List of vulnerable wordpress plugins. Hacked, dangerous, vulnerable

Author : admin

**Have your wordpress has been hacked recently? Mine has Don't despair, below is a list of famous Wordpress Plugins for its hackability.
Hope this helps you prevent your self on time and wipe out all the unnecessery plugins.
Double check the version number of Vulnerable plugins, and remove it only when you're sure its hackable. If you're sure you happen to run on your Wordpress Blog or site one of the below plugins immediately deactivate and delete it.**

Vulnerability types

A quick reminder of the most common security holes and issues WordPress plugins face. Please note that most problems are a combination of two or more types listed below.

Arbitrary file viewing

Instead of allowing only certain file source to be viewed (for example plugin templates) the lack of checks in the code allows the attacker to view the source of any file, including those with sensitive information such as wp-config.php

Arbitrary file upload

Lack of file type and content filtering allows for upload of arbitrary files that can contain executable code which, once run, can do pretty much anything on a site

Privilege escalation

Once the attacker has an account on the site, even if it’s only of the subscriber type, he can escalate his privileges to a higher level, including administrative ones.

SQL injection

By not escaping and filtering data that goes into SQL queries, malicious code can be injected into queries and data deleted, updated or inserted into the database. This is one of the most common vulnerabilities.

Remote code execution (RCE)

Instead of uploading and running malicious code, the attacker can run it from a remote location. The code can do anything, from hijacking the site to completely deleting it.

Plugin Name	Vulnerability Type	Min / Max Versions Affected
1 Flash Gallery	**arbitrary file upload**	**1.3.0 / 1.5.6**
360 Product Rotation	**arbitrary file upload**	**1.1.3 / 1.2.0**
Tevolution	**arbitrary file upload**	**2.0 / 2.2.9**
Addblockblocker	**arbitrary file upload**	**0.0.1**
Ads Widget	**remote code execution (RCE)**	**2.0 / *n/a***
Advanced Access Manager	**privilege escalation**	**3.0.4 / 3.2.1**
Advanced Ajax Page Loader	**arbitrary file upload**	**2.5.7 / 2.7.6**
Advanced Video Embed Embed Videos Or Playlists	**arbitrary file viewing**	***n/a* / 1.0**
Analytic	**remote code execution (RCE)**	**1.8**
Analytics Counter	**PHP object injection**	**1.0.0 / 3.4.1**
Appointments	**PHP object injection**	**1.4.4 Beta / 2.2.0**
Asgaros Forum	**settings change**	**1.0.0 / 1.5.7**
Aspose Cloud Ebook Generator	**arbitrary file viewing**	**1.0**
Aspose Doc Exporter	**arbitrary file viewing**	**1.0**
Aspose Importer Exporter	**arbitrary file viewing**	**1.0**
Aspose Pdf Exporter	**arbitrary file viewing**	**1.0**
Attachment Manager	**arbitrary file upload**	**1.0.0 / 2.1.1**
Auto Attachments	**arbitrary file upload**	**0.2.7 / 0.3**
Bbpress Like Button	**SQL injection**	**1.0 / 1.5**
Bepro Listings	**arbitrary file upload**	**2.0.54 / 2.2.0020**
Blaze Slide Show For Wordpress	**arbitrary file upload**	**2.0 / 2.7**
Brandfolder	**local file inclusion (LFI)**	**2.3 / 3.0**

