

Painel

Posts

Mídia

Páginas

Comentários

Elementor

Modelos

Aparência

Plugins

Plugins instalados

Adicionar novo

Editor de arquivos de plugin

Usuários

Ferramentas

Configurações 3

Backuply

Recolher menu

Plugins

Adicionar novo

Todos (6) | Ativos (4) | Desativados (2) | Atualizações automáticas desativadas (6)

Ações em massa ▼ Aplicar

Pesquisar plugins instalados...


6 item

<input type="checkbox"/>	Plugin	Descrição	Atualizações automáticas
<input type="checkbox"/>	Akismet Anti-Spam Ativar Excluir	Usado por milhões, Akismet é possivelmente a melhor maneira do mundo para proteger seu blog contra spam . Ele mantém seu site protegido mesmo enquanto você dorme. Para começar: ative o plugin Akismet e vá para a página Configurações do Akismet para configurar sua chave API. Versão 5.1 Por Automattic Ver detalhes	Ativar atualizações automáticas
<input type="checkbox"/>	Backuply Desativar	Backuply is a Wordpress Backup plugin. Backups are the best form of security and safety a website can have. Versão 1.1.2 Por Softaculous Ver detalhes	Ativar atualizações automáticas
<input type="checkbox"/>	Elementor Configurações Desativar Atualize agora	O construtor de sites Elementor tem de tudo: editor de páginas arraste-e-solte, design perfeito em pixels, edição responsiva para dispositivos móveis e mais. Comece agora! Versão 3.12.2 Por Elementor.com Ver detalhes Documentação e perguntas frequentes Tutoriais em vídeo	Ativar atualizações automáticas
<input type="checkbox"/>	Elementor Header & Footer Builder Settings Desativar	This powerful plugin allows creating a custom header, footer with Elementor and display them on selected locations. You can also create custom Elementor blocks and place them anywhere on the website with a shortcode. Versão 1.6.13 Por Brainstorm Force, Nikhil Chavan Ver detalhes	Ativar atualizações automáticas
<input type="checkbox"/>	Hello Dolly Ativar Excluir	Isto não é só um plugin, é algo que simboliza a esperança e o entusiasmo de uma geração inteira resumida em duas palavras cantadas por Louis Armstrong: Hello, Dolly. Quando ativar este plugin, você verá trechos aleatórios da letra da canção Hello, Dolly do lado direito de cada tela de administração. Versão 1.7.2 Por Matt Mullenweg Ver detalhes	Ativar atualizações automáticas
<input type="checkbox"/>	Really Simple SSL Improve security - Upgrade Suporte Configurações Desativar	Lightweight SSL & Hardening Plugin Versão 6.2.4 Por Really Simple Plugins Ver detalhes	Ativar atualizações automáticas

ritos

Palavra-chave ▼ all in one security

1.036 itens << < 1




All-In-One Security (AIOS) – Security and Firewall

Instalar agora

Mais detalhes

Protect your website investment with All-In-One Security (AIOS) – a comprehensive and easy to use security plugin designed especially for WordPress.




iThemes Security

The Best WordPress Security Plugin to Secure & Protect WordPress

Por iThemes

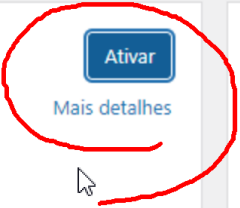
1.036 itens



All-In-One Security (AIOS) – Security and Firewall


Protect your website investment with All-In-One Security (AIOS) – a comprehensive and easy to use security plugin designed especially for WordPress.

Por All In One WP Security & Firewall Team



Ativar

Mais detalhes



iThemes Security

The Best WordPress Security Plugin to Secure & Protect WordPress

Por iThemes

		Versão
<input type="checkbox"/>	All in One WP Security Configurações Desativar	Em to Versão
<input type="checkbox"/>	Backuply Desativar	Backu Versão
<input type="checkbox"/>	Elementor	O con

Configurações

All In One WP Security and Firewall

Our PHP-based firewall has been created to give you even greater protection. To ensure the PHP-based firewall runs before any potentially vulnerable code in your WordPress site can be reached, it will need to be set up.

