WAYS TO MITIGATE WORDPRESS THREATS

Joan Logose

Jinja Virtual Wordpress Meetu

30th Jan 2021

CONTENTS OF THIS TEMPLATE

As more and more users take up WordPress as a CMS, the level of threats is also increasing. The good thing is, it can be controlled.

Just like web analytics, threats also need to be monitored. It is hard to fight an enemy you don’t know. It is important to have some basics on how some of these threats present themselves.

Most common WordPress security threats;

Brute force

Forced login

01

Malware

Malicious code

02

SQL Injections

Unauthorized access to database

03

04

Cross site scripting

Vulnerable scripts

05

DOS/DdOS

Denial of service

06

Hijacking a user

Users who are unaware

Effects of security issues

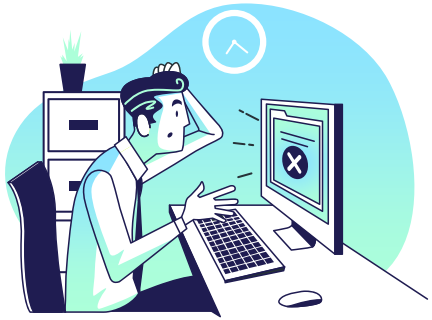
- Loss of trust from customers
- Downtime
- Damaged reputation
- Fines from authorities
- Ultimately, loss of revenue.
- Blacklisting on google etc

What

You can do

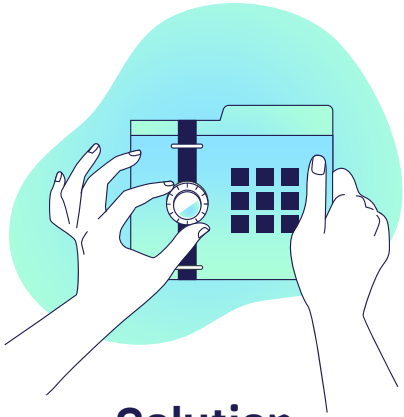
There are simple steps you can take even if you are not a security pro

THREAT VS. SOLUTION
Brute force



Problem

Brute force attacks refer to the use of trial and error method to access the website via the login page using multiple username and password combinations over and over again. Since most of us access websites this way, it is also one of the most common methods hackers use.



Solution

Strong username and passwords.

Fcvdrfghr / KOpOvpcxTKRCmXFpmC8

Two-factor authentication

Delete inactive high permission users

Lockout users with too many attempts

WordPress	[...] **Background Update Failed** - WordPress site: https://b...	1:11 AM
WordPress 62	[...] **Site Lockout Notification** - Site Lockout Notification Site Lockout ...	12:53 AM
WordPress	[...] **Site Lockout Notification** - Site Lockout Notification Site Lockout N...	12:36 AM
WordPress 8	[...] **Site Lockout Notification** - Site Lockout Notification Site Locko...	12:32 AM
WordPress	[...] **Site Lockout Notification** - Site Lockout Notification Site Locko...	11:55 PM

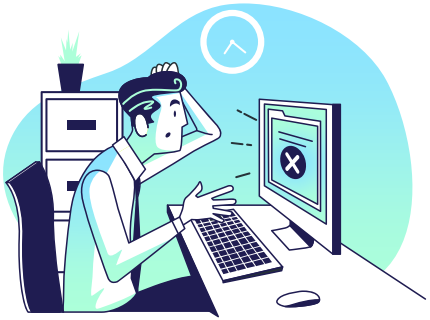
Site Lockout Notification

Site Lockout Notification

Host/User	Lockout in Effect Until	Reason
User: *admin*	2021-01-28 11:08:15	user tried to login as "admin."
Host: *107.180.122.58*	2021-01-28 11:08:15	user tried to login as "admin."

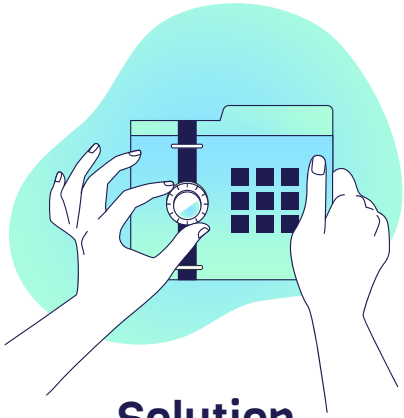
Release lockouts from the Active Lockouts section of the settings page.

