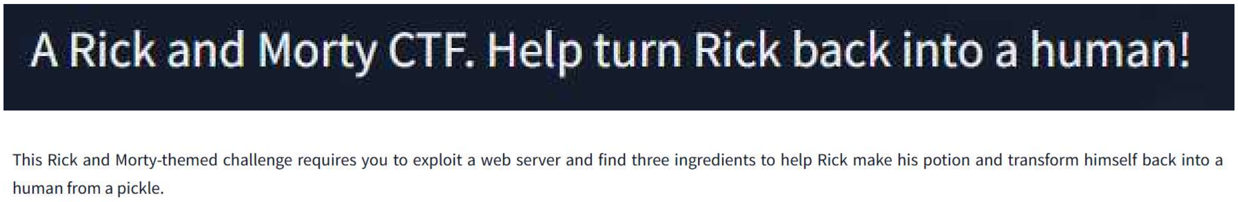
thm picklerick

[TryHackMe | Pickle Rick]

Situation



A Rick and Morty CTF. Help turn Rick back into a human!

This Rick and Morty-themed challenge requires you to exploit a web server and find three ingredients to help Rick make his potion and transform himself back into a human from a pickle.

Reference Pickle Rick Is Born | Rick and Morty | Max (youtube.com)

You need to know basic operation and understanding on linux (commands, permissions exedra)

You need to know basic terms like

Vulnerability definition cybersecurity a weakness or vulnerability that can be exploited to gain unauthorized access to a computer

What is a Vulnerability? Definition + Examples | UpGuard

What is a Cybersecurity Vulnerability? Definition and Types - SecurityScorecard

What are Vulnerabilities, Exploits, and Threats? | Rapid7

Exploit definition cybersecurity a piece of code or software that aims to find and exploit security holes in an application or computer

What Is an Exploit? - Cisco

Exploit in Computer Security | Fortinet

What is an Exploit? | UpGuard

Exploit Definition | What is exploit? (malwarebytes.com)

Payload definition cybersecurity a piece of code that is transferred to a computer or an application that we want to attack that performs a certain task

What is a Payload in Cybersecurity? - Scaler Topics

What is a Payload? (techtarget.com)

Payload | Malwarebytes Glossary

CVE Common Vulnerabilities and Exposures – documentation of vulnerabilities

What is a CVE? (redhat.com)

CVE Explained - What It Is, How It Is Determined, and More (heimdalsecurity.com)

[What Is CVE (Common Vulnerabilities and Exposures)? | IBM]

[CVE - CVE (mitre.org)]

Brute Force is attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.

[What is a Brute Force Attack? | Definition, Types & How It Works (fortinet.com)]

[What is a Brute Force Attack? | Definition, Types & How It Works (fortinet.com)]

[What is a Brute Force Attack? Definition & Examples - CrowdStrike]

first I connect to it with **my machine: kali linux**

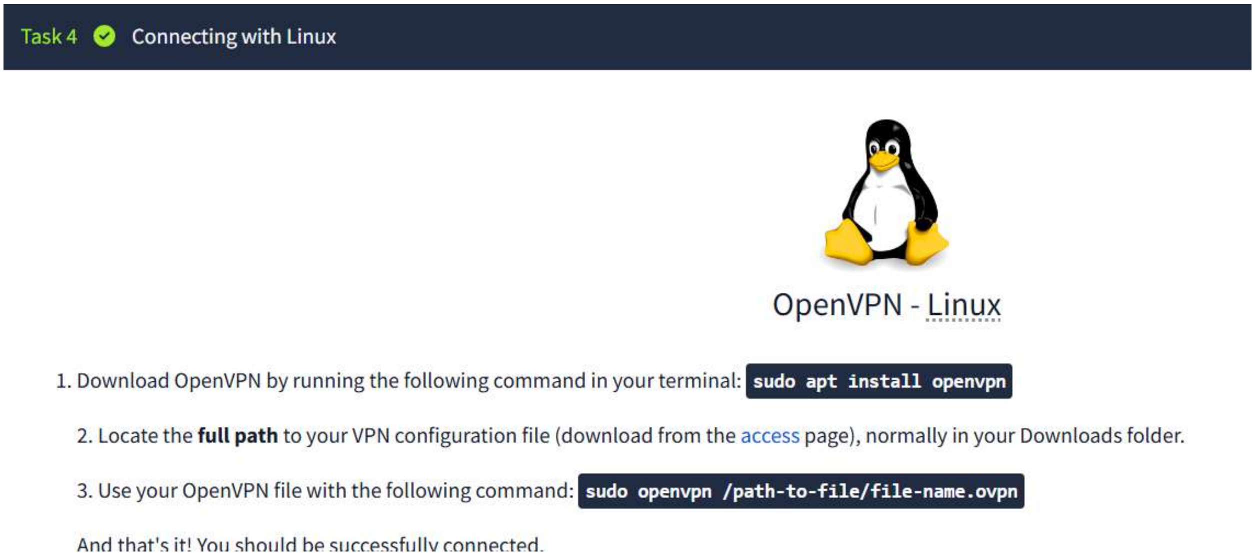
on my kali linux I download a configuration file of software openvpn from try hack me

go to connect to thm(try hack me) press on starting point press on openvpn

There is an option/exist an option to use Tryhackme's machine called attack box or to connect with a vpn connection with a software called open vpn through your kali linux computer

Guide to connect with open vpn [TryHackMe | OpenVPN]

We press on access on this website



Task 4 Connecting with Linux

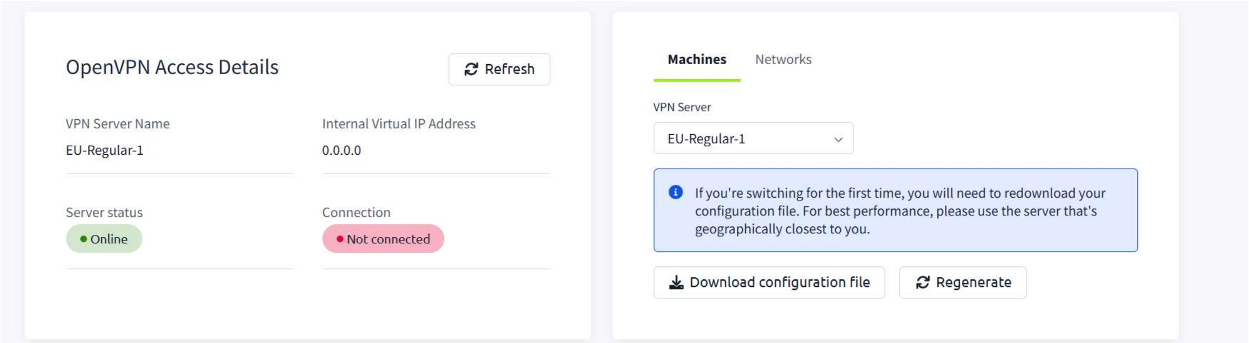
1. Download OpenVPN by running the following command in your terminal: `sudo apt install openvpn`
2. Locate the **full path** to your VPN configuration file (download from the access page), normally in your Downloads folder.
3. Use your OpenVPN file with the following command: `sudo openvpn /path-to-file/file-name.ovpn`

And that's it! You should be successfully connected.

It lead us to [TryHackMe | Access]

There select a server type and download a settings file

Choose vpn server and press download vpn setting file



OpenVPN Access Details

VPN Server Name: EU-Regular-1

Internal Virtual IP Address: 0.0.0.0

Server status: ● Online

Connection: ● Not connected

VPN Server: EU-Regular-1

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

If we get stuck with an OpenSSL error: error:0480006C:PEM routines::no start line:Expecting: CERTIFICATE

OpenSSL: error:0A080009:SSL routines::PEM lib

A solution to change the server type from EU-Regular-1 to another server

[VPN issue : r/tryhackme (reddit.com)]()

[Starting Point VPN issue: OpenSSL error - no start line : r/hackthebox (reddit.com)]()

[Openvpn SSL error - Off-topic - Hack The Box :: Forums]()

EU-West-Regular-1 server worked for me

The settings file is related to the user you registered with to Tryhackme

If you download in kali linux, the file will be downloaded to the Downloads folder

You see the download vpn in you'r user download folder

Open vpn should be automatically installed on kali linux operating system

If not installed, install command sudo apt install openvpn -y

What is openvpn is software to connect to a vpn server via configuration file

[Business VPN For Secure Networking | OpenVPN]()

[What Is OpenVPN? | OpenVPN]()

Connect linux ubuntu to openvpn

[How To Set Up and Configure an OpenVPN Server on Ubuntu 20.04 | DigitalOcean]()

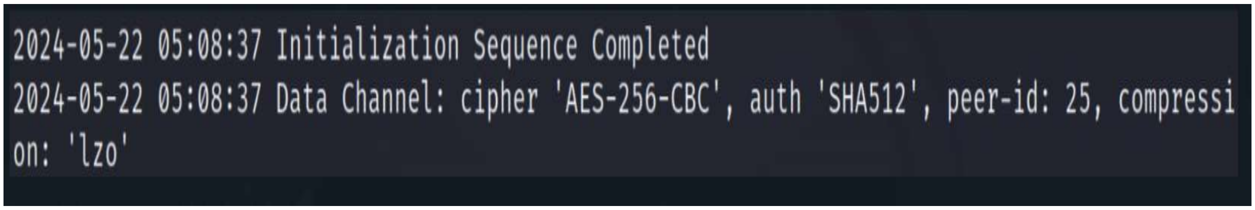
I connect to tryhackme picklerick with **my machine: kali linux** to be in the same network

I want able to scan it and solve the machine

Connecting to tryhackme with Open vpn, opening a terminal and typing the command sudo openvpn /where file.onpn is

Example sudo openvpn /home/user/Downloads/ Tryhackme user.ovpn

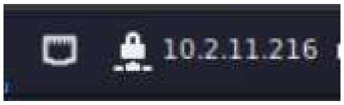
If everything went successfully you will get a screen in terminal: Initialization Sequence Completed



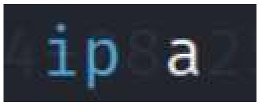
```
2024-05-22 05:08:37 Initialization Sequence Completed
2024-05-22 05:08:37 Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 25, compressi
on: 'lzo'
```

[Getting Started with OpenVPN | Try Hack Me Help Center]()

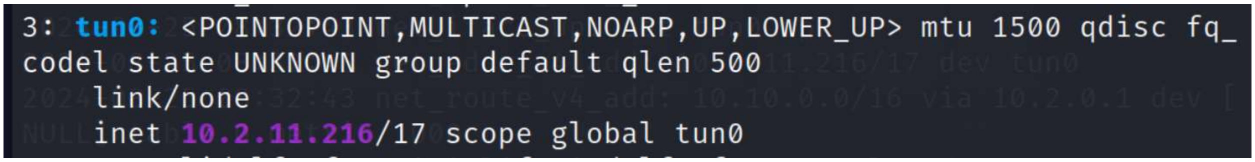
You see also a sign above



You can also check with the ip a command in another terminal and see the results – validation way



```
ip a
```



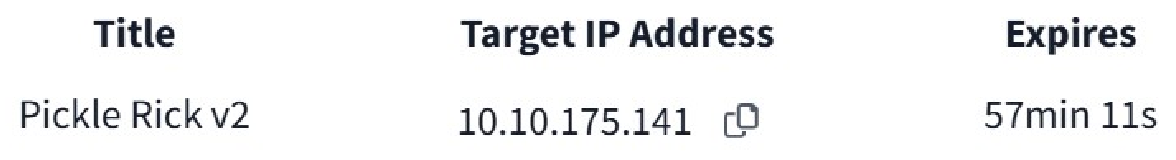
```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_
codel state UNKNOWN group default qlen 500
    link/none
    inet 10.2.11.216/17 scope global tun0
```

*If you need more time to solve the machine, there is an option to click Add one hour to the tryhackme machine

Then open a new terminal, so that 2 terminal windows are open

In the second terminal window you can check a connection to the tryhackme machine that we need to attack with the ping tryhackme machine ip command

I will get trthackme ip



Title	Target IP Address	Expires
Pickle Rick v2	10.10.175.141	57min 11s

Picklerick machine – try hack me machine – my target

try hack me machine can be change it ip -day 1 ip be different from day 2 ip

On the commands I use flags/options of command

I check connection between thm picklerick_ip with kali linux command: ping -c 2 picklerick_ip

Meaning

Command ping check connectivity between 2 devices

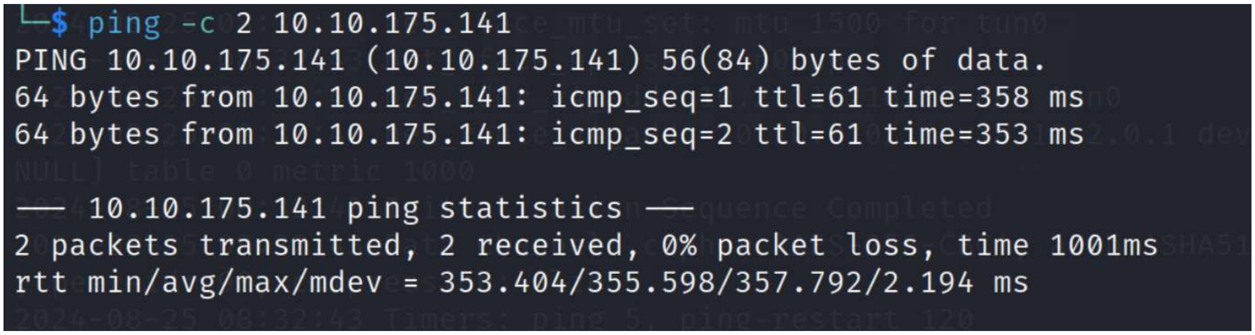
Flag -c cancel sending ping

Number 2 after 2 times cancel sending ping

Number picklerick_ip – ip of picklerick machine

[ping(8) - Linux man page (die.net)]

[How to Check Network Connectivity in Linux | ping Command - GeeksforGeeks]



```
└─$ ping -c 2 10.10.175.141
PING 10.10.175.141 (10.10.175.141) 56(84) bytes of data.
64 bytes from 10.10.175.141: icmp_seq=1 ttl=61 time=358 ms
64 bytes from 10.10.175.141: icmp_seq=2 ttl=61 time=353 ms

--- 10.10.175.141 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 353.404/355.598/357.792/2.194 ms
```

Results 2 packets transmitted, 2 received, 0% packet loss meaning I have connection with sea machine

I want to scan picklerick machine search for information to see vulnerabilities I can exploit

I'am using command nmap

[nmap(1) - Linux man page (die.net)]

[Nmap: the Network Mapper - Free Security Scanner](https://nmap.org)

[What is Nmap and How to Use it – A Tutorial for the Greatest Scanning Tool of All Time (freecodecamp.org)](https://freecodecamp.org)

[nmap(1) - Linux manual page (man7.org)](https://man7.org)

I use nmap command: nmap -sV -Pn --open ip

Meaning

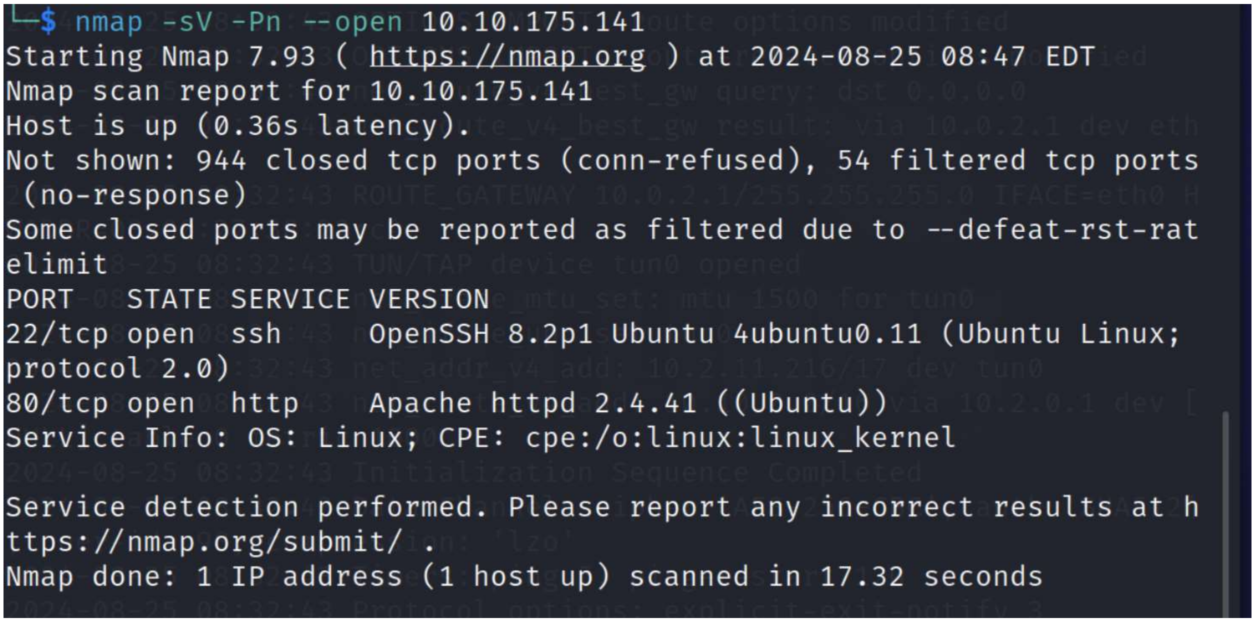
Command nmap command to scan devices and see variabilities

Flag -sV check for services and services versions

Flag -Pn don't do ping

Flag –open show only open ports

Ip my target ip who I scan



```
└─$ nmap -sV -Pn --open 10.10.175.141
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-25 08:47 EDT
Nmap scan report for 10.10.175.141
Host is up (0.36s latency).
Not shown: 944 closed tcp ports (conn-refused), 54 filtered tcp ports
 (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-rat
elimit
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

The open ports on the machine are 22, 80

I see 2 services OpenSSH 8.2p1, Apache httpd 2.4.41

If these services are new to you search them in google

http

[HTTP | MDN (mozilla.org)](https://mozilla.org)

[What is HTTP (w3schools.com)](https://w3schools.com)

[What is HTTP ? - GeeksforGeeks](https://geeksforgeeks.org)

Ssh

What is SSH? | Secure Shell (SSH) protocol | Cloudflare

What Is SSH: Secure Shell Explained | phoenixNAP KB

What is SSH? SSH Meaning in Linux (freecodecamp.org)

Ftp

https://www.bing.com/search?q=Ftp&form=ANNTH1&refig=9709a6cd44cb478cb3c998b4e0e67fed&pc=U531

How to Use Linux FTP Command to Transfer Files | Linuxize

How to Connect to FTP Servers in Windows (Without Extra Software) (howtogeek.com)

OpenSSH version of service ssh enable you to connect to remote server on ssh

OpenSSH

OpenSSH - Wikipedia

Httpd version of service http of Apache web server

Welcome! - The Apache HTTP Server Project

httpd - Wikipedia

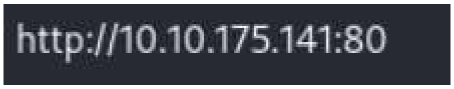
Vsftpd version of service ftp enable you to connect ftp share files

Secure FTP Server - vsftpd - Documentation (rockylinux.org)

vsftpd - Wikipedia

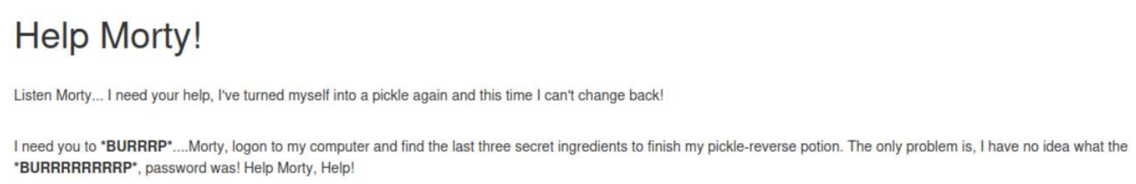
now I enter picklerick machine vie browser firefox in url I type http://10.10.175.141:80

url What is a URL? - Learn web development | MDN (mozilla.org)



