Seguridad en WordPress

Lo que siempre miro cuando analizo un WordPress y cómo protegerte de ello

Fernando Castillo

Experto en ciberseguridad

00

¿Quién soy?

Durante **los últimos 7 años**

...he analizado cientos

de vulnerabilidades en negocios online

Qué hay mejor que un ladrón para

proteger una caja fuerte

La mentalidad del hacker

Suscríbete a la newsletter:

https://casbeep.com

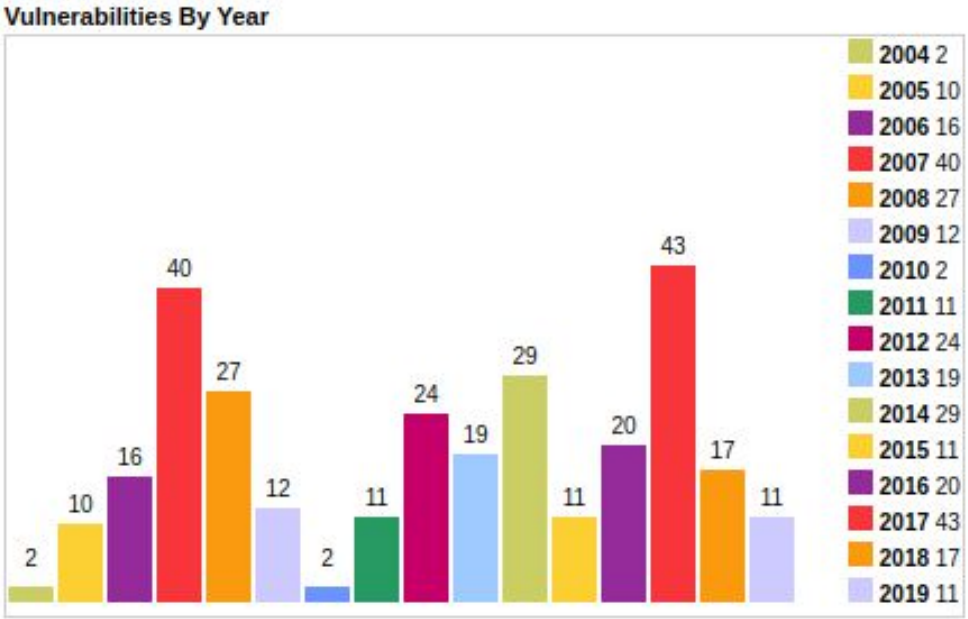
Fernando Castillo

Ayudo a emprendedores a proteger sus negocios online

01

¿Es WordPress seguro?

Contras



Fuente: cvedetails.com

Pros

wpscan.org

WPScan

WordPress Security Scanner

Homepage - WPScan.io - Vulnerability Database - WordPress Security Plugin

wpvulndb.com

WPScan Vulnerability Database

Cataloging **21631** WordPress Core Vulnerabilities, Plugin Vulnerabilities and Theme vulnerabilities.

Email Alerts | Submit a Vulnerability | Try our API

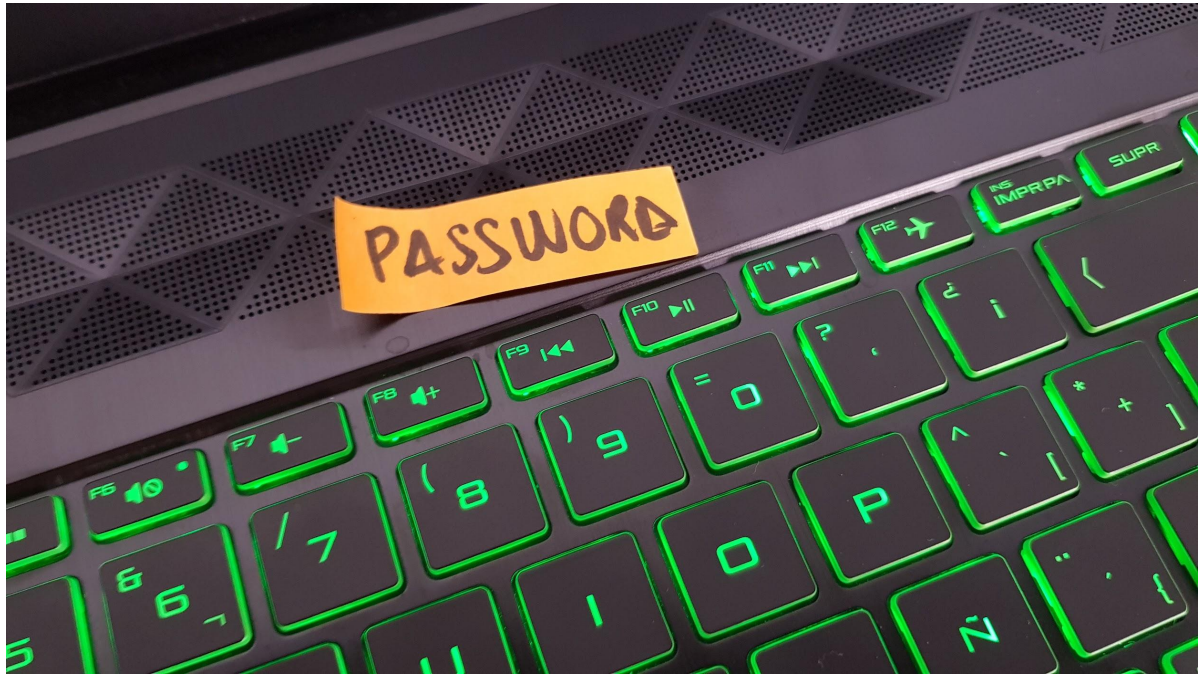
¿Soy realmente un objetivo?

El 60,8% de CMS son Wordpress

El 34% de sitios web son Wordpress

Si estás en Internet, **lo eres**

El sentido común es el **menos común** de todos los sentidos



02

Hosting

Versión de PHP

7.2 en adelante

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 7 months ago*	30 Nov 2019	*7 months ago*	30 Nov 2020	*in 4 months*
7.3	6 Dec 2018	*1 year, 6 months ago*	6 Dec 2020	*in 5 months*	6 Dec 2021	*in 1 year, 5 months*
7.4	28 Nov 2019	*7 months ago*	28 Nov 2021	*in 1 year, 4 months*	28 Nov 2022	*in 2 years, 4 months*

¿Hosting compartido o VPS?

```
root@ubuntu-s-1vcpu-2gb-fra1-01:~/software/ip2hosts# ./ip2hosts.sh 185.66.41.67
143comunicacion.com
25talentos.com
abarkatxo.com
adminfincassantiago.com
adnemprendedores.com
adsevilla.es
agabogadoslaboralistas.com
agicg.es
aimur.org
alberto-corsin-jimenez.org
alboraninterpretacion.com
aldebarandetectives.com
aliemusica.com
allsurance.es
almamiabeourdream.net
alvacu.es
antonanzaspeluqueros.com
```

Certificado SSL

Casbeep

03

Contraseñas

La contraseña es como tu **cepillo de dientes**

Cambialo a menudo

No lo compartas con nadie

Requisitos de una **contraseña segura**

Sistema infalible para acordarte de tu contraseña segura

Un día vi, una vaca sin rabo vestida de uniforme.

Udv,uvsrvdu.

Udv,uvsrvdu.69

Udv,uvsrvdu.69

¡Buena contraseña!

