INTERNET PENSANTE®

Inovando a cada instante

Checklist de Segurança, para o premiado e fantástico CMS Open Source:

Joomla!®

Versões: 3.x, 4.x e, em breve 5.x

Autor: Bráulio Machado Campos – CEO – Internet Pensante®.
Versão: #08, revisada; Ano de 2023.

*As orientações apresentadas nesse **Checklist**, são em sua maioria para o CMS Joomla e Servidores dos Sistemas Operativos Linux baseados, em sua última versão estável em produção do ano de 2023. Mas também podem servir para outros CMS, em algumas partes. Não obstante, preste bastante atenção ao fazer suas alterações e, sempre consulte a documentação de seu CMS favorito, aqui no caso, o CMS Joomla.*

→ ***ATENÇÃO:*** *Este pequeno Checklist e, seu Autor, não se responsabilizam pelas informações apresentadas aqui e alterações inadequadas que você em seu CMS JoomLa, como desenvolvedor e, fizer seu CMS Joomla em produção. Portanto, use uma instalação do Joomla em **não** produção em seu computador, para você treinar, antes de colocar em prática no seu projeto final e torná-lo online e público na Rede Mundial de Computadores: A Internet.*

→ ***SUGESTÃO:*** ***Imprima*** *essas dicas e, use-as como o seu **Checklist** ao desenvolver com o **Joomla**, em sua última versão estável, segura e, em produção.*

→ **MOTIVAÇÃO:** O Autor desse trabalho, cansado de sempre ter problemas de segurança com o Joomla, resolveu criar esse **Checklist**, **INÉDITO**, para sempre poder revisar o Joomla antes de publicar na Internet e entregá-lo ao cliente, tentando manter o site saudável para o público visitante.

→ **CHECKLIST:**

1) → Consertar a base do banco de dados instalado após a instalação do Joomla :
Extensões > Gerenciar > Banco de Dados > “Corrigir”;

2) → Manter o CMS Joomla sempre atualizado! O sistema do Joomla, envia e-mails para o seu e-mail cadastrado como usuário administrador, quando há novas atualizações do Joomla. Então, sempre confira se há novidades de updates em sua caixa de entrada de e-mail;

3) → Desabilite o relatório de erros pois eles pesam o seu website e mostram aos possíveis invasores, as falhas de segurança do seu website Joomla. Para desabilitar o relatório basta seguir a seguinte sequência: Configurações Globais – Sistema – Relatório de Erros -> nenhum;

4) → Barrar o diretório “../administrator”, pode ser feito com o arquivo ".htacces" e senha. MAS preste atenção: Mantenha o cabeçario original que o Joomla gera quando é instalado. Caso o contrário seja removido, dará erro 500 (“*Internal Server Error*”) e, praticamente seu site ficará travado e sem segurança;

5) → As versões 1.5.xx, 1.6.xx e, 1.7.xx, já estão **sem suporte** há bastantes anos ! Use sempre as mais recentes, a partir do Joomla 3.3.6 ou superior ! Muitas melhorias foram implementadas, inclusive na questão de segurança;

6) → Ter e fazer um backup do seu site sempre : Tanto dos arquivos do Site, quanto do Banco de Dados. Pode se utilizar o “Akeeba Backup” que é um componente **totalmente gratuito**: (https://www.akeeba.com/products/akeeba-backup.html). Também, após fazer a atualização dos componentes, módulos, plugins e, novas publicações nos artigos do site e, uploads de arquivos, fazer o backup, sempre;

7) → Ofuscar o diretório “../administrator” com plugins. Alguns plugins danificam o Joomla, em algumas atualizações do Joomla, portanto fique a tento e antes de fazer essa operação, faça um bakcup com o AkeebaBackup;

8) → ***AdminExile*** : Um redirecionador que gera um link com um *token* alternativo que só você tem acesso e, é através dele que você acessa seu painel de login para ir no painel de controle do Joomla (http://extensions.joomla.org/extension/adminexile);

9) → Alterar o nome de usuário "admin" para outro usuário super-administrador;

10) → Fazer senhas complexas/fortes para o superadministrador, inclusive com caracteres especiais (“!@#$%*()_+º), letras e números (Maiúsculos e minúsculos);

Exemplo: “ !EP!IfuCRexiS67Qec0# ”.

Site gerador de senhas complexas: https://my.norton.com/extspa/passwordmanager

11) → Instalar plugins de dupla autenticação ou autenticação de dois fatores. Quanto mais camadas, melhor. Mas aumenta as suas chances de errar durante o processo de login. **Exemplo:** (http://en.wikipedia.org/wiki/Google_Authenticator) e (https://support.google.com/accounts/answer/1066447?hl=en);

12) → **ATUALIZADO, ano de 2023:** Salvar todos os seus dados de acesso (usuário e senha) em um pendrive e caso queira, também pode anotar em uma folha de papel e guardar essas informações em um local de sua confiança; Use esse pendrive em um computador que não seja Linux, com por exemplo o Linux Ubuntu e outros, pois as distribuições Linux não te dão garantia e, para configurar o FireWall isso é todo a mão, diferente do Microsoft Windows ® (Sempre última versão, por exemplo Microsoft Windows 11 ®) que já vem todo configurado e, o Linux Distribuições não tem Antivírus muito bom gratuito, se quiser tem que pagar.

RESUMINDO: Não use Linux para produções online, só Microsoft Windows ® Systems Versões ou Apple Systems Versões, todos esses sistemas: Legalizados; Originais e, Pagos, vale muito a pena;

13) → Instalar plugin para evitar ataques do tipo *MySQL Injection*. Há plugins que te avisam via email sobre tentativas de ataques;

14) → Ativar *plugin* que avisa por e-mail novas atualizações do Joomla;

15) → Instalar componente, *plugin* de UpDate automático do Joomla.

Exemplo:

(https://www.joomlashack.com/blog/tutorials/auto-updates-joomla) e

(http://www.templatemonster.com/help/joomla-3-x-automatic-engine-update.html#gref);

16) → Procurar hospedagem de sites que possuem sistemas de defesa de ataques *DoS* ou D*DoS* ou DRDoS e que mostrem os IPs que mais acessam seu site e diretórios;

17) → Desabilitar módulos de login de usuários, deixá-los despublicados ou desinstalados. **Exemplo:**

GET 404 /component/users/?view=login&return=aHR0cDovL3Byb3NlZ2JoLmNvbS5ici9pbmRleC5waHA/b3B0aW9uPWNvbV9waG9jYWRvd25sb2FkJnZpZXc9Y2F0ZWdvcnkmZG93bmxvYWQ9MTg6YXZlbnRhaXMtZS1sdXZhcy1lbS10aGVybW9jcm9uLWlnbmlmdWdvLWF0ZS0yNTBvLWNhdC04LTkmaWQ9NDpwZXJpc3NhdG8=

Ou :

/component/mailto/?tmpl=component&template=allrounder-j1.6&link=31a090ce209f02470a4e91b98467838ecf871201 ;

18) → Verificar se o template é elegível para o uso em um site de produção e, principalmente não use template pirata. Verificar se não há históricos de códigos maliciosos em seu sistema de template ou framework, pesquise na internet sobre isso e, veja se esse template e ou seu framework são atualizados constantemente e ou, se o projeto do seu template ou framework foi descontinuado: morreu e o seu site está *offline*. Também, após isso e, testar uma infinidade de templates, remova/desinstale os que você não vai usar em seu site, afinal: "*Há algum motivo para manter sua roupa antiga ?* ";

