



# Segurança em WordPress

## *Hardening*

**Para hoje: 01/02/24**

- Introdução ao WordPress: WordPress e sua popularidade como plataforma de gerenciamento de conteúdo;
- Importância da Segurança: especialmente considerando o grande número de sites que usam o WordPress;
- Causas das Ameaças: Escolha de Temas e Plugins InSeguros, Falta de Atualizações;
- Bônus Insight: Configuração de uma Ferramenta de proteção Cloudflare (WAF, CDN antDDoS);

# 1 - INTRO

## *Sobre este talk*

### **Motivação deste Talk?**

Criamos o site do SHC, agora precisamos aplicar segurança no servidor e na aplicação, por que não compartilhar isso com a comunidade?

Além disso:

- **Palestra destinada a desenvolvedores, Agências de Marketing, Comunidade de Segurança e demais interessados.**
- **Case no final: Atendimento a uma agência de Mkt;**

# 1 - INTRO

---

Antes de começar....

**WordPress é totalmente seguro?**

# 1 - INTRO

Antes de começar....

## O que é Hardning?

O "hardening" refere-se ao processo de fortalecimento ou tornar mais resistente um sistema, aplicação, ou infraestrutura contra ameaças de segurança.

O processo de "hardening" é contínuo, pois as ameaças de segurança evoluem ao longo do tempo. Manter sistemas seguros requer monitoramento constante, atualizações regulares e ajustes nas configurações de segurança conforme necessário.

# 2 – ESCOLHENDO A INFRAESTRUTURA DE HOSPEDAGEM

## Opções: VPS ou Host Compartilhado?

**VPS:** Servidor Virtual Privado (VPS) é uma solução de hospedagem que simula um servidor dedicado dentro de um ambiente compartilhado. Em vez de compartilhar um único servidor físico com vários usuários, cada VPS é uma máquina virtual independente que funciona em um servidor físico. Cada VPS tem seu próprio sistema operacional, recursos dedicados e acesso root ou administrativo.

**Host Compartilhado:** vários usuários e suas respectivas contas de hospedagem compartilham os recursos de um único servidor físico. Cada usuário possui sua própria conta isolada, mas todos eles compartilham os mesmos recursos, como CPU, memória RAM, armazenamento e largura de banda. Esse modelo é frequentemente usado em serviços de hospedagem de sites compartilhados, onde várias páginas da web são hospedadas no mesmo servidor.

Hostinger, Hostigator, UOL Hosts, etc.

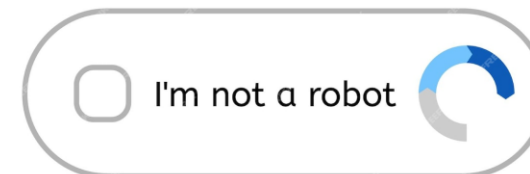
# 3 - MEDIDAS DE SEGURANÇA

## *Principais medidas*

### **Proteção para Formulários**

O termo "CAPTCHA" refere-se a um teste ou desafio projetado para determinar se o usuário é humano ou um programa de computador automatizado, como um bot. CAPTCHA é uma sigla para "Completely Automated Public Turing test to tell Computers and Humans Apart".

O principal objetivo do CAPTCHA é proteger os sites contra atividades automatizadas indesejadas, como registros automáticos de contas, envios automáticos de formulários ou outros tipos de abuso. Geralmente, os CAPTCHAs envolvem tarefas que são fáceis para os seres humanos, mas desafiadoras para os computadores resolverem.



# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Proteção para Formulários de Contato

The screenshot shows the WordPress admin dashboard with a sidebar on the left containing menu items like 'Mídia', 'Páginas', 'Comentários', 'Eventos', 'Blog', 'Contato', 'Formulários de contato', 'Integração', 'Elementor', 'Modelos', 'Essential Addons', 'ElementsKit', 'Aparência', 'Plugins', and 'Usuários'. The 'Contato' menu item is highlighted. The main content area displays two settings cards for 'Proteção anti-spam':

- Akismet**: Os CAPTCHAs são projetados para distinguir spambots de humanos e, portanto, são indefesos contra spammers humanos. Ao contrário dos CAPTCHAs, o Akismet verifica os envios de formulários no banco de dados global de spam; isso significa que o Akismet é uma solução abrangente contra spam. É por isso que consideramos o Akismet a peça central da estratégia de prevenção de spam. [Filtragem de spam com Akismet](#)
- reCAPTCHA**: O reCAPTCHA protege você contra spam e outros tipos de abuso automatizado. Com o módulo de integração reCAPTCHA do Contact Form 7, você pode bloquear envios de formulários abusivos por robôs de spam. [reCAPTCHA \(v3\)](#)  
✓ reCAPTCHA está ativo neste site.  
[Definir integração](#)

The screenshot shows the wpforms website interface. At the top, there is a navigation menu with items: 'Geral', 'E-mail', 'CAPTCHA', 'Validação', 'Pagamentos', 'Integrações', 'Geolocalização', 'Acesso', and 'Diversos'. The 'CAPTCHA' menu item is selected and highlighted. Below the navigation, the heading 'CAPTCHA' is displayed, followed by the text: 'Um CAPTCHA é uma técnica anti-spam que ajuda a proteger o seu site contra spam e abusos, mas permitindo a passagem de pessoas reais c...'. Below this text, there are four selectable options, each with an icon and a label:

- hCaptcha**: Represented by a blue hand icon.
- reCAPTCHA**: Represented by a blue and grey circular arrow icon. This option is currently selected, indicated by an orange border around its box.
- Turnstile**: Represented by an orange cloud icon.
- Nenhum**: Represented by a grey circle with a diagonal slash icon.

# 3 - MEDIDAS DE SEGURANÇA

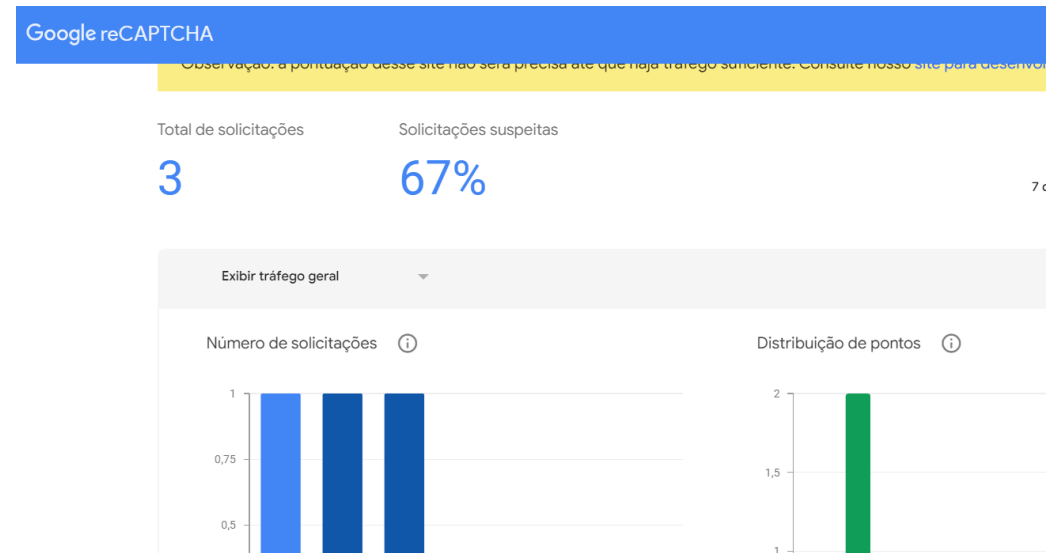
## Principais medidas

### Proteção para Formulários de Contato

<https://www.google.com/recaptcha/about/>

Objetivo: reCAPTCHA V2 é mais focado em verificar a humanidade do usuário no momento da interação, enquanto reCAPTCHA V3 fornece uma pontuação de confiança ao longo do tempo para permitir ações mais personalizadas.

