Delivery

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

Target Information Gathering

IP - 10.10.10.222

OS - Linux

Port scanning

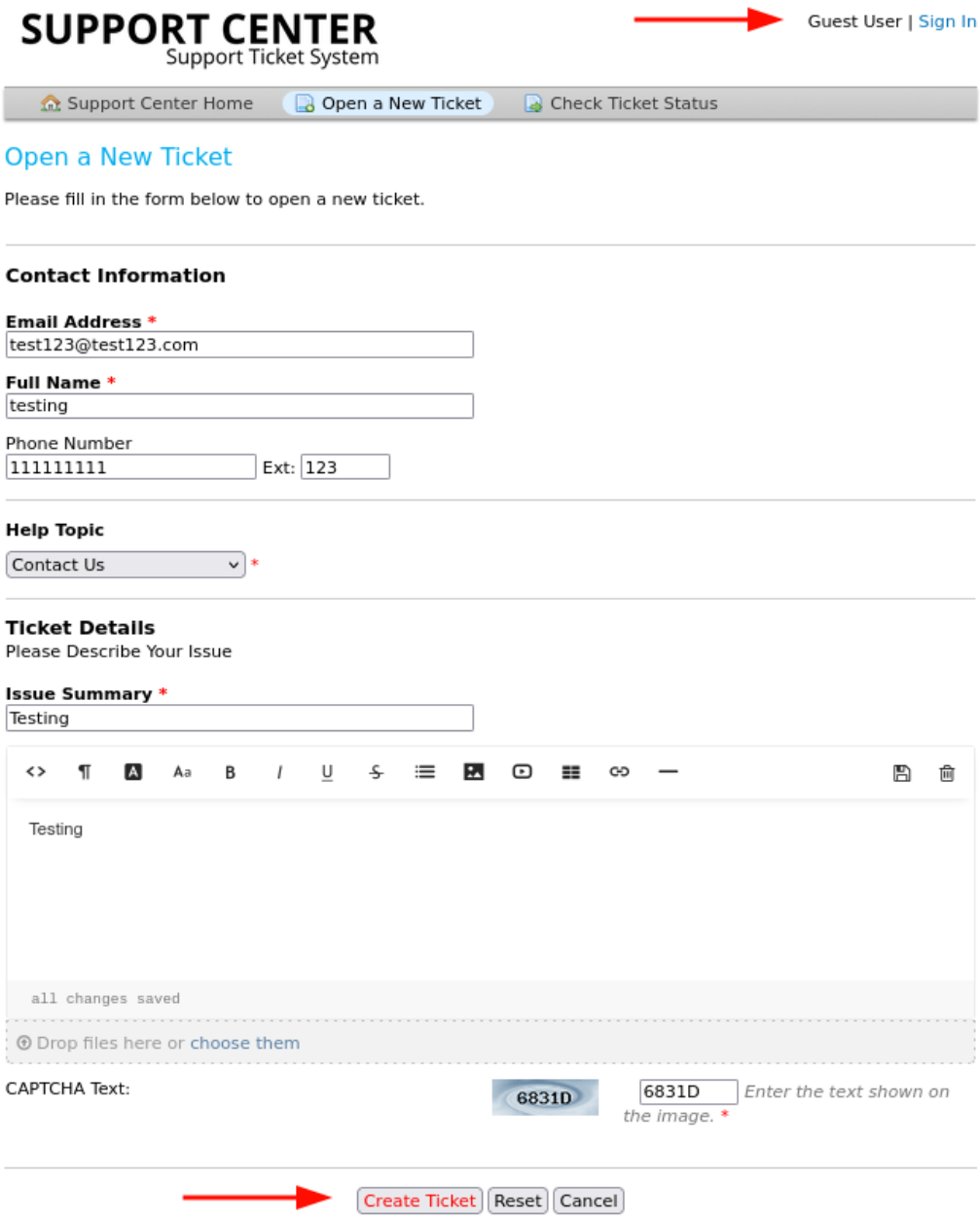
Port	Protocol	State	Service
22	tcp	open	ssh
80	tcp	open	http
8065	tcp	open	unknown

