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

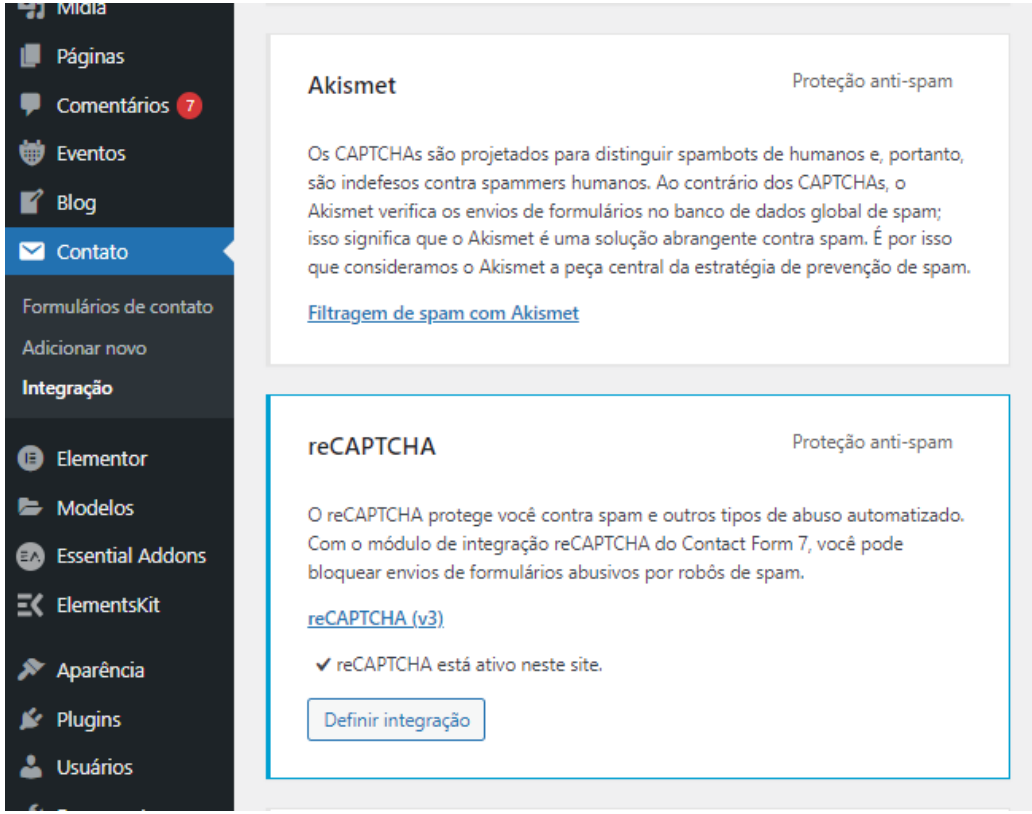
O termo "CAPTCHA" refere-se a um teste ou desafio projetado para determinar se o usuário é humano ou um programa de computador automatizado, como um bot. CAPTCHA é uma sigla para "Completely Automated Public Turing test to tell Computers and Humans Apart".