Malware



Problem

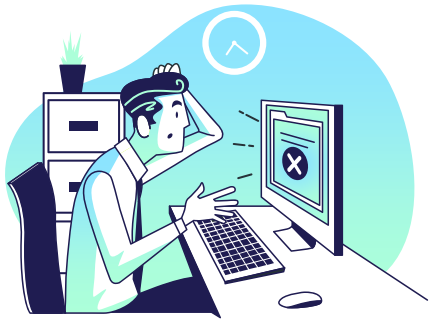
This is when malicious software or simply code is used to gain unauthorized access to a website to gather sensitive data.



Solution

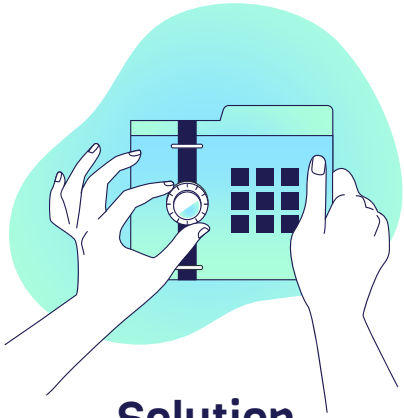
Always scan your website for malware(There are plugins for this if you don't know how to check your website files manually)

Cross site scripting (XSS)



