CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNOLÓGICA EM
Redes de Computadores

EDUARDO LONARDI BARBALHO DE SANTANA JUNIOR
VIRGÍLIO SANTIAGO JOSÉ DE SOUSA

SEGURANÇA EM WORDPRESS

RECIFE/2020

EDUARDO LONARDI BARBALHO DE SANTANA JUNIOR
VIRGÍLIO SANTIAGO JOSÉ DE SOUSA

SEGURANÇA EM WORDPRESS

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: MSc, Adilson da Silva.

RECIFE/2020

S232s Santana Junior, Eduardo Lonardi Barbalho de
Segurança em Wordpress./ Eduardo Lonardi Barbalho de Santana Junior; Virgílio Santiago José de Sousa. - Recife : O Autor, 2020.
24 p.

Orientador(a): Adilson da Silva

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes de Computadores, 2020.

1. Segurança WordPress. 2. Blindagem WordPress. 3. Administradores de Sites. I. Centro Universitário Brasileiro - UNIBRA.II. Título.

CDU: 004.7

EDUARDO LONARDI BARBALHO DE SANTANA JUNIOR
VIRGÍLIO SANTIAGO JOSÉ DE SOUSA

SEGURANÇA EM WORDPRESS

Artigo aprovado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores, pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

_____

Prof.º Msc. Adilson da Silva

Professor Orientador

_____

Prof.º Msc. Renan Costa Alencar

Professor Examinador

_____

Prof.º Dr. Humberto Caetano Cardoso da Silva

Professor Examinador

Recife, ___/___/____

NOTA:_____

Dedicamos esse trabalho a nossos pais,colegas de trabalho e professores.

AGRADECIMENTOS

A Deus, o primeiro lugar, que fez com que nossos objetivos fossem alcançados durante todos os nossos anos de estudos.

Ao meu orientador, que nos ajudou a manter sempre o foco.

Aos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o nosso processo de aprendizado.

“Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre.”

(Paulo Freire)

LISTA DE FIGURAS

SUMÁRIO

Segurança no WordPress

Eduardo Lonardi Barbalho de Santana Junior

Virgílio Santiago José de Sousa

Adilson da Silva [1]

Resumo:
Este artigo tem como um objetivo apresentar o conceito de um CMS, suas vantagens e os mais usados no mercado. Será escolhido o WordPress devido a sua representatividade no mercado, por ser bastante intuitivo e possuir uma curva de aprendizado menor sobre os demais concorrentes. Com toda essa visibilidade no mercado, o WordPress é visado bastante por hackers a atacar a sua plataforma. Com isso será apresentado os principais ataques na Web e ao WordPress bem como as respectivas soluções para cada ataque.Será apresentado o conceito de segurança, a informação como pode ser classificada de acordo com as diretrizes da sua empresa e segurança da informação e seus pilares, como: Integridade, Disponibilidade e Confidencialidade.

Palavras-chave:
Segurança-WordPress - Blindagem WordPress-Administradores de Sites.

1 INTRODUÇÃO

Com o avanço das informações em tempo real, surgiu uma necessidade de aplicações que facilitem de maneira intuitiva o gerenciamento dessas informações. Além de não exigirem tanto conhecimento técnico para manusear e não serem tão custosas financeiramente. O advindo dos Sistemas de Gerenciamento de Conteúdos, em inglês *Content Management System* - CMS, facilitou todo esse processo.Segundo o artigo publicado pela Sucuri(2019), atualmente existem 3 principais Sistemas de Gerenciamento de Conteúdo, que são o WordPress, Joomla e o Drupal. Este artigo tem com objetivo o uso do WordPress bem como utilizá-lo de maneira segura de acordo os pilares da Segurança da Informação. Além de informar os principais ataques a aplicações de maneira geral e específica ao WordPress.

1 Professor Adilson da Silva da UNIBRA. Msc. E-mail para contato: adilsondasilva.professor@gmail.com.

Será abordado boas práticas de segurança para o desenvolvimento de sites seguros em Wordpress. Será retratado as principais formas de ataque e como evitá-las com uso de ferramentas e práticas de segurança. Temas como, SEO, boas práticas de segurança, plugin de segurança, core do wordpress desatualizado, backup e permissão de usuários serão abordados.

De acordo com artigo publicado Computerworld (2018), o WordPress registrou uma participação de 62% no mercado de CMS(Sistema de Gerenciamento de Conteúdo) em 2019 e o mesmo representa 35% de todos os sites que existem no mundo. O wordpress é uma plataforma das mais usadas no mundo como relata a pesquisa, por isso ela é muito visada pelos hackers para efetuar invasões. O wordpress não é uma plataforma insegura mas como retrata no artigo publicado na 2WP(2020) parte da segurança é de quem administra os sites na plataforma. Os administradores do site devem estar ciente dos riscos relacionado a segurança da informação e seguir as regras de segurança que o wordpress informa também, para isso é de suma importância manter sempre o core (núcleo) do wordpress atualizado e seus respectivos plugins também.

2 REFERENCIAL TEÓRICO

2.1 CMS

O termo CMS vem do inglês *Content Management System*, que significa Sistema de Gestão de Conteúdo, com o objetivo trazer uma maior facilidade na questão de gerir os conteúdos publicados em um site, loja virtual ou blog. Como explica Silva (2013), “um sistema de gestão de conteúdo é constituído por ferramentas necessárias para criar ou gerir conteúdos em tempo real”.

Em 1997, como explica em sua publicação o Tobias (2018), a empresa Typo3, visando a facilitar a vida dos criadores de site, criou o conceito e o primeiro CMS, que seria criar, gerenciar e publicar conteúdos na internet, tudo isso de forma simples e sem exigir conhecimentos avançados de desenvolvimento web.

Segundo um artigo publicado por Clemente (2019), as principais funcionalidades de um CMS são de: criação e publicação de páginas, edição de texto e de código do site, moderação de comentários, controle de estoque e sistemas de venda(caso seja e-commerce), instalação de plugins e extensões para

aumentar as funções do site, bibliotecas de mídias, para carregar imagens e vídeos que serão usados no site e dentre outros.

Segundo a publicação do Tobias (2018), apresenta outras vantagens em utilizar o um CMS que seriam:

Adição de recursos extras como extensões e plugins, aplicações de técnicas de SEO,logs de acesso,responsividade automática,área administrativa de fácil acesso de qualquer local sem a necessidade de softwares específicos, criação e edição de URLs amigáveis para otimizar o SEO e alterações no visual de forma simplificada.

2.1.1 PRINCIPAIS FERRAMENTAS

Como relata a publicação feita pela Sucuri (2019) sobre o mercado de CMS aponta 3 principais sistemas de gerenciamento de conteúdo que são: WordPress, Joomla e Drupal.

2.1.1.1 WordPress

O WordPress é um CMS (Content Management System) ou seja um sistema de gerenciamento de conteúdo que é usado para administrar sites, blogs, lojas virtuais, portais de notícia e entre outros. De acordo com a Computerworld (2018) , o WordPress registrou uma participação de 62% no mercado de CMS em 2019 e cerca de 35% de todos os sites do mundo são em WordPress.

