O Guia Definitivo para Proteger Sites de Clientes

KINSTA

Para a versão sempre atualizada, por favor scaneie o código QR acima ou vá para:
https://www.kinsta.com/pt/ebooks

Publicado por KINSTA

O Guia Definitivo para Proteger Sites de Clientes

Conteúdo

O Guia Definitivo para Proteger Sites de Clientes

De acordo com as estatísticas da Internet, mais de 100.000 sites são hackeados todos os dias. 😮 É por isso que é tão importante levar algum tempo e seguir as seguintes recomendações abaixo sobre como melhor reforçar a sua segurança WordPress.

Quando se trata de segurança do WordPress, há muito mais do que apenas bloquear o seu site, embora nós lhe daremos as melhores recomendações sobre como fazer isso abaixo

Invista em Hospedagem Segura de WordPress

Vamos começar com a segurança a nível de servidor web, pela qual a sua hospedagem WordPress é responsável. É muito importante que você escolha um host no qual possa confiar o seu negócio à medida que você transfere os sites dos seus clientes para eles.

Se você está hospedando o WordPress em seu próprio VPS, então você precisa ter o conhecimento técnico para fazer essas coisas você mesmo. Mas, para ser honesto, tentar ser um administrador de sistema para economizar US$ 20/mês não é uma maneira eficaz de administrar um negócio.

O endurecimento do servidor é a chave para manter um ambiente WordPress totalmente seguro. São necessárias várias camadas de medidas de segurança a nível de hardware e software para garantir que a infra-estrutura de TI que hospeda os sites WordPress seja capaz de se defender contra ameaças sofisticadas, tanto físicas como virtuais.

Por esta razão, os servidores que hospedam WordPress devem ser atualizados com o mais recente sistema operacional e software (de segurança), bem como cuidadosamente testados e verificados quanto a vulnerabilidades e malware.

Também devem existir firewalls e sistemas de detecção de intrusão a nível de servidor para manter os sites dos seus clientes bem protegidos, mesmo durante as fases de instalação do WordPress e construção do site. No entanto, todos os softwares instalados na máquina destinados a proteger o conteúdo do WordPress devem ser compatíveis com os mais recentes sistemas de gerenciamento de banco de dados para manter um ótimo desempenho. O servidor também deve ser configurado para usar uma rede segura e protocolos de criptografia de transferência de arquivos (como SFTP em vez de FTP) para esconder o conteúdo sensível de intrusos maliciosos.

Nós usamos a plataforma Google Cloud aqui na Kinsta para todos os nossos clientes WordPress para garantir uma hospedagem WordPress segura. A segurança está incorporada em nossa arquitetura desde o início e é um método muito mais seguro do que outros disponíveis hoje.

Use a Versão Mais Recente do PHP

PHP é a espinha dorsal de qualquer site WordPress, por isso é muito importante ter a certeza que os sites dos seus clientes estão a usar a última versão no seu servidor. Cada versão principal do PHP é tipicamente totalmente suportada por dois anos após o seu lançamento.

Durante esse tempo, bugs e questões de segurança são corrigidos regularmente. A partir de hoje, qualquer pessoa rodando na versão PHP 7.1 ou inferior não tem mais suporte de segurança e está exposta a vulnerabilidades de segurança não corrigidas.

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
7.2	30 Nov 2017	*2 years, 2 months ago*	30 Nov 2019	*2 months ago*	30 Nov 2020	*in 9 months*
7.3	6 Dec 2018	*1 year, 2 months ago*	6 Dec 2020	*in 9 months*	6 Dec 2021	*in 1 year, 9 months*
7.4	28 Nov 2019	*2 months ago*	28 Nov 2021	*in 1 year, 9 months*	28 Nov 2022	*in 2 years, 9 months*

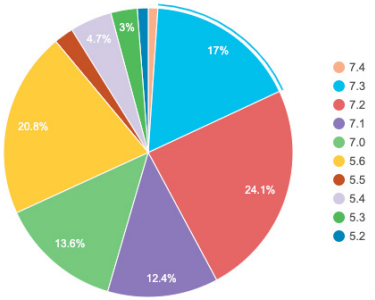
Or, visualised as a calendar:

Key

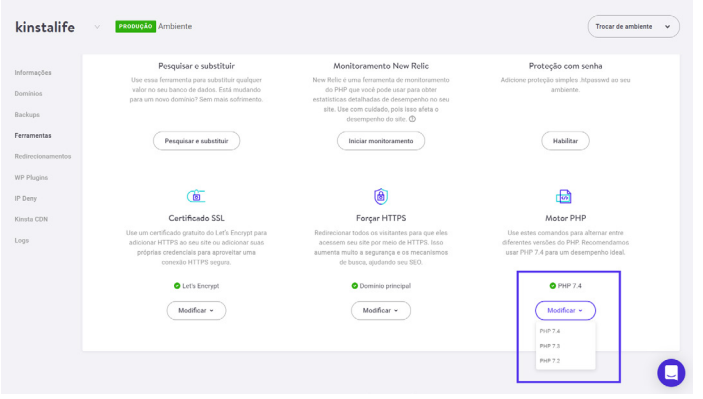
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

E adivinhe o quê? De acordo com a página oficial de Estatísticas do WordPress, cerca de 34% dos usuários do WordPress ainda estão no PHP 5.6 ou inferior, o que significa que mais de um terço dos usuários estão atualmente usando versões do PHP que não são mais suportadas. Isso é assustador!

