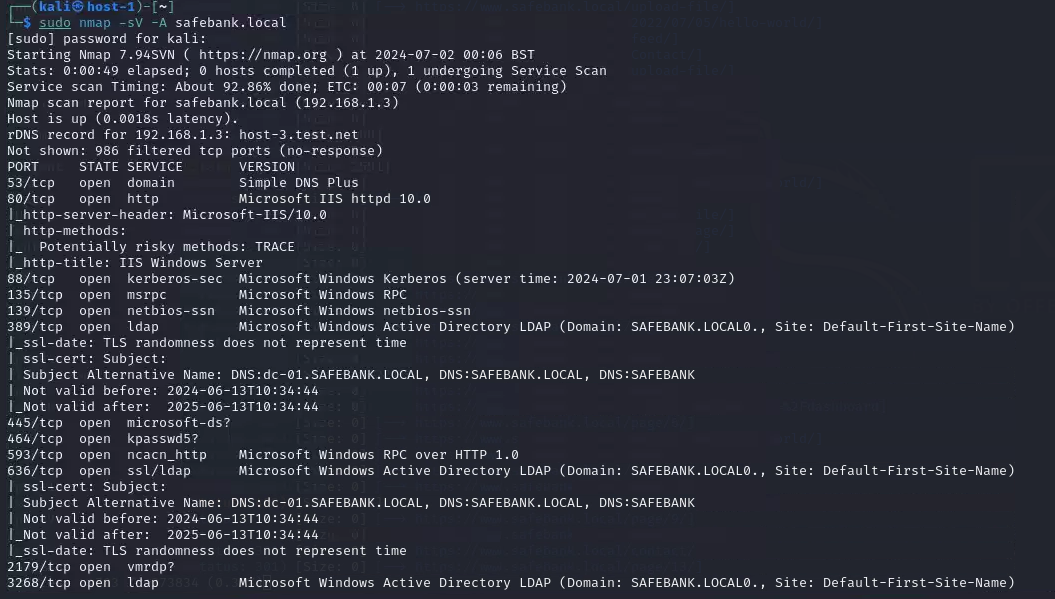
**Birdo Write-up**

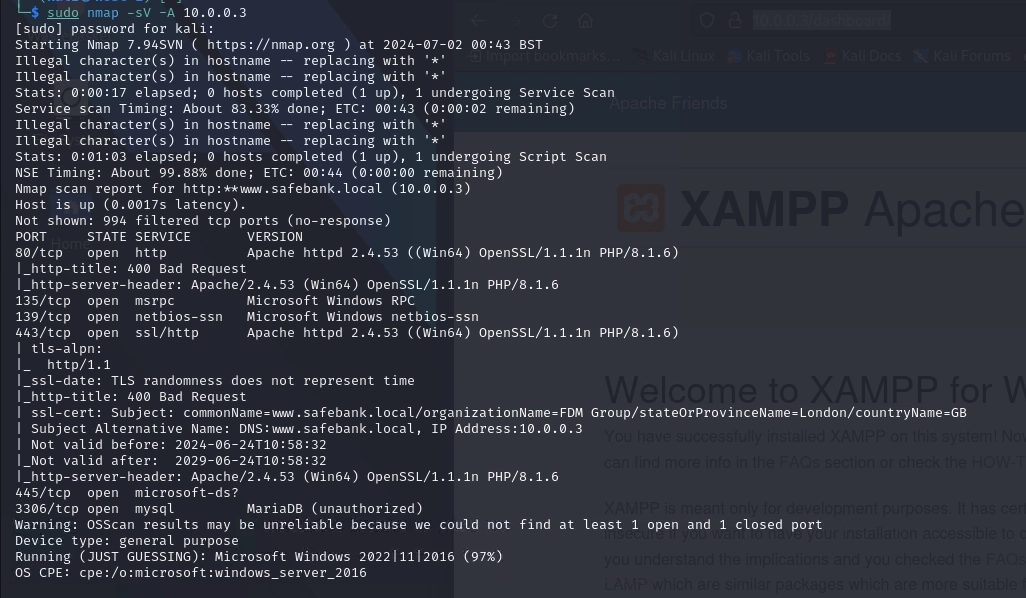
**First Nmap prompts nothing special, looks like none of the services are actually vulnerable but the web-application’s.**

**The IP is 10.0.0.3, it's using a local domain called safebank.local, the local domain has its only separate set of services running on it, including the IP itself.**