- Tu contraseña es resistente al pirateo.
- Tu contraseña no aparece en ninguna base de datos de contraseñas filtradas.

Tu contraseña puede ser descifrada con un ordenador común en...

327 siglos

En ese tiempo puedes ir y volver a la Luna 1333 veces.

Expire User Passwords

Require certain users to change their passwords on a regular basis.

Require password reset every 30 days

For users in these roles

- [x] Administrator
- [x] Editor
- [x] Author
- [x] Contributor
- [x] Subscriber

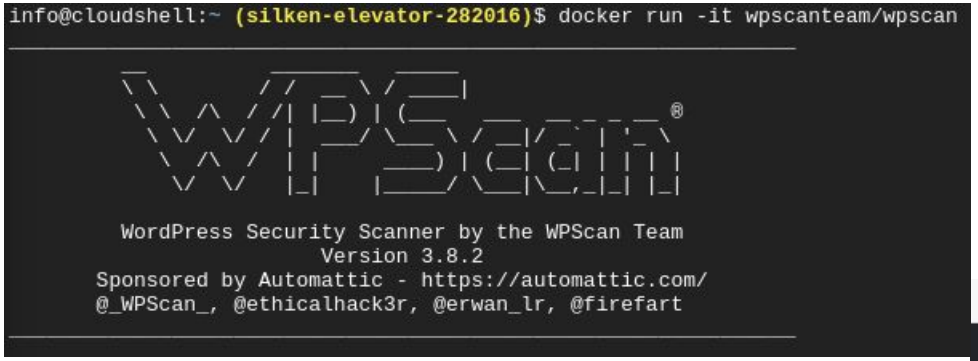
Expire User Passwords

Por Miller Media

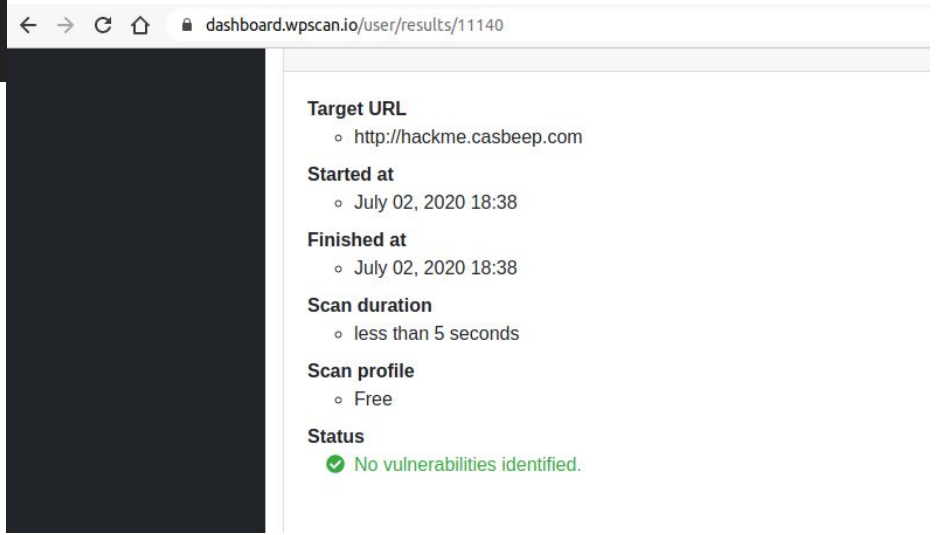
04

Fuerza bruta

wpscan.org



wpscan.io



docker run -it --rm wpscanteam/wpscan --url http://hackme.casbeep.com/

Casbeep

SecLists

diccionarios de usuarios y claves

github.com/danielmiessler/SecLists

README.md

About SecLists

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. The goal is to enable a security tester to pull this repository onto a new testing box and have access to every type of list that may be needed.

This project is maintained by Daniel Miessler, Jason Haddix, and g0tmi1k.

- Discovery
- Fuzzing
- IOCs
- Miscellaneous
- Passwords
- Pattern-Matching
- Payloads
- Usernames
- Web-Shells

SecLists Usuarios

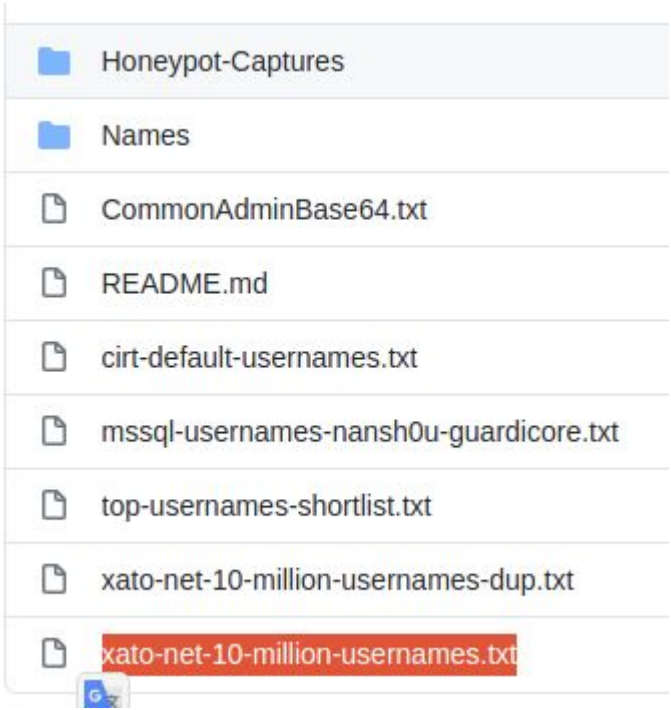
Branch: master ▾ **SecLists** / Usernames / Names / **malenames-usa-top1000.txt**

g0tmi1k Started sorting "Miscellaneous/" & "Fuzzing/"

1 contributor

1000 lines (1000 sloc) | 6.52 KB

```
1  JAMES
2  JOHN
3  ROBERT
4  MICHAEL
5  WILLIAM
6  DAVID
7  RICHARD
8  CHARLES
9  JOSEPH
```



SecLists Claves

Branch: master ▾ **SecLists** / Passwords / **Leaked-Databases** /

kazkansouh committed 607c329 on 27 May ...

..

000webhost.txt	strip trailing white
Ashley-Madison.txt	strip trailing white
Lizard-Squad.txt	strip trailing white
adobe100.txt	Renamed folders
alleged-gmail-passwords.txt	Close **#291** - Fix
bible-withcount.txt	Renamed folders
bible.txt	Renamed folders
carders.cc.txt	Close **#291** - Fix
elitehacker-withcount.txt	Renamed folders
elitehacker.txt	Renamed folders

- 10-million-password-list-top-500.txt
- 100k-most-used-passwords-NCSC.txt
- 10k-most-common.txt
- 500-worst-passwords.txt

govolution Create tomcat-betterdefaultpasslist.txt ...