If you already have our .htaccess-based firewall enabled, you will still need to set up the PHP-based firewall to benefit from its protection.

To set up the PHP-based firewall, press the 'Set up now' button below:

[Set up now](#)[Dismiss](#)

Configurações gerais

[.htaccess Arquivo](#)[wp-config.php Arquivo](#)[Delete plugin settings](#)[WP version info](#)[Importar / Exportar](#)[Advanced settings](#)[Two factor authentication](#)

Para informações, atualizações e documentação, por favor visite o [All In One WP Security & Firewall Plugin](#) Página.

Plugin de segurança WP

Thank you for using the AIOS security plugin. There are a lot of security features in this plugin.

To start, go through each security option and enable the "basic" options. The more features you enable, the more security points you will achieve.

Before doing anything we advise taking a backup of your .htaccess file, database and wp-config.php.

- [Fazer backup de seu banco de dados](#)
- [Fazer backup do arquivo .htaccess](#)
- [Fazer backup do arquivo wp-config.php](#)

Desabilitar recursos de segurança

Se você acha que algumas funcionalidades do plugin em seu site estão quebrado devido a um recurso de segurança que você habilitou neste plugin, então use a seguinte opção para desativar todos os recursos de segurança deste plugin.

[Usuários](#)[Ferramentas](#)[Configurações 3](#)[Segurança WP](#)[Dashboard](#)[Settings](#)[User Accounts](#)[User Login](#)[User Registration](#)

Plugin de segurança WP

Thank you for using the AIOS security plugin. There are a lot of security features in this plugin.

To start, go through each security option and enable the "basic" options. The more features you enable,

Before doing anything we advise taking a backup of your .htaccess file, database and wp-config.php.

- [Fazer backup de seu banco de dados](#)
- [Fazer backup do arquivo .htaccess](#)
- [Fazer backup do arquivo wp-config.php](#)

Quer saber mais sobre os desenvolvedores por trás deste plugin?

[Team UpdraftPlus](#)

Status de característica crítica



Abaixo está o estado atual dos recursos críticos que você deve ativar em seu site para atingir um nível mínimo de segurança recomendado

Nome de usuário admin

ON

OFF

Login logout

ON

OFF

Permissão de arquivo

ON

OFF

Firewall básico

ON

OFF

- Modelos
- Aparência
- Plugins
- Usuários
- Ferramentas
- Configurações 3
- Segurança WP**
- Dashboard
- Settings
- User Accounts
- User Login
- User Registration
- Database Security
- Filesystem Security
- Blacklist Manager
- Firewall
- Brute Force
- Spam Prevention
- Scanner
- Maintenance
- Miscellaneous

- Login logout
- Registros de falhas de login
- Forçar saída**
- Logs de atividade de conta
- Usuários conectados
- Additional settings

Definir um período de expiração para a sessão de administração do WP é uma maneira simples para proteger contra o acesso não autorizado ao seu site a partir do seu computador. Este recurso permite que você especifique um período de tempo em minutos, após o qual a sessão de administração irá expirar e o usuário será forçado a voltar a iniciar sessão.

Opções de saída do usuário à força

- Básico
- 0/5

Habilitar saída do usuário WP à força:

☒ Marque esta opção se você deseja forçar um usuário wp a ser desconectado após um período de tempo configurado

Desconectar usuário WP após XX minutos:

120

(Minutos) O usuário será obrigado a efetuar login novamente após este período de tempo tem passado.