19) → Não é mais recomendado mover o arquivo "configuration.php". Prestar atenção quando for atualizar o Joomla ! Sugestão em inglês no fórum oficial: (https://forum.joomla.org/viewtopic.php?t=770037);

20) → Há extensões que são pagas que são melhores, mas há extensões gratuitas que também dão conta do "recado";

21) → As permissões para diretório são "0755" e para arquivos são "0644". Verificar se estão assim;

22) → Instalar o seu Joomla sempre dos "MagicsBox" ou "Autoinstaladores" ou "ToolsBox"(Scripts pré-instalados) da empresa de hospedagem de sites que você contratou. Desenvolver o site sempre no servidor que vai estar em produção, para garantir as configurações das permissões de diretórios e, arquivos padrões do sistema da empresa de hospedagem;

23) → Link Oficial para o "Security Checklist" (Lista de Controle): https://docs.joomla.org/Security_Checklist ;

24) → Link Oficial para a "A Few Basic Security Rules" (Algumas regras básicas de segurança): http://vel.joomla.org/articles/1632-a-few-basic-security-rules ;

25) → Ocultar o <meta name="generator" content="Joomla XXX" /> no Joomla 3

Exemplo:

"
- *Acesse o seu FTP e vá até a pasta /libraries/joomla/document/html/renderer;*
- *Baixe o arquivo "head.php";*
- *No Joomla 3.x procure o comentário "// Don't add empty generators" em :*

($buffer .= $tab . '<meta name="generator" content="' . htmlspecialchars($generator) . '" />' . $lnEnd;)

- *Renomeie como quiser a linha alterando o* ***content="CONTEÚDO QUE QUISER"****;*
- *Salve o arquivo e suba no FTP novamente.*

*O mesmo com o campo // **Don't add empty descriptions .** "*

* ***No entanto, parece que não está funcionando. Então, caso não funcione, será necessário o uso de algum extensão que altere esses campos ;***

26) → Usar o sistema de *captcha*, também em formulários.

Exemplo:

http://extensions.joomla.org/extensions/extension/contacts-and-feedback/forms/chronoforms

http://extensions.joomla.org/extension/keycaptcha ;

27) → Caso não queira usar as extensões de formulário de contato : Use algum gratuito online ou, hospede seu formulário de contato em outra conta ou servidor, assim se evita *injections* e, é um controle melhor na identificação de problemas com formulários de contato;

28) → **LG Offline Page** (Site offline): Usar alguma extensão para descaracterizar a página pública principal e, sem os campos de acesso ao usuário como "*user*" e "*senha*". Ao despublicar os campos de formulário de login "user" e "senha" evita-se o MySQL Injection nesses campos.
Exemplo: (http://extensions.joomla.org/extensions/extension/miscellaneous/offline/lg-offline-page);

29) → Altere o "*favicon*" (http://www.etc....) padrão do Joomla, removendo-o ou alterando para algum "*favicon*" de sua preferência. Alguns *plugins* ou componentes fazem isso. **Exemplo:** (https://www.phoca.cz/phocafavicon);

30) → De costume, sempre verifique os códigos das extensões que você usa. É só abrir o arquivo compactado e verificar. Após, comprimir o arquivo em ".zip";

31) → Habilite as opções "Adicionar sufixo de URL" e "Utilizar mod_rewrite" nas "Configurações globais";

32) → Configure as URLs amigáveis (http://www.seusite.net/viagem-para-israel-2021) nas configurações globais. Assim os motores de busca, como o Google, Bing, e DuckDuckGo, encontram o seu site e seu conteúdo com mais eficiência e costuma notar que o seu site ficará no topo do ranking desses motores de buscas;

33) → Desabilite algumas funções vulneráveis do PHP : disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open. Verifique com o arquivo "teste.php" com o código <?php phpinfo(); ?> . Isso mostrará as configurações do php em seu servidor. O Joomla também exibe isso na parte de configurações na administração;

34) → Desativar o RG_EMULATION. Consultar seu provedor de hospedagem de sites, caso não tenha acesso;

35) → **ATUALIZADO, ano de 2023:** Dê preferência, use o Microsoft Windows ® (Sempre última versão, por exemplo Microsoft Windows 11 ®) que já vem todo configurado e, o Linux Distribuições não tem Antivírus muito bom gratuito, se quiser tem que pagar. **RESUMINDO:** Não use Linux para produções online, só Microsoft Windows ® Systems Versões ou Apple Systems ® Versões, todos esses sistemas: Sempre ATUALIZADOS; Legalizados; Originais e mais Antivírus como o AVAST (https://www.avast.com), Pagos. Vale realmente, muito, para administrar o seu Joomla via navegador de internet mais recente e atualizado, aqui no caso o navegador recomendado é o **Opera com VPN** (Virtual Private Network – Rede Privada de Trabalho) GRATUITA (https://www.opera.com/computer) ou a **VPN GRATUITA RiseUp** (https://riseup.net/pt/vpn), assim pode evitar que os dados

trafegados na internet entre seu site em desenvolvimento e o seu servidor, sejam monitorados por espiões e, que vírus monitorem seu acesso ao CMS JoomLa, diferente do *Linux Distribuições*, que infelizmente ainda hoje é bem possível de terem vírus como keyloggers, spywares, trojans, etc e, não tem antivírus completo e eficaz e, o firewall tem que ser configurado tudo em *verbatim*;

36) → Conceda apenas os privilégios necessários ao usuário do banco (Mysql e outros), isso, geralmente já vem configurado pela empresa de hospedagem de sites que você contratou;

37) → Integre o seu site com os serviços de proteção da empresa CloudFlare, para protegê-lo contra ataques *DoS* ou D*DoS* ou DRDoS e IPs reconhecidamente considerados como fonte de ataques: (https://www.cloudflare.com/ddos);

38) → Bloquear IPs com tentativas de invasão. Pode ser feito manualmente: Através do arquivo do lado do servidor, o ".htacces" com a função, exemplo :

" Order Deny,Allow "
Deny from xxx.xxx.xxx.xxx
" "

Ou, através do painel de controle de sua hospedagem de sites, geralmente em: "Gerenciador de IP > Bloquear um endereço de IP". Há recursos mais avançados a nível de acesso remoto (SSH) que capturam esses e-mails com tentativas de invasão, e mostram o diretório que foi o acesso/tentativa de invasão no Linux, por exemplo;

39) → Caso no futuro precise mudar a senha porque esqueceu-a, acesse o seu gerenciador de banco de dados via Terminal SSH > MySQL, ou pelo sistema web-based *PhpMyAdmin*. Em *users*, edite, e configure para o tipo MD5 que é para criptografia da senha no MySql ou outros sistemas SGBDs: Sistemas gerenciadores de banco de dados;

40) → Alguns links comumente usados para tentativas de SQL Injection :