1 contributor

79 lines (79 sloc) | 1.1 KB

```
admin:
admin:admanager
admin:admin
admin:admin
ADMIN:ADMIN
admin:adrole1
admin:adroot
admin:ads3cret
admin:adtomcat
admin:advagrant
admin:password
admin:password1
admin:Password1
admin:tomcat
```

Atacando al usuario **admin**

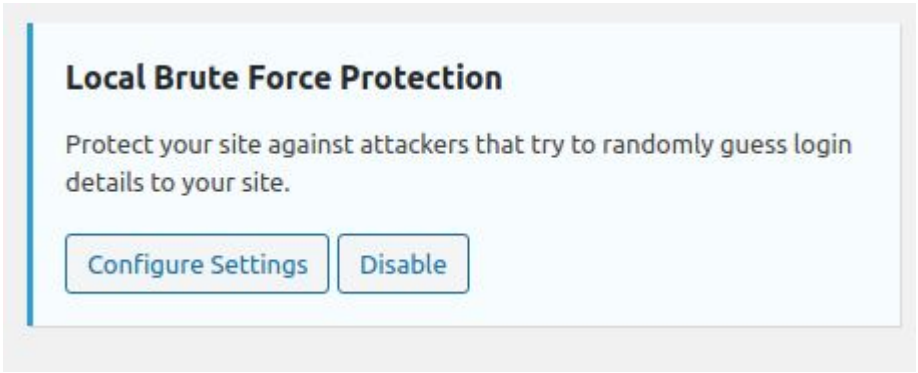
git clone https://github.com/danielmiessler/SecLists.git

wget https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/best15.txt

docker run -it --rm -v /home/info/:/files wpscanteam/wpscan --url http://hackme.casbeep.com/ -U admin --passwords /files/best15.txt

Casbeep

Protegiéndonos de la **fuerza bruta**



Multiple Authentication Attempts per XML-RPC Request

WordPress' XML-RPC feature allows hundreds of username and password guesses per request. Use the recommended "Block" setting below to prevent attackers from exploiting this feature.

Block (recommended)

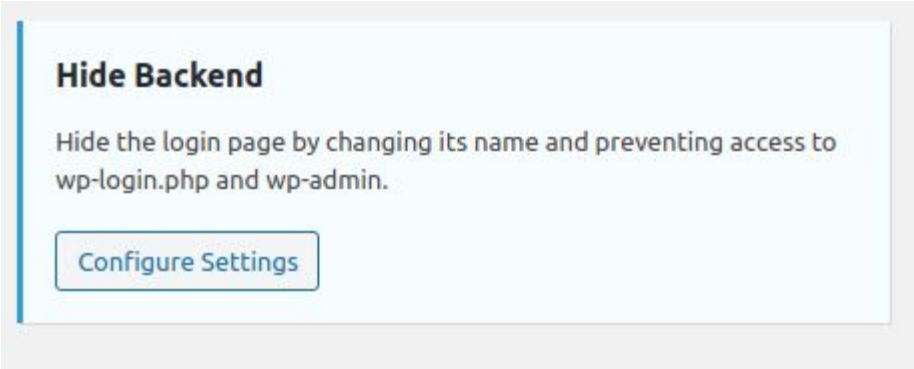
- **Block** - Blocks XML-RPC requests that contain multiple login attempts. This setting is highly recommended.
- **Allow** - Allows XML-RPC requests that contain multiple login attempts. Only use this setting if a service requires it.

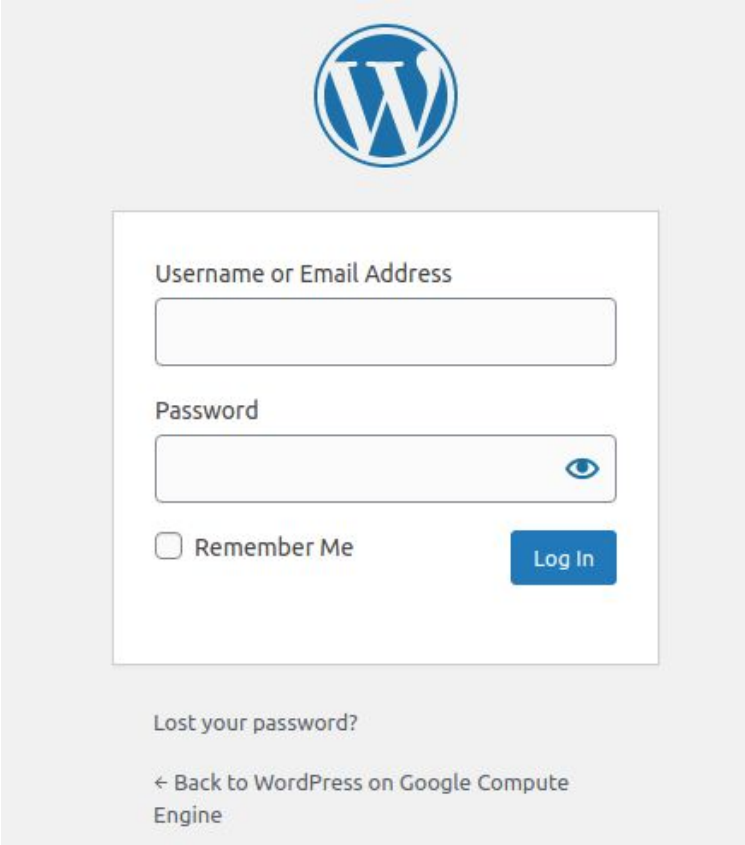
Protegiéndonos de la **fuerza bruta**

```
[+] Performing password attack on Xmlrpc against 1 user/s
Error: Unknown response received Code: 403
Body:
Error: Unknown response received Code: 403
Body: <?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>500</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string>&lt;!DOCTYPE html&gt;
&lt;html&gt;
&lt;head&gt;
        &lt;meta http-equiv=&quot;Content-Type&quot; content=
        &lt;meta name=&quot;viewport&quot; content=&quot;widt
        &lt;link href=&quot;http://hackme.casbeep.com/wp-cont
        &lt;meta name='robots' content='noindex,follow' /&gt;
        &lt;title&gt;Forbidden&lt;/title&gt;
```