Salvar configurações

	0755	0755	Nenhuma ação necessária.
	0755	0755	Nenhuma ação necessária.
	0644	0644	Nenhuma ação necessária.
dex.php	0644	0644	Nenhuma ação necessária.
/	0755	0755	Nenhuma ação necessária.
themes	0755	0755	Nenhuma ação necessária.
plugins	0755	0755	Nenhuma ação necessária.
	0755	0755	Nenhuma ação necessária.
	0755	0755	Nenhuma ação necessária.
hp	0644	0640	Conjunto recomendado de permissões
	Permissões atuais	Permissões recomendadas	Ação recomendada

+

Permissões de arquivos
Edição de arquivo PHP
Acesso ao arquivo WP
Logs do sistema hospedeiro

Edição de arquivo

O painel do Wordpress por padrão permite que os administradores editar arquivos PHP, tais como arquivos de plugin e tema. Isso é muitas vezes a primeira ferramenta que um invasor irá usar se for capaz de fazer o login, uma vez que permite a execução de código. Este recurso irá desativar a capacidade para as pessoas editar arquivos PHP através do painel de controle.

Desativar edição de arquivo PHP

Básico

0/10

Desativar a capacidade para editar arquivos PHP:
☒ Marque esta opção se você deseja remover a capacidade de pessoas para editar arquivos PHP através do painel WP

Salvar configurações

Permissões de arquivos

Edição de arquivo PHP

Acesso ao arquivo WP


Logs do sistema hospedeiro


Arquivos WordPress

Esse recurso permite-lhe impedir o acesso a arquivos, como readme.html, license.txt e wp-config-sample.php, que são entregues com todas as instalações WP.

Ao impedir o acesso a esses arquivos que você está escondendo algumas peças-chave de informação (por exemplo, informações de versão do WordPress) dos potenciais hackers.

Impedir o acesso a arquivos padrão do WP

 Básico

 0/10

Impedir o acesso a arquivos de instalação padrão do WP:

☒ Marque esta opção se você deseja impedir o acesso a readme.html, license.txt and wp-config-sample.php.

Salvar configuração

Regras básicas do firewall

Regras adicionais do firewall

Regras do firewall de lista negra 6G

Robôs da internet

Impedir hotlinks

Deteção de intrusões


Proteção de firewall adicional


Este recurso permite que você ative as configurações de firewall mais avançadas para o seu site.

As regras de firewall avançado são aplicadas através da inserção de código especial para seu arquivo .htaccess atualmente ativo.

Devido à natureza do código que está sendo inserido no arquivo .htaccess, esse recurso pode quebrar algumas funcionalidades para certos plugins e, portanto, você é aconselhado a fazer backup antes de fazer qualquer configuração.

Listagem do conteúdo do diretório

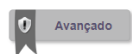
 Intermediário

 0/5

Desabilitar visualizações de índice:

☒ Marque esta opção se você deseja desativar o diretório e lista de arquivos. [+ Mais informação](#)

Rastrear e acompanhar

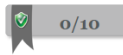
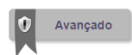


Desabilitar o rastreamento e acompanhamento:

☒ Marque esta opção se você deseja desativar o rastreamento e acompanhamento. [- Mais informação](#)

Ataque de rastreamento HTTP (XST) pode ser usado para retornar solicitações de cabeçalho e cookies de apoio e outras informações.
Esta técnica de hacking é geralmente usado em conjunto com ataques de script entre sites (XSS).
Desabilitação de rastreamento e acompanhamento em seu site irá ajudar a evitar ataques de rastreamento HTTP.

Postagem de comentário proxy



Proibir postagem de comentários de proxy:

☒ Marque esta opção se você deseja proibir postagem de comentários de proxy. [- Mais informação](#)

Essa configuração negará quaisquer solicitações que usam um servidor proxy ao postar comentários.
Proibindo comentários de proxy, você está em efeito, eliminando alguns SPAM e outras solicitações de proxy.

Configurações do firewall

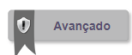
Esse recurso permite que você ative o 6G (ou 5G legado) regras de proteção de segurança de firewall projetado e produzido por [Perishable Press](#).

The 6G Blacklist is an updated and improved version of the 5G Blacklist that is PHP-based and doesn't use a .htaccess file. If you have the 5G Blacklist active, you might consider activating the 6G Blacklist instead.