O WordPress trás de forma bastante intuitiva maneiras de como administrar o conteúdo dentro de um site. Segundo a publicação do Clemente (2020), “de forma mais específica, ele tem como missão facilitar a criação e a edição de conteúdos em um site sem a necessidade de usar uma linguagem de programação”.

A ideia é tornar possível que até um produtor de conteúdo sem conhecimento algum em códigos consiga, de forma simples e intuitiva, gerenciar todo o seu portal, loja ou blog.Isso engloba a criação de textos, uso de imagens e vídeos, elaboração de formulários, sem contar as várias opções de personalização do layout do site e muitas outras funções.

O Surgimento do WordPress começa a partir da interrupção de um projeto chamado B2 Cafelog, que era uma plataforma para desenvolvimento de blogs. Esse projeto se iniciou em 2001 e foi abandonado em 2003, mais precisamente no dia 27 de maio, quando começou o WordPress (na versão 0.7).

Portanto, o WordPress é uma variação do extinto B2 Cafelog. Seus fundadores são Matt Mullenweg e Mike Little. O WordPress desde a sua versão 1.5.1.2 começaram a fazer mais correções voltadas a área de segurança em seu próprio site o wordpress.org que noticia desde a versão 1.5.1.2 até a mais atual (5.3.1) como funções para inserir no código do seu site, informações sobre os possíveis brechas e como foram corrigidas.

O WordPress possui duas versões disponíveis aos usuários: a plataforma wordpress.com e o wordpress.org.O wordpress.com é um serviço que fornece hospedagem gratuita de blogs e sites com o uso do software do WordPress.

O wordpress.org é uma plataforma de código aberto, que pode ser baixada gratuitamente no site oficial e instalada em um servidor a escolha.

A plataforma foi desenvolvida na linguagem de programação PHP.

Segundo Neves (2013), “a principal característica do WordPress é sua plasticidade em relação ao visual possuindo um sistema de temas e o usuário pode organizar o conteúdo através de widgets sem precisar editar o código”.

Uma desvantagem seria a dificuldade de realizar a escalabilidade, pois isso resultará em um desempenho menor do que o esperado.

2.1.1.2 Joomla

Foi criado em 2005, é o resultado da separação entre a equipe de desenvolvedores do Mambo e a empresa Miro, detentora dos direitos do Mambo. Conforme Neves(2013) explica o Joomla é indicado especialmente para quem deseja construir sites de comércio virtual, pois tem recursos que favorecem esta opção.

Neves(2013), ainda ressalta os pontos fortes a instalação consistente e segura, permite um grande número de extensões e também tem uma comunidade atuante. Já como pontos fracos apresentam uma customização ou adição de funcionalidades que são complicadas para um usuário não técnico, possui uma fraca interação no qual não é adequado para blogs.

2.1.1.3 Drupal

O Drupal foi criado por *Dries Buytaert,* inicialmente como um pequeno site de notícias e avisos. Á medida que os seus utilizadores começaram a discutir e aplicar no site novas tecnologias, a sua estrutura foi se aperfeiçoando até que *Dries*

resolveu, em 2001, lançar esse sistema como um software de código aberto para o mercado, sob nome comercial de Drupal. Segundo Silva (2013), “ele é projetado para ser facilmente aumentado através de módulos e temas. Alguns vêm com toda instalação do Drupal, enquanto outros podem ser retirados de modo individual através do seu site e instalados separadamente”.

O Drupal é ideal para projetos grandes ou que necessitam realizar escalabilidade.

A Desvantagem de utilizar o Drupal é que este possui uma comunidade menor em comparação com os dois CMS citados acima, isso dificulta em questões de suporte,recursos além de exigir um conhecimento técnico avançado para usuários.

2.2 SEGURANÇA

2.2.1 Conceitos

Segundo o dicionário Michaelis (2002), segurança é uma condição marcada por uma sensação de paz e tranquilidade. Sêmola (2003) define segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.A segurança da informação como área do conhecimento visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos. Silva e Silveira (2007), descrevem os pilares da segurança da informação como: “A integridade da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental. A disponibilidade garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário. A confidencialidade da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do conteúdo”. Sêmola (2003) acrescenta a estes

objetivos os de: “legalidade, garantia de que a informação foi produzida em conformidade com a lei. Autenticidade, garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação”.

2.2.1.1 Informação

Na era da informação, o patrimônio das empresas deixou de ser composto apenas de bens tangíveis, mas também composto da informação como um ativo da empresa ou seja um bem valioso para a empresa.

De acordo com a publicação realizada pela Alleasy(2018), no qual explica a importância da informação, em tempos de troca de dados de maneira instantânea usando a internet e com o armazenamento de um volume de informações jamais visto, torna necessário ainda mais as classificações da informação.

É necessário saber o nível das informações que a empresa possui e classificá- la.

É possível ser classificado em 4 partes.

Pública, quando a informação pode vir a público sem consequências danosas ao funcionamento normal da organização mantendo a integridade e disponibilidade.

Interna, esse tipo de informação deve ser evitado, embora as consequências do uso desautorizado não sejam por demais sérias. Sua integridade é importante.

Secreta, a informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a empresa.

Confidencial, informação restrita aos limites da organização, cuja divulgação ou perda pode levar ao desequilíbrio operacional e, eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo, podendo permitir uma vantagem do concorrente.

Segundo o artigo publicado por Marciano (2006) os ativos da informação estão sujeitos a diversos eventos e potencialidades nocivos à sua segurança, dividido em três categorias: ameaças, vulnerabilidades e incidentes.

Segundo Dias(2006) uma das definições apresentadas para ameaça é “evento ou atitude indesejável (roubo,incêndio, vírus, etc) que potencialmente remove, desabilita, danifica ou destrói um recurso.”Recurso este podendo ser um “componente de um sistema computacional, podendo ser recurso físico,software,hardware ou informação”Dias(2006).

Segundo Marciano(2006), uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda um usuário ou um gestor de informações

consideradas sensíveis. Vulnerabilidade ainda pode ser a interseção de três elementos: uma suscetibilidade ou falha do sistema, acesso do atacante a falha e a capacidade do atacante explorar a falha.

Segundo o *Centro de Estudos,* Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores. Em geral, toda situação onde uma entidade de informação está sob risco é considerado um incidente de segurança.

2.2.2 Ataques mais Comuns

Segundo Marciano(2006), “um ataque corresponde à concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante a uma ação deliberada e por vezes meticulosamente planejada”. Segundo uma publicação do Stefanini(2019) um ataque é feito seguindo os seguintes passos.
Na primeira etapa, o invasor reconhece uma potencial brecha. Quanto antes isso é feito, menor é a probabilidade de ele dar errado. Durante a análise, o software avalia a possibilidade de ataques e quais ferramentas são as ideais para a situação.
Na adaptação, a segurança do dispositivo está em risco e seus dados podem ser acessados remotamente. Por fim, o invasor tem acesso a todas as informações que deseja. Ele pode, inclusive, alterar e deletar elementos cruciais para o funcionamento da empresa.

De acordo com a publicação realizada pela sucuri a respeito do *ToP 10 Open Web Application Security Project - OWASP(*2018*)* relata as 10 vulnerabilidades mais comuns , mostra seus riscos, impactos e contramedidas. Destas 10, três serão listadas neste trabalho.

