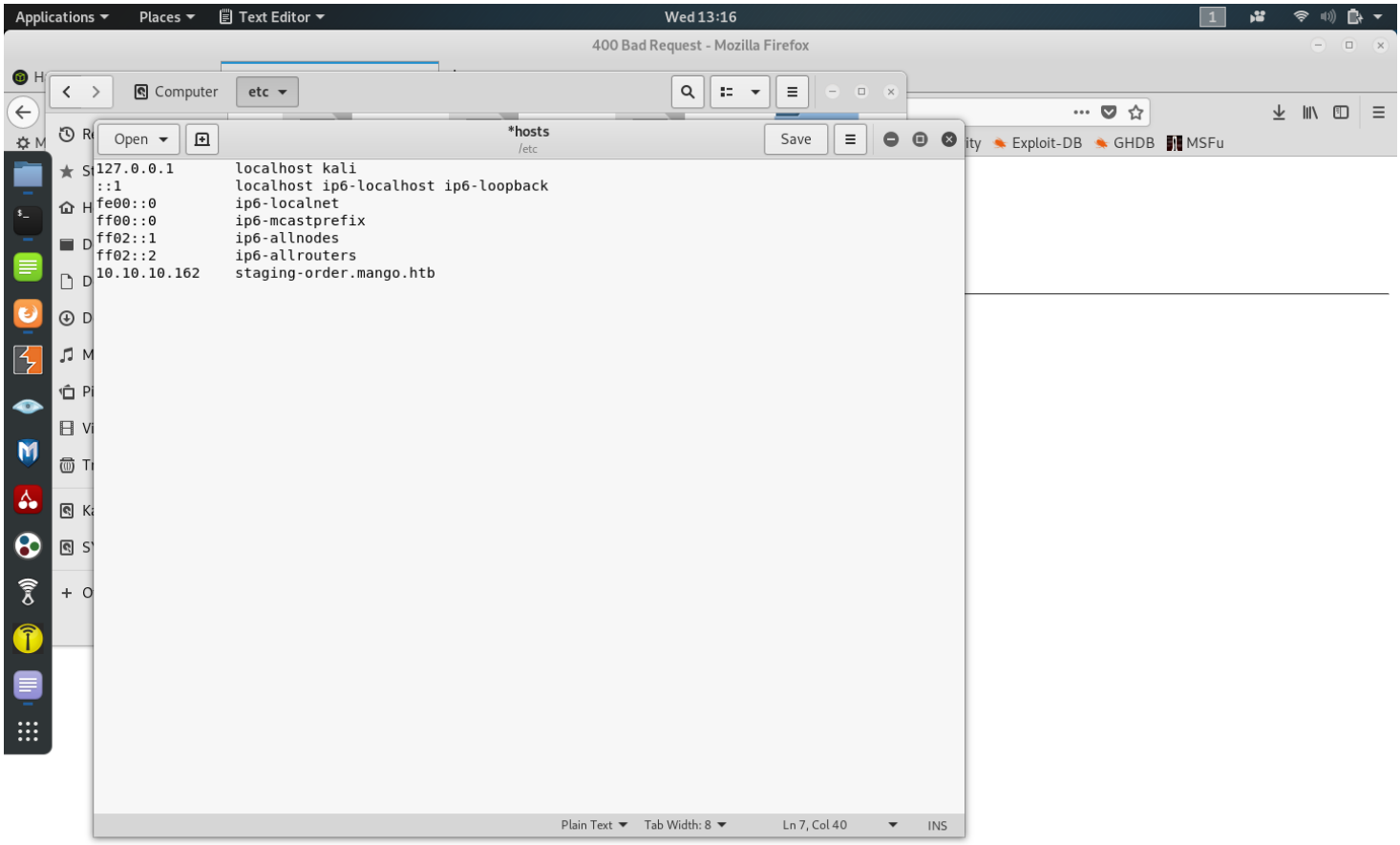
MANGO (10.10.10.162)