Versões do PHP



Aqui na Kinsta só recomendamos o uso de versões estáveis e suportadas do PHP, incluindo 7.2, 7.3, e 7.4. PHP 5.6, 7.0, e 7.1 foram eliminados gradualmente. Você pode até alternar entre versões do PHP com um clique de um botão dentro do seu painel MyKinsta.



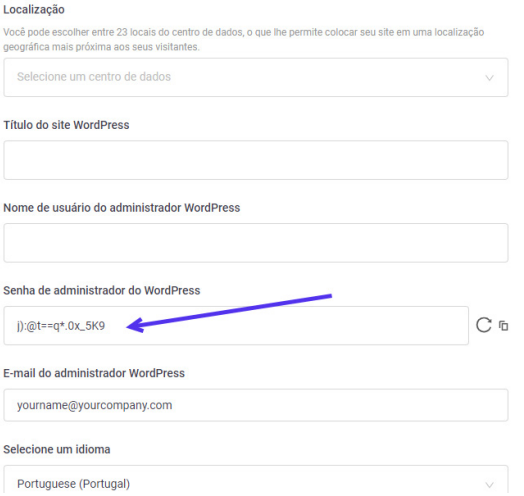
Se quiser experimentar você mesmo, vá ao demo.kinsta.com e experimente!

Use Nomes de Usuário e Senhas Inteligentes

Surpreendentemente, uma das melhores formas de reforçar a sua segurança WordPress é simplesmente usar nomes de utilizador e palavras-passe inteligentes. Parece muito fácil, certo? Bem, confira a lista anual da SplashData de 2019 das senhas mais populares roubadas ao longo do ano (ordenadas por ordem de popularidade).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

A senha mais popular é “123456”. Esta é uma das razões porque aqui na Kinsta no novo instalador do WordPress, na verdade forçamos uma senha complexa a ser usada para qualquer login wp-admin de seus clientes (como visto abaixo no nosso processo de instalação com um clique). Isto não é opcional.



Confira esta funcionalidade com a demonstração do MyKinsta.

O núcleo da função wp_hash_password do WordPress utiliza a estrutura de hashing de senha phpass e oito passes de hashing baseado em MD5. E no que diz respeito à sua instalação do WordPress, você nunca deve usar o nome de usuário padrão "admin" nos sites de seus clientes, em vez de criar nomes de usuário WordPress únicos para suas contas de administrador.

Também é importante usar senhas diferentes para cada site cliente. A melhor forma de as guardar é localmente numa base de dados encriptada no seu computador.

Uma boa ferramenta gratuita para isto é o KeePass. Se você não quiser ir por este caminho, há também gerenciadores de senhas online, como o 1Password ou o LastPass.

Use Sempre a Versão mais Recente do WordPress, Plugins e Temas

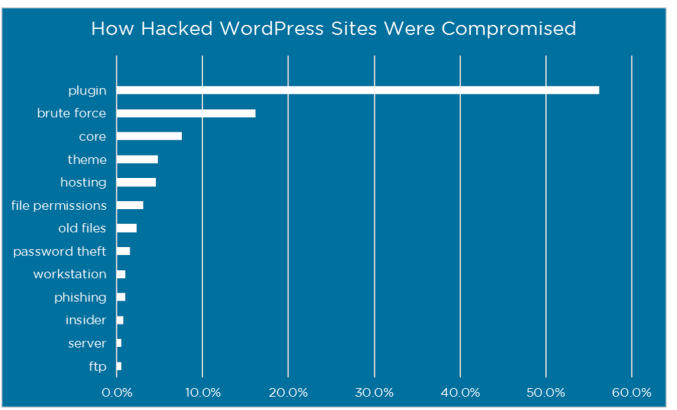
Outra forma muito importante de reforçar a segurança dos sites dos seus clientes é mantê-los sempre atualizados. Isto inclui o núcleo do WordPress, plugins e temas. Estes são atualizados por uma razão, e muitas vezes incluem melhorias de segurança e correções de bugs.

Infelizmente, milhões de empresas por aí, estão rodando versões desatualizadas de software WordPress e plugins, e ainda acreditam

que estão no caminho certo do sucesso empresarial. Eles citam razões para não atualizar, tais como “seu site vai quebrar” ou “as modificações do núcleo vão desaparecer” ou “o plugin X não vai funcionar” ou “eles simplesmente não precisam da nova funcionalidade”.