```
http://10.10.175.141:80
```

I see



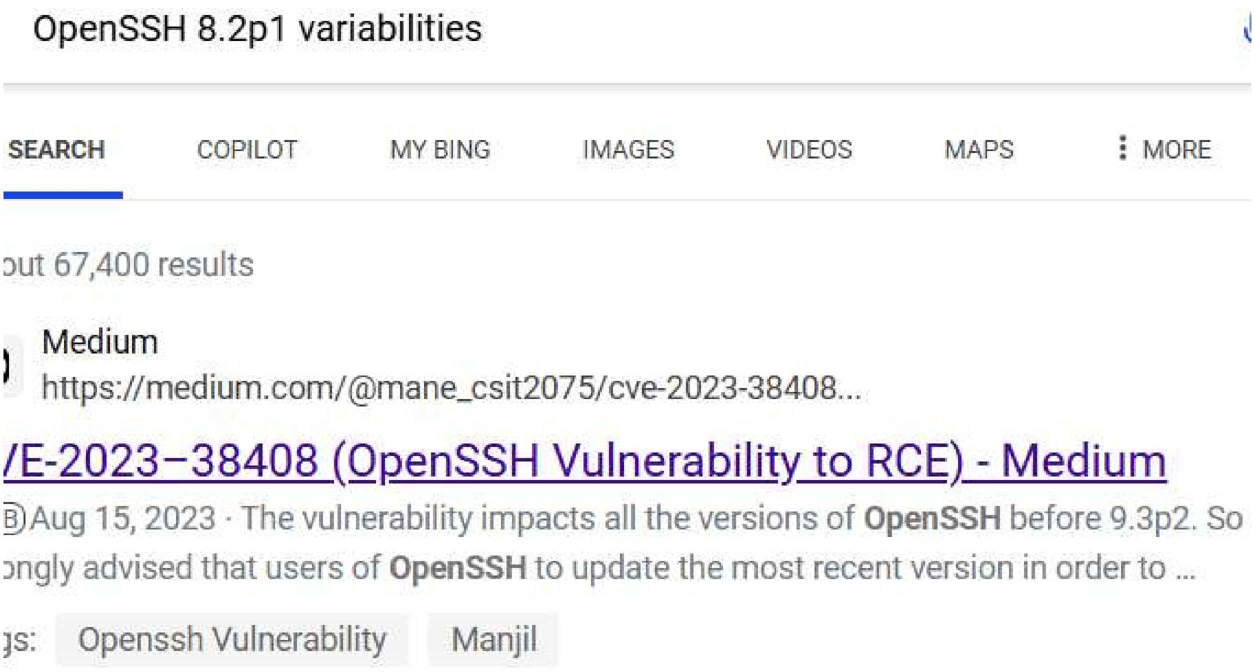
Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Meaning I need to connect to rick pc connect to his account and find three secret ingredients to finish his pickle-reverse potion

I search in google OpenSSH 8.2p1 variabilities



OpenSSH 8.2p1 variabilities

out 67,400 results

Medium
https://medium.com/@mane_csit2075/cve-2023-38408...

/E-2023–38408 (OpenSSH Vulnerability to RCE) - Medium

Aug 15, 2023 · The vulnerability impacts all the versions of **OpenSSH** before 9.3p2. So
ongly advised that users of **OpenSSH** to update the most recent version in order to ...

gs: Openssh Vulnerability Manjil

I found cve-2023-38408

Cve-2023-38408 OpenSSH vulnerability that exposes Linux systems to RCE

[CVE-2023–38408 (OpenSSH Vulnerability to RCE) | by Manjil | Medium]()

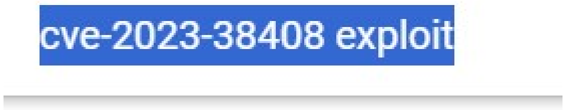
[NVD - CVE-2023-38408 (nist.gov)]()

[CVE - CVE-2023-38408 (mitre.org)]()

[SSH Attack - Explication CVE-2023-38408 - YouTube]()

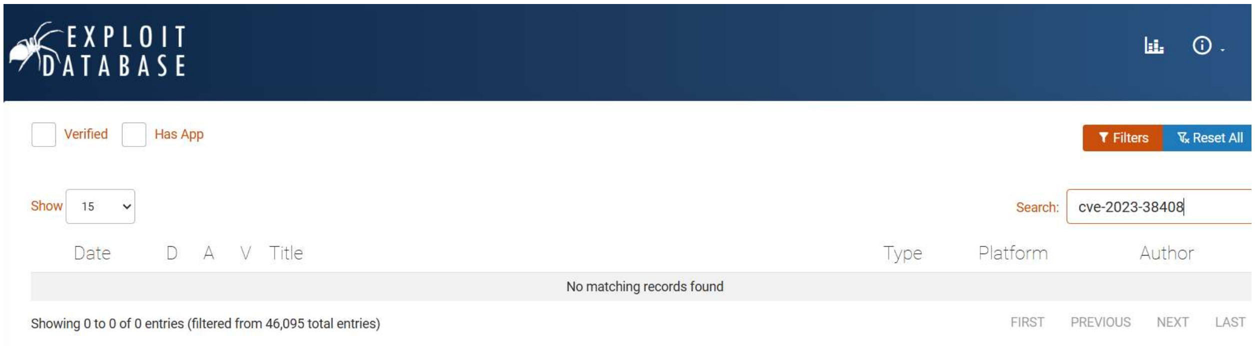
[TryHackMe | CVE-2023-38408]()

I search cve-2023-38408 exploit



cve-2023-38408 exploit

I search on exploited



Search: cve-2023-38408

No matching records found

Showing 0 to 0 of 0 entries (filtered from 46,095 total entries)

I search on githab

cve-2023-38408 exploit github

I found kali-mx/CVE-2023-38408: PoC for the recent critical vuln affecting OpenSSH versions < 9.3p2 (github.com)

I also found Openbsd Openssh version 8.2 : Security vulnerabilities, CVEs (cvedetails.com)

I found CVE-2023-48795

CVE-2023-48795 found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack

Openbsd Openssh version 8.2 : Security vulnerabilities, CVEs (cvedetails.com)

NVD - CVE-2023-48795 (nist.gov)

CVE - Search Results (mitre.org)

I search on githab

CVE-2023-48795 exploite github

I found CVE-2023-48795 / Terrapin Attack · Issue #81 · janmojzis/tinyssh (github.com)

Terrapin Attack Breaking Down SSH Security (youtube.com)

log.039 CVE-2023-48795 Terrapin Attack na OpenSSH ChaCha20-Poly1305 SSH MITM exploit i scanner (youtube.com)

Download a machine to try this attack from Release v1.0.3 · RUB-NDS/Terrapin-Scanner (github.com)

Terrapin attack a cryptographic attack on the commonly used SSH protocol that is used for secure command-and-control throughout the Internet. The Terrapin attack can reduce the security of SSH by using a downgrade attack via man-in-the-middle interception

Terrapin attack - Wikipedia

On OpenSSH before 9.6 the attack bypasses the keystroke timing obfuscation feature, which may allow MitM attackers to brute-force SSH passwords by inspecting the SSH network packets.

SSH Protocol Flaw CVE-2023-48795 Terrapin Attack: All You Need To Know (jfrog.com)

Terrapin attack is a prefix truncation attack targeting the SSH protocol. More precisely, Terrapin breaks the integrity of SSH's secure channel. By carefully adjusting the sequence numbers during the handshake, an attacker can remove an arbitrary amount of messages sent by the client or server at the beginning of the secure channel without the client or server noticing it.

Terrapin Attack (terrapin-attack.com)

prefix truncation attack on the Binary Packet Protocol (BPP) in SSH involves an attacker manipulating encrypted SSH packets.

Prefix Truncation Attack on the Binary Packet Protocol (BPP) in SSH might involve an attacker who intercepts SSH packets and removes the initial portion of the data in a packet before it reaches the destination

Hacking SSH Connections by exploiting SSH Protocol Vulnerabilities: Different Terrapin Attack Vectors (exploitone.com)

I search in google Apache httpd 2.4.41 variabilities

Apache httpd 2.4.41 variabilities

I found CVE-2024-40725

CVE-2024-40725 Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers.

Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project

NVD - CVE-2024-40725 (nist.gov)

CVE - CVE-2024-40725 (mitre.org)

I search on google

CVE-2024-40725 exploit

I search on YouTube

CVE-2024-40725

I found CVE-2024-40725 Apache 2.4.0/2.4.61 HTTP Request Smuggling , Custom nuclei template . (youtube.com)

I found CVE-2020-13938

CVE-2020-13938 Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project

CVE - CVE-2020-13938 (mitre.org)

NVD - CVE-2020-13938 (nist.gov)

I found CVE-2021-26690

CVE-2021-26690 Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project

NVD - CVE-2021-26690 (nist.gov)

CVE - CVE-2021-26690 (mitre.org)

I found CVE-2021-41773

CVE-2021-41773 The vulnerability arises from the mishandling of URL-encoded path traversal characters in the HTTP GET request.

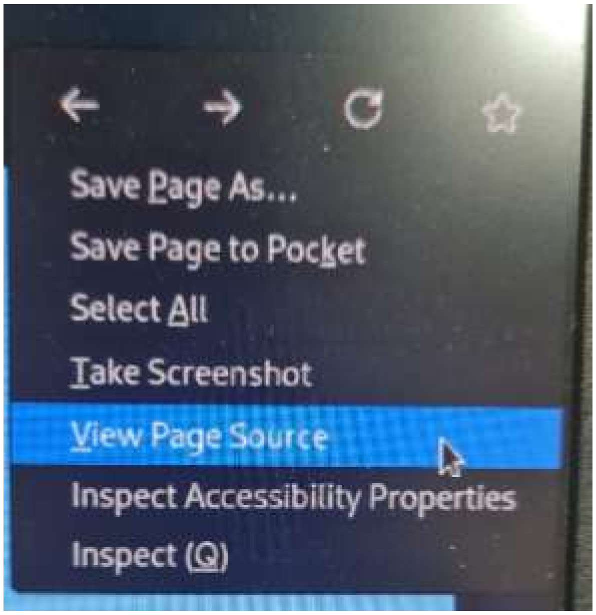
Apache HTTP Server CVE-2021-41773 Exploited in the Wild | Rapid7 Blog

NVD - CVE-2021-41773 (nist.gov)

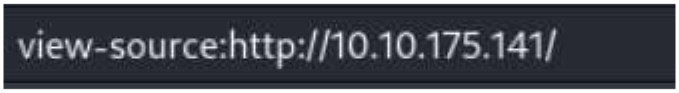
CVE - Search Results (mitre.org)

On the website I go to it source code to search massages maybe exist there information I can exploit to connect to rick pc

click right mouse button from option list click on view source page

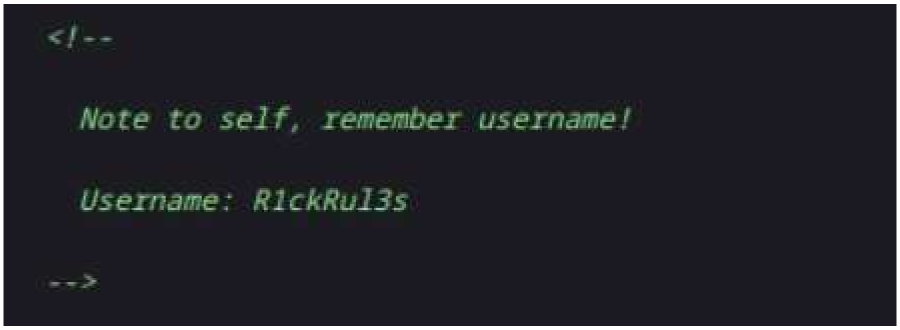


Open new page called source page



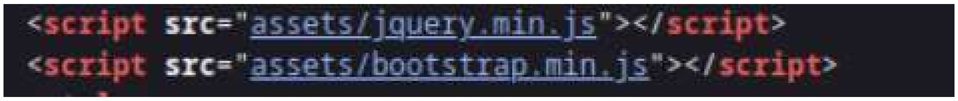
```
view-source:http://10.10.175.141/
```

I found massage color green that say username: R1ckRul3s



```
<!--

  Note to self, remember username!

  Username: R1ckRul3s

-->
```

I also see folder called assent that used on build the website



```
<script src="assets/jquery.min.js"></script>
<script src="assets/bootstrap.min.js"></script>
```

I search hidden folders and pages on the website I’am search login page

For that I used gobuster command:

gobuster dir -u MACHINE_IP -w list.txt

command gobuster need a list to compare file on brute-force attack

can see how to use gobuster with command: man gobuster

Meaning

Command gobuster allow you to search hidden files and directors on a web server

Flag dir allow the classic directory brute-forcing mode on webite

Flag -u represent url

url What is a URL? - Learn web development | MDN (mozilla.org)

MACHINE_IP   target ip which I attack

Flag -w use a list on brute-force

File list.txt   a list use to compare file on brute-force

I search on google a list compare file on brute-force, i have found: common.txt

common.txt list locate on route/location /usr/share/wordlists/dirb/

Gobuster Tutorial – How to Find Hidden Directories, Sub-Domains, and S3 Buckets (freecodecamp.org)

How To Use GoBuster To Find Hidden Files/Directories (youtube.com)

Dirb scan website content search viewed and hidden files

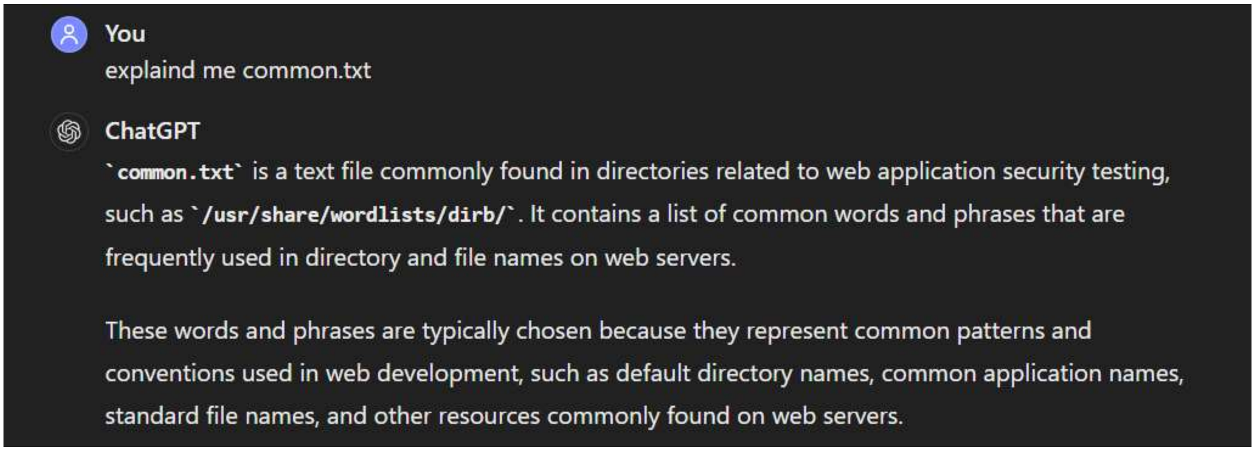
dirb | Kali Linux Tools

/usr/share/wordlists/dirb/ a folder that content search viewed and hidden files on website

common.txt a list to search and compare file on brute-force

search on chat gpt after purpose of common.txt

write common.txt list contains similar patterns and conventions in web development



You

explaind me common.txt

ChatGPT

`common.txt` is a text file commonly found in directories related to web application security testing, such as `/usr/share/wordlists/dirb/`. It contains a list of common words and phrases that are frequently used in directory and file names on web servers.

These words and phrases are typically chosen because they represent common patterns and conventions used in web development, such as default directory names, common application names, standard file names, and other resources commonly found on web servers.

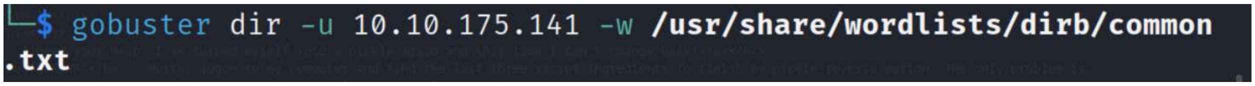
common.txt list content

wordlists/common.txt · f43c03a2bef91118debffd6cec9573f21bb5f9e8 · Kali Linux / Packages / dirb · GitLab

dirb/wordlists/common.txt at master · v0re/dirb · GitHub

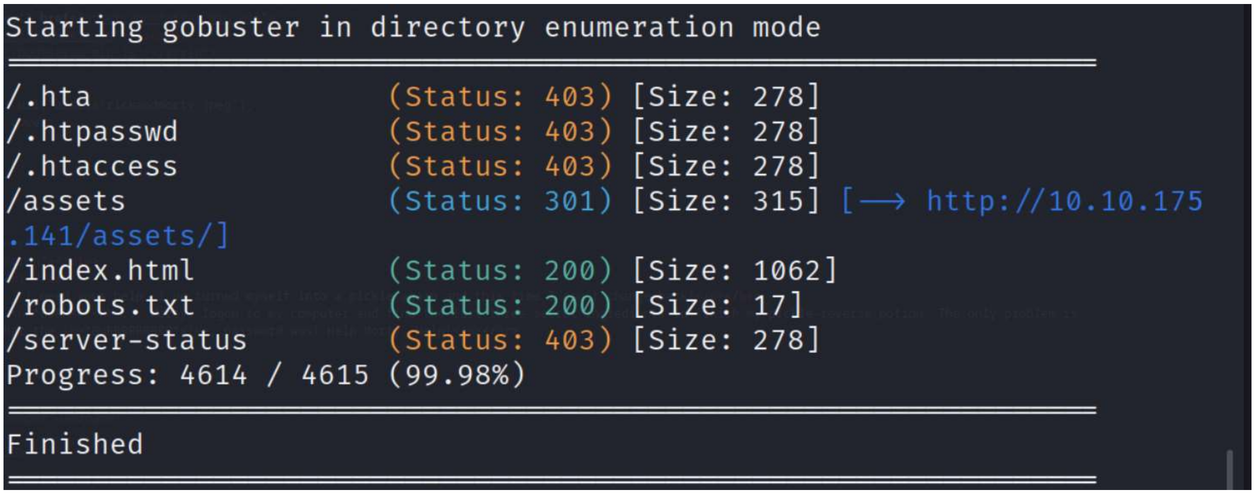
Gobuster tool use option dir to search and compare file from website to common.txt list on brute force

I type: gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirb/common.txt



```
└─$ gobuster dir -u 10.10.175.141 -w /usr/share/wordlists/dirb/common
.txt
```

Results



```
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.10.175
.141/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

In the results we see certain codes: status 403, status 301, status 200

Interpretation of codes code 200 successful communication with the site, code 301 referral to another place on the site, code 403 page not found on the server

[What are HTTP Status Codes? List Of Important Status Codes - Moz]()

[HTTP response status codes - HTTP | MDN (mozilla.org)]()

I see documents index.html, robots.txt and folder assets

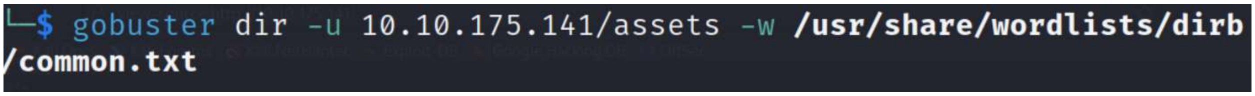
robot.txt a file contains website road map and some configurations

[Robots.txt Introduction and Guide | Google Search Central | Documentation | Google for Developers]()

[What is robots.txt? | How a robots.txt file works | Cloudflare]()

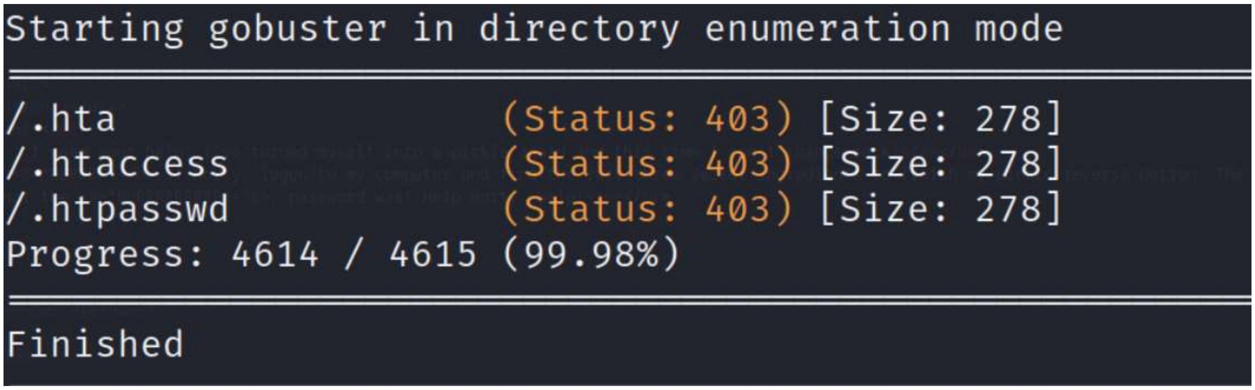
[robots.txt configuration - Security on the web | MDN (mozilla.org)]()

I used gobuster command on folder assets command: gobuster dir -u 10.10.175.141/assets -w /usr/share/wordlists/dirb/common.txt



```
└─$ gobuster dir -u 10.10.175.141/assets -w /usr/share/wordlists/dirb
/common.txt
```

Results



```
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
```

I use another list called directory-list-2.3-small.txt

command gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

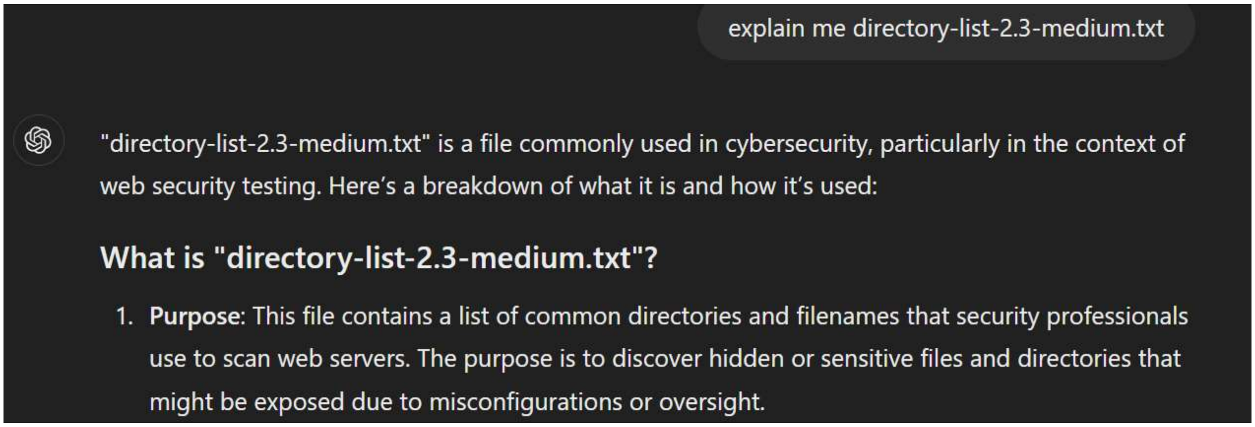
dirbuster scan website content search viewed and hidden files

[dirbuster | Kali Linux Tools]()

/usr/share/wordlists/dirbuster a folder that content search viewed and hidden files on website

search on chat gpt after purpose of directory-list-2.3-medium.txt

directory-list-2.3-medium.txt list includes a range of potential directory and file names that are often targeted in security assessments.

