Mango

Interesting

HTTP and HTTPS configs differ
Hostname is leaked in SSL Cert

admin@mango.htb

NoSQL Injection

The login page has a bunch of mangos. Hmm.... MongoDB?????
This has to be a NoSQL Injection on a MongoDB

The following causes a 302 Found (injecting a not equals expression)
username[$ne]=doggydoggerton&password[$ne]=easterfrog&login=login

The following also causes a 302 Found, indicating that there is 5 character username:
username[$regex]=^.{5}$&password[$ne]=easterfrog&login=login

Note:
- The 302 found is a redirect to http://staging-order.mango.htb/home.php
- The page does not seem very interesting

Scripting

using a python script, we are able to enumerate usernames and passwords
from the mongodb database

creds:

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

priv esc

linpeas tells us of an suid binary:
/usr/lib/jvm/java-11-openjdk-amd64/bin/jjs

gtfobins tells us how to use this for priv esc!

however, only group admin can run jjs

we were only allowed to ssh as mango, but can su into admin

First, generate ssh keys
Then, as admin, run the gtfobin hack to write an ssh public key in /root/.ssh/authorized_keys
now, we can ssh as root!