Lista negra 6G é uma lista negra simples, flexível, que ajuda a reduzir o número de solicitações de URL maliciosas que atingem seu site.

The added advantage of applying the 6G firewall to your site is that it has been tested and confirmed by the people at PerishablePress.com to be an optimal and least disruptive set of security rules for general WP sites.

Configurações de firewall / lista negra 6G



Habilitar proteção de firewall 6G:

☒ Marque esta opção se você deseja aplicar a proteção de firewall de lista negra 6G de perishablepress.com para o seu site. [+ Mais informação](#)

Habilitar proteção de firewall 5G legado:

☒ Marque esta opção se você deseja aplicar a proteção de firewall de lista negra 5G de perishablepress.com para o seu site. [+ Mais informação](#)

[Salvar configurações de firewall 5G/6G](#)

Block DEBUG method:

☒ Check this to block the DEBUG request method

Block MOVE method:

☒ Check this to block the MOVE request method

Block PUT method:

☐ Check this to block the PUT request method [+ Mais informação](#)

Block TRACK method:

☒ Check this to block the TRACK request method

Save request methods settings

6G other settings

Block query strings:

☒ Check this to block all query strings recommended by 6G

Block request strings:

☒ Check this to block all request strings recommended by 6G

Block referrers:

☒ Check this to block all referrers recommended by 6G

Block user-agents:

☒ Check this to block all user-agents recommended by 6G

Save other settings

Configurações 3

Segurança WP

Dashboard

Settings

User Accounts

User Login

User Registration

Database Security

Filesystem Security

Blacklist Manager

Se o seu site permite que as pessoas criem suas próprias contas, este recurso irá definir automaticamente uma conta recém registrada para cada usuário registrado.

Você pode ver todas as contas que foram recentemente registradas no seu site.

Básico

0/20

Habilitar aprovação manual de novos registros:

☐ Marque esta opção para habilitar a aprovação manual de novos registros.

Salvar configurações

Aprovação manual

Captcha em registro


Registration honeypot


Este recurso permite que você adicione uma formulário captcha na página de registro WordPress.

Usuários que tentam registrar também precisará digitar a resposta a uma simples questão de matemática - se entrarem com a resposta errada, o plugin não irá permitir-lhes para se registrar.

Portanto, adicionando um formulário captcha na página de registro é outra técnica de prevenção de registro SPAM eficaz, ainda que simples.

Configurações de captcha na página de registro

 Básico

 0/20


You should set [CAPTCHA settings](#) before activating this feature.


Habilitar captcha na página de registro:

☒ Marque esta opção se você deseja inserir um formulário captcha na página de registro de usuário do WordPress (se você permitir o registro do usuário).

Salvar configurações

Configurações de renomeação da página de login

 Intermediário

 0/10

This feature can lock you out of admin if it doesn't work correctly on your site. Before activating this feature you must read the following [message](#).

NOTE: If you are hosting your site on WPEngine or a provider which performs server caching, you will need to ask the host support people to NOT cache your renamed login page.

Habilitar recurso de renomeação da página de login:

☒ Marque esta opção se você deseja ativar o recurso de renomeação da página de login

URL da página de login:

https://cooperparques.com.br/

Enter a string which will represent your secure login page slug. You are encouraged to choose something which is hard to guess and only you will remember.

Salvar configurações

Renomeação da página de login

Prevenção baseadas em cookies de força bruta

CAPTCHA settings

Lista branca de login

Pote de mel

CAPTCHA settings

This feature allows you to add a CAPTCHA form on various WordPress login pages and forms. Adding a CAPTCHA form on a login page or form is another effective yet simple "Brute Force" prevention technique. You have the option of using either [Cloudflare Turnstile](#), [Google reCAPTCHA v2](#) or a plain maths CAPTCHA form.