2.2.2.1 Injeção

Uma injeção de código ocorre quando um invasor envia dados inválidos para o aplicativo Web com a intenção de fazer algo que o aplicativo não foi projetado/programado para fazer.

O exemplo mais comum sobre essa vulnerabilidade de segurança seja a consulta *Structured Query Language* - SQL consome dados não confiáveis.
Essa consulta pode ser explorada chamando a página da web que a executa com o seguinte URL: http://example.com/app/accountView?id= 'ou' 1 '=' 1, causando o retorno de todas as linhas armazenadas na tabela de banco de dados. Abaixo está o código de execução um modelo de código de execução.

Figura 1 - código de execução

```
String query = “SELECT * FROM contas WHERE custID = '” + request.getParameter (“id”) + “'”;
```

Fonte: Os autores

O núcleo de uma vulnerabilidade de injeção de código é a falta de validação e limpeza dos dados usados pelo aplicativo Web, o que significa que essa vulnerabilidade pode estar presente em quase qualquer tipo de tecnologia.
Qualquer aplicação que aceite esses parâmetros como entrada pode ser potencialmente vulnerável a um ataque de injeção de código. A prevenção de vulnerabilidades de injeção de código depende realmente da tecnologia que está sendo utilizada. Caso estiver utilizando o WordPress, pode minimizar as vulnerabilidades de injeção de código, mantendo-o no mínimo de plugins e temas instalados.
Prevenir injeções de SQL requer manter os dados separados de comandos e consultas.
Use LIMIT e outros controles SQL em consultas para impedir a divulgação em massa de registros em caso de injeção de SQL.
A opção ideal é utilizar uma API segura, que evite ou use intencionalmente ou forneça uma interface parametrizada ou migrar para usar *Object Relational Mapping Tools -ORMs.*

2.2.2.2 Autenticação quebrada

Uma vulnerabilidade desse modo pode permitir que um invasor use métodos manuais e ou automáticos para tentar obter controle sobre qualquer conta que deseja em um sistema ou pior ainda obter o controle completo sobre o sistema.

A autenticação quebrada geralmente se refere a problemas lógicos que ocorrem no mecanismo de autenticação do aplicativo, como um mau gerenciamento de sessões propenso à enumeração de nome de usuário, quando um atacante usa técnicas de força bruta para adivinhar ou confirmar usuários válidos em um sistema.
Para minimizar riscos é importante, evitar de deixar a página de login dos administradores acessíveis ao público a todos visitante do site. Como por exemplo: /administrador no Joomla, /wp-admin/ no WordPress, /usuário/login no Drupal. Utilizando outros prefixos.
A segunda forma mais comum dessa falha é permitir que os atacantes utilizam a combinação de usuário e senha nessas páginas.
As recomendações técnicas da OWASP são as seguintes:
Sempre que possível, implementar a autenticação multifator para impedir ataques automatizados, de preenchimento de credenciais, força bruta e reutilização de credenciais roubadas.
Não enviar ou implantar com credenciais padrão, principalmente para usuários administrativos.
Limite ou adie cada vez mais as tentativas de logon com falhas. Registre todas as falhas e alerte os administradores quando forem detectados ataques de credenciais, força bruta ou outros ataques.

2.2.2.3 Exposição de dados confidenciais

A exposição sensível a dados é uma das vulnerabilidades mais difundidas na lista da OWASP. Consiste em comprometer os dados que deveriam ter sido protegidos.Exemplos de dados sensíveis: Credenciais de acesso, número de cartão de crédito, informação médica, e outras informações vitais à empresa ou o de cunho pessoal.

Identificar quais dados são sensíveis de acordo com as leis de privacidade, requisitos regulatórios ou necessidades de negócios.
Armazenar senhas usando *função de hash*, como Argon 2,scrypt,bcrypt ou PBKDF2.
Garantir que algoritmos, protocolos e chaves padrão atualizados e fortes estejam em vigor, utilizando o gerenciamento de chaves adequado.

3 DELINEAMENTO METODOLÓGICO

Os dados levantados a partir dessa pesquisa bibliográfica tem como o objetivo de explicar o que é um Sistema de Gerenciamento de Conteúdo - CMS e sua importância para a divulgação de informações, quais são os principais no mercado e como usá los para cada situação que for necessária, como por exemplo do uso do WordPress, para a criação de blogs e sites institucionais, o Joomla para criação de e-commerce , e o Drupal para projetos mais robustos ou que necessitam de ser escalável.

O entendimento do que é Segurança da Informação, seus pilares, integridade, disponibilidade e confidencialidade, fazendo uma conexão com a classificação da informação . Relatando os principais ataques no mundo na Web e no WordPress, suas respectivas contramedidas.

Com isso será apresentado os principais ataques ao WordPress de acordo com uma publicação realizada do Sucuri (2019) e suas contramedidas, tendo como ponto de vista do atacante e de quem fará a retaguarda e explicando a sua importância.

4 RESULTADOS

4.1 Vulnerabilidades do WordPress

Será abordado as principais vulnerabilidades no plataforma de acordo com a publicação da Sucuri (2019) , além de como evitar os principais ataques.

4.2 Software Desatualizado

Segundo um levantamento feito pela Sucuri junto com a GoDaddy (2019), apresentou diversos pontos de vulnerabilidades em sites wordpress e comparativo com outros cms também. Um dos pontos foram o sistema desatualizado. Segundo o relatório em 2019, 56% de todos os aplicativos CMS estavam desatualizados no ponto de infecção. Muitos ignoram a atualização do WordPress, por falta de conhecimento ou por achar que o site nunca vai ser invadido porque não é tão relevante. Mas nas atualizações sempre vem correções importantes de bug e segurança ou adição de uma nova funcionalidade. Por isso sempre é necessário sempre manter o core do WP atualizado.

Além do core do WP, manter os plugins sempre atualizados, verificando patchs de atualização. Analisar as possíveis brechas de segurança que os plugins em seu site pode apresentar.

O sitecheck do Sucuri é uma ferramenta web que faz uma checagem de todos plugins instalados, verifica malware, versão do php, verifica se o site está em alguma blacklist e dá outras dicas para manter o seu site seguro. Para que possa verificar no sitecheck basta inserir o domínio do seu site.

4.3 SEO (Search Engine Optimization)

Ainda sobre o relatório foi relatado (2019), que cerca de 62% dos sites (a partir da análise dos casos obtidos pela Sucuri e a GoDaddy) tiveram uma infecção por spam de SEO.

Segundo o site Seo Master (2013), SEO (Search Engine Optimization), também conhecido como otimização de sites, é rapidamente definido como uma forma de aumentar os acessos do seu site através de um conjunto de técnicas e estratégias que permitem que um site melhore seu posicionamento nos resultados orgânicos dos mecanismos de busca, como Google e Bing. No WordPress o plugin de SEO mais conhecido é o Yoast SEO ele possui mais de 135 milhões de downloads. Bots são programados pelos atacantes realizando um ataque de spam seo a inundar bases de dados dos websites com informações desnecessárias ou maliciosas.