Desafios: V2 apresenta desafios diretos ao usuário, enquanto V3 funciona nos bastidores sem exigir interação explícita





# 3 - MEDIDAS DE SEGURANÇA
















## Principais medidas

### Proteção para comentários

Comentários

Todos (9) | Meu (0) | Pendentes (7) | Aprovados (2) | Spam (0) | Lixo (1)

Ações em massa  Todos os tipos de comentá    9 it

<input type="checkbox"/>	Autor	Comentário	Em resposta para	Enviado em
<input type="checkbox"/>	 Elizabetht myngirls.online ElizabethK3F@gmail.com 46.8.23.243	Content for your website <a href="http://myngirls.online/">http://myngirls.online/</a>	1ª Reunião 2024 – Planejamento Ver Post  	01/02/2024 às 13:14
<input type="checkbox"/>	 Eva ztd.bardou.online/adm EvaPKI@gmail.com 92.119.193.140	Cool website. There is a suggestion <a href="https://ztd.bardou.online/adm">https://ztd.bardou.online/adm</a>	1ª Reunião 2024 – Planejamento Ver Post  	01/02/2024 às 09:56
<input type="checkbox"/>	 Sheilat ztd.bardou.online/adm SheilaBjF@gmail.com 45.90.196.109	I offer mutually beneficial cooperation <a href="https://ztd.bardou.online/adm">https://ztd.bardou.online/adm</a>	1ª Reunião 2024 – Planejamento Ver Post  	01/02/2024 às 04:09
<input type="checkbox"/>	 Juliett ztd.bardou.online/adm JulietrbF@gmail.com 188.130.185.51	SEO Optimizers Team <a href="https://ztd.bardou.online/adm">https://ztd.bardou.online/adm</a>	1ª Reunião 2024 – Planejamento Ver Post  	31/01/2024 às 22:26
<input type="checkbox"/>	 Karent ztd.bardou.online/adm Karengqv@gmail.com 109.248.204.221	Free analysis of your website <a href="https://ztd.bardou.online/adm">https://ztd.bardou.online/adm</a>	1ª Reunião 2024 – Planejamento Ver Post  	31/01/2024 às 16:38



WordPress



nopCommerce



Wikipédia

# 3 - MEDIDAS DE SEGURANÇA

## *Principais medidas*

**Dilema das atualizações:**

**Atualização automática ou não?**

Com as atualizações automáticas, se houver algum erro de compatibilidade entre plugins ou com o *template*, você só vai ficar sabendo quando acessar o site. E se isso demorar...

# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Atualização de Plugins

Plugins [Adicionar plugin](#) Opções de tela ▾ Ajuda ▾

Todos (19) | Ativos (18) | Desativado (1) | Indispensável (1) | Atualizações automáticas desativadas (19)

Ações em massa ▾ [Aplicar](#) 19 itens

<input type="checkbox"/>	Plugin	Descrição	Atualizações automáticas
<input type="checkbox"/>	<b>All-in-One WP Migration</b> <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Ferramenta de migração para todos os seus dados do blog. Importe ou exporte o conteúdo do seu blog com um único clique. Versão 7.79   Por <a href="#">ServMask</a>   <a href="#">Ver detalhes</a>   <a href="#">Contate o Suporte</a>   <a href="#">Traduzir</a>	<a href="#">Ativar atualizações automáticas</a>
<input type="checkbox"/>	<b>Contact Form 7</b> <a href="#">Configurações</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Só mais um plugin de formulário de contato. Simples, mas flexível. Versão 5.8.6   Por <a href="#">Takayuki Miyoshi</a>   <a href="#">Ver detalhes</a>	<a href="#">Ativar atualizações automáticas</a>
<input type="checkbox"/>	<b>Custom Post Type UI</b> <a href="#">Sobre</a>   <a href="#">Ajuda</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Admin UI panel for registering custom post types and taxonomies Versão 1.15.1   Por <a href="#">WebDevStudios</a>   <a href="#">Ver detalhes</a>	<a href="#">Ativar atualizações automáticas</a>
<input type="checkbox"/>	<b>Duplicate Page</b> <a href="#">Configurações</a>   <a href="#">Doar</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Duplicate posts, páginas e posts personalizados com um único clique. Versão 4.5.3   Por <a href="#">mndpsingh287</a>   <a href="#">Ver detalhes</a>	<a href="#">Ativar atualizações automáticas</a>
<input type="checkbox"/>	<b>Elementor</b> <a href="#">Configurações</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>   <a href="#">Obter o Elementor Pro</a>	O construtor de sites Elementor tem tudo: construtor de páginas do tipo arrastar e soltar, design perfeito em pixels, edição responsiva para dispositivos móveis e muito mais. Comece agora! Versão 3.19.0   Por <a href="#">Elementor.com</a>   <a href="#">Ver detalhes</a>   <a href="#">Documentação e perguntas frequentes</a>   <a href="#">Tutoriais em</a>	<a href="#">Ativar atualizações automáticas</a>

# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Atualização de Plugins

Plugins [Adicionar plugin](#)

**A versão foi atualizada!**  
Encontrando problemas após atualizar a versão? Não se preocupe - reunimos todas as correções para resolução de problemas comuns. [Encontre uma solução](#)

Todos (19) | Ativos (18) | Desativado (1) | Indispensáveis (2)

Ações em massa [Aplicar](#)

Plugin	Descrição
<input type="checkbox"/> All-in-One WP Migration <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Ferramenta de migração para todos os seus dados do blog. Importe ou exporte o conteúdo do seu blog com um único clique. Versão 7.79   Por ServMask   <a href="#">Ver detalhes</a>   <a href="#">Contate o Suporte</a>   <a href="#">Traduzir</a>
<input checked="" type="checkbox"/> Contact Form 7 <a href="#">Configurações</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	Só mais um plugin de formulário de contato. Simples, mas flexível. Versão 5.8.6   Por Takayuki Miyoshi   <a href="#">Ver detalhes</a>
<input type="checkbox"/> Custom Post Type UI <a href="#">Sobre</a>   <a href="#">Ajuda</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	
<input type="checkbox"/> Duplicate Page <a href="#">Configurações</a>   <a href="#">Doar</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	
<input type="checkbox"/> Elementor <a href="#">Configurações</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>   <a href="#">Obter o Elementor Pro</a>	
<input type="checkbox"/> Elementor Header & Footer Builder <a href="#">Settings</a>   <a href="#">Desativar</a>   <a href="#">Traduzir</a>	
<input type="checkbox"/> ElementsKit Lite <a href="#">Desativar</a>   <a href="#">Traduzir</a>   <a href="#">Settings</a>   <a href="#">Go Premium</a>	
<input type="checkbox"/> Essential Addons for Elementor	

### Habilitar manualmente:

<https://www.wowf.com.br/como-configurar-atualizacao-automatica-do-wordpress.html>



Início **Sites** Hospedagem E-mails Domínios VPS Faturas



### Configurações das atualizações automáticas

#### Atualizações automáticas para temas, plugins e para o software WordPress

DESABILITADO

Nosso sistema atualizará automaticamente todas as versões mais recentes disponíveis do núcleo do WordPress, temas e plugins. Recomendamos mantê-los sempre atualizados para garantir a segurança do seu site.

Ativar atualizações automáticas

[Ocultar configurações avançadas](#)

