Luke

Synopsis

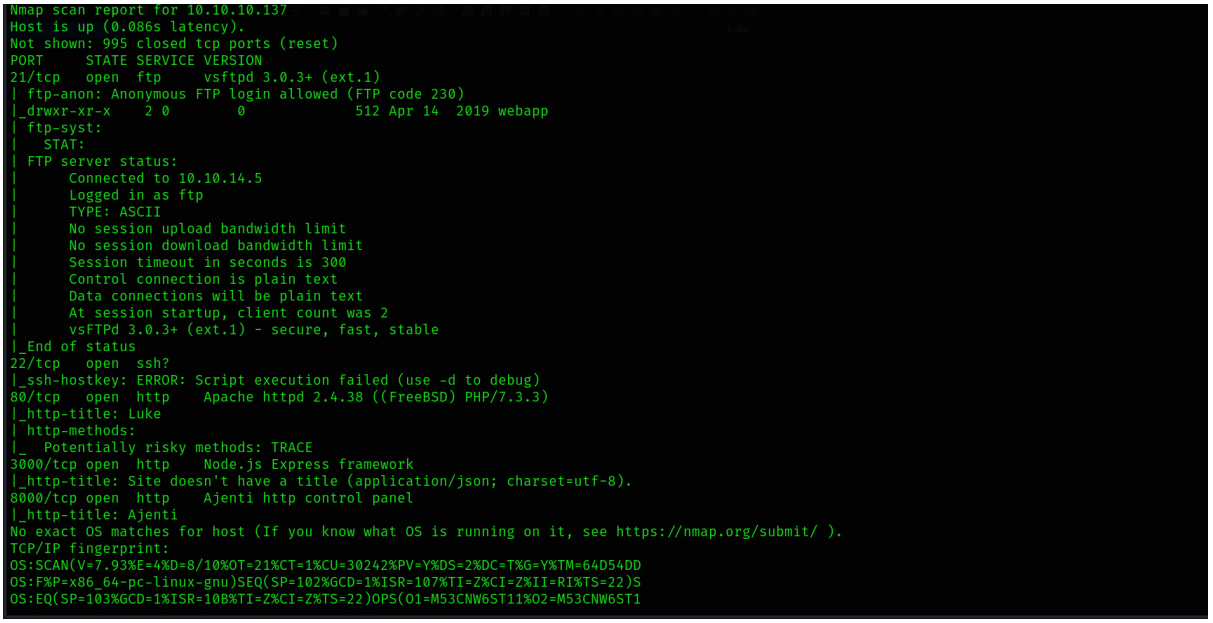
Luke is a medium difficulty Linux box featuring server enumeration and credential reuse. A configuration file leads to credential disclosure, which can be used to authenticate to a NodeJS server. The server in turn stores user credentials, and one of these provides access to a password protected folder 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

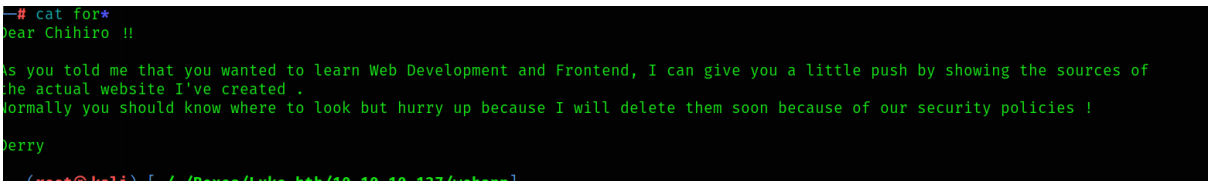
- Enumeration
- NodeJS enumeration

Exploitation

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

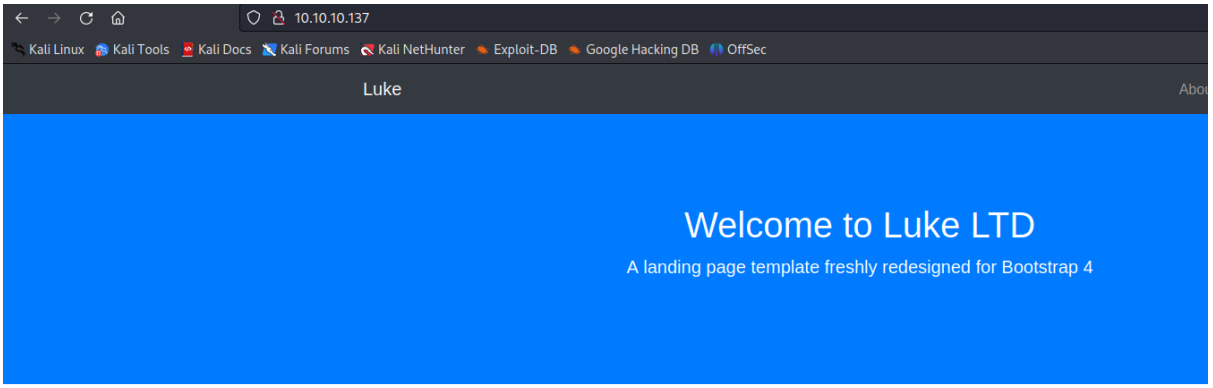


We see that FTP and 3 web ports are open
First we checked a content of FTP but we didn’t find anything interesting there