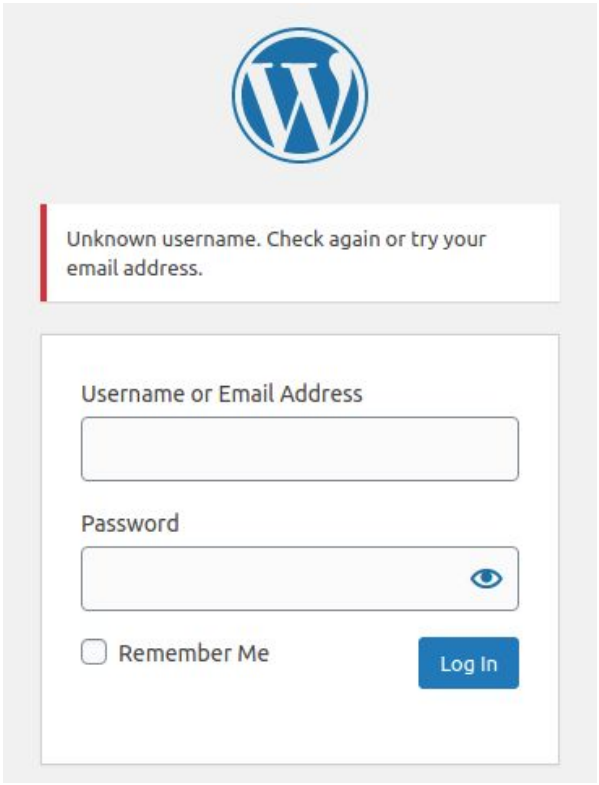
Casbeep

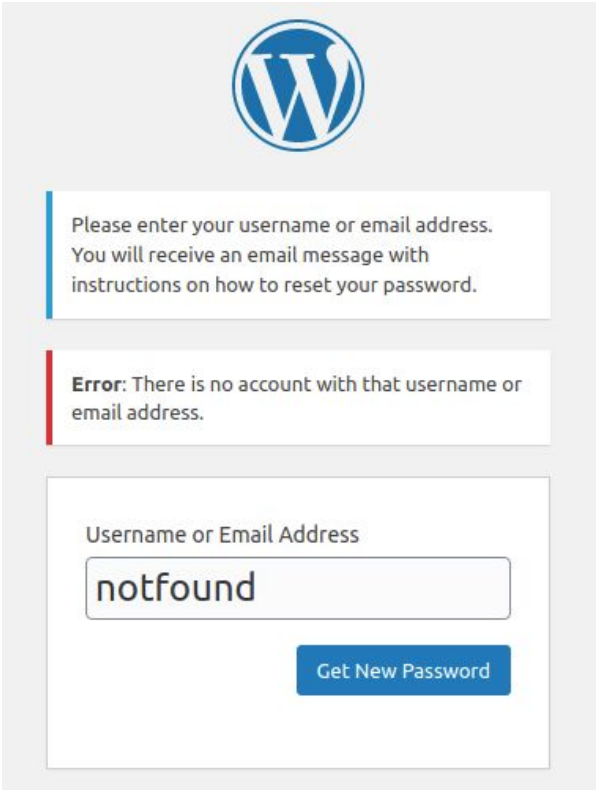
Panel de login **al público**





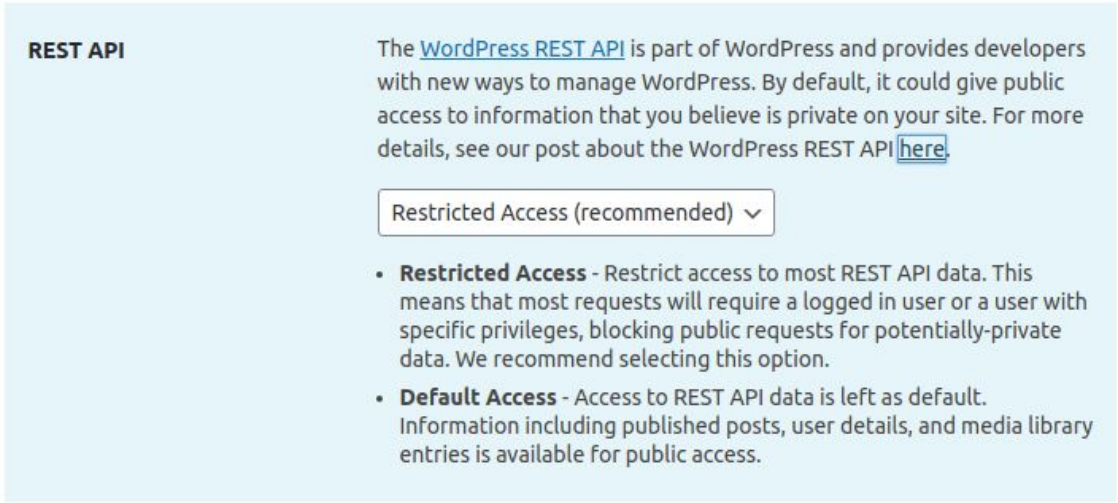
Enumerando **usuarios**





Enumerando **usuarios**

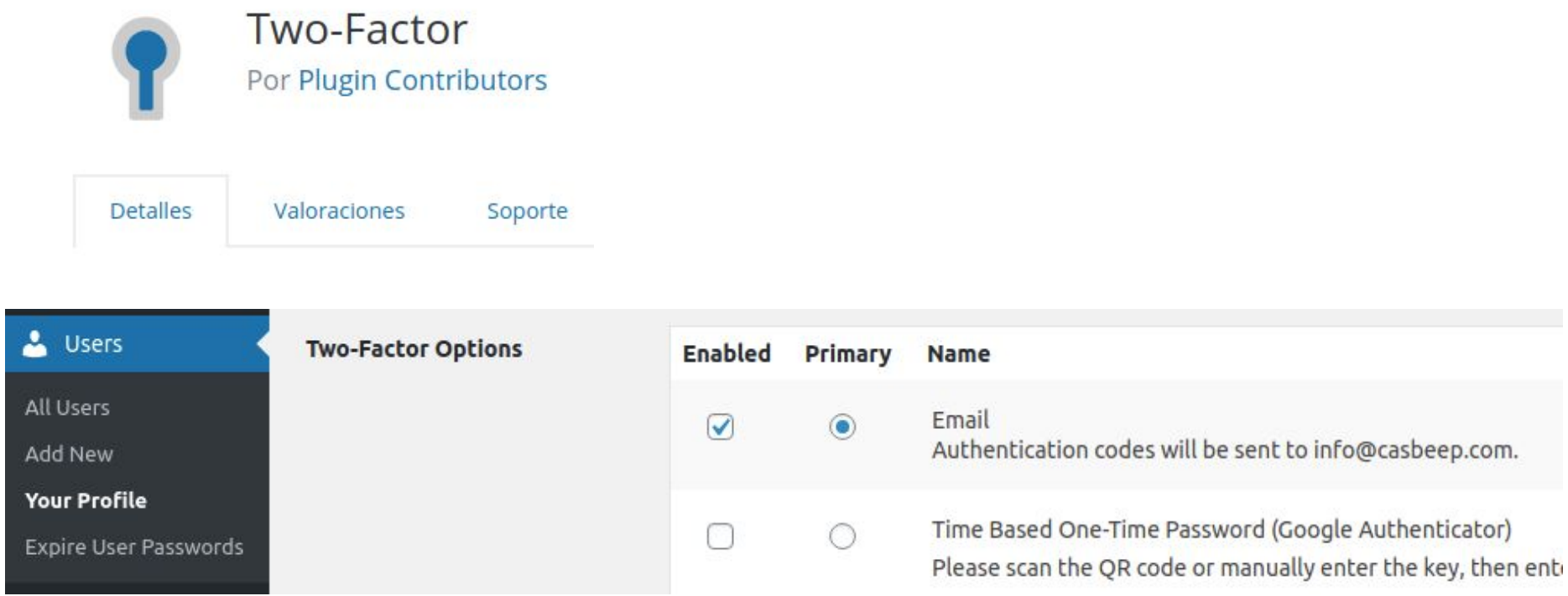

```
{"code":"itsec_rest_api_access_restricted","message":"You do not have sufficient permission to access this endpoint. Access to REST API requests is restricted by iThemes Security settings.","data":{"status":401}}
```

Segundo factor de autenticación (2FA)

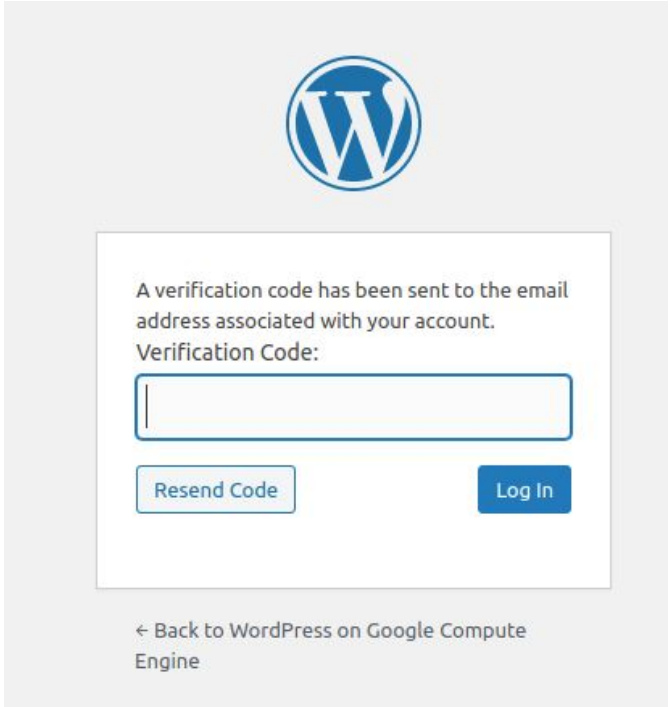
Método para confirmar que el usuario es quien dice ser combinando **dos secretos distintos**.