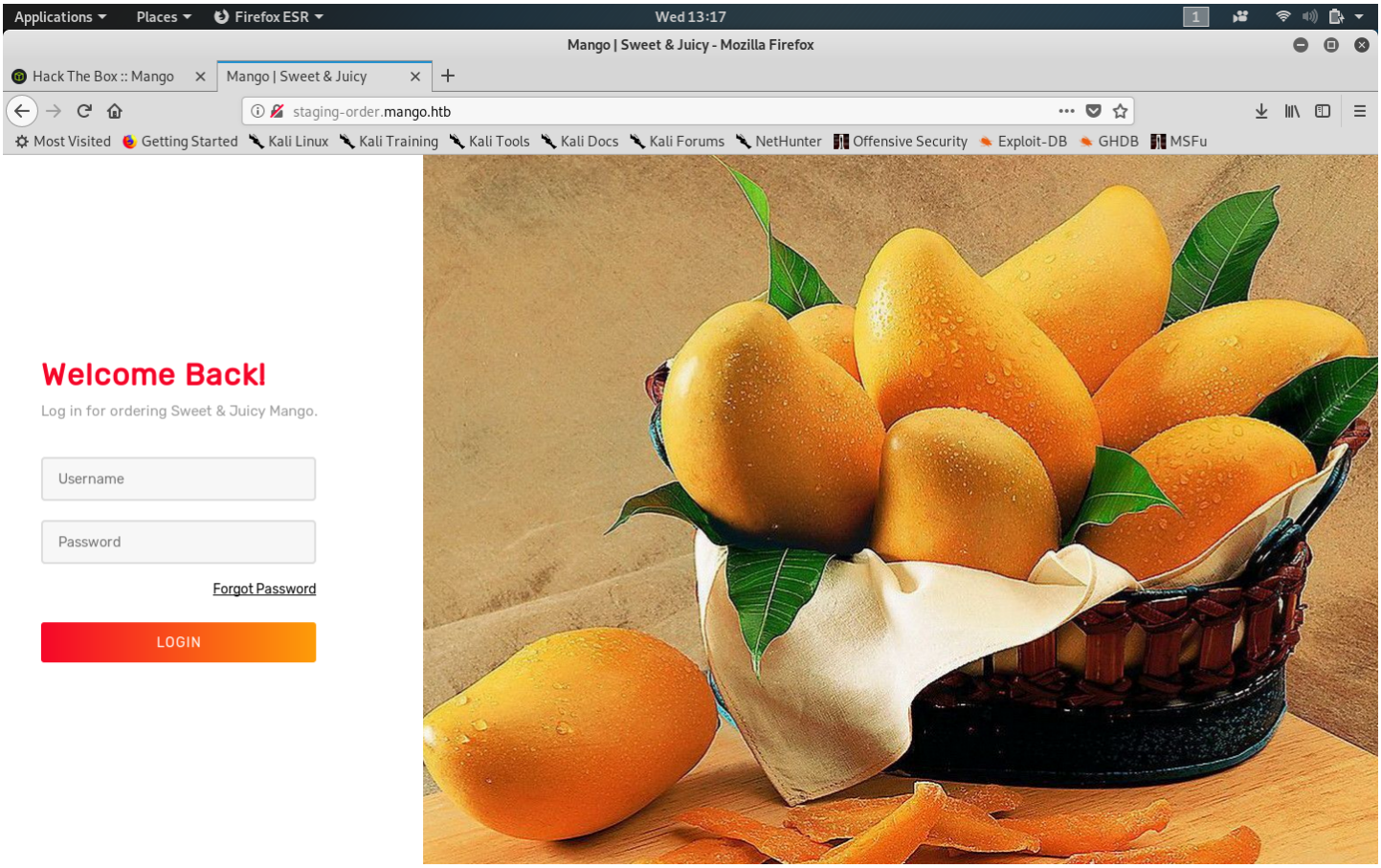


MANGO (10.10.10.162)

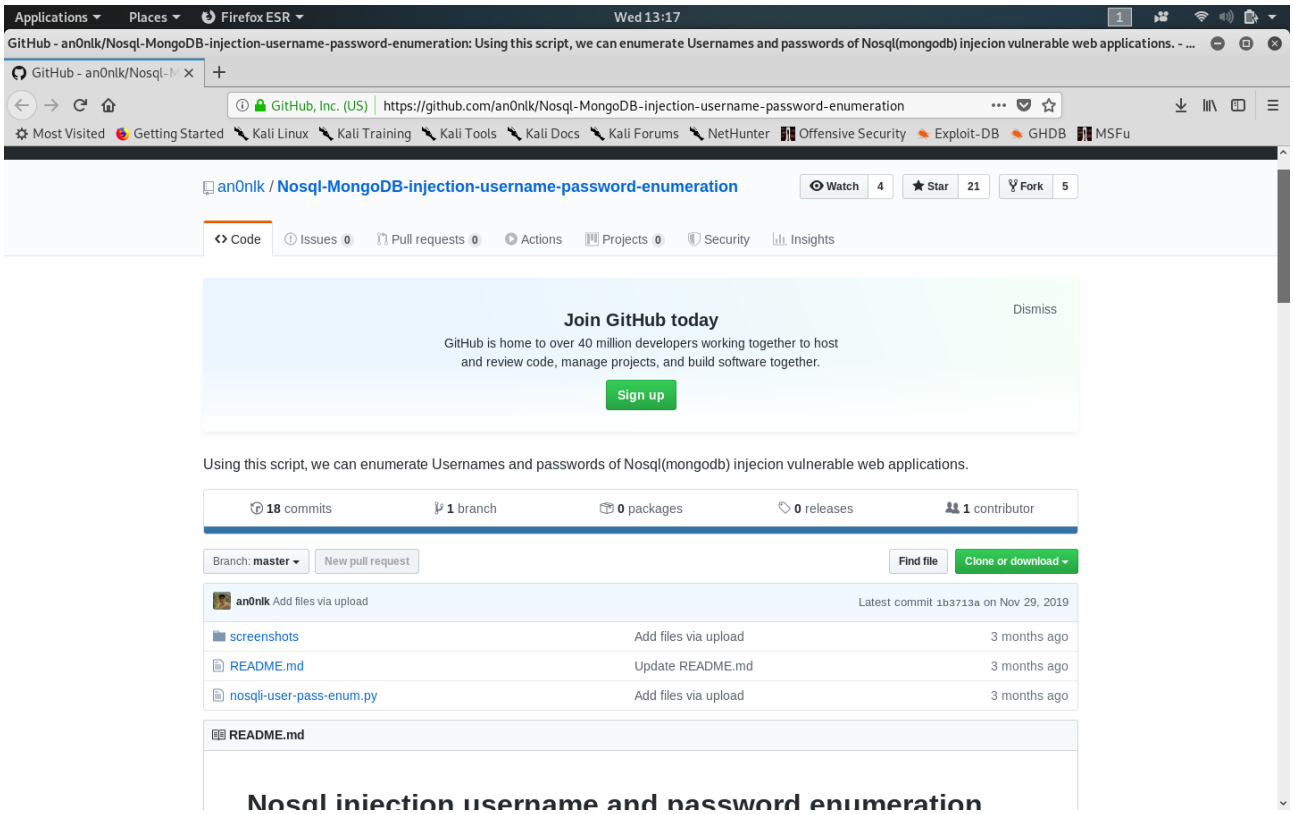




6.Juicy found at staging-order.mango.htb



7.MongoDB Query Object Injection sounds super difficult but it is actually quite simple. Without proper sanitization of inputs to MongoDB queries, we can simply enumerate things like variable length, contents, included characters, using a systematic passing of MongoDB's query objects.
MONGODB EXPLOIT

