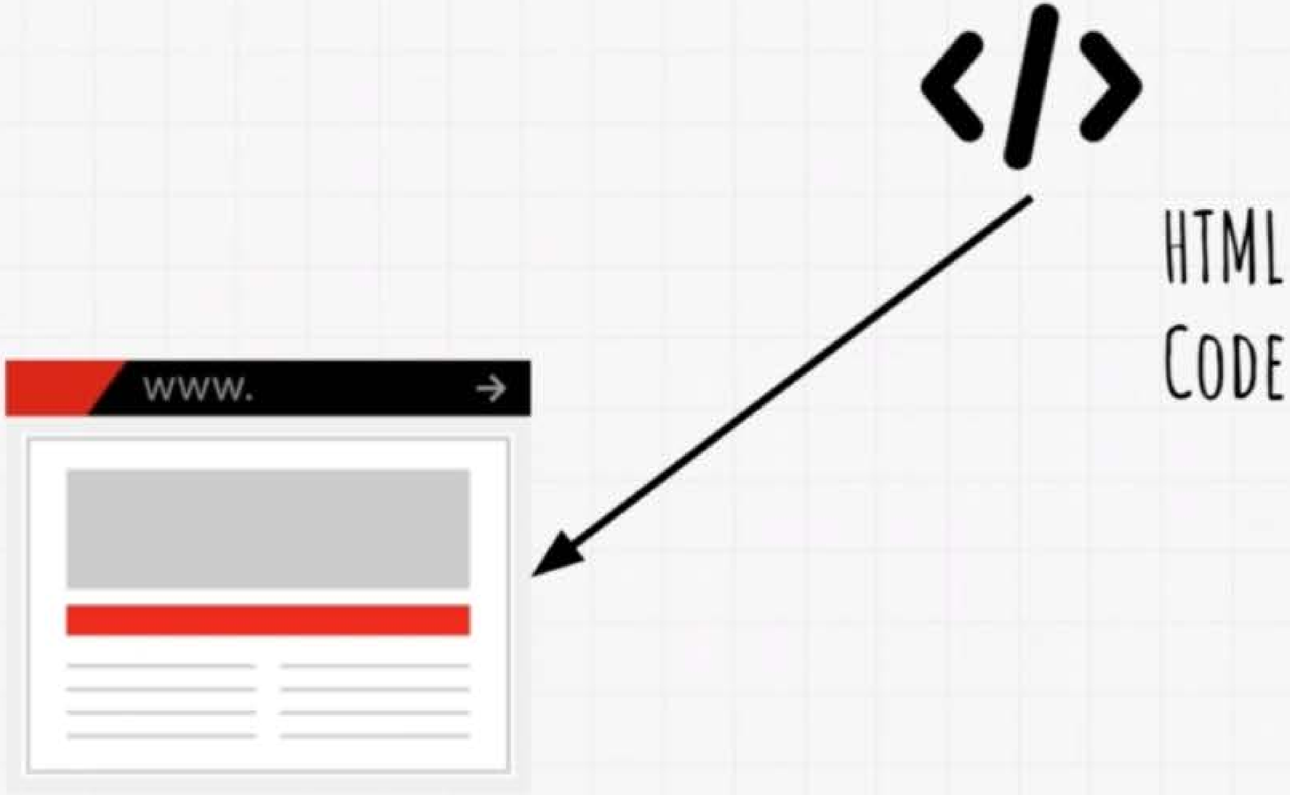
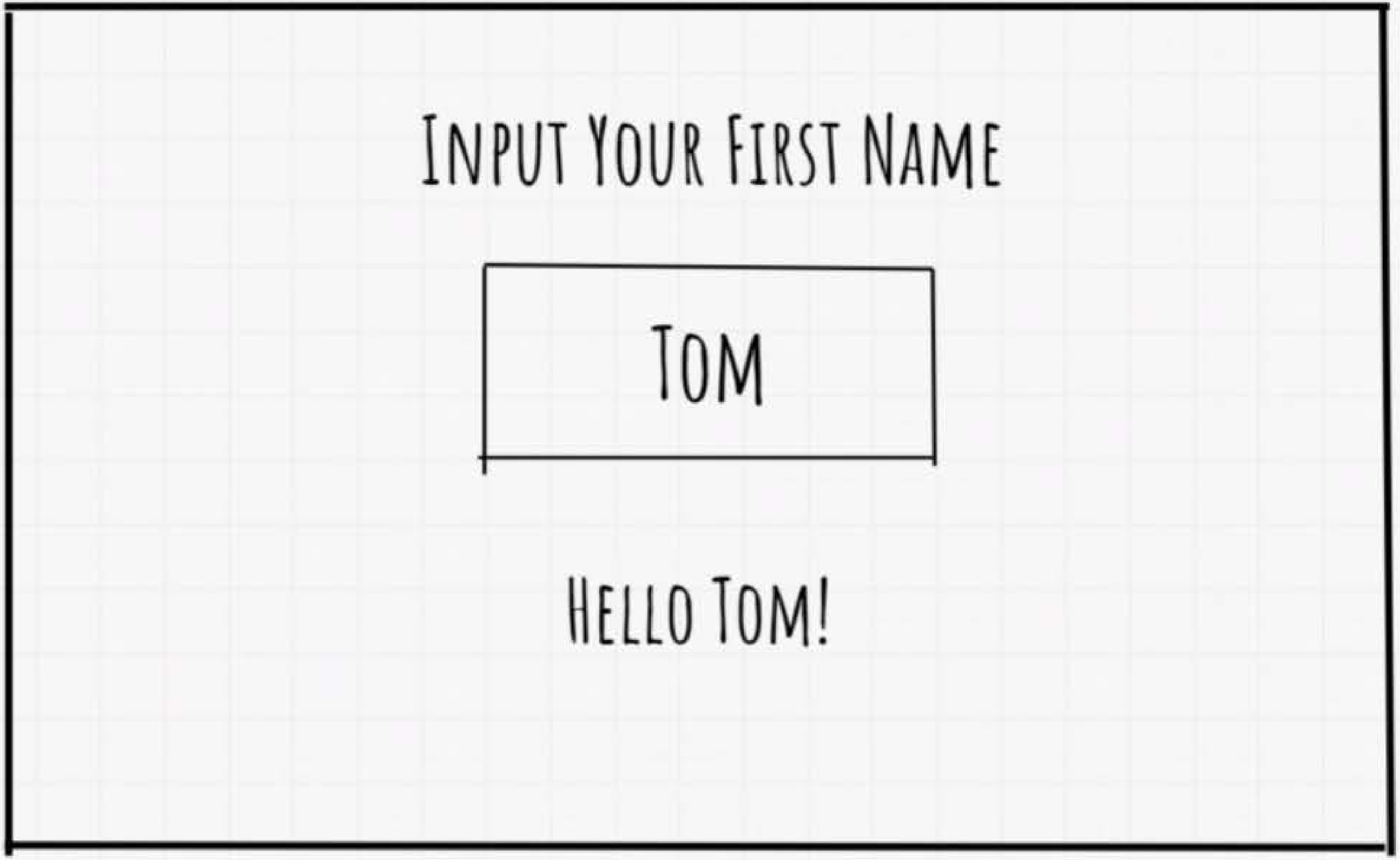
1.



HTML Code

1.



Input Your First Name

Tom

Hello Tom!

1.

<H1>TEST</H1> ?