Configurações das atualizações automáticas do software WordPress

Não atualizar

Configurações das atualizações automáticas de temas

Não atualizar

Configurações das atualizações automáticas de plugins

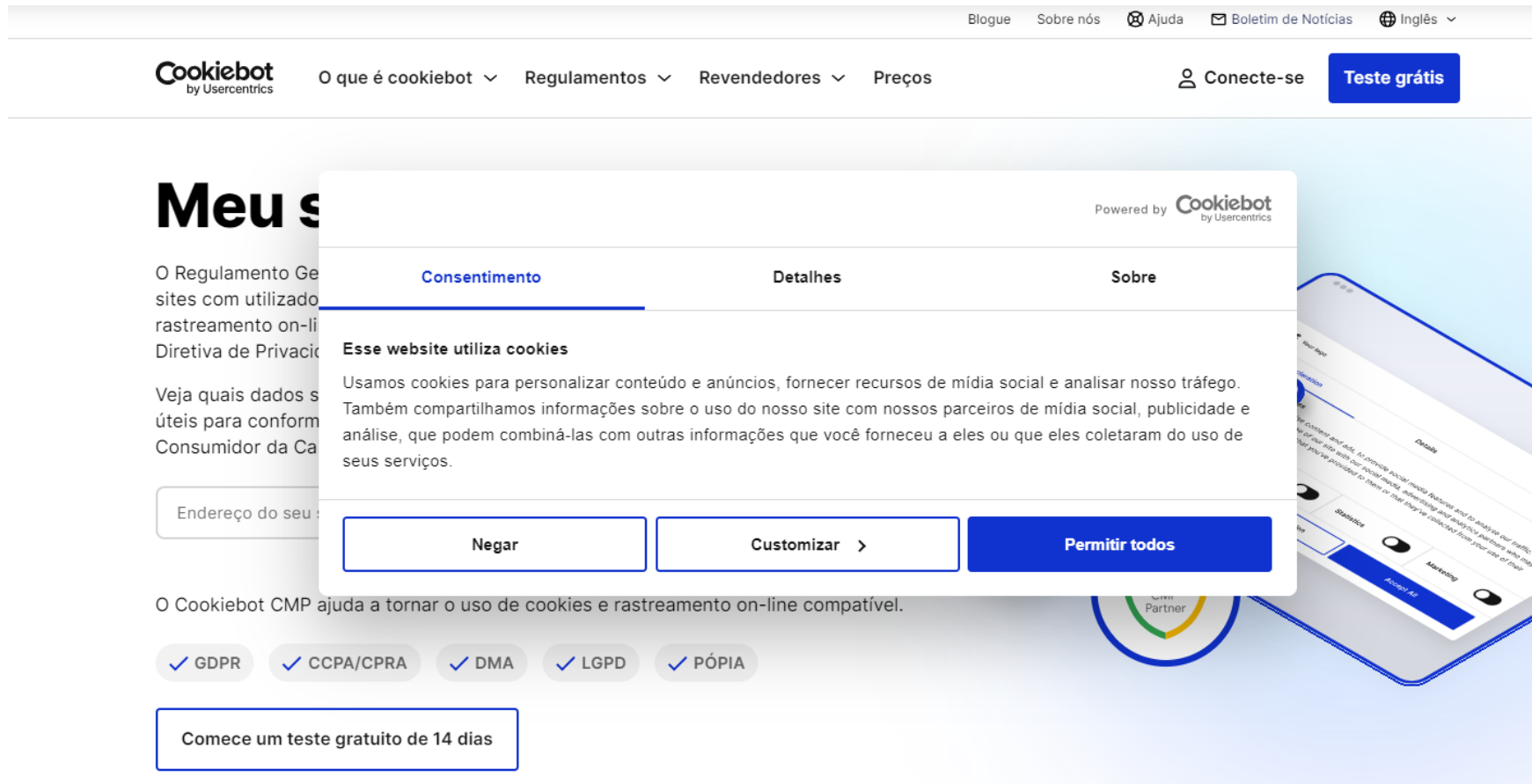
Não atualizar

Aplicar configurações

# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Consentimento de cookies



The screenshot displays the Cookiebot website interface. At the top, there is a navigation bar with links for 'Blogue', 'Sobre nós', 'Ajuda', 'Boletim de Notícias', and 'Inglês'. Below this, the Cookiebot logo and navigation menu are visible, including 'O que é cookiebot', 'Regulamentos', 'Revendedores', and 'Preços'. A 'Conecte-se' button and a 'Teste grátis' button are also present.

The main content area features a large heading 'Meu s' and a sub-heading 'O Regulamento Ge... sites com utilizado... rastreamento on-li... Diretiva de Privaci...'. Below this, there is a section titled 'Veja quais dados s... úteis para conform... Consumidor da Ca...'. A search bar with the placeholder 'Endereço do seu...' is visible.