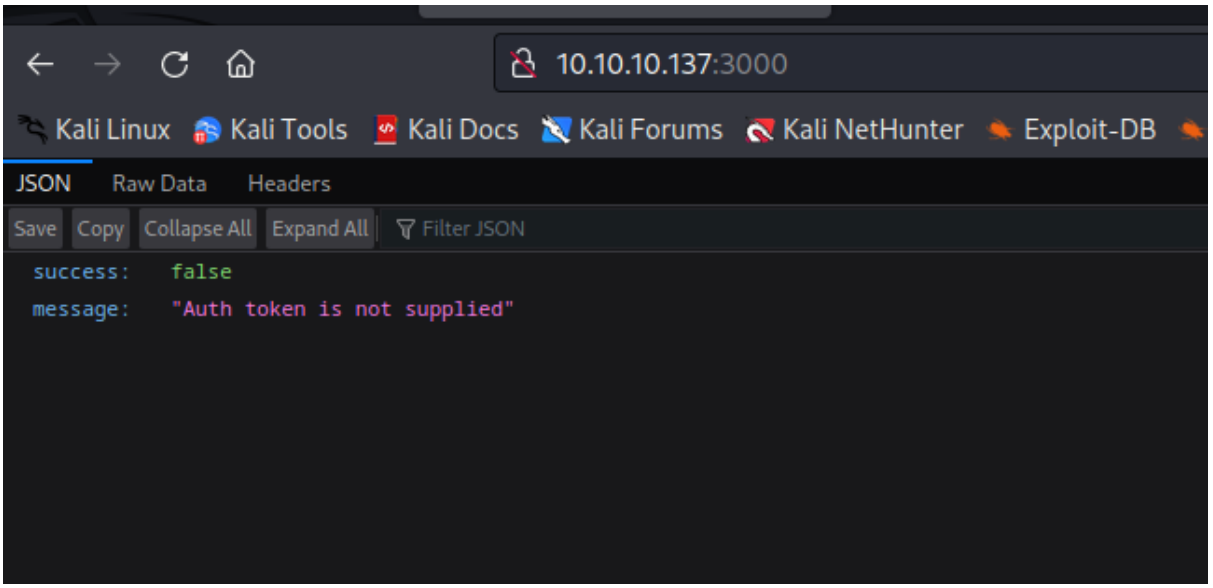


Next, we access all 3 web ports what gave us the following pages

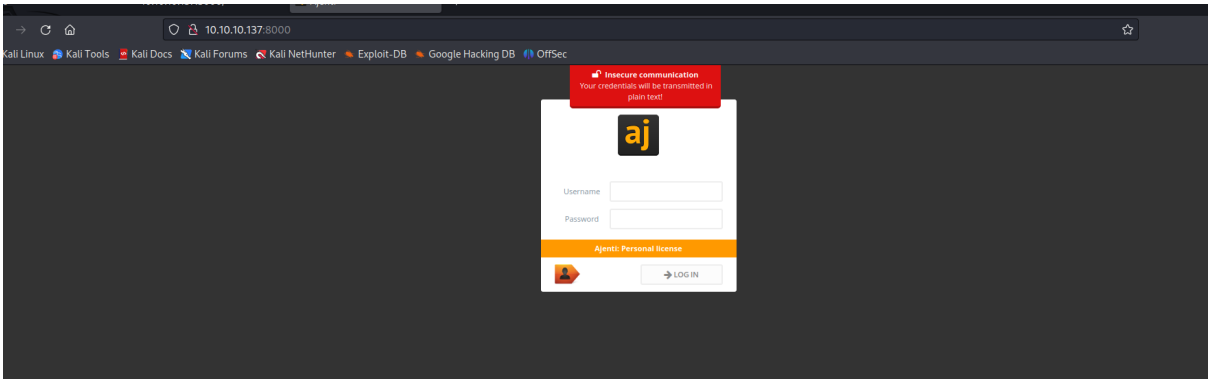
80/HTTP



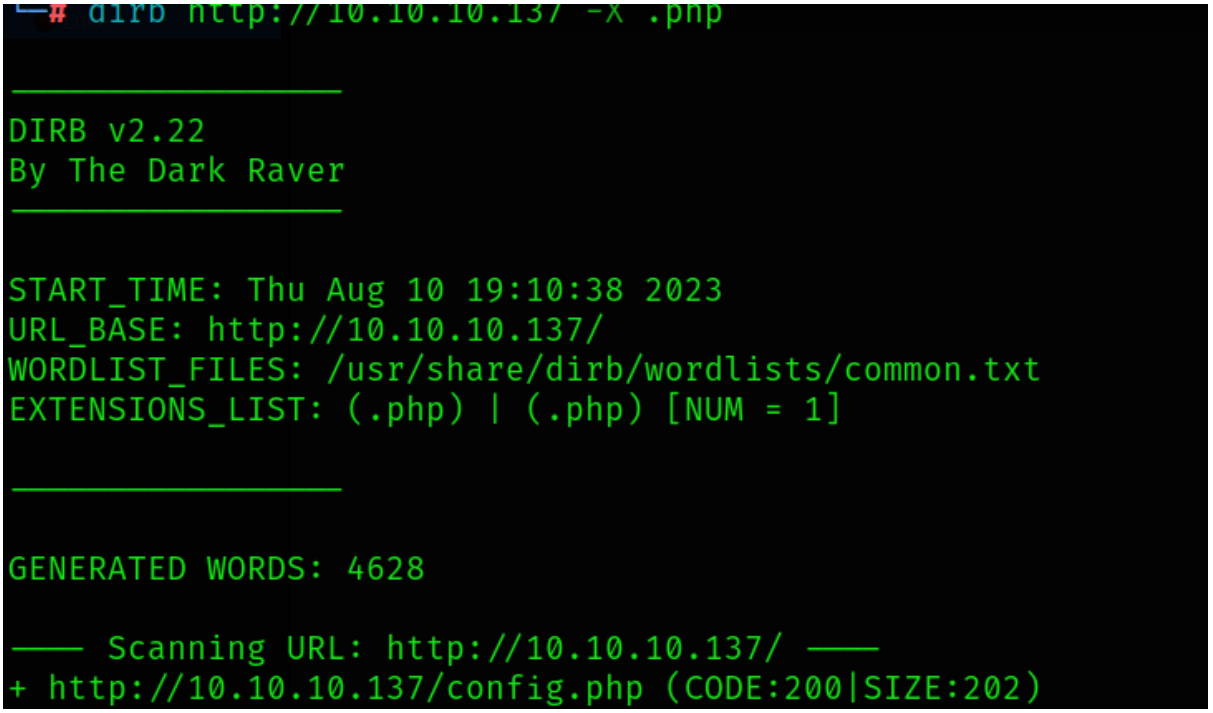
3000/HTTP