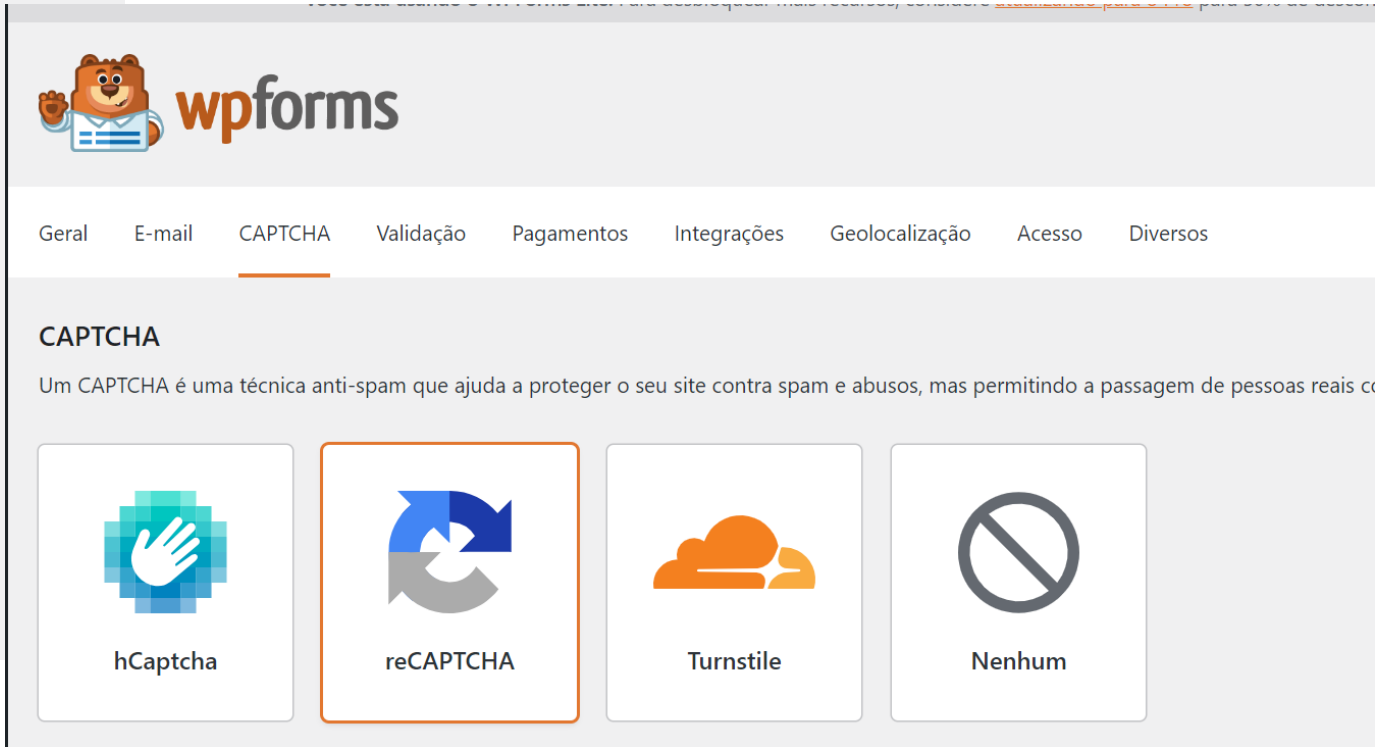
O principal objetivo do CAPTCHA é proteger os sites contra atividades automatizadas indesejadas, como registros automáticos de contas, envios automáticos de formulários ou outros tipos de abuso. Geralmente, os CAPTCHAs envolvem tarefas que são fáceis para os seres humanos, mas desafiadoras para os computadores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

3 - MEDIDAS DE SEGURANÇA

Principais medidas

Proteção para Formulários de Contato





3 - MEDIDAS DE SEGURANÇA

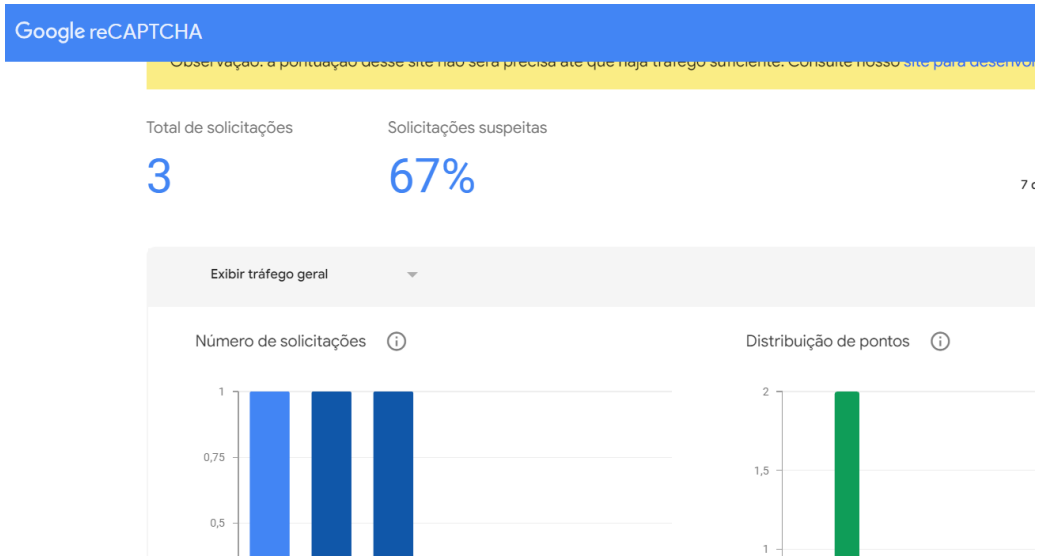
Principais medidas

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.