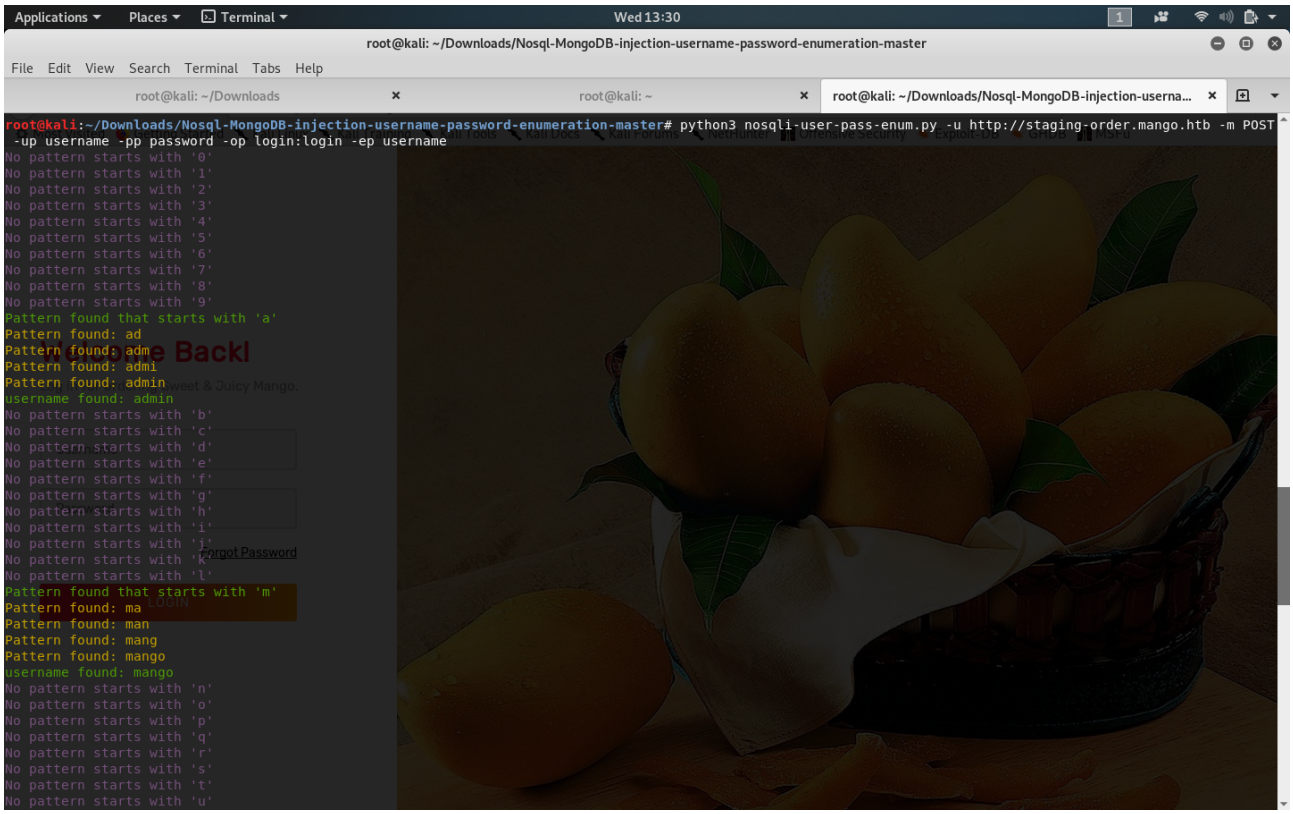


MANGO (10.10.10.162)

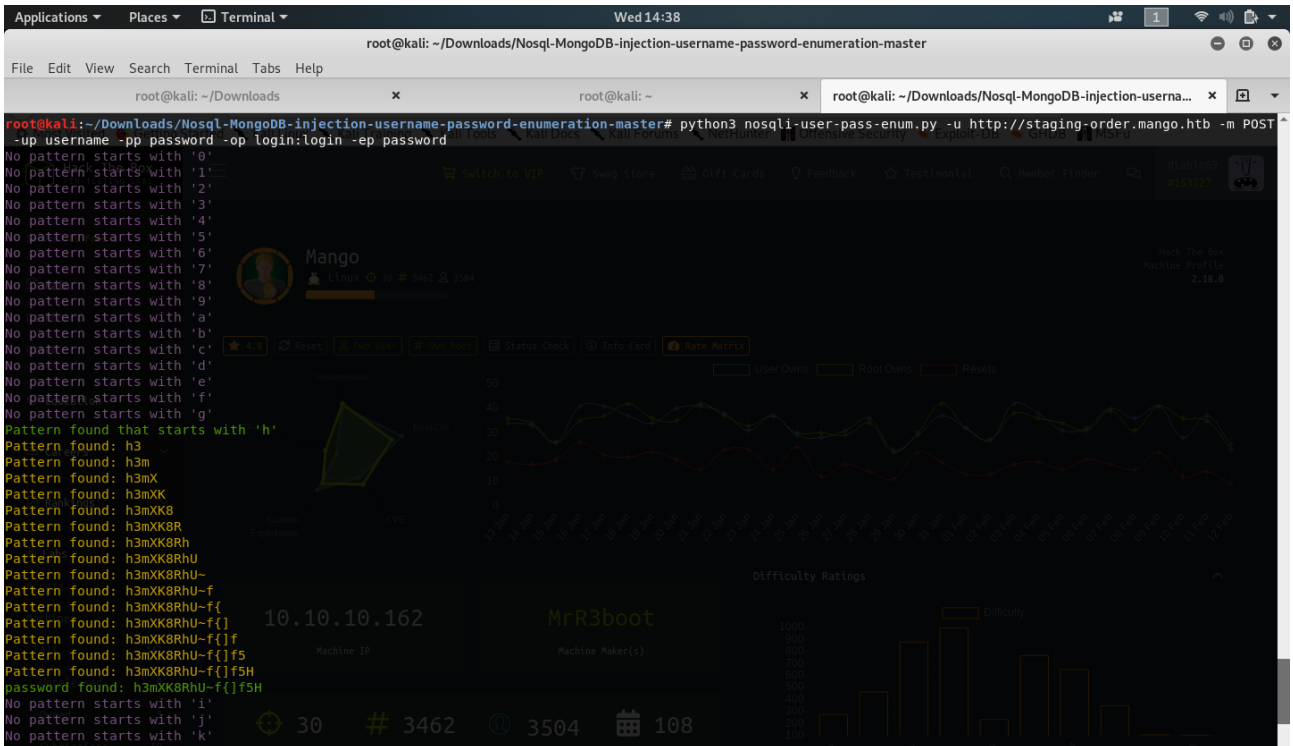
https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration.git

