

Luke

Synopsis

Luke is a medium difficulty Linux box featuring server enumeration and credential reuse. A configuration file leads to credential disclosure, which can be used to authenticate to a NodeJS server. The server in turn stores user credentials, and one of these provides access to a password protected folder containing configuration files. From this, the Ajenti password can be obtained and used to sign in, and execute commands in the context of root

Skills

- Enumeration
- NodeJS enumeration

Exploitation

As always we start with the nmap to check what services/ports are open

```

nmap scan report for 10.10.10.137
Host is up (0.086s latency).
Not shown: 995 closed tcp ports (reset)
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 2019 webapp
ftp-syst:
STAT:
FTP server status:
  Connected to 10.10.14.5
  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?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http     Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
|_http-title: Luke
|_http-methods:
|_ Potentially risky methods: TRACE
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/10%OT=21%CT=1%CU=30242%PV=Y%D=2%DC=T%G=Y%TM=64D54DD
OS:F&P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=107%TI=Z%CI=Z%II=RI%TS=22)S
OS:EQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%TS=22)OPS(O1=M53CNW6ST11%O2=M53CNW6ST1

```

We see that FTP and 3 web ports are open
First we checked a content of FTP but we didn't find anything interesting there

```

--# cat for*
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 !

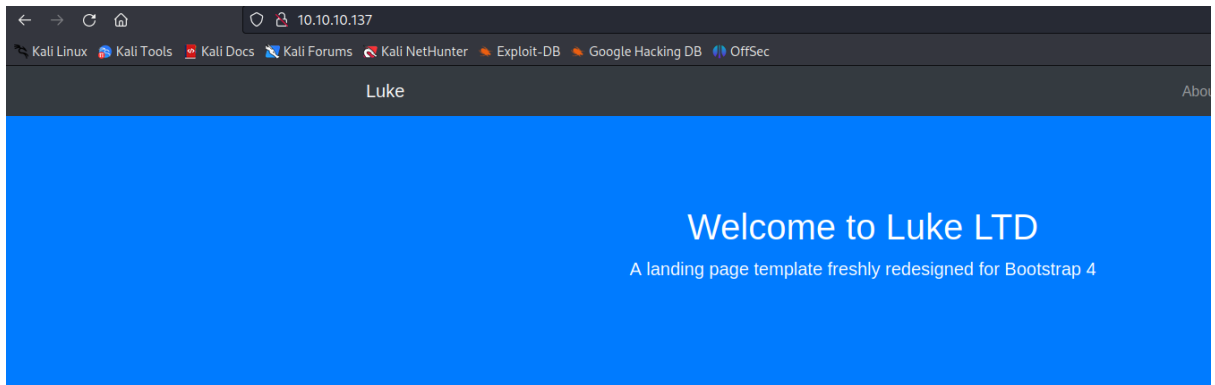
Derry

root@kali: / # cd /var/www/html/10.10.10.127/webapp/