The central focus is a white modal window titled 'Esse website utiliza cookies'. It contains the following text: 'Usamos cookies para personalizar conteúdo e anúncios, fornecer recursos de mídia social e analisar nosso tráfego. Também compartilhamos informações sobre o uso do nosso site com nossos parceiros de mídia social, publicidade e análise, que podem combiná-las com outras informações que você forneceu a eles ou que eles coletaram do uso de seus serviços.' At the bottom of the modal, there are three buttons: 'Negar', 'Customizar >', and 'Permitir todos'.

Below the modal, there is a section titled 'O Cookiebot CMP ajuda a tornar o uso de cookies e rastreamento on-line compatível.' followed by a row of compliance icons: 'GDPR', 'CCPA/CPRA', 'DMA', 'LGPD', and 'PÓPIA'. A 'Comece um teste gratuito de 14 dias' button is located at the bottom of the page.

# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Política de Privacidade

/chat.openai.com/c/d64cecd6-7325-43fa-ae74-83abae161435



ChatGPT 3.5 ▾

#### POLÍTICA DE PRIVACIDADE

**Data de Vigência:** [Inserir data de vigência]

Bem-vindo à [Nome da Empresa ou Site] ("Nós", "Nosso", ou "Empresa"). Esta Política de Privacidade descreve como coletamos, usamos, compartilhamos e protegemos as informações pessoais dos usuários ("Usuários" ou "Você") em nosso site [[www.seusite.com](http://www.seusite.com)] ("Site") e em nossos serviços relacionados.

#### 1. INFORMAÇÕES QUE COLETAMOS:

##### 1.1. Informações de Identificação Pessoal:

- Nome
- Endereço de e-mail
- Número de telefone



# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Cabeçalhos Adição de Segurança Remoção dos *Disclosure*

Cabeçalhos de segurança HTTP são instruções adicionadas às respostas HTTP pelos servidores web para ajudar a reforçar a segurança do aplicativo web. Esses cabeçalhos fornecem diretrizes aos navegadores sobre como lidar com o conteúdo e interações com o site, ajudando a prevenir diversas vulnerabilidades e ataques. Aqui estão alguns cabeçalhos de segurança comuns:

- Content Security Policy (CSP)
- Strict-Transport-Security (HSTS)
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- Referrer-Policy
- Feature-Policy
- Expect-CT

Por plugin ou outra ferramenta externa como  
Cloudflare

```
(chucky@ DESKTOP-U2VUPRK) - [~]
$ curl -I https://sucurihc.org
HTTP/2 200
date: Sat, 03 Feb 2024 12:51:13 GMT
content-type: text/html; charset=UTF-8
link: <https://sucurihc.org/wp-json/>; rel="https://ap
link: <https://sucurihc.org/wp-json/wp/v2/pages/23>; r
link: <https://sucurihc.org/>; rel=shortlink
cf-cache-status: DYNAMIC
report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.comIi%2Fxn8aqZ7rhyd4GNqK36g4JjToj29sc%2Fihu393A0wCDt%2FV:604800}
nel: {"success_fraction":0,"report_to":"cf-nel","max_a
x-frame-options: 1
server: cloudflare
cf-ray: 84facdd9eba32553-GIG
alt-svc: h3=":443"; ma=86400
```