Breadcrumbs Ez	**remote code execution (RCE)**	***n/a***
Candidate Application Form	**arbitrary file viewing**	**1.0**
Category Grid View Gallery	**arbitrary file upload**	**0.1.0 / 0.1.1**
Cherry Plugin	**arbitrary file upload**	**1.0 / 1.2.6**
Chikuncount	**arbitrary file upload**	**1.3**
Cip4 Folder Download Widget	**arbitrary file viewing**	**1.4 / 1.10**
Cms Commander Client	**PHP object injection**	**2.02 / 2.21**
Contus Video Gallery	**arbitrary file viewing**	**2.2 / 2.3**
Cookie Eu	**remote code execution (RCE)**	**1.0**
Cp Image Store	**arbitrary file viewing**	**1.0.1 / 1.0.5**
Cross Rss	**arbitrary file viewing**	**0.5**
Custom Content Type Manager	**remote code execution**	**0.9.8.8**
Custom Lightbox	**possible remote code execution (RCE)**	**0.24**
Cysteme Finder	**arbitrary file viewing**	**1.1 / 1.3**
Db Backup	**arbitrary file viewing**	**1.0 / 4.5**
Delete All Comments	**arbitrary file upload**	**2.0**
Developer Tools	**arbitrary file upload**	**1.0.0 / 1.1.4**
Disclosure Policy Plugin	**remote file inclusion (RFI)**	**1.0**
Display Widgets	**remote code execution**	**2.6**
Dop Slider	**arbitrary file upload**	**1.0**
Download Zip Attachments	**arbitrary file viewing**	**1**
Downloads Manager	**arbitrary file upload**	**1.0 Beta / 1.0 rc-1**
Dp Thumbnail	**arbitrary file upload**	**1.0**
Dropbox Backup	**PHP object injection**	**1.0 / 1.4.7.5**
Dukapress	**arbitrary file viewing**	**2.3.7 / 2.5.3**
Ebook Download	**arbitrary file viewing**	**1.1**
Ecstatic	**arbitrary file upload**	**0.90 (x9) / 0.9933**
Ecwid Shopping Cart	**PHP Object Injection**	**3.4.4 / 4.4.3**
Enable Google Analytics	**remote code execution (RCE)**	***n/a***
Estatik	**arbitrary file upload**	**1.0.0 / 2.2.5**
Event Commerce Wp Event Calendar	**persistent cross-site scripting (XSS)**	**1.0**
Filedownload	**arbitrary file viewing**	**0.1**
Flickr Gallery	**PHP object injection**	**1.2 / 1.5.2**
Form Lightbox	**option update**	**1.1 / 2.1**
Formidable	**information disclosure**	**1.07.5 / 2.0.07**
Fresh Page	**arbitary file upload**	**.11 / 1.1**
Front End Upload	**arbitrary file upload**	**0.3.0 / 0.5.3**
Front File Manager	**arbitrary file upload**	**0.1**
Fs Real Estate Plugin	**SQL injection**	**1.1 / 2.06.03**
G Translate	**remote code execution (RCE)**	**1.0 / 1.3**
Gallery Objects	**SQL injection**	**0.2 / 0.4**
Gallery Slider	**remote code execution (RCE)**	**2.0 / 2.1**
Genesis Simple Defaults	**arbitrary file upload**	**1.0.0**
Gi Media Library	**arbitrary file viewing**	**1.0.300 / 2.2.2**

Google Analytics Analyze	**remote code execution (RCE)**	**1.0**
Google Document Embedder	**SQL injection**	**2.5 / 2.5.16**
Google Maps By Daniel Martyn	**remote code exection (RCE)**	**1.0**
Google Mp3 Audio Player	**arbitrary file viewing**	**1.0.9 / 1.0.11**
Grapefile	**arbitrary file upload**	**1.0 / 1.1**
Gravityforms	**reflected cross-site scripting (XSS)**	**1.7 / 1.9.15.11**
Hb Audio Gallery Lite	**arbitrary file viewing**	**1.0.0**
History Collection	**arbitrary file viewing**	**1.1. / 1.1.1**
Html5avmanager	**arbitrary file upload**	**0.1.0 / 0.2.7**
I Dump Iphone To Wordpress Photo Uploader	**arbitrary file upload**	**1.1.3 / 1.8**
Ibs Mappro	**arbitrary file viewing**	**0.1 / 0.6**
Image Export	**arbitrary file viewing**	**1.0.0 / 1.1.0**
Image Symlinks	**arbitrary file upload**	**0.5 / 0.8.2**
Imdb Widget	**arbitrary file viewing**	**1.0.1 / 1.0.8**
Inboundio Marketing	**arbitrary file upload**	**1.0.0 / 2.0**
Infusionsoft	**arbitrary file upload**	**1.5.3 / 1.5.10**
Inpost Gallery	**local file inclusion (LFI)**	**2.0.9 / 2.1.2**
Invit0r	**arbitrary file upload**	**0.2 / 0.22**
Is Human	**remote code execution**	**1.3.3 / 1.4.2**
Iwp Client	**PHP object injection**	**0.1.4 / 1.6.0**
Jssor Slider	**arbitrary file upload**	**1.0 / 1.3**
Like Dislike Counter For Posts Pages And Comments	**SQL injection**	**1.0 / 1.2.3**
Mac Dock Gallery	**arbitrary file upload**	**1.0 / 2.7**
Magic Fields	**arbitrary file upload**	**1.5 / 1.5.5**
Mailchimp Integration	**remote code execution (RCE)**	**1.0.1 / 1.1**
Mailpress	**local file inclusion (LFI)**	**5.2 / 5.4.6**
Mdc Youtube Downloader	**arbitrary file viewing**	**2.1.0**
Menu Image	**malicious JavaScript loading**	**2.6.5 / 2.6.9**
Miwoftp	**arbitrary file viewing**	**1.0.0 / 1.0.4**
Mm Forms Community	**arbitrary file upload**	**1.0 / 2.2.6**
Mobile App Builder By Wappress	**arbitrary file upload**	***n/a* / 1.05**
Mobile Friendly App Builder By Easytouch	**arbitrary file upload**	**3.0**
Multi Plugin Installer	**arbitrary file viewing**	**1.0.0 / 1.1.0**
Mypixs	**local file inclusion (LFI)**	**0.3**
Nmedia User File Uploader	**arbitrary file upload**	**1.8**
Option Seo	**remote code execution (RCE)**	**1.5**
Page Google Maps	**remote code execution (RCE)**	**1.4**
Party Hall Booking Management System	**SQL injection**	**1.0 / 1.1**
Paypal Currency Converter Basic For Woocommerce	**arbitrary file viewing**	**1.0 / 1.3**