```

Next, we access all 3 web ports what gave us the following pages

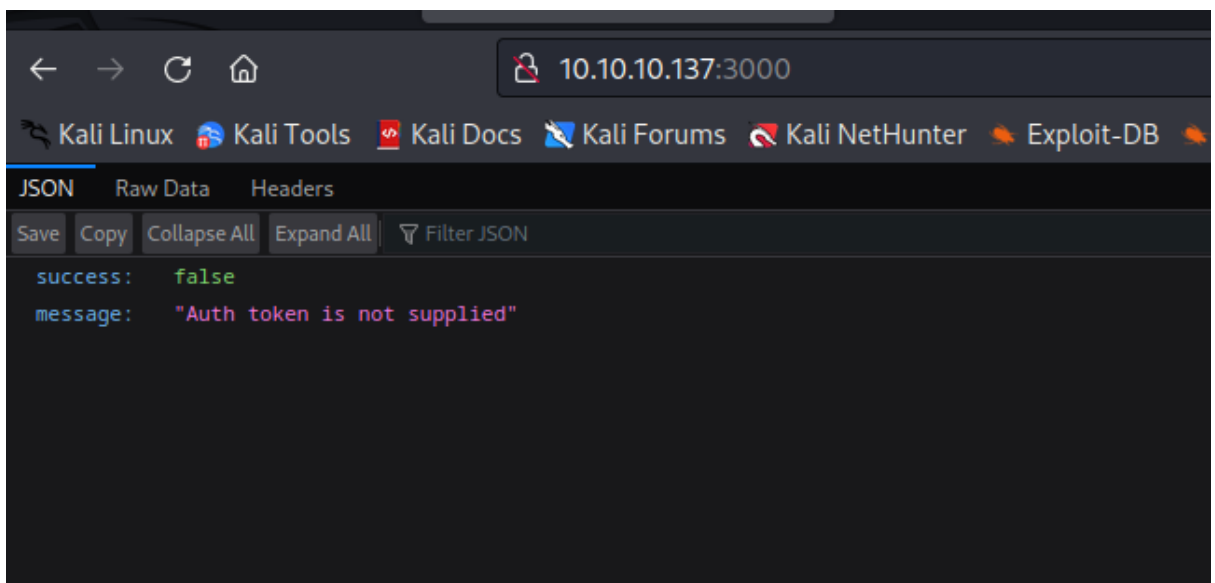
80/HTTP



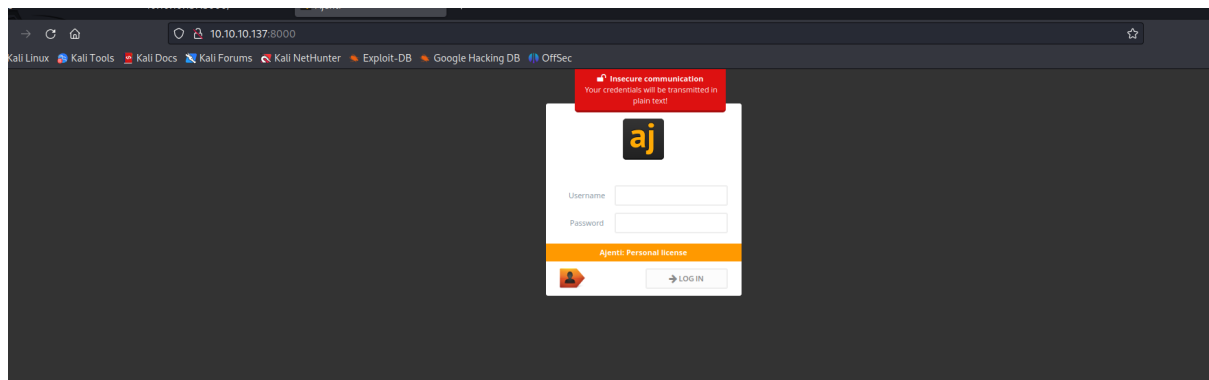
About this page

This is the beginning of our website

3000/HTTP



8000/HTTP



After initial inspection of the web applications, we launched dirb on the port 80/HTTP what discovered two directories /config.php and /management

```