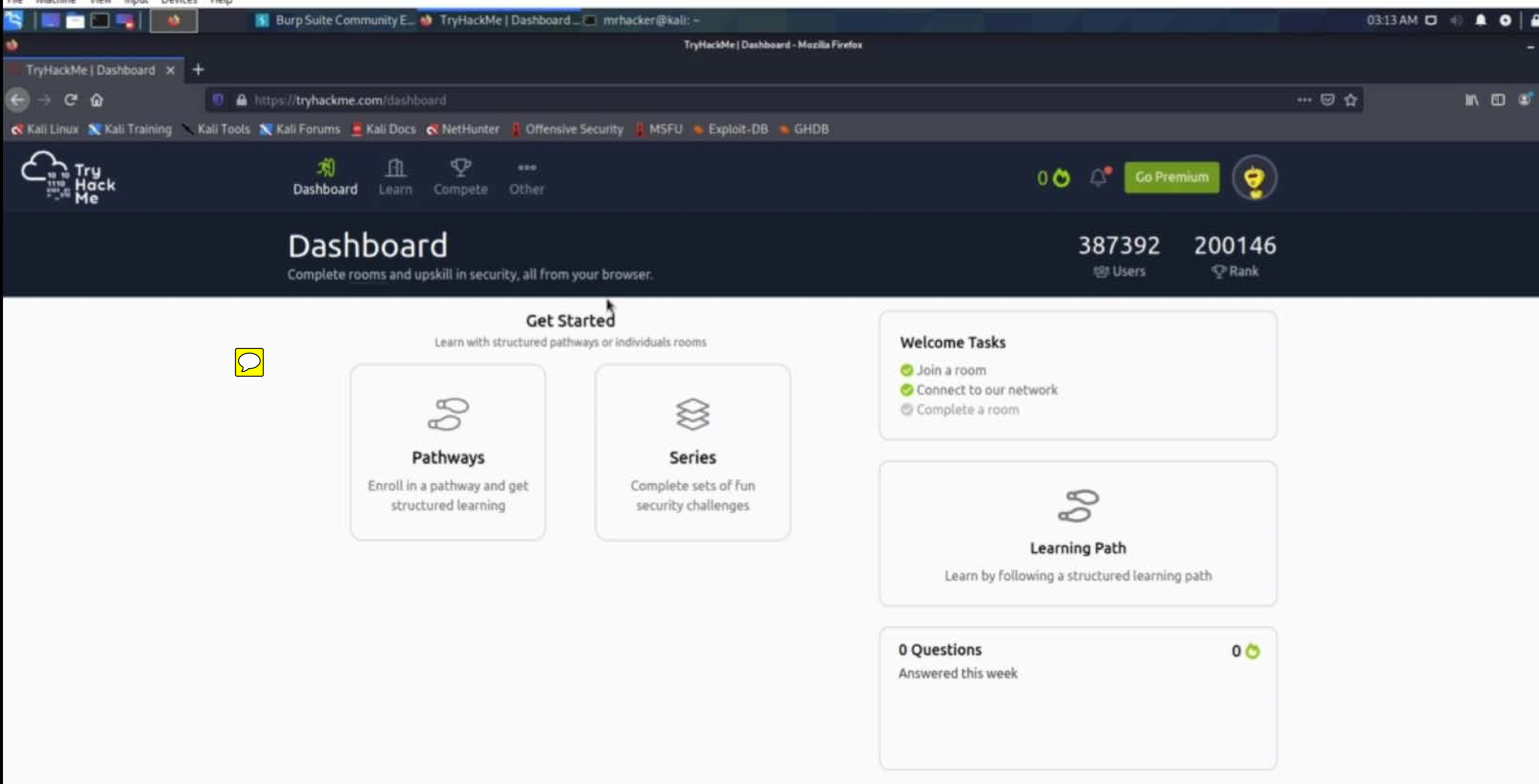
```
<div class="vulnerable_code_area">
    <form name="HTMLi" action="#" method="GET">
      <p>What's your name?</p>
      <input type="text" name="name">
      <input type="submit" value="Submit">
    </form>
    <pre>Hello Tom</pre>
  </div>
```

1.

<H1>TEST</H1> ?

```
<div class="vulnerable_code_area">
    <form name="HTMLi" action="#" method="GET">
      <p>What's your name?</p>
      <input type="text" name="name">
      <input type="submit" value="Submit">
    </form>
    <pre>Hello <h1>TEST</h1></pre>
  </div>
```

YEP, THIS IS HTML!



Dashboard

Complete rooms and upskill in security, all from your browser.

387392 Users

200146 Rank

Get Started

Learn with structured pathways or individuals rooms

Pathways

Enroll in a pathway and get structured learning

Series

Complete sets of fun security challenges

Welcome Tasks

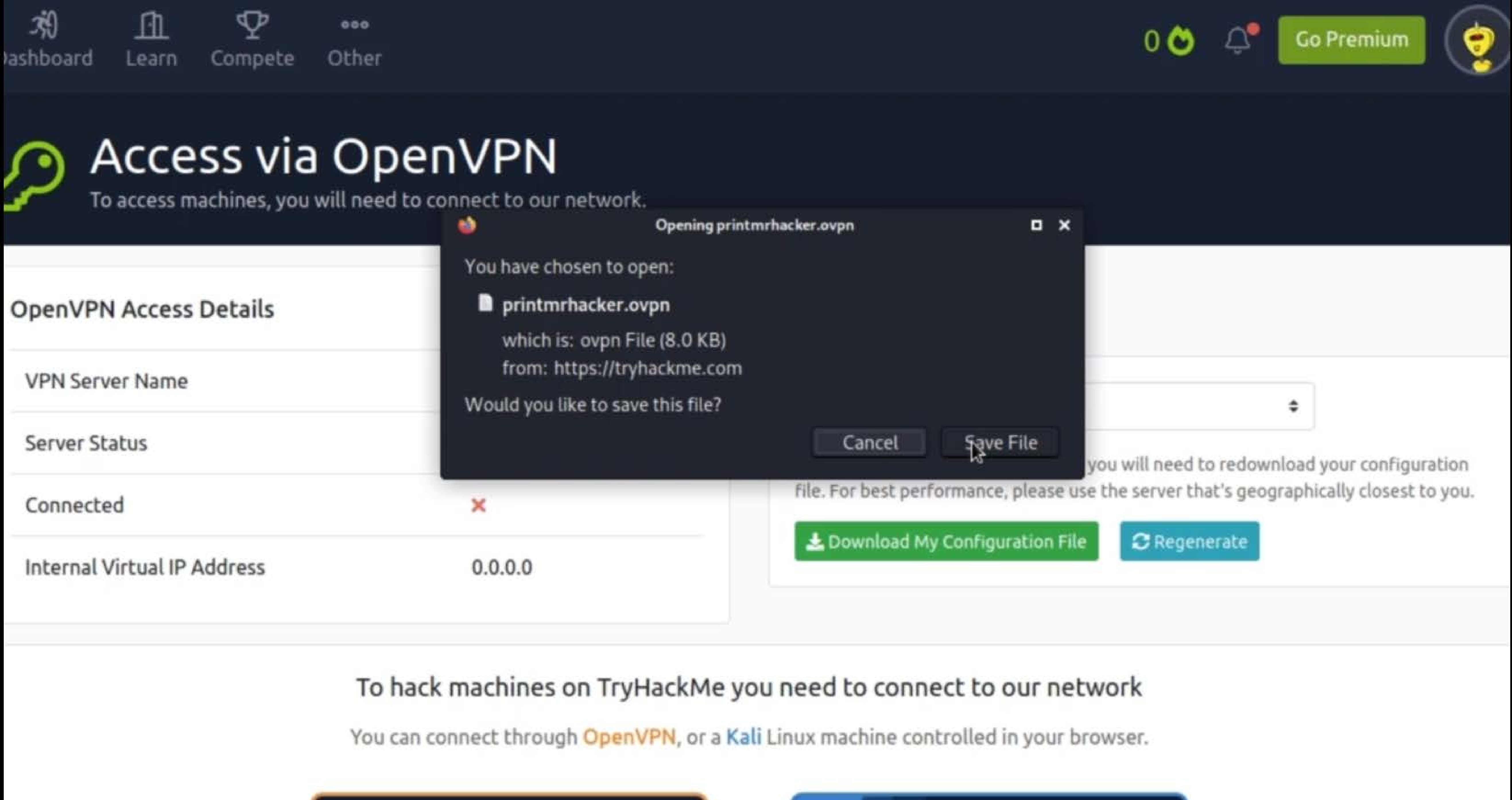
- ✓ Join a room
- ✓ Connect to our network
- ○ Complete a room

Learning Path

Learn by following a structured learning path

0 Questions 0

Answered this week



Access via OpenVPN

To access machines, you will need to connect to our network.

Opening printmrhacker.ovpn

You have chosen to open:

printmrhacker.ovpn

which is: ovpn File (8.0 KB)
from: https://tryhackme.com

Would you like to save this file?