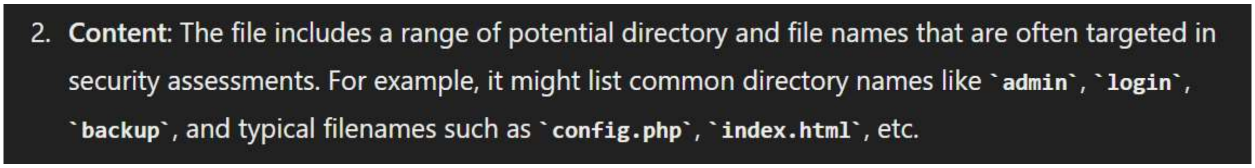


explain me directory-list-2.3-medium.txt

"directory-list-2.3-medium.txt" is a file commonly used in cybersecurity, particularly in the context of web security testing. Here's a breakdown of what it is and how it's used:

What is "directory-list-2.3-medium.txt"?

1. **Purpose**: This file contains a list of common directories and filenames that security professionals use to scan web servers. The purpose is to discover hidden or sensitive files and directories that might be exposed due to misconfigurations or oversight.



2. **Content**: The file includes a range of potential directory and file names that are often targeted in security assessments. For example, it might list common directory names like `admin`, `login`, `backup`, and typical filenames such as `config.php`, `index.html`, etc.

Before this check if directory-list-2.3-medium.txt list contain README.md if you want to add more word to this list example README.md

Command cat /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt | grep README.md

Meaning

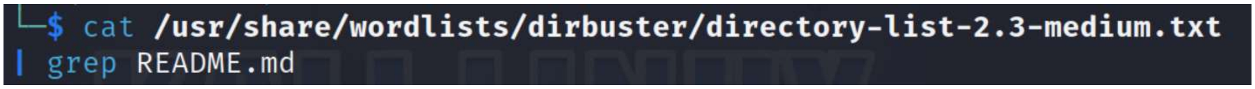
Command cat open and print document

List /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

| take command from cat and run it with grep

Command grep find and show word that I tell you

README.md the word



```
└─$ cat /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
| grep README.md
```

If it not exists you need to add README.md to directory-list-2.3-medium.txt

You will canter with an error because only root user can write to this document

Command echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Meaning

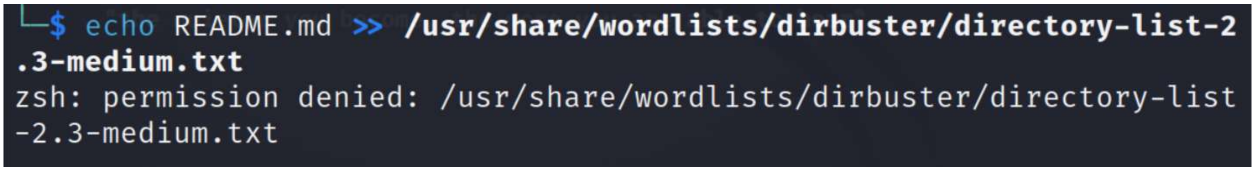
Command echo print word typed after it to screen

README.md word I want to enter to directory-list-2.3-medium.txt list

Sine > write word overwrite existing words on a document

Sine >> write word add to existing words on a document

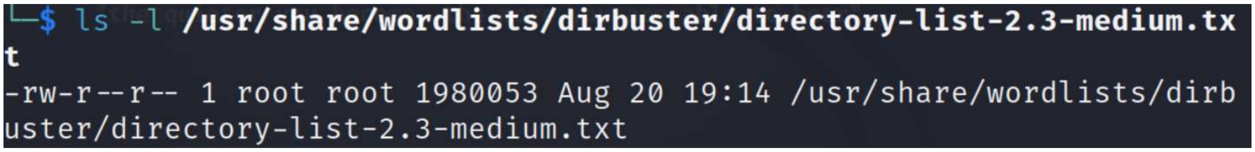
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt where the list locates



```
└─$ echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2
.3-medium.txt
zsh: permission denied: /usr/share/wordlists/dirbuster/directory-list
-2.3-medium.txt
```

command ls -l show permissions and owner of a file or directory

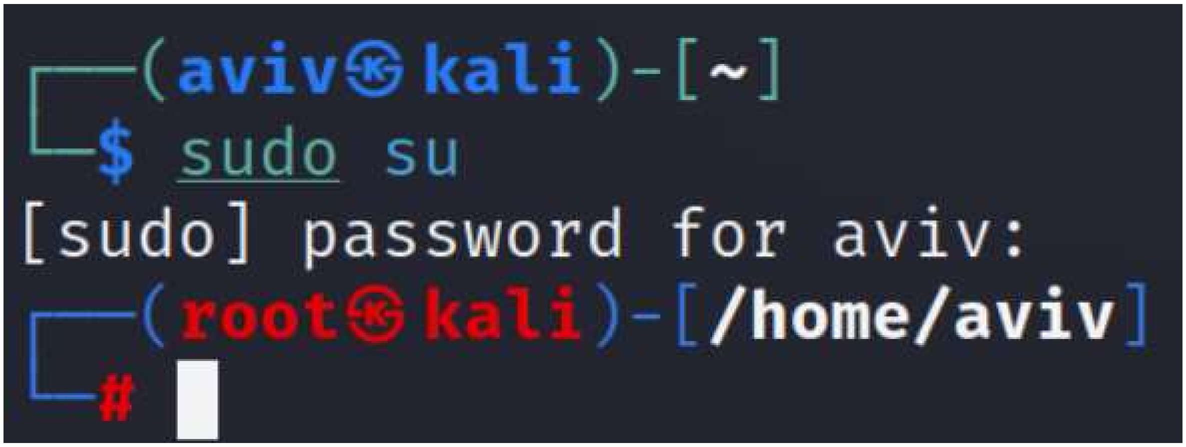
I typed ls -l /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
└─$ ls -l /usr/share/wordlists/dirbuster/directory-list-2.3-medium.tx
t
-rw-r--r-- 1 root root 1980053 Aug 20 19:14 /usr/share/wordlists/dirb
uster/directory-list-2.3-medium.txt
```

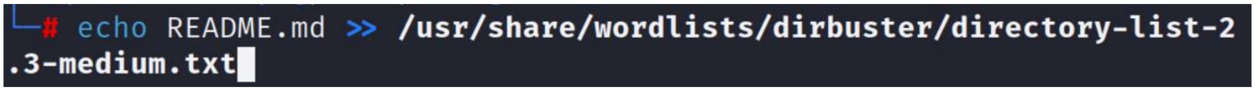
solve enter as root command sudo su

you need to enter you’r user password



```
┌──(aviv㉿kali)-[~]
└─$ sudo su
[sudo] password for aviv:
┌──(root㉿kali)-[/home/aviv]
└─# 
```

Now try to add again README.md to /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt list

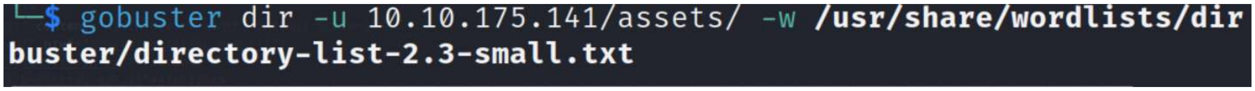


```
└─# echo README.md >> /usr/share/wordlists/dirbuster/directory-list-2
.3-medium.txt
```

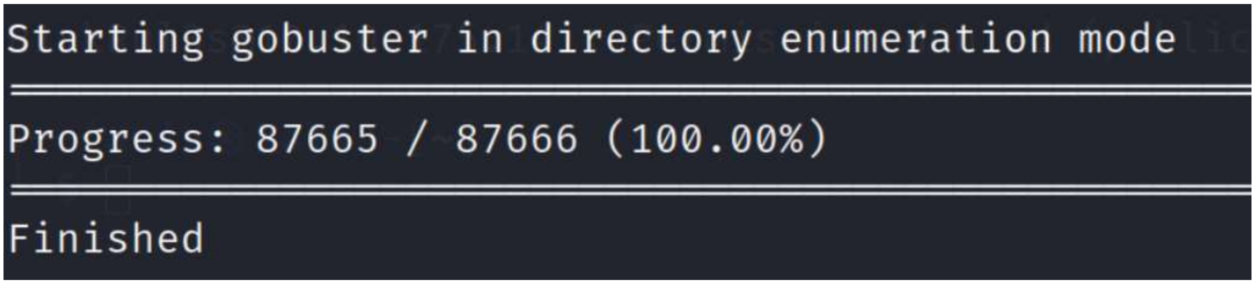
I did the same with directory-list-2.3-small.txt list

I typed gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Or gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt



```
└─$ gobuster dir -u 10.10.175.141/assets/ -w /usr/share/wordlists/dir
buster/directory-list-2.3-small.txt
```

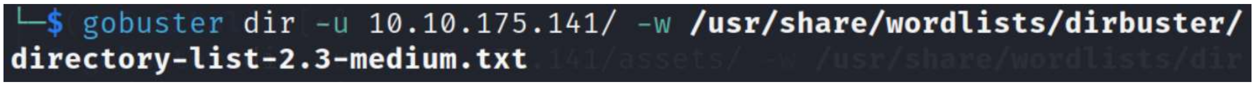


```
Starting gobuster in directory enumeration mode
===============================================================
Progress: 87665 / 87666 (100.00%)
===============================================================
Finished
```

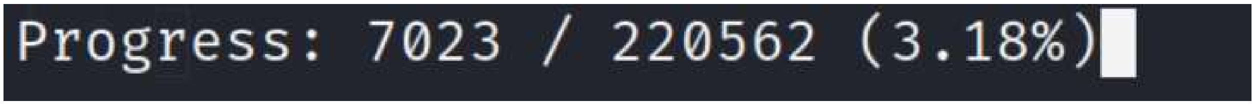
Results not found hidden files

Lets tray directory-list-2.3-medium.txt list

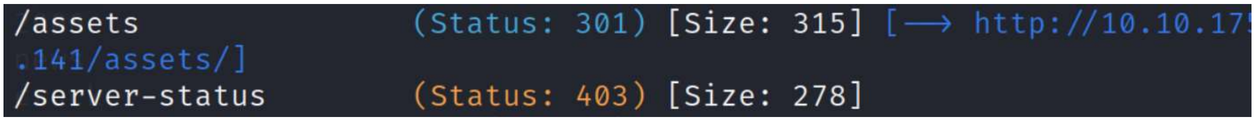
I typed gobuster dir -u MACHINE_IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



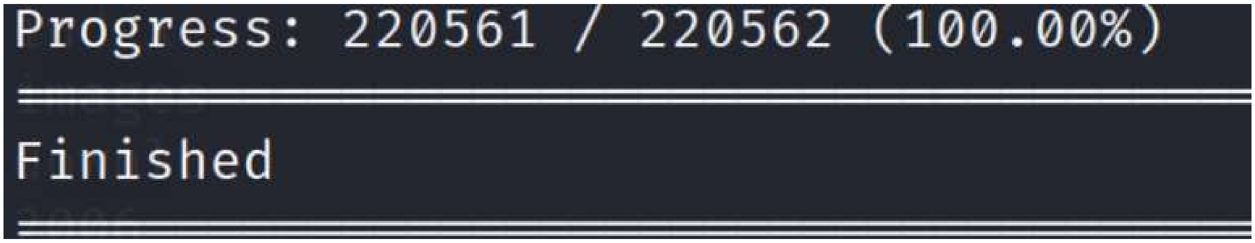
```
└─$ gobuster dir -u 10.10.175.141/ -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
```



```
Progress: 7023 / 220562 (3.18%)
```



```
/assets               (Status: 301) [Size: 315] [⟶ http://10.10.17
.141/assets/]
/server-status        (Status: 403) [Size: 278]
```



```
Progress: 220561 / 220562 (100.00%)
===============================================================
Finished
===============================================================
```

Meaning word login.php not exist in directory-list-2.3-medium.txt list and in directory-list-2.3-small.txt list

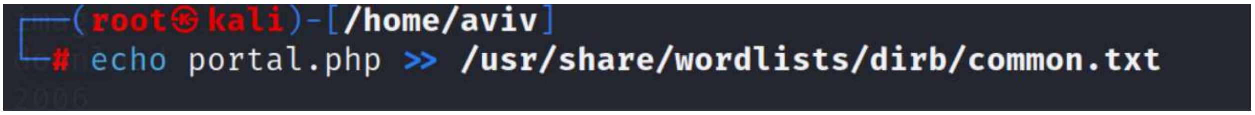
From [Pickle Rick CTF Writeup (Full and Detailed) — TryHackMe | by Matheus Heidemann | Medium] I see I need to see login.php, portal.php between the results of gobuster

I add word like login.php, portal.php, README.md to /usr/share/wordlists/dirb/common.txt

Enter as root command sudo su

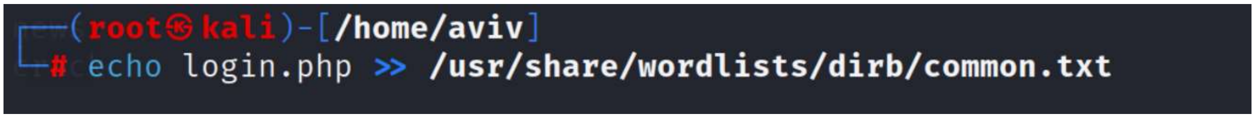
You need to put you'r user account password

Command echo login.php >> /usr/share/wordlists/dirb/common.txt



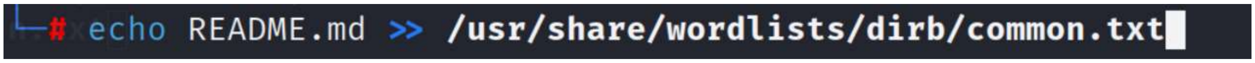
```
┌──(root㉿kali)-[/home/aviv]
└─# echo portal.php >> /usr/share/wordlists/dirb/common.txt
```

Command echo login.php >> /usr/share/wordlists/dirb/common.txt