Attacking Via Scripts

python3 nosqli-user-pass-enum.py -u http://staging-order.mango.htb \ -m POST -up username -pp password -op login:login -ep username



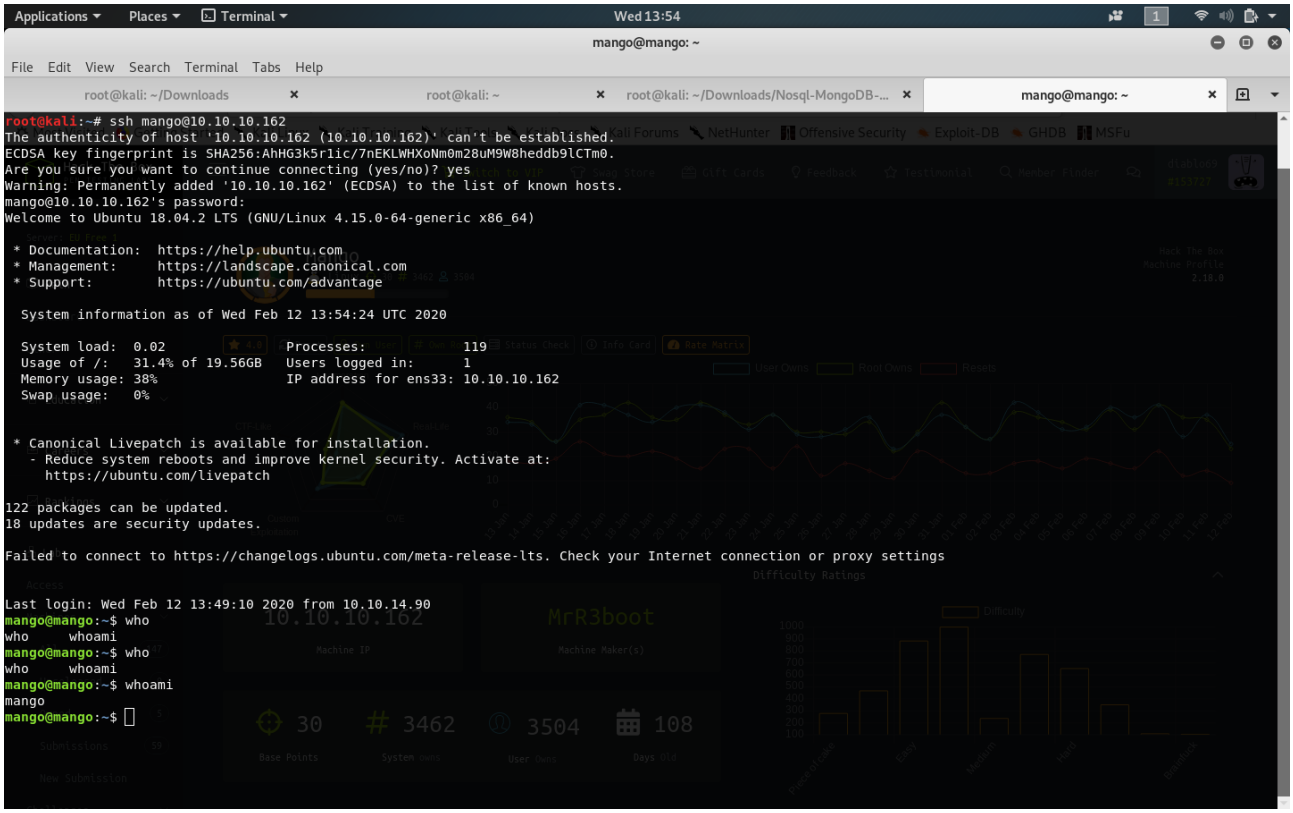
python3 nosqli-user-pass-enum.py -u http://staging-order.mango.htb \ -m POST -up username -pp password -op login:login -ep password