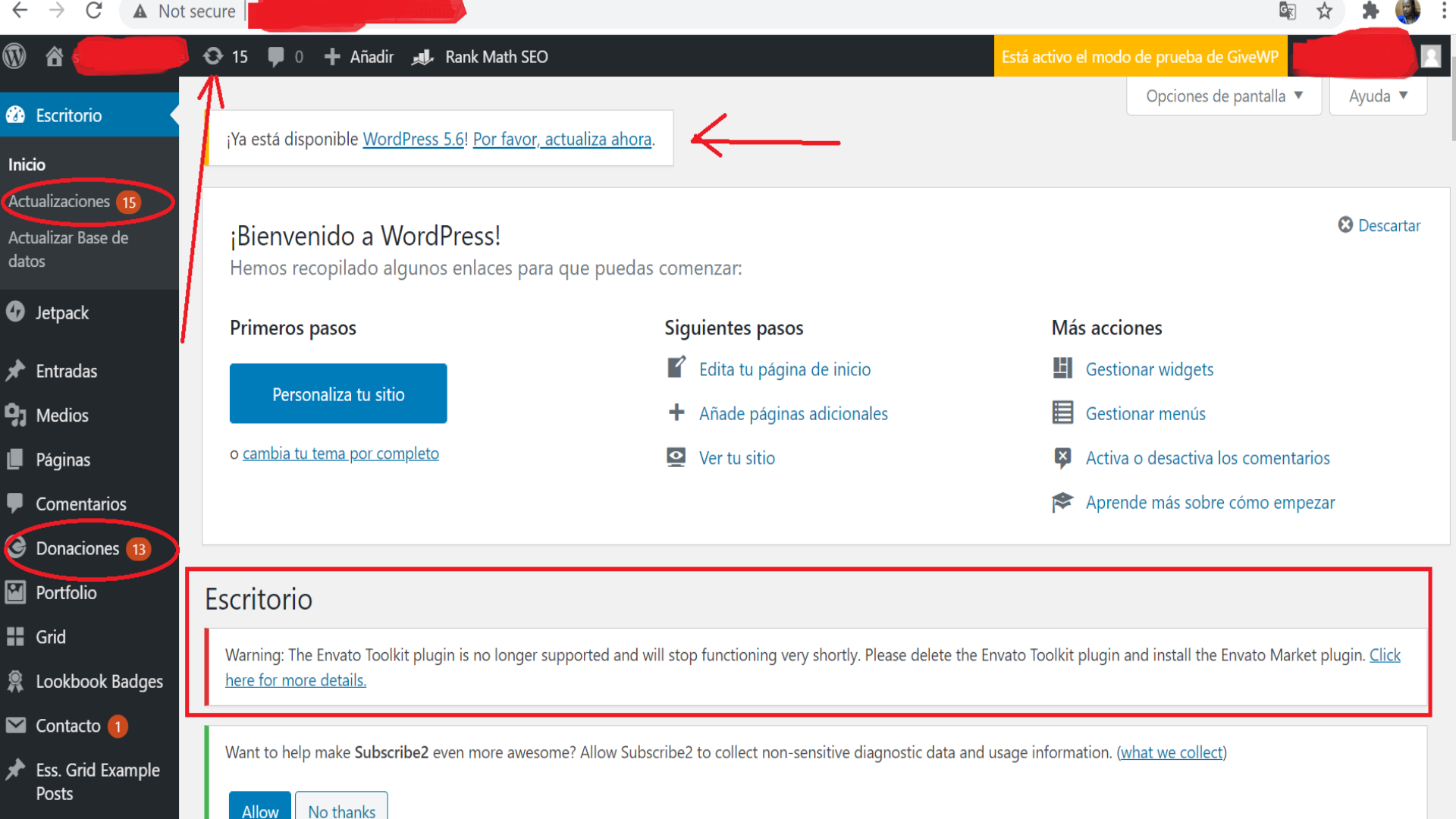
Problem

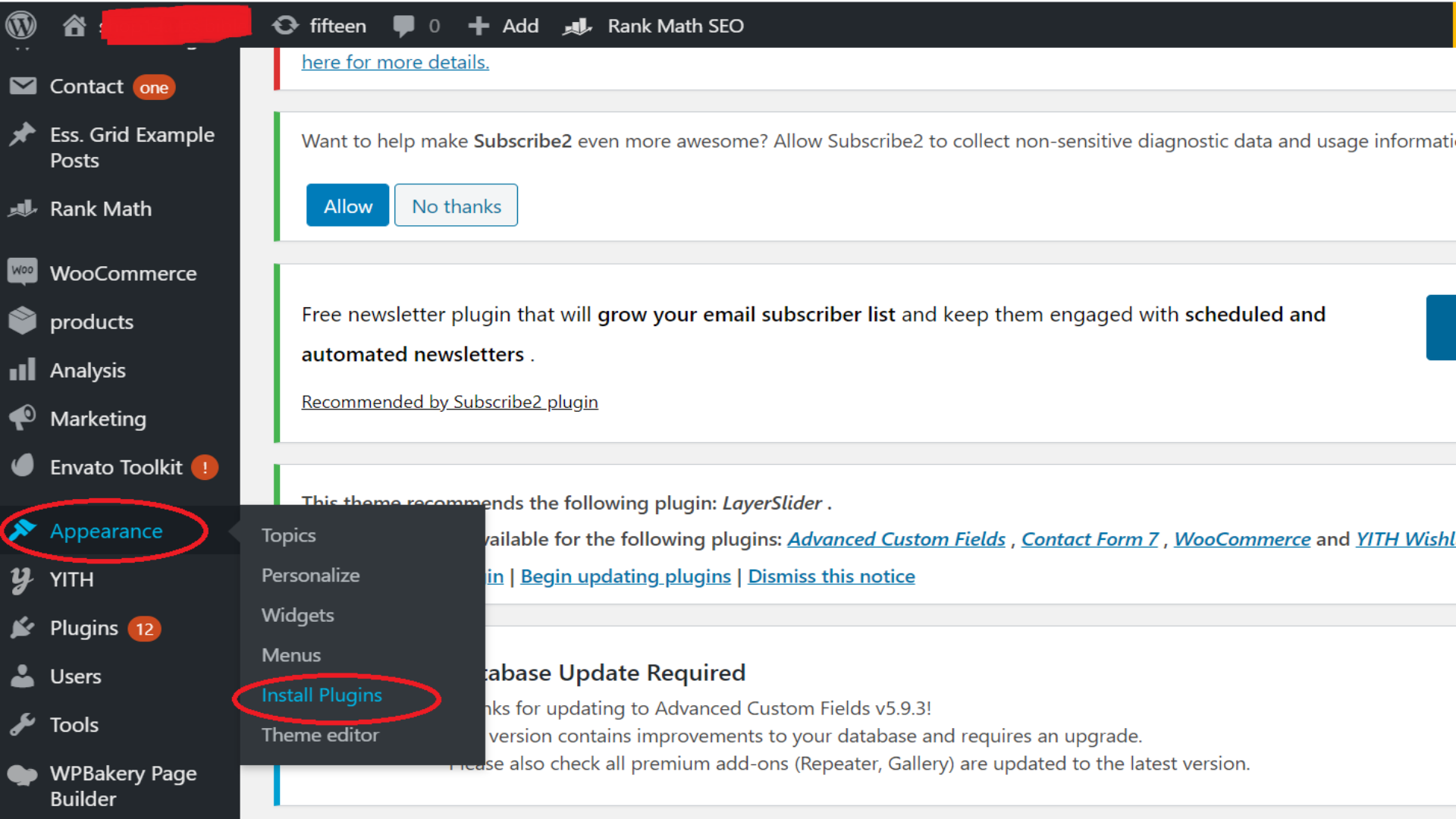
Here an attacker tries to get a user to load a page which has vulnerable scripts (JS)