Muitos desses ataques estão refletido a softwares desatualizado . Como o estudo representa cerca de 44% de todos os sites vulneráveis tinham um mais de uma ferramenta instalada vulnerável e 10% deles tinham pelo menos quatro componentes vulneráveis.Abaixo a tabela mostra quais os principais softwares com vulnerabilidades e a referente porcentagem. E faz um alerta para que sempre manter os softwares atualizados com as últimas versões de segurança para reduzir os riscos.

Figura 2 - Os dados referentes aos plugins com maior índice de vulnerabilidade relatado.

Top Software with Vulnerabilities	Percentage
Contact Form 7	34.73%
Yoast SEO	15.83%
WP Mail SMTP by WPForms	6.00%
SnapCreek	5.99%
Slider Revolution	5.68%
Freemius Library	4.92%
File Manager	3.42%
Gravity Forms	2.61%
Yellow Pencil	2.20%
Blog Designer	1.87%

(Fonte:Sucuri (2019),Relatório produzido pela Sucuri em conjunto com a Godaddy)

Uma forma também de evitar os ataques de spam é a utilização de captcha. Um software bastante utilizado é o Advanced noCaptcha & invisible captcha possui mais de 100 mil instalações ativas. Com ele é possível colocar captcha em qualquer formulário no site, incluindo no painel administrativo para efetuar o login e o “perdeu a senha” .

4.4 Permissão de Usuários

Como explica a publicação no Hostinger (2017),um ponto importante é no processo de criação de usuários, deve criar políticas de para criação de senhas e de permissões para navegar no painel administrativo.

Quando é criado um usuário preciso que redefina a senha colocando uma combinação de números, letras e caracteres especiais e que não deixe ela exposta para que outra pessoa possa se passar por ele. Na questão sobre Permissão a nível de usuário deve verificar se é necessário que o usuário tenha a função de administrador, editor ou outra função. E encaixá lo na função adequada a cada caso.

Como ressalta o hostinger (2017), existem 5 tipos de usuários que são: Administrador,Editor,Autor,Contribuinte e Assinante.

Administrador: possui acesso total a todas as funcionalidades disponíveis pelo site.Como por exemplo controle total a usuários,temas, plugins, posts,comentários,páginas e configuração do wordpress.

Editor: possui acesso a gerenciar e publicar quaisquer posts, mesmo aqueles criados por outros usuários. Por exemplo controle total a posts,páginas e comentários moderação. Além de poder editar seu próprio perfil.

Autor: essa função de usuário pode apenas gerenciar e publicar apenas suas próprias postagens. Possui controle total apenas em suas próprias postagens e pode editar seu próprio perfil.

Contribuinte: podem gerenciar suas próprias postagens sem publicá-las.

Assinante: podem apenas gerenciar seu perfil.

4.5 Backup

Outra questão se diz respeito ao Backup. Como explica Oliveira(2003) Backup ou cópia de segurança é a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados. É muito importante manter uma rotina, fazendo o backup tanto dos arquivos e do banco de dados, para caso ocorra algo informado acima poder restaurar de imediato. É interessante manter rotinas para cada tipo de backup por exemplo os arquivos e banco a cada 15 dias, em horário específicos. O WordPress disponibiliza um plugin gratuito no qual podemos fazer todo esse processo de backup se chama Updraftplus (2017). Fácil de configurar, seu backup pode ser salvo em uma conta na updraftplus em uma versão paga da ferramenta mas também de forma gratuita na nuvem em aplicações como Google Drive,Dropbox, Amazon S3 e entre outros. Além de ser notificado quando o backup acontecer.

4.6 Boas Práticas no WordPress

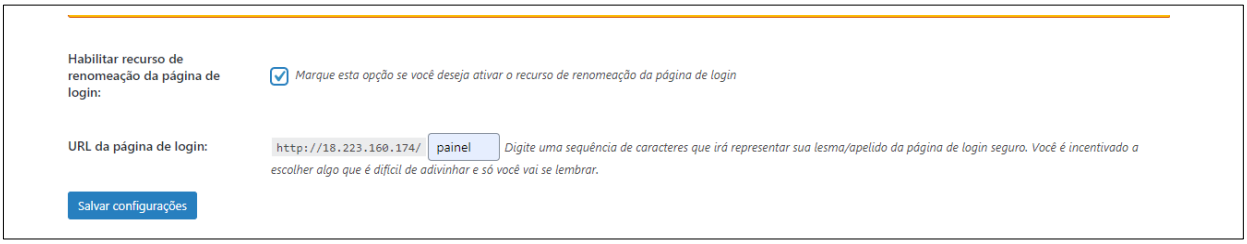
Além de todas essas questões tratadas, outro ponto importante seria algumas práticas no seu website como:

4.6.1 Alteração na URL de administração do Wordpress

Como explica no blog da hostnet(2020),por padrão, a url de acesso ao painel de administração do wordpress é o meuendereco.com.br/wp-admin, atacantes utilizam esse padrão para executar ataques de força bruta. Uma forma de dificultar esse ataque é a alteração desta url.

Para realizar essa alteração utilize a ferramenta All In One WP Security(será explanado mais sobre essa ferramenta ao decorrer do artigo). Força Bruta > Renomeação da página de login.

Figura 3 - Renomeação da página de login



(Fonte: os autores)

4.6.2 Desabilitando execução PHP em pastas específicas

Como explica no hostinger(2019), criminosos podem fazer upload de scripts nas pastas de uploads do WordPress. Por padrão esta pasta é usada somente para upload de arquivos de mídia. Para desabilitar a execução é necessário a criação de um arquivo .htaccess no diretório /wp-content/uploads com o seguinte script.

Figura 4 - Negando o upload de arquivos php

```
<Files *.php>
deny from all
</Files>
```

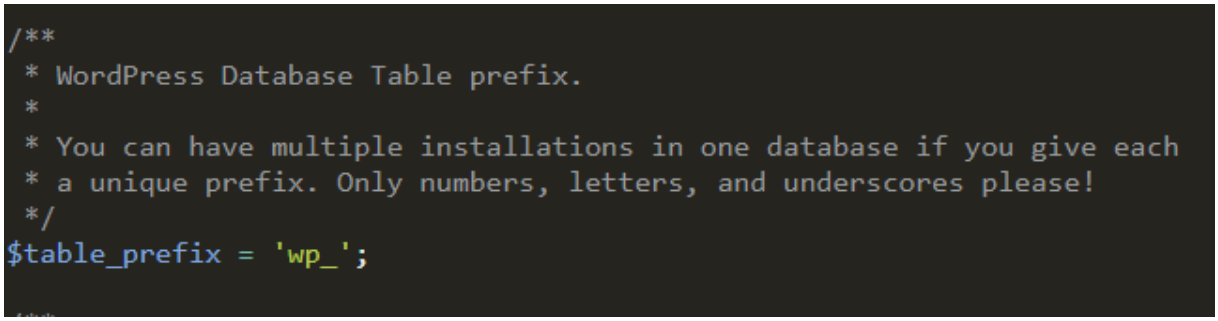
4.6.3 Alterando o prefixo padrão do WordPress para evitar SQL Injections

Segundo o Devmedia (2007), é uma técnica de ataque baseada na manipulação do código SQL, que é a linguagem utilizada para troca de informações entre aplicativos e bancos de dados relacionais.