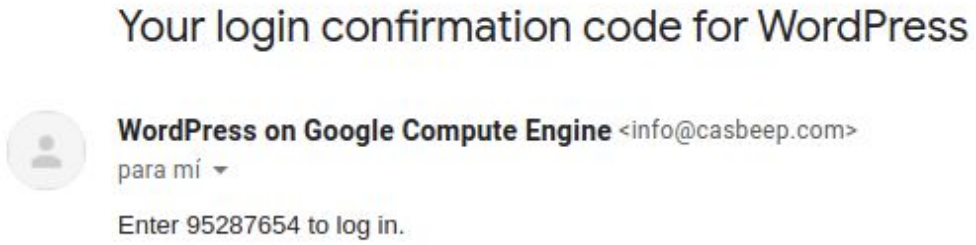
Segundo factor de autenticación (2FA)



Casbeep

Segundo factor de autenticación (2FA)



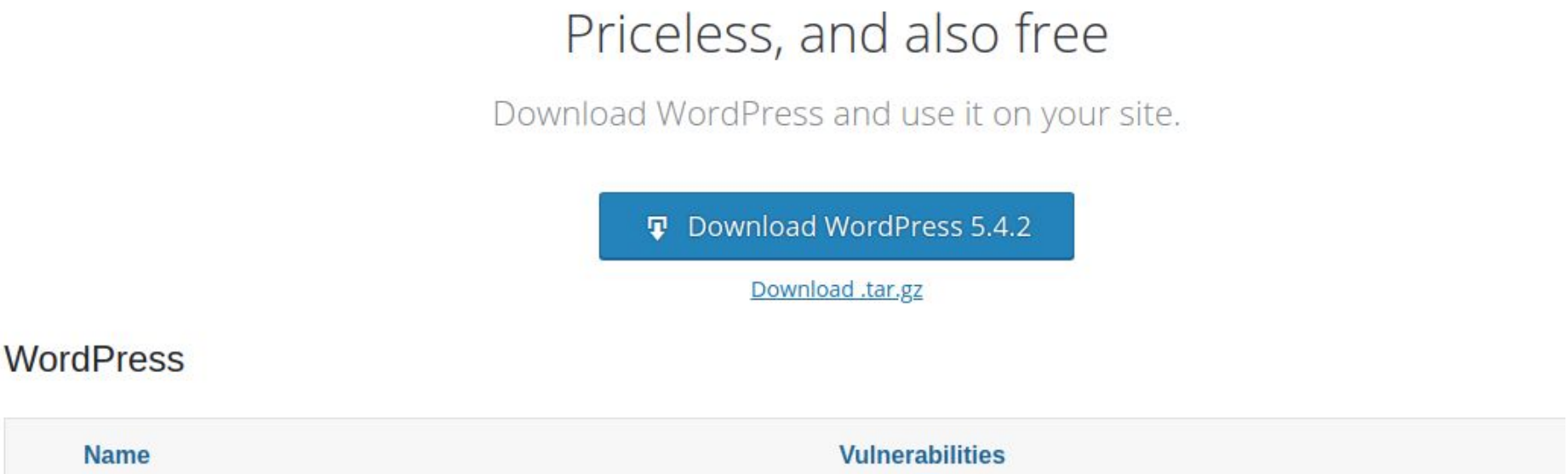


Casbeep

05

Versiones y actualizaciones

Versión del core



Últimas actualizaciones

Security Category Archive

« Back to blog

June 10, 2020	WordPress 5.4.2 Security and Maintenance Release
April 29, 2020	WordPress 5.4.1
December 13, 2019	WordPress 5.3.1 Security and Maintenance Release
November 19, 2019	WordPress 5.2.4 Update
October 14, 2019	WordPress 5.2.4 Security Release
September 5, 2019	WordPress 5.2.3 Security and Maintenance Release
March 12, 2019	WordPress 5.1.1 Security and Maintenance Release
December 13, 2018	WordPress 5.0.1 Security Release
July 5, 2018	WordPress 4.9.7 Security and Maintenance Release
April 3, 2018	WordPress 4.9.5 Security and Maintenance Release

Security Updates

WordPress versions 5.4 and earlier are affected by the following bugs, which are fixed in version 5.4.2. If you haven't yet updated to 5.4, there are also updated versions of 5.3 and earlier that fix the security issues.

- Props to Sam Thomas (jazzy2fives) for finding an XSS issue where authenticated users with low privileges are able to add JavaScript to posts in the block editor.
- Props to Luigi – (gubello.me) for discovering an XSS issue where authenticated users with upload permissions are able to add JavaScript to media files.
- Props to Ben Bidner of the WordPress Security Team for finding an open redirect issue in *wp_validate_redirect()*.
- Props to Nrimo Ing Pandum for finding an authenticated XSS issue via theme uploads.
- Props to Simon Scannell of RIPS Technologies for finding an issue where *set-screen-option* can be misused by plugins leading to privilege escalation.
- Props to Carolina Nymark for discovering an issue where comments from password-protected posts and pages could be displayed under certain conditions.

Ramas con soporte

Version 4.8.14

On June 10, 2020, WordPress 4.8.14 was released to the public.

codex.wordpress.org/Supported_Versions

WordPress, as downloaded from https://wordpress.org/download/ and *only* from https://wordpress.org/download/.

The **only current officially supported version** is WordPress 5.3. Previous major releases before this may or may not get security updates as serious exploits are discovered.

Beta versions, nightly builds, and Subversion check outs
ARE NOT SUPPORTED
on the WordPress support forums or on the WordPress Codex.

If you are unable or unwilling to file bug reports, and help fix problems, please do not use anything other than the officially released versions.

Some folks in the WordPress IRC channel or Slack *might* be familiar with unreleased versions, but it'll be hit-or-miss, and no guarantee of support is provided.

Support Policy

WordPress will be backported security updates when possible, but there are no guarantee and no timeframe for older releases. There are no fixed period of support nor Long Term Support (LTS) version such as Ubuntu's. None of these are safe to use, except the latest series, which is actively maintained.

For the list of WordPress Versions, refer WordPress_Versions.

Actualizaciones automáticas

valor por defecto minor

```
1 | define( 'WP_AUTO_UPDATE_CORE', true );
```

`WP_AUTO_UPDATE_CORE` can be defined with one of three values, each producing a different behavior:

- Value of `true` – Development, minor, and major updates are all **enabled**
- Value of `false` – Development, minor, and major updates are all **disabled**
- Value of `'minor'` – Minor updates are **enabled**, development, and major updates are **disabled**

Versiones de plugins y temas

Plugin	Descripción
Akismet Anti-Spam Activar | Borrar	Used by millions, Akismet is quite possibly the best way in the world to **protec** to set up your API key. Versión 4.1.5 | Por Automattic | Ver detalles

Hay disponible una nueva versión de Akismet Anti-Spam. Revisa los detalles de la versión 4.1.6 o actualízalo ahora.