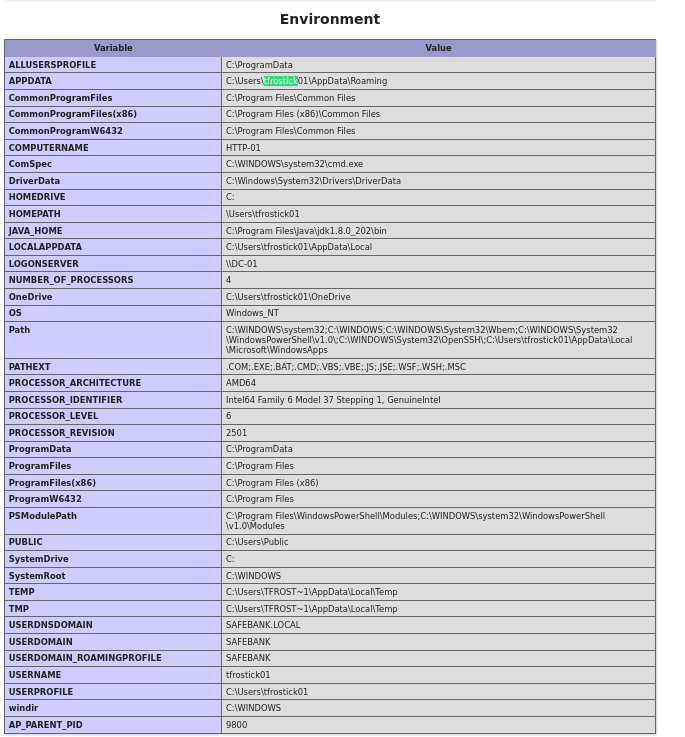
**Scan on the Domain :**

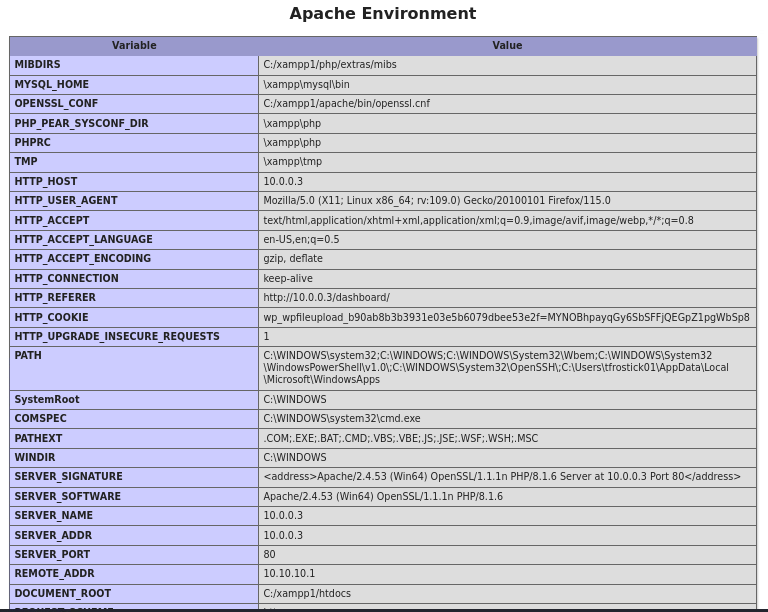
****

**Scan on the IP :**

****

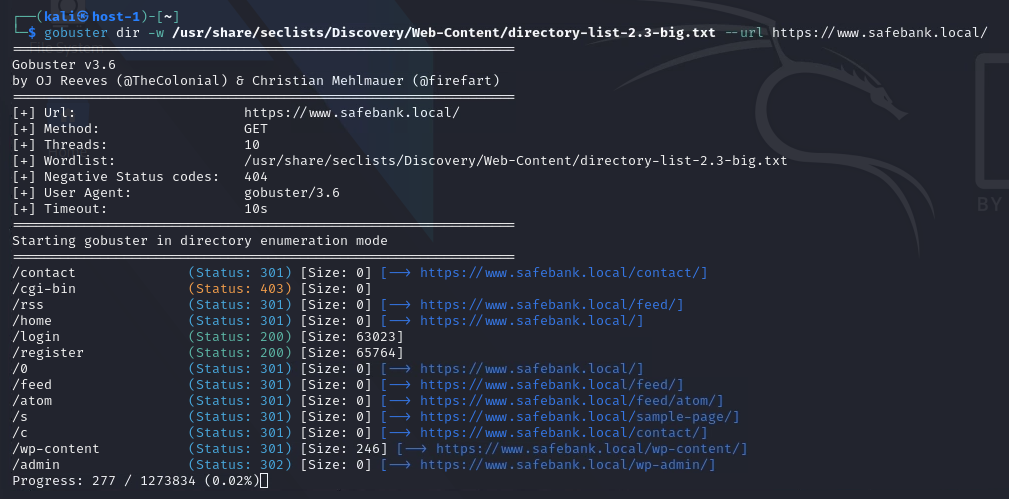
**The port 80 on the IP Exposes the PHPInfo page which also disclosures the User running the application and on what machine, seems to been windows and a user called “tfrostick01”**