Php Analytics	**arbitrary file upload**	***n/a***
Pica Photo Gallery	**arbitrary file viewing**	**1.0**
Pitchprint	**arbitrary file upload**	**7.1 / 7.1.1**
Plugin Newsletter	**arbitrary file viewing**	**1.3 / 1.5**
Post Grid	**file deletion**	**2.0.6 / 2.0.12**
Posts In Page	**authenticated local file inclusion (LFI)**	**1.0.0 / 1.2.4**
Really Simple Guest Post	**local file inclusion (LFI)**	**1.0.1 / 1.0.6**
Recent Backups	**arbitrary file viewing**	**0.1 / 0.7**
Reflex Gallery	**arbitrary file upload**	**1.0 / 3.0**
Resume Submissions Job Postings	**arbitrary file upload**	**2.0 / 2.5.3**
Return To Top	**remote code execution (RCE)**	**1.8 / 5.0**
Revslider	**arbitrary file viewing**	**1.0 / 4.1.4**
S3bubble Amazon S3 Html 5 Video With Adverts	**arbitrary file viewing**	**0.5 / 0.7**
Sam Pro Free	**local file inclusion (LFI)**	**1.4.1.23 / 1.9.6.67**
Se Html5 Album Audio Player	**arbitrary file viewing**	**1.0.8 / 1.1.0**
Sell Downloads	**arbitrary file viewing**	**1.0.1**
Seo Keyword Page	**remote code execution (RCE)**	**2.0.5**
Seo Spy Google Wordpress Plugin	**arbitrary file upload**	**2.0 / 2.6**
Seo Watcher	**arbitrary file upload**	**1.3.2 / 1.3.3**
Sexy Contact Form	**arbitrary file upload**	**0.9.1 / 0.9.8**
Share Buttons Wp	**remote code execution (RCE)**	**1.0**
Showbiz	**arbitrary file viewing**	**1.0 / 1.5.2**
Simple Ads Manager	**information disclosure**	**2.0.73 / 2.7.101**
Simple Download Button Shortcode	**arbitrary file viewing**	**1.0**
Simple Dropbox Upload Form	**arbitrary file upload**	**1.8.6 / 1.8.8**
Simple Image Manipulator	**arbitrary file viewing**	**1.0**
Simplr Registration Form	**privilege escalation**	**2.2.0 / 2.4.3**
Site Import	**remote page inclusion**	**1.0.0 / 1.2.0**
Slide Show Pro	**arbitrary file upload**	**2.0 / 2.4**
Smart Slide Show	**arbitrary file upload**	**2.0 / 2.4**
Smart Videos	**remote code execution (RCE)**	**1.0**
Social Networking E Commerce 1	**arbitrary file upload**	**0.0.32**
Social Sharing	**possible arbitrary file upload**	**1.0**
Social Sticky Animated	**remote code execution (RCE)**	**1.0**
Spamtask	**arbitrary file upload**	**1.3 / 1.3.6**
Spicy Blogroll	**local file inclusion (LFI)**	**0.1 / 1.0.0**
Spotlightyour	**arbitrary file upload**	**1.0 / 4.5**
Stats Counter	**PHP object injection**	**1.0 / 1.2.2.5**
Stats Wp	**remote code execution**	**1.8**
Store Locator Le	**unrestricted email sending**	**2.6 / 4.2.56**