# dirb http://10.10.10.137 -X .php

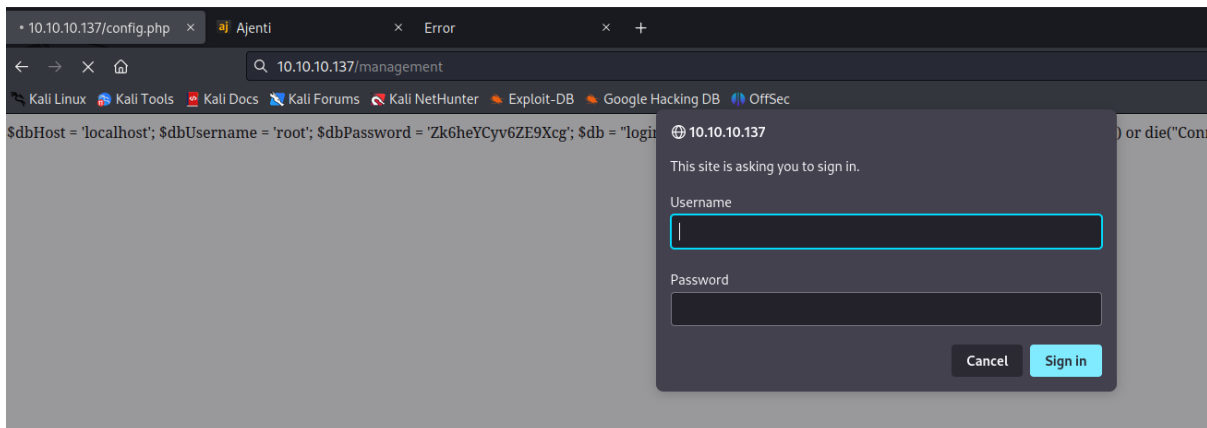
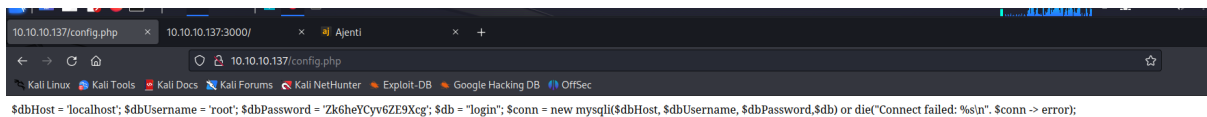
DIRB v2.22
By The Dark Raver

START_TIME: Thu Aug 10 19:10:38 2023
URL_BASE: http://10.10.10.137/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

GENERATED WORDS: 4628

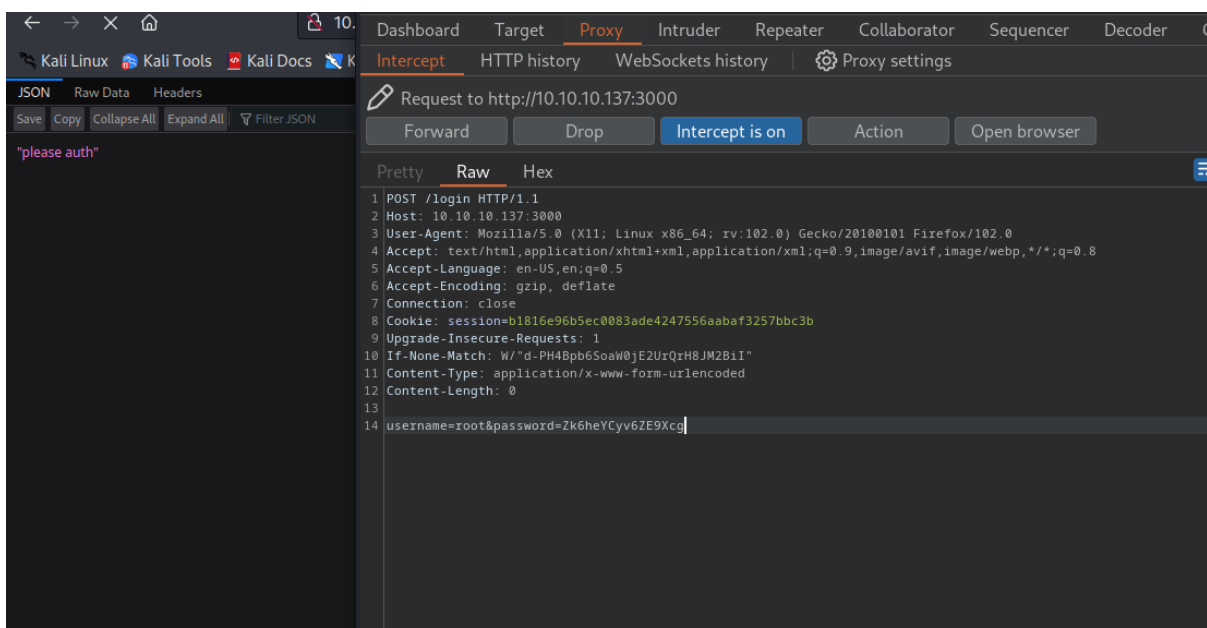
— Scanning URL: http://10.10.10.137/ —
+ http://10.10.10.137/config.php (CODE:200|SIZE:202)
```