Penetration Proof of Concept

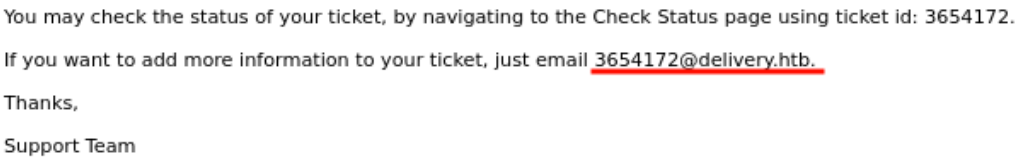
Initial Access | User Flag

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:

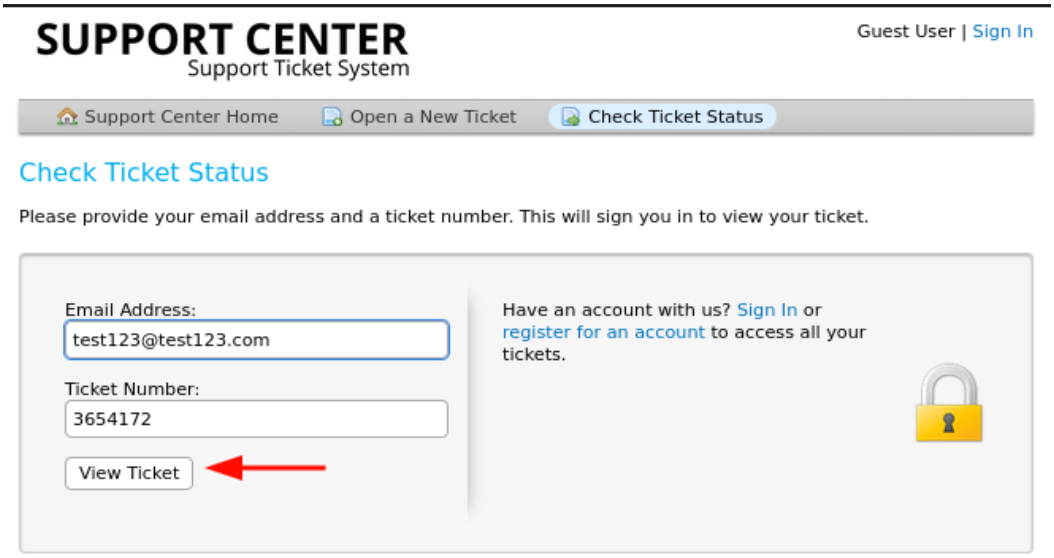
- http://helpdesk.delivery.htb/
- http://delivery.htb:8065/
  On the first one, there is the possibility for any user to create a ticket and send it to help-desk by creating a test account.