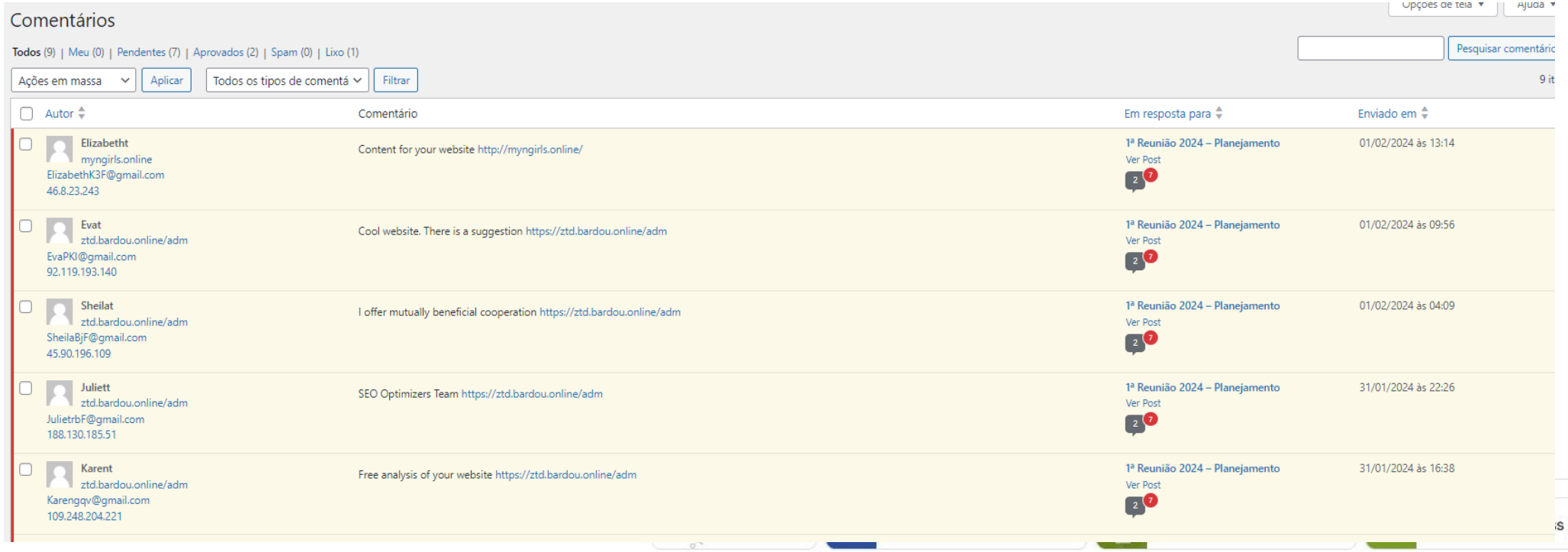
Desafios: V2 apresenta desafios diretos ao usuário, enquanto V3 funciona nos bastidores sem exigir interação explícit



3 - MEDIDAS DE SEGURANÇA