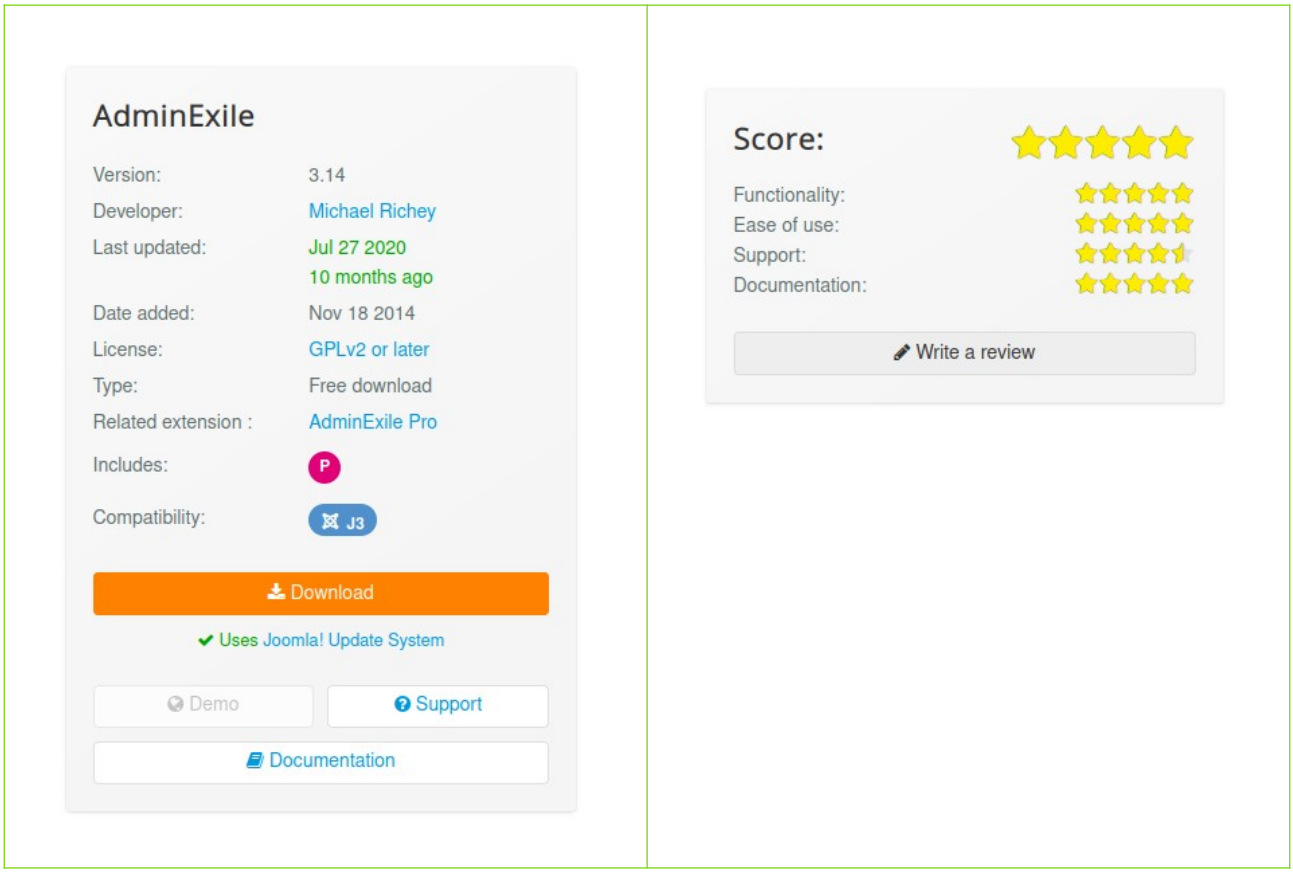
http://SeuSite/component/users/?view=remind
http://SeuSite/component/users ;

41) → ATENÇÃO: Verifique no back-end do Joomla, em: Plugins > "User – Joomla" > "Auto-criar Usuários". Por padrão vem "Sim" (habilitado). **Desmarcar** e, colocar na opção "**Não**". (**TESTE** antes de fazer isso.);

42) → Instalar extensões de Firewalls, proteção da Administração no Joomla, como por **exemplo**:

- Centora Security ™;
- DMC Firewall;
- AdminTools;
- Securitycheck;
- jHackGuard;
- RS Firewall.
- Pesquisar no repositório oficial do projeto Joomla sobre extensões de segurança (https://extensions.joomla.org/instant-search/?jed_live%5Bquery%5D=Secure%20Admin);

43) → Sempre verifique se a extensão é bem revisada, atualizada e avaliada, constantemente. **Exemplo:** (https://extensions.joomla.org/extension/**adminexile**);



44) → Caso tenha acesso de instalação de programas em seu servidor, seja uma VPS ou Clound VPS, ou servidor alugado, é interessante instalar programas antivírus para o Linux e específicos para a varredura de sites. Para isso existe o Nikto2, que é um antivírus para administradores de CMS, como o Joomla, que faz uma varredura nos CMS. (https://cirt.net/Nikto2). Temos também o *ClamV*, que é um antivírus livre (“gratuito”) para o sistema operacional Linux (http://www.clamav.net);

45) → **Teste de segurança no Joomla :**
Projetos : nikto, joomscan, owasp, sucuri, netsparker.

http://www.beyondsecurity.com,
https://www.acunetix.com,
http://sitecheck.sucuri.net
https://www.netsparker.com

**Alguns são gratuitos, mas outros são pagos;*

46) → **Antivírus Website Protection** : Um antivírus para o Joomla. Possui a versão free e a versão paga. Na versão free esse componente funciona em modo trial de 14 dias. (http://extensions.joomla.org/extensions/extension/access-a-security/site-security/antivirus-website-protection);

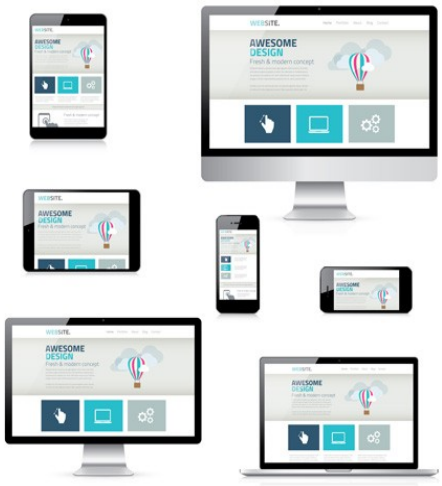
47) → Faça testes em seu site usando programas e distribuições Linux que já vêm com muitos programas, como a distribuição Linux Back|Track. (http://www.backtrack-linux.org) ou (https://www.kali.org);

48) →

⚠ **NUNCA** instale um componente, módulo, plugin ou template: **ANTIGO**, quando uma dessas extensões já estiverem instaladas e atualizadas em sua última versão no Joomla. O back-end (Administração) vai sumir, ocasionando a perda do painel e sistema de administração do site, impossibilitando dar prosseguimento na manutenção no site. **Portanto:** Não faça isso, **NUNCA**! ☠ ☠ ☠

49) → Para que o seu template Joomla, se encaixe em todas as telas das tecnologias eletrônicas da internet nos dias de hoje, sempre use templates **RESPONSIVOS** ou **RESPONSE** ou **RESPONSIVE**.