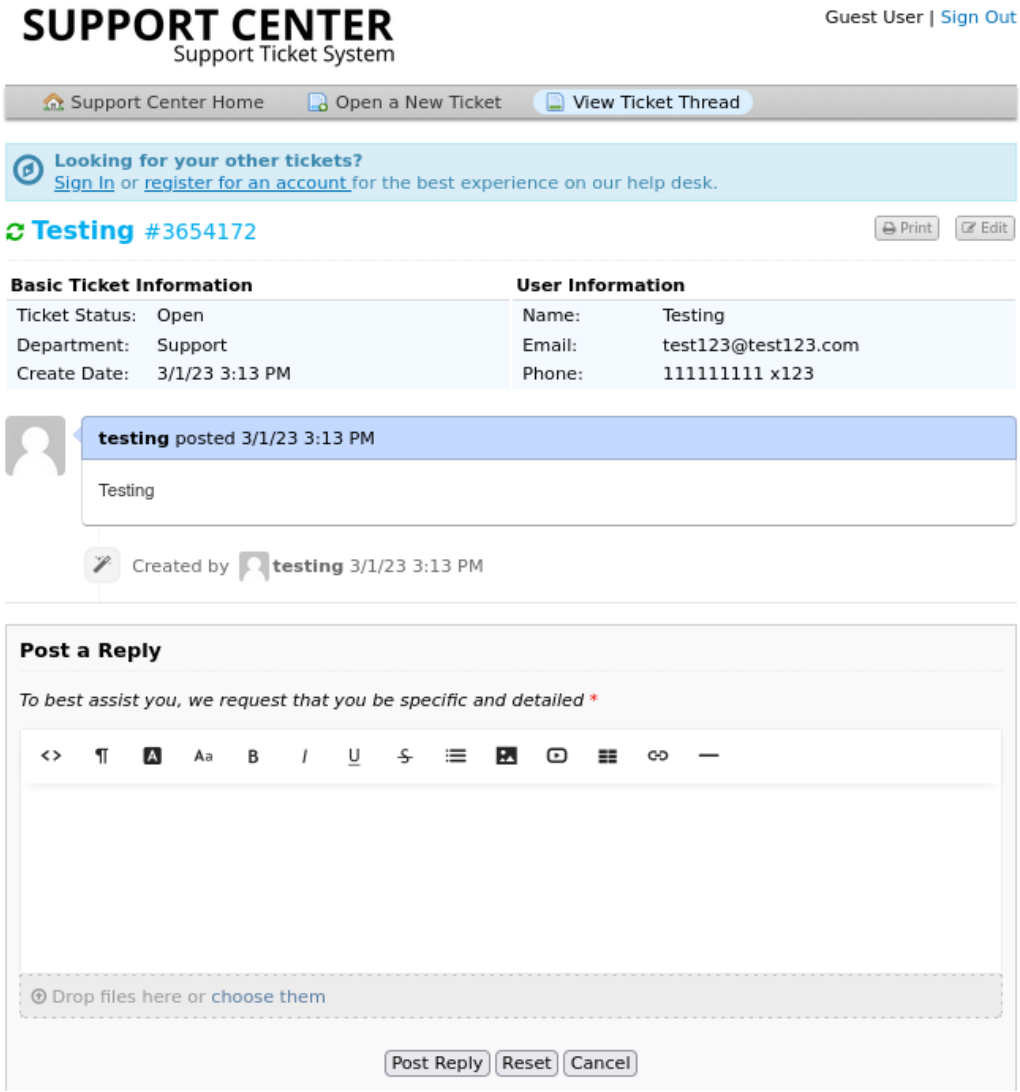
By creating this ticket, there is an automated response that returns back an internal mail.



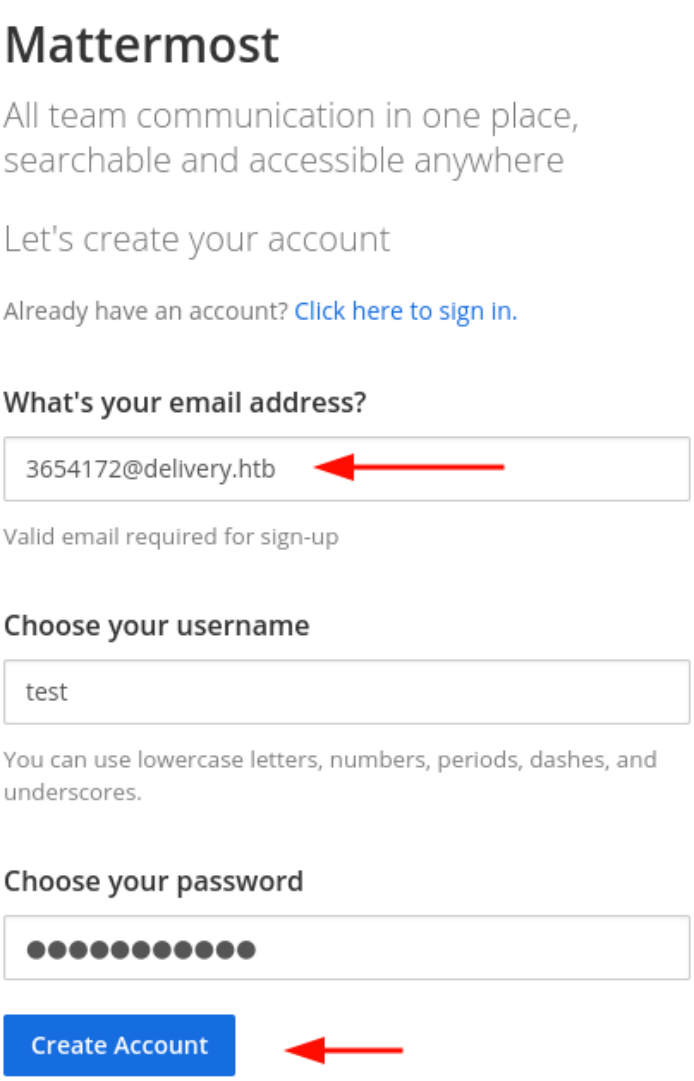
There is an option to log in to check the ticket status.