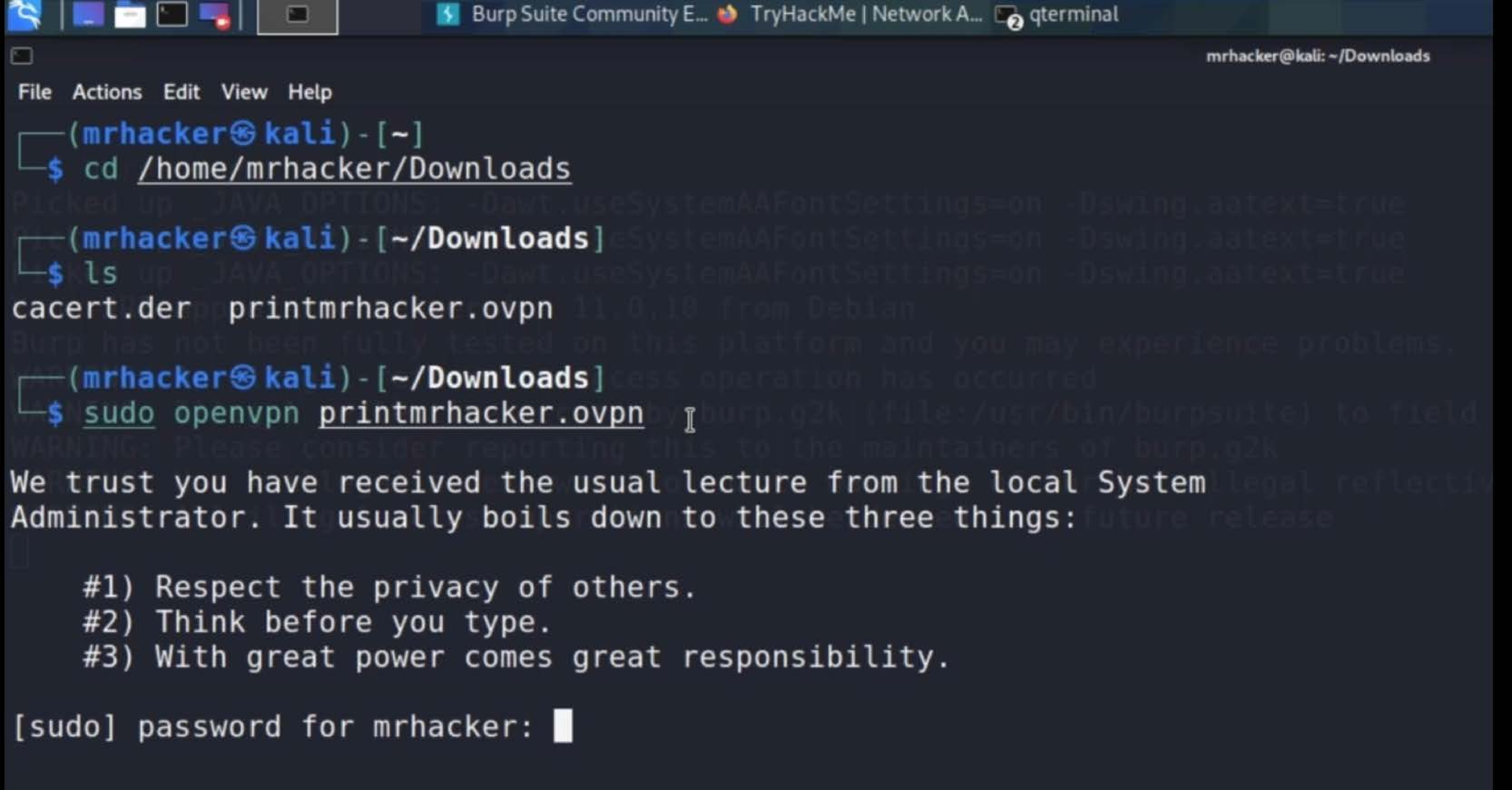
OpenVPN Access Details

VPN Server Name	
Server Status	
Connected	✗
Internal Virtual IP Address	0.0.0.0

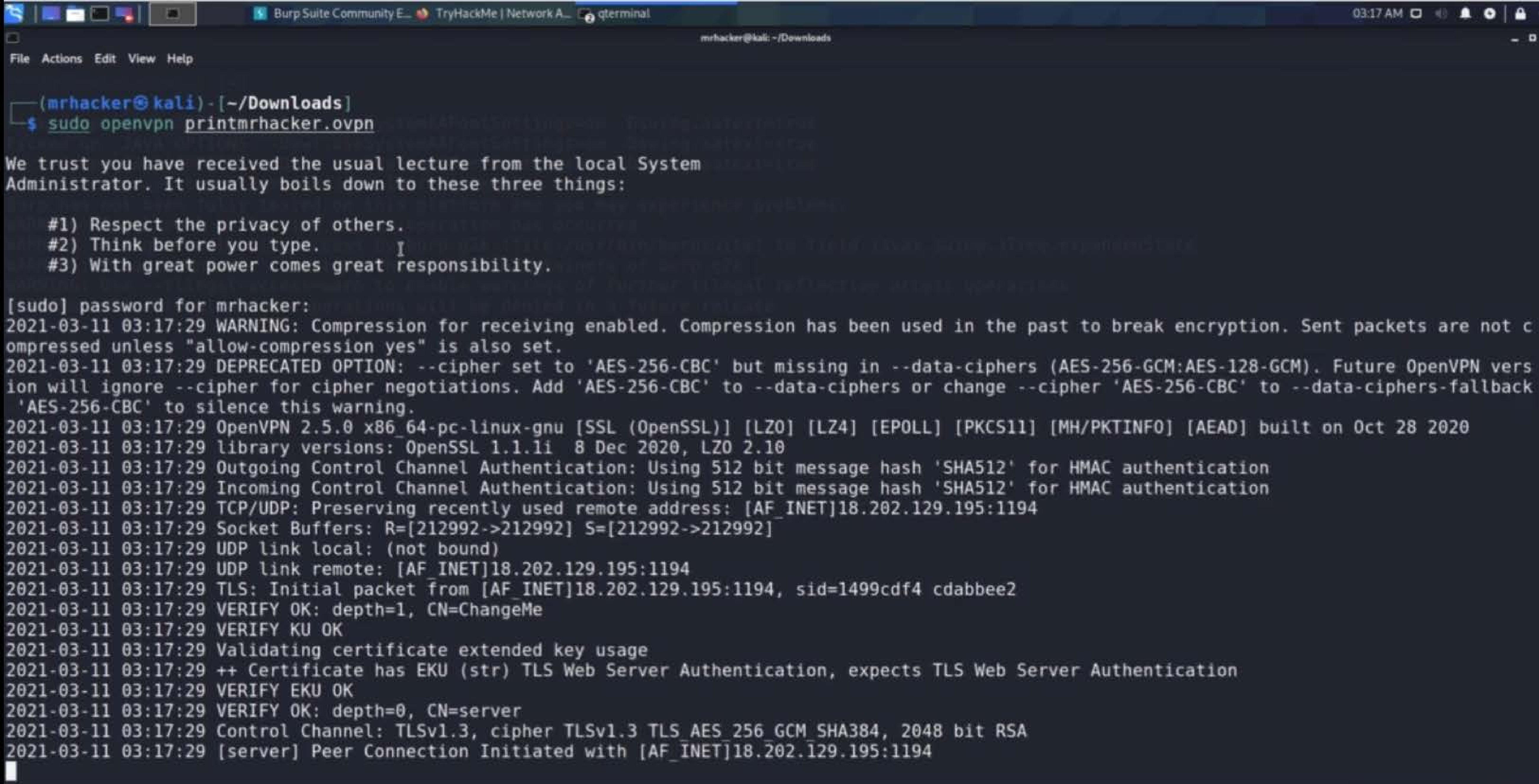
you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