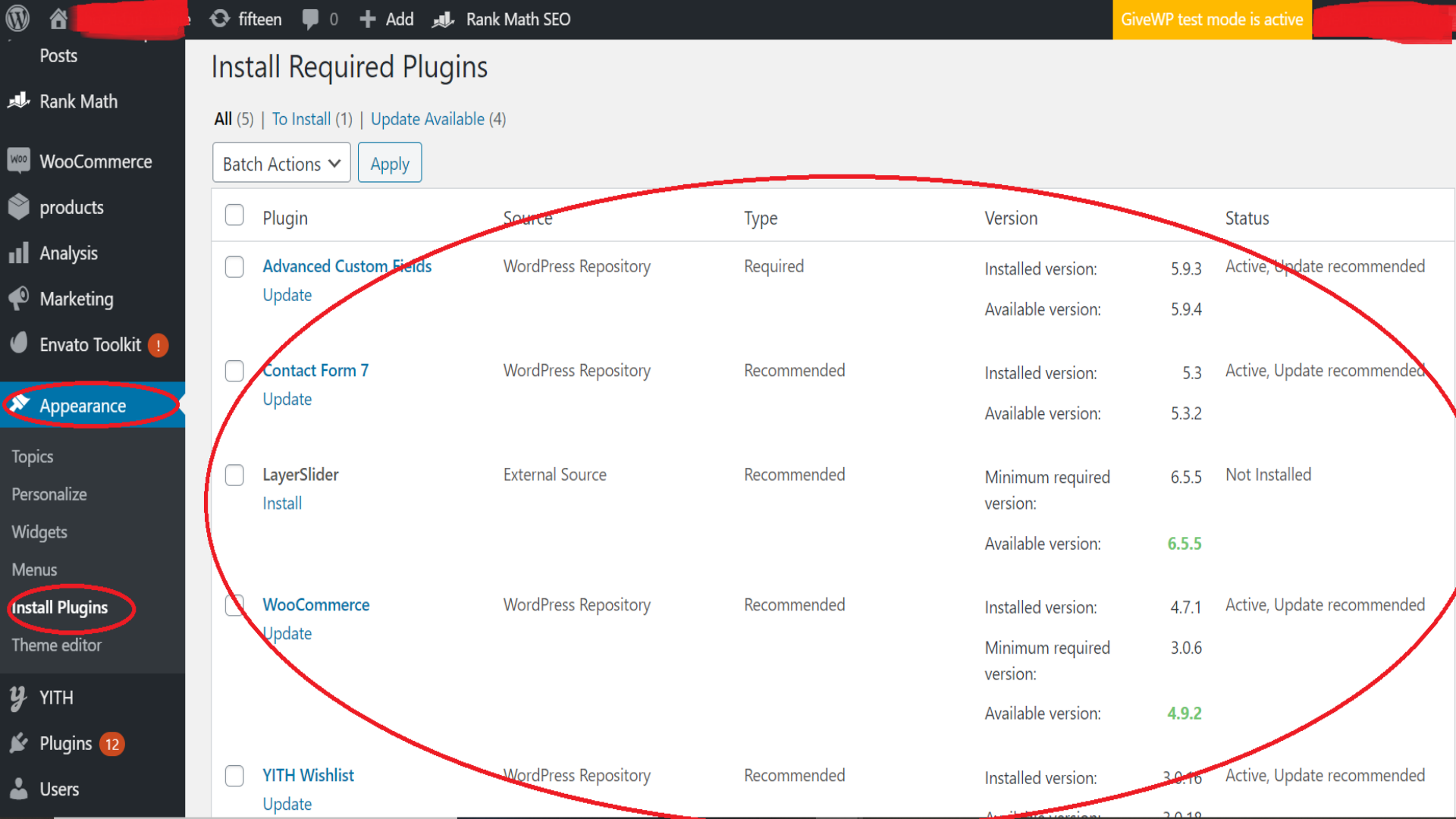


Solution

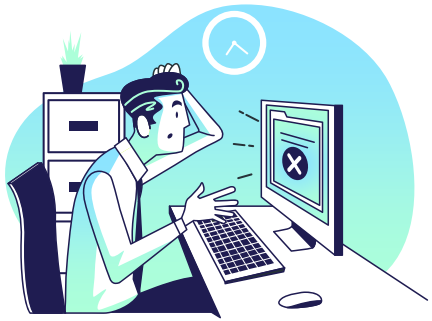
Update, update update!!


Not secure
15
0
Añadir
Rank Math SEO
Está activo el modo de prueba de GiveWP
Opciones de pantalla
Ayuda
Escritorio
Inicio
Actualizaciones 15
Actualizar Base de datos
Jetpack
Entradas
Medios
Páginas
Comentarios
Donaciones 13
Portfolio
Grid
Lookbook Badges
Contacto 1
Ess. Grid Example Posts
¡Ya está disponible WordPress 5.6! Por favor, actualiza ahora.
¡Bienvenido a WordPress!
Hemos recopilado algunos enlaces para que puedas comenzar:
Descartar
Primeros pasos
Personaliza tu sitio
o cambia tu tema por completo
Siguientes pasos
Edita tu página de inicio
Añade páginas adicionales
Ver tu sitio
Más acciones
Gestionar widgets
Gestionar menús
Activa o desactiva los comentarios
Aprende más sobre cómo empezar
Escritorio
Warning: The Envato Toolkit plugin is no longer supported and will stop functioning very shortly. Please delete the Envato Toolkit plugin and install the Envato Market plugin. Click here for more details.
Want to help make Subscribe2 even more awesome? Allow Subscribe2 to collect non-sensitive diagnostic data and usage information. (what we collect)
Allow
No thanks


fifteen
0
Add
Rank Math SEO
here for more details.
Want to help make Subscribe2 even more awesome? Allow Subscribe2 to collect non-sensitive diagnostic data and usage informati
Allow
No thanks
Free newsletter plugin that will grow your email subscriber list and keep them engaged with scheduled and automated newsletters .
Recommended by Subscribe2 plugin
ends the following plugin: LayerSlider .
vailable for the following plugins: Advanced Custom Fields , Contact Form 7 , WooCommerce and YITH Wishl
in | Begin updating plugins | Dismiss this notice
abase Update Required
ks for updating to Advanced Custom Fields v5.9.3!
version contains improvements to your database and requires an upgrade.
ase also check all premium add-ons (Repeater, Gallery) are updated to the latest version.
Contact one
Ess. Grid Example Posts
Rank Math
WooCommerce
products
Analysis
Marketing
Envato Toolkit !
Appearance
YITH
Plugins 12
Users
Tools
WPBakery Page Builder
Topics
Personalize
Widgets
Menus
Install Plugins
Theme editor

