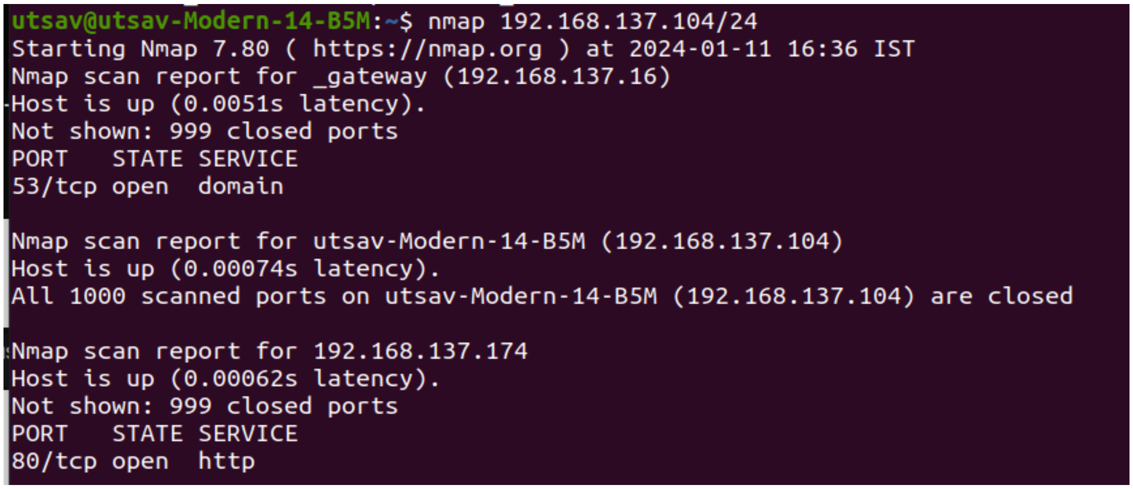
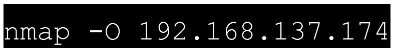
Challenge - 1 : Gain Access to Remote Server

After login as a guest I searched and reviewed previous submissions then I got to know that I have to use nmap to scan any open ports of the vm machine.So, i do nmap scan on my wireless network ip and check for any open ports.



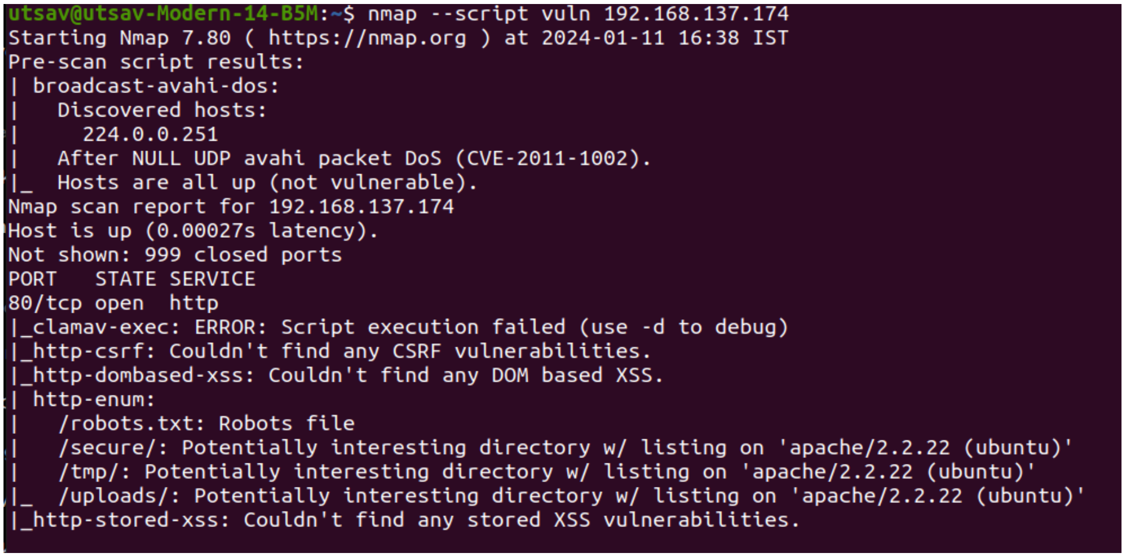
```
utsav@utsav-Modern-14-B5M:~$ nmap 192.168.137.104/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-11 16:36 IST
Nmap scan report for _gateway (192.168.137.16)
Host is up (0.0051s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for utsav-Modern-14-B5M (192.168.137.104)
Host is up (0.00074s latency).
All 1000 scanned ports on utsav-Modern-14-B5M (192.168.137.104) are closed

Nmap scan report for 192.168.137.174
Host is up (0.00062s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

Then i found that 1 port is open to check it run another nmap scan which tell me that which os is running on this port using



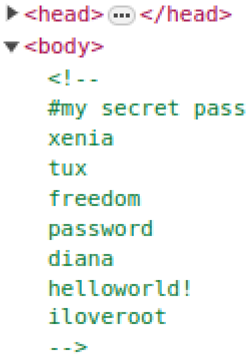
```
nmap -O 192.168.137.174
```

I found linux is running on it so then i ran script scanning to found any vulnerability on that ip.