To hack machines on TryHackMe you need to connect to our network

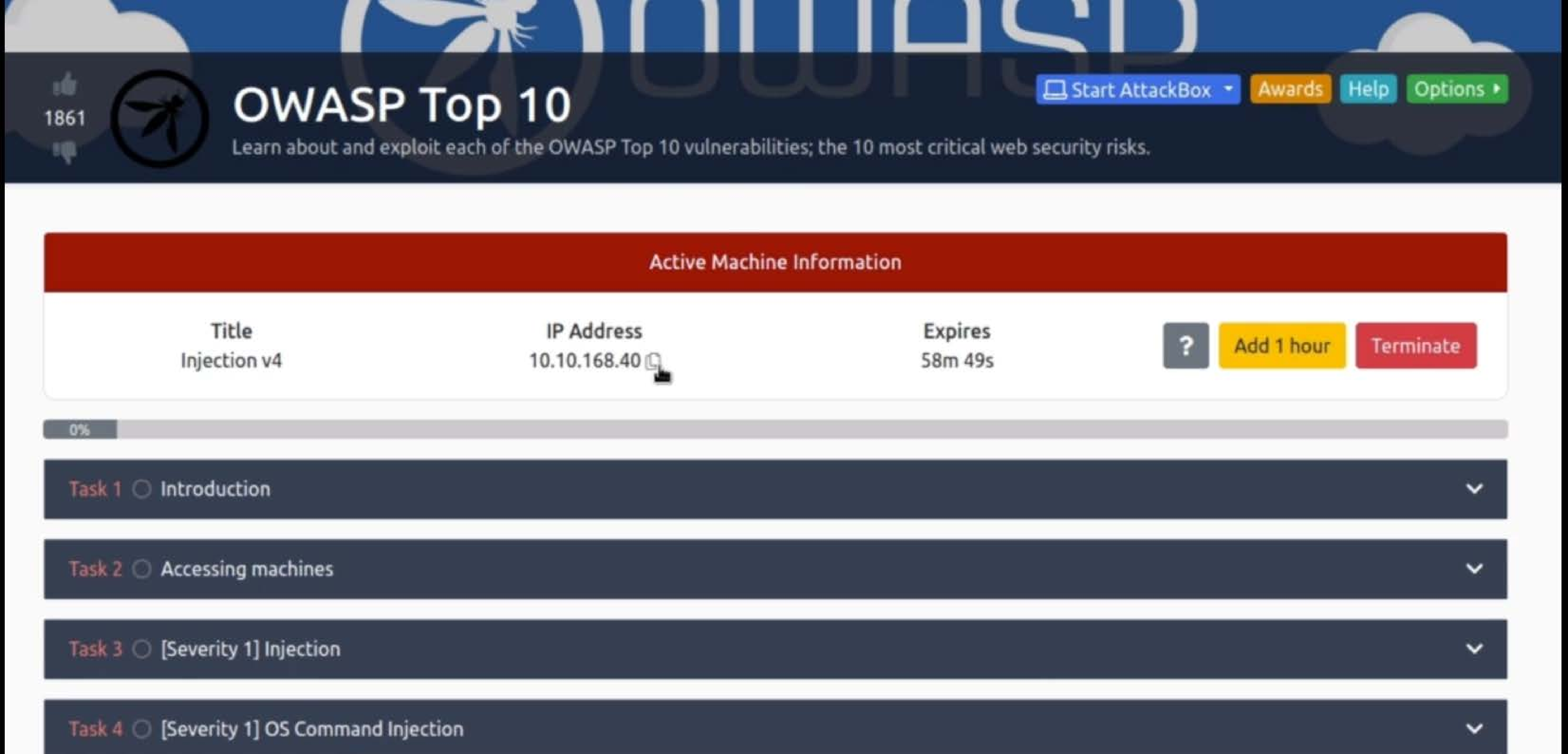
You can connect through OpenVPN, or a Kali Linux machine controlled in your browser.



```
┌──(mrhacker㉿kali)-[~]
└─$ cd /home/mrhacker/Downloads

┌──(mrhacker㉿kali)-[~/Downloads]
└─$ ls
cacert.der  printmrhacker.ovpn

┌──(mrhacker㉿kali)-[~/Downloads]
└─$ sudo openvpn printmrhacker.ovpn

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for mrhacker: 
```



```
┌──(mrhacker㉿kali)-[~/Downloads]
└─$ sudo openvpn printmrhacker.ovpn

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for mrhacker:
2021-03-11 03:17:29 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not c
ompressed unless "allow-compression yes" is also set.
2021-03-11 03:17:29 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN vers
ion will ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to --data-ciphers-fallback
 'AES-256-CBC' to silence this warning.
2021-03-11 03:17:29 OpenVPN 2.5.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Oct 28 2020
2021-03-11 03:17:29 library versions: OpenSSL 1.1.1i  8 Dec 2020, LZO 2.10
2021-03-11 03:17:29 Outgoing Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
2021-03-11 03:17:29 Incoming Control Channel Authentication: Using 512 bit message hash 'SHA512' for HMAC authentication
2021-03-11 03:17:29 TCP/UDP: Preserving recently used remote address: [AF_INET]18.202.129.195:1194
2021-03-11 03:17:29 Socket Buffers: R=[212992->212992] S=[212992->212992]
2021-03-11 03:17:29 UDP link local: (not bound)
2021-03-11 03:17:29 UDP link remote: [AF_INET]18.202.129.195:1194
2021-03-11 03:17:29 TLS: Initial packet from [AF_INET]18.202.129.195:1194, sid=1499cdf4 cdabbee2
2021-03-11 03:17:29 VERIFY OK: depth=1, CN=ChangeMe
2021-03-11 03:17:29 VERIFY KU OK
2021-03-11 03:17:29 Validating certificate extended key usage
2021-03-11 03:17:29 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2021-03-11 03:17:29 VERIFY EKU OK
2021-03-11 03:17:29 VERIFY OK: depth=0, CN=server
2021-03-11 03:17:29 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 2048 bit RSA
2021-03-11 03:17:29 [server] Peer Connection Initiated with [AF_INET]18.202.129.195:1194
```



OWASP Top 10

Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.

Active Machine Information

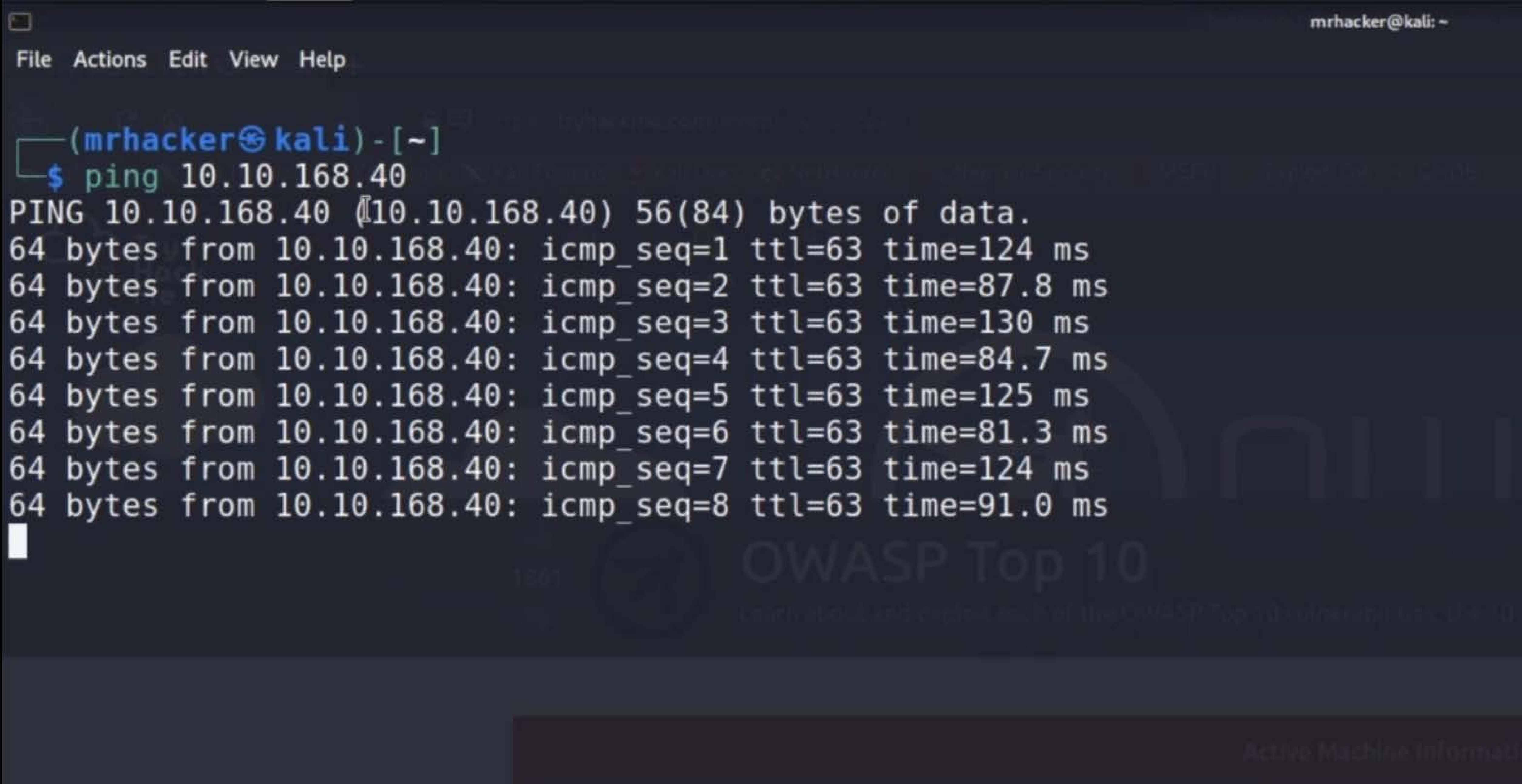
Title	IP Address	Expires
Injection v4	10.10.168.40	58m 49s