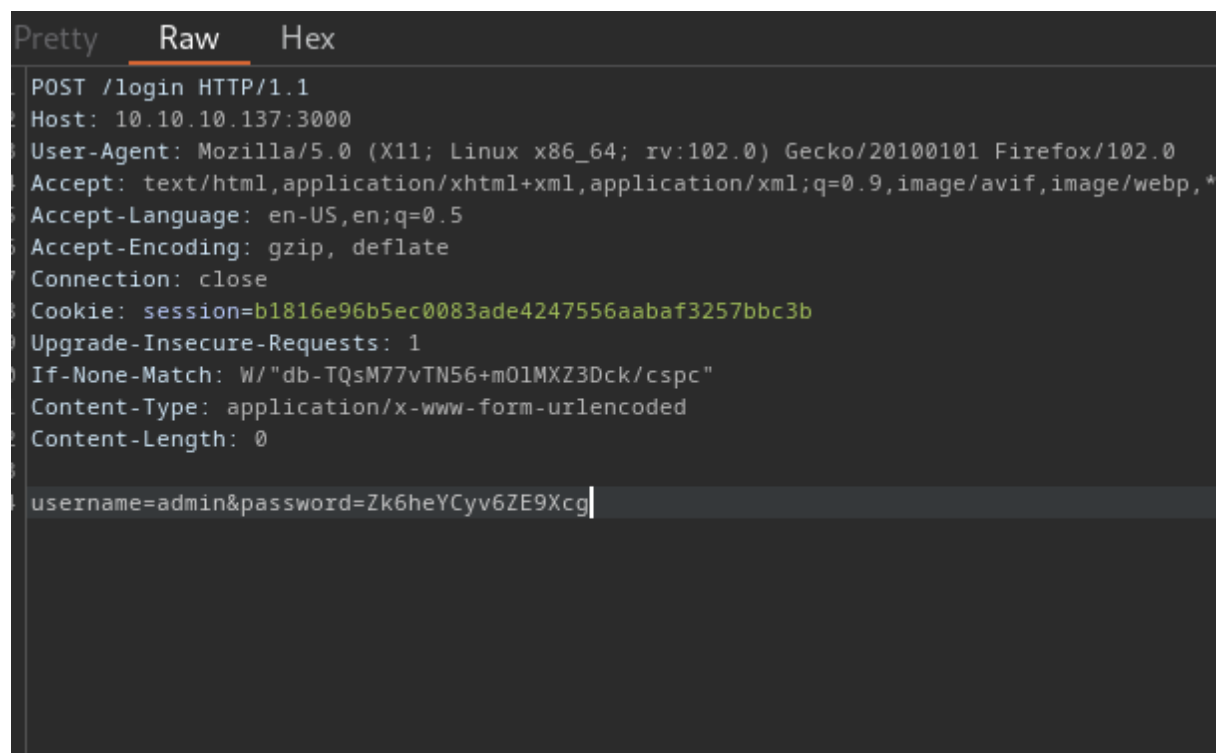
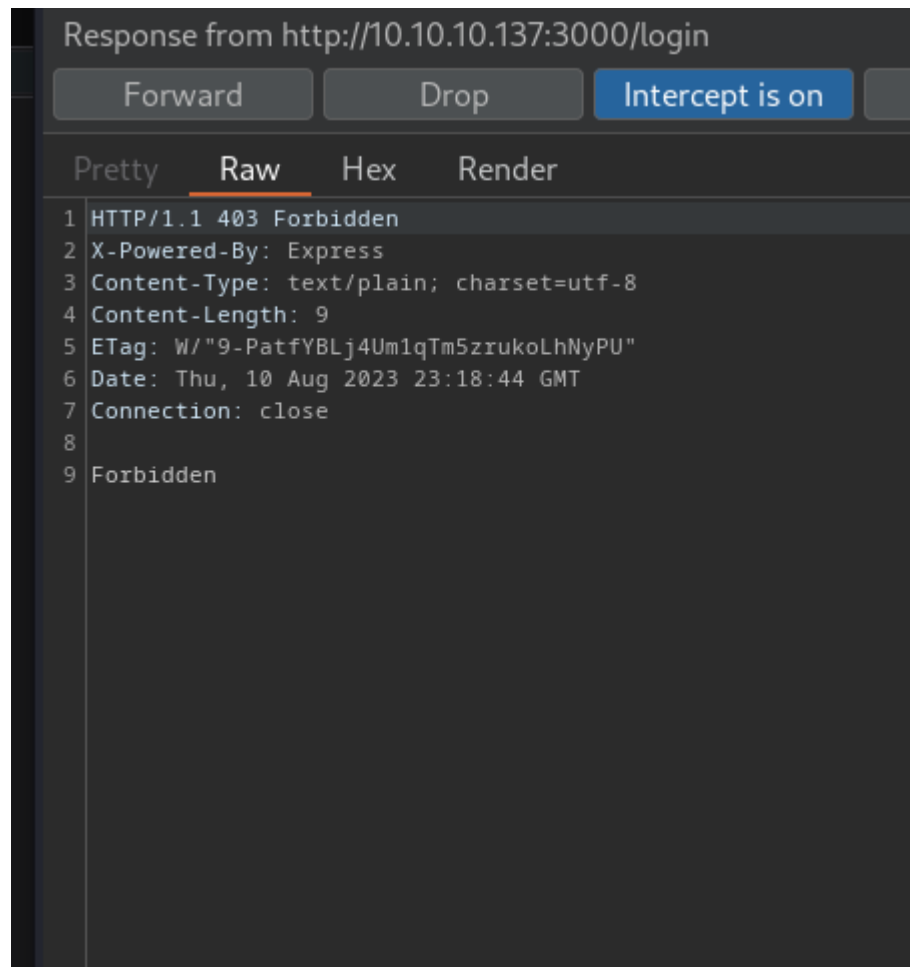
/config.php gave as set of credentials, yet we couldn't use them to login to the /management