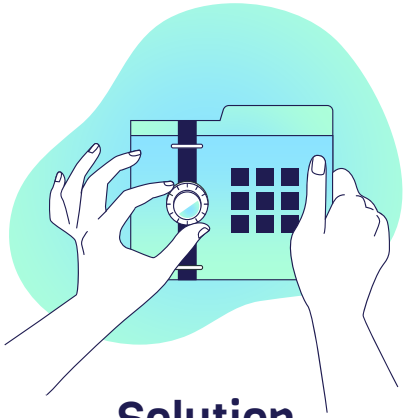

fifteen
0
Add
Rank Math SEO
GiveWP test mode is active
Posts
Rank Math
WooCommerce
products
Analysis
Marketing
Envato Toolkit
Appearance
Topics
Personalize
Widgets
Menus
Install Plugins
Theme editor
YITH
Plugins 12
Users
Install Required Plugins
All (5) | To Install (1) | Update Available (4)
Batch Actions
Apply
Plugin
Source
Type
Version
Status
Advanced Custom Fields
Update
WordPress Repository
Required
Installed version: 5.9.3
Available version: 5.9.4
Active, Update recommended
Contact Form 7
Update
WordPress Repository
Recommended
Installed version: 5.3
Available version: 5.3.2
Active, Update recommended
LayerSlider
Install
External Source
Recommended
Minimum required version: 6.5.5
Available version: 6.5.5
Not Installed
WooCommerce
Update
WordPress Repository
Recommended
Installed version: 4.7.1
Minimum required version: 3.0.6
Available version: 4.9.2
Active, Update recommended
YITH Wishlist
Update
WordPress Repository
Recommended
Installed version: 3.0.16
Active, Update recommended

DoS & DdOS – Distributed denial of service



Problem

This attack tries to prevent legitimate users from accessing your website. Here the attacker sends more requests than the webserver server can handle. Another way successful attacks occur is when the attacker sends bogus requests – forms, search function, product order forms.

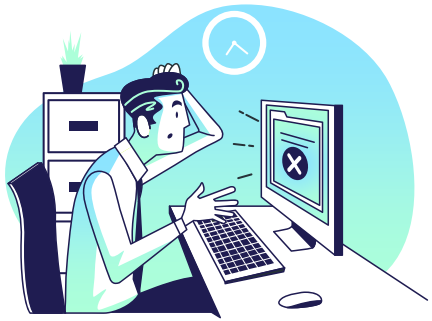


Solution

Install plugins that scan for malware, monitor unsusual traffic, country blocking.

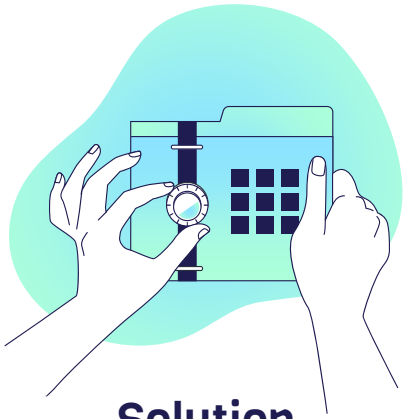
PS- slows down website and can increase bouncerate

SQL injection



Problem

Here an attacker gains access to your website's MySQL database and can add or delete tables they want from your website at that point. Like adding an admin user



Solution

Updates wordpress, PHP, Plugins!! .

products
Analysis
Marketing
Envato Toolkit !
Appearance
YITH
Plugins 12
Users
Tools
WPBakery Page Builder
Settings
Custom Fields
Demo Install
Slider Revolution
Ess. Grid

Mandatory update of WooCommerce database

WooCommerce has been updated! For everything to work properly we have to update your database to the most recent version. The database update process runs in the background and may take a while, so please be patient. Advanced users can update via WP CLI .

Update WooCommerce database | Learn more about updates

Your theme (Blaszok Child) contains outdated copies of some WooCommerce template files. You may need to update these files to ensure they are compatible with the current version of WooCommerce. Suggestions to fix this: Discard

1. Update your theme to the latest version. If there is no update available contact the author of your theme to ask about compatibility with the current version of WooCommerce
2. If you have copied over a template file to change something, then you will have to copy the new version of the template and apply your changes again.

Learn more about templates | View affected templates

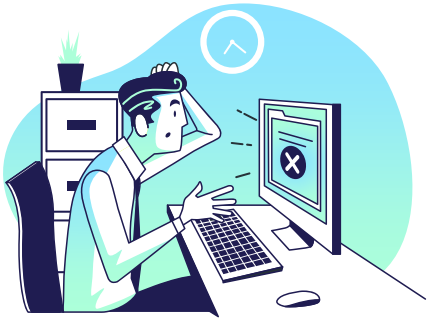
Geolocation has not been configured. Discard

You must enter a valid license key on the MaxMind integration settings page in order to use the geolocation service. If you do not need the geolocation service for shipping or taxes, you should change the customer's default location on the general settings page .

Update database - GiveWP needs to update your database to the latest version. The following process will make updates to your site's database. Please create a full backup before continuing.