Task 1 ○ Introduction

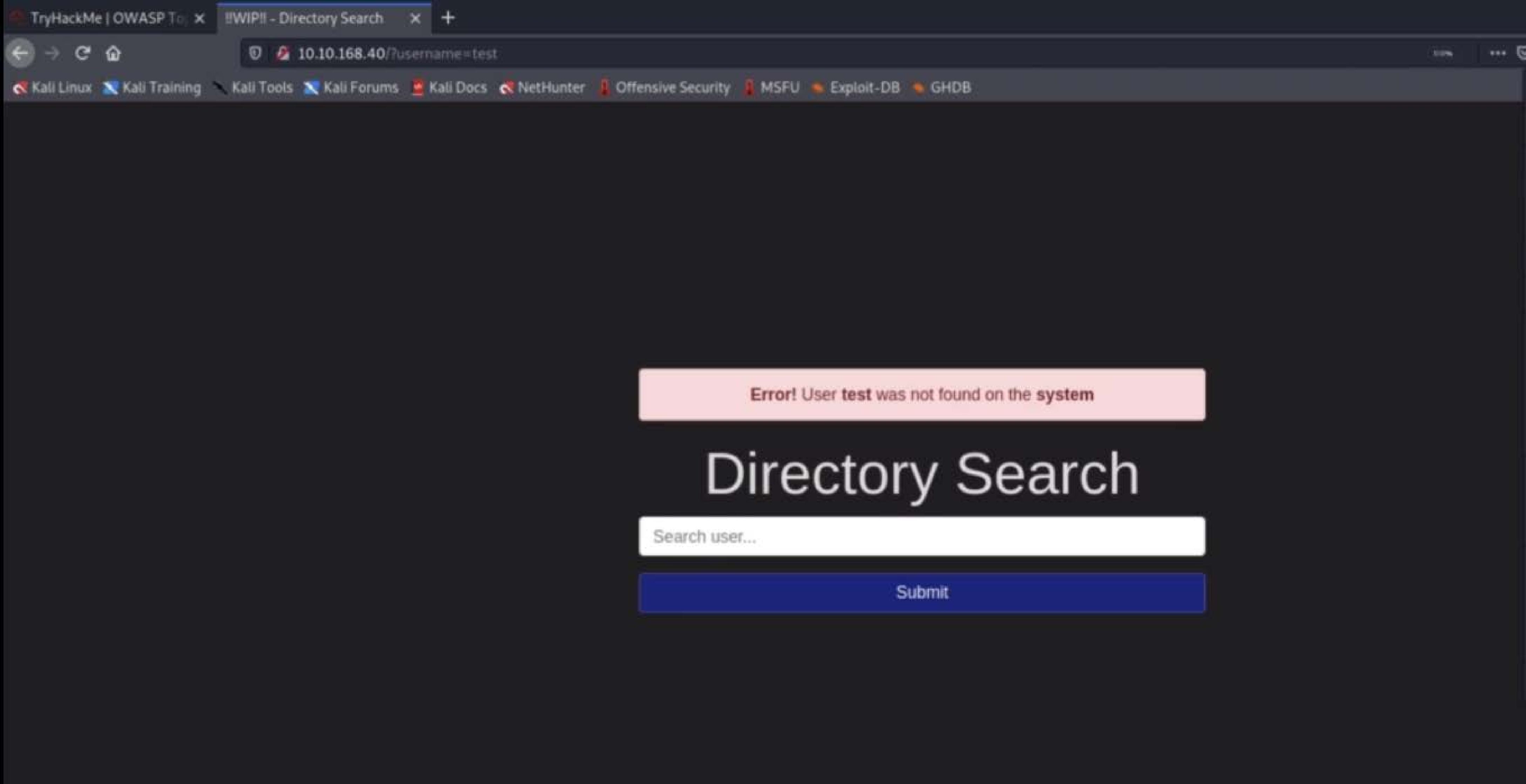
Task 2 ○ Accessing machines

Task 3 ○ [Severity 1] Injection

Task 4 ○ [Severity 1] OS Command Injection



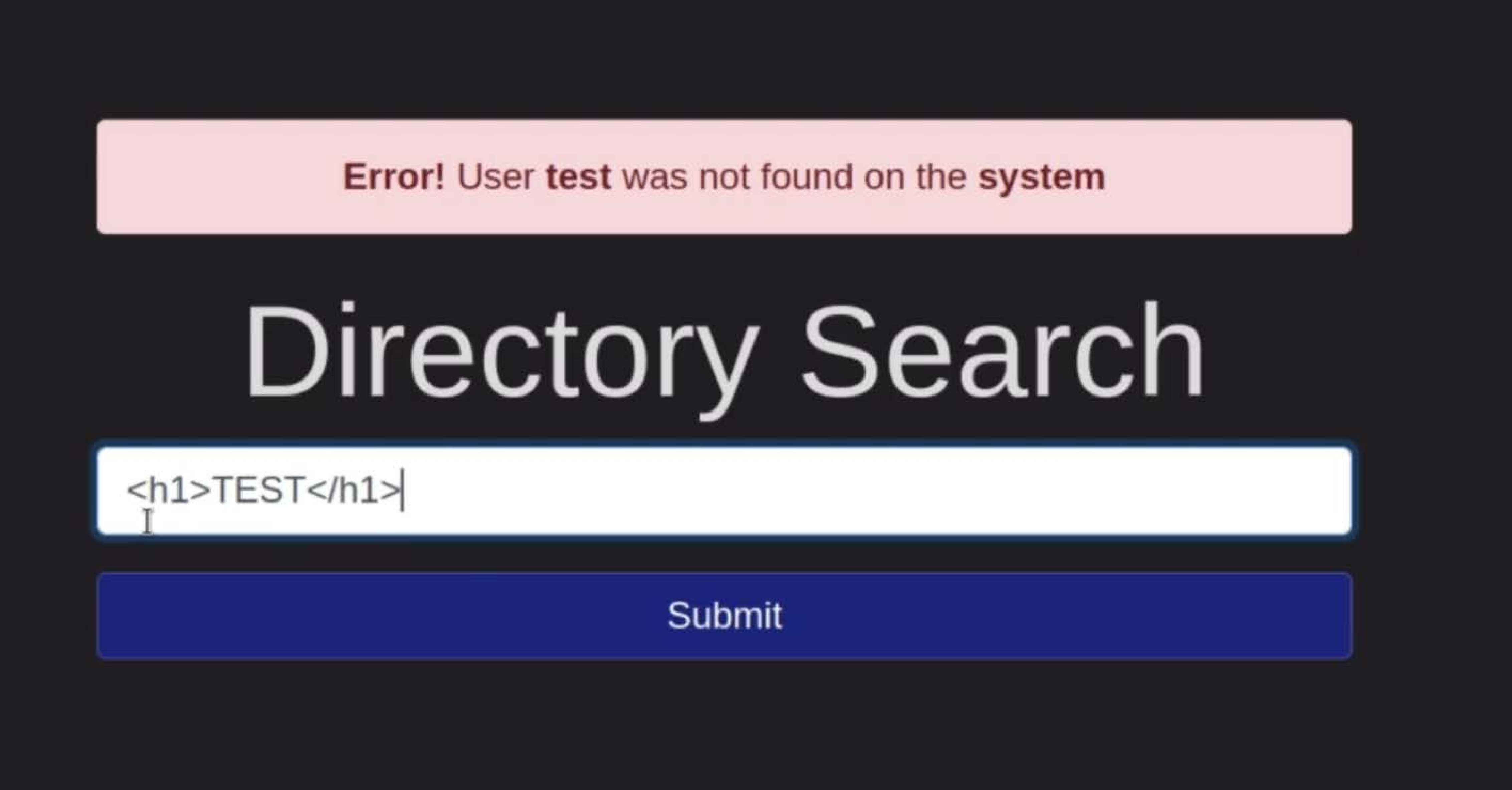
```
┌──(mrhacker㉿kali)-[~]
└─$ ping 10.10.168.40
PING 10.10.168.40 (10.10.168.40) 56(84) bytes of data.
64 bytes from 10.10.168.40: icmp_seq=1 ttl=63 time=124 ms
64 bytes from 10.10.168.40: icmp_seq=2 ttl=63 time=87.8 ms
64 bytes from 10.10.168.40: icmp_seq=3 ttl=63 time=130 ms
64 bytes from 10.10.168.40: icmp_seq=4 ttl=63 time=84.7 ms
64 bytes from 10.10.168.40: icmp_seq=5 ttl=63 time=125 ms
64 bytes from 10.10.168.40: icmp_seq=6 ttl=63 time=81.3 ms
64 bytes from 10.10.168.40: icmp_seq=7 ttl=63 time=124 ms
64 bytes from 10.10.168.40: icmp_seq=8 ttl=63 time=91.0 ms
```