```
┌──(root㉿kali)-[/home/aviv]
└─# echo login.php >> /usr/share/wordlists/dirb/common.txt
```

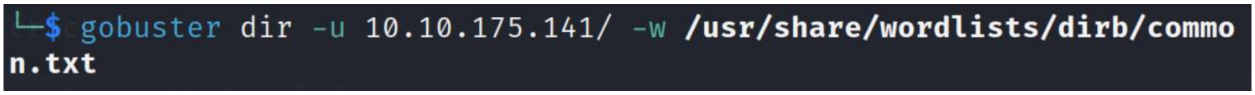
Command echo README.md >> /usr/share/wordlists/dirb/common.txt



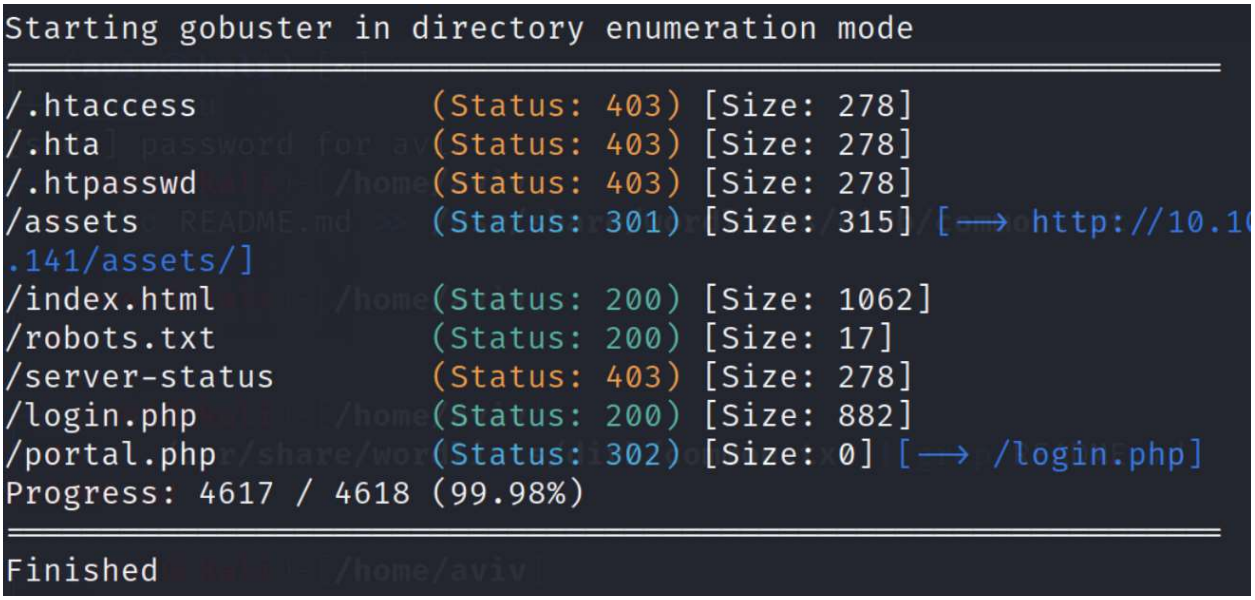
```
└─# echo README.md >> /usr/share/wordlists/dirb/common.txt
```

I add this words to directory-list-2.3-small.txt list and directory-list-2.3-medium.txt list

I run again command gobuster dir -u ip -w /usr/share/wordlists/dirb/common.txt



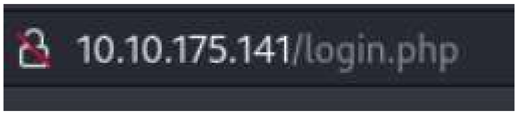
```
└─$ gobuster dir -u 10.10.175.141/ -w /usr/share/wordlists/dirb/commo
n.txt
```



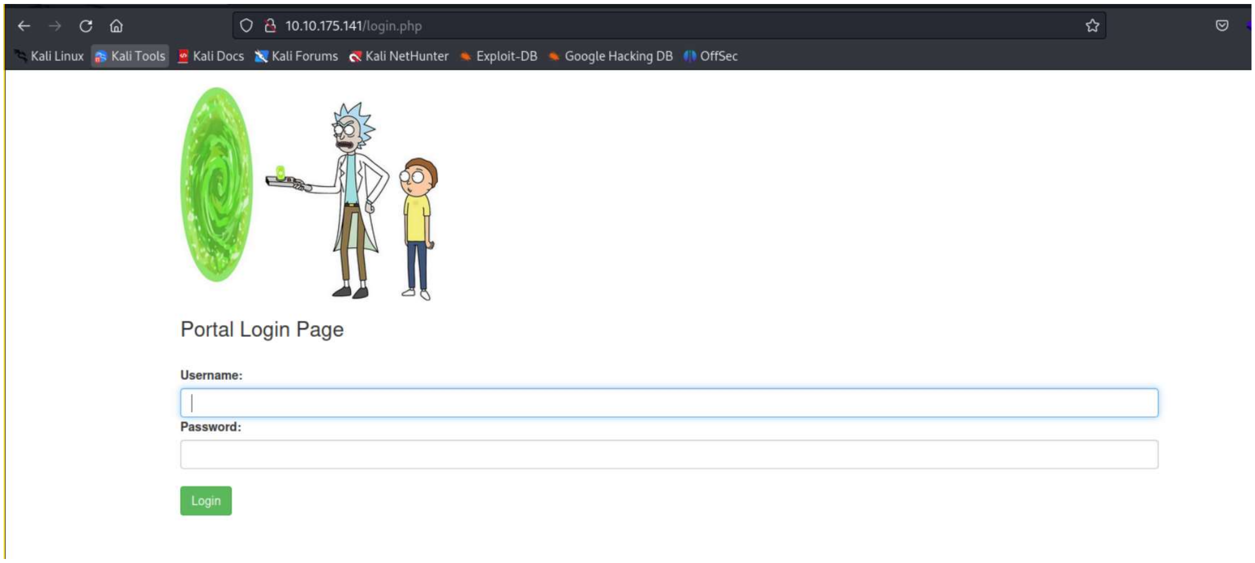
```
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.1
.141/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 278]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
Progress: 4617 / 4618 (99.98%)
===============================================================
Finished
```

Results found page called login.php

I enter page: login.php



10.10.175.141/login.php

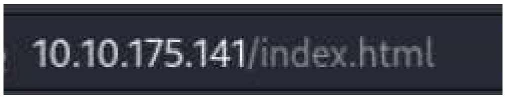


Portal Login Page

Username:

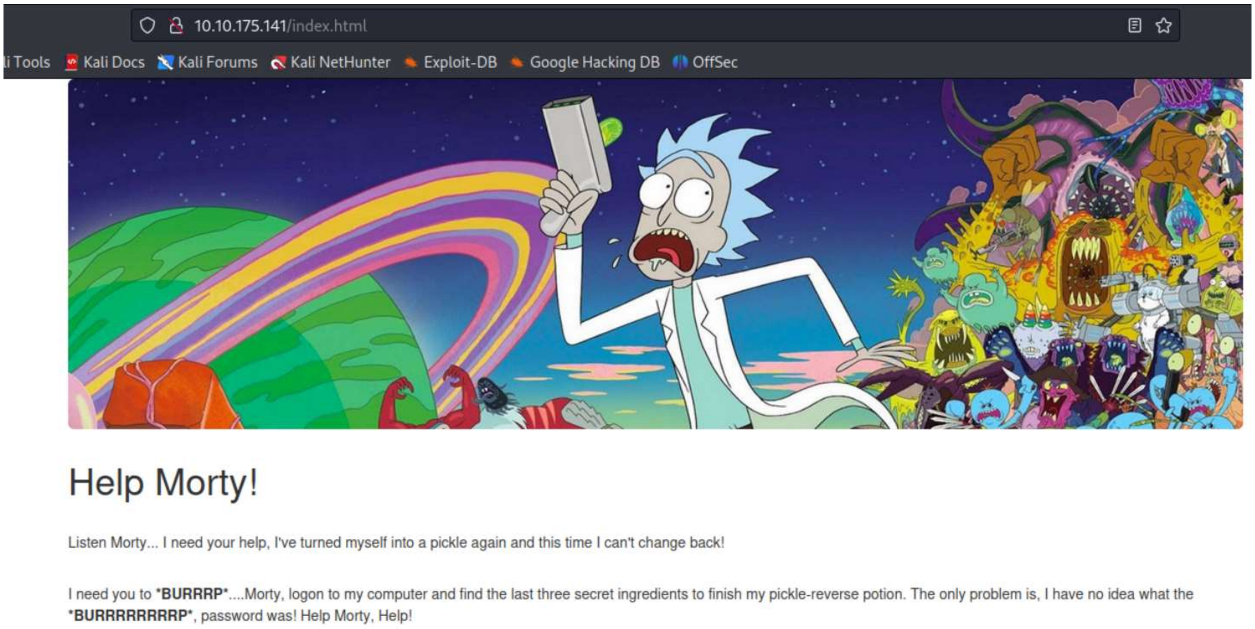
Password:

I enter index.html



10.10.175.141/index.html

I get the same page

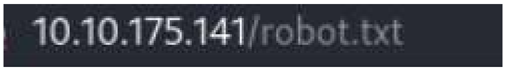


Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

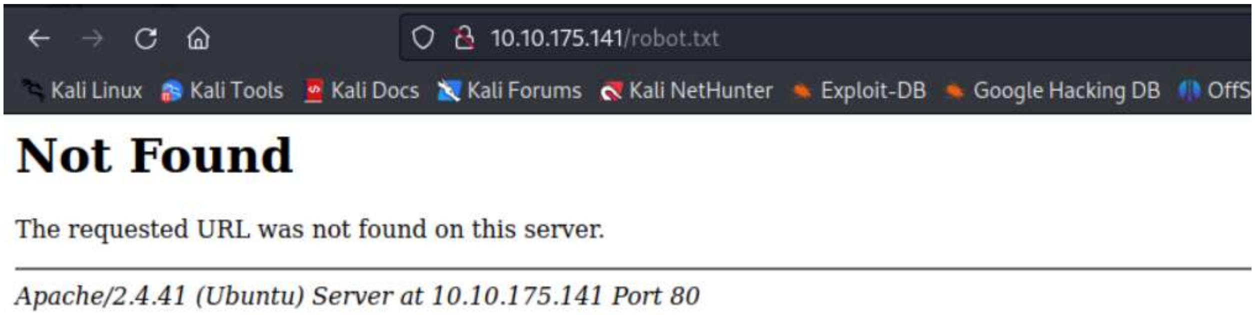
I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

I enter robot.txt



10.10.175.141/robot.txt

I get massage not found with server os



Not Found

The requested URL was not found on this server.

Apache/2.4.41 (Ubuntu) Server at 10.10.175.141 Port 80

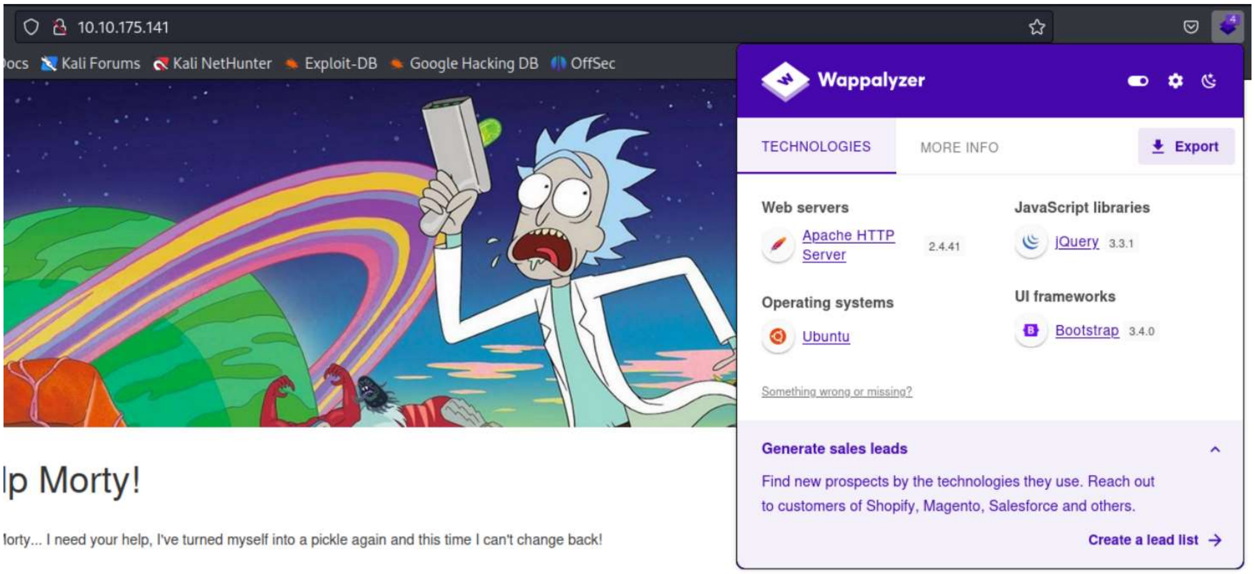
I can verify it using wappaluzer extension

Install extension wappalyzer -allow you to see what technologies website is using

and active wappalyzer extension

https://www.wappalyzer.com/

you can search wappalyzer extension to you’r web browser and install it



lp Morty!

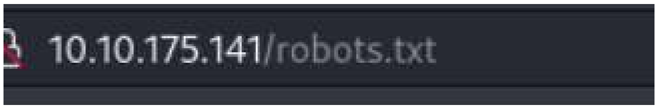
lorty... I need your help, I've turned myself into a pickle again and this time I can't change back!

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

I see also Apache HTTP Server is 2.4.41 like what nmap scan found

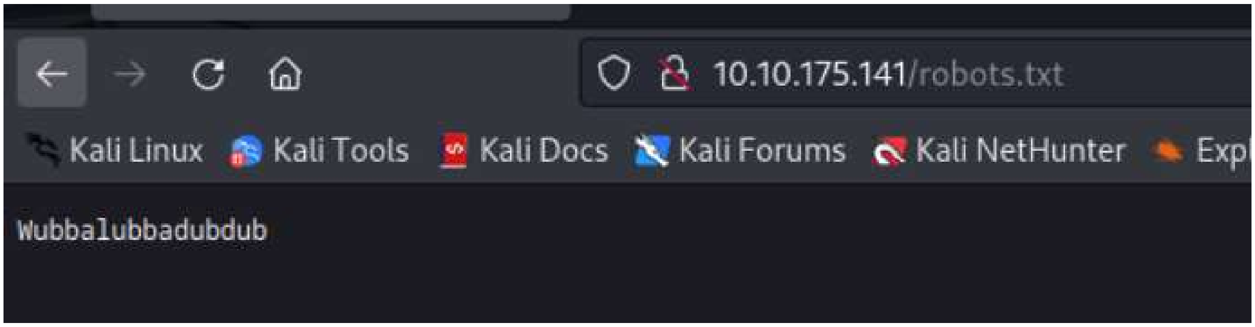
I see also server os is ubuntu like what nmap scan found

I enter robots.txt



10.10.175.141/robots.txt

Results



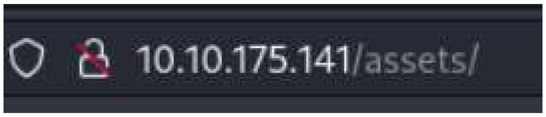
10.10.175.141/robots.txt

```
Wubbalubbadubdub
```

Found word Wubbalubbadubdub -it could be a password

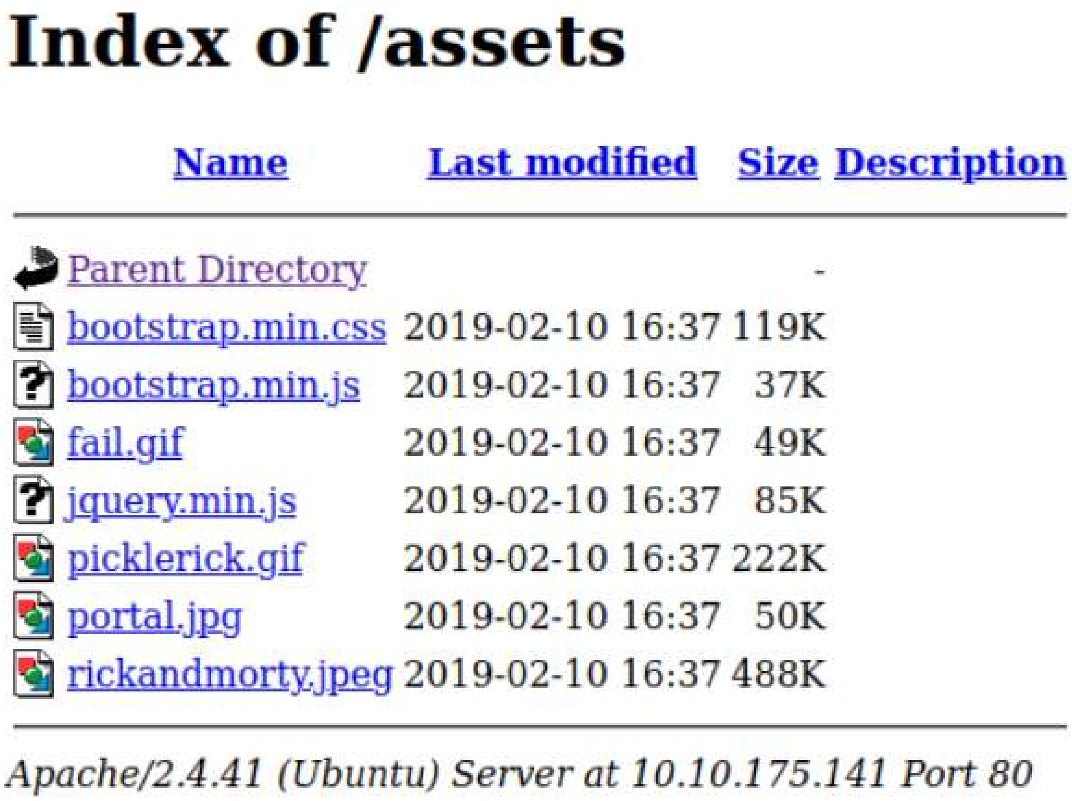
It misconfiguration of robot.txt I don’t supposed to have access to robot.txt

Now I enter folder assets



10.10.175.141/assets/

Resoles



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.min.css	2019-02-10 16:37	119K	
bootstrap.min.js	2019-02-10 16:37	37K	
fail.gif	2019-02-10 16:37	49K	
jquery.min.js	2019-02-10 16:37	85K	
picklerick.gif	2019-02-10 16:37	222K	
portal.jpg	2019-02-10 16:37	50K	
rickandmorty.jpeg	2019-02-10 16:37	488K	

Apache/2.4.41 (Ubuntu) Server at 10.10.175.141 Port 80

The files with extension gif and jpeg are pictures, files with extension js are java script files, files with extension css are css files

Html

[HTML Tutorial (w3schools.com)]()

[HTML: HyperText Markup Language | MDN (mozilla.org)]()

Css

[CSS Tutorial (w3schools.com)]()

[CSS: Cascading Style Sheets | MDN (mozilla.org)]()

Js

[JavaScript Tutorial (w3schools.com)]()

[JavaScript | MDN (mozilla.org)]()

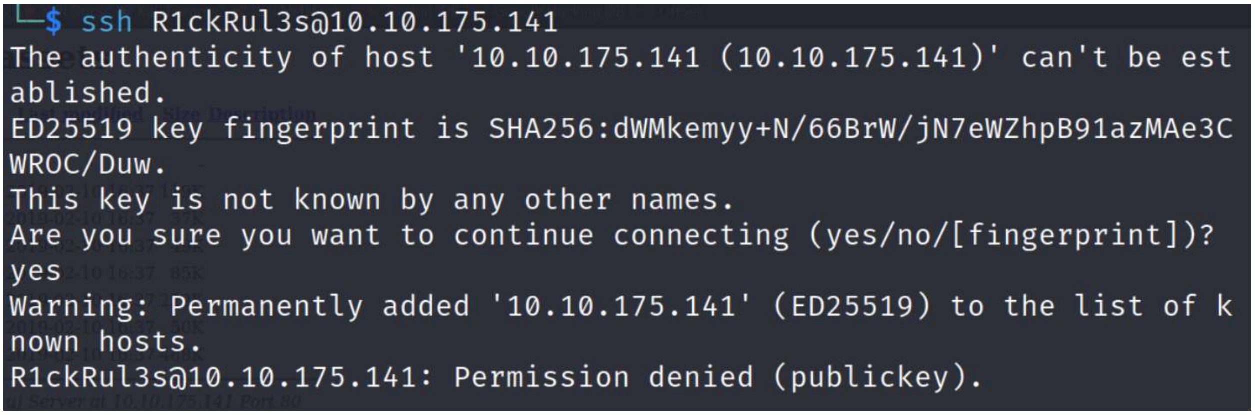
Lets try to see if username and password that I found connect me to shh

USERNAME: R1ckRul3s Password: Wubbalubbadubdub

I run commans ssh username@ip

I weel need to enter a password

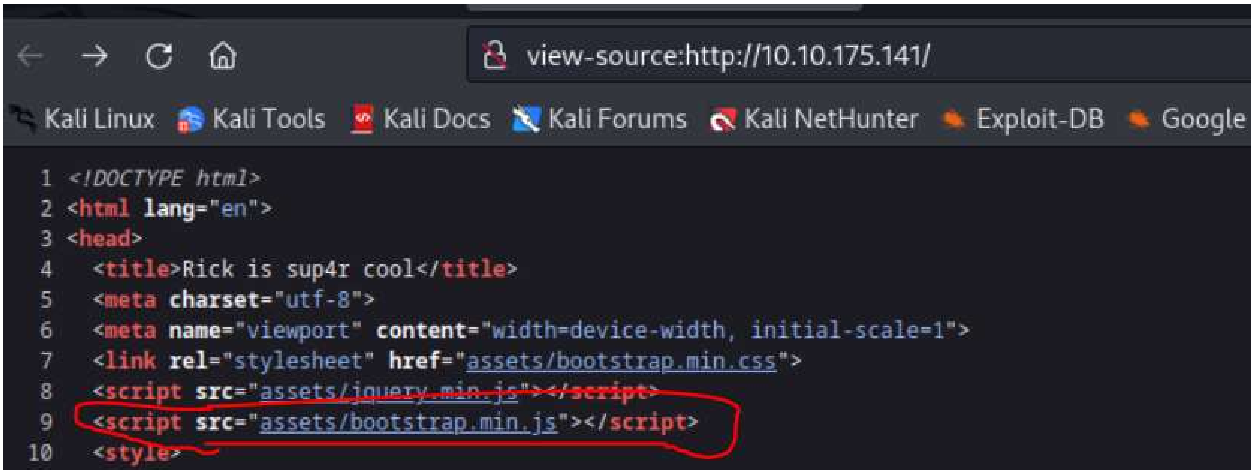
So I type ssh R1ckRul3s@picklerick_ip



```
└─$ ssh R1ckRul3s@10.10.175.141
The authenticity of host '10.10.175.141 (10.10.175.141)' can't be est
ablished.
ED25519 key fingerprint is SHA256:dWMkemyy+N/66BrW/jN7eWZhpB91azMAe3C
WROC/Duw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
yes
Warning: Permanently added '10.10.175.141' (ED25519) to the list of k
nown hosts.
R1ckRul3s@10.10.175.141: Permission denied (publickey).
```

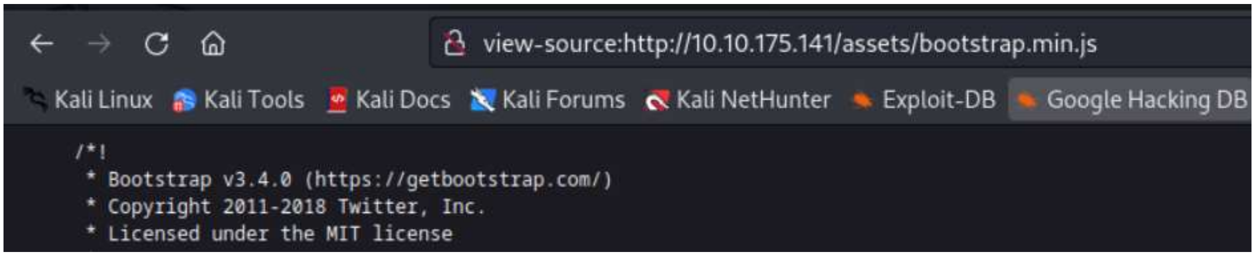
meaning R1ckRul3s is not username in the server

I see on source page file: assets/bootstrap.min.js



