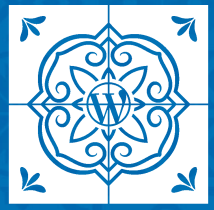

WORDCAMP
LISBOA 2023

Seu WordPress não tem segurança.

E isso é culpa sua!

Luiz Calderaro

A culpa é minha e eu coloco ela em quem eu quiser!

Homer Simpson.

Introdução

Existem milhares de linguagens de programação, existem centenas de frameworks, bibliotecas, plugins, temas e, ainda assim, ouvimos sempre que o WordPress é inseguro.

A ideia dentro desta apresentação é remover o conceito de que o WordPress é inseguro e, ainda mais, mostrar que a culpa da falta de segurança está em todos nós, ou seja, a culpa é sua.

Tópicos

1. WordPress e sua ascensão ao estrelato.
2. WordPress e sua fama de Bad Boy.
3. O Conto do Pedrocas um developer WordPress
4. A segurança está em todos os lados.
5. Como pensar, vender, desenvolver sempre com o conceito de segurança

WordPress e sua ascensão

WordPress teve sua release inicial em 27 de maio de 2003 ou seja, 20 anos atrás.

WordPress é um CMS, serve apenas para Blog?

Posso fazer tudo com o WordPress?

Por que o WordPress ficou tão famoso?

- WordPress is free
- WordPress é open-source
- Existem plugins para tudo
- WordPress é a melhor plataforma de blogging no mercado
- WordPress prioriza SEO
- The Do-It-Yourself website
- Temas e templates
- É suportado por uma enorme comunidade e pela indústria

Por que o WordPress tem fama de Bad Boy?

WordPress é um ecossistema vivo e sempre em evolução.

O WordPress é altamente extensivo, possui uma infinidade de plugins e temas que suprem a necessidade de milhares de empresas espalhadas pelo mundo.

- Enorme base de utilizadores padronizados
- Altamente customizável
- Normalmente personalizado por utilizadores menos técnicos
- Um gigantesco ecossistema de plugins e temas
- Grátis/Barato para hospedar
- Retrocompatibilidade

WordPress pelo mundo

- 43% dos sites no mundo rodam WordPress
- 64,3% dos CMS's usam WordPress
- 38% dos top 10.000 sites foram construídos em WordPress
- Mais de 22% dos domínios comprados dentro dos EUA rodam WordPress
- Todos os dias mais de 1.000 novos sites em WordPress juntam-se ao mais de 10 milhões de websites rastreados pelo W3Techs.com

WORDCAMP
LISBOA 2023

O Conto do Pedro e do Zé do dedão

Pedro, O Freelancer.

Pedro é um freelancer PHP que acabou de começar a carreira, escolheu o WordPress por ser uma porta relativamente fácil para a entrada no mercado de IT e pretende um dia trabalhar em uma grande empresa.

WORDCAMP
LISBOA 2023

Zé do dedão, o empresário dos calçados.

Zé é um empresário consolidado no mundo dos calçados, porém, durante a pandemia do COVID 19 ele precisou, com muita urgência, criar uma identidade na internet para continuar as suas vendas.

WORDCAMP
LISBOA 2023

Os Requisitos

Zé do dedão quer um e-commerce para poder continuar a vender os seus sapatos já que, suas lojas estão fechadas por causa da COVID 19.

Ele também quer entregar para toda a Europa, isso significa que o site deve ter suporte multilingue, deve ter meios de pagamentos disponíveis em todos os Países da UE e também cálculo de frete automático.

Como ele tem muita urgência, ele gostaria que o site estivesse pronto em no máximo 2 semanas.

A proposta

O Pedrocas quer muito ganhar o projeto e, para isso, ele vai colocar um valor irresistível. 500€ para fazer o site inteiro.

Pra isso ele pensou, posso usar WordPress e WooCommerce e existem dezenas de plugins para cálculo do frete, sistema de pagamentos, e o tema ele pega um qualquer em um site, coloca em um host compartilhado que não tem informação alguma sobre segurança e diz: Acredito que consigo fazer tudo no final de semana e pois ainda tenho outros sites para entregar.

O Processo

Pedro conseguiu fazer o site no final de semana, fez mais horas do que estava à espera, mas precisava vasculhar na internet plugins que fizessem exatamente aquilo que ele precisava para o projeto.

Conseguiu montar tudo, sabia que em alguns plugins precisava pagar, mas conseguiu eles em um site sem precisar de nada.

Mas claro, ele pensou em segurança, colocou um certificado HTTPS.

O Resultado

Após um mês com o site no ar e mesmo ele apresentando algumas falhas, o Zé conseguiu fazer boas vendas. Porém, em um fim de semana o site foi invadido, dados dos clientes foram expostos e compras foram feitas.

O Zé viu o negócio dele todo ir embora e o seu prejuízo foi incalculável.

Depois de imensas tentativas de contacto com o Pedro para perceber o que havia acontecido, Pedro disse que o WordPress era inseguro e desapareceu, nunca mais atendeu uma ligação.

As primeiras análises do projeto.

As primeiras falhas de segurança acontecem exatamente na gestão do projeto, principalmente quando subestimamos a complexidade.

- Restrição tripla
  - Bom, Rápido, Barato, Concluído
- Ser ágil
- Comunicação
- Transparência
- Prazos
- Valores

Dados sobre falhas de segurança em sites WordPress.

De acordo com a pesquisa feita pela Sucuri, 60.04% dos sites analisados continham ao menos um backdoor, 52% dos sites continham algum tipo de SEO Spam e 95.62% deles eram sites WordPress

- 8% dos sites em WordPress são invadidos por passwords fracas
- 52% dos sites WordPress são invadidos estão out of date
- 17.8% das vulnerabilidades reportadas pelo WPScan são causadas por plugins de WordPress
- 39% das vulnerabilidades no WordPress são problemas de cross-site scripting (XSS)
- 2% das vulnerabilidades do WordPress são causadas por temas.

WORDCAMP
LISBOA 2023

E agora, quem poderá nos defender?

Segurança durante o projeto.

Como eu gosto de dizer, segurança vai desde o planeamento do projeto até a sua manutenção depois de entregue.

- Seja sempre sincero com o seu cliente
- Escolha uma infraestrutura que seja adequada ao tipo de negócio do cliente
  - WPEngine
  - SiteGround
  - Kinsta
  - AWS
  - Google Cloud
  - Microsoft Azure
- Antes de usar qualquer plugin, leia os logs, garanta que eles estão atualizados e que falhas de segurança são sempre implementadas.
- Nunca modifique um plugin, ou ele faz 100% do que o projeto precisa ou é necessário criar um.
- Nunca, mas nunca pense em usar password fracas, 123456 é coisa do passado.

Mais segurança.

E guardamos os melhores para o final

- Cloudflare Plugin
- Sucuri Plugin
- Root MySQL Access
- Desabilite o registo
- Two-factor Authentication (2FA)
- Tenha a certeza de que o debug log está desligado
- Restringir a API REST do WordPress
- Source Code Analysis Tools
    - Codacy
    - Agnito
    - Betterscan
- RASP (Runtime Application Self-Protection)

A segurança de um site está diretamente ligada com todo o seu processo de desenvolvimento.

WORDCAMP
LISBOA 2023

Obrigado! Alguma questão?

Luiz Calderaro

WakeUp, Software solutions
@lzcalderaro

lzcalderaro@gmail.com
https://wakeup.pt