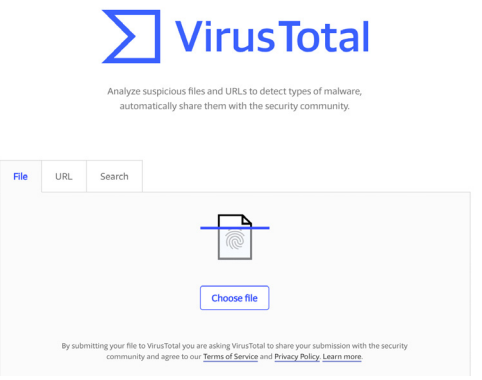
Na verdade, os sites quebram principalmente por causa de bugs em versões mais antigas do WordPress. As modificações principais nunca são recomendadas pela equipe do WordPress e por desenvolvedores especialistas que entendem os riscos envolvidos. E as atualizações do WordPress incluem, em sua maioria, patches de segurança obrigatórios, juntamente com a funcionalidade adicional necessária para executar os plugins mais recentes.

Você sabia que foi relatado que as vulnerabilidades dos plugins representam 55,9% dos pontos de entrada conhecidos para os hackers? Foi isso que o WordFence encontrou em um estudo onde entrevistaram mais de 1.000 proprietários de sites WordPress que haviam sido vítimas de ataques. Ao atualizar seus plugins, você pode garantir melhor que não seja uma dessas vítimas.



Também é recomendável que você só instale plugins confiáveis para os seus clientes. As categorias “featured” e “popular” no repositório WordPress podem ser um bom lugar para começar. Ou faça o download diretamente do site do desenvolvedor. Nós desencorajamos fortemente qualquer uso de plugins e temas WordPress nulos.

Você pode usar uma ferramenta online como o VirusTotal para verificar um plugin ou arquivos de tema para ver se ele detecta algum tipo de malware.



Existem também muitos recursos para ajudá-lo a manter-se a par das últimas atualizações e vulnerabilidades de segurança do WordPress. Veja algumas delas incluídas abaixo:

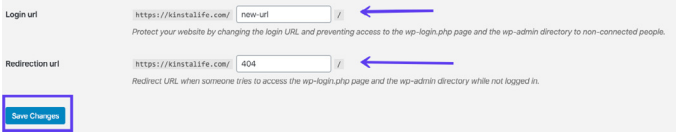
- WP Security Bloggers: Um fantástico recurso agregado de mais de 20 feeds de segurança.
- WPScan Vulnerability Database: Catálogos com mais de 10.000 vulnerabilidades de WordPress Core, Plugin e Tema.
- ThreatPress: Dase de dados diariamente atualizada de plugins WordPress, temas e vulnerabilidades centrais do WordPress
- Arquivo Oficial de Segurança WordPress

Bloqueie seu WordPress Admin

Às vezes a estratégia popular de segurança WordPress por obscuridade é apropriadamente eficaz para um negócio online médio e um site WordPress. Se você torna mais difícil para os hackers encontrar certos backdoors, então você tem menos probabilidade de ser atacado. Bloquear a área de administração do WordPress dos seus clientes e o login é uma boa maneira de aumentar a sua segurança. Duas grandes maneiras de fazer isso é primeiro alterando o seu URL de login padrão wp-admin e também limitando as tentativas de login.

Como Mudar o seu URL de Login do WordPress

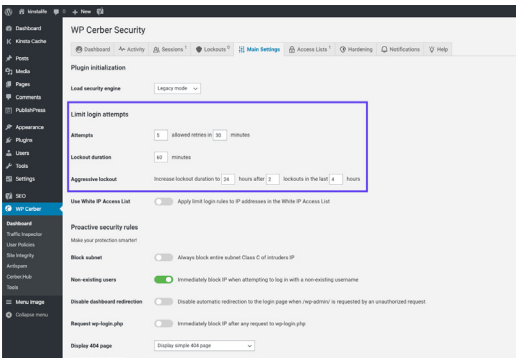
Por padrão o URL de login do seu site WordPress é domain.com/wp-admin. Um dos problemas com isso é que todos os bots, hackers e scripts lá fora também sabem disso. Ao mudar a URL você pode se tornar menos um alvo e se proteger melhor contra ataques de força bruta. Esta não é uma solução de conserto, é simplesmente um pequeno truque que pode definitivamente ajudar a protegê-lo.



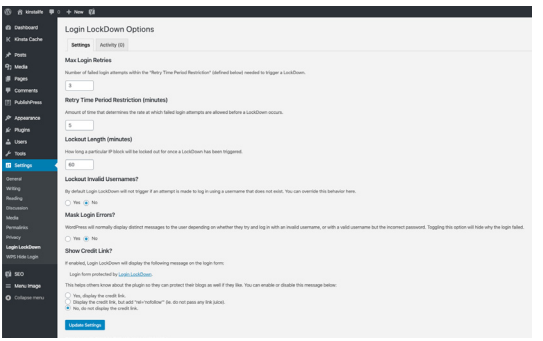
Para alterar o seu URL de login do WordPress, recomendamos usar o plugin gratuito WPS Hide login. Apenas lembre-se de escolher algo único que não esteja já em uma lista que um bot ou script possa tentar escanear.

Como Limitar Tentativas de Login

Embora a solução acima de alterar a URL de login do seu administrador possa ajudar a diminuir a maioria das más tentativas de login, colocar um limite no lugar também pode ser muito eficaz. O plugin gratuito Cerber Limit Login Attempts é uma ótima maneira de facilmente configurar durações de bloqueio, tentativas de login, listas brancas e listas negras de IP.