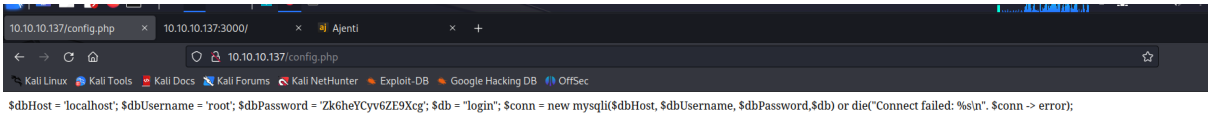
8000/HTTP

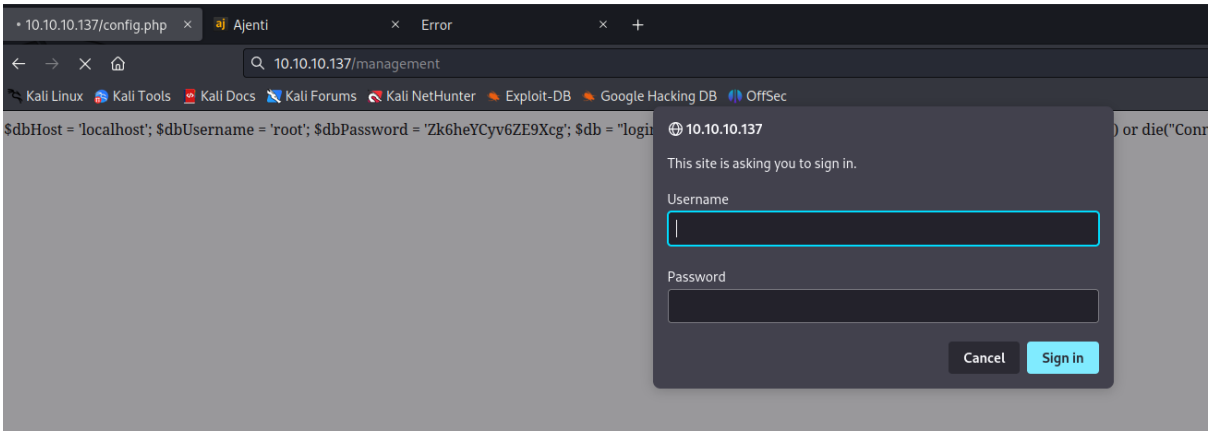


After initial inspection of the web applications, we launched dirb on the port 80/HTTP what discovered two directories /config.php and /management



