

Delivery

- 🏷️ **Tags** : #03-2023 #report
- 🔗 **CTF link**: [Delivery](#)
- 📖 **Resources**: [HelpDesk Vuln](#)

Target Information Gathering

IP - 10.10.10.222

OS - Linux

Port scanning

| Port | Protocol | State | Service |
|------|----------|-------|---------|
| 22 | tcp | open | ssh |
| 80 | tcp | open | http |
| 8065 | tcp | open | unknown |

Penetration Proof of Concept

Initial Access | User Flag

As can be seen in the Nmap scanning, the victim machine is running an HTTP web page.

By analyzing the page source code, there are two links pointing to another pages:

- <http://helpdesk.delivery.htb/>
- <http://delivery.htb:8065/>

On the first one, there is the possibility for any user to create a ticket and send it to help-desk by creating a test account.

Open a New Ticket

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

Contact Information

Email Address *

test123@test123.com

Full Name *

testing

Phone Number

111111111

Ext: 123

Help Topic

















Contact Us

Ticket Details

Please Describe Your Issue

Issue Summary *

Testing

<>    Aa  B  /           

Testing

all changes saved

Drop files here or [choose them](#)

CAPTCHA Text:

6831D

6831D

Enter the text shown on the image. *

Create Ticket

Reset

Cancel

By creating this ticket, there is an automated response that returns back an internal mail.

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 3654172.

If you want to add more information to your ticket, just email 3654172@delivery.htb.

Thanks,

Support Team

There is an option to log in to check the ticket status.


Check Ticket Status

Please provide your email address and a ticket number. This will sign you in to view your ticket.

Email Address:

Ticket Number:

Have an account with us? [Sign In](#) or [register for an account](#) to access all your tickets.



Once opened, the ticket is displayed

 **Looking for your other tickets?**
[Sign In](#) or [register for an account](#) for the best experience on our help desk.

Testing #3654172

 Print

 Edit

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 3/1/23 3:13 PM

User Information

Name: Testing
Email: test123@test123.com
Phone: 111111111 x123



testing posted 3/1/23 3:13 PM

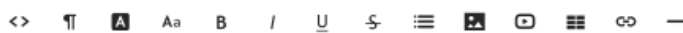
Testing




Created by  **testing** 3/1/23 3:13 PM

Post a Reply

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



 Drop files here or [choose them](#)

Let's see if the internal mail given can be used to log in the second web page by creating an account using the support mail

Mattermost

All team communication in one place,
searchable and accessible anywhere

Let's create your account

Already have an account? [Click here to sign in.](#)

What's your email address?

Valid email required for sign-up


Choose your username


You can use lowercase letters, numbers, periods, dashes, and
underscores.

Choose your password

Once the account is created a *Please verify your mail* message is displayed.
Because how the help-desk software works, this mail is displayed in the
ticket's portal. All it has to be done is refreshing the page.

 [Support Center Home](#)

 [Open a New Ticket](#)

 [View Ticket Thread](#)



Looking for your other tickets?

[Sign In](#) or [register for an account](#) for the best experience on our help desk.

 **Testing** #3654172

 Print

 Edit

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 3/1/23 3:13 PM

User Information

Name: Testing
Email: test123@test123.com
Phone: 111111111 x123



testing posted 3/1/23 3:13 PM



---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=goon87csp7wfg1dwom8mutqxcwfp8spc1b6hzaqz5yd15o3eaidzdu13tpm9wbdy&email=3654172%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  **testing** 3/1/23 3:13 PM

Post a Reply

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

 Drop files here or [choose them](#)

 Post Reply


 Reset

 Cancel

Now the internal business communication tool can be accessed with legitimate credentials

Mattermost

All team communication in one place,
searchable and accessible anywhere

✓ Email Verified 

3654172@delivery.htb


●●●●●●●●●●


Sign in

Don't have an account? [Create one now.](#)

[I forgot my password.](#)

Once inside, root messages can be read and credentials for ssh are obtained.

 **root** 3:29 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** 4:58 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.

User flag ✓

Privilege Escalation | Root flag

Once on the system, by examining the files, it can be seen how Matter-most is configured.

Inside `/opt/mattermost/config/config.json` there are some valid credentials to connect into a mysql server.

```
"SqlSettings": {  
  "DriverName": "mysql",  
  "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?  
charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s"  
  ...  
}
```

Here it can be seen that a MySQL server is running on port 3306. It can be connected by using `mysql -u mmuser -p` and inserting `Crack_The_MM_Admin_PW` as a password.

The SQL service is a MariaDB database which stores users and passwords. Databases, tables and columns can be shown by using `show databases / tables / columns`. Once there, a root hash password can be obtained. If going back to the root message on Matter-most app, they are often reusing *PleaseSubscribe!* password or variants.

Using `echo PleaseSubscribe! | hashcat -r /usr/share/hashcat/rules/best64.rule --stdout >> variants.txt` we can create different variants for that original string.

Then, using john tool the root password can be cracked as `john root_hash_insidefile.txt --wordlist=variants.txt`

Now it possible to log in as root by using ***PleaseSubscribe!21***

Root Flag ✓