WP Rollback

Por Impress.org

Detalles | Valoraciones

Descripción | Instalación | Registro de cambios | Valoraciones

4.1.6

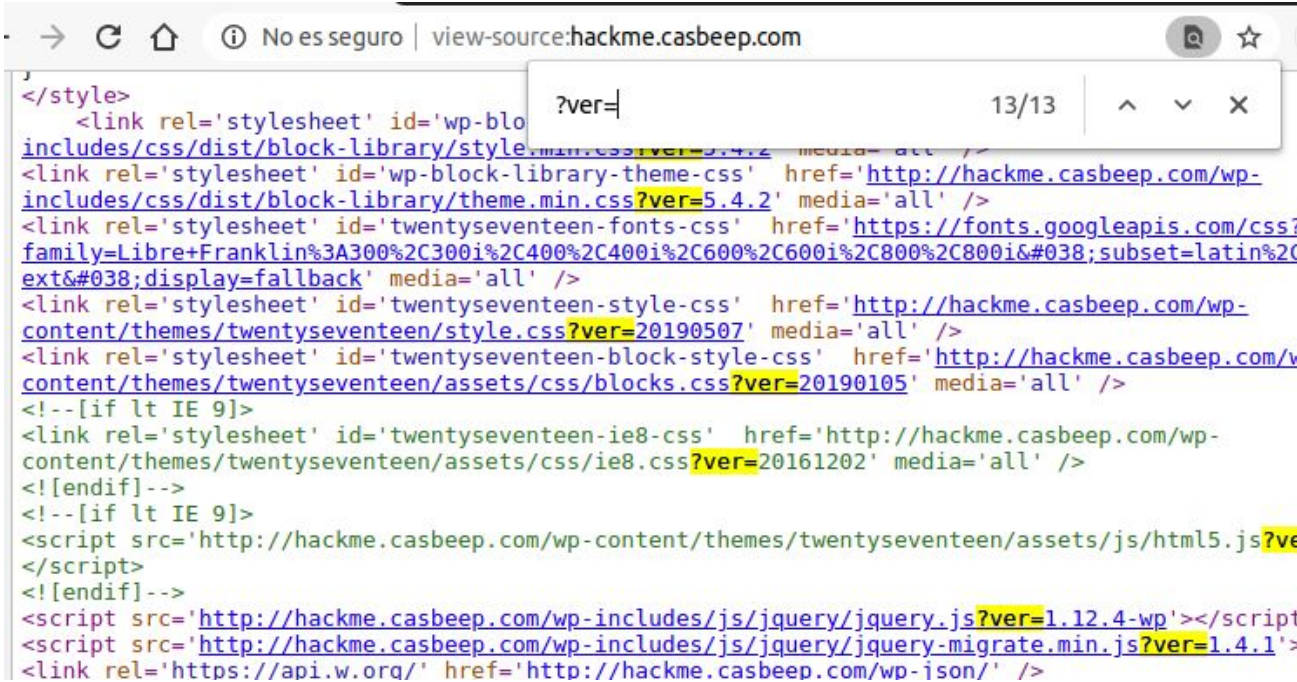
Fecha de lanzamiento – 4 de junio de 2020

- Desactiva el botón «Comprobar el spam» hasta que se cargue la página para evitar errores al hacer clic para volver a comprobar directamente la variable de la cola.
- Añade el filtro `akismet_enable_mshots` para permitir desactivar las ventanas emergentes de captura de pantalla en la página de administración de edición de comentarios.

Esconder la versión

Casbeep

Esconder la versión


No es seguro | view-source:hackme.casbeep.com
?ver=
13/13
</style>
<link rel='stylesheet' id='wp-block-library-theme-css' href='http://hackme.casbeep.com/wp-includes/css/dist/block-library/theme.min.css?ver=5.4.2' media='all' />
<link rel='stylesheet' id='twentyseventeen-fonts-css' href='https://fonts.googleapis.com/css?family=Libre+Franklin%3A300%2C300i%2C400%2C400i%2C600%2C600i%2C800%2C800i&subset=latin%2Cext&display=fallback' media='all' />
<link rel='stylesheet' id='twentyseventeen-style-css' href='http://hackme.casbeep.com/wp-content/themes/twentyseventeen/style.css?ver=20190507' media='all' />
<link rel='stylesheet' id='twentyseventeen-block-style-css' href='http://hackme.casbeep.com/wp-content/themes/twentyseventeen/assets/css/blocks.css?ver=20190105' media='all' />
<!--[if lt IE 9]>
<link rel='stylesheet' id='twentyseventeen-ie8-css' href='http://hackme.casbeep.com/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=20161202' media='all' />
<![endif]-->
<!--[if lt IE 9]>
<script src='http://hackme.casbeep.com/wp-content/themes/twentyseventeen/assets/js/html5.js?ve
</script>
<![endif]-->
<script src='http://hackme.casbeep.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script
<script src='http://hackme.casbeep.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'>
<link rel='https://api.w.org/' href='http://hackme.casbeep.com/wp-json/' />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://hackme.casbeep.com/xmlrpc.php?rsd" />
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://hackme.casbeep.com/wp-includes/wlwmanifest.xml" />
<meta name="generator" content="WordPress 5.4.2" />
<link rel="canonical" href="http://hackme.casbeep.com/" />
<link rel='shortlink' href='http://hackme.casbeep.com/' />
<link rel="alternate" type="application/json+oembed" href="http://hackme.casbeep.com/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fhackme.casbeep.com%2F" />
<link rel="alternate" type="text/xml+oembed" href="http://hackme.casbeep.com/wp-json/oembed/1.0/embed?url=http%3A%2F%2Fhackme.casbeep.com%2F&format=xml" />
<style type="text/css" id="custom-background-css">
body.custom-background { background-color: #ffffff; }
</style>
</head>
<body class="home blog custom-background wp-embed-responsive hfeed">

Skip to content
<header id="masthead" class="site-header" role="banner">

Hackme Casbeep
Just another WordPress site

<nav id="site-navigation" class="main-navigation" role="navigation">

<button class="menu-toggle" aria-controls="top-menu" aria-expanded="false">Menu</button>

</nav>
</header>

<main id="main" class="site-main" role="main">
<article id="post-1" class="post-1 post type-post status-publish format-standard hentry category-uncategorized">
<header class="entry-header">
<h2 class="entry-title">Hello world!</h2>
</header>

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

<footer class="entry-footer">
Posted in Uncategorized
</footer>
</article>
</main>