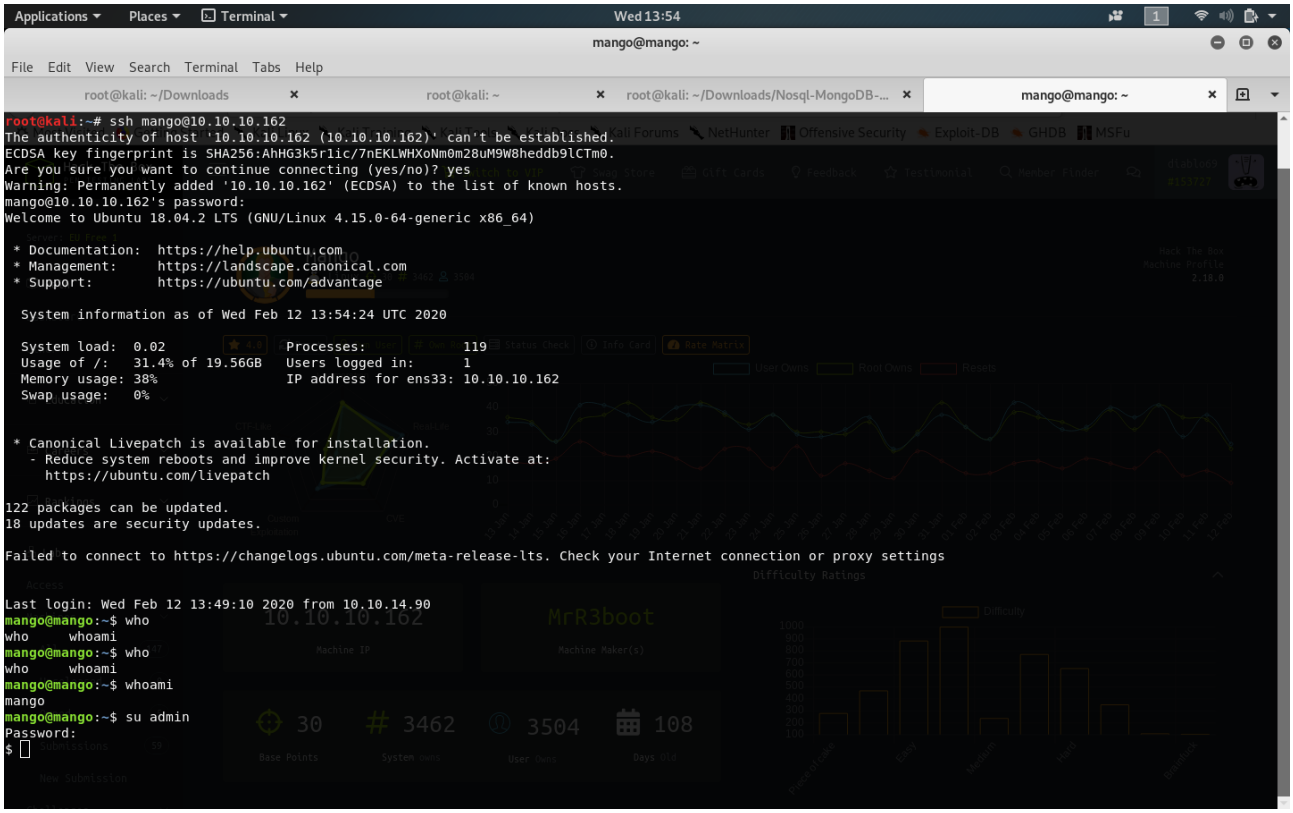
MANGO (10.10.10.162)

We got 2 UserNames and 2 Password:-
admin and mango and passwords for both of thrm.