Como retrata o hostinger(2019), no wordpress ao instalar o mysql deve sempre se atentar ao prefixo das tabelas no banco, pois pode ser um vetor de ataque de sql injection. Por padrão o prefixo é o “wp”. Durante a instalação do wordpress é suma importância a troca desse prefixo por outro a fim de dificultar o ataque.
Para alterar o prefixo de site WordPress já existente, é importante salientar que deve ser feito um backup do banco com suas tabelas, antes de iniciar esse procedimento.

Utilizando um Cliente FTP ou um Gerenciador de Arquivo de sua hospedagem, encontre o arquivo wp-config.php e busque por $table_prefix.

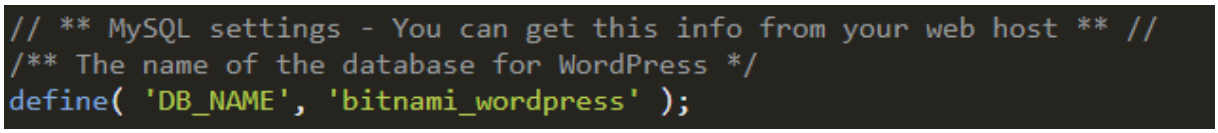
Figura 5 - Alterando o prefixo da tabela no arquivo wp-config.php



(Fonte: os autores)

Pode ser inserido números e letras. Depois de salvar verifique o nome do banco no mesmo arquivo wp-config.php. Será utilizado o prefixo ‘wp_sec’ nas tabelas.

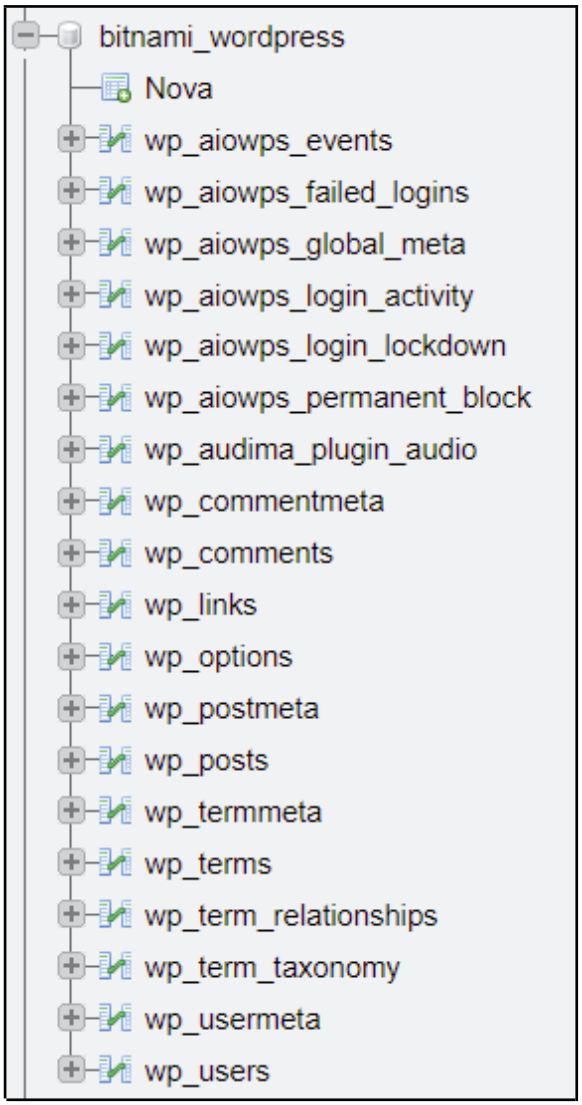
Figura 6 - Verificando o nome do banco de dados no arquivo wp-config.php



(Fonte: os autores)

A instalação padrão do Wordpress contém 12 tabelas, cada uma delas deve ser atualizada.

Figura 7 - Listagem das tabelas do banco de dados utilizando o phpmyadmin



(Fonte: os autores)

Em alguns temas ou plugins é possível criar tabelas adicionais no banco de dados. Com isso as tabelas adicionais devem ser atualizadas também.

Alterar cada tabela manualmente vai exigir um tempo excessivo, mas podemos usar o SQL queries para acelerar o processo.

Figura 8 - Exemplo de renomeação das tabelas do banco de dados de forma automática

```
RENAME table `wp_commentmeta` TO `wp_seccommentmeta`;
RENAME table `wp_comments` TO `wp_seccomments`;
RENAME table `wp_links` TO `wp_seclinks`;
RENAME table `wp_options` TO `wp_secoptions`;
RENAME table `wp_postmeta` TO `wp_secpostmeta`;
RENAME table `wp_posts` TO `wp_secposts`;
RENAME table `wp_terms` TO `wp_secterms`;
RENAME table `wp_termmeta` TO `wp_sectermmeta`;
RENAME table `wp_term_relationships` TO `wp_secterm_relationships`
RENAME table `wp_term_taxonomy` TO `wp_secterm_taxonomy`;
RENAME table `wp_usermeta` TO `wp_secusermeta`;
RENAME table `wp_users` TO `wp_secusers`;
```

(Fonte: os autores)

Dependendo do número de plugins que você tem instalado, alguns valores do seu banco de dados terão que ser atualizados manualmente. Isto pode ser feito executando SQL queries separadas em options e usermeta.

Para a table options deve usar:

Figura 9 - obtendo todos os dados da tabela *option* onde se inicia o campo por wp

```
SELECT * FROM `wp_secopitions` WHERE `option_name` LIKE '%wp_%'
```

Para a table usermeta deve usar:

Figura 10 - obtendo todos os dados da tabela *usermeta* onde se inicia o campo por wp

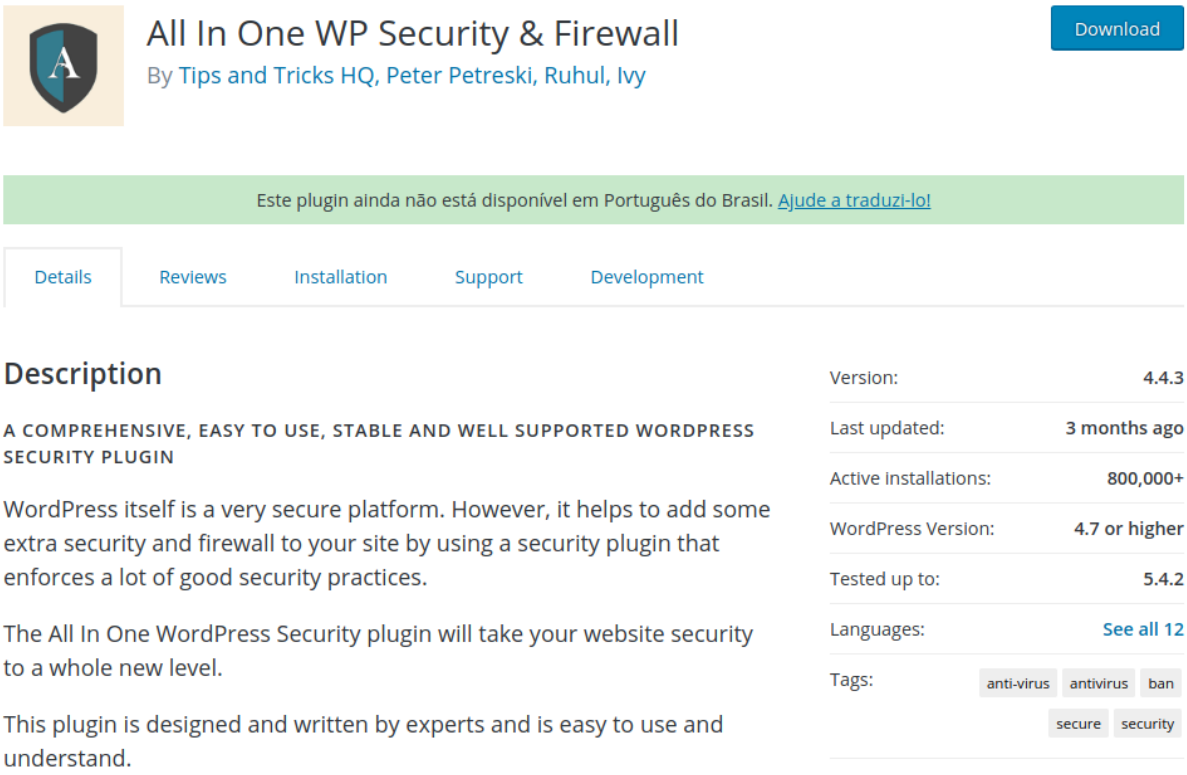
```
SELECT * FROM `wp_secusermeta` WHERE `meta_key` LIKE '%wp_%'
```