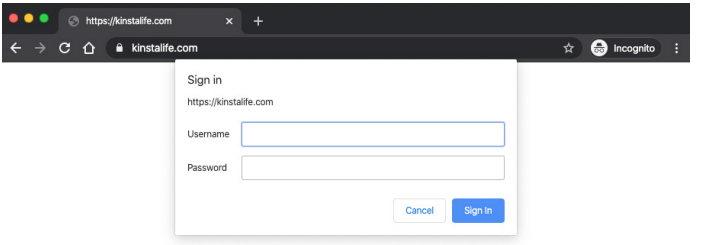
Se você está procurando por uma solução de segurança WordPress mais simples, outra ótima alternativa é o plug-in gratuito Login Lockdown.



O Login LockDown registra o endereço IP e o carimbo da hora de cada tentativa de login falhada. Se mais de um certo número de tentativas for detectado dentro de um curto período de tempo a partir do mesmo intervalo de IP, então a função de login é desativada para todos os pedidos a partir desse intervalo. E é completamente compatível com o plugin de login WPS Hide, que mencionamos acima.

Se você mudar o site dos seus clientes para Kinsta, você não precisa instalar nenhum plugin adicional para os limites da nossa plataforma e bloqueia automaticamente as tentativas maliciosas.

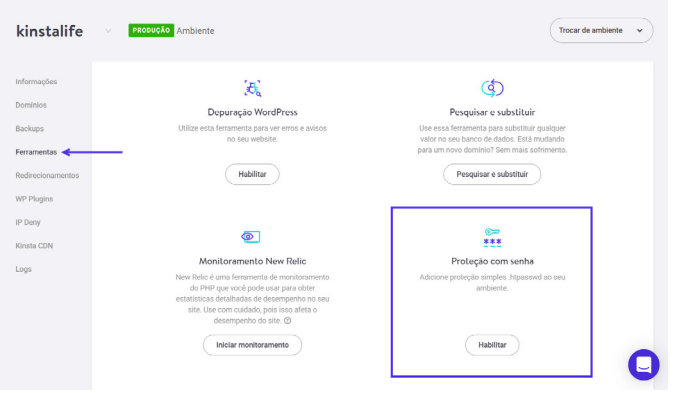
Como Adicionar Autenticação HTTP Básica (Proteção htpasswd)
Outra forma de bloquear o seu administrador é adicionar autenticação HTTP. Isso requer um nome de usuário e senha antes mesmo de poder acessar a página de login do WordPress.



Confira esta funcionalidade com a demonstração do MyKinsta.

Importante: Isto geralmente não deve ser usado em sites de comércio eletrônico ou sites de membros. Mas pode ser uma forma muito eficaz de evitar que os bots atinjam o seu site.

Se você hospedar os sites de seus clientes na Kinsta, você pode usar nossa ferramenta de proteção por senha fácil (htpasswd) no painel MyKinsta (veja em ação na conta de demonstração gratuita do MyKinsta). Você pode encontrá-lo na seção “Ferramentas” do seu site. Basta clicar em “Ativar”, escolher um nome de utilizador e uma palavra-passe e está pronto para começar!



Confira esta funcionalidade com a demonstração do MyKinsta.

Depois de ativado, cada site WordPress precisará de autenticação para acessá-lo. Você pode alterar as credenciais a qualquer momento ou desativá-las quando você não precisar mais delas.

Vantagem da Autenticação de Dois Factores (2FA)

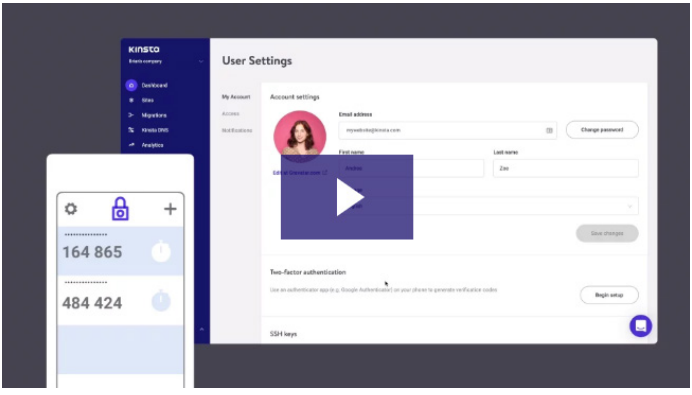
A autenticação de dois fatores envolve um processo de dois passos no qual você precisa não apenas da sua senha para fazer o login, mas também de um segundo método para fazer o login. Na maioria dos casos, isto é 100% eficaz na prevenção de ataques de força bruta aos sites WordPress dos seus clientes.

Há duas partes quando se trata de autenticação de dois fatores para sites de clientes, no entanto.