Doing ssh of mango

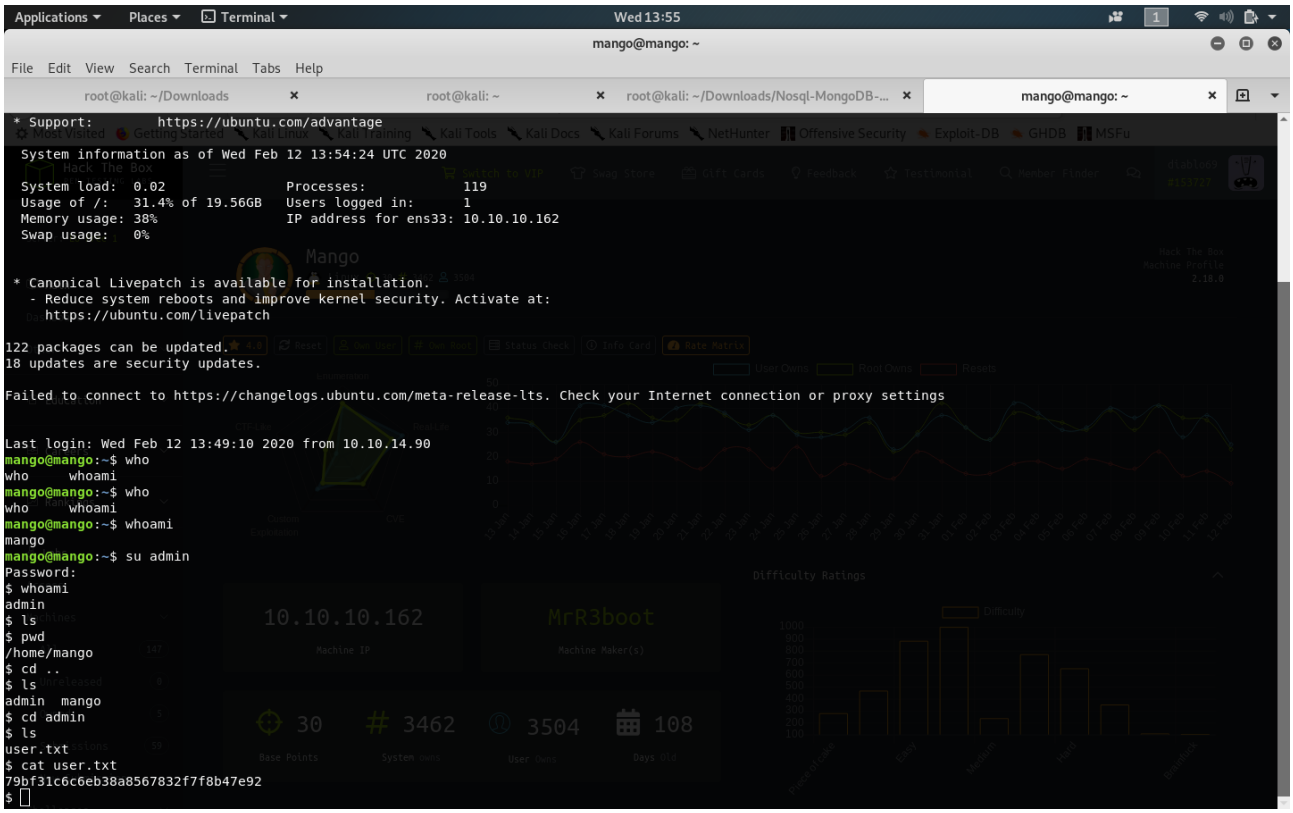


for admin we type su admin and types the password for the same.

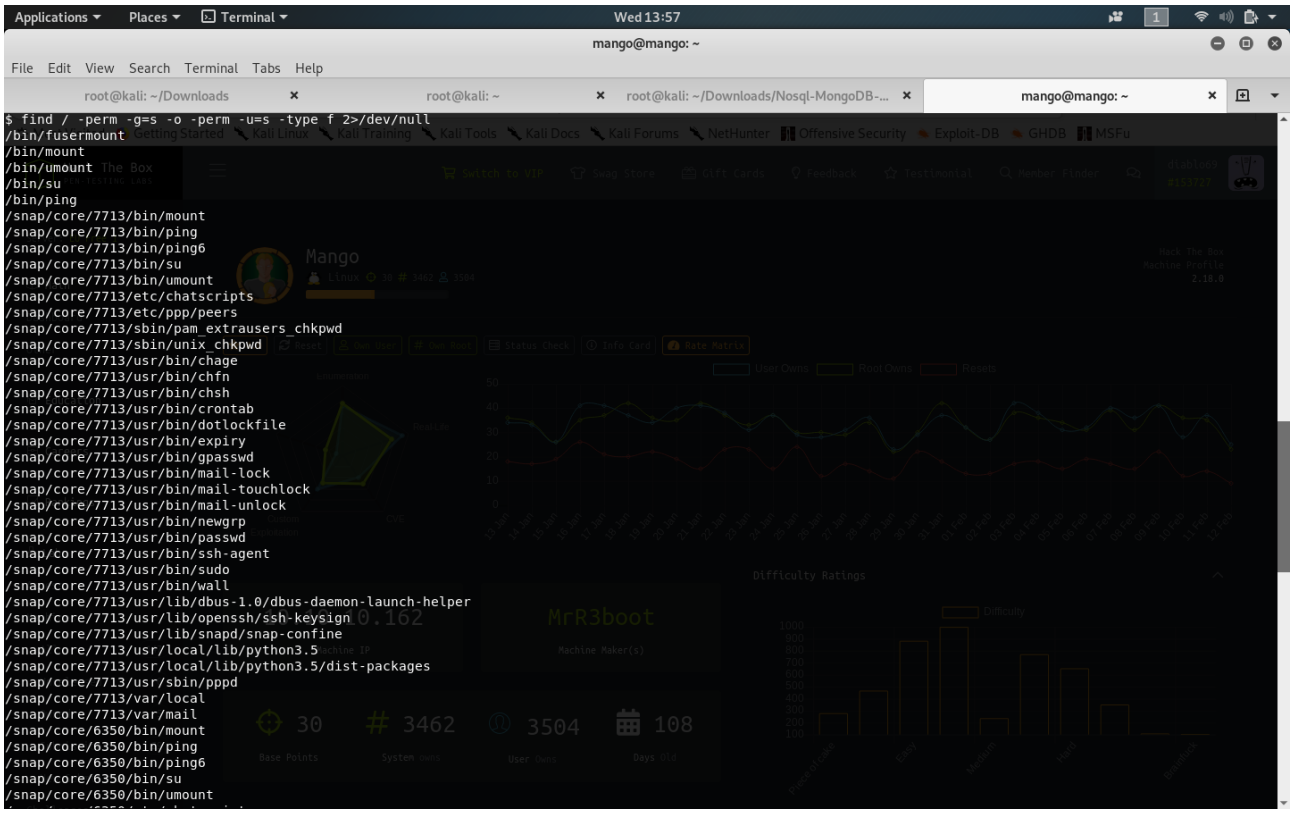


MANGO (10.10.10.162)