Basta depois atualizar os campos com o prefixo antigo (wp_) para o novo prefixo. Agora a segurança do seu banco de dados está melhor a impedir ataques de SQL Injection.

4.7 Plugin de Segurança

Além de todas essas práticas é suma importância o uso de um plugin de segurança. Com mais 800.000 instalações ativas e 100% gratuito o All In One WP Security & Firewall(2020), é um plugin de segurança com fácil configuração e bem completo.

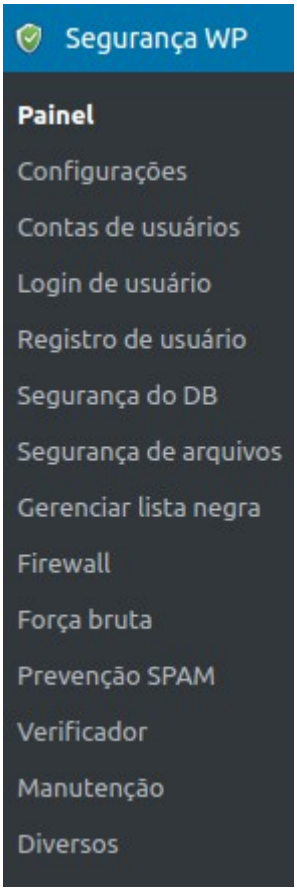
Figura 11- Plugin de Segurança disponível no wordpress.org



(Fonte: All in one Security and Firewall(2020))

A ferramenta possui diversas funções, mas dentre todas essas funcionalidades será abordada 5 delas:

Figura 12 - Ferramentas do Plugin All One WP Security & Firewall



(Fonte: os autores)

4.7.1 Contas de Usuários

Por padrão no wordpress o usuário administrador vem com user ‘admin’ devemos fazer a alteração do mesmo bem como o nome de login não pode ser o mesmo nome do ‘apelido’. Esta modificação deve ser realizada pois como explica no One(2020), hackers muitas vezes tentam obter acesso à sua administração WordPress com um ataque de força bruta, com o nome de login padrão fica mais fácil a tentativa de ataque. No plugin de segurança (All In One WP Security & Firewall) é realizada a alteração em Contas de Usuário > Nome de usuário WP.

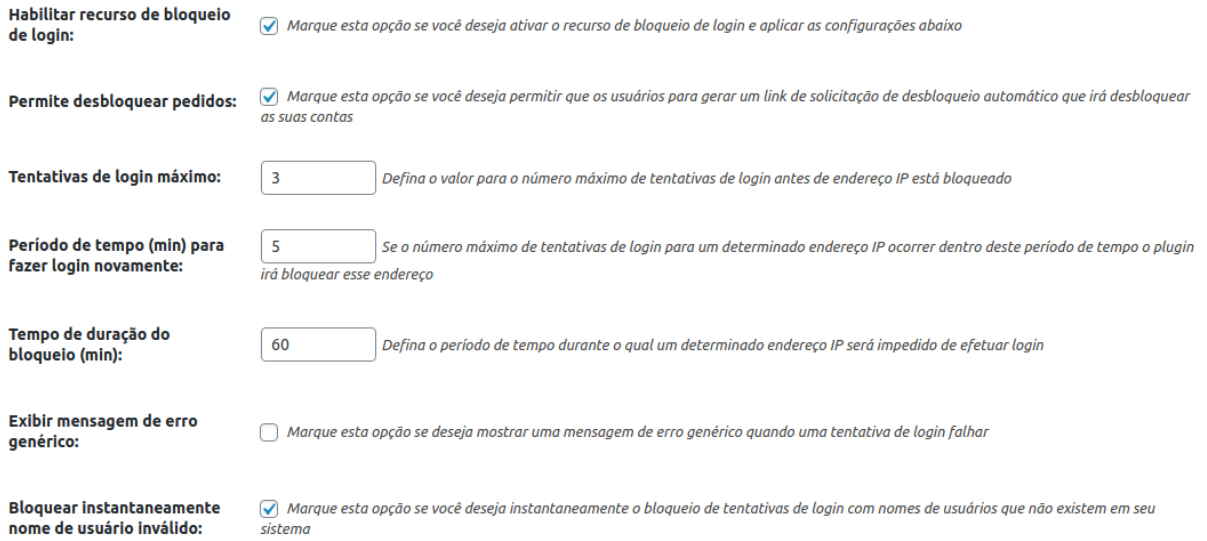
Para realizar a alteração no ‘apelido’ o nome que é exposto publicamente para que ele não seja o mesmo do login o caminho é Contas de Usuário > Nome de exibição. Após cada alteração terá um check com uma pontuação ao lado. Para cada ajuste nas ferramentas do plugin tem uma pontuação e um nível.