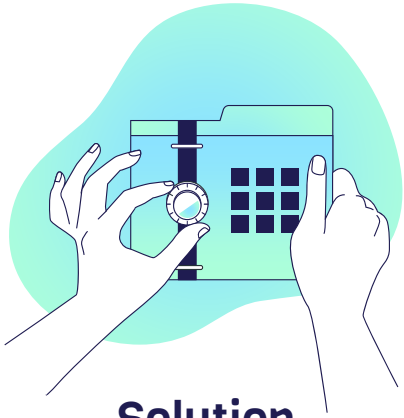
Run the updater

Hijacking a user



Problem

This happens when one leaves their dashboard un attended, loss of PC or unprofessional password storage



Solution

Educate users

Change passwords frequently

2SA

Other ways

Change login url

wpuganda/wp-admin

Wpuganda/8uhgyt5rfd

Wordpress salts

Enable these using plugins as they add characters to your password eg. - fcdrsr/fc$d!r@s#r

Keep up to date/ Training

There are free webinars by security companies like https://ithemes.com/training/

Security plugins

Take advantage of free versions of security plugins; Wordfense, iThemes etc

Out of office

If you have set office hours and you are sure you wont access website at a set time, you can prevent any admin work

Enable auto updates

Wordpress now has this. It can be dangerous and can cause plugin conflict with themes ets but can also save you

SALES AND DISTRIBUTION

Web advisor websites

Prevent long strings in the url

Enforce password change

Users

Monitor your Admin users

Refuse compromised passwords

Payments

Passwordless login

Monitor payment gateways

Log files

Emails

Read your emails as they often have warnings from security plugins

Hosting

Get reputable hosting

BACKUP YOUR WEBSITE

Appearance
YITH
Plugins 12
Users
All users
Add new
Profile
Tools
WPBakery Page Builder
Settings
Custom Fields
Demo Install
Slider Revolution
Ess. Grid
Punch Fonts

Your GiveWP extension is not receiving critical updates and new features because you have license key 1 inactive. Please activate your license to receive updates and priority support

Action required: Please update the Recurring Donations extension to version **1.9.4** or higher to be compatible with GiveWP **2.5.5** or higher. If you are having any problems, please revert to GiveWP version 2.5.4 or lower using the WP Rollback plugin and contact support for quick assistance.

We have spotted new content type (s) (give_forms), you might want to check your title and meta page and sitemap settings .

All (1) | Administrator (1)

Search Users

Batch Actions Apply Change profile to ... Change

1 item

Username	Name	Email	Profile	Tickets
demoadmin	-	[redacted]	Administrator	2
Username	Name	Email	Profile	Tickets

Batch Actions Apply Change profile to ... Change

1 item

Company name (optional)

Country / Region *

United Kingdom (UK)

Street address *

House number and street name

Apartment, room, etc. (optional)

Town / City *

Province (optional)

Zip code *

KJV GP83 LARGE PRINT × 3	£ 75.00
KJV 53 ENGLISH BIBLE × 1	£ 25.00
SUBTOTAL	**£ 100.00**
TOTAL	**£ 100.00**

Cash on delivery

Pay in cash at the time of delivery.

PayPal

I have read and agree to the terms and conditions of the website *

ORDERING

Note;

It’s not always about hackers.

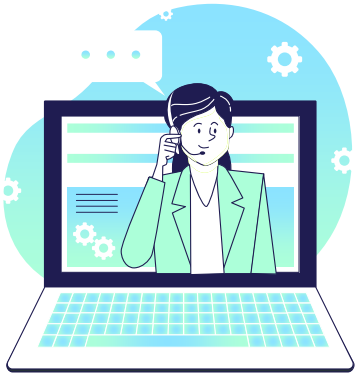
You can be a threat to your own website.

How?

- If you don’t update; conflicts, incompatibility between plugins, themes and core can lead to downtime. (things like white, blank screen)
- If you don’t manage your website caching well, it can affect your website
- Too many animations can increase bounce rate
- Uncoordinated colours on your website

Can threats totally be wiped out

NO! But if we carry out small tasks to improve security, we can reduce the number of successful attacks.



THANKS!!!

Do you have any questions?

Joan Logose

+256792692020

jlogose@gmail.com