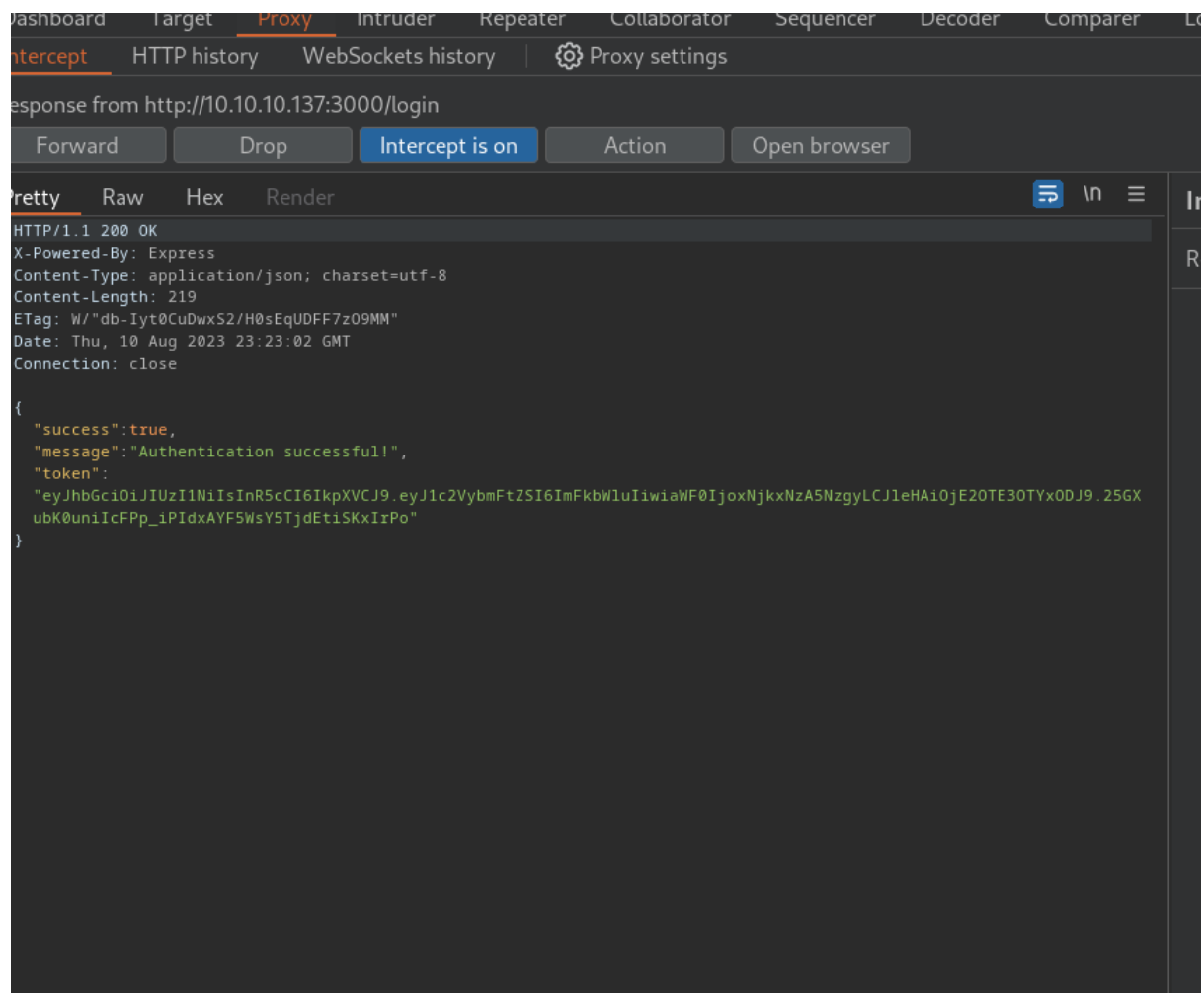


That's why we moved to the port 3000/HTTP

Accessing this port immediately informed us about failed authentication, so we supplied credentials that we got from /config.php files and as result we got JWT token