<footer id="colophon" class="site-footer" role="contentinfo">

Proudly powered by WordPress

</footer>

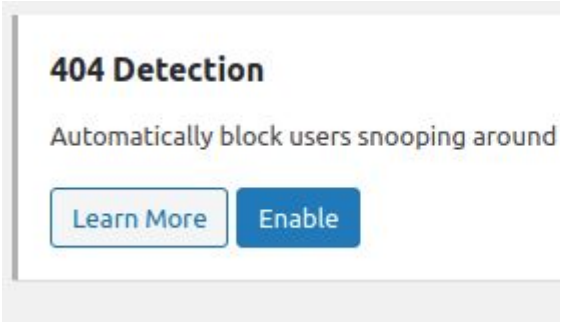
<script type="text/javascript">
/(trident|msie)/i.test(navigator.userAgent)&&document.getElementById&&window.addEventListener&&window.addEventListener("hashchange",function(){var t,e=location.hash.substring(1);/^[A-z0-9_-]+$/.test(e)&&(t=document.getElementById(e))&&(/^(?:a|select|input|button|textarea)$/i.test(t.tagName)||(t.tabIndex=-1),t.focus())},!1);
</script>
<script type="text/javascript">
var wpcom_emoji_settings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/12.0.0-1\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/12.0.0-1\/svg\/","svgExt":".svg","source":{"concatemoji":"http:\/\/hackme.casbeep.com\/wp-includes\/js\/wp-emoji-release.min.js?ver=5.4.2"}};
!function(e,a,t){var n,r,o,i=a.createElement("canvas"),p=i.getContext&&i.getContext("2d");function s(e,t){var a=String.fromCharCode;p.clearRect(0,0,i.width,i.height),p.fillText(a.apply(this,e),0,0);e=i.toDataURL();return p.clearRect(0,0,i.width,i.height),p.fillText(a.apply(this,t),0,0),e===i.toDataURL()}function c(e){var t=a.createElement("script");t.src=e,t.defer=t.type="text/javascript",a.getElementsByTagName("head")[0].appendChild(t)}for(o=Array("flag","emoji"),t.supports={everything:!0,everythingExceptFlag:!0},r=0;r<o.length;r++)t.supports[o[r]]=function(e){if(!p||!p.fillText)return!1;switch(p.textBaseline="top",p.font="600 32px Arial",e){case"flag":return s([127987,65039,8205,9895,65039],[127987,65039,8203,9895,65039])?!1:!s([55356,56826,55356,56819],[55356,56826,8203,55356,56819])&&!s([55356,57332,56128,56423,56128,56418,56128,56421,56128,56430,56128,56423,56128,56447],[55356,57332,8203,56128,56423,8203,56128,56418,8203,56128,56421,8203,56128,56430,8203,56128,56423,8203,56128,56447]);case"emoji":return!s([55357,56424,55356,57342,8205,55358,56605,8205,55357,56424,55356,57340],[55357,56424,55356,57342,8203,55358,56605,8203,55357,56424,55356,57340])}return!1}(o[r]),t.supports.everything=t.supports.everything&&t.supports[o[r]],"flag"!==o[r]&&(t.supports.everythingExceptFlag=t.supports.everythingExceptFlag&&t.supports[o[r]]);t.supports.everythingExceptFlag=t.supports.everythingExceptFlag&&!t.supports.flag,t.DOMReady=!1,t.readyCallback=function(){t.DOMReady=!0},t.supports.everything||(n=function(){t.readyCallback()},a.addEventListener?(a.addEventListener("DOMContentLoaded",n,!1),e.addEventListener("load",n,!1)):(e.attachEvent("onload",n),a.attachEvent("onreadystatechange",function(){"complete"===a.readyState&&t.readyCallback()})),(n=t.source||{}).concatemoji?c(n.concatemoji):n.wpemoji&&n.twemoji&&(c(n.twemoji),c(n.wpemoji)))}(window,document,wpcom_emoji_settings);
</script>
</body>
</html>
```

Casbeep
```

Esconder la versión

Casbeep

Esconder la versión



OOPS! THAT PAGE CAN'T BE FOUND.

It looks like nothing was found at this location. Maybe try a search?

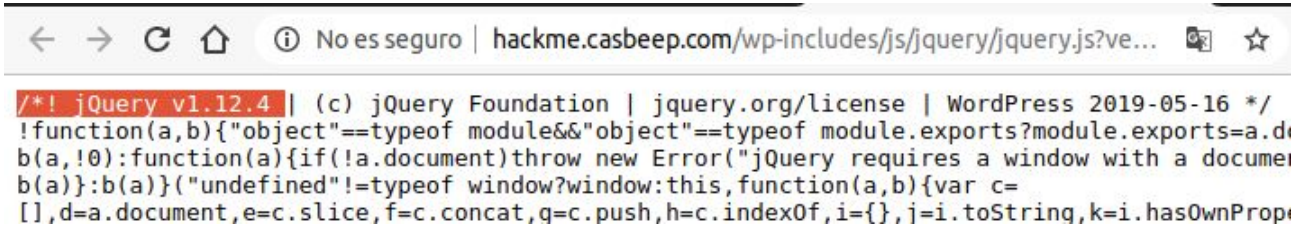
Search ...

Casbeep

Esconder la versión


```
=== iThemes Security (formerly Better WP Security) ===
Contributors: ithemes, chrisjean, mattdanner, timothyblynjacobs
Tags: security, security plugin, malware, hack, secure, block, SSL, admin, htaccess, lockdown
password, brute force, ban, permissions, bots, user agents, xml rpc, security log
Requires at least: 5.2
Tested up to: 5.4
Stable tag: 7.7.1
Requ s PHP: 5.6
Lice : GPLv2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html

== License ==
Released under the terms of the GNU General Public License.
```




```
/*! jQuery v1.12.4 | (c) jQuery Foundation | jquery.org/license | WordPress 2019-05-16 */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.d
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a docume
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i={},j=i.toString,k=i.hasOwnProp
```

06

¡Oh no
me han “jakiado”!

Copias de seguridad

Database Backups

Create backups of your site's database. The backups can be created manually and on a schedule.