Exemplo:



50) → **Resumo de extensões do Joomla para implementar mais segurança**:

→ Admin Exile: Cria uma chave de senha e ainda redireciona o endereço do diretório administrador para outra página de sua escolha.
https://extensions.joomla.org/extension/adminexile

→ Akeeba Systems:
→ Admin Tools Core: Ferramentas de segurança e administração.
https://extensions.joomla.org/extension/admin-tools
→ Backup: Sistema mundialmente conhecido de backup.
https://extensions.joomla.org/extension/akeeba-backup

→ cUpdater: Avisa por e-mail nova versão do Joomla.
https://extensions.joomla.org/extension/cupdater

→ OH Security: Excelente contra o wget (ATENÇÃO: Não use esse programa direto de seu computador e rede, simplesmente o seu site vai te bloquear, sendo necessário o reboot de seu modem-roteador) e, faz logs de atividades criminosas em seu site. (*UpDate: Até o momento 23 de julho de 2023, o site está fechado, mas online, com mensagem "Forbidden", acredito que esteja sendo reformulado para uma versão mais avançada do CMS JoomLa, talvez a versão 5*):
https://www.orangehatstudios.com/joomla-extensions/ohsecurity

→ Security Check FireWall: Parede de fogo gratuita para o Joomla.
https://extensions.joomla.org/extension/securitycheck

→ SQL Injection: Extensão para bloquear ataques SQL Injection.
https://extensions.joomla.org/extension/marco-s-sql-injection

→ Mini Orange Joomla Network Security.
https://extensions.joomla.org/extension/web-security-lite-secure-login-and-backup-for-joomla

→ Coala Web Traffic: Grava e monitora os IPs dos visitantes do site.
https://extensions.joomla.org/extension/coalaweb-traffic (*UpDate: Até o momento 23 de julho de 2023, essa extensão "Coala Web Traffic" foi EXCLUÍDA do sistema de extensões do JoomLa e não há previsão de retorno, simplesmente o site do produtor não existe mais: https://coalaweb.com*):

→ Admin Tools Profissional (Extensão Paga ($))
https://extensions.joomla.org/extension/access-a-security/site-security/admin-tools-professional/

51) → **Certificado SSL:** Hoje em dia todos os sites devem ter o certificado SSL, é barato e é excelente para o ranking de seu site nos motores de busca como o Google, Bing, DuckDuckGo, etc. MAS e se ocorrer de você ter o seu certificado SSL instalado em seu serviço de hospedagem de sites e, por ventura o navegador de internet mostrar que não está instalado, aparecendo um cadeado, dependendo do navegador, na cor vermelha ou riscado? Devemos então, forçar para que o Joomla, faça o certificado SSL ser publicado em todo o site. Assim:

→ Menu: “Sistema”
→ Configurações Globais
→ Aba: “Servidor”
→ Configurações do Servidor
→ Opção: “Forçar HTTPS”
→ Selecionar a opção: “Todo o Site”
→ Clicar no botão verde “Salvar”.

OBSERVAÇÃO: *A compra e, a instalação do Certificado SSL na WebLink.com.br, é muito fácil, tudo é feito pelo Painel de Controle. A instalação do Certificado SSL é apenas clicar em um botão. Pronto !*

52) → **COOKIES:** Na data de 25 de novembro 2009, a diretiva 2009/136/EC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Pt:PDF) altera duas outras diretivas em relação aos direitos dos utilizadores na matéria das redes de comunicações eletrônicas e dos serviços (Diretiva 2002/22/EC) e do tratamento de dados pessoais e da proteção da privacidade no setor das comunicações eletrônicas (Diretiva 2002/58/EC). Faz dar direito ao usuário o controle sobre como os cookies são utilizados no sites visitados, logo esses visitantes ficam sabendo como esses arquivos cookies são copiados para o seu dispositivo e o que esses fazem, entre o site e o visitante/usuário, e os visitantes podem aceitar ou não a utilização dos cookies durante sua navagaçã no site em que está. Para isso, alguns desenvolvedores, criaram e disponibilizaram algumas extensões gratuitas para serem instaladas no CMS Joomla.

Essas extensões são:

→ CookiePro CCPA
https://extensions.joomla.org/extension/site-management/cookie-control/cookiepro-ccpa
→ Cookie Hint
https://extensions.joomla.org/extension/cookiehint
→ EB Sticky Cookie Notice
https://extensions.joomla.org/extension/eb-sticky-cookie-notice

53) → **PERMISSÕES DE ARQUIVOS nos Servidores Linux**

Usando as extensões “Security Check” e ” Admin Tools Core”, faça:

1→ Uma verificação de permissões de arquivos e diretórios usando a extensão “Security Check”, acessando o menu principal do Joomla em “Componentes”, clicando no item chamado “ Verificar Estado ” que está acima de um circulo com algum número em porcentagem “%”, vai carregar a página de “Informações do Sistema” > “Estado Geral” > Deve estar em vermelho a caixa de mensagem do lado direito da tela, escrito “Há arquivos com permissões incorretas?”, se sim, vai aparecer uma mensagem em vermelho escrito “1 problema(s) encontrado(s)”, clicar no ícone de ferramenta / , vai ir para outra página e terá um título na cor cinza “ ANÁLISE MANUAL ” em que você vai ter que clicar no botão “ Iniciar ” acima de uma tabela da cor verde , com o nome de “Estado”, e então será feita uma varredura e o resultado vai aparecer na tabela da cor azul abaixo de “ RESUMO DA ANÁLISE ” com o nome de “Arquivos/Pastas com permissões Mal configuradas”, abaixo será mostrada a quantidade de arquivos e pastas com permissões erradas, esse é o campo mais importante dessa análise, pode mostrar tudo de 1 à infinitos arquivos com problemas de permissões.

Como resolver isso ?

2→ Acessar o menu principal do Joomla em “Componentes” e clicar em “Admin Tools Core” ou “Ferramentas do Administrador”, o nome vai variar de acordo com o sistema de língua instalado em seu Joomla. Após carregar a página, ir em “Tools”, clicar em “Permissions Configuration”, vai carregar a página, clique no botão laranja “ Save and Apply custom permissions ”. Vai aparecer uma mensagem em verde dizendo que as permissões de customização foram bem aplicadas. Clique em “Voltar”, vai lá embaixo em “Tools” e clique em “Fix Permissions”, vai aparecer uma janela padrão do Joomla de diálogo mostrando uma barra de progresso indicando 100%, pode clicar no “x” para fechar.

3→ Volte na extensão “Security Check” e, faça o mesmo procedimento do item 1 desse passo a passo. Clique novamente em “ Iniciar ” e veja agora que em “Arquivos/Pastas com permissões Mal configuradas”, aparecerá o numero zero “0”, o que indica que todas as permissões de arquivos e pastas do Joomla estão consistentes e seguros, o que pode ser mostrado na barra de progresso na cor verde o numeral 100% quando ainda nessa página se clica em “Redirecionar para informações do sistema”, logo o seu Joomla já está um pouco mais seguro em relação as famossas permissões de chmod do Linux. Mas esse 100% , só é mostrado quando todos os itens de “Estado Geral” estão satisfeitas, pode ser que o campo “Two factor authentication enabled”, esteja por exemplo, sem estar ativado com alguma extensão desse tipo de segurança. Clicando na ferramenta sugerida, basta ativar os plugins: “Two Factor Authentication – YubiKey” e “Two Factor Authentication -

Google Authenticator” e, após a ativação, é aconselhavel a configuração desses respectivos plugins do Joomla.

