Ganofins Blog

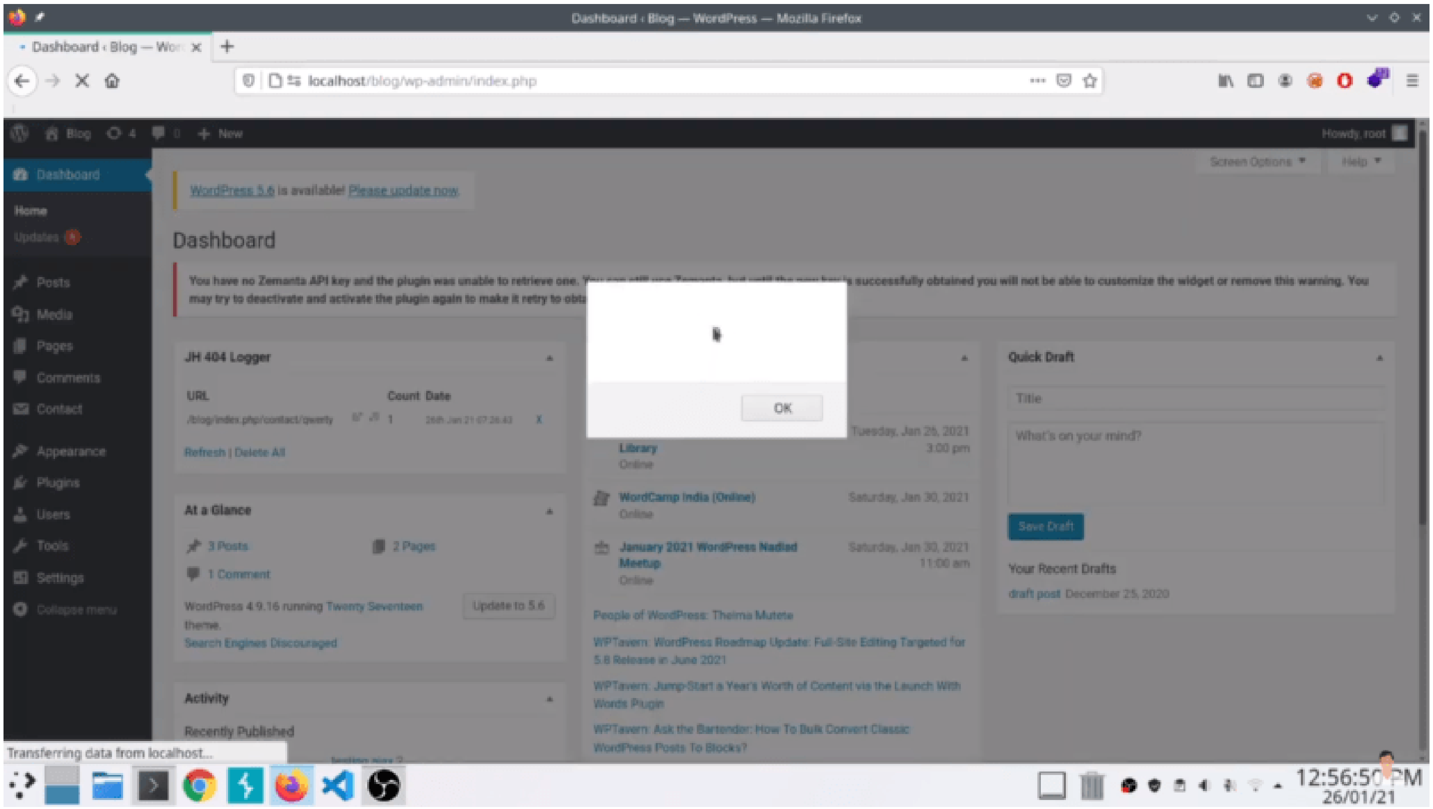
Learn Today Apply Today

Home › My First CVE-2021-24176

WRITEUPS

My First CVE-2021-24176

2 YEARS AGO   READ TIME: 2 MINUTES   BY GANOFINS   LEAVE A COMMENT



WordPress 5.6 is available! Please update now.