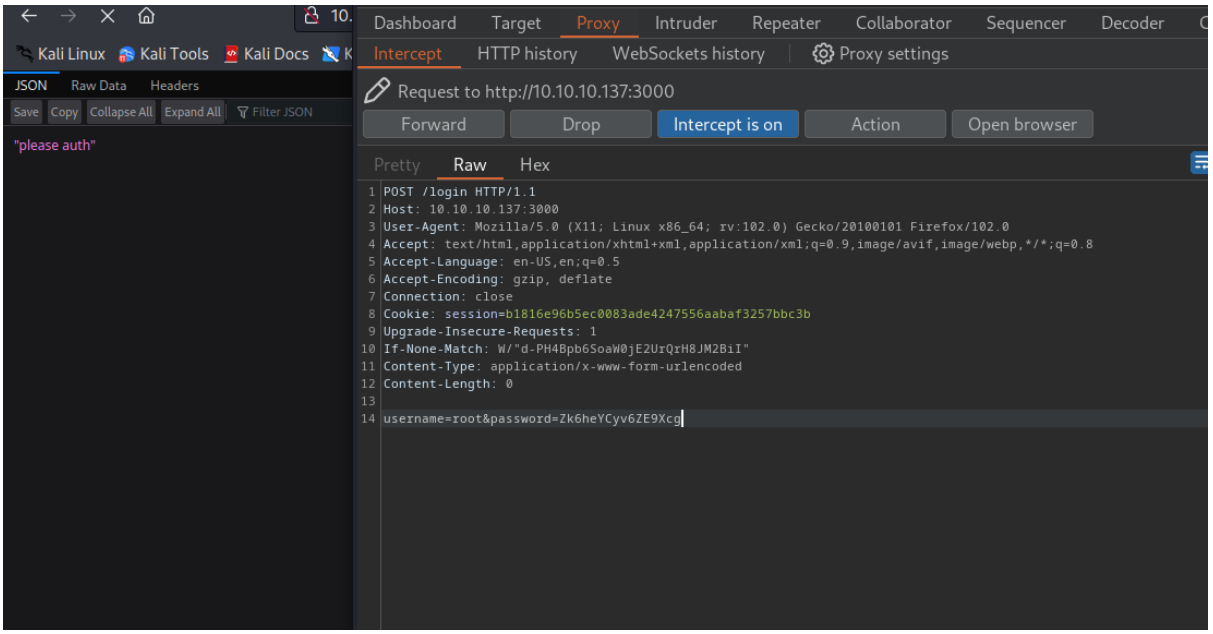
/config.php gave as set of credentials, yet we couldn't use them to login to the /management