Pronto ! Seu Joomla já está mais saudável.

54) → DOIS FATORES DE AUTENTICAÇÃO

Pegando o fim do item anterior, número 53, desse Checklist do Joomla, temos agora os plugins de autenticação em duas etapas:
“Two Factor Authentication – YubiKey”
“Two Factor Authentication - Google Authenticator”

O sistema YubiKey (https://www.yubico.com) é um pendrive com informações criptografadas em que você pode **$ Comprar $** para usar sua chave no Joomla.

O sistema Google Authenticator (https://support.google.com/accounts/answer/1066447), já é GRATUITO. Você tem que fazer o download do aplicativo em seu smartphone, pois o sistema usa QR Code. Mas devemos lembrar que o sistema Linux Android não é tão seguro, então, se você quiser investir em um iPhone, é bem interessante, pois a Apple, garante uma maior segurança em seus smartphones.

No entanto, você pode permanecer com esses dois plugins ativados, para futuramente você poder usar um desses dois fatores de dupla proteção em seu Joomla. No painel de controle no menu Usuários, selecione o usuário pretendido, clique em “Editar”, e vá na última aba “Autenticação em Duas Etapas”, e em “Método de autenticação”, salve a opção “Desabilitar Autenticação em Duas Etapas”. Você vai notar que abaixo estão aparecendo as opções propostas pelo Joomla que são o Autenticador do Google e YubiKey.

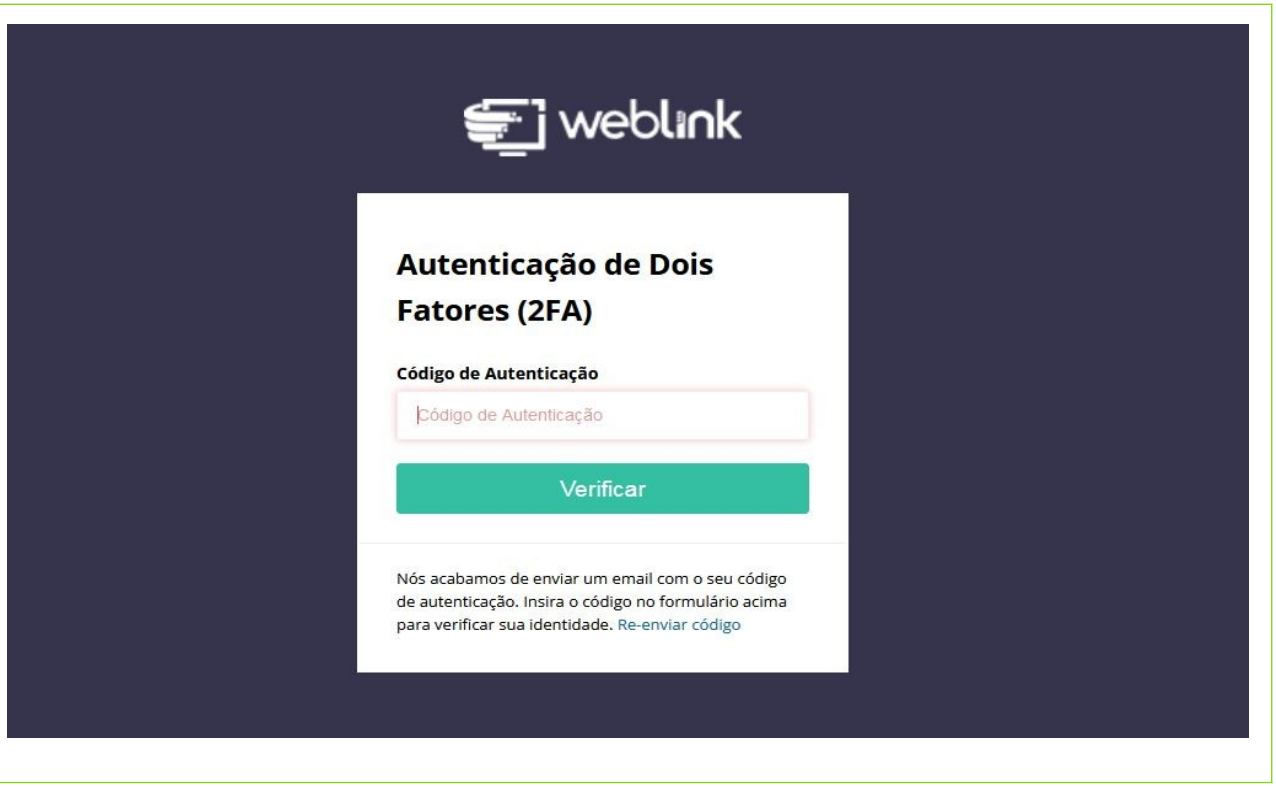
NUNCA SALVE a marcação de NENHUM desses plugins de dupla autenticação, pois você poderá perder totalmente o acesso ao seu site Joomla e, isso será um GRANDE PROBLEMA para você retornar a administração do seu site.

Claro, há uma extensão, já mencionada aqui nesse Checklist que é o **AdminExile**, esse não garante uma proteção de login tão avançada como o sistema YubiKey ou o Google Authenticator, mas ajuda a melhor o sistema de login do Administrator.

55) → **BLOQUEIO DO DIRETÓRIO “** /administrator **” NO SERVIDOR**

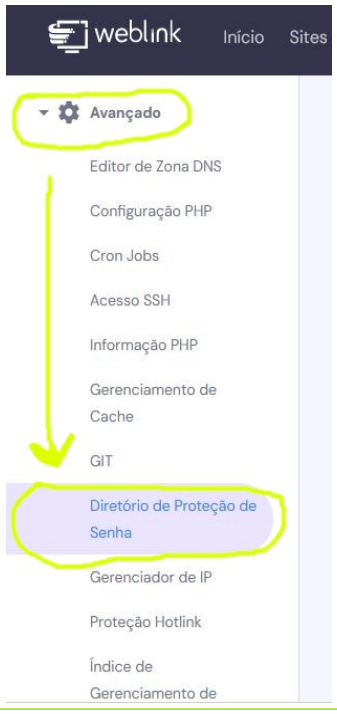
Como sugestão, de excelente painel de controle, use a empresa de hospedagem de sites Linux, a WebLink sucursal da Hostinger.