Dashboard

You have no Zemanta API key and the plugin was unable to retrieve one. You can still use Zemanta, but until the new key is successfully obtained you will not be able to customize the widget or remove this warning. You may try to deactivate and activate the plugin again to make it retry to obta[in]

JH 404 Logger

URL	Count	Date	
/blog/index.php/contact/qwerty	1	26th Jan 21 07:26:43	X

Refresh | Delete All

At a Glance

3 Posts   2 Pages   1 Comment

WordPress 4.9.16 running Twenty Seventeen theme.

Search Engines Discouraged

Activity

Recently Published

Library — Online — Tuesday, Jan 26, 2021 3:00 pm

WordCamp India (Online) — Online — Saturday, Jan 30, 2021

January 2021 WordPress Nadiad Meetup — Online — Saturday, Jan 30, 2021 11:00 am

People of WordPress: Thelma Mutete

WPTavern: WordPress Roadmap Update: Full-Site Editing Targeted for 5.8 Release in June 2021

WPTavern: Jump-Start a Year's Worth of Content via the Launch With Words Plugin

WPTavern: Ask the Bartender: How To Bulk Convert Classic WordPress Posts To Blocks?

Quick Draft

Title

What's on your mind?

Your Recent Drafts

draft post December 25, 2020

Hello everyone,

A while back, when I was hunting on a private program on HackerOne. Let's call it **redacted.com**. I saw it was using WordPress CMS at **redacted.com/blog/**

I performed ffuf scan with my custom WordPress plugin wordlist and found some interesting plugins. One of which was JH 404 Logger plugin. Being a PHP enthusiast, I quickly downloaded WordPress and extracted it to my Apache httpd server directory, and started the server. Then I installed the JH 404 Logger plugin on it.

Then I checked what it really does and what are its functionalities. It is a simple plugin to record the visits at 404 URLs with their paths and counts and displays that on the WordPress dashboard but the catch is, it doesn't sanitize the path of 404 URL which I found by reviewing the source code of the plugin.
So, I immediately created a 404 URL with the payload –

```
http://localhost/blog/non_existing_path'"><img src=qw.jpg onerror=alert(0)>'
```

Quickly created a report and sent it to that private program. But guess what, they marked it as Informative. Cause it wasn't in their scope. But it was never mentioned in their scope that redacted.com/blog is not in scope. They only mentioned blog.redacted.com is not in-scope in their policy.
I tried explaining even though redacted.com/blog is not in scope, but still, this vulnerability impacts the main domain **redacted.com** which is in-scope. As because of this vulnerability in this plugin an attacker can perform stored XSS and they weren't even using ***httponly*** flag on their auth cookie. It can allow an attacker to steal the victim's cookie or execute any arbitrary Javascript code. But they kept denying this and never accepted it and guess what they are still using this plugin at **redacted.com/blog**

Moving ahead then I thought to report it to the developer of this plugin. But he never responded back to me even after several tries. So then, I reported it to the WordPress team but they said due to a high number of reports every day I won't receive any further communication regarding this. Then I reported this vulnerability to wpscan and in no time they verified and assigned a CVE id CVE-2021-24176 to it.

That's how I got my first CVE.

CVE-2021-24176 POC

Thanks for reading 🙂
Lemme know in the comments if you're interesting to know how I got my 2nd CVE id.

ϟ cve ϟ cve-2021-24176 ϟ ganofins ϟ ganofins cve ϟ ganofins exploits ϟ ganofins writeups

PREV POST

CVE-2019-15739

NEXT POST

Story of 6 failed OAuth bugs

ganofins

Related Posts

Story of 6 failed OAuth bugs

1 YEAR AGO

Leave a Reply

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

Comment

Name *

Email *

Website

Post Comment

Type Keywords & Hit Enter

SUBSCRIBE TO OUR NEWSLETTER

Name*

Email*

Subscribe

RECENT POSTS

Story of 6 failed OAuth bugs

My First CVE-2021-24176

CVE-2019-15739

I wrote a Python module Proxy Extractor

How to change the YouTube app view subscriber count settings back to 100k or 10m instead of lakh or crore?

MENU

- Home
- How To Tutorials
- Language
  - JavaScript
  - PHP
  - Python
- Exploits
  - CVE
- Writeups