Principais medidas

Proteção para comentários



3 - MEDIDAS DE SEGURANÇA

Principais medidas

Dilema das atualizações:

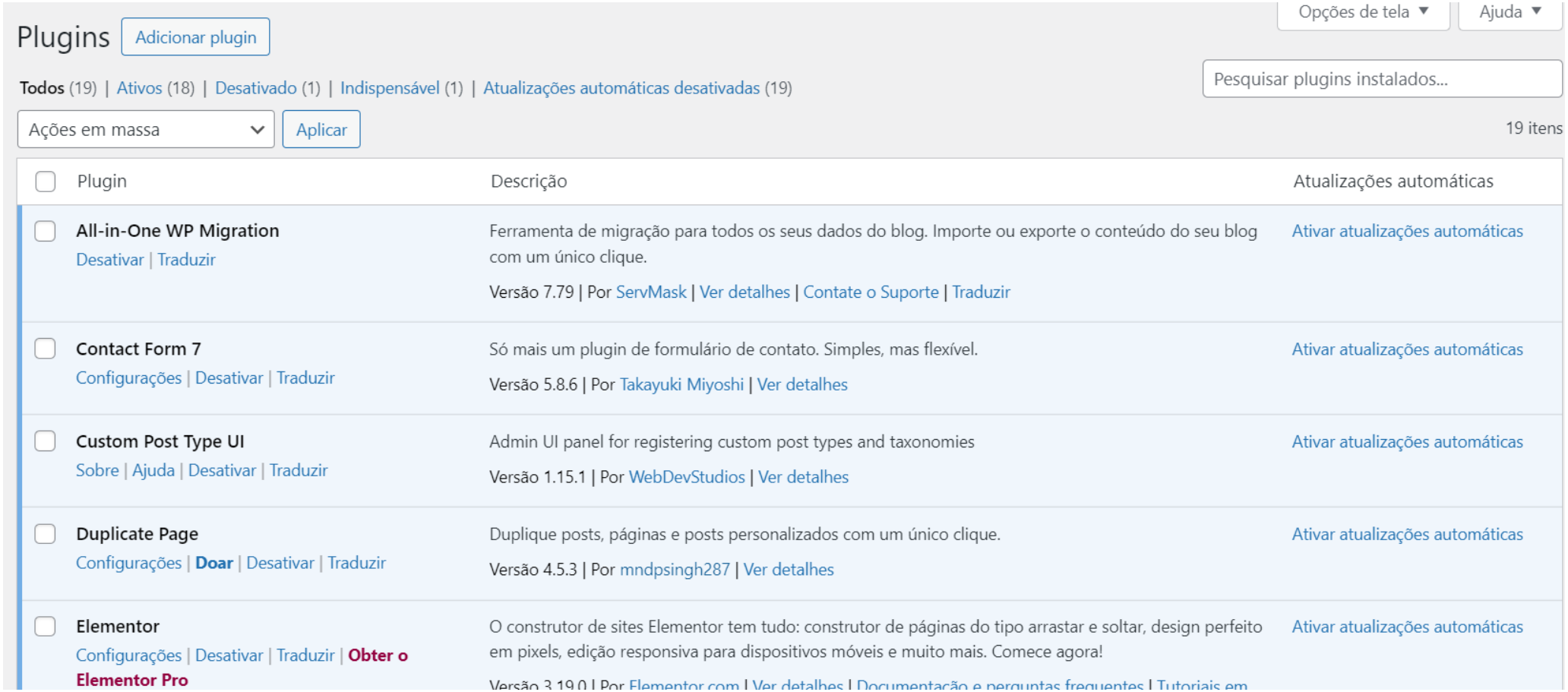
Atualização automática ou não?