4.7.2 Login de Usuário

De acordo com a Documentação do Segurança WP(2020) fornece uma ferramenta para controle de acesso ao usuário. Nela é possível delimitar o máximo de tentativas de login, o período de tempo para fazer o login novamente, tempo de duração de bloqueio, nesta última opção o range do ip do usuário é bloqueado pelo

o tempo em que o administrador quiser, podendo, antes do tempo realizar o desbloqueio manual no próprio Segurança WP. Outra opção também é de bloquear o nome de um usuario invalido, ou seja, que não existe no painel. Ao final das configurações o painel pode se encontrar assim:

Figura 13 - Painel das configurações de Login do usuário no Plugin de Segurança



(Fonte: os autores)

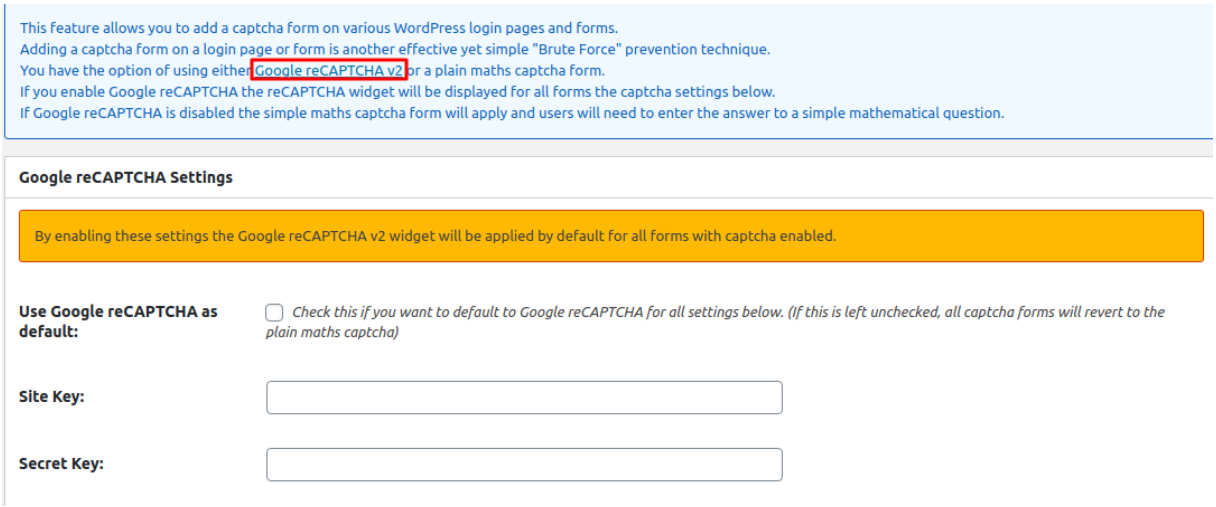
4.7.3 Força Bruta

Nesta opção o plugin trás funcionalidades bem interessantes. É permitido a troca da url de acesso ao painel, pois o caminho padrão é o wp-admin, assim como explica a Hostgator(2020),para realizar essa alteração basta acessar a aba renomeação da página de login e colocar o nome da url que deseja. Outra funcionalidade é o uso do captcha, que habilitado quando o usuário vai iniciar a sessão, resetar a senha dentre outras situações. Para habilitar entre na aba Captcha Login e marque o checkbox.

Figura 14- Configurações de Força Bruta do Plugin

(Fonte:os autores)

Nele também é permitido uma adesão do reCaptcha do Google conforme explicado abaixo.



(Fonte: os autores)

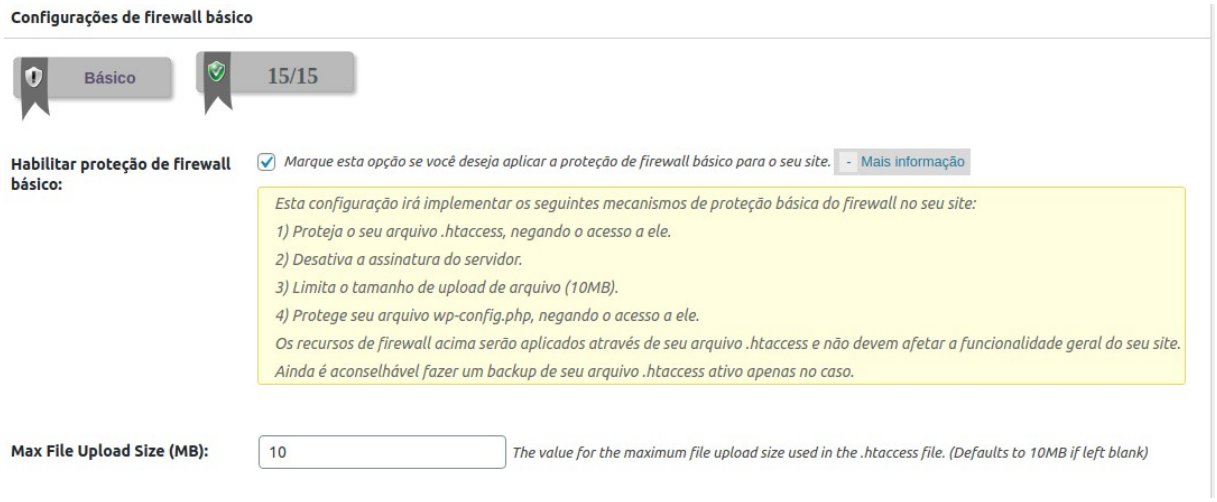
Para realizar a configuração deste captcha, deve clicar onde está o texto em destaque após isso, será levado a uma página na qual deve ser preenchida com o domínio do seu site e a versão do captcha. Após, será gerado uma chave do site e uma chave secreta que deverá ser inserida nestes campos respectivamente.

Navegando por Força Bruta > Pote de Mel.O Pote de Mel apresenta funcionalidade contra bots. Essa funcionalidade consiste em adicionar um campo visível apenas a robôs no formulário de login, no qual se ele é marcado o plugin detecta que é um robô que está fazendo login e faz com o que o bot seja redirecionado para o seu endereço localhost - http://127.0.0.1.

4.7.4 Firewall

É importante além de todas essas configurações realizadas o uso de um firewall para melhorar o nível de segurança.

Figura 15- Configurações de Firewall do Plugin de Segurança



(Fonte: os autores)

4.7.5 Proteção de Cópia

De acordo com a Documentação do Segurança WP(2020),essa funcionalidade ela é interessante se você deseja que nenhum visitante copie as informações do seu site por meios de teclas de atalho e nem utilizando o cursor do mouse. Localizada em Diversos > Proteção de Cópia.

Ao final de todos os ajustes no painel do Segurança WP (All In One WP Security & Firewall) é exibido um velocímetro de 0 à 515 e nele irá ter a pontuação baseada nas configurações realizada pelo administrador. Mas não é necessário que todas as configurações serem feitas para obter o valor máximo, as configurações devem ser realizadas adequadamente para cada cenário.

5 CONSIDERAÇÕES FINAIS

Foram abordados os conceitos sobre o que é um CMS,que seria um sistema de gerenciamento de conteúdo,com o objetivo de criar e gerenciar o conteúdo na internet de maneira mais simples e ágil. Os principais no mercado são, WordPress, Joomla e Drupal. Sendo o WordPress, o abordado neste trabalho por ter uma comunidade mais atuante em relação aos seus concorrentes, ser o líder de mercado, além de apresentar mais intuitivamente como gerenciar o conteúdo, por possuir uma curva de aprendizado menor em relação aos demais , ou seja mais simples o entendimento. Em um site institucional por exemplo, sendo rentável tanto a equipe e a empresa que presta serviço, por ser opensource ou seja código aberto não tem gastos com licença e a equipe a facilidade de trabalhar com a ferramenta. Foram explanados conceitos de segurança, bem com os pilares do mesmo, integridade tem como objetivo garantir a exatidão da informação, disponibilidade sempre manter a informação ou o serviço disponível e confidencialidade é a garantia de que somente pessoas autorizadas terão acesso a informação, protegendo-a de acordo com o grau de sigilo do conteúdo e esses aplicados a classificação da informação a sua empresa. Neste trabalho foram listados os principais ataques, como Backdoor e Ddos (Ataque de negação de Serviço) e os ataques mais comuns como injeção sql, dados sensíveis e quebra de autenticação a todo tipo de aplicação e os mais relatados de acordo com a publicação do Sucuri (2019) a plataforma do WordPress como por exemplo o Spam SEO e como evitá los, com o objetivo que o administrador do site entenda como funciona cada ataque e se previna utilizando as contramedidas sugeridas.