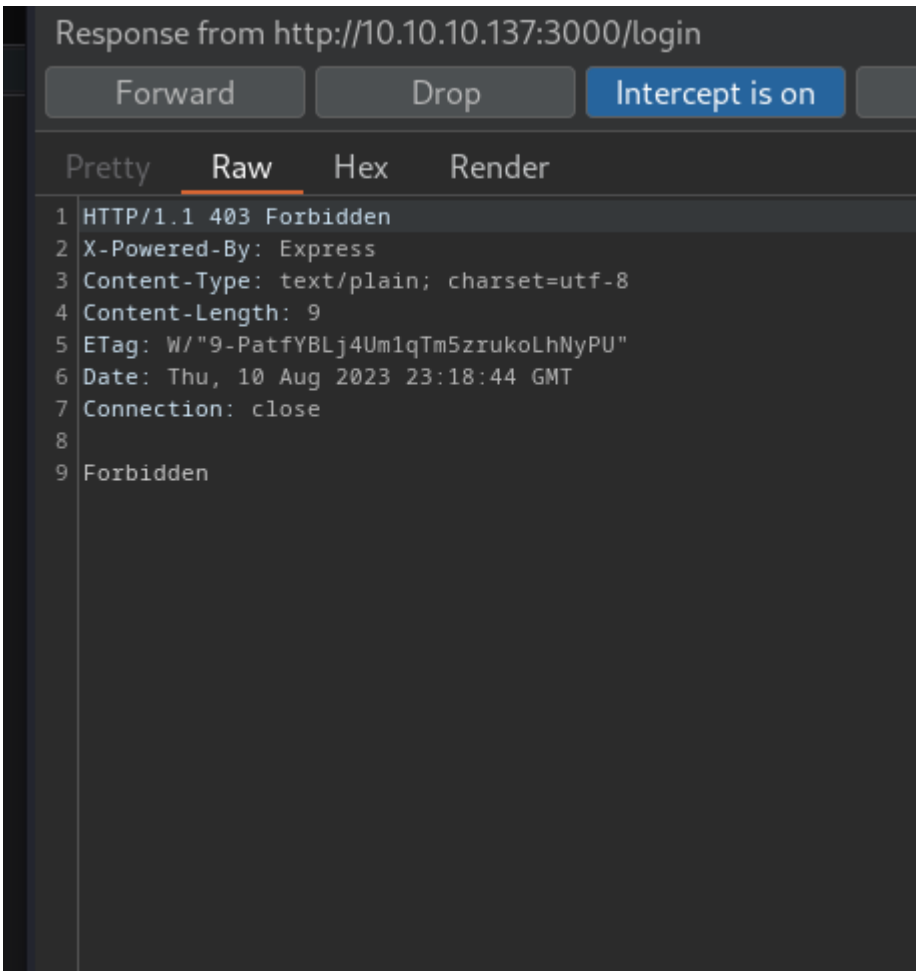


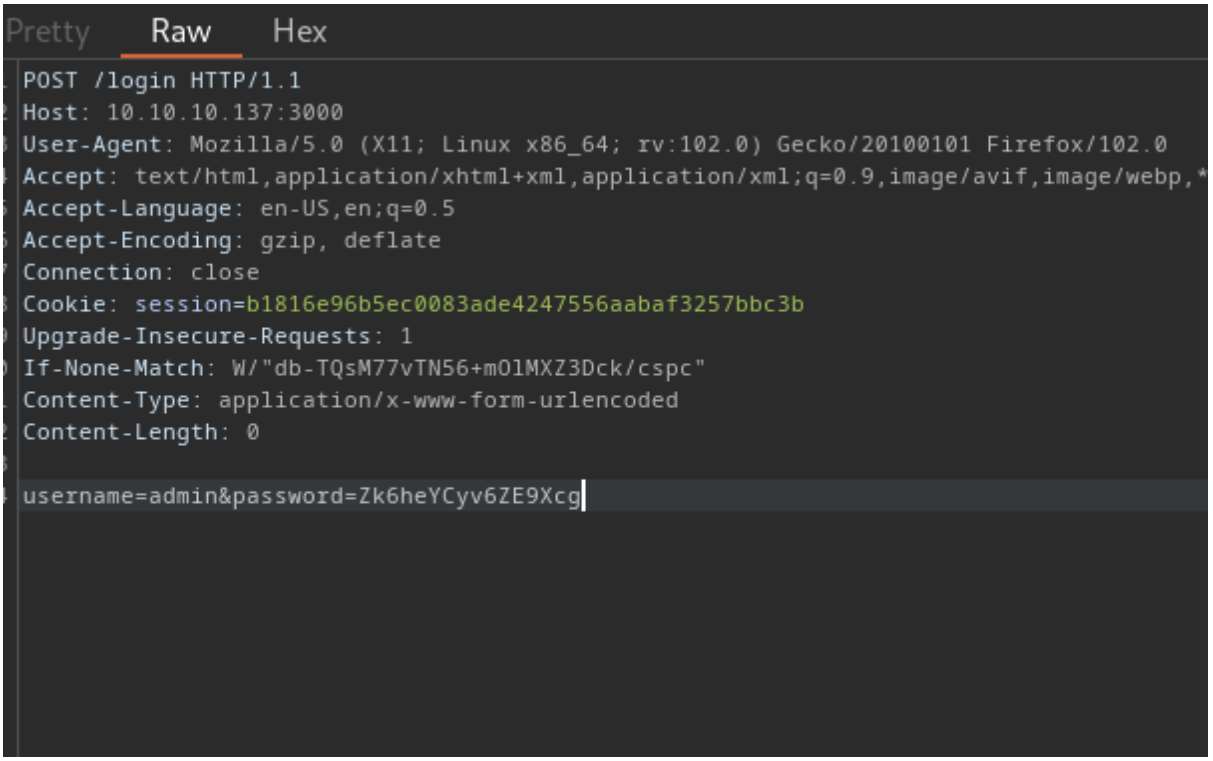