# 3 - MEDIDAS DE SEGURANÇA

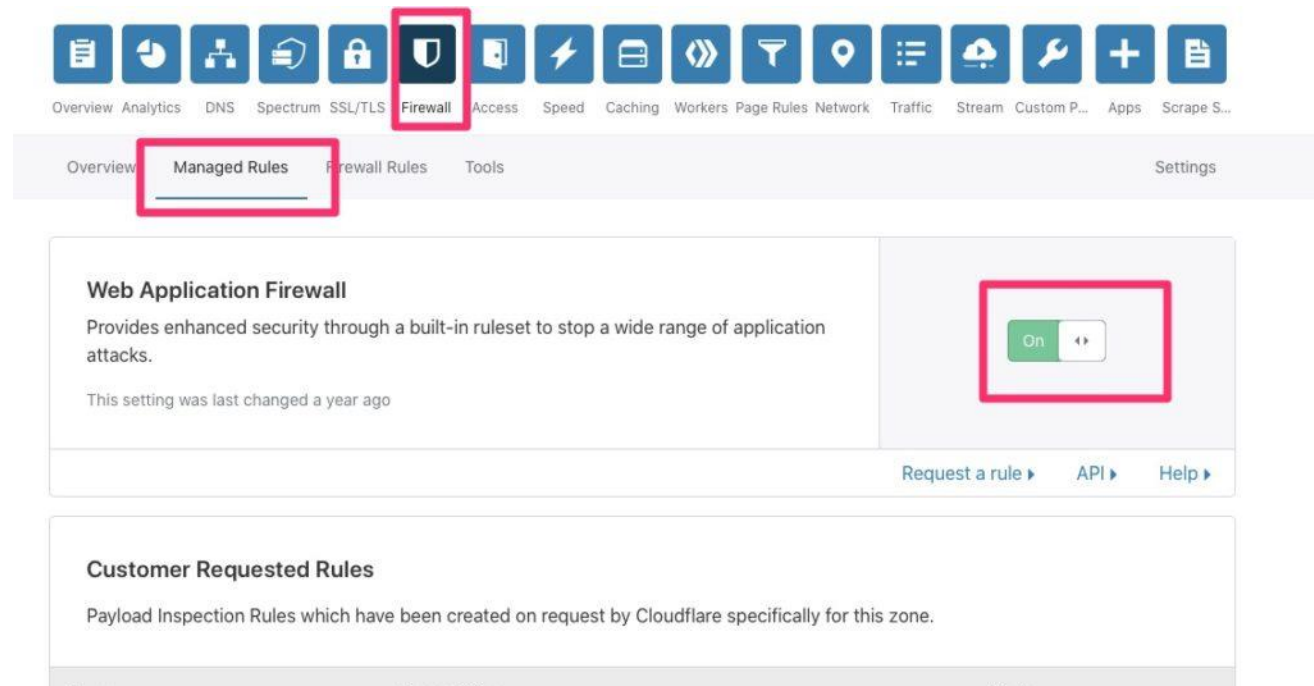
## Principais medidas

### WAF

O WAF (Web Application Firewall) é uma solução de segurança que protege aplicativos web contra diversas ameaças online, como ataques de injeção de SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), entre outros. O principal objetivo de um WAF é filtrar, monitorar e bloquear o tráfego HTTP que chega ao aplicativo web, com foco na proteção das camadas de aplicação.