1- Faça login na https://www.weblink.com.br/cpanel-login , ou em seu painel de hospedagem de sites da empresa contratada para hospedagem do seu site/portal no CMS JoomLa e, após a primeira tela de login com os campos “Endereço de Email” | “Senha”, clique em ENTRAR; Você vai entrar na página de autenticação de 2 fatores ou 2FA:

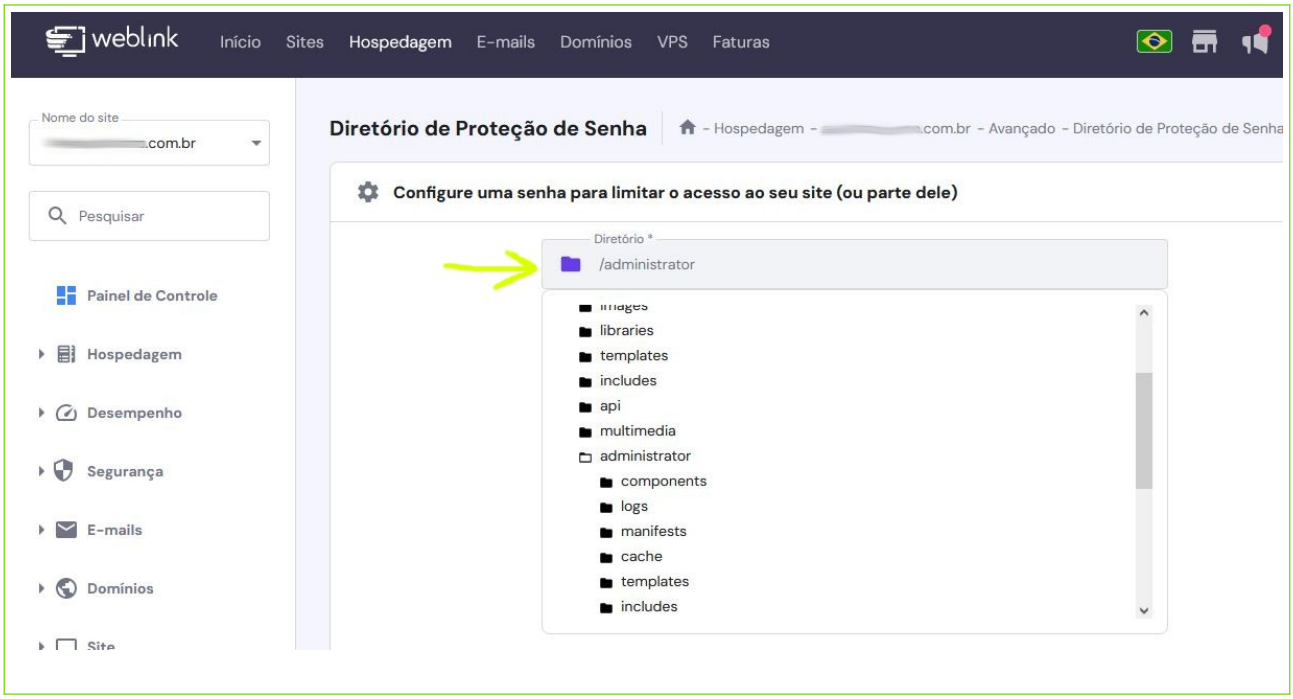


2- A WebLink.com.br está dentro dos sistemas da Hostinger, logo você vai receber um e-mail com o código enviado pelos servidores da Hostinger, para você colocar esse código conforme o item 1 acima, desse CheckList de Segurança do CMS JoomLa. No botão verde acima, clique em VERIFICAR.

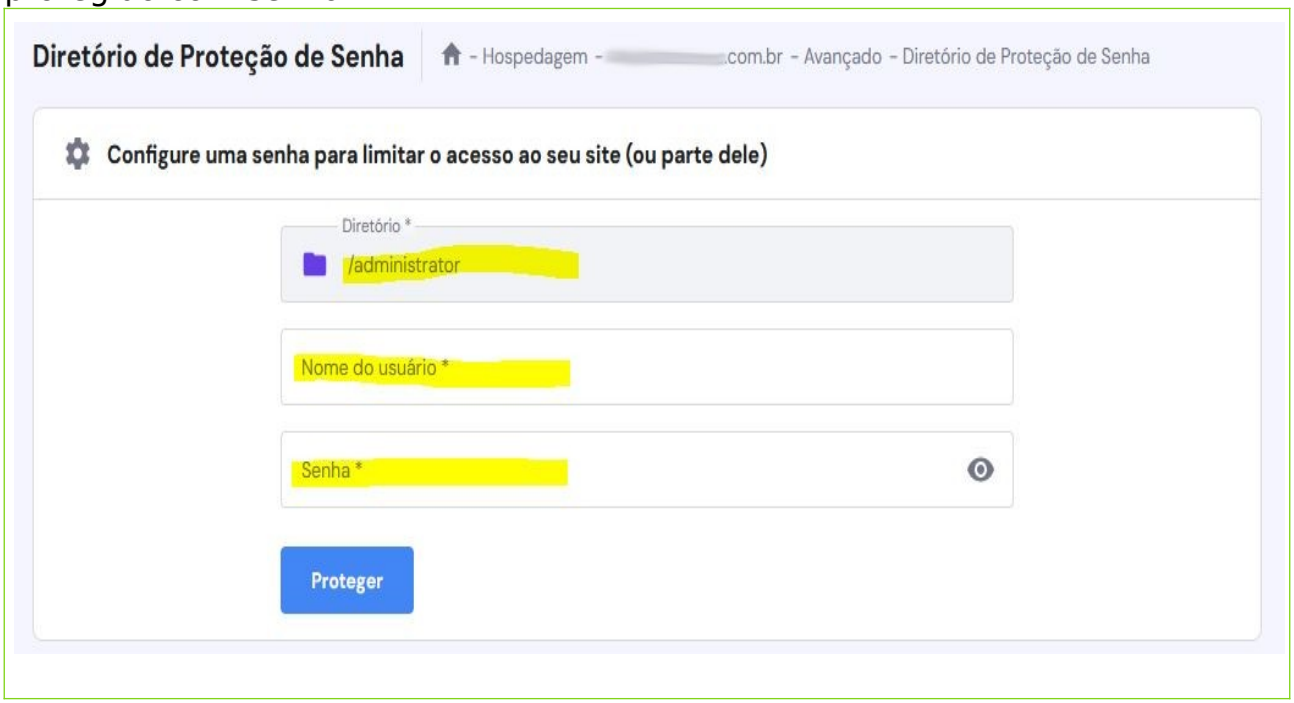
3- No Painel de Controle, no lado esquerdo, procure pelo menu "**Avançado**", clique e, procure pelo link "**Diretório de Proteção de Senha**":