Error! User **test** was not found on the **system**

Directory Search

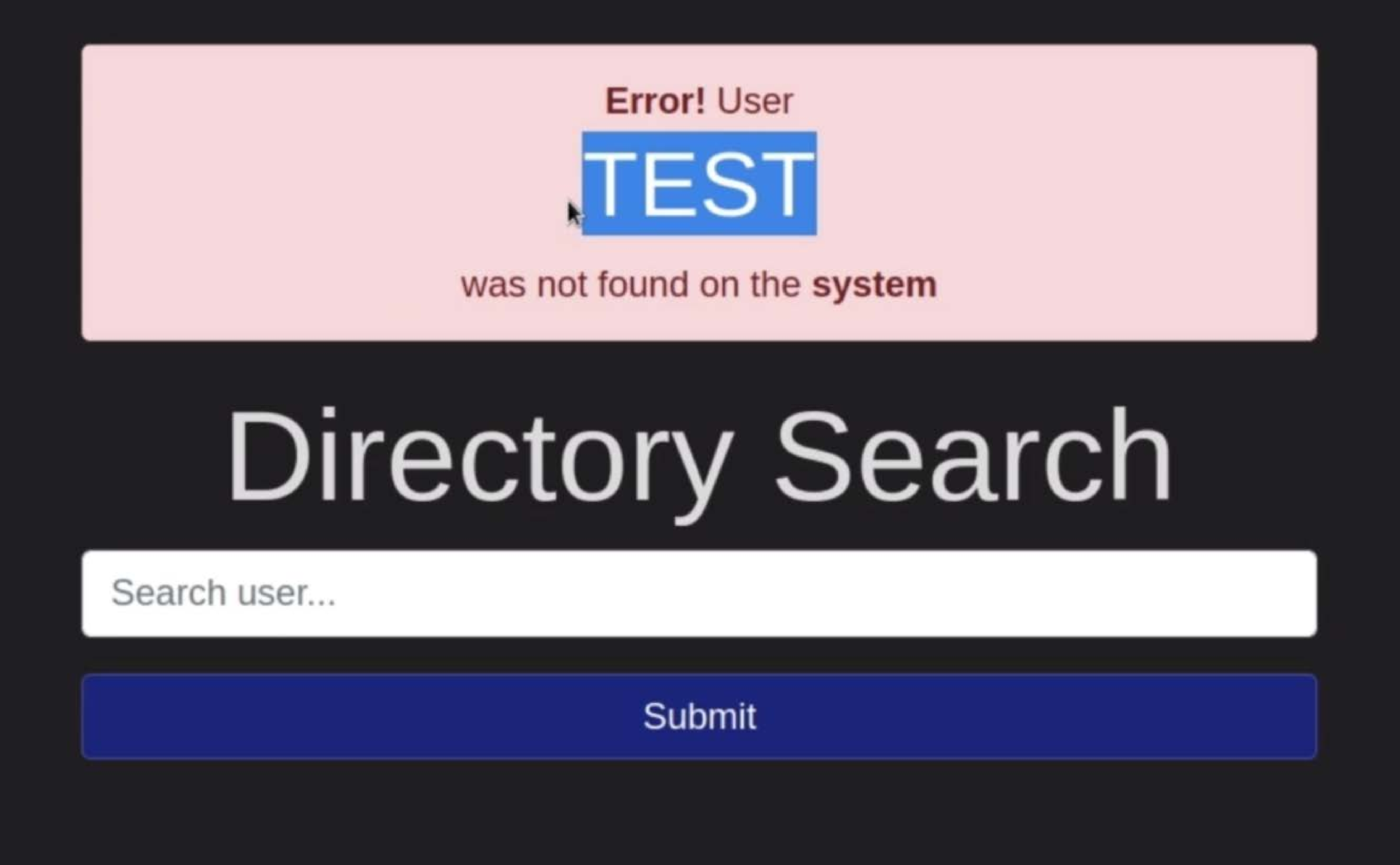
Search user...