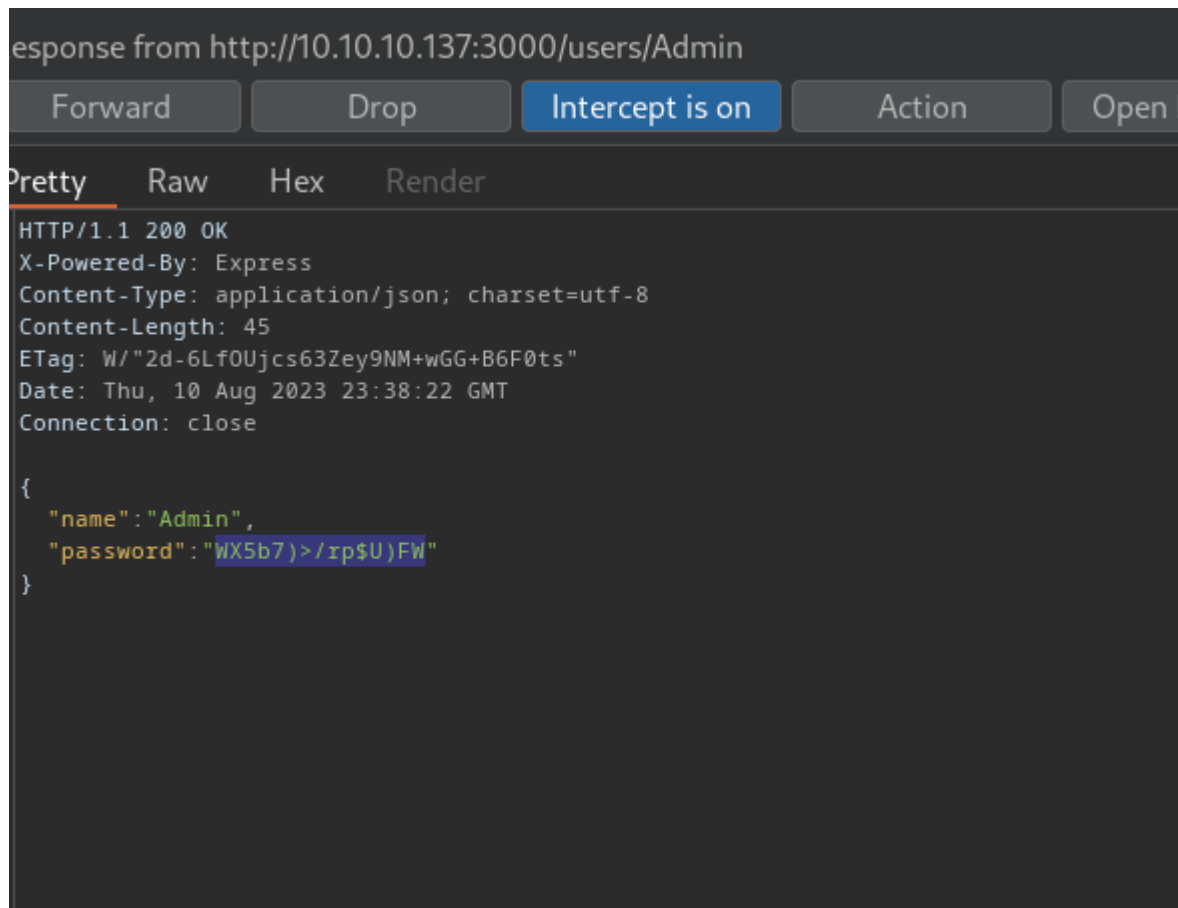




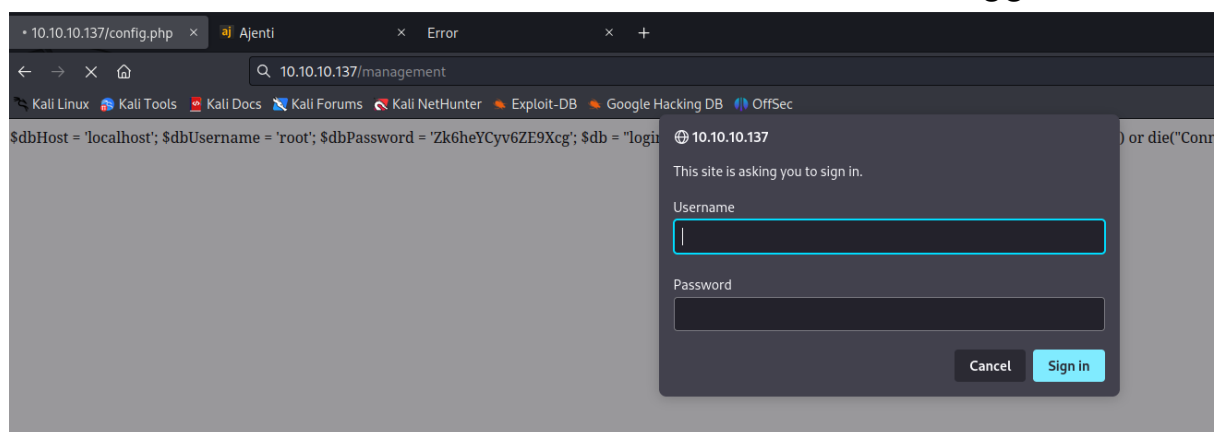
We added this token to the header and then access /user directory what listed all the users