O primeiro é a sua conta e ou painel de controle que você tem com o seu provedor de hospedagem web. Se alguém tiver acesso a isto, pode alterar todas as senhas dos seus clientes, apagar os seus sites, alterar os registos DNS e todo o tipo de coisas horríveis. Aqui na Kinsta usamos o Authenticator-based 2FA para o seu painel de controle do MyKinsta porque:

- O Authenticator-based 2FA é mais seguro do que o 2FA baseado em SMS porque não está ligado ao seu número de telemóvel e não depende da tecnologia de SMS herdada. Isto torna o 2FA baseado no Authenticator resistente às técnicas de troca de SIM.
- O Authenticator-based 2FA pode ser usado com aplicativos gerenciadores de senhas como o 1Password para maior comodidade. Ao adicionar os seus dados 2FA a um gerenciador de senhas, você não terá que confiar em um dispositivo externo para fazer login no MyKinsta.

Aqui está como é fácil ativá-lo:



A segunda parte da autenticação de dois fatores diz respeito às instalações reais do WordPress de seus clientes. Para estes existem alguns plugins que você pode querer testar e recomendar:

- Autenticação de Dois Fatores Duo
- Google Authenticator
- Two Factor Authentication

Após instalar e configurar um dos plugins acima em um site do cliente, eles normalmente terão um campo adicional em sua página de login no WordPress para inserir seu código de segurança. Ou, com o plugin Duo, eles primeiro fazem login com suas credenciais e depois são obrigados a escolher um método de autenticação, como Duo Push, call, ou passcode.

Use HTTPS para Conexões Criptografadas - Certificado SSL

Uma das formas mais esquecidas de reforçar a segurança do WordPress é instalar um certificado SSL e executar sites sobre HTTPS. HTTPS (Hypertext Transfer Protocol Secure) é um mecanismo que permite a qualquer navegador ou aplicativo da Web conectar-se com segurança a um site. Um grande equívoco é que se os sites dos seus clientes não estão aceitando cartões de crédito, eles não precisam de SSL.

Bem, vamos explicar algumas razões pelas quais o HTTPS é importante para além do comércio eletrônico. Muitos hosts, incluindo Kinsta, oferecem certificados SSL gratuitos com Let's Encrypt.

6 Principais Razões Porque é que o HTTPS é importante para Além do Comércio Eletrônico

1. Segurança Adicionada
Qual é a importância dos dados de login dos seus clientes? Bem, você deve saber que toda vez que um usuário faz login, essa informação está sendo passada para o servidor em texto simples. HTTPS é absolutamente vital para manter uma conexão segura entre um website e um navegador. Desta forma, você pode evitar melhor que hackers e ou um intermediário tenham acesso aos sites de seus clientes.

2. SEO
O Google disse oficialmente que o HTTPS é um fator de classificação. Como a maioria dos seus clientes provavelmente tiraria qualquer vantagem possível de SEO e SERPs para vencer os seus concorrentes, isto é um "no brainer".

3. Confiança e Credibilidade
De acordo com uma pesquisa da GlobalSign, 28,9% dos visitantes procuram a barra de endereços verde em seu navegador. E 77% deles estão preocupados que seus dados sejam interceptados ou mal utilizados online. Ao ver esse cadeado verde, os clientes terão instantaneamente mais tranquilidade sabendo que seus dados são mais seguros.

4. Dados de Referência
Muitas pessoas não percebem que o HTTPS para dados de referência HTTP está bloqueado no Google Analytics. Então, o que acontece com os dados? Bem, a maior parte deles são apenas agrupados junto com a seção "tráfego direto". Se alguém está indo de HTTP para HTTPS, o referenciador ainda é passado.

5. Avisos do Chrome
A partir de 24 de Julho de 2018, versões do Chrome 68 e superiores começaram a marcar todos os sites não-HTTPS como "Não Seguro" e, a partir de 2020, o popular navegador começou a depreciar o suporte a versões antigas do TLS. O Google está deixando muito mais claro para os visitantes que um site WordPress pode não estar rodando em uma conexão segura. É por isso que o HTTPS é mais importante do que nunca!

6. Desempenho

Por causa de um protocolo chamado HTTP/2, muitas vezes, aqueles que rodam sites corretamente otimizados sobre HTTPS podem até mesmo ver melhorias de velocidade. O HTTP/2 requer HTTPS por causa do suporte do navegador. A melhoria no desempenho deve-se a uma variedade de razões como HTTP/2 poder suportar melhor

multiplexação, paralelismo, compressão HPACK com codificação Huffman, a extensão ALPN e o server push.

E com o TLS 1.3, as conexões HTTPS são ainda mais rápidas. Kinsta suporta o TLS 1.3 em todos os nossos servidores e o nosso Kinsta CDN.

Confira nosso guia de migração em profundidade para WordPress HTTPS para que você se levante e saiba mais em nossa comparação TLS vs SSL.

Desativar XML-RPC

Nos últimos anos, o XML-RPC tornou-se um alvo cada vez maior de ataques por força bruta. Existem alguns plugins WordPress como o Jetpack que dependem do XML-RPC, mas a maioria das pessoas lá fora não vai precisar disso e pode ser benéfico simplesmente desativar o acesso a ele..

Se você é um cliente da Kinsta, não precisa se preocupar com isso, pois implementamos medidas ativas e passivas para impedir ataques e intenções maliciosas em seu caminho. Especificamente, quando um ataque através de XML-RPC é detectado, um pequeno trecho de código é adicionado ao arquivo de configuração Nginx para pará-los de produzir um erro 403.