We recommend [Cloudflare Turnstile](#) as a more privacy-respecting option than Google reCAPTCHA

Default CAPTCHA:

No CAPTCHA

No CAPTCHA

Cloudflare Turnstile

Google reCAPTCHA V2

Simple math CAPTCHA

Salvar configurações

Básico

0/20

Habilitar captcha na página de login: ☒ Marque esta opção se você deseja inserir um formulário captcha na página de login

Configurações do formulário captcha de senha perdida

Básico

0/10

Habilitar captcha na página senha perdida: ☒ Marque esta opção se você deseja inserir um formulário captcha na página de senha perdida

Configurações personalizadas do formulário captcha de login

Básico

0/20

Habilitar captcha no formulário de login personalizado: ☒ Marque esta opção se você deseja inserir o captcha em um formulário de login personalizado gerado pela seguinte função WP: wp_login_form()

Renomeação da página de login

Prevenção baseadas em cookies de força bruta

CAPTCHA settings

Lista branca de login

Pote de mel

Esse recurso permite que você adicione um campo oculto especial "pote de mel" na página de login do WordPress. Isso só será visível para os robôs e não seres humanos. Desde que os robôs geralmente preencher cada campo de entrada de um formulário de login, eles também apresentará um valor para o campo de pote de mel oculto especial. A maneira de trabalho de potes de mel é que um campo oculto é colocado em algum lugar dentro de uma forma que apenas os robôs irão apresentar. Se esse campo contém um valor quando o formulário é enviado, em seguida, um robô muito provavelmente apresentou a forma e isso consequentemente é tratado com. Portanto, se o plugin detecta que este campo tem um valor quando o formulário de login é enviado, então o robô que está tentando fazer o login para o seu site será redirecionado para seu endereço localhost - http://127.0.0.1.

Configurações do formulário de login pote de mel

Intermediário

0/10

Habilitar pote de mel na página de login: ☒ Marque esta opção se você deseja ativar o recurso pote de mel para a página de login

Salvar configurações

Configurações de SPAM de comentário

Adicionar captcha para formulário de comentários

This feature will add a CAPTCHA field in the WordPress comments form.
Adicionando um campo de captcha no formulário de comentário é uma maneira simples de reduzir grandemente SPAM de comentários de robôs sem usar regras .htaccess.



Básico



0/20

Habilitar captcha em
formulários de comentário:

☒ Marque esta opção se você deseja inserir um campo captcha em formulários o comentário

Bloquear comentários spambot

A large portion of WordPress blog comment spam is mainly produced by automated bots and not necessarily by humans.
Este recurso irá minimizar consideravelmente o tráfego e carga inútil e desnecessário em seu servidor, resultante de comentários de spam, bloqueando todas as solicitações de comentário que não são originários do seu domínio.
Em outras palavras, se o comentário não foi enviado por um ser humano que fisicamente apresentou o comentário em seu site, a solicitação será bloqueada.



Básico



0/10

Bloquear spambots de publicar
comentários:

☒ Marque esta opção se você deseja aplicar uma regra de firewall que irá bloquear comentários provenientes de spambots. [+ Mais informação](#)

Proteção de cópia

Quadros

User enumeration

WP REST API

Salt

Impedir que o seu site seja exibido em um quadro

Esse recurso permite que você impeça que outros sites de exibir qualquer um dos seus conteúdos através de um frame ou iframe.
Quando habilitado, esse recurso irá definir o parâmetro inválido "X-Frame-Options" para "sameorigin" no cabeçalho HTTP.

Habilitar proteção iFrame:

☒ Marque esta opção se você deseja impedir que outros sites exiba seu conteúdo em um frame ou iframe.

Salvar configurações

Proteção de cópia

Quadros

User enumeration

WP REST API

Salt

Evitar enumeração de usuários

Esse recurso permite-lhe evitar externas de usuários/robôs de buscar a informação do usuário com urls como `"/?author=1"`.

Quando habilitado, esse recurso irá imprimir um erro "proibido", em vez das informações do usuário.

Desabilitar enumeração de usuários:

☒ Marque esta opção se você deseja parar com a enumeração de usuários.

Salvar configurações