ELEMENTOS DE SEGURANÇA PARA SITES WORDPRESS

1. CDN, GEOBLOCKING, PREVENÇÃO DE BOTS E ATAQUES DE NEGAÇÃO DE SERVIÇO

Implementar uma camada de CDN impede uso de banda com recursos estáticos, além de melhorar índices de SEO. Soluções como CloudFare e Akamai permitem limitar o acesso em países específicos (de onde partam a maior quantidade de ataques, por exemplo), detectar e prevenir acesso de bots que realizem escaneamento (scraping) ou outras ações indesejadas, além de impedir ataques de negação de serviço.

2. PLUGINS

Extensões disponibilizadas no portal do WooCommerce tendem a ser atualizadas com maior frequência e acompanharem o ritmo de releases do WooCommerce. É recomendável iniciar a busca de soluções no portal, e em seguida partir para opções de plugins no repositório oficial do WordPress.

3. APIS DO WOOCOMMERCE E WORDPRESS

As APIs do Wordpress e WooCommerce abrem um grande leque de possibilidades de interações automatizadas com o sistema. Caso a implementação não siga o modelo headless, é recomendado avaliar quais integrações com meios de pagamentos, serviços de logística, dentre outros, que necessitem enviar call-backs e realizar interações via webhooks com a aplicação, trabalhando com whitelists de endpoints mínimos necessários, incluindo checagem de domínios e/ou IPs dos requisitantes, além de rotacionar chaves de API.

4. XML-RPC

Utilizado pelos aplicativos móveis do WordPress e funcionalidades como pingback, as chamadas XML-RPC abrem uma porta para ataques de DDoS e não possuem impacto negativo na experiência do usuário caso desabilitadas.

5. CAPTCHA

É recomendado utilizar captchas como reCaptcha ou hCaptcha em formulários como comentários ou login para evitar ataques de replicação ou força bruta. A maioria das implementações hoje possui configurações de níves de segurança esperados, que podem ser mais ou menos intrusivos na experiência do usuário de acordo com o comportamento de navegação avaliado.

6. AUTENTICAÇÃO DE DOIS FATORES

Vazamentos de senhas reutilizadas pelos usuários em outros sites podem ser fontes de exposição de dados ou compras fraudulentas, por isso é recomendada a utilização de métodos de autenticação de dois fatores, que dificultam essa possibilidade em até 99,9% (estudo da Microsoft).

7. HEADLESS CMS

É possível trabalhar com o WooCommerce completamente desacoplado do frontend, utilizando chamadas REST, cenário em que é possível avaliar durante o desenvolvimento quais endpoints da API devem ser expostos e trabalhar com uma whitelist. O painel administrativo pode ser disponibilizado em outro domínio, inclusive.

8. MEIOS DE PAGAMENTO COM PÁGINAS EXTERNAS OU IFRAMES

Como detalhado na documentação do WooCommerce, a utilização de meios de pagamento com processos de checkout externos (redirecionamento ou iframe) impede a interação do usuário com campos de dados de cartão, geração de imagens QrCode para PIX ou códigos de barras para boletos bancários dentro do site, delegando ao próprio meio de pagamento essa etapa sensível, sendo este responsável pela segurança do processo. Neste modelo, por exemplo, nenhum dado de cartão de crédito é transmitido entre o site e meio de pagamento.