Adicionar os Cabeçalhos de Segurança HTTP mais Recentes

Outro passo que você pode dar para endurecer a segurança do WordPress do seu cliente é tirar proveito dos cabeçalhos de segurança HTTP. Estes são normalmente configurados ao nível do servidor web e

dizem ao navegador como se comportar ao lidar com o conteúdo dos sites dos seus clientes. Existem muitos cabeçalhos de segurança HTTP diferentes, mas abaixo estão normalmente os mais importantes.

- Content Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- Opções X-Frame-Options
- Alfinetes- Chaves-Públicas
- X-Content-Type

Você pode verificar quais cabeçalhos estão rodando atualmente em cada instalação do WordPress, lançando os devtools Chrome e olhando para o cabeçalho na resposta inicial do seu site.

Aqui está um exemplo na kinstalife.com (um site de demonstração). Pode ver que estamos a utilizar o cabeçalho de opções do tipo "x-content-type-options".

Quando se trata de sites clientes, como no exemplo mostrado, as x-content-type-options são sempre adicionadas por padrão, enquanto x-frame-options e strict-transport-security são definidas apenas se necessário.

Se precisar de digitalizar os sites dos seus clientes, pode fazê-lo com a ferramenta gratuita Securityheaders.io, de Scott Helme.

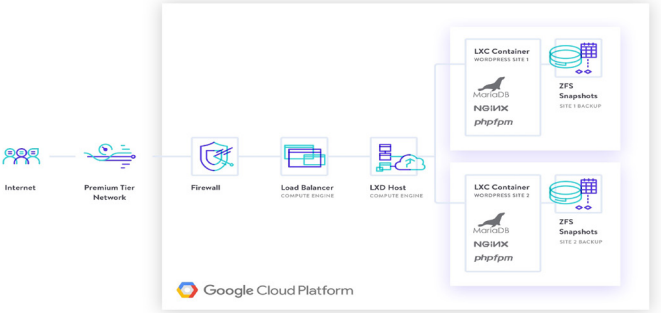
Também é importante lembrar que quando você implementa cabeçalhos de segurança HTTP, como isso pode afetar seus subdomínios do WordPress. Por exemplo, se você adicionar o cabeçalho da Política de Segurança de Conteúdo e restringir o acesso por domínios, então você precisa adicionar seus próprios subdomínios também. Se você não tiver certeza de como implementá-los, você pode sempre perguntar ao seu host se ele pode ajudar.

Use os Plugins de Segurança do WordPress

Há muitos grandes desenvolvedores e empresas por aí que fornecem grandes soluções para ajudar a proteger melhor o seu site WordPress. As notáveis são:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security
- VaultPress
- Google Authenticator – Two Factor Authentication
- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinsta tem firewalls de hardware, segurança ativa e passiva, verificações de tempo de atividade em minutos e pontuação de outros recursos avançados para evitar que os atacantes tenham acesso aos seus dados. Se, apesar dos nossos melhores esforços, o seu site estiver comprometido, nós o consertaremos de graça.

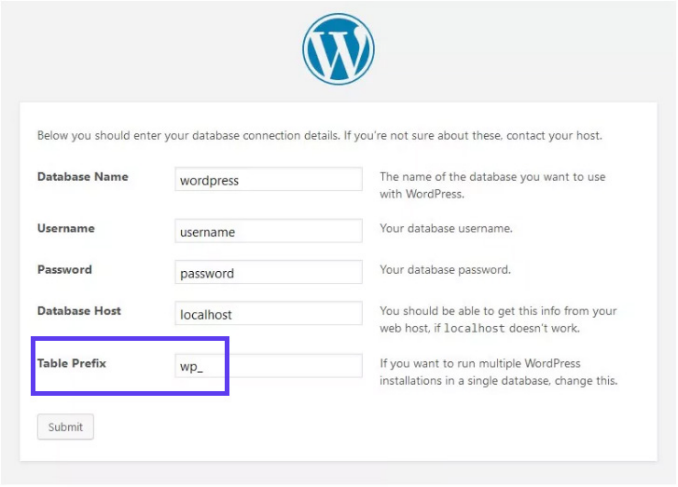


Uma característica muito importante que muitos plugins de segurança incluem é um utilitário de checksum. Isso significa que eles inspecionam cada uma das instalações do WordPress do seu cliente e procuram por modificações nos arquivos principais, como fornecido pelo WordPress.org (através da API). Quaisquer alterações ou modificações nesses arquivos podem indicar um hack.

Você também pode usar o WP-CLI para executar o seu próprio checksum. Confira estes plugins adicionais de segurança WordPress que podem ajudar a bloquear os bandidos.

Segurança da Base de Dados Harden

Há algumas maneiras de melhorar a segurança do seu banco de dados WordPress. A primeira é usar um nome de banco de dados inteligente. Ao mudar o nome da sua base de dados para um nome mais obscuro, ajuda a proteger o seu site, tornando mais difícil para os hackers identificarem e acederem aos detalhes da sua base de dados.