We find User.txt

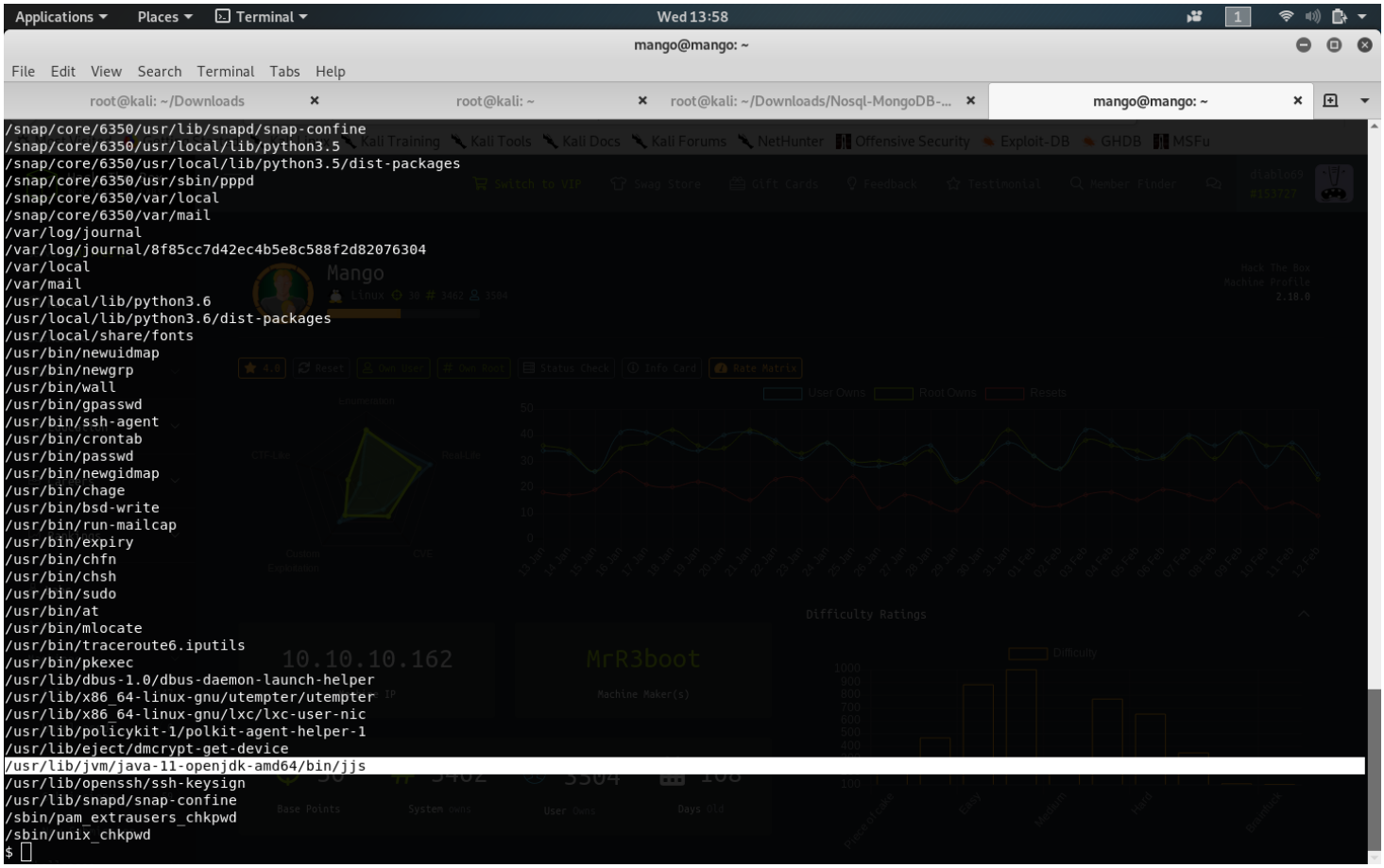


We Search for suid or guid.