```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
```

When I enter it I see Bootstrap v3.4.0



```
/*!
 * Bootstrap v3.4.0 (https://getbootstrap.com/)
 * Copyright 2011-2018 Twitter, Inc.
 * Licensed under the MIT license
```

I can see it on wappalyzer: Bootstrap v3.4.0

Lets search what it is and vulnerabilities to it

Bootstrap is a free, open-source front-end development framework for the creation of websites and web apps

https://getbootstrap.com/docs/5.3/getting-started/introduction/

https://www.techtarget.com/whatis/definition/bootstrap

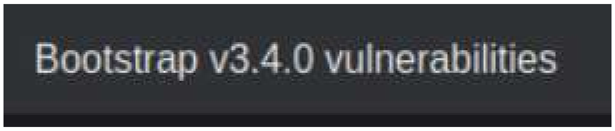
https://www.w3schools.com/bootstrap/

Term front-end is client pc, the client user interface with the website

https://airfocus.com/glossary/what-is-a-front-end/

https://en.wikipedia.org/wiki/Frontend_and_backend

I search Bootstrap v3.4.0 vulnerabilities



Bootstrap v3.4.0 vulnerabilities

I found Bootstrap v3.4.0 vulnerabilitie to XSS (Cross-site Scripting)

https://security.snyk.io/package/npm/bootstrap/3.4.0

https://www.tenable.com/plugins/was/112373

like CVE-2016-10735 using xss is possible in the data-target attribute,

https://www.cvedetails.com/cve/CVE-2016-10735/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10735

https://nvd.nist.gov/vuln/detail/CVE-2016-10735

like cve-2018-14041 using XSS is possible in the data-target property of scrollspy.

https://nvd.nist.gov/vuln/detail/cve-2018-14041

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14041

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2018-14041

xss

Cross Site Scripting (XSS) | OWASP Foundation

What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy (portswigger.net)

What is Cross Site Scripting (XSS) ? - GeeksforGeeks

For using xss I use software burpsuite that is a tool for testing and scanning web applications for vulnerabilities

[Learn Burp Suite on Kali Linux: Part 1 - Linux Tutorials - Learn Linux Configuration]

[Burp Suite Tutorial - Web Pentesting Beginners Guide - 2023 (kalilinuxtutorials.com)]

[burpsuite | Kali Linux Tools]

[Mastering Burp Suite: The Ultimate Web Application Hacking Tool (youtube.com)]

On kali linux burpsuite install as default version burp suite community edition

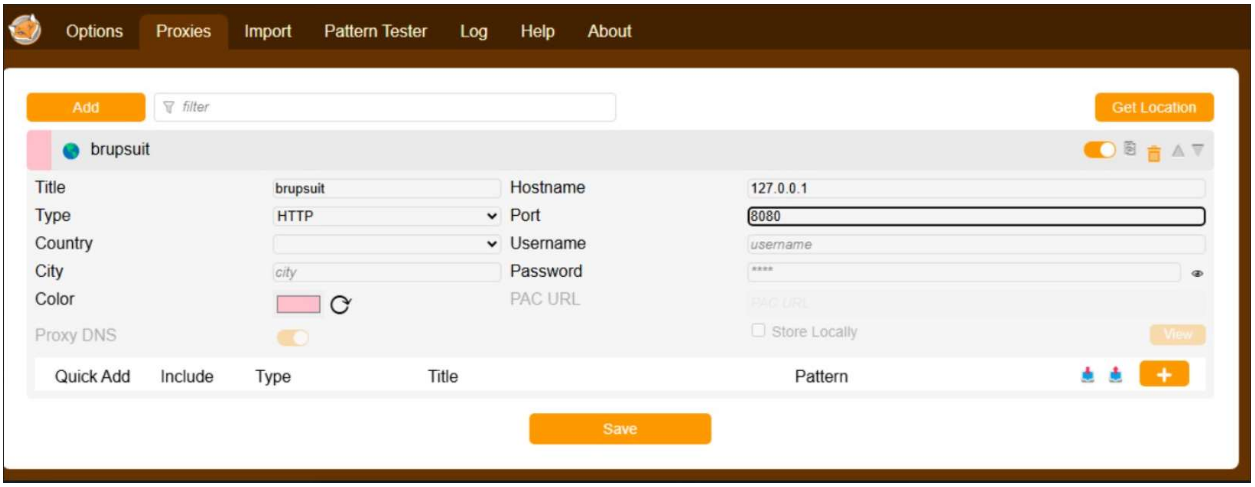
I can download and install on my browser foxyproxy extension

[FoxyProxy (google.com)]

After installing foxyproxy extension I go to extension press foxyproxy press on setting

Go to proxies configure like on the picture

Title file name type http hostname localhost ip 127.0.0.1 port 8080



brupsuit

Title brupsuit

Type HTTP

Country

City city

Color

Hostname 127.0.0.1

Port 8080

Username username

Password ****

PAC URL

As default foxyproxy is disable I enable it click on the file that I created

*Important when foxyproxy is running in the browser and Burp Suite the proxy tab intercept is running - we will not have internet

When the Burp Suite froxy intercept tab is running, we will have to click once on forwarding a forward request

Connect foxyproxy to burpsuite

We will run Burp Suite, we will go to proxy to intercept, change intercept is off to on

In the browser click plugins foxyproxy change to froxy which we did

We will get an error when surfing the Internet because we need a certificate to run froxyproxy burp suite ca certificate

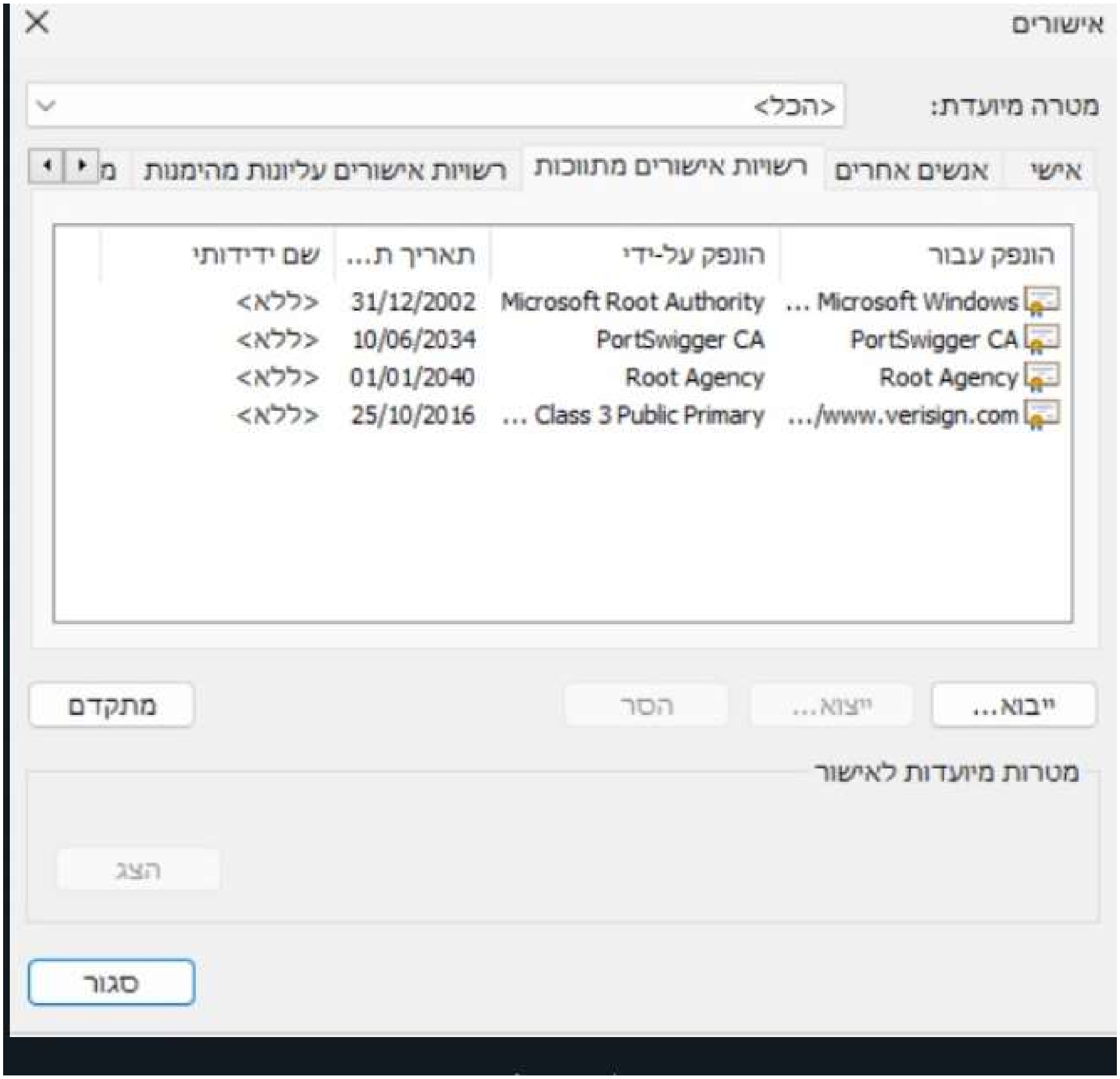
[Installing Burp's CA certificate in Chrome - Windows - PortSwigger]()

Go to [http://burpsuite:8080/]() download ca certificate

In the browser we will go to the security settings for certificate management, we will click there to attach a new certificate from an import file / we will select the file we downloaded and select a name automatically putting the file where it belongs

[View Certificate Details In Microsoft Edge - ComputerSluggish]()

Result file portswigger CA

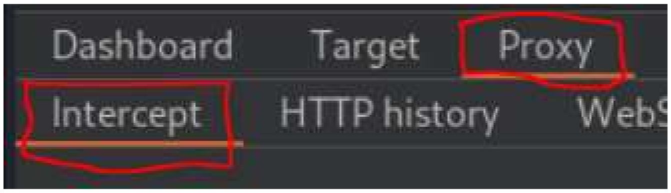


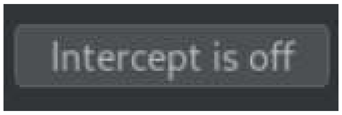
מטרה מיועדת: <הכל>

הונפק עבור	הונפק על-ידי	תאריך ת...	שם ידידותי
... Microsoft Windows	Microsoft Root Authority	31/12/2002	<ללא>
PortSwigger CA	PortSwigger CA	10/06/2034	<ללא>
Root Agency	Root Agency	01/01/2040	<ללא>
.../www.verisign.com	... Class 3 Public Primary	25/10/2016	<ללא>

You can also go to the proxy tab in the burp suite browser and click open browser to search for a website

We will activate the intercept option, go to the proxy tab, for the intercept option, click intercept is off, then in burpsuite, click forward a few times



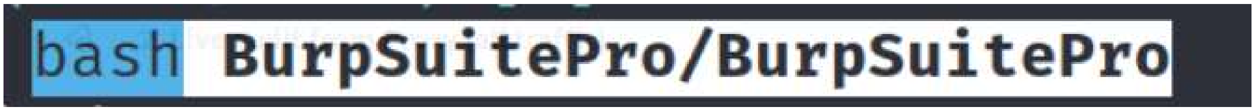


If the burpsuite software is not installed, it can be installed with the command sudo apt install burpsuite

Burp Suite community edition software will be installed

I am using Burp Suite pro version

I ran the BurpSuitePro/BurpSuitePro bash command software



```
bash BurpSuitePro/BurpSuitePro
```

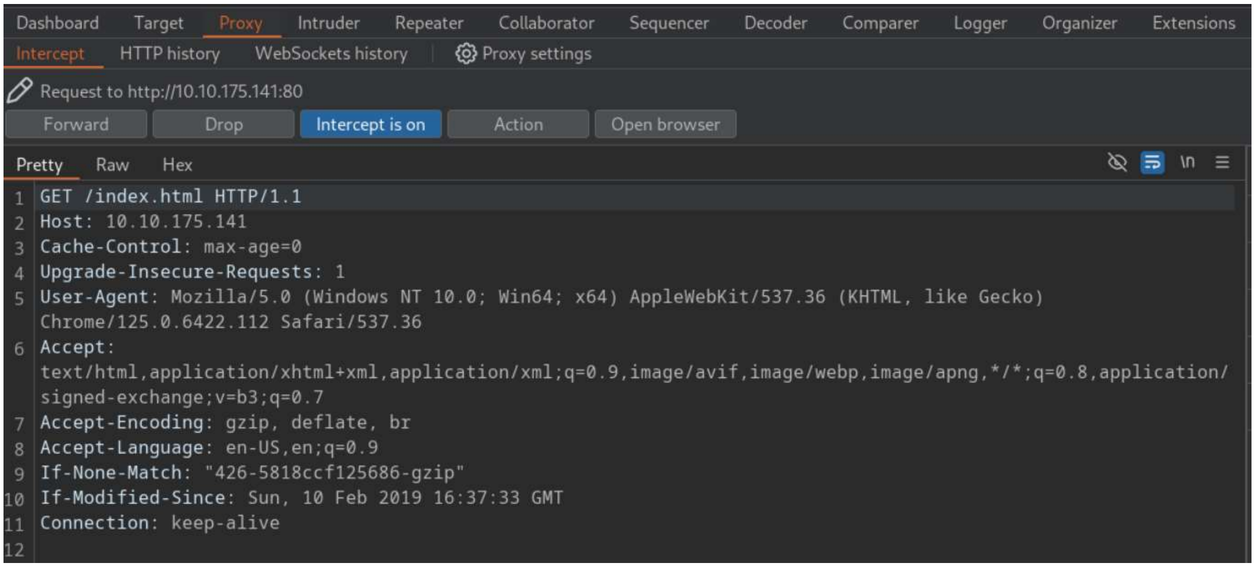
There is another free software like burpsuite calles zapproxy

[ZAP (zaproxy.org)]()

[ZAP – Getting Started (zaproxy.org)]()

[TryHackMe | Introduction to OWASP ZAP]()

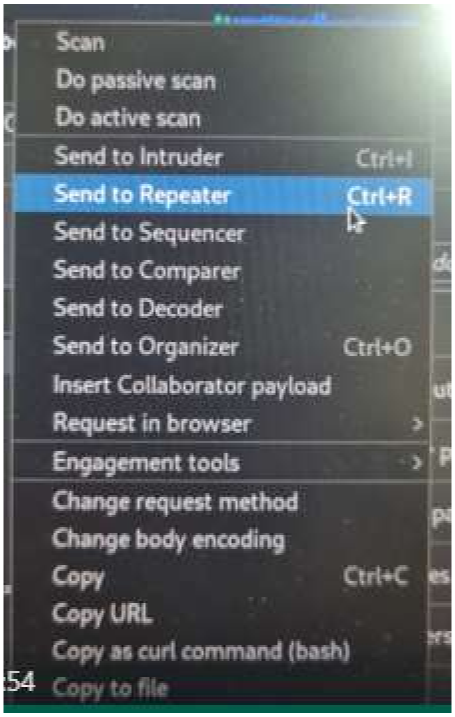
If the zopproxy software is not installed, it can be installed with the command sudo apt install zapproxy

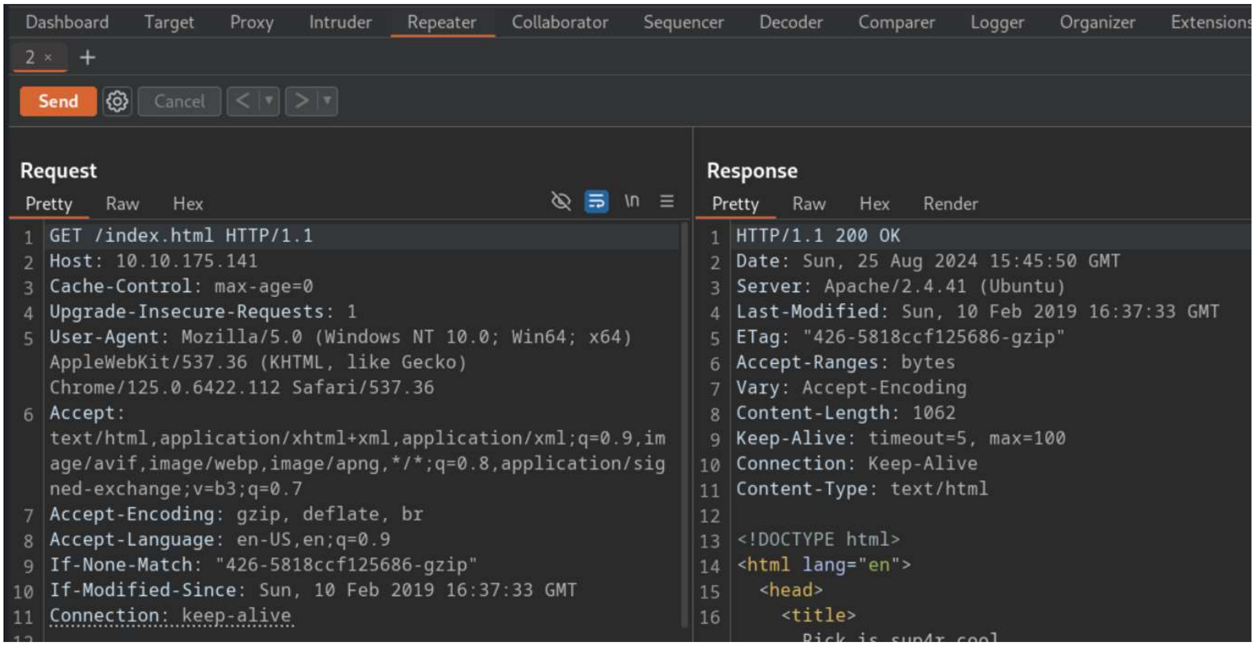


```
GET /index.html HTTP/1.1
Host: 10.10.175.141
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "426-5818ccf125686-gzip"
If-Modified-Since: Sun, 10 Feb 2019 16:37:33 GMT
Connection: keep-alive

```

I send it to burpsuite repeater tab

click right mouse button from option list click on send to repeater

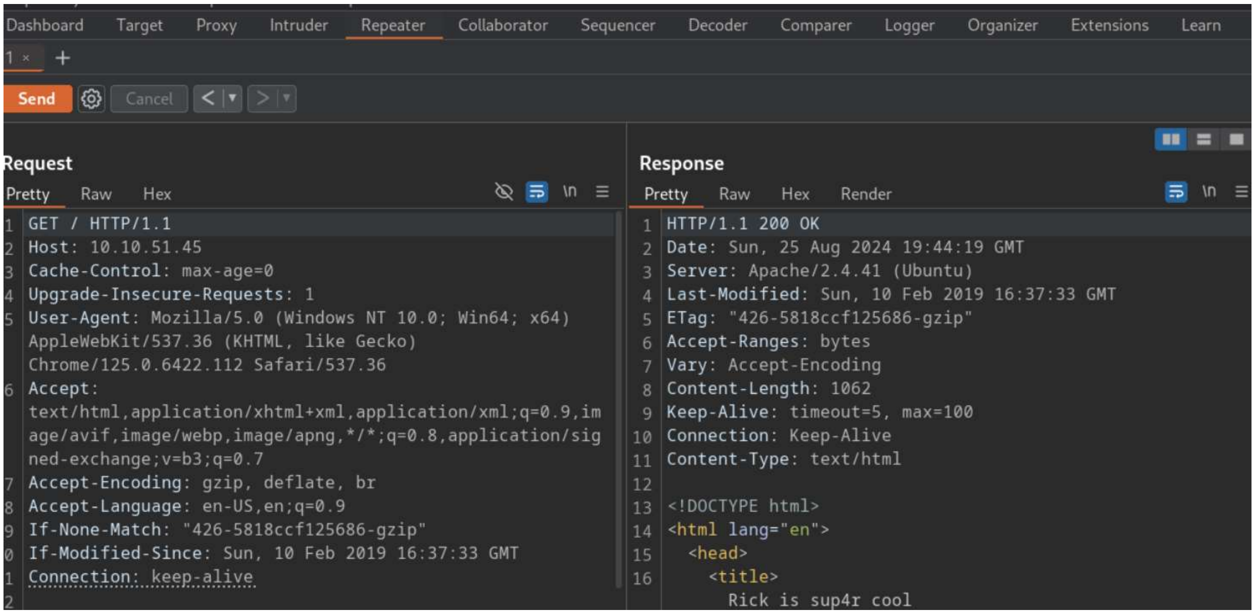