```
utsav@utsav-Modern-14-B5M:~$ nmap --script vuln 192.168.137.174
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-11 16:38 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.137.174
Host is up (0.00027s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|   /secure/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /tmp/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Then i check the ip address with robots.txt and found that disallowed path but there i found nothing except for /nothing where on inspect i found some commented passwords

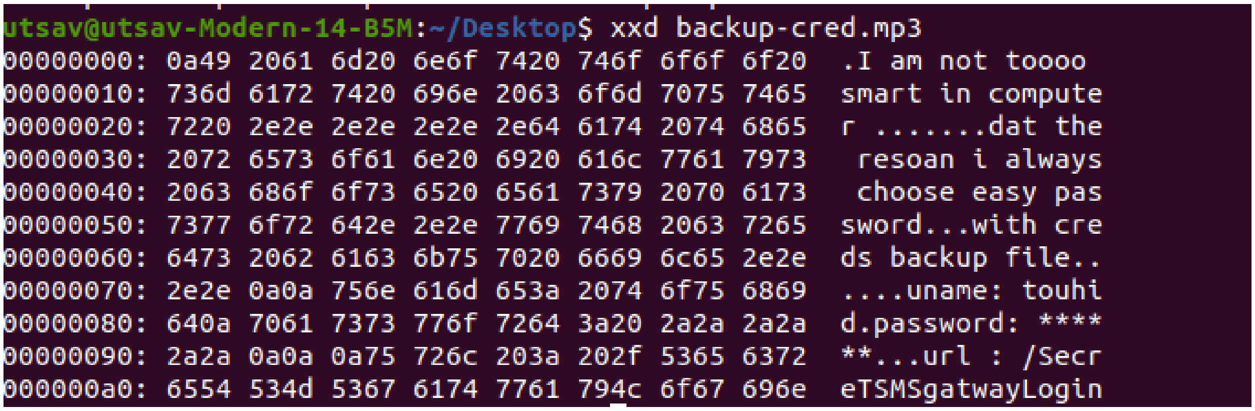


```
▶<head>⋯</head>
▼<body>
   <!--
   #my secret pass
   xenia
   tux
   freedom
   password
   diana
   helloworld!
   iloveroot
   -->
```

Then I checked for /secure which is hidden and found a backup.zip file there. I opened it and found an mp3 file inside it and it is not opening so I thought about changing its extension. First I tried some possible extensions randomly but didn't succeeded.after that i googled to find a command to know about the correct extension of a file and found a command.