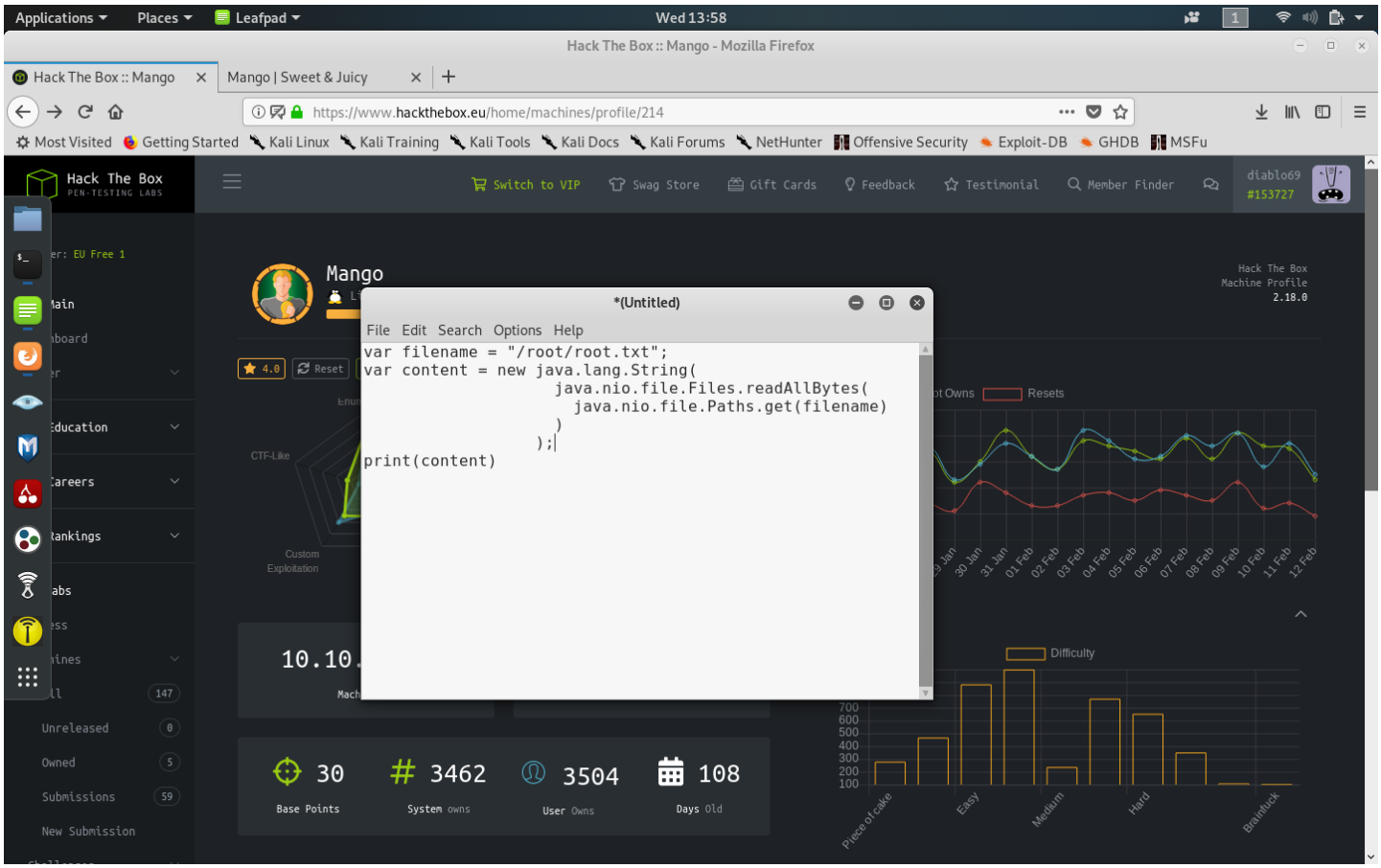


MANGO (10.10.10.162)

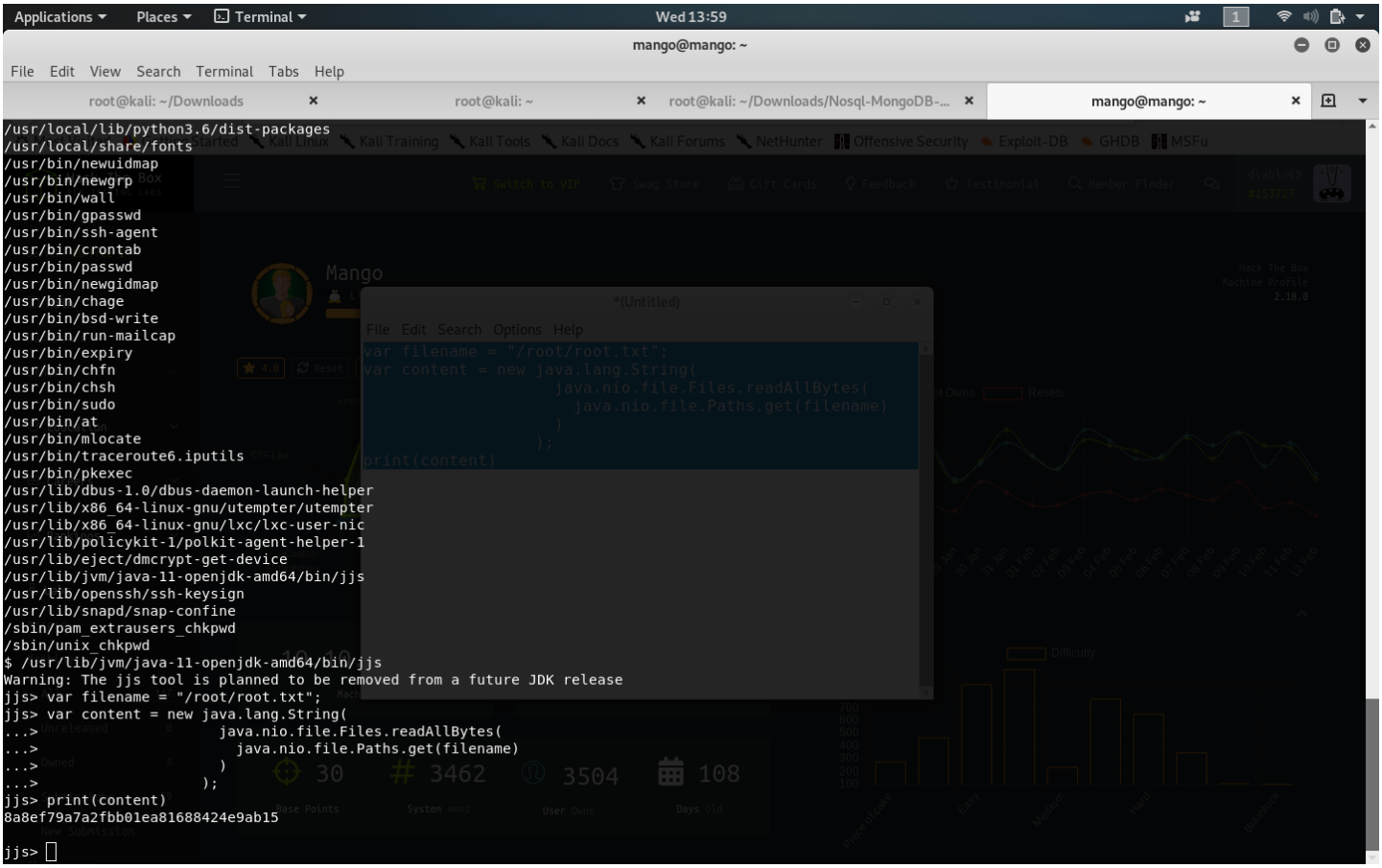
We found Java SDK in the Victim Machine using root.



Wrote a Simple java code to extract root.



MANGO (10.10.10.162)



VOILA! YOU GOT BOTH ROOT AND USER!