Por plugin e/ou outra ferramenta externa como Cloudflare

Recomendado: Defender





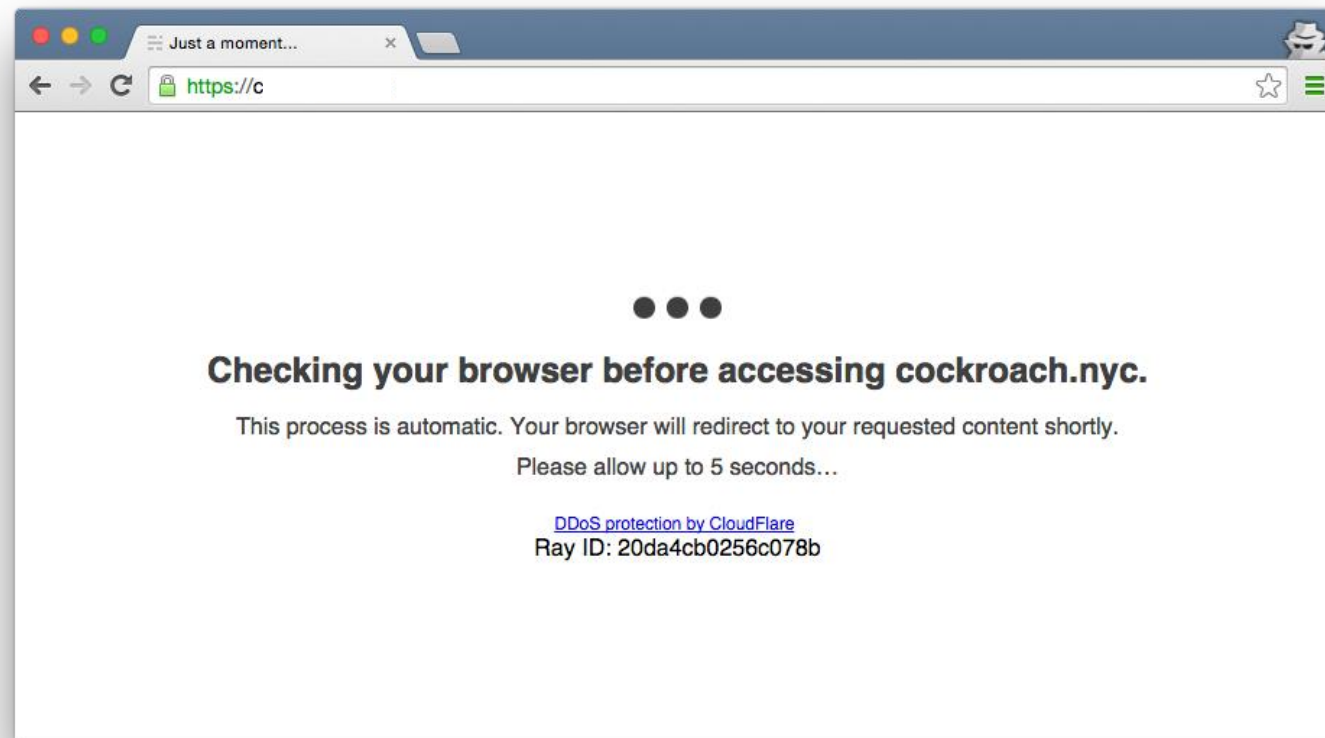
# 3 - MEDIDAS DE SEGURANÇA

## *Principais medidas*

### Proteção contra DoS/DDoS

A proteção contra *DDoS* (*Distributed Denial of Service*) é crucial para garantir a disponibilidade e o desempenho de um site ou serviço online, protegendo contra ataques que buscam sobrecarregar a infraestrutura do servidor. Aqui estão algumas estratégias e tecnologias comumente utilizadas para proteção contra DDoS:

Recomendado: Cloudflare



# 3 - MEDIDAS DE SEGURANÇA

## Principais medidas

### Bruteforce


Bruteforce, ou ataque de força bruta, é uma técnica utilizada em segurança da informação e hacking para tentar quebrar a senha de um sistema, conta ou criptografia através da tentativa exaustiva de todas as combinações possíveis. Esse método envolve testar sistematicamente todas as combinações de senhas até encontrar a correta.

### Proteção contra Bruteforce:


- Evita consumo de recursos do servidor/aplicação;
- Evita possibilidade de acesso indevido a aplicação;

### Recomendado:

- Plugin Limit Login Attempts



The screenshot displays the 'Limit Login Attempts' plugin interface. On the left is a dark sidebar menu with the following items: 'Limit Login Attempts' (highlighted), 'Painel de controle', 'Configurações', 'Logs', 'Depurar', 'Ajuda', and 'Premium'. The main content area shows a title 'Tentativas de acesso que falharam, por país' and a subtitle 'Rede Global (usuário)'. Below this is a table with two columns: 'País' and 'Attempts'.

País	Attempts
 United States	169.039
 China	153.612
 Germany	92.670

# 3 - MEDIDAS DE SEGURANÇA

## *Principais medidas – Fechamento*

Seguem as outras recomendações, algumas foram apresentação.

Recomendações de *Hardning*, podem ser aplicadas usando o Plugin defender, outros plugins e ferramentas instaladas no server, como:

- Alterar página de Login para uma página não preditiva - Defender;
- Alterar estrutura de diretórios do WP, é uma das técnicas para mascarar que a aplicação não é WP (lembrando que sempre será possível para saber de alguma forma);
- Proteção contra scanner de diretórios (bloquear IP de origem para erros 404) plugin apresentado foi o Defender e Redirection para logs – Inteligência de ameaças;
- Uso de um HIDS no server, como exemplo o OSSEC;
- Uso de ferramenta para monitorar os Logs da aplicação.