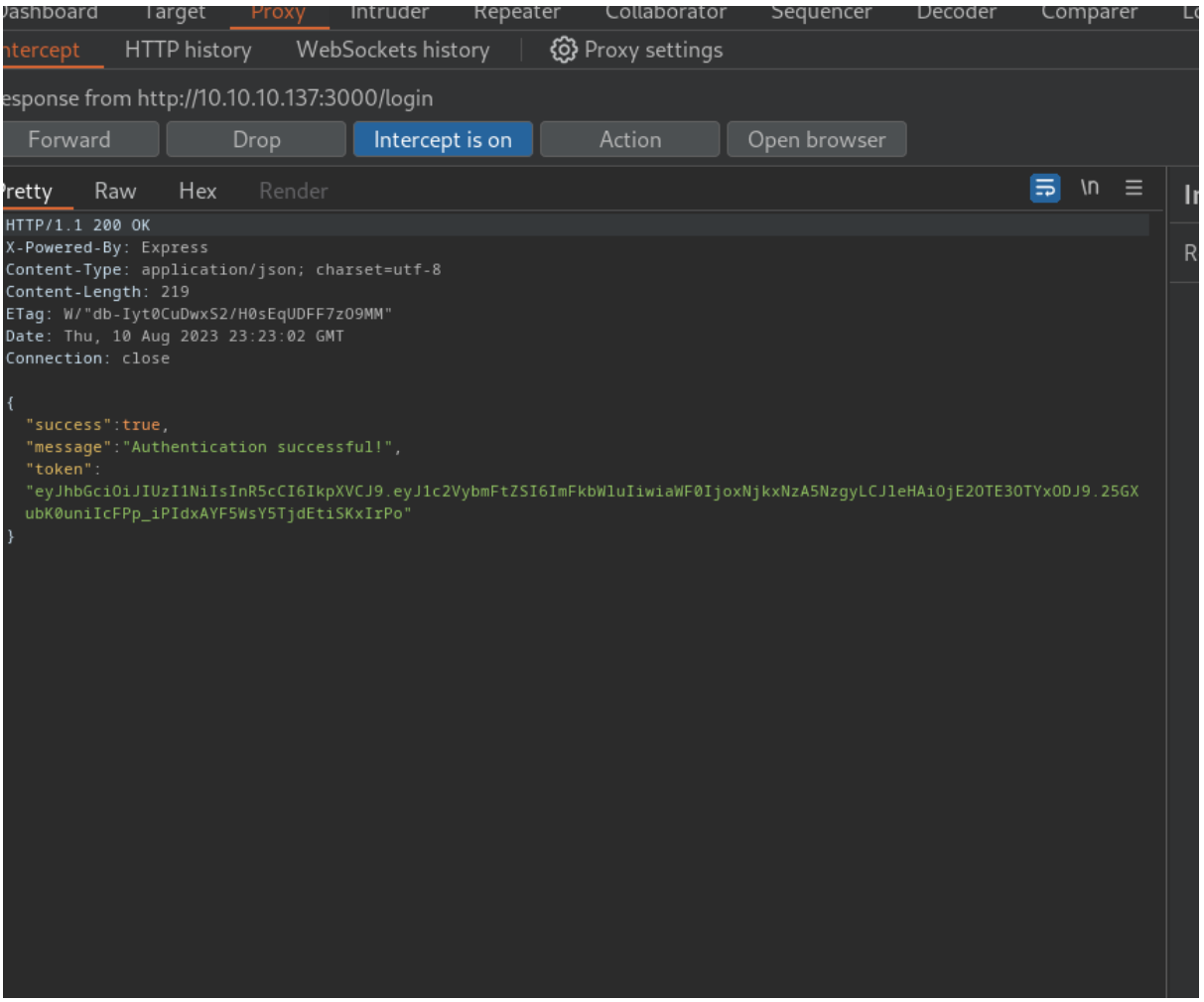
That’s why we moved to the port 3000/HTTP