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

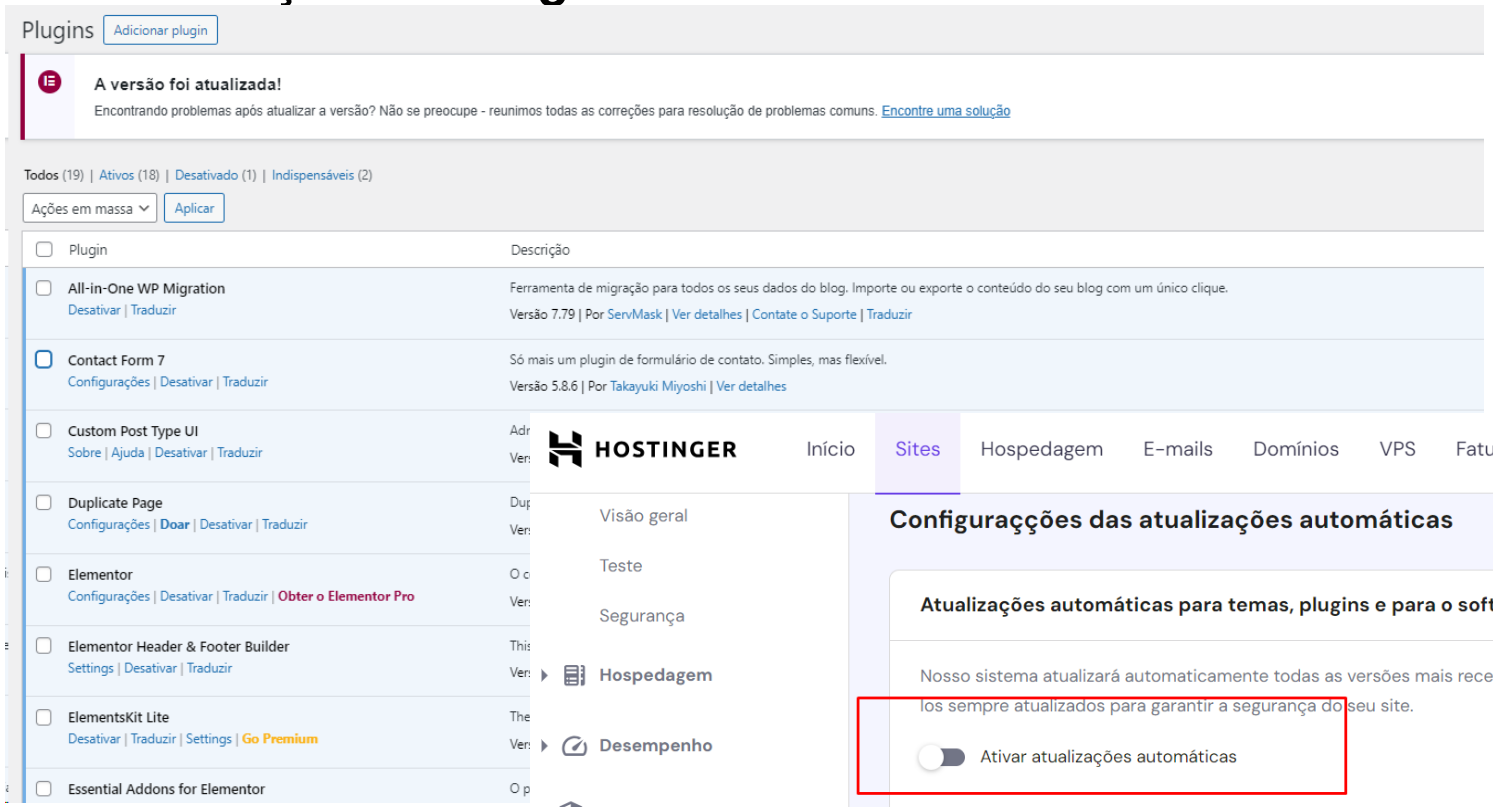
Atualização de Plugins

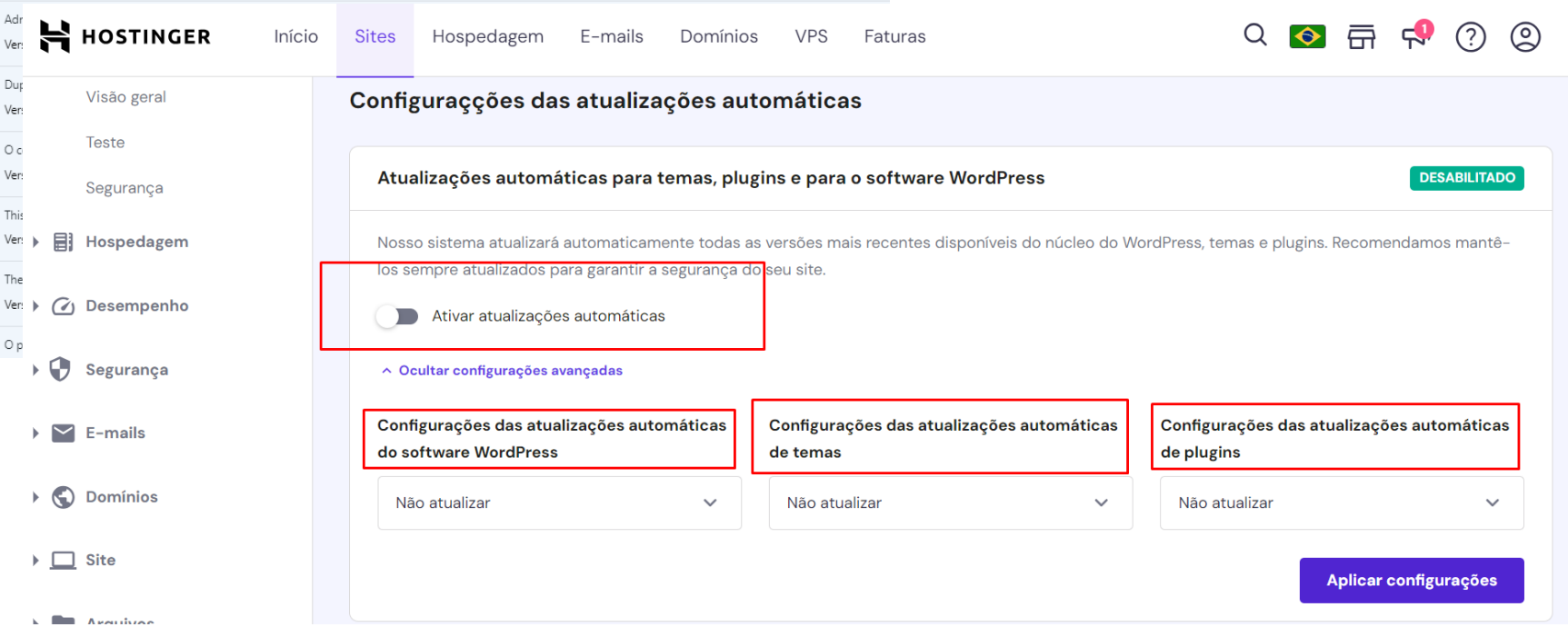