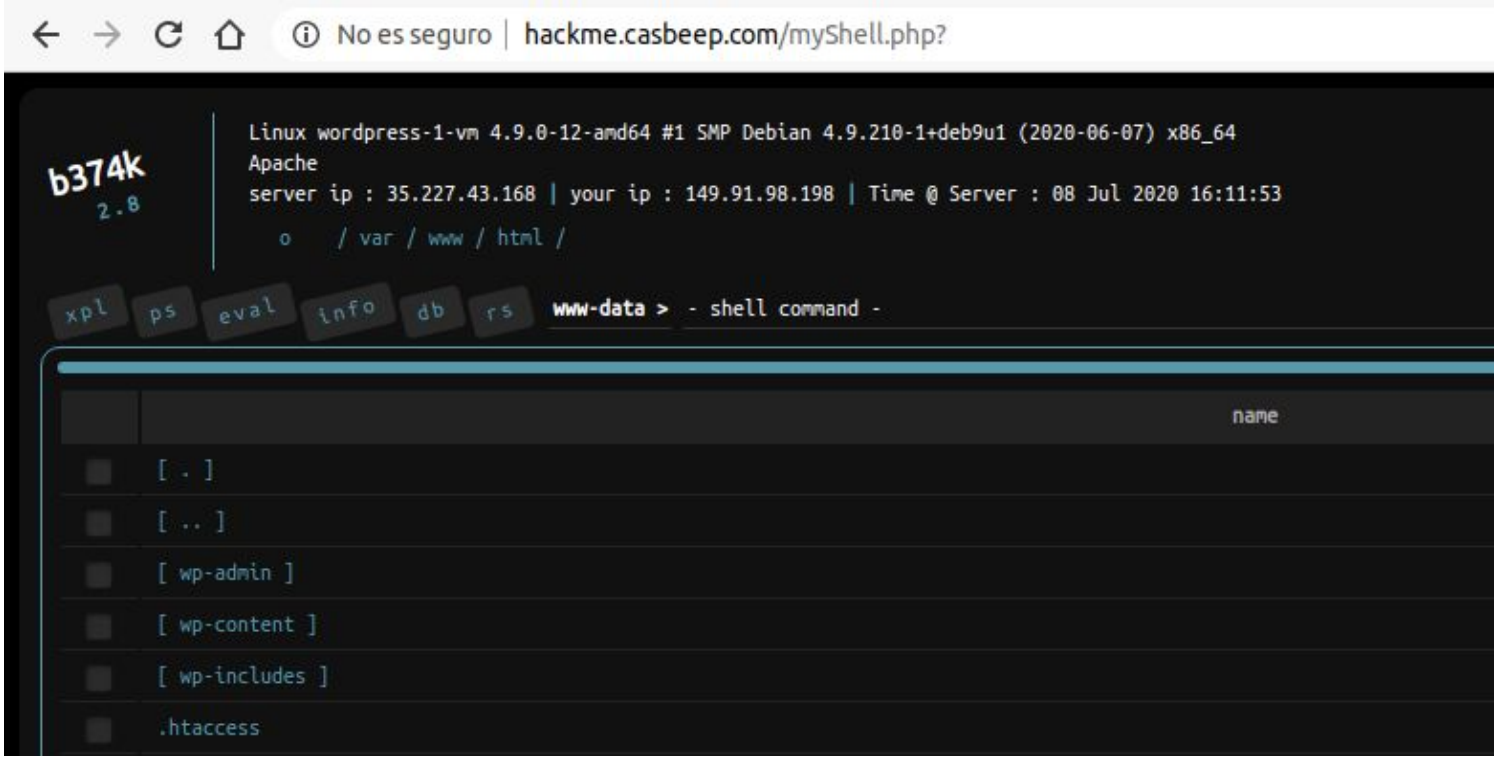
Configure Settings | Disable

Duplicator – WordPress Migration Plugin

WordPress migration and backups are much easier with Duplicator! Clone, backup, move and transfer an entire site from one location to another.

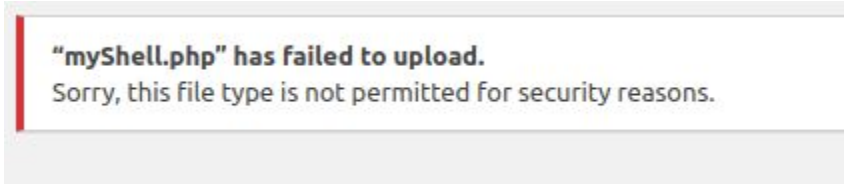
By Snap Creek

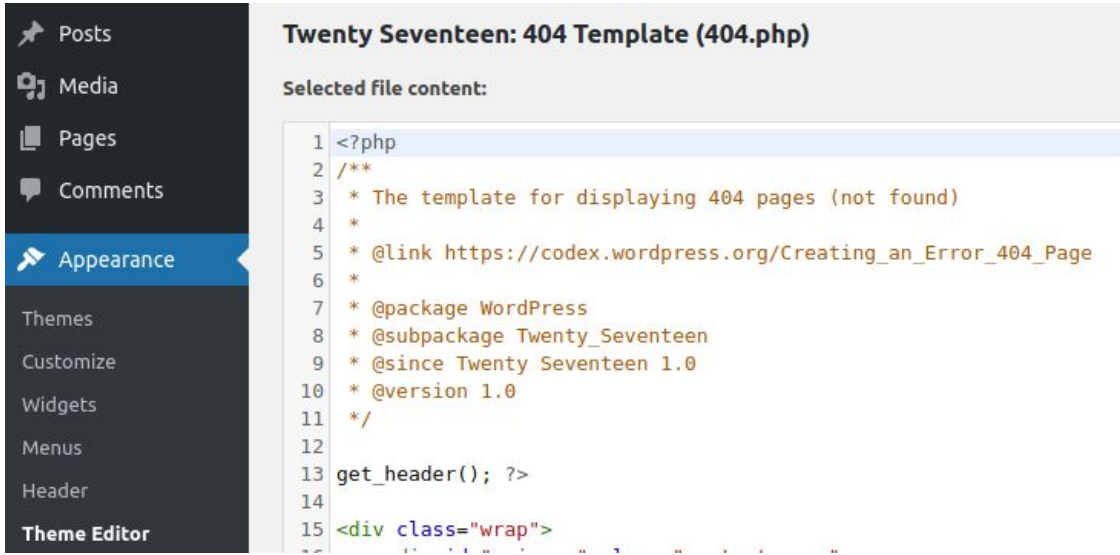
Webshells



Casbeep

Webshells



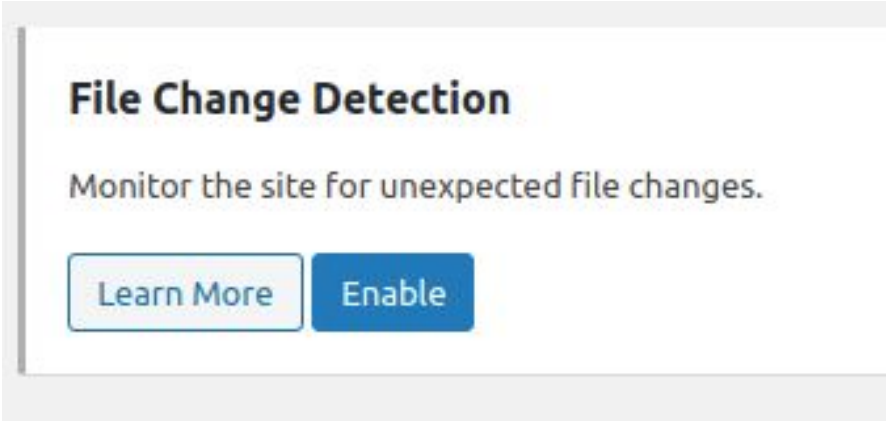


Protección contra webshells

File Editor

☑ Disable File Editor

Disables the file editor for plugins and themes requiring users to have access to the file system to modify files. Once activated you will need to manually edit theme and other files using a tool other than WordPress.



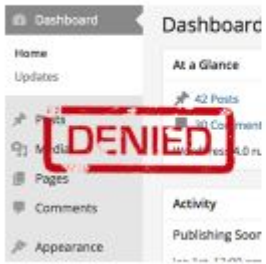
Usuarios

Membership ☐ Anyone can register

User Switching

Instant switching between user accounts in WordPress.

By John Blackbourn & contributors



Remove Dashboard Access

Allows you to disable Dashboard access for users of a specific role or capability. Disallowed users are redirected to a chosen URL.

By Drew Jaynes (DrewAPicture)

Revisar plugins y temas

Herramientas de **desinfección**

Cerber Security, Anti-spam & Malware Scan

Protection against hacker attacks and bots. Malware scanner & integrity checker. User activity log. Antispam reCAPTCHA. Limit login attempts.

By Cerber Tech Inc.

Se encontró código sospechoso

Se ha encontrado una instrucción de código sospechosa

`Line 7: eval`

May be used to execute malicious code on the web server. Pairing with base64_decode function indicates malicious code.

Se han encontrado firmas de código sospechosas

`Line 7: $r9f35db4(`

A variable function call. Usually is used to hinder malware detection. (VARF)

Suscríbete a la newsletter:

https://casbeep.com

FIN