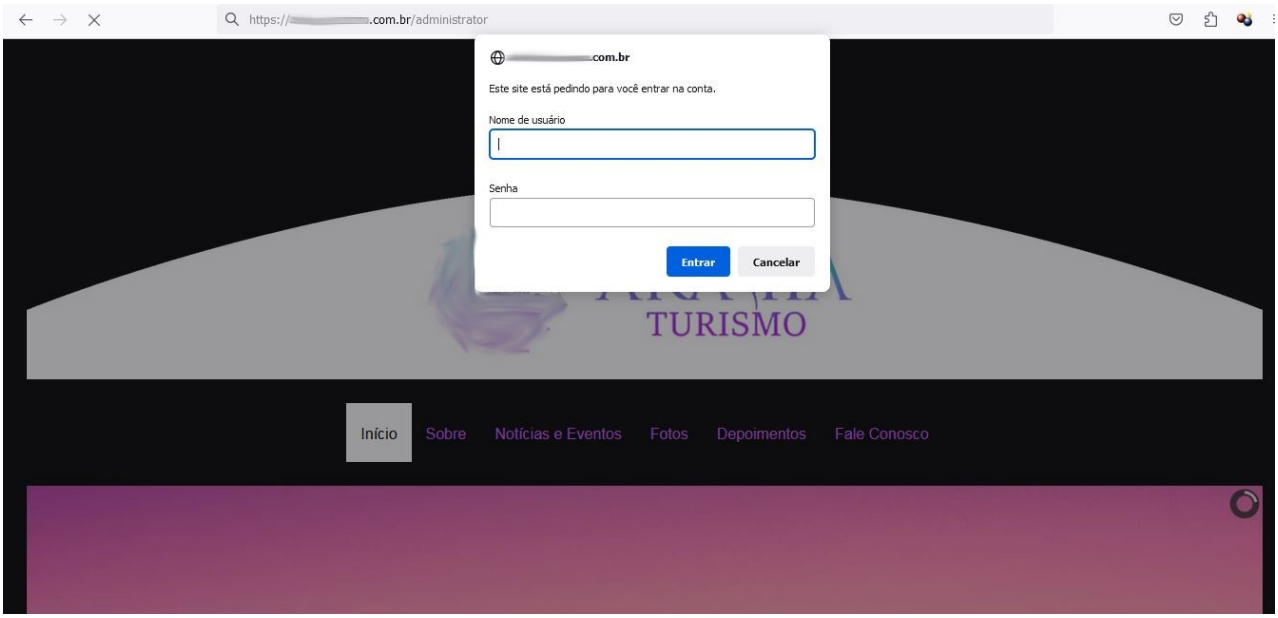
4- Ao carregar essa página, clique onde está a seta amarelada, deve estar aparecendo a raiz do sistema operacional do Linux que é "/". Clique e vai carregar o menu em cascata. Selecione a árvore de diretórios, procure por "/**administrator**", clique e, assim vai selecionar o diretório administrativo do CMS JoomLa. É esse diretório que mostra o arquivo "**administrator/index.php**", onde é a página de LogIn para a parte administrativa do JoomLa. Pelos campos de "usuário" e "senha", é que os hackers/crackers, fazem o uso da força bruta, como os SQL Injections e as Injeções de códigos maliciosos para na força bruta, tentarem entrar em seu painel de controle e derrubar o seu site !



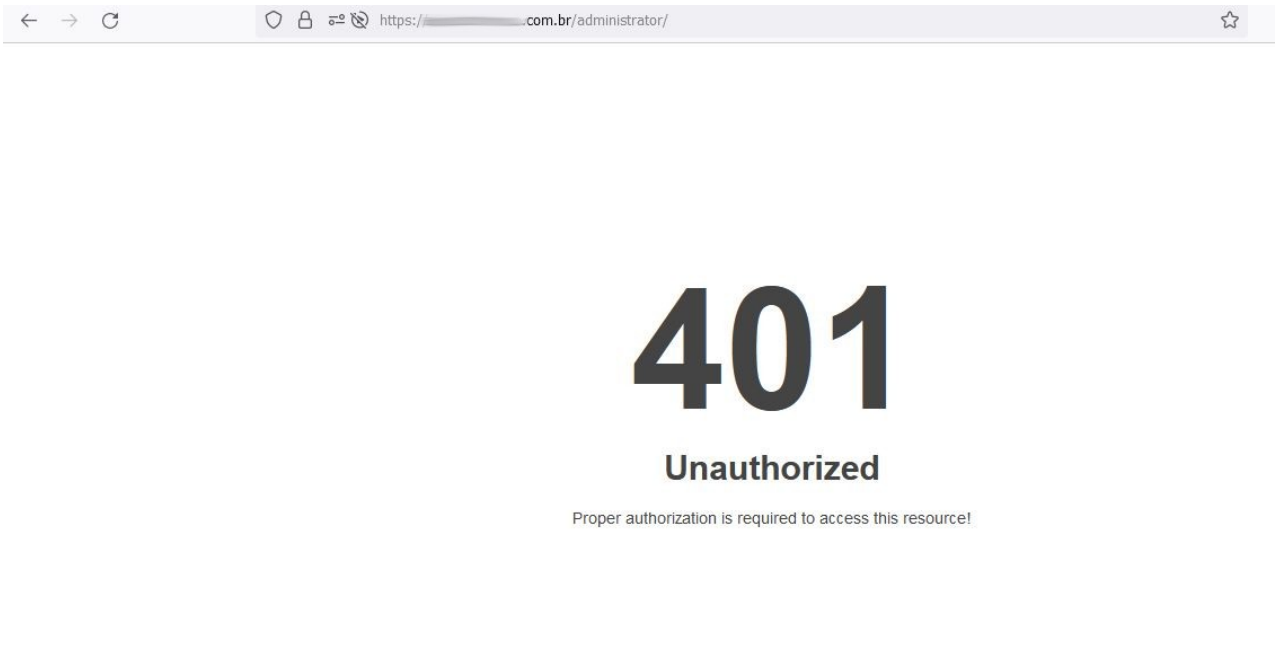
5- Agora, crie um **usuário** e **senha** para esse diretório "**/administrator**" ficar protegido com senha:



O resultado final é apresentado abaixo, após você criar e salvar os dados conforme orientado acima:



Por exemplo, se a pessoa não souber o usuário e a senha, há a negação de serviço com e o acesso é negado e, é apresentado o erro “401” do servidor de hospedagem de seu site:



Caso o seu serviço de hospedagem de sites / empresa de hospedagem de sites, não possua essa facilidade em seu painel de controle, venha para a WebLink.com.br e seja:

FELIZ !

→ **SUGESTÃO DE ALGUMAS EMPRESAS DE HOSPEDAGEM DO CMS JOOMLA:**

Internacional:

→ Rochen – Empresa Oficial que hospeda o Projeto Joomla:
https://www.rochen.com/joomla-hosting

→ Hostinger:
https://www.hostinger.com

→ Verperx:
https://verpex.com/joomla-hosting

→ A2 Hosting:
https://www.a2hosting.com/joomla-hosting

TOP Web Hosting Mundiais:

→ Top Hosting:
https://web-hosting.thetop10sites.com/top-web-hosting-intl.html

→ 9 Best Hosting:
https://www.hostingadvice.com/best/joomla-hosting

→ 6 Best Hosting:
https://www.websiteplanet.com/blog/best-web-hosting-joomla

No Brasil:

→ WebLink:
https://www.weblink.com.br

→ LocaWeb:
https://www.locaweb.com.br

→ KingHost:
https://king.host

→ Brasil Cloud:
https://brasilcloud.com.br/hospedagem-de-sites

TOP Brasil Web Hosting:

→ WebSitePlanet “As 10 melhores”:
https://www.websiteplanet.com/pt-br/web-hosting

→ Tudo Sobre Hospedagem de Sites:
https://tudosobrehospedagemdesites.com.br/melhor-hospedagem-de-site

→ **SITES DE TESTE DE SEGURANÇA PARA O CMS JOOMLA:**

Esses são os melhores aplicativos e empresas com soluções de análise, relatório e segurança para o seu site ou portal em Joomla:

→ Cirt: Site com várias soluções gratuitas para testes de segurança nos servidores Linux baseados:

https://cirt.net

→ Nikto: Scanner open source testes redundantes, com relatório final em html:

https://cirt.net/nikto2
https://github.com/sullo/nikto

→ Nikto Online:

https://nikto.online

NOTA: O site acima: “nikto.online”, está sendo remodelado para, aparentemente ser melhor e, está sendo apoiado nesse site, clique aqui: invicti.com/blog/news/netsparker-is-now-invicti-signaling--a-new-era-for-modern-appsec