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 181
5 ETag: W/"b5-cGsywmWiRpCno11EZqocljZF8A8"
6 Date: Thu, 10 Aug 2023 23:28:33 GMT
7 Connection: close
8
9 [
10   {
11     "ID": "1",
12     "name": "Admin",
13     "Role": "Superuser"
14   },
15   {
16     "ID": "2",
17     "name": "Derry",
18     "Role": "Web Admin"
19   },
20   {
21     "ID": "3",
22     "name": "Yuri",
23     "Role": "Beta Tester"
24   },
25   {
26     "ID": "4",
27     "name": "Dory",
28     "Role": "Supporter"
29   }
30 ]
```

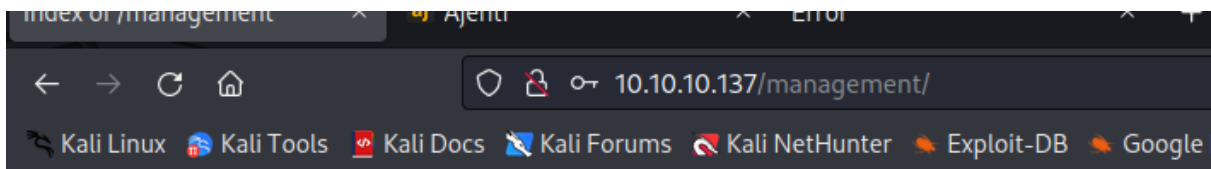
Then we accessed each of the users to get their credentials



After extracting credentials for all the users, we returned to the port 80/HTTP and tried to login to the /management with the newly obtained credentials, and this time it worked - we are logged in

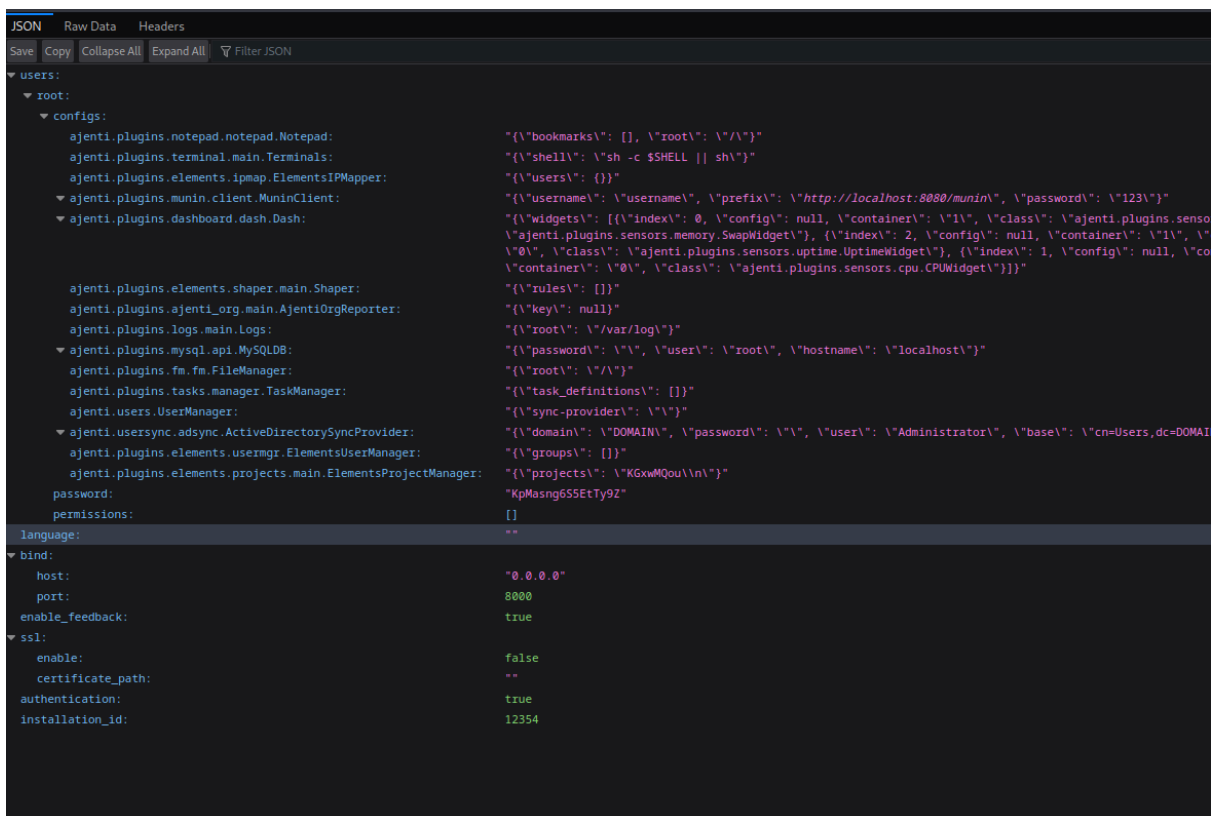


Inside we found another set of credentials

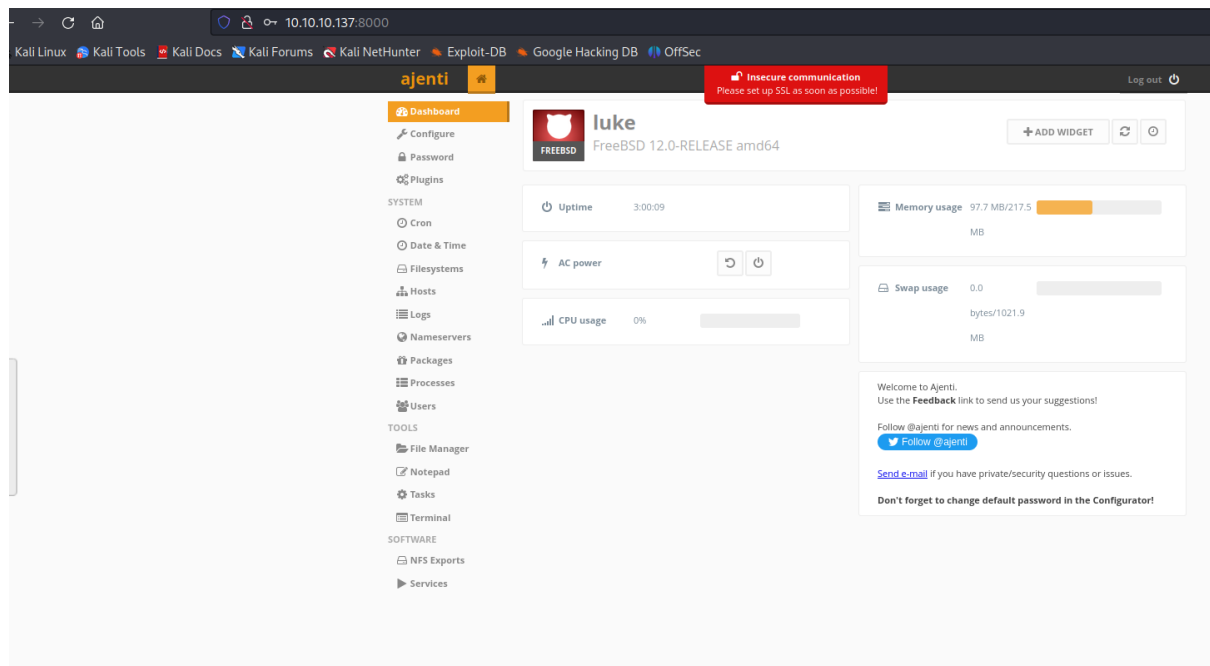


Index of /management

- [Parent Directory](#)
- [config.json](#)
- [config.php](#)
- [login.php](#)



We used those credentials to login to the Ajenti running on the port 8000/HTTP



After login as an administrator user to the Ajenti we created our own terminal what gave us a remote code execution as a root user

Bad -c option

whoami

root

ls -al

total 89217