File filename

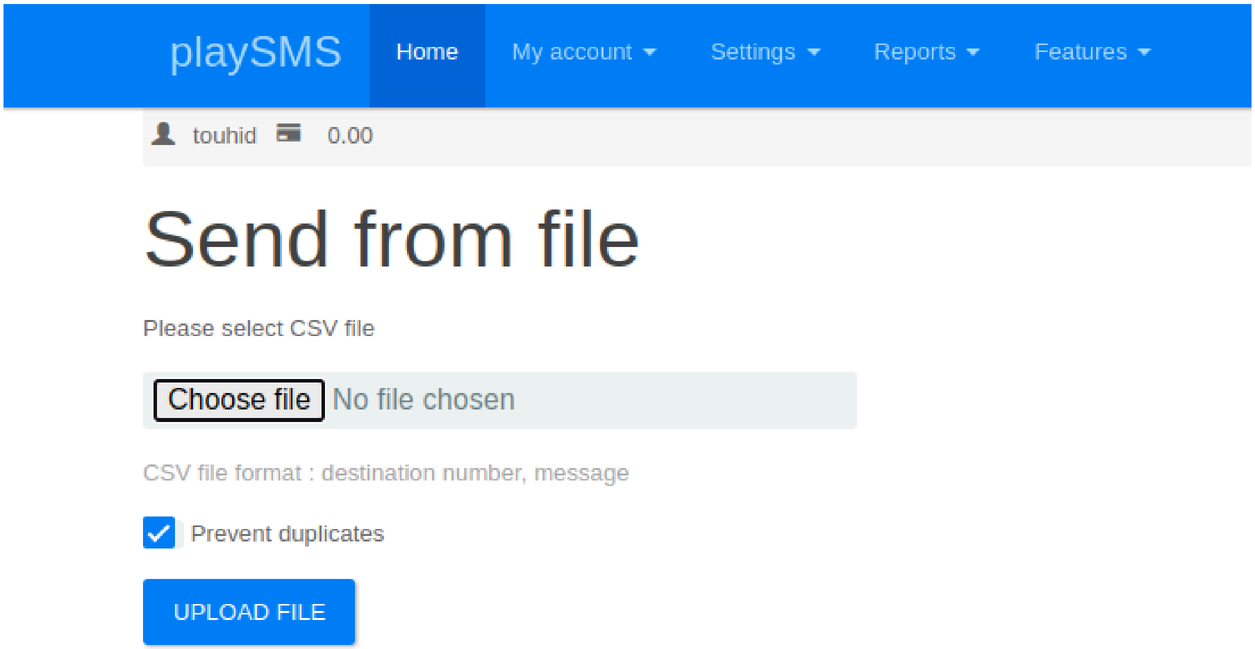
Which gave me ASCII text as output and searched and found to use hex code command to retrieve it and found the lines inside that file.



```
utsav@utsav-Modern-14-B5M:~/Desktop$ xxd backup-cred.mp3
00000000: 0a49 2061 6d20 6e6f 7420 746f 6f6f 6f20  .I am not toooo
00000010: 736d 6172 7420 696e 2063 6f6d 7075 7465  smart in compute
00000020: 7220 2e2e 2e2e 2e2e 2e64 6174 2074 6865  r .......dat the
00000030: 2072 6573 6f61 6e20 6920 616c 7761 7973   resoan i always
00000040: 2063 686f 6f73 6520 6561 7379 2070 6173   choose easy pas
00000050: 7377 6f72 642e 2e2e 7769 7468 2063 7265  sword...with cre
00000060: 6473 2062 6163 6b75 7020 6669 6c65 2e2e  ds backup file..
00000070: 2e2e 0a0a 756e 616d 653a 2074 6f75 6869  ....uname: touhi
00000080: 640a 7061 7373 776f 7264 3a20 2a2a 2a2a  d.password: ****
00000090: 2a2a 0a0a 0a75 726c 203a 202f 5365 6372  **...url : /Secr
000000a0: 6554 534d 5367 6174 7761 794c 6f67 696e  eTSMSgatwayLogin
```

Here i got the uname - touhid and password : ****** and url so i went on the url given and found a login page there after i put uname and password there it is showing me invalid and i could not also recover the password so after searching a lot on google and trying using different tools i did not get anything. Then I thought of trying the above passwords which I got from inspecting /nothing and voila one of the passwords worked and i logged in.

There I found a send a file option and I tried to use the same thing which was in previous submissions: a reverse shell attack using a php script.



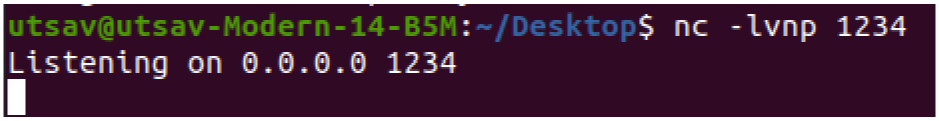
Send from file

Please select CSV file

CSV file format : destination number, message

☑ Prevent duplicates

And tried to listen it to the port of my machine but didn't get anything.



```
utsav@utsav-Modern-14-B5M:~/Desktop$ nc -lvnp 1234
Listening on 0.0.0.0 1234
█
```