```
GET /index.html HTTP/1.1
Host: 10.10.175.141
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "426-5818ccf125686-gzip"
If-Modified-Since: Sun, 10 Feb 2019 16:37:33 GMT
Connection: keep-alive
```

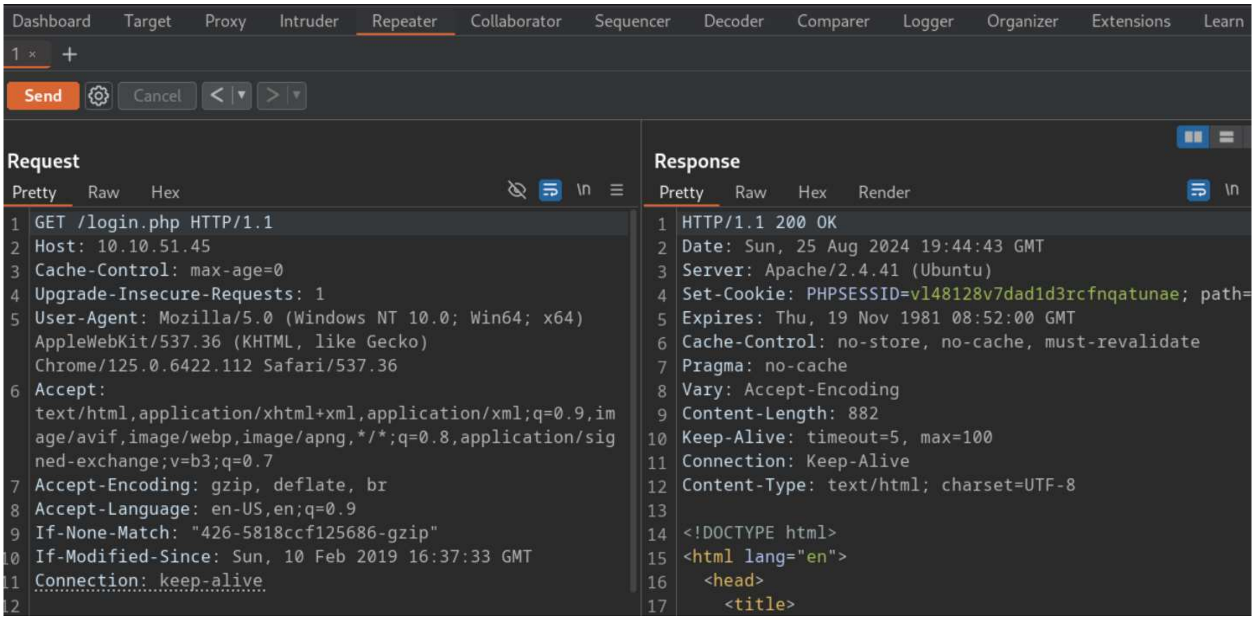
```
HTTP/1.1 200 OK
Date: Sun, 25 Aug 2024 15:45:50 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 10 Feb 2019 16:37:33 GMT
ETag: "426-5818ccf125686-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 1062
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
```

Lets try to change file and folders in the website



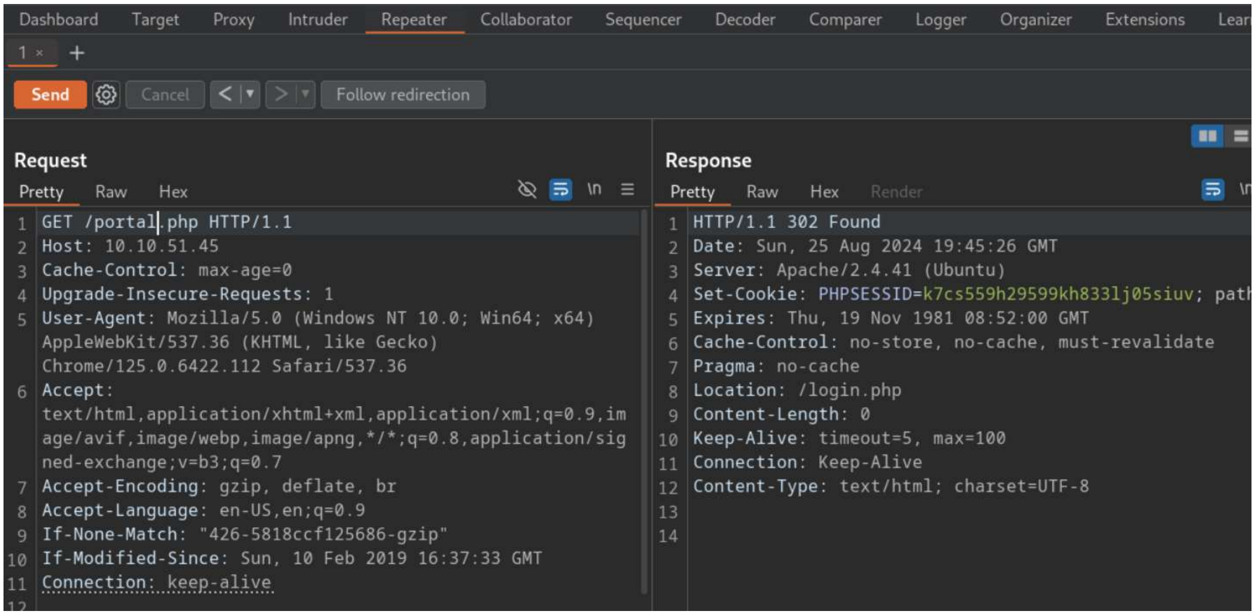
```
GET / HTTP/1.1
Host: 10.10.51.45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "426-5818ccf125686-gzip"
If-Modified-Since: Sun, 10 Feb 2019 16:37:33 GMT
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sun, 25 Aug 2024 19:44:19 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 10 Feb 2019 16:37:33 GMT
ETag: "426-5818ccf125686-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 1062
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      Rick is sup4r cool
```



```
GET /login.php HTTP/1.1
Host: 10.10.51.45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "426-5818ccf125686-gzip"
If-Modified-Since: Sun, 10 Feb 2019 16:37:33 GMT
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sun, 25 Aug 2024 19:44:43 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=vl48128v7dad1d3rcfnqatunae; path=
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 882
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
```



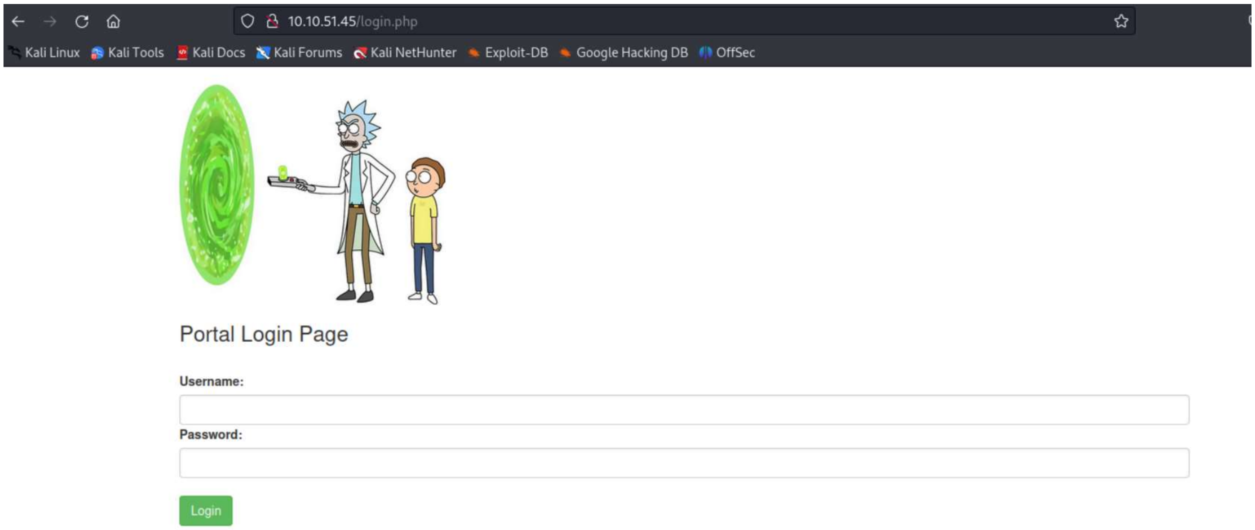
```
GET /portal.php HTTP/1.1
Host: 10.10.51.45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/125.0.6422.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
If-None-Match: "426-5818ccf125686-gzip"
If-Modified-Since: Sun, 10 Feb 2019 16:37:33 GMT
Connection: keep-alive
```

```
HTTP/1.1 302 Found
Date: Sun, 25 Aug 2024 19:45:26 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: PHPSESSID=k7cs559h29599kh833lj05siuv; path
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: /login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

I can move between folders on the website

Lets try to login to login.php

Tryhackme ip change to 10.10.51.45

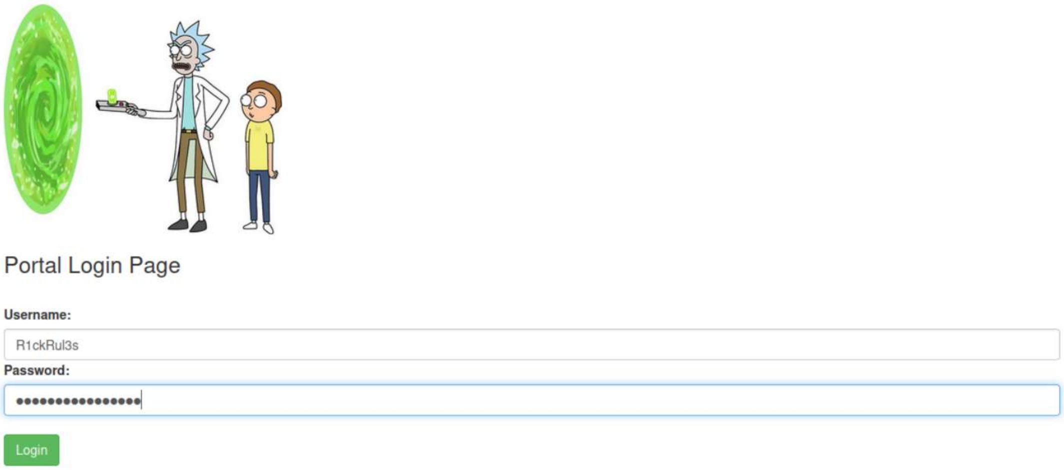


Portal Login Page

Username:

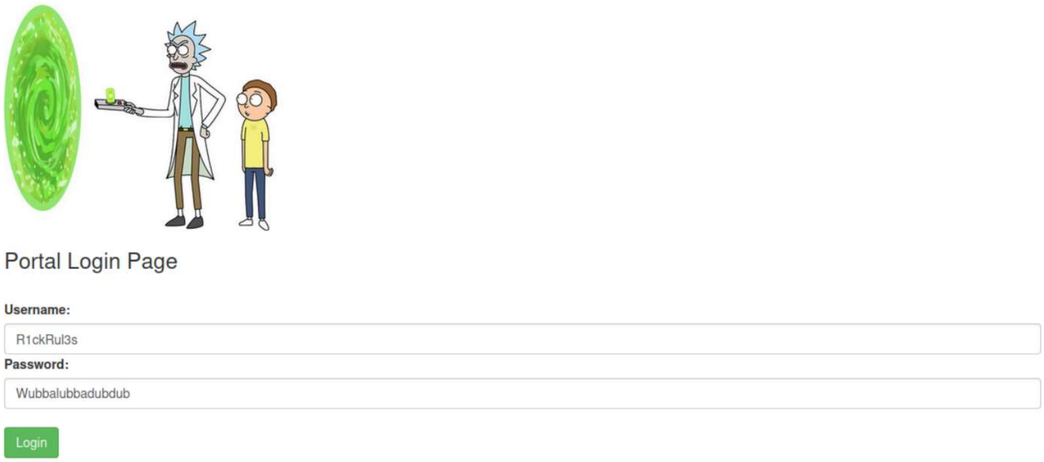
Password:

Lets put R1ckRul3s in username and Wubbalubbadubdub in password


Portal Login Page

Username: R1ckRul3s

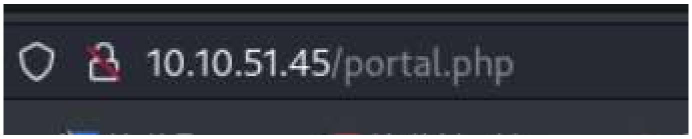
Password: ●●●●●●●●●●●●●●●●


Portal Login Page

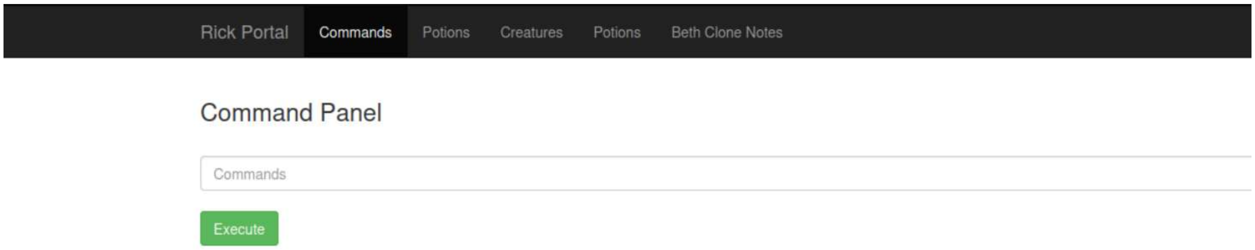
Username: R1ckRul3s

Password: Wubbalubbadubdub

I enter the website



10.10.51.45/portal.php



Command Panel

what is website command panel?

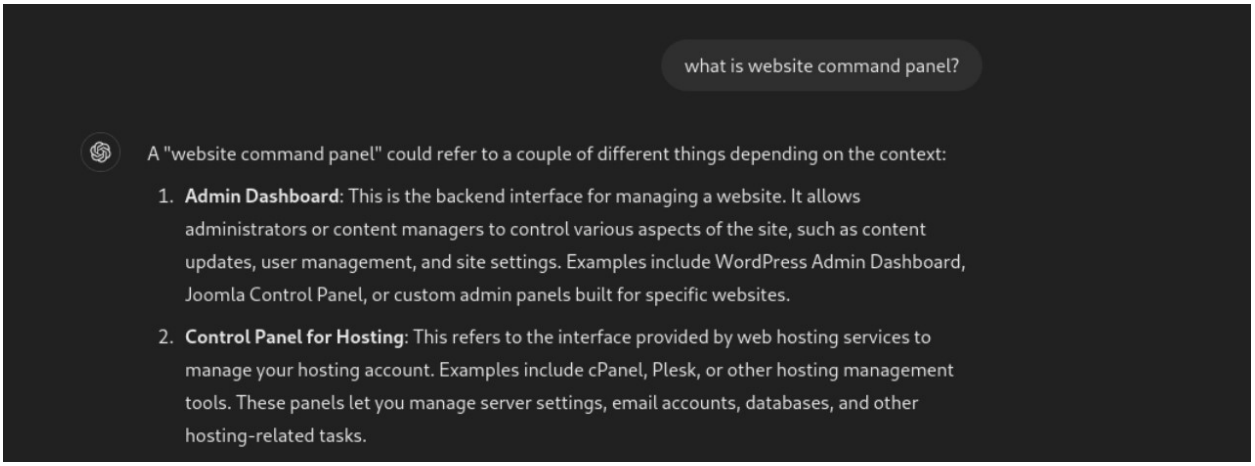
what is website command panel

Cpanel or command panel is a popular control dashboard that helps you manage your web hosting server using a human-friendly web-based interface

[What Is cPanel? The Control Dashboard Explained for Beginners (kinsta.com)]

[CommandPanels] I understand is a gui way to run commands from os like using website

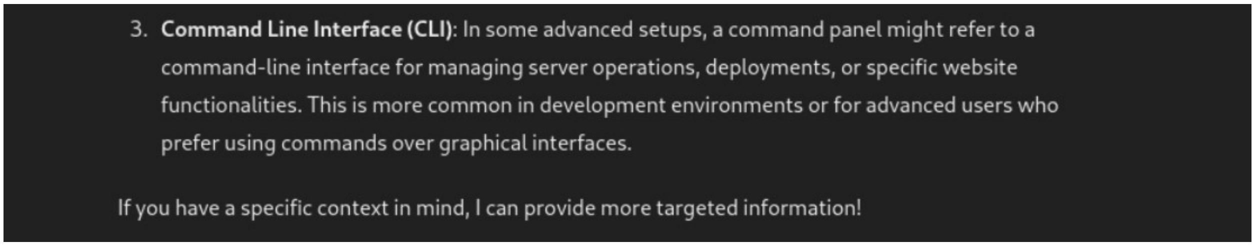
I ask chatgpt what is website command panel?



what is website command panel?

A "website command panel" could refer to a couple of different things depending on the context:

1. **Admin Dashboard**: This is the backend interface for managing a website. It allows administrators or content managers to control various aspects of the site, such as content updates, user management, and site settings. Examples include WordPress Admin Dashboard, Joomla Control Panel, or custom admin panels built for specific websites.
2. **Control Panel for Hosting**: This refers to the interface provided by web hosting services to manage your hosting account. Examples include cPanel, Plesk, or other hosting management tools. These panels let you manage server settings, email accounts, databases, and other hosting-related tasks.

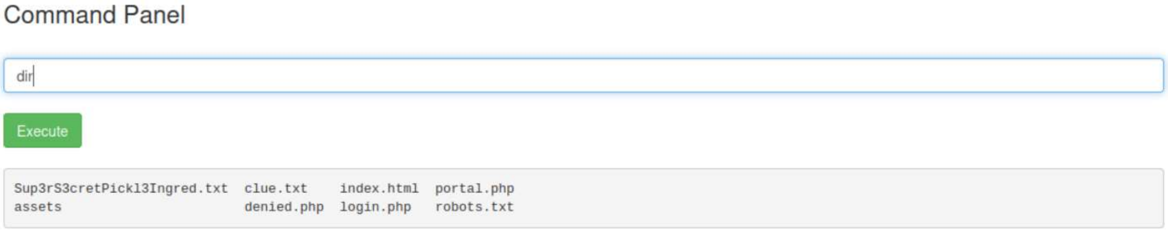


3. **Command Line Interface (CLI)**: In some advanced setups, a command panel might refer to a command-line interface for managing server operations, deployments, or specific website functionalities. This is more common in development environments or for advanced users who prefer using commands over graphical interfaces.

If you have a specific context in mind, I can provide more targeted information!