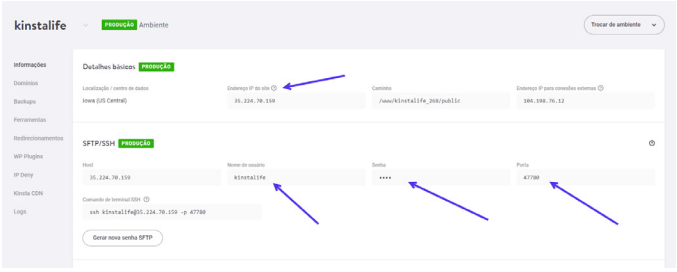


Uma segunda recomendação é usar um prefixo de tabela de banco de dados diferente. Quando você instala o WordPress, ele pede um prefixo de tabela. Por padrão, o WordPress utiliza wp_. Mudar isso para algo como 39xw_ pode ser muito mais seguro.

Se você é um cliente Kinsta e hospeda todos os sites dos seus clientes connosco, isto não é necessário. Nós temos o site e a base de dados bloqueados para si!

Use Sempre Ligações Seguras

Nunca é demais salientar como é importante usar ligações seguras! Certifique-se de que seu host WordPress está tomando precauções, tais como oferecer SFTP ou SSH. SFTP ou Secure File Transfer Protocol (também conhecido como SSH file transfer protocol), é um protocolo de rede utilizado para transferências de arquivos. É um método mais seguro vs FTP padrão.



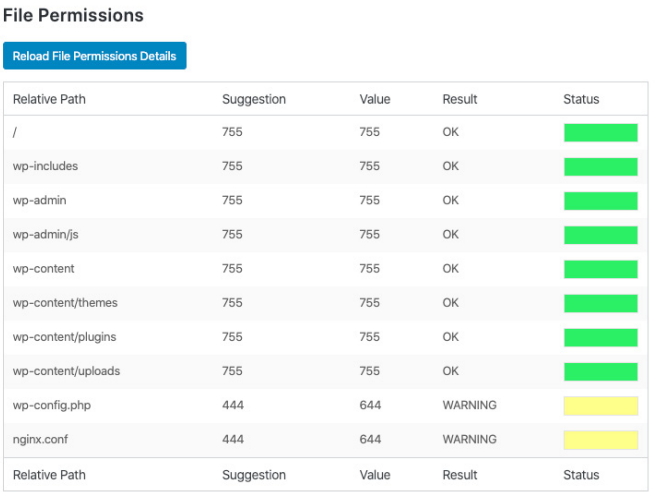
Confira esta funcionalidade com a demonstração do MyKinsta.

Só suportamos conexões SFTP em Kinsta para garantir que seus dados permaneçam seguros e criptografados. A maioria dos hosts WordPress também usam normalmente a porta 22 para SFTP. Nós levamos isto um passo adiante na Kinsta e cada site tem uma porta randomizada que pode ser encontrada no seu painel MyKinsta.

Verificar Permissões de Arquivo e Servidor

As permissões de arquivo nas instalações de seus clientes e servidores web são cruciais para aumentar a segurança desses ambientes. Se as permissões são muito frouxas, alguém pode facilmente ganhar acesso ao seu site e causar estragos. Por outro lado, se as suas permissões forem demasiado rígidas, isto pode quebrar a funcionalidade do seu site. Portanto, é importante ter as permissões corretas definidas em todos os âmbitos.

Você pode usar um plugin gratuito como o iThemes Security para verificar as permissões nos sites WordPress dos seus clientes.



Aqui estão algumas recomendações típicas para permissões quando se trata de permissões de arquivos e pastas no WordPress:

- Todos os arquivos devem ser 644 ou 640. Exceção: wp-config.php deve ser de 440 ou 400 para evitar que outros usuários no servidor o leiam.
- Todos os diretórios devem ser 755 ou 750.
- Nenhum diretório deve ser dado 777, nem mesmo carregar diretórios.

Veja o artigo do WordPress Codex sobre alteração de permissões de arquivo para uma explicação mais detalhada.

Proteção DDoS

DDoS é um tipo de ataque DOS onde múltiplos sistemas são usados para atingir um único sistema causando um ataque de Negação de Serviço (DoS). Os ataques DDoS não são nada de novo - de acordo com a Britannica o primeiro caso documentado data do início do ano 2000. Ao contrário de alguém que pirateia o seu site, estes tipos de ataques normalmente não prejudicam o seu site, mas simplesmente derrubam o seu site por algumas horas ou dias.

O que você pode fazer para se proteger? Uma das melhores recomendações é usar um serviço de segurança de terceiros respeitável como o Cloudflare ou Sucuri.

Sua avançada proteção DDoS pode ser usada para mitigar ataques DDoS de todas as formas e tamanhos, incluindo aqueles que têm como alvo os protocolos UDP e ICMP, bem como ataques SYN/ACK, amplificação DNS e Layer 7. Outros benefícios incluem

colocar você atrás de um proxy que ajuda a esconder seu endereço IP de origem, embora ele não seja à prova de balas.

Não ignore o fornecedor que a sua hospedagem web usa porque isso também é muito importante.

