**CVE-2021-41773 - Apache HTTP Server Path Traversal 0-Day – POC**

**Rezka Norhafizah**

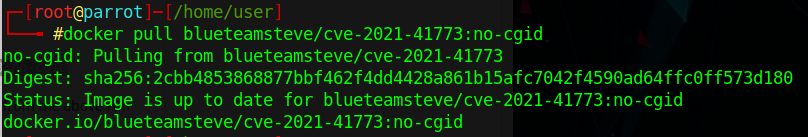
Ini adalah PoC dari CVE-2021-41773 Apache path traversal & RCE (Apache version 2.4.49)

Reference : [*https://hub.docker.com/r/blueteamsteve/cve-2021-41773*](https://hub.docker.com/r/blueteamsteve/cve-2021-41773)

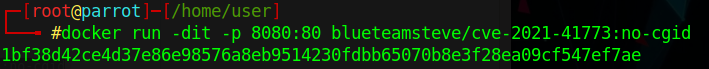
Pertama-tama, install docker :

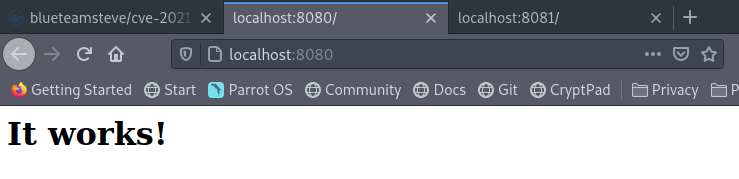


Lalu, pull docker image dari situs di atas :

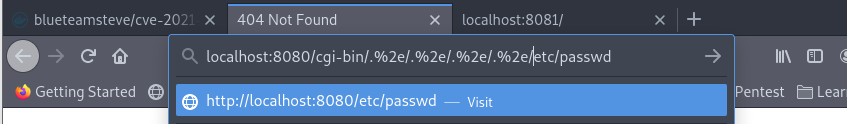


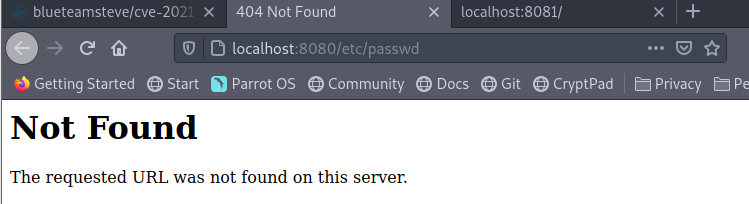
Dan jalankan docker image tersebut pada port 8080 :



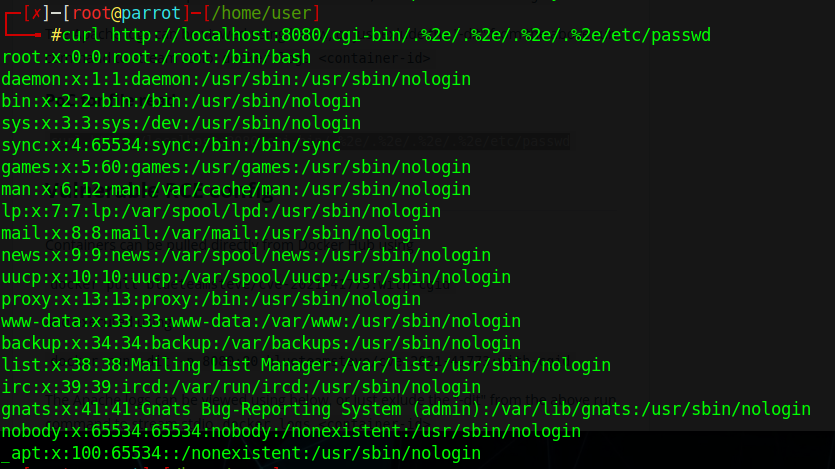


Setelah itu, saya coba langsung ketikkan perintah /cgi-bin/.%2e/.%2e /.%2e /.%2e /etc/passwd sebagai parameter (referensi : [*https://www.exploit-db.com/exploits/50383?fbclid=IwAR0Z6s3sV6\_bXp62YiU192LOJB2HKjsU4VQIAF7APAZ9PcE\_jNPxWc\_EVFo*](https://www.exploit-db.com/exploits/50383?fbclid=IwAR0Z6s3sV6_bXp62YiU192LOJB2HKjsU4VQIAF7APAZ9PcE_jNPxWc_EVFo)) untuk melihat user yang ada namun ternyata tidak berhasil :





Kemudian, saya coba request menggunakan curl di terminal bypass tersebut dan ternyata langsung berhasil :



Kemudian saya coba melihat user id machine :