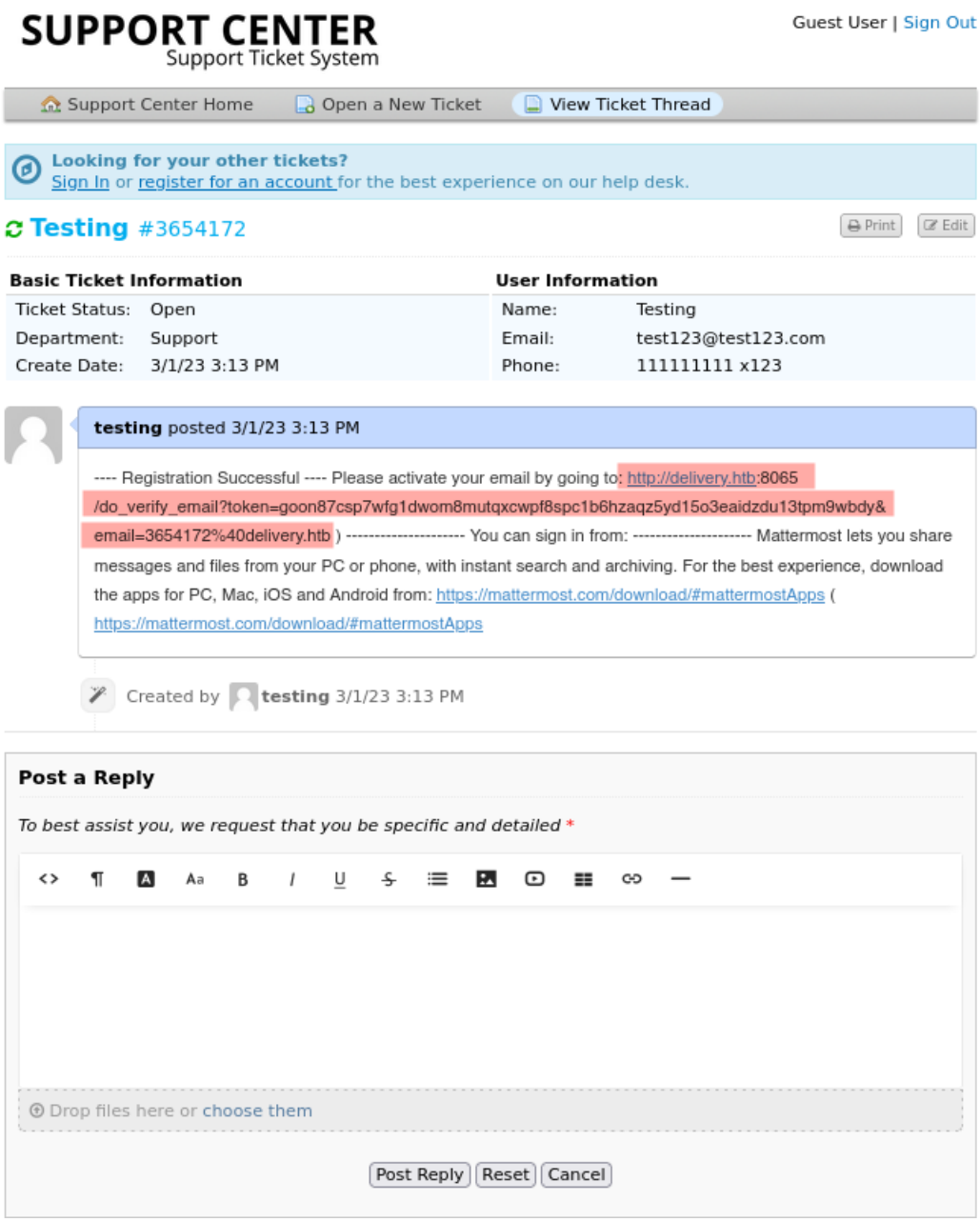
Once opened, the ticket is displayed



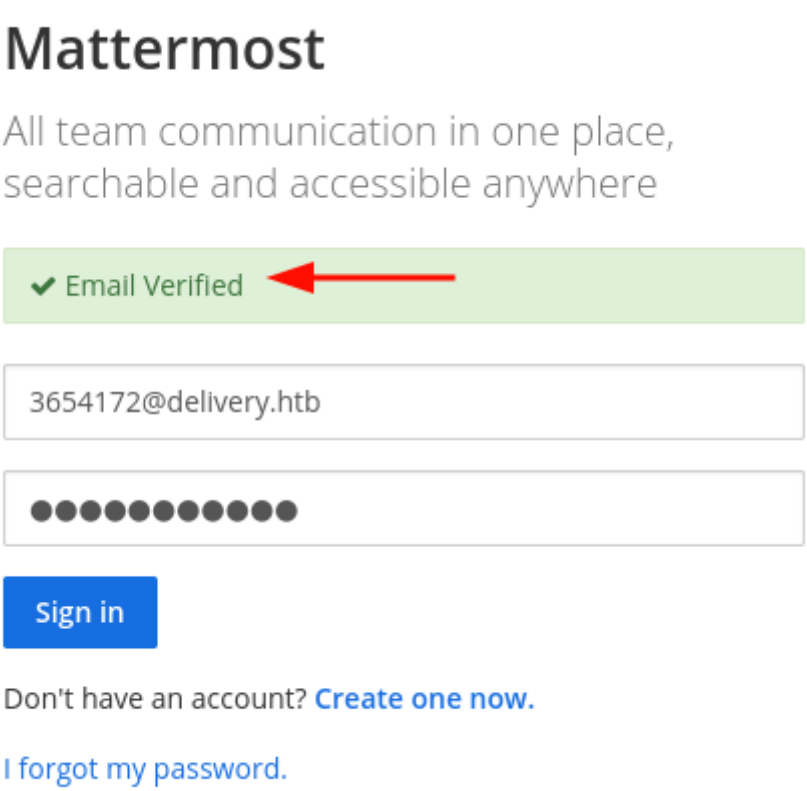
Let's see if the internal mail given can be used to log in the second web page by creating an account using the support mail



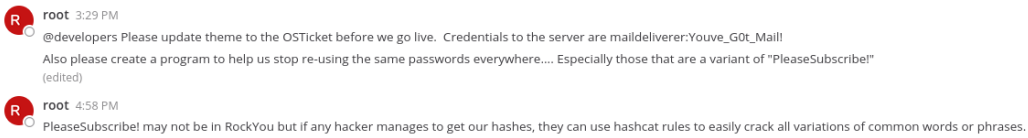
Once the account is created a *Please verify your mail* message is displayed. Because how the help-desk software works, this mail is displayed in the ticket's portal. All it has to be done is refreshing the page.



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



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



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)/matt
ermost?
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 *PleaseSuscribe!* 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 ✔