drwxr-xr-x	20	root	wheel	512	Aug 10 21:46	.
drwxr-xr-x	20	root	wheel	512	Aug 10 21:46	..
-rw-r--r--	2	root	wheel	951	Dec 7 2018	.cshrc
-rw-r--r--	2	root	wheel	470	Dec 7 2018	.profile
drwxrwxr-x	2	root	operator	512	Mar 30 2019	.snap
-r-----	1	root	wheel	33554432	Mar 30 2019	.sujournal
-r--r--r--	1	root	wheel	6177	Dec 7 2018	COPYRIGHT
drwxr-xr-x	2	root	wheel	1024	Apr 26 2021	bin
drwxr-xr-x	9	root	wheel	1536	Nov 2 2021	boot
dr-xr-xr-x	8	root	wheel	512	Aug 10 21:46	dev
-rw-----	1	root	wheel	4096	Aug 10 21:46	entropy
drwxr-xr-x	26	root	wheel	2560	Oct 1 2020	etc
lrwxr-xr-x	1	root	wheel	8	Mar 30 2019	home -> usr/home
drwxr-xr-x	4	root	wheel	1536	Dec 7 2018	lib
drwxr-xr-x	3	root	wheel	512	Mar 30 2019	libexec
drwxr-xr-x	2	root	wheel	512	Dec 7 2018	media
drwxr-xr-x	3	root	wheel	512	Apr 6 2019	mnt
drwxr-xr-x	2	root	wheel	512	Dec 7 2018	net
drwxr-xr-x	3	root	wheel	512	Apr 14 2019	nodeapp
dr-xr-xr-x	2	root	wheel	512	Dec 7 2018	proc
drwxr-xr-x	2	root	wheel	2560	Dec 7 2018	rescue
-rw-----	1	root	wheel	11954496	Oct 28 2021	restoresymtable
drwxr-xr-x	5	root	wheel	512	Nov 2 2021	root
drwxr-xr-x	2	root	wheel	2560	Dec 7 2018	sbin
lrwxr-xr-x	1	root	wheel	11	Dec 7 2018	sys -> usr/src/sys
drwxrwxrwt	7	root	wheel	512	Aug 11 00:46	tmp
drwxr-xr-x	15	root	wheel	512	Mar 30 2019	usr
drwxr-xr-x	25	root	wheel	512	Aug 11 00:46	var

_