Lets check what folder we have on ubuntu server via command panel on website

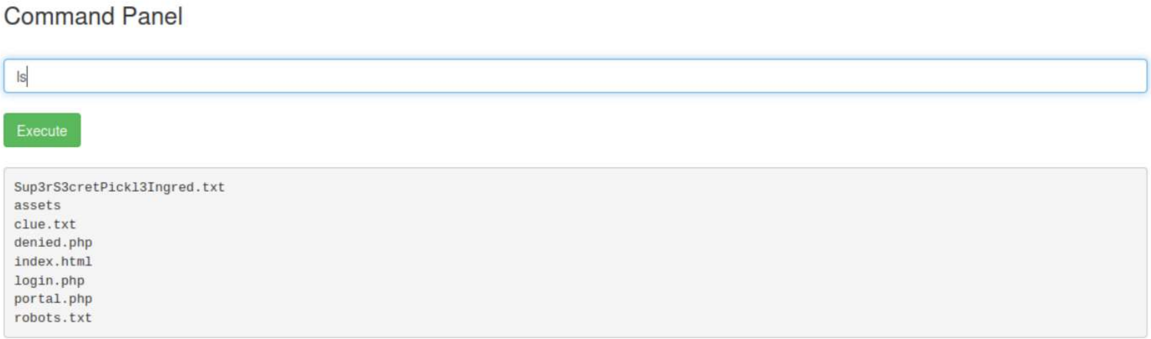
I type command dir



```
dir
```

```
Sup3rS3cretPickl3Ingred.txt  clue.txt    index.html  portal.php
assets                       denied.php  login.php   robots.txt
```

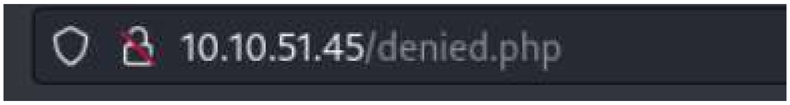
I type command ls



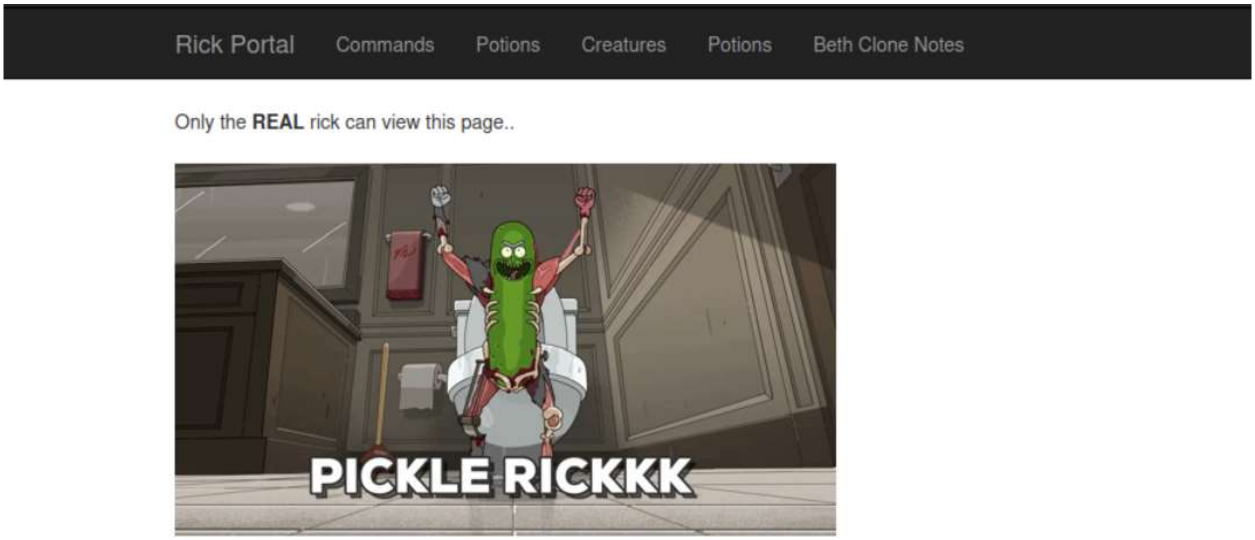
```
ls
```

```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

Lets enter denied.php see what this page

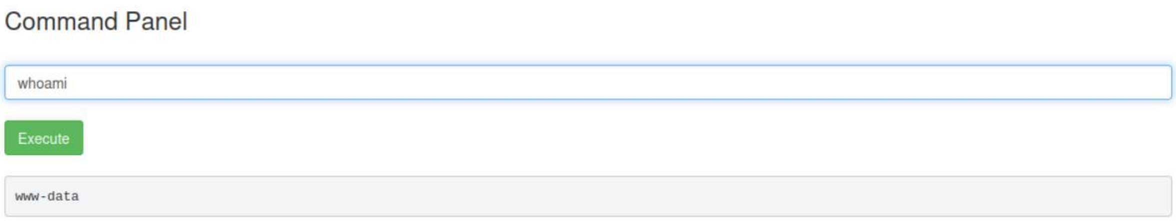


10.10.51.45/denied.php



Only the **REAL** rick can view this page..

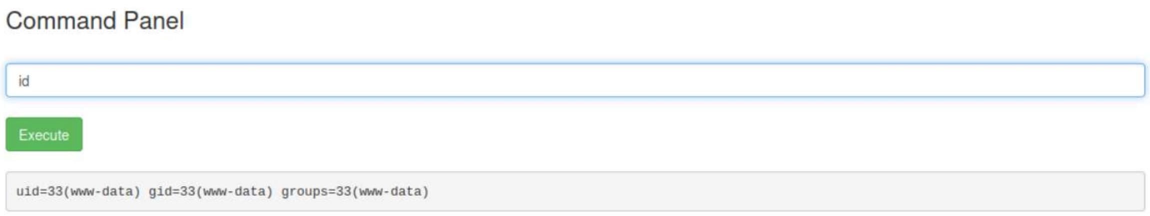
Lets see who the user I login as command whoami



```
whoami
```

```
www-data
```

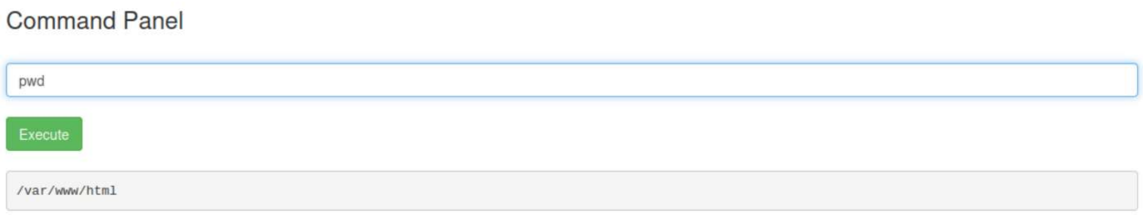
Lets see which groups the user I login as member command id



```
id
```

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Lets check where am I command pws



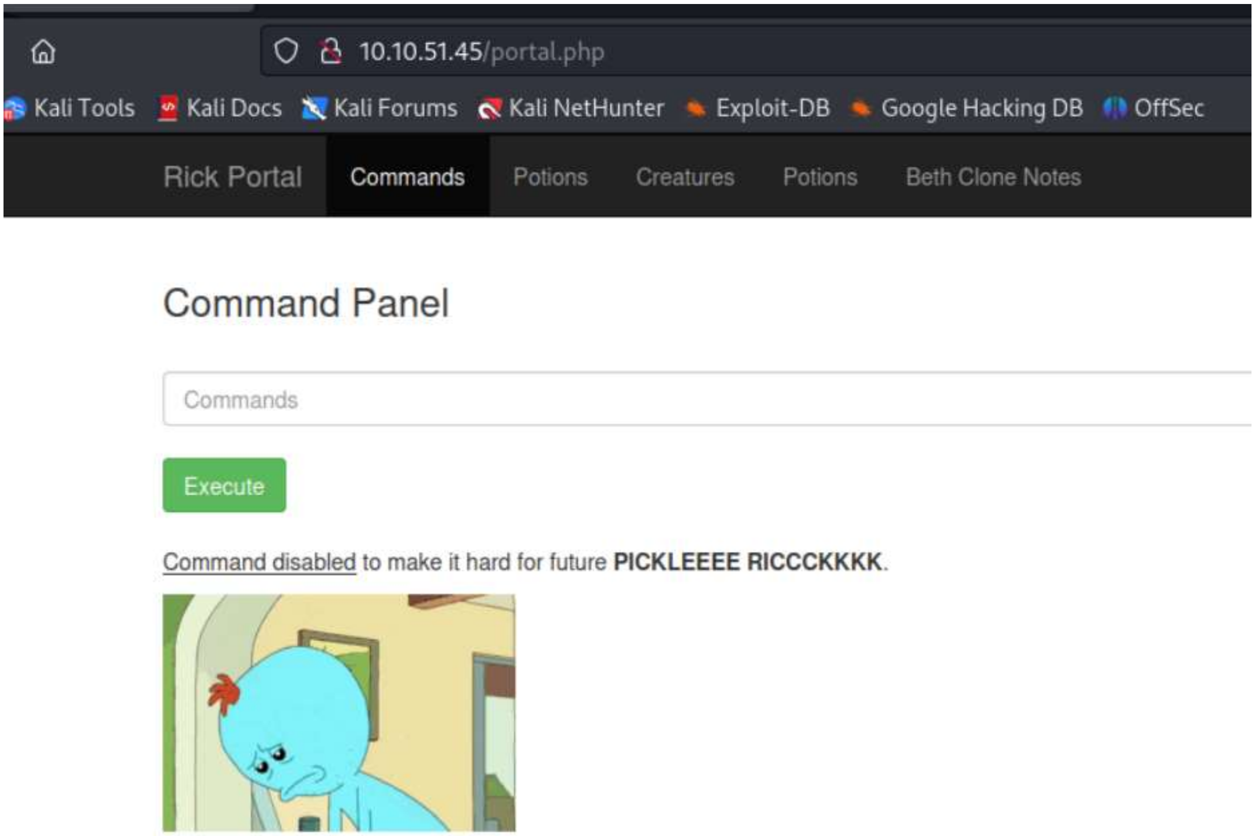
```
pwd
```

```
/var/www/html
```

On portal.php I see Sup3rS3cretPickl3Ingred.txt document

Lets read it command cat Sup3rS3cretPickl3Ingred.txt

Don’t work command cat is disable

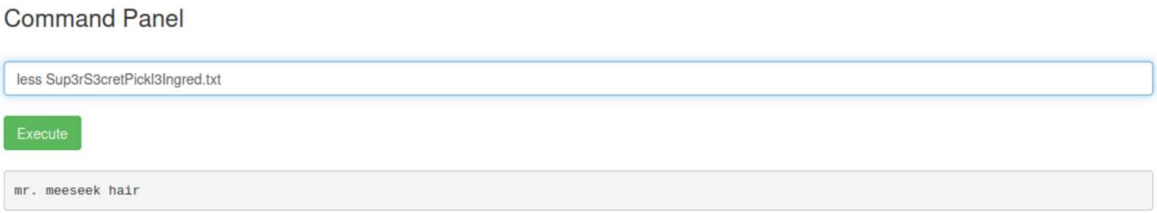


Command Panel

Command disabled to make it hard for future **PICKLEEEE RICCCKKKK**.

Lets try another command less Sup3rS3cretPickl3Ingred.txt

Found Sup3rS3cretPickl3Ingred.txt content: mr. meeseek hair



Command Panel

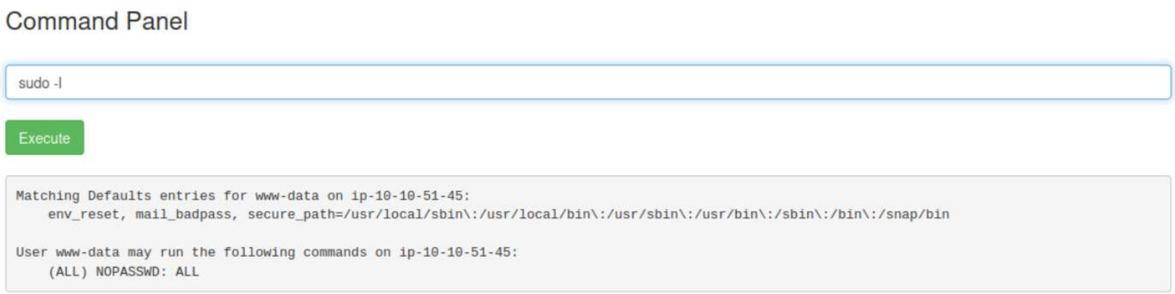
```
less Sup3rS3cretPickl3Ingred.txt
```

```
mr. meeseek hair
```

Question: What is the first ingredient that Rick needs?

Answer: mr. meeseek hair

Lets see which list insade sudo group command sudo -l



```
sudo -l
```

```
Matching Defaults entries for www-data on ip-10-10-51-45:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-51-45:
    (ALL) NOPASSWD: ALL
```

command sudo -l that say which users members of sudo group

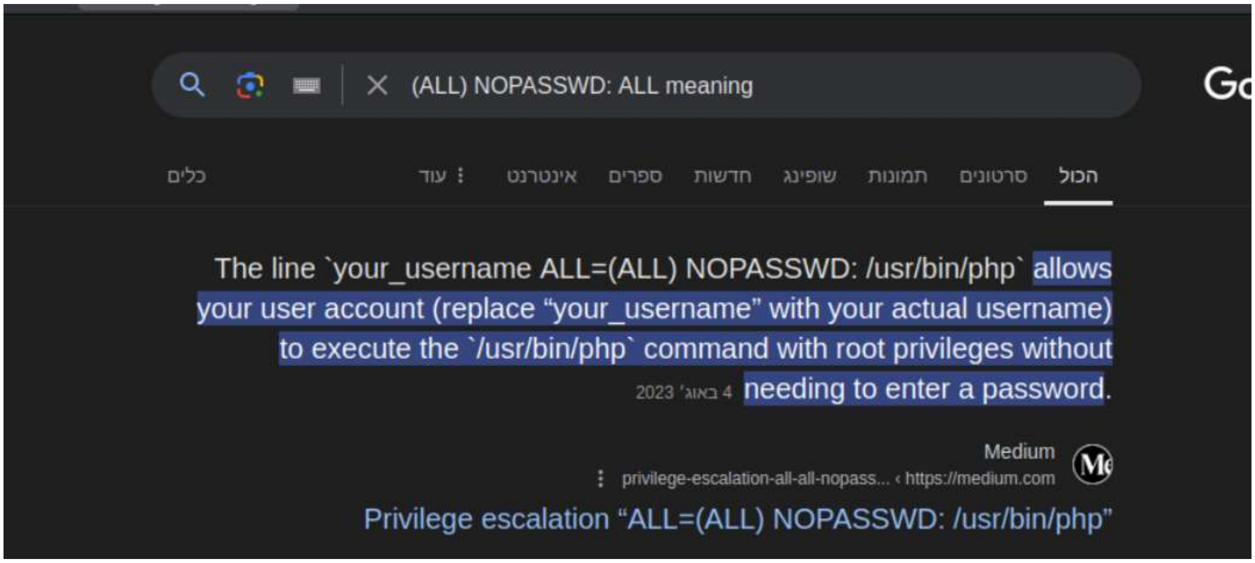
[Sudo Command in Linux | Linuxize]

[A Beginner's Guide to Understanding sudo on Ubuntu (howtoforge.com)]

[sudo(8): execute command as another user - Linux man page (die.net)]

[sudo(8) - Linux manual page (man7.org)] list a user's privileges for the remote host

Command (ALL) NOPASSWD: ALL meaning


(ALL) NOPASSWD: ALL meaning
הכול
סרטונים
תמונות
שופינג
חדשות
ספרים
אינטרנט
עוד
כלים
Medium
privilege-escalation-all-all-nopass... ‹ https://medium.com

The line `your_username ALL=(ALL) NOPASSWD: /usr/bin/php` allows your user account (replace “your_username” with your actual username) to execute the `/usr/bin/php` command with root privileges without needing to enter a password. 4 באוג׳ 2023

Privilege escalation “ALL=(ALL) NOPASSWD: /usr/bin/php”

https://medium.com/@rebaleos0/privilege-escalation-all-all-nopasswd-usr-bin-php-241a2c43e58d

users or groups are able to run sudo without authenticating. This makes it a big security risk so be very careful with this command.

NOPASSWD: or PASSWD: specifies whether a password is required. This is optional and defaults PASSWD unless the default has been changed in sudoers configuration.

https://superuser.com/questions/1495807/can-someone-explain-what-is-user-all-all-nopasswdall-does-in-sudoers-file

Means to run ALL commands without a password for a specific user

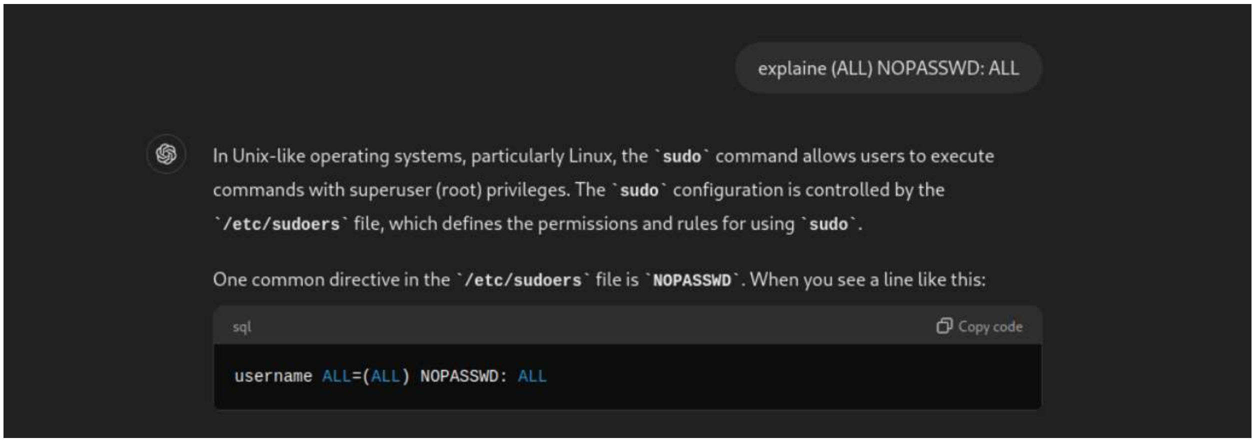
https://stackoverflow.com/questions/47423552/what-is-the-meaning-of-jenkins-all-all-nopasswd-all-and-does-it-create-a-se

Meaning of chatgpt

Command ALL here means the user can execute commands as any user, including root.

Command NOPASSWD This directive specifies that no password is required when the user executes the command(s) specified.

Command ALL after NOPASSWD means any command can be run without requiring a password.

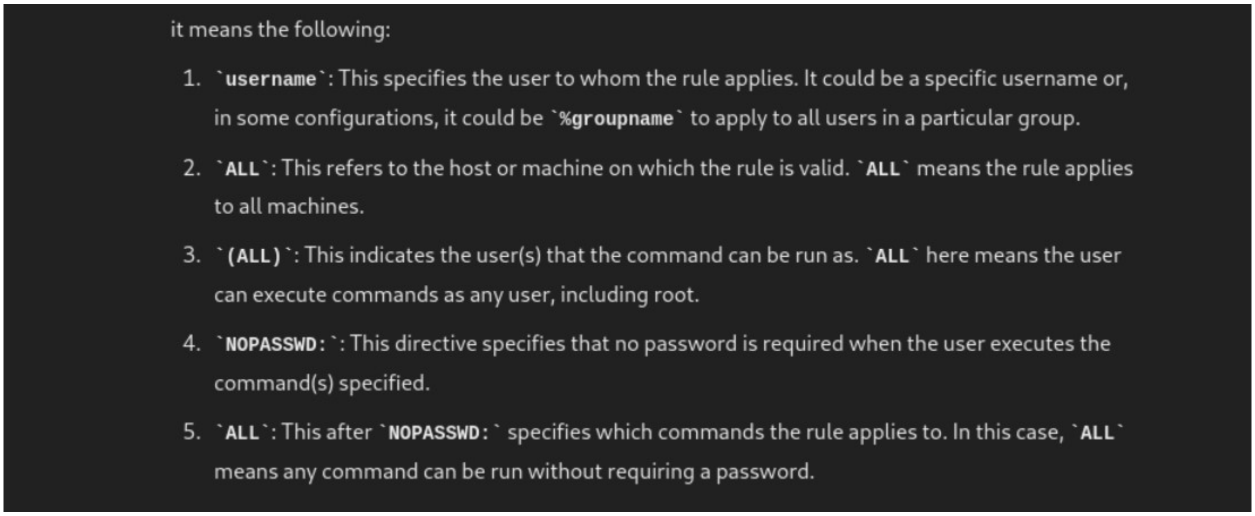


explaine (ALL) NOPASSWD: ALL

In Unix-like operating systems, particularly Linux, the `sudo` command allows users to execute commands with superuser (root) privileges. The `sudo` configuration is controlled by the `/etc/sudoers` file, which defines the permissions and rules for using `sudo`.

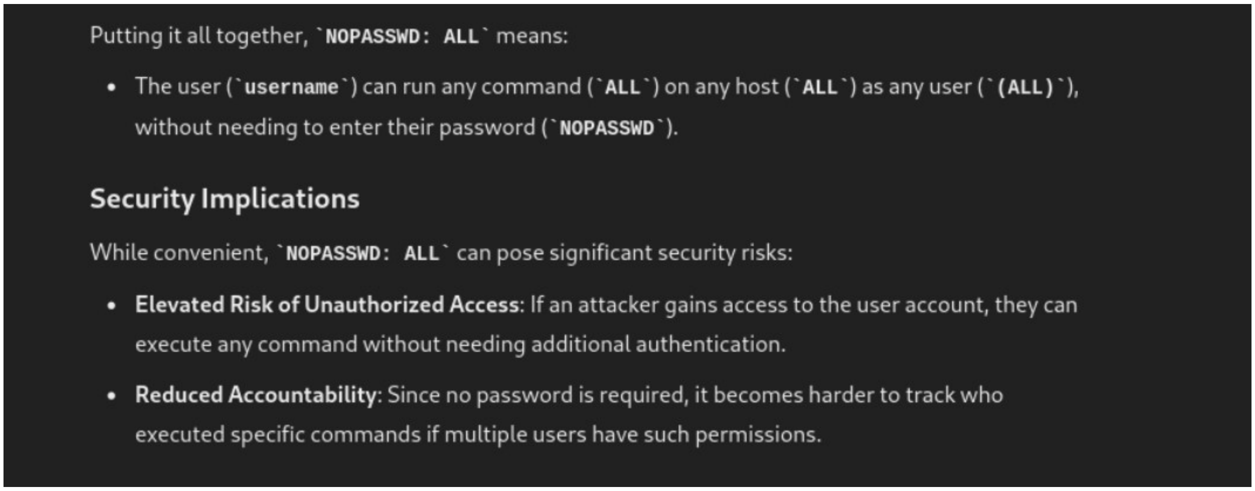
One common directive in the `/etc/sudoers` file is `NOPASSWD`. When you see a line like this:

```sql
username ALL=(ALL) NOPASSWD: ALL
```



it means the following:

1. `username`: This specifies the user to whom the rule applies. It could be a specific username or, in some configurations, it could be `%groupname` to apply to all users in a particular group.
2. `ALL`: This refers to the host or machine on which the rule is valid. `ALL` means the rule applies to all machines.
3. `(ALL)`: This indicates the user(s) that the command can be run as. `ALL` here means the user can execute commands as any user, including root.
4. `NOPASSWD:`: This directive specifies that no password is required when the user executes the command(s) specified.
5. `ALL`: This after `NOPASSWD:` specifies which commands the rule applies to. In this case, `ALL` means any command can be run without requiring a password.



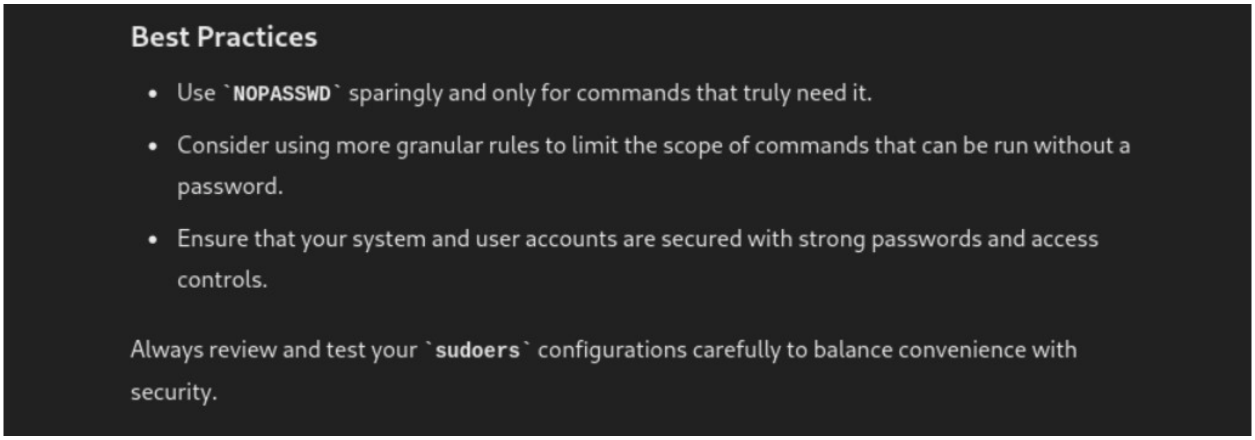
Putting it all together, `NOPASSWD: ALL` means:

- The user (`username`) can run any command (`ALL`) on any host (`ALL`) as any user (`(ALL)`), without needing to enter their password (`NOPASSWD`).

Security Implications

While convenient, `NOPASSWD: ALL` can pose significant security risks:

- **Elevated Risk of Unauthorized Access**: If an attacker gains access to the user account, they can execute any command without needing additional authentication.
- **Reduced Accountability**: Since no password is required, it becomes harder to track who executed specific commands if multiple users have such permissions.



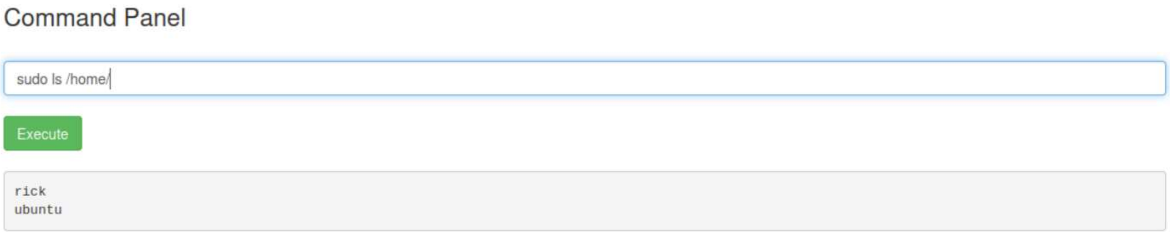
Best Practices

- Use `NOPASSWD` sparingly and only for commands that truly need it.
- Consider using more granular rules to limit the scope of commands that can be run without a password.
- Ensure that your system and user accounts are secured with strong passwords and access controls.

Always review and test your `sudoers` configurations carefully to balance convenience with security.

So Command (ALL) NOPASSWD: ALL meaning user www-data can run all commands as root user

I enter home folder to see which user active on the system command sudo ls /home

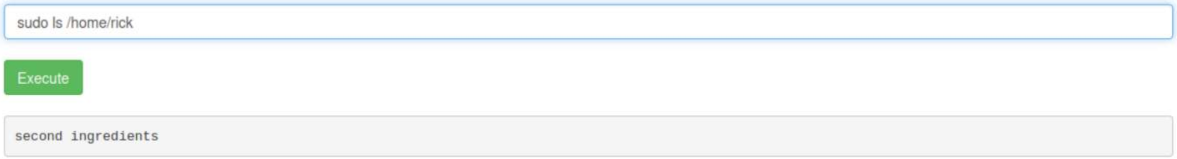


Command Panel

```
sudo ls /home/
```

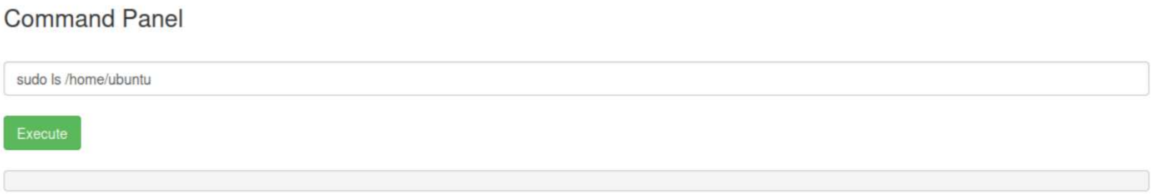
```
rick
ubuntu
```

Lets see what files their contain command sudo ls /home/rick and sudo ls /home/ubuntu



```
sudo ls /home/rick
```

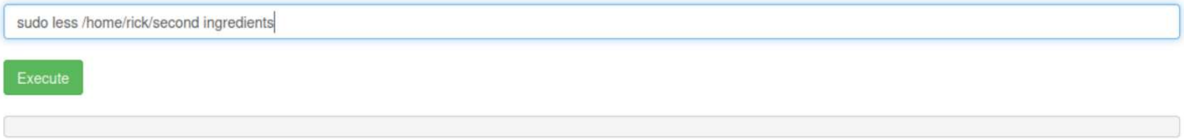
```
second ingredients
```



```
sudo ls /home/ubuntu
```

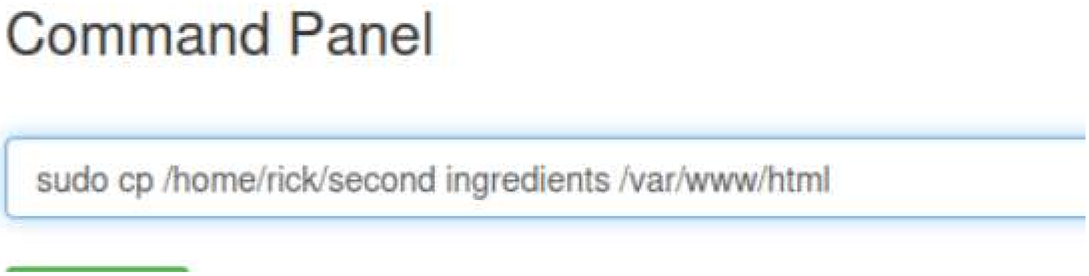
On rick folder I see second ingredients document

Lets read it command sudo less /home/rick/second ingredients

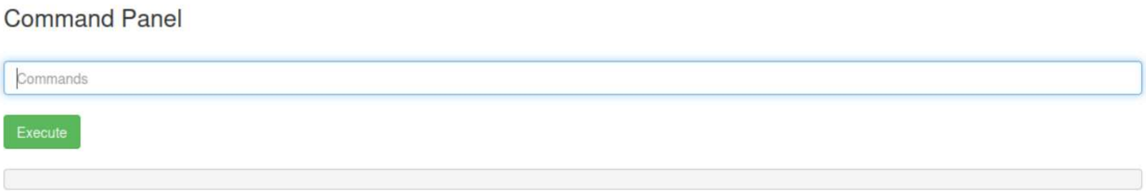


```
sudo less /home/rick/second ingredients
```

Lets copy the document to /var/www/html a folder user www-data have permissions on files there command sudo cp /home/rick/second ingredients /var/www/html/

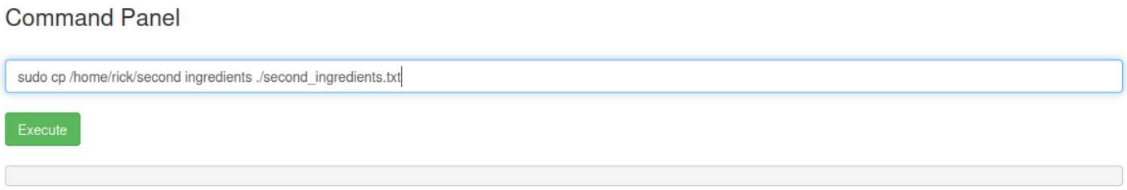


```
sudo cp /home/rick/second ingredients /var/www/html
```



Not work

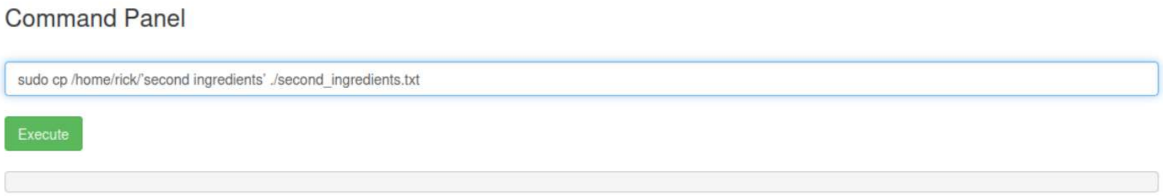
Lets try sudo cp /home/rick/second ingredients ./second_ingredients.txt



```
sudo cp /home/rick/second ingredients ./second_ingredients.txt
```

Not work

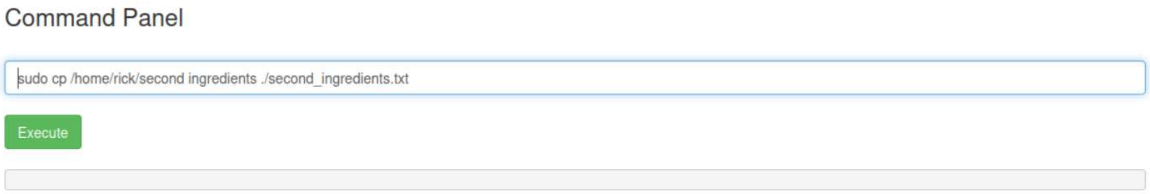
Lets try sudo cp /home/rick/second ingredients ./second_ingredients.txt



```
sudo cp /home/rick/'second ingredients' ./second_ingredients.txt
```

Not work

Lets try sudo cp /home/rick/second ingredients ./second_ingredients.txt



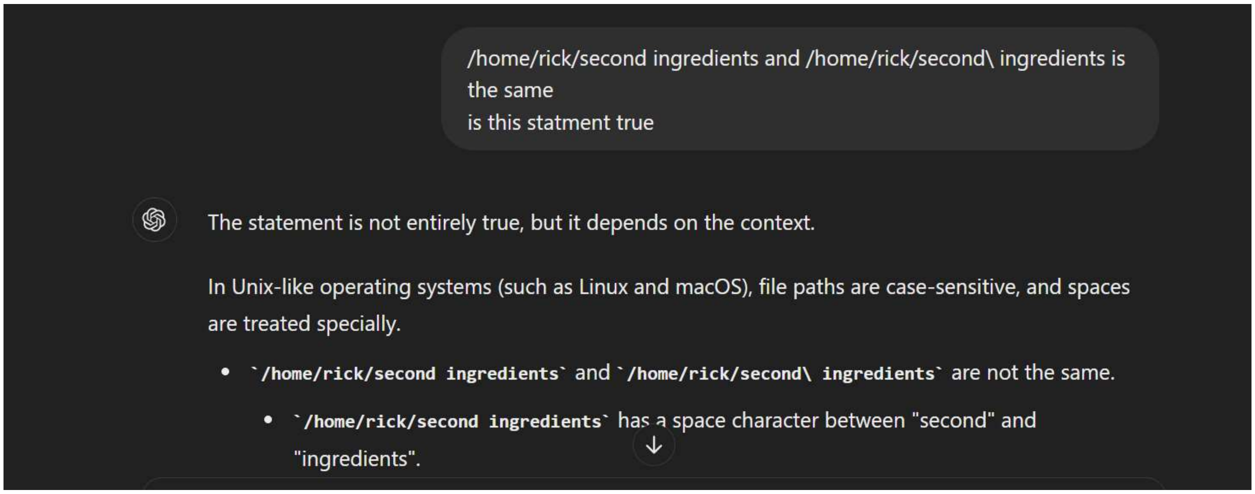
```
sudo cp /home/rick/second ingredients ./second_ingredients.txt
```

Not work

Lets leave copy the document to our folder

/home/rick/second ingredients and /home/rick/second\ ingredients is the same

I ask chat gpt: /home/rick/second ingredients and /home/rick/second\ ingredients is the same is this statment true

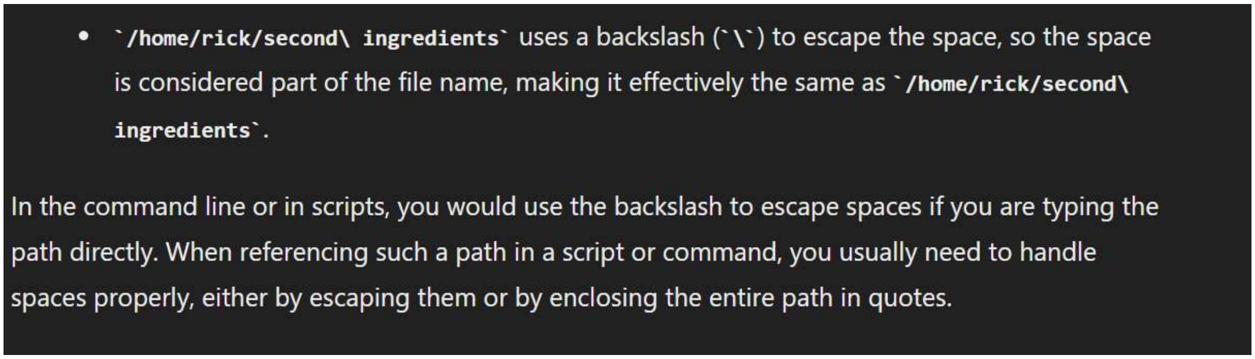


/home/rick/second ingredients and /home/rick/second\ ingredients is the same
is this statment true

The statement is not entirely true, but it depends on the context.

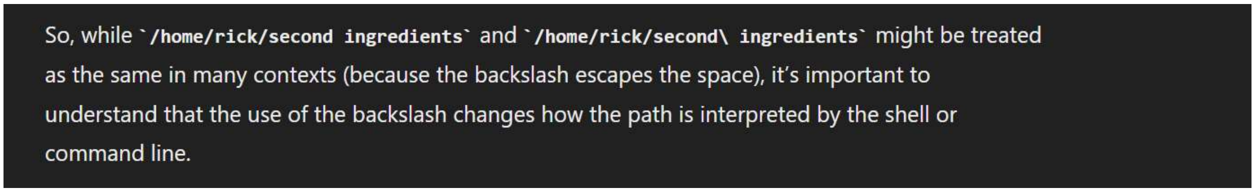
In Unix-like operating systems (such as Linux and macOS), file paths are case-sensitive, and spaces are treated specially.

- `/home/rick/second ingredients` and `/home/rick/second\ ingredients` are not the same.
  - `/home/rick/second ingredients` has a space character between "second" and "ingredients".



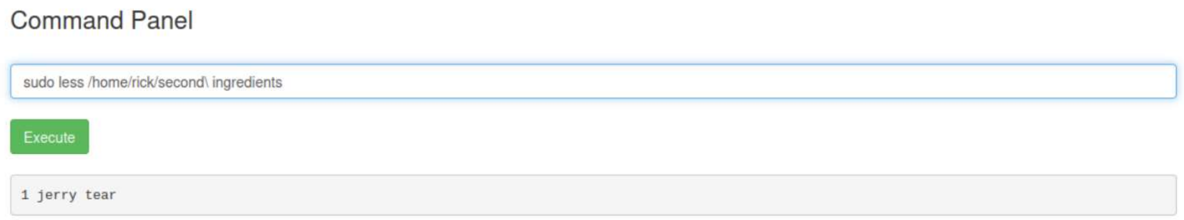
  - `/home/rick/second\ ingredients` uses a backslash (`\`) to escape the space, so the space is considered part of the file name, making it effectively the same as `/home/rick/second\ ingredients`.

In the command line or in scripts, you would use the backslash to escape spaces if you are typing the path directly. When referencing such a path in a script or command, you usually need to handle spaces properly, either by escaping them or by enclosing the entire path in quotes.



So, while `/home/rick/second ingredients` and `/home/rick/second\ ingredients` might be treated as the same in many contexts (because the backslash escapes the space), it's important to understand that the use of the backslash changes how the path is interpreted by the shell or command line.

So lets try read second ingredients command sudo less /home/rick/second\ ingredients



```
sudo less /home/rick/second\ ingredients
```

```
1 jerry tear
```

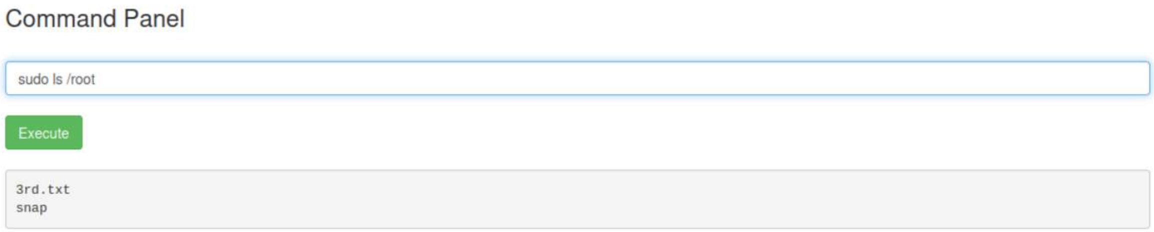
Found second ingredients content: 1 jerry tear

Question: What is the second ingredient in Rick's potion?

Answer: 1 jerry tear

I know their user root on the system and it user folder is /root

Lets see what file inside /root folder command sudo ls /root

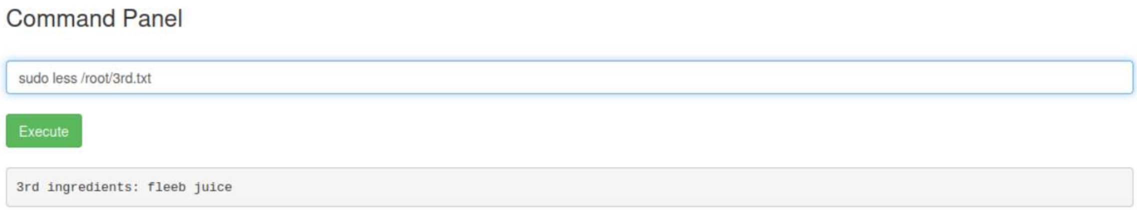


```
sudo ls /root
```

```
3rd.txt
snap
```

On /root folder I see 3rd.txt ducoment

So lets try read 3rd.txt command sudo less /root/3rd.txt



```
sudo less /root/3rd.txt
```

```
3rd ingredients: fleeb juice
```

Found 3rd.txt content: fleeb juice

Question: What is the last and final ingredient?

Answer: fleeb juice