Diante dessas infomações, é possivel entender como o CMS é importante nos dias de hoje, por otimizar os envios das informações seja por sites instituicionais, blogs e dentre outros. E reforçar a necessidade de sempre estar bem informado sobre os ataques mais comuns relatados na Web e como se defender.Foram apresentadas ferramentas no wordpress gratuitas, que ajuda na proteção do seu site além de boas práticas de Segurança no WordPress foram sugeridas a fim de que o administrador do site, verifique os temas abordados e que possa implementar todas essas práticas e conceitos no seu local de trabalho. Para assim manter o seu WordPress o mais seguro possível.

6 TRABALHOS FUTUROS

Este artigo é sugerido para profissionais que administram sites em WordPress, para que sigam as melhores práticas de desenvolvimento e manutenção. Ressaltando as boas práticas, que muitos ignoram , como por exemplo manter o seu wordpress atualizado sempre bem como os seus plugins. Seguindo as práticas informado neste artigo é possível manter um bom nível de segurança no seu wordpress.

Serão abordados técnicas mais arrojadas tanto de prevenção quanto de ataque explorando mais a fundo os principais ataques relatados pela OWASP e a Sucuri.

REFERÊNCIAS

SILVA, André Filipe Ferreira da. **Os sistemas de gestão de conteúdos: as diferenças entre Joomla, Drupal e Wordpress**. 2013. Dissertação de Mestrado

NEVES, Luã Castro. **Sistema de Gerenciamento de Conteúdo**. 2013. Tese de Doutorado. UNIVERSIDADE CATÓLICA DE PELOTAS

TOBIAS, Helder.**O que é CMS, como funcionam e quais são os mais utilizados**. DialHost, 2018. Disponível em: (https://www.dialhost.com.br/blog/o-que-e-cms/). Acesso em: (26/06/2020)

SÊMOLA, Marcos. Módulo Security Solutions S/A. **Gestão da segurança da informação: visão executiva da segurança da informação aplicada ao security officer**. 2003.

SILVA NETTO, Abner da; SILVEIRA, Marco Antonio Pinheiro da. **Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas**. **JISTEM-Journal of Information Systems and Technology Management**, v. 4, n. 3, 2007

Alleasy. **Classificação das informações: como definir níveis de segurança?**. Alleasy, 2018. Disponível em: (https://www.alleasy.com.br/2018/06/19/classificacao-de-informacoes/). Acesso em: (26/06/2020).
MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem socia**l. 2006
DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Axcel Books, 2000

PALMA, Fernando. **Incidentes de Segurança da Informação: conceito,exemplos e cases**. Portal GSTI, 2014. Disponível em: (https://www.portalgsti.com.br/2014/01/incidentes-de-seguranca-da-informacao-conceito-exemplos-e-cases.html). Acesso em: (26/06/2020)

Stefanni Group. **Ataques à segurança da informação: conheça as principais ameaças**. Stefanni Group, 2019. Disponível em: (https://stefanini.com/pt-br/trends/artigos/ameacas-a-seguranca-da-informacao). Acesso em: (26/06/2020)

Sucuri. **OWASP Top 10 Security Risks & Vulnerabilities.** Sucuri, 2020. Disponível em: (https://sucuri.net/guides/owasp-top-10-security-vulnerabilities-2020/). Acesso em: (26/06/2020)

Computerworld**, Wordpress Representa 30% dos Sites Web**. Computerworld, 2018. Disponível em: (https://computerworld.com.br/2018/03/05/wordpress-representa-30-dos-sites-na-web).
Acesso em: (16/04/2020).

Clemente,M. **O que é WordPress, para que serve e principais segredos**. Rock Content, 2019. Disponível em: (https://rockcontent.com/blog/wordpress/). Acesso em: (11/04/2020).

Sucuri**, 2019 Website Threat Research Report**. Sucuri, 2019.
Disponível em: (https://sucuri.net/reports/2019-hacked-website-report/). Acesso em: (11/04/2020)

Sucuri sitecheck, Free website security check & malware scanner. **Sucuri sitecheck**, 2019. Disponível em: (https://sitecheck.sucuri.net/). Acesso em: (11/04/2020).

Ariane, G**. Como criar e gerenciar licenças e permissões para usuários de WordPress**. Hostinger, 2017.

Disponível em: (https://www.hostinger.com.br/tutoriais/criar-gerenciar-licencas-permissoes-wordpress/).
Acesso em: (08/05/2020).

OLIVEIRA, Wilson. **Técnicas para hackers e soluções para segurança: versão 2**. Centro Atlantico, 2003.

Updraftplus**, UpdraftPlus WordPress Backup Plugin**. UpdraftPlus, 2020.
Disponível em: (https://wordpress.org/plugins/updraftplus/).
Acesso em: (08/05/2020).

Advanced noCaptcha & invisible Captcha (v2 & v3). Advanced noCaptcha & invisible Captcha (v2 & v3),2020.
Disponível em: (https://br.wordpress.org/plugins/advanced-nocaptcha-recaptcha/#description)
Acesso em: (11/05/2020)

Hostnet, **Alterando a URL de administração WordPress**. Hostnet, 2020.
Disponível em: (https://www.hostnet.com.br/info/alterando-a-url-de-administracao-do-wordpress/).
Acesso em: (08/06/2020).

Hostinger**. Segurança WordPress: 12 dicas de segurança na internet que todo site precisa ter**, Hostinger, 2019.
Disponível em: (https://www.hostinger.com.br/tutoriais/como-aumentar-seguranca-no-wordpress/).
Acesso em: (08/06/2020).

DevMedia, SQL Injection**, DevMedia,** 2007
Disponível em: (https://www.devmedia.com.br/sql-injection/6102)
Acesso em: (09/06/2020).

All In One WP Security & Firewall. A comprehensive, easy to use, stable and well supported wordpress security plugin**. All In One WP Security & Firewall,** 2020.

Disponível em: (https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/). Acesso em: (11/06/2020).

One**, Melhore a segurança do seu site Wordpress,** One**,** 2020.

Disponível em:

(https://help.one.com/hc/pt-br/articles/115005586009-Melhore-a-seguran%C3%A7a-do-seu-site-WordPress/).

Acesso em: (11/06/2020).

Hostgator**, Como alterar o link de acesso ao painel do wordpress?**. Hostgator, 2020.

Disponível em:

(https://suporte.hostgator.com.br/hc/pt-br/articles/360007993313-Como-alterar-o-link-de-acesso-ao-painel-do-WordPress-).

Acesso em: (12/06/2020).

Neto,Costa Paulo**. WordPress é seguro?**. 2WP**,** 2020.

Disponível em: (https://2wp.com.br/artigos/seguranca-do-wordpress/). Acesso em: (12/06/2020).