3 - MEDIDAS DE SEGURANÇA

Principais medidas

Atualização de Plugins





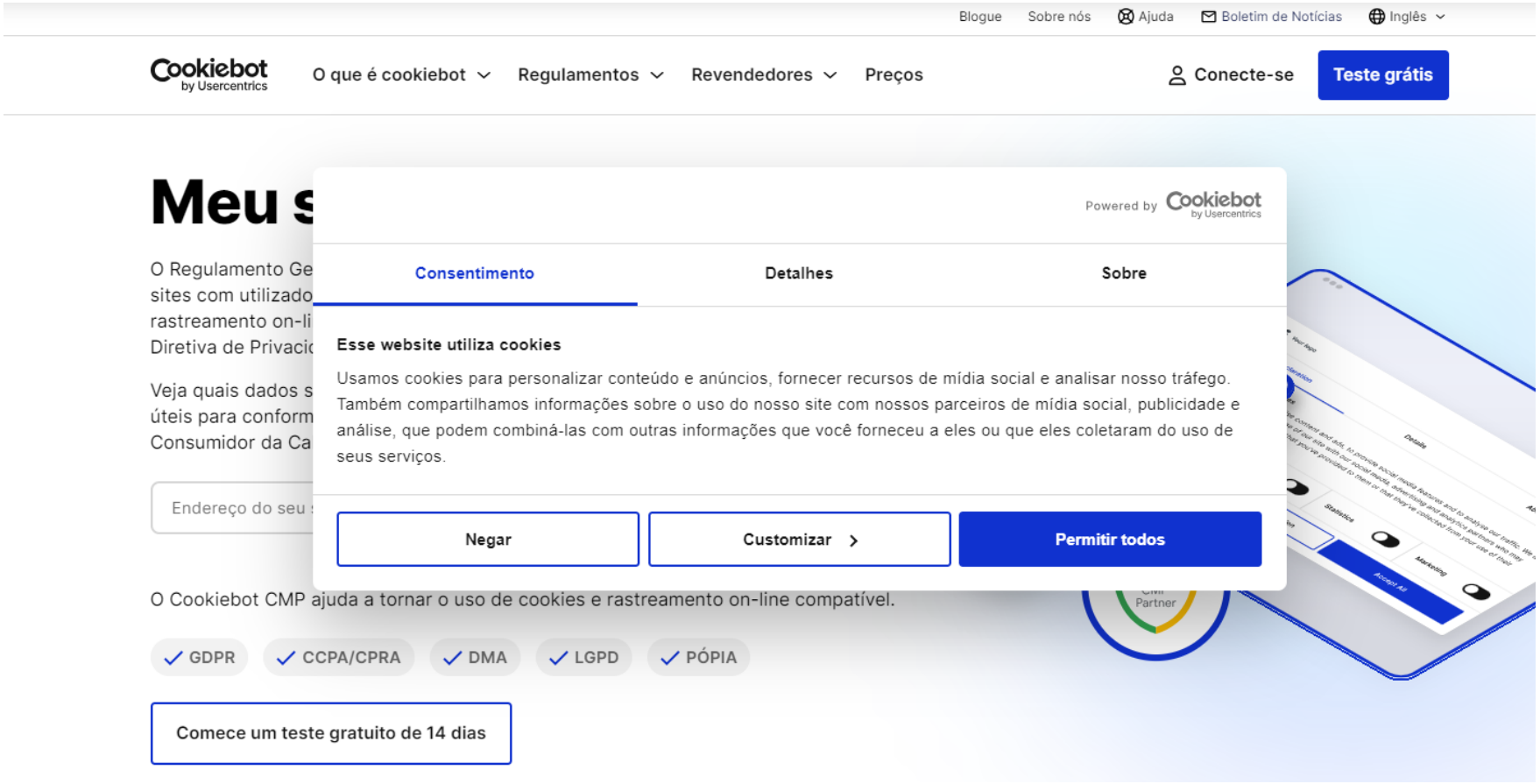
Habilitar manualmente:

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

3 - MEDIDAS DE SEGURANÇA

Principais medidas

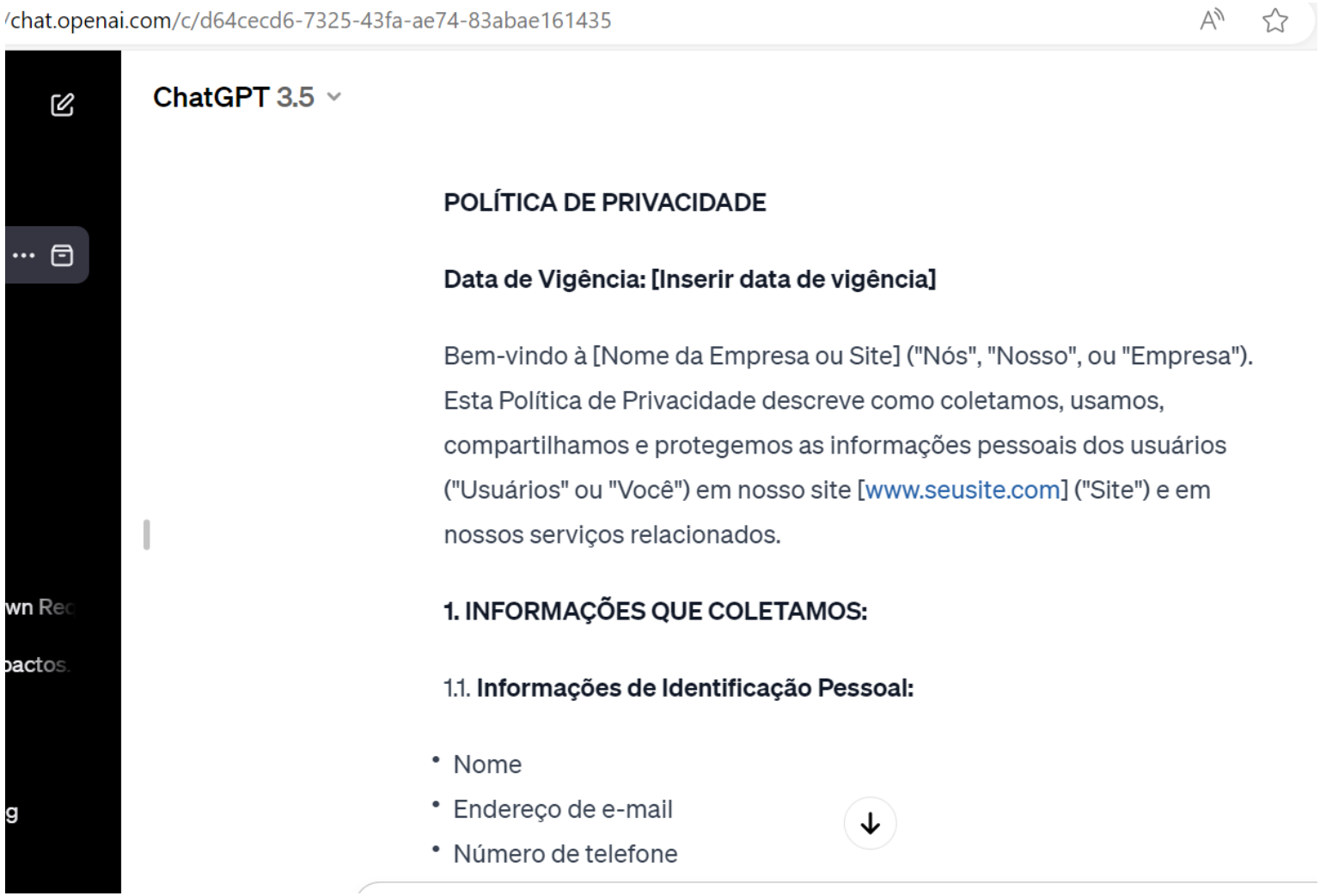
Consentimento de cookies



3 - MEDIDAS DE SEGURANÇA

Principais medidas

Política de Privacidade



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.cloud
mIi%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
```

SUCURIHC H4Ck3r Space

TLP:CLEAR

3 - MEDIDAS DE SEGURANÇA

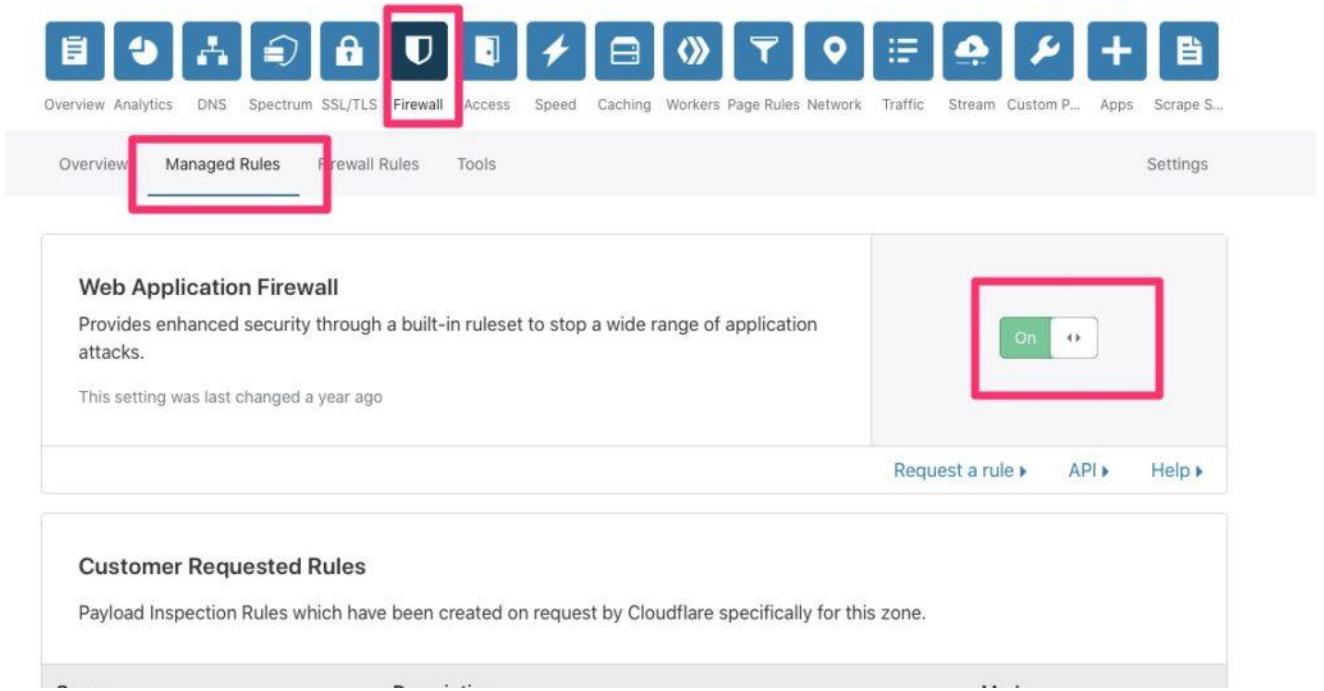