→ Nmap: Scanner de Mapa da Rede:

https://nmap.org

→ Nmap Online:

https://nmap.online

→ CMS Explorer: Pode ser usado para auxiliar nos testes de segurança. Embora não execute verificações de segurança diretas, a opção "*explorar*" pode ser usada para revelar arquivos ocultos / de biblioteca que normalmente não são acessados por clientes da web, mas, mesmo assim, são acessíveis. Isso é feito recuperando a árvore de origem atual do módulo e, em seguida, solicitando esses nomes de arquivo do sistema de destino. Essas solicitações podem ser enviadas por meio de um proxy distinto para ajudar a "inicializar" ferramentas de teste de segurança como Burp, Paros, Webinspect, entre outros:

https://cirt.net/CMS-Explorer

→ Joom Scan: Projeto de código aberto em linguagem de programação perl para detectar vulnerabilidades Joomla CMS e analisá-las, com relatório final em html:

https://tools.kali.org/web-applications/joomscan

→ Sucuri: Verificação de segurança gratuita de site e scanner de malware:

http://sitecheck.sucuri.net

→ Tenable: Empresa eficaz para resolver os desafios no quesito de vulnerabilidades mais dificeis da atualidade. Alguns de seus produtos são: Nessus, Tenable.ad, Tenable Lumin:

https://tenable.com

→ Proactive Risk: O objetivo dessa empresa é proteger os ativos certos das ameaças certas com as medidas certas. Algumas de suas soluções são: PENTESTON® - Identify, PROTECTIT®, MONITORIT® Workforce Analytics & Productivity:

www.proactiverisk.com

→ Beyond Security: Segurança automatizada para todo propósito :

http://www.beyondsecurity.com

→ Acunetix: Encontre, corrija e evite vulnerabilidades:

https://www.acunetix.com

→ INVICTI: Reduz drasticamente o risco de ataques. Testes de segurança de aplicativos precisos e automatizados que escaláveis:

https://www.invicti.com

→ ADENDO: Links Oficiais do Projeto CMS JoomLa

Mais informações sobre como melhorar a segurança do JoomLa, nos sites Oficiais :

→ Checklist Oficial:
https://docs.joomla.org/Security_Checklist

→ Segurança:
https://docs.joomla.org/Security

→ Códigos utilizados pelo Projeto Joomla sobre erros de extensões:
https://extensions.joomla.org/support/knowledgebase/error-codes/unpublished-extensions-error-codes

→ Joomla Fórum Oficial:
https://forum.joomla.org

→ Centro de Anúncios de Orientações sobre Correções de Segurança:
https://developer.joomla.org/security-centre.html

→ Buscador de Empresas e Profissionais para Serviços de Segurança :
https://community.joomla.org/service-providers-directory/listings/category/view/117-joomla-security.html

→ Lista de componentes inseguros (Joomla® Vulnerable Extensions List):
https://extensions.joomla.org/vulnerable-extensions/about

→ Veja alguns dos parceiros produtores das extensões do CMS JoomLA:
https://www.joomla.org/about-joomla/extension-partners.html

→ Caso queira acompanhar o desenvolvimento do CMS JoomLa, esse é o link oficial do projeto:
https://github.com/joomla

→ SITES BASEADOS PARA AS DICAS DESSE CHECKLIST:

https://www.hostinger.com.br/tutoriais/joomla-para-iniciantes

https://www.security.unicamp.br/artigos/22-dicas-seguranca-joomla.html

http://www.frhost.com.br/blog/seguranca/seguranca-joomla-tornando-o-joomla-mais-seguro

https://canaltech.com.br/internet/10-dicas-para-preservar-a-seguranca-do-seu-site-em-joomla

https://forum.joomla.org/viewforum.php?f=374

http://www.webmaster.pt/joomla-tutorial-seguranca-4.html

http://forum.joomla.org/viewforum.php?f=374

https://ajuda.hoteldaweb.com.br/aumente-seguranca-seu-joomla

https://ajuda.hostnet.com.br/seguranca-para-joomla

https://docs.joomla.org/Security/Guide/pt

→ **TEMPLATES:**

https://www.criarsites.com/templates-gratis-para-o-joomla

https://www.templatemonster.com/pt-br/free-templates

https://forum.joomla.org/viewtopic.php?t=225325

→ **DICA DE PESQUISA** Google: Digite junto com as “aspas” no campo de pesquisa:

"download template responsive free joomla 3"

O resultado da pesquisa vai retornar todos os sites com templates responsivos e gratuitos para Joomla 3.x. O mesmo pode ser feito com o CMS Joomla 4.x e, em um futuro próximo, também poderá ser feito com a versão que já está em andamento de programação e execução a versão 5.x do CMS JoomLa, com previsão de lançamento para o fim desse ano de 2023.

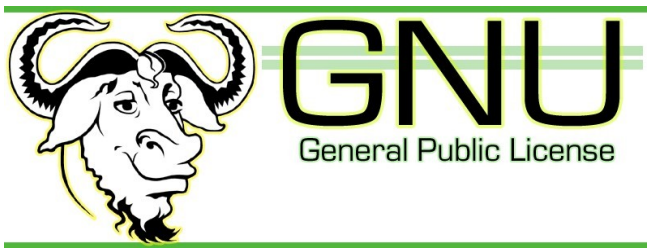
EXEMPLO:

"download template responsive free joomla 3"

"download template responsive free joomla 4"

"download template responsive free joomla 5"

→ LICENÇA DESSA OBRA:



Essa obra:

“ ***Checklist de Segurança, para o premiado e fantástico CMS Open Source: Joomla Versões:*** *3.x e, 4.x ”,*

Está sob a licença adotada para a sua publicação:
GPL GNU, versão 3.

→ *Você pode consultar sobre essa licença:* ***GPL GNU 3****, nos links abaixo:*

- *Licença pura: https://www.gnu.org/licenses/gpl-3.0.html*
- *Licença traduzida: http://licencas.softwarelivre.org/gpl-3.0.pt-br.html*
- *Guia rápido: https://www.gnu.org/licenses/quick-guide-gplv3.pt-br.html*

→ *As imagens dessa obra foram retiradas da internet, são de domínio público e, aqui não visam lucro.*

→ CONSIDERAÇÕES FINAIS:

Com o breve lançamento do Joomla 4, muitas novidades vão existir, entre outras versões que serão desenvolvidas nos próximos anos do CMS Joomla, então, esse ***Checklist****, sempre estará em constante atualização, de anos em anos.*

→ O AUTOR:

O Autor dessa obra, incentiva qualquer implementação pela comunidade, desde que entre em contato com o mesmo para a devida implementação nesse ***Checklist*** *e, a atualização de sua versão. Caso queira a publicação de seu nome nesse material, também é bem vindo.*

Este pequeno ***Checklist*** *é* ***LIVRE*** *sob a licença GPL GNU v.3 e, não possui em qualquer hipótese de diretivas comerciais.*

É um PRESENTE para a Comunidade Joomla!

Nobres Saudações ! Grande abraço ! Tudo de bom !

Por,
Bráulio Machado Campos – CEO – Projeto: Internet Pensante ®.