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



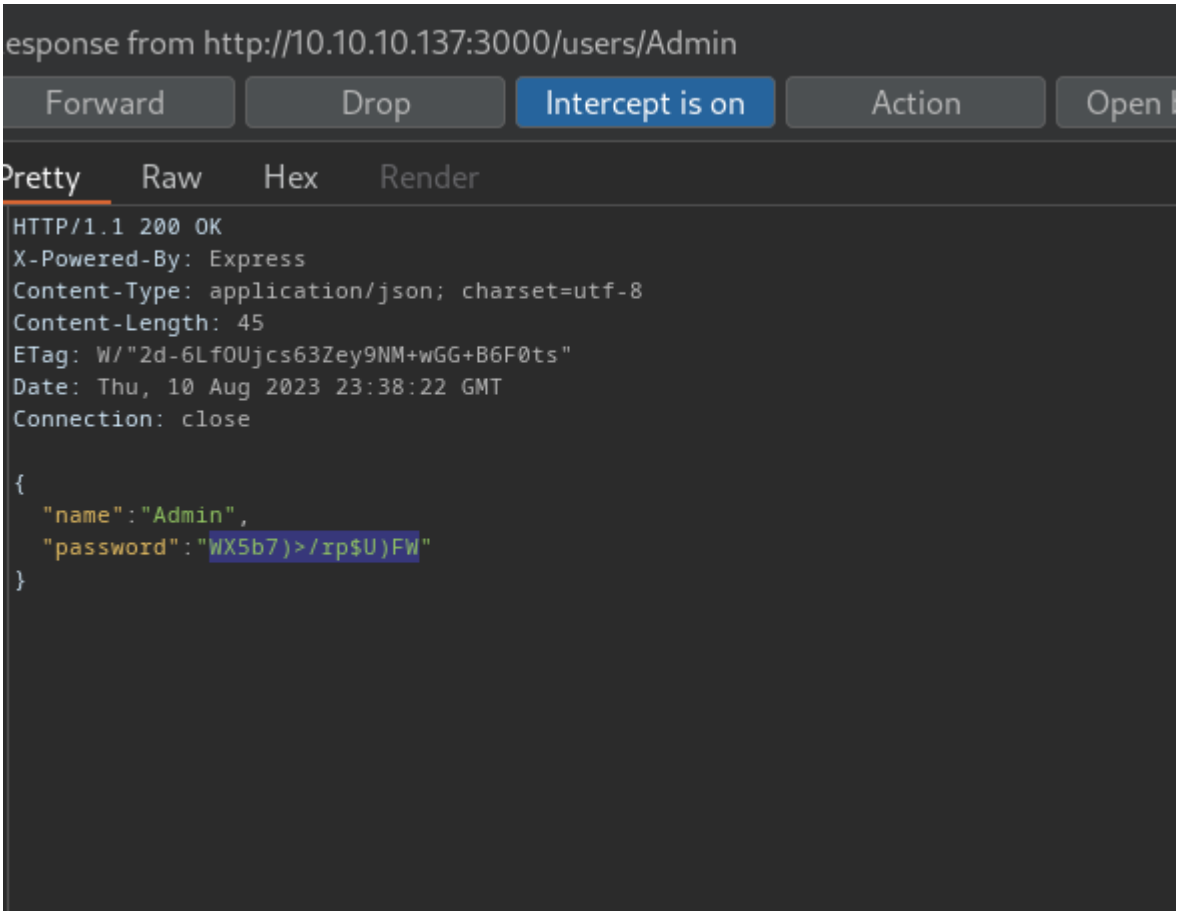

Response from http://10.10.10.137:3000/login
Forward
Drop
Intercept is on
Pretty
Raw
Hex
Render
1 HTTP/1.1 403 Forbidden
2 X-Powered-By: Express
3 Content-Type: text/plain; charset=utf-8
4 Content-Length: 9
5 ETag: W/"9-PatfYBLj4Um1qTm5zrukoLhNyPU"
6 Date: Thu, 10 Aug 2023 23:18:44 GMT
7 Connection: close
8
9 Forbidden


Pretty
Raw
Hex
POST /login HTTP/1.1
Host: 10.10.10.137:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: session=b1816e96b5ec0083ade4247556aabaf3257bbc3b
Upgrade-Insecure-Requests: 1
If-None-Match: W/"db-TQsM77vTN56+mOlMXZ3Dck/cspc"
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
username=admin&password=Zk6heYCyv6ZE9Xcg

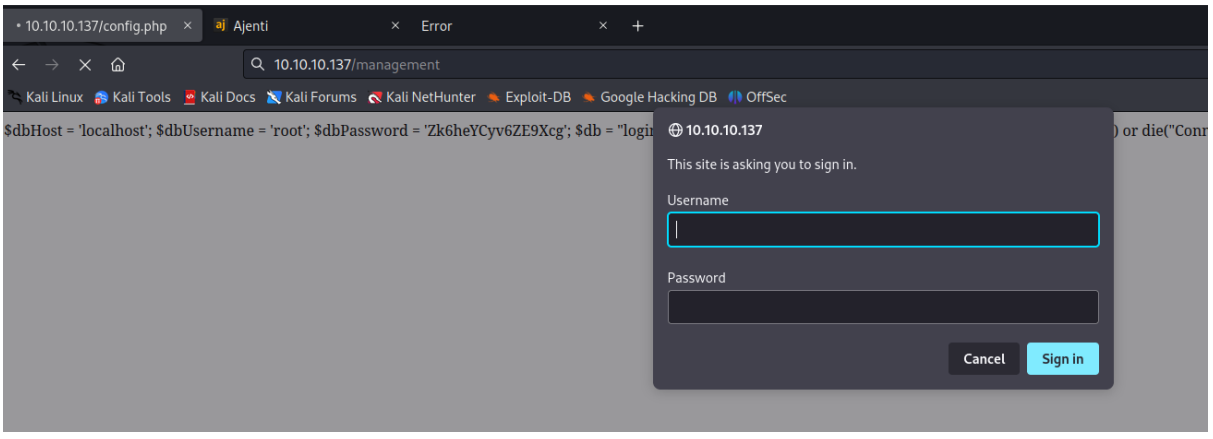


We added this token to the header and then access /user directory what listed all the users

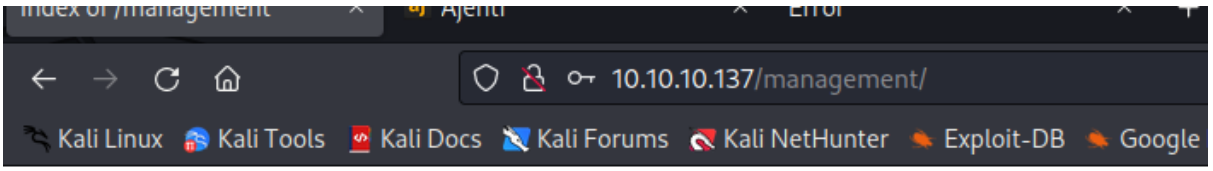
Then we accessed each of the users to get their credentials