Principais medidas

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



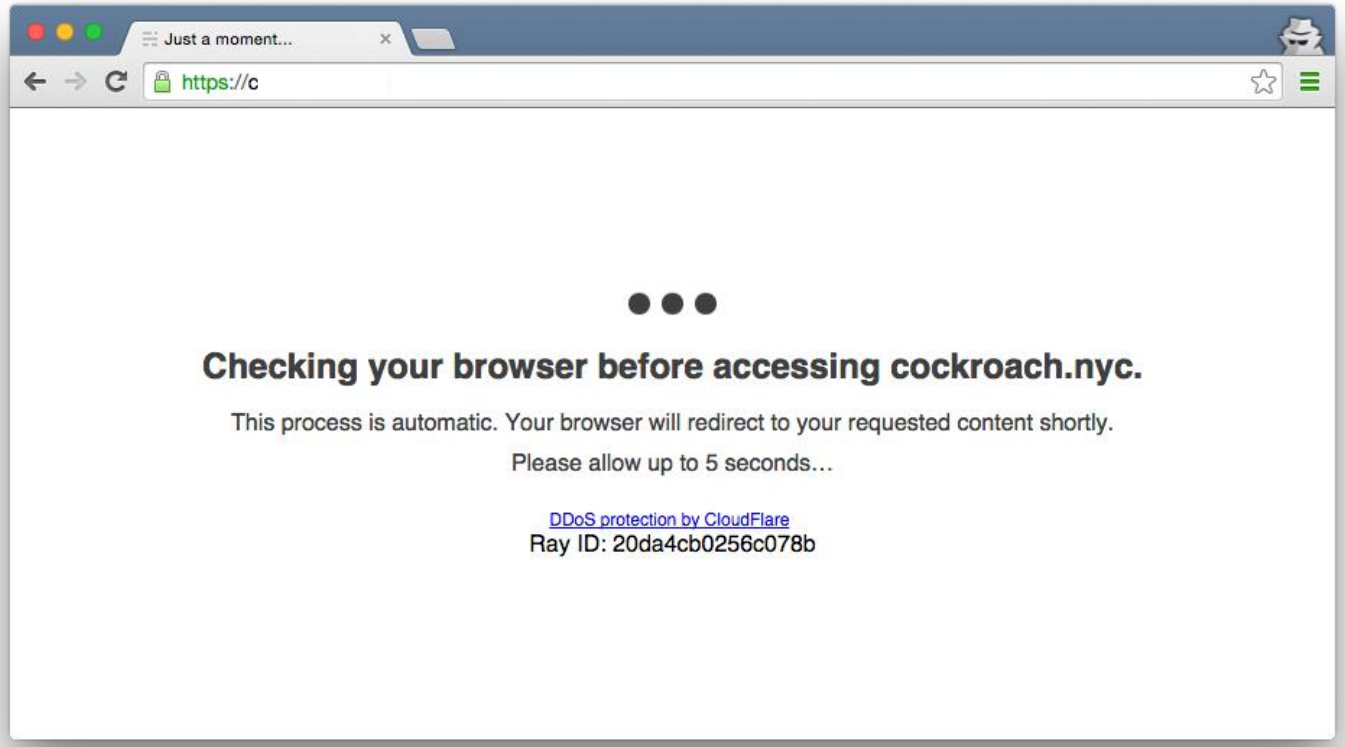
3 - MEDIDAS DE SEGURANÇA

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

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 mascaras que a aplicação não é WP (lembrando que sempre será possível para saber de alguma forma);
- Proteção contra scaner 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.