Error! User **test** was not found on the **system**

Directory Search

<h1>TEST</h1>

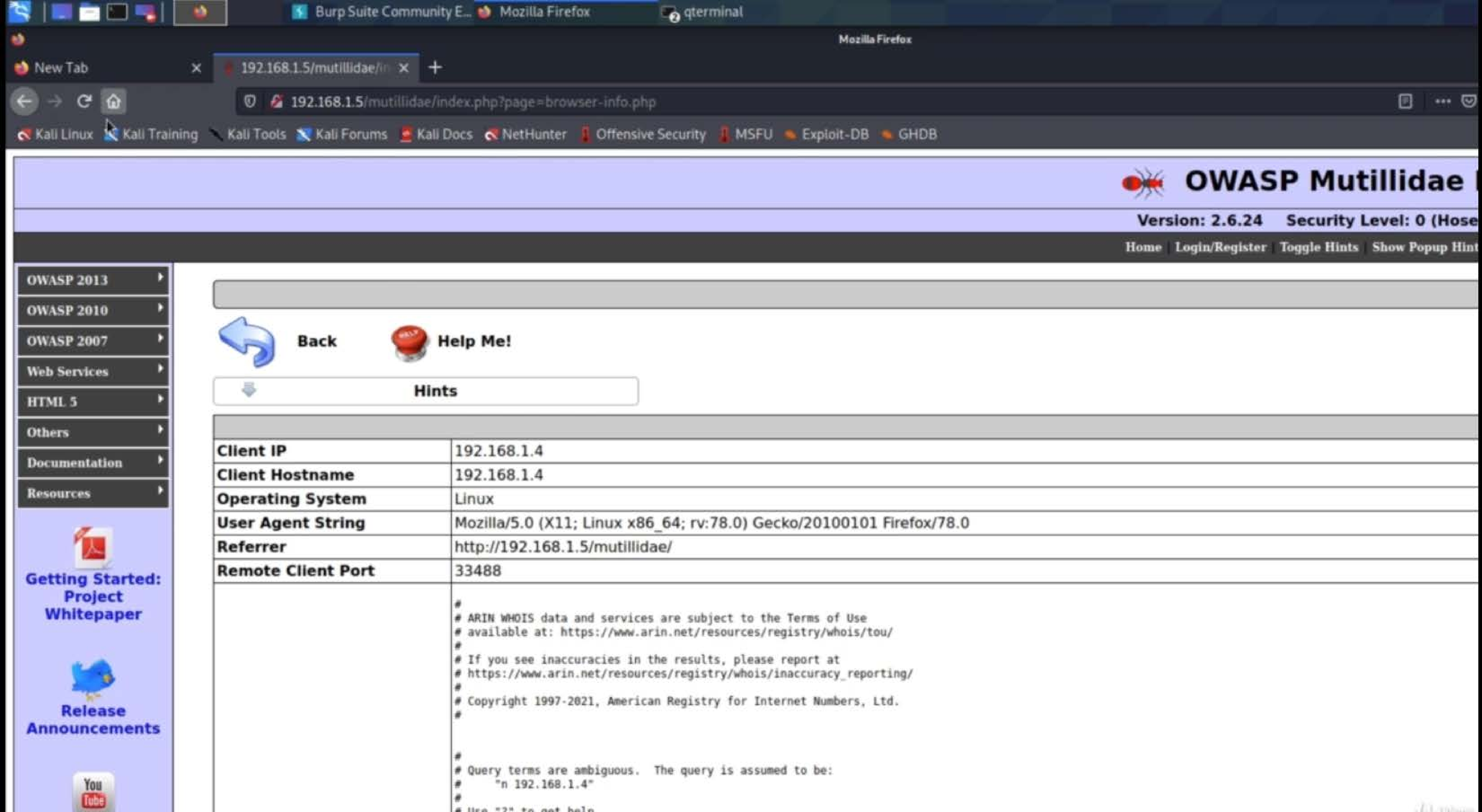


Error! User

TEST

was not found on the **system**

Directory Search

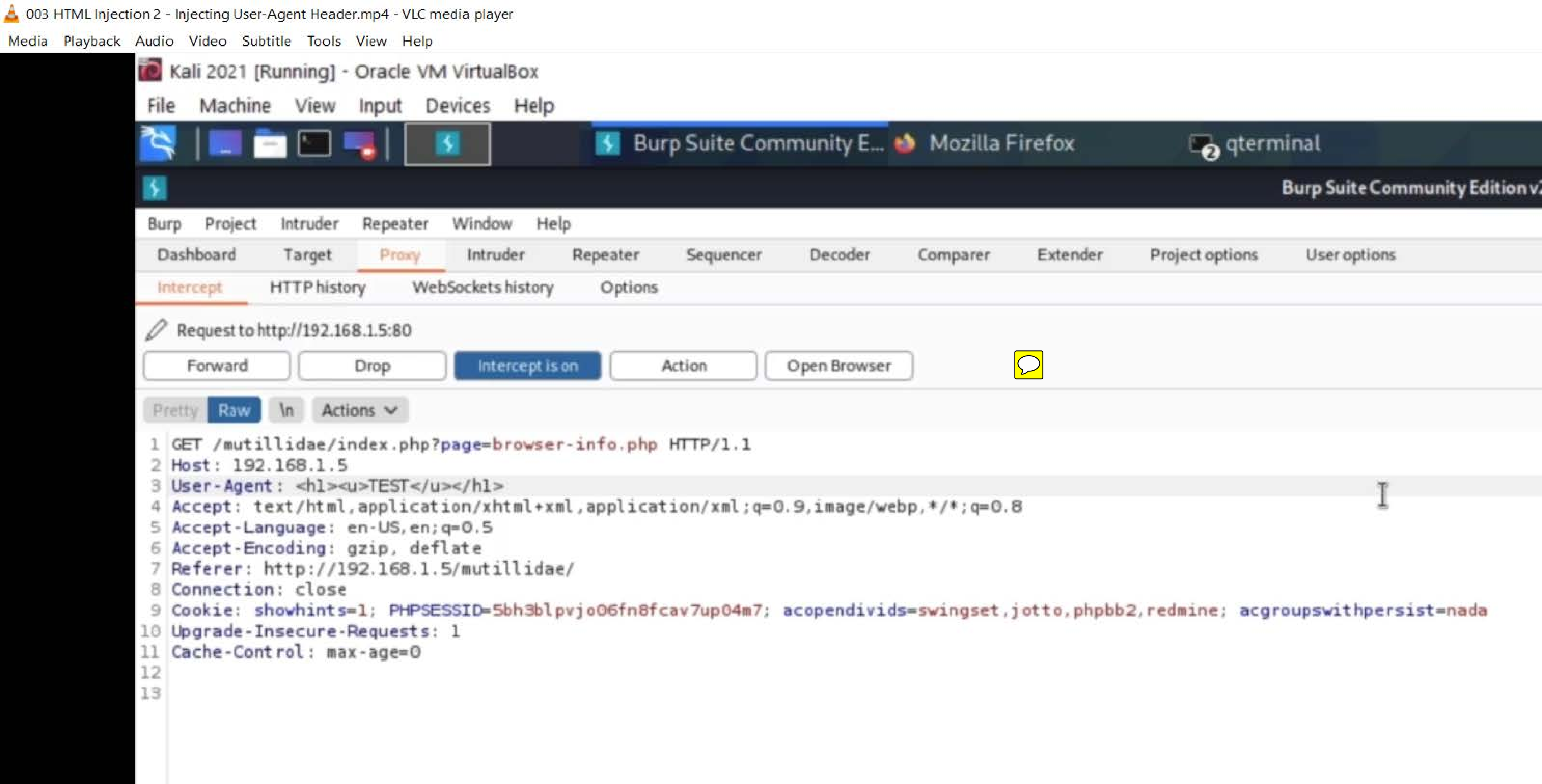


192.168.1.5/mutillidae/index.php?page=browser-info.php

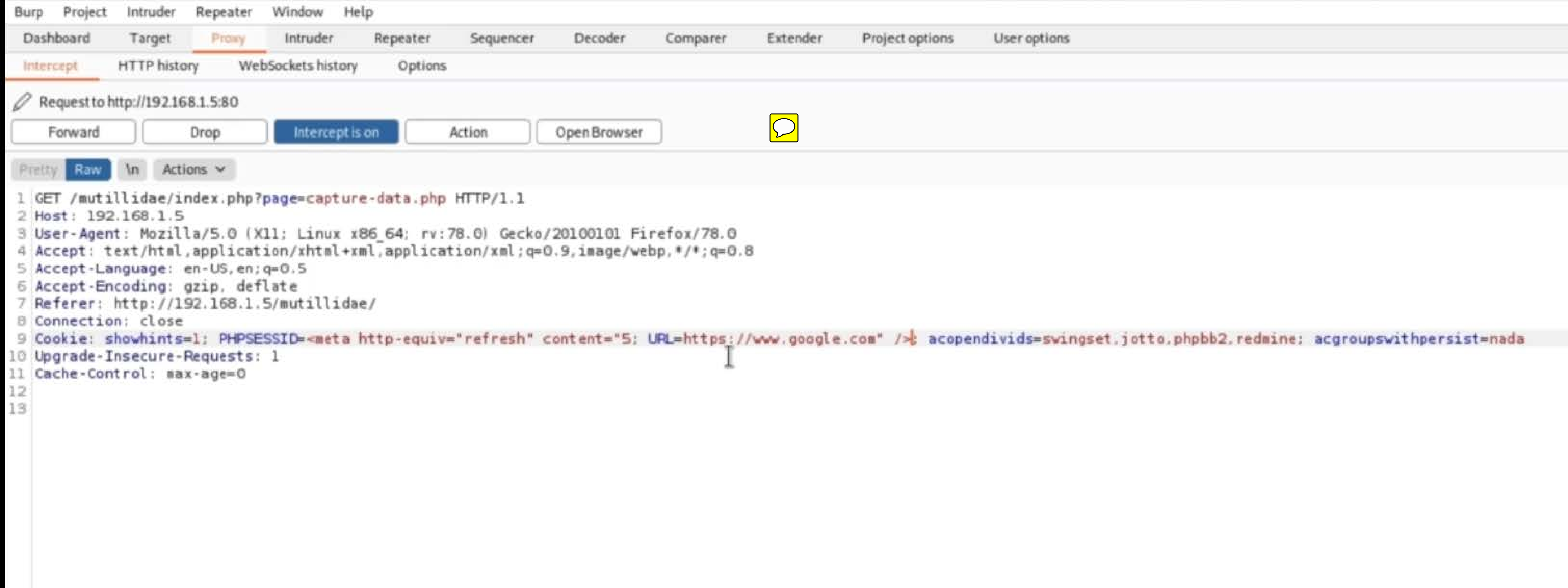
Version: 2.6.24 Security Level: 0 (Hose

Client IP	192.168.1.4
Client Hostname	192.168.1.4
Operating System	Linux
User Agent String	Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Referrer	http://192.168.1.5/mutillidae/
Remote Client Port	33488

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#



#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 192.168.1.4"
#
# Use "?" to get help
```

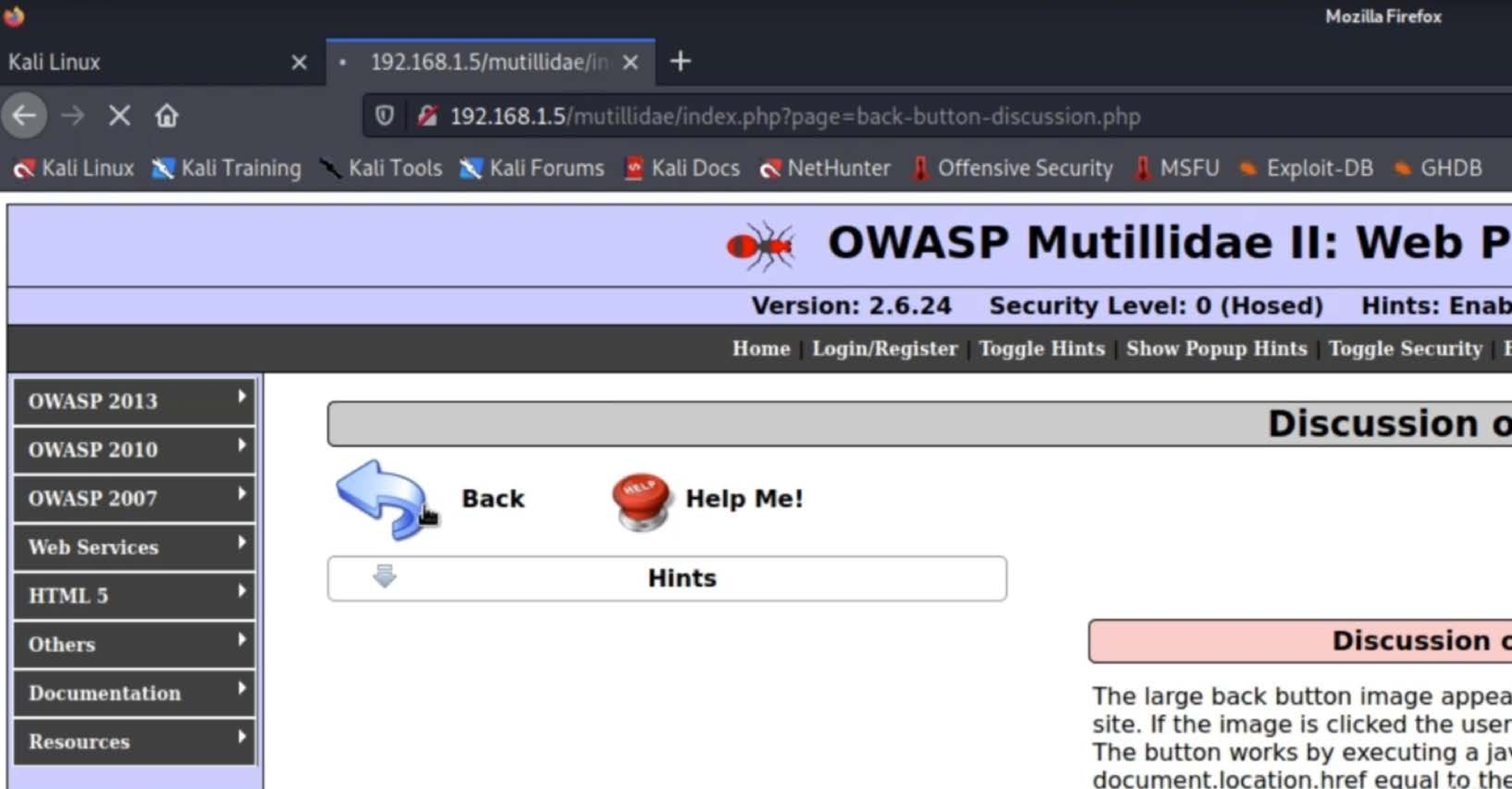

003 HTML Injection 2 - Injecting User-Agent Header.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Kali 2021 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Burp Suite Community E...
Mozilla Firefox
qterminal
Burp Suite Community Edition v
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://192.168.1.5:80
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions

```
GET /mutillidae/index.php?page=browser-info.php HTTP/1.1
Host: 192.168.1.5
User-Agent: <h1><u>TEST</u></h1>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.5/mutillidae/
Connection: close
Cookie: showhints=1; PHPSESSID=5bh3blpvjo06fn8fcav7up04m7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```



Request to http://192.168.1.5:80

```
GET /mutillidae/index.php?page=capture-data.php HTTP/1.1
Host: 192.168.1.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.5/mutillidae/
Connection: close
Cookie: showhints=1; PHPSESSID=<meta http-equiv="refresh" content="5; URL=https://www.google.com" />; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



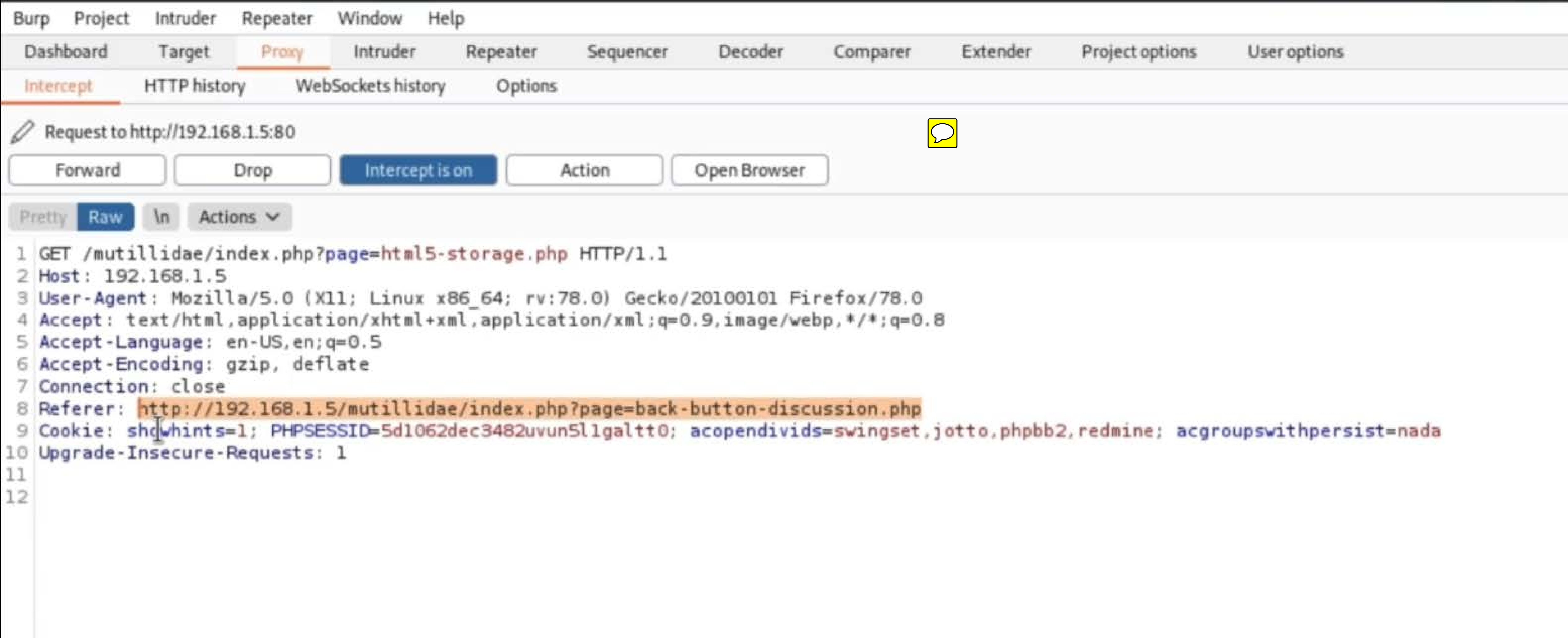
OWASP Mutillidae II: Web P

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enab

Discussion o

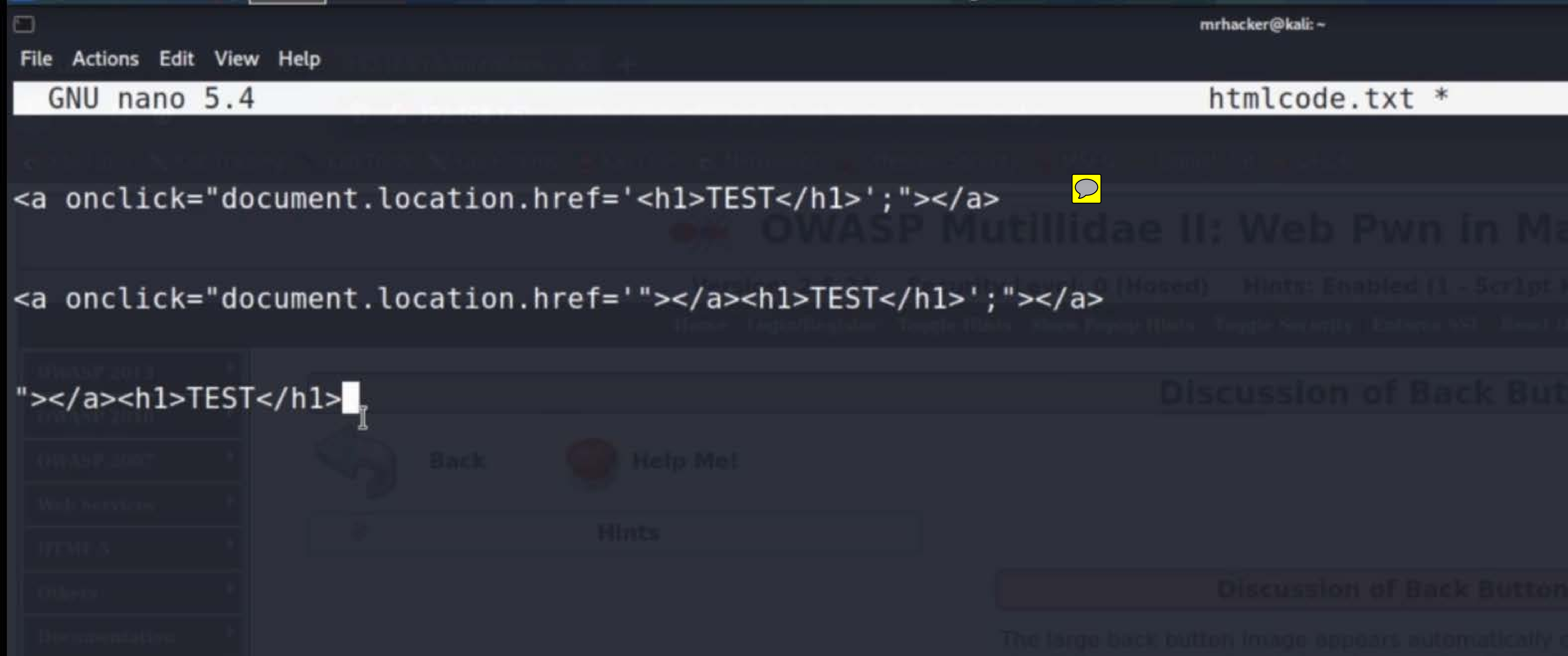
Discussion o

The large back button image appea
site. If the image is clicked the user
The button works by executing a ja
document.location.href equal to the



Request to http://192.168.1.5:80

```
GET /mutillidae/index.php?page=html5-storage.php HTTP/1.1
Host: 192.168.1.5
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.1.5/mutillidae/index.php?page=back-button-discussion.php
Cookie: showhints=1; PHPSESSID=5d1062dec3482uvun5l1galtt0; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1


```



```
  GNU nano 5.4                                                      htmlcode.txt *

<a onclick="document.location.href='<h1>TEST</h1>';"></a>

<a onclick="document.location.href='"></a><h1>TEST</h1>';"></a>

"></a><h1>TEST</h1>
```