Tera Charts	reflected cross-site scripting (XSS)	0.1 / 1.0
The Viddler Wordpress Plugin	cross-site request forgery (CSRF)/cross-site scripting (XSS)	1.2.3 / 2.0.0
Thecartpress	local file inclusion (LFI)	1.1.0 / 1.1.5
Tinymce Thumbnail Gallery	arbitrary file viewing	v1.0.4 / v1.0.7
Ultimate Product Catalogue	arbitrary file upload	1.0 / 3.1.1
User Role Editor	privilege escalation	4.19 / 4.24
Web Tripwire	arbitrary file upload	0.1.2
Webapp Builder	arbitrary file upload	2.0
Website Contact Form With File Upload	arbitrary file upload	1.1 / 1.3.4
Weever Apps 20 Mobile Web Apps	arbitrary file upload	3.0.25 / 3.1.6
Woocommerce Catalog Enquiry	arbitrary file upload	2.3.3 / 3.0.0
Woocommerce Product Addon	arbitrary file upload	1.0 / 1.1
Woocommerce Products Filter	authenticated persistent cross-site scripting (XSS)	1.1.4 / 1.1.4.2
Woopra	arbitrary file upload	1.4.1 / 1.4.3.1
Wordpress File Monitor	persistent cross-site scripting (XSS)	2.0 / 2.3.3
Wp Appointment Schedule Booking System	persistent cross-site scripting (XSS)	1.0
Wp Business Intelligence Lite	arbitrary file upload	1.0 / 1.0.7
Wp Crm	arbitrary file upload	0.15 / 0.31.0
Wp Custom Page	arbitrary file viewing	0.5 / 0.5.0.1
Wp Dreamworkgallery	arbitrary file upload	2.0 / 2.3
Wp Easybooking	reflected cross-site scripting (XSS)	1.0.0 / 1.0.3
Wp Easycart	authenticated arbitrary file upload	1.1.27 / 3.0.8
Wp Ecommerce Shop Styling	authenticated arbitrary file viewing	1.0 / 2.5
Wp Editor	authenticated arbitrary file upload	1.0.2 / 1.2.5.3
Wp Filemanager	arbitrary file viewing	1.2.8 / 1.3.0
Wp Flipslideshow	persistent cross-site scripting (XSS)	2.0 / 2.2
Wp Front End Repository	arbitrary file upload	1.0.0 / 1.1
Wp Handy Lightbox	remote code execution (RCE)	1.4.5
Wp Homepage Slideshow	arbitrary file upload	2.0 / 2.3
Wp Image News Slider	arbitrary file upload	3.0 / 3.5
Wp Levoslideshow	arbitrary file upload	2.0 / 2.3
Wp Miniaudioplayer	arbitrary file viewing	0.5 / 1.2.7
Wp Mobile Detector	authenticated persistent cross-	3.0 / 3.2

	site scripting (XSS)	
Wp Mon	**arbitrary file viewing**	**0.5 / 0.5.1**
Wp Online Store	**arbitrary file viewing**	**1.2.5 / 1.3.1**
Wp Piwik	**persistent cross-site scripting (XSS)**	**0.10.0.1 / 1.0.10**
Wp Popup	**remote code execution (RCE)**	**2.0.0 / 2.1**
Wp Post Frontend	**arbitrary file upload**	**1.0**
Wp Property	**arbitrary file upload**	**1.20.0 / 1.35.0**
Wp Quick Booking Manager	**persistent cross-site scripting (XSS)**	**1.0 / 1.1**
Wp Royal Gallery	**persistent cross-site scripting (XSS)**	**2.0 / 2.3**
Wp Seo Spy Google	**arbitrary file upload**	**3.0 / 3.1**
Wp Simple Cart	**arbitrary file upload**	**0.9.0 / 1.0.15**
Wp Slimstat Ex	**arbitrary file upload**	**2.1 / 2.1.2**
Wp Superb Slideshow	**arbitrary file upload**	**2.0 / 2.4**
Wp Swimteam	**arbitrary file viewing**	**1 / 1.44.1077**
Wp Symposium	**arbitrary file upload**	**13.04 / 14.11**
Wp Vertical Gallery	**arbitrary file upload**	**2.0 / 2.3**
Wp Yasslideshow	**arbitrary file upload**	**3.0 / 3.4**
Wp2android Turn Wp Site Into Android App	**arbitrary file upload**	**1.1.4**
Wpeasystats	**local file inclusion (LFI)**	**1.8**
Wpmarketplace	**arbitrary file viewing**	**2.2.0 / 2.4.0**
Wpshop	**arbitrary file upload**	**1.3.1.6 / 1.3.9.5**
Wpstorecart	**arbitrary file upload**	**2.0.0 / 2.5.29**
Wptf Image Gallery	**arbitrary file viewing**	**1.0.1 / 1.0.3**
Wsecure	**remote code execution (RCE)**	**2.3**
Wysija Newsletters	**arbitrary file upload**	**1.1 / 2.6.7**
Xdata Toolkit	**arbitrary file upload**	**1.6 / 1.9**
Zen Mobile App Native	**arbitrary file upload**	**3.0**
Zingiri Web Shop	**arbitrary file upload**	**2.3.6 / 2.4.3**
Zip Attachments	**arbitrary file viewing**	**1.0 / 1.4**

Have your WordPress site been hacked?

Don’t despair; it happens to the best of us. It’s tough to give generic advice without having a look at your site.