****

****

**I saw that Mariadb was up on 10.0.0.3, as Unauthorised but every time I tried to login I got a tls handshake error, still not caught up on why. [ I do have a ‘.CRT’ file in my home directory thats either for the machines configuration or for the pentest]**

**I then started to brute-force the directories of the web-application using Gobuster, Making some interesting finds like a login-page, file-upload and a forgotten-password page. As well as a registration page.**

****

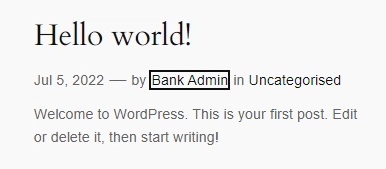
**I went to the registration page to create a user and test out the forgotten-password page. It seems like either SMTP / email services are not working or the configuration is disabled / needed to do so.**

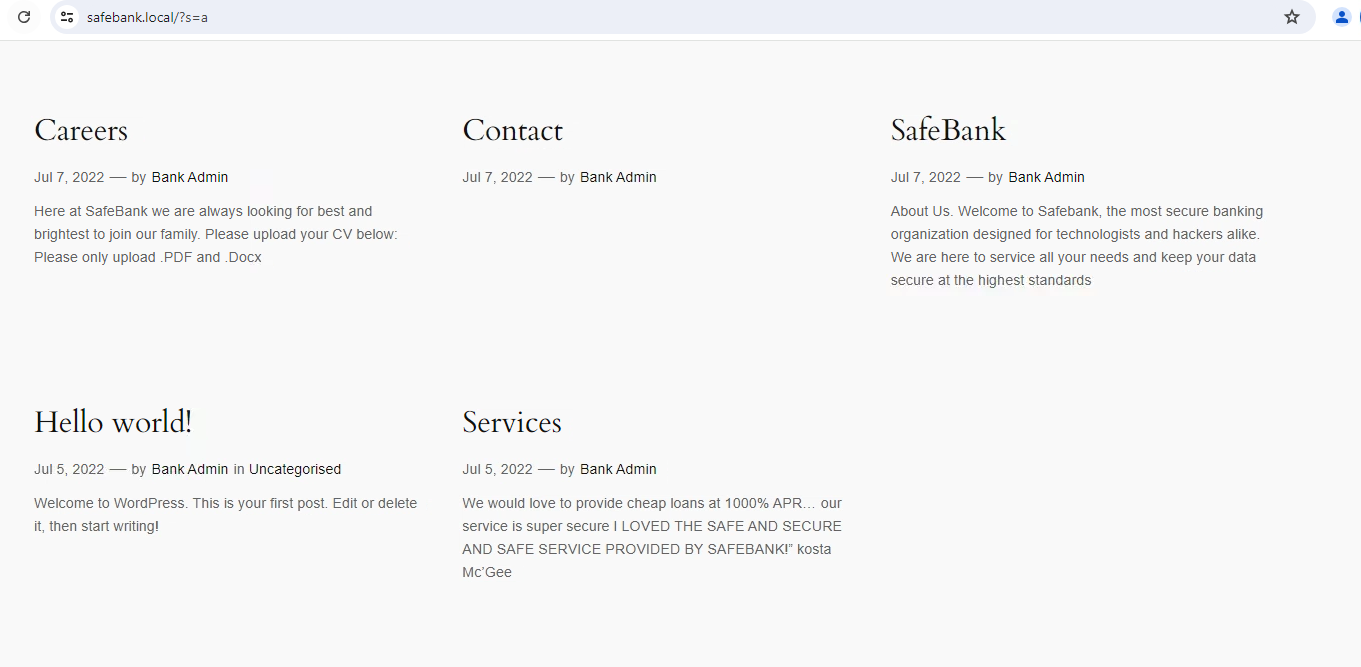
**I also logged in using the created user i made, i was able to access the wordpress dashboard with no privileges or any vulnerable plugins, But i was also able to access the file-upload page.**

**The file upload-page only accepts .docs and PDFs files, knowing that it will need to be intercepted later on to test bypassing those extensions.**

**I continued looking, and went into the wordpress blog posts, there was a uncategorized blog from a User called**

**‘sbsiteadmin’**

****

****

**Which is labelled as the Bank Admin for the web-page, restarting the password for this only worked with the username: ‘sbsiteadmin’**

**The plan now is to try and brute-force the password for the ‘Bank admin’ account which will hopefully give us more privileges to play around with like adding plugins or changing themes / Custom php pages.**