Firewalls de hardware, como o Google Cloud Platform Firewall que usamos na Kinsta, estão instalados e têm restrições muito rígidas baseadas em software para proteger os sites dos seus clientes e também têm software instalado para detectar ataques DDoS à medida que eles acontecem.

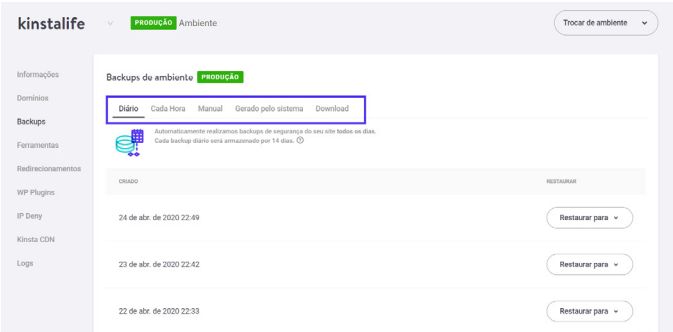
Isto significa que você e os seus clientes obtêm o benefício de um modelo de segurança que tem sido construído ao longo de 15 anos e que atualmente protege produtos e serviços como o Gmail, Search, etc. A Google emprega atualmente mais de 500 profissionais de segurança a tempo inteiro.

No topo da plataforma Google Cloud, também usamos contentores Linux (LXC e LXD) para orquestrá-los, o que nos permite isolar completamente não apenas cada conta, mas cada site WordPress separado.
Mesmo assim, as coisas vão para o Sul? Kinsta fornece reparação gratuita de hackers e remoção de malware. Se um dos sites dos seus clientes estiver infectado, a nossa equipe de suporte fará tudo o que for necessário para limpar.

Obtenha mais detalhes sobre como levamos a segurança a sério na Kinsta!

Sempre Aceite Backups

Não importa quão seguro o seu site seja, ele nunca será 100% seguro. É por isso que você quer backups no caso do pior acontecer. Os backups são a única coisa que todos sabem que precisam, mas nem sempre são aceites. A maioria das recomendações aqui descritas são medidas de segurança que você pode tomar para proteger melhor os sites dos seus clientes e o seu negócio.



Confira esta funcionalidade com a demonstração do MyKinsta.

A maioria dos provedores de hospedagem WordPress gerenciados agora fornecem backups. Kinsta tem 5 tipos diferentes de backups:

- Diariamente: Kinsta cria backups automáticos de todos os sites dos seus clientes a cada 24 horas para que você possa descansar facilmente à noite.

- De hora em hora: Se precisar de um horário de backup mais frequente, pode ativar backups automáticos de 6 horas ou de hora em hora para qualquer site alvo que o requeira (isto vem em cima do seu plano mensal).
- Manual: se os backups automáticos não forem suficientes, você pode criar backups manuais para cada site que estiver gerenciando e ter esta cópia adicional disponível por 14 dias ou mais, com base no seu plano atual.
- Gerado pelo sistema: antes de tarefas críticas como a utilização da ferramenta de busca-substituição no MyKinsta, movendo um ambiente de teste para produção (ao vivo) e restaurando um backup para o seu ambiente de produção (ao vivo), Kinsta irá acionar backups gerados pelo sistema.
- Arquivo para download: se tudo isso não for suficiente, uma vez por semana, você poderia baixar um arquivo zip de cada site cliente contendo arquivos do site e um arquivo SQL contendo o conteúdo da base de dados do site.

As opções de backup não vêm sozinhas, pois Kinsta permite restaurar facilmente qualquer site com um único clique. Isso é conveniente, não é?

Teste gratuitamente como é fácil criar cópias de segurança com o MyKinsta!

Se a sua hospedagem não tiver backups, há alguns plugins populares do WordPress que você pode usar para automatizar o processo.

Plugins de Backup WordPress

Os plugins de backup do WordPress permitem que você pegue seus backups via FTP ou integre com uma fonte externa de armazenamento como Amazon S3, Google Cloud Storage, Google Drive ou Dropbox. Recomendamos vivamente uma solução incremental para que utilize menos recursos:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta não permite plugins de backup não-incrementais devido a problemas de desempenho: tratamos de tudo isto a nível de servidor para que não abrande os sites dos seus clientes.

Resumo

A segurança é um jogo de camadas. Quanto mais você tiver sucesso em empilhar novas camadas de segurança umas sobre as outras, mais seguros se tornarão os sites dos seus clientes. Tudo começa com o uso de senhas inteligentes, mantendo o núcleo e os plugins atualizados e seguindo outras melhores práticas de segurança que já abordamos aqui.

Mas isso não é tudo que você deve fazer para diminuir suas chances de ter que lidar com sites de clientes hackeados. Ao escolher um

host WordPress gerenciado como a Kinsta, a maioria das medidas de segurança são tomadas para você, permitindo que você construa uma base sólida, segura e escalável para garantir o futuro dos sites dos seus clientes. E o do seu negócio.

Quer experimentar como é fácil gerenciar sites de clientes na Kinsta?

Confira o demo.mykinsta.com! 


KINSTA