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

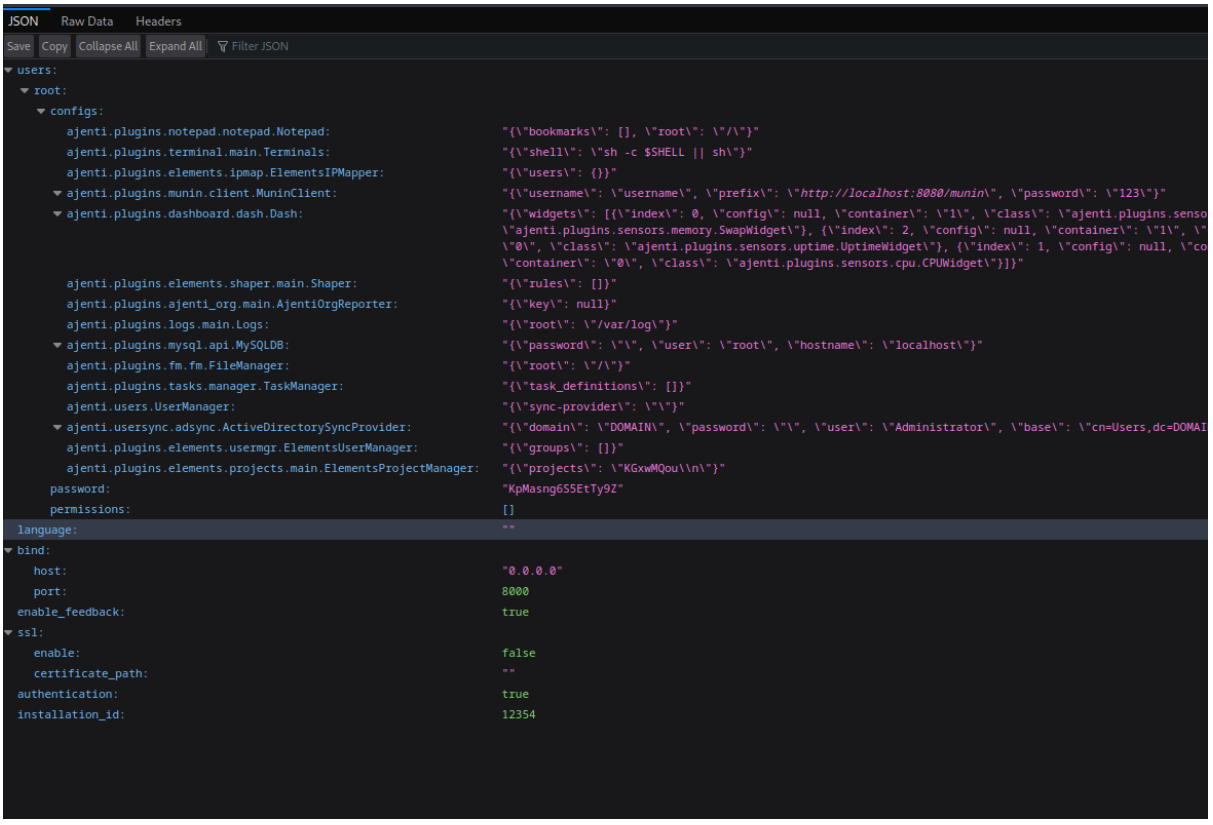


Inside we found another set of credentials

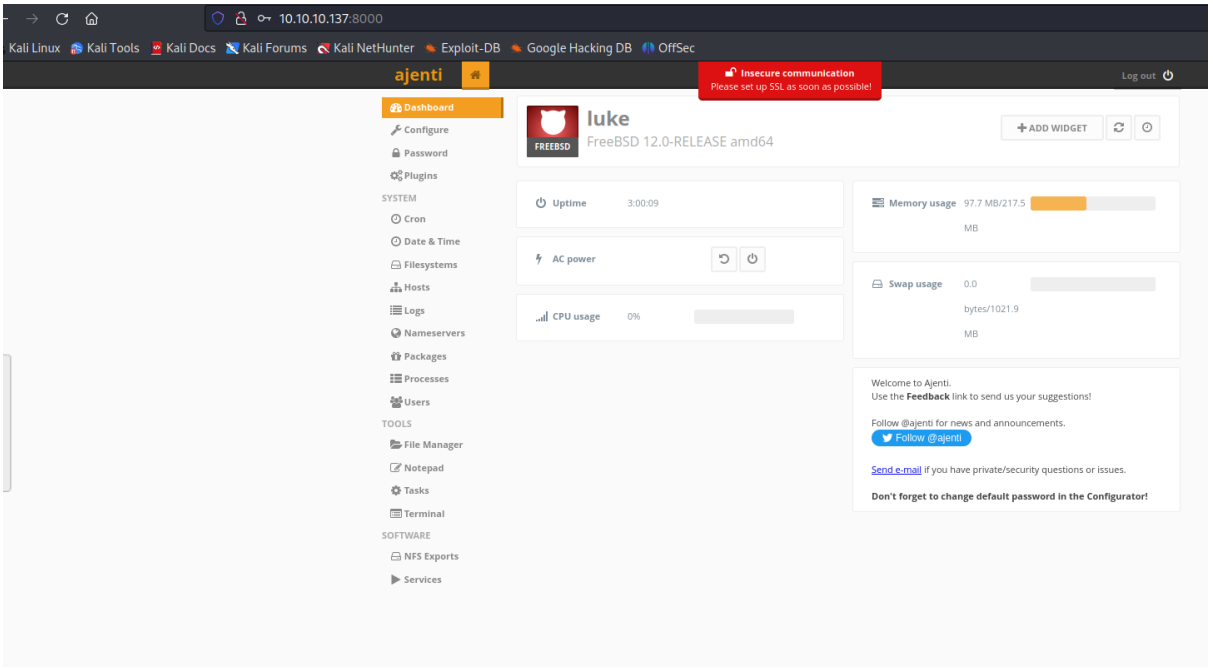


Index of /management

- 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
# _
```