Checklist de Segurança para Joomla

- Efetue um backup completo de todos os arquivos e do banco e restaure localmente
- Mudar prefixo das tabelas durante a isntalação. Após a instalação precisará alterar todo o banco mudando o prefixo de todas as tabelas
- Criar novo super usuário e remover o de ID 62. Lembre de usar senha forte para o super usuário
- Ativar URLs amigáveis e mod_rewrite
- Mover configuration.php para fora do public_html, usando:

require_once(dirname(**FILE**) . '/../../portal.cfg');

- Bloquear cadastro de usuários pelo site caso não tenha necessidade: Configuração Global - Sistema - Permitir Cadastro de Usuários - Não
- Alterar metatags em Configuração Global - Configurações de Meta Dados (Trocar Joomla por outra palavra)
- Adicionar a tag do template (para ocultar na origem do código HTML):

setGenerator('Ribafs - Desenvolvimento Web'); ?>

- Instalar extensões:
- AdminTools
- Plugin osolcapcha
- com_encrypt
- jHackGuard

Uma boa ferramenta de backup é o com_simplebackup - https://github.com/ribafs/com_simplebackup

Usar a ferramenta:

joomlascan - https://github.com/rezasp/joomscan

Um bom tutorial - http://www.100security.com.br/joomscan/

sudo apt-get install libswitch-perl

- Download
- Descompactar e acessar a pasta

Atualizar ./joomscan.pl update

Checar a atualização

svn co https://joomscan.svn.sourceforge.net/svnroot/joomscan joomscan

Varrer site procurando vulnerabilidades

./joomscan.pl -u http://www.joomla.org

Ativar o cache

Otimizar as tabelas do banco no phpmyadmin

Usando Captcha (plg_osolcaptcha) para forms adicionais.

array(true) para form vertical e false para horizontal

```
<?php
global $mainframe;
//set the argument below to true if you need to show vertically( 3 cells one
below the other )
$mainframe->triggerEvent('onShowOSOLCaptcha', array(false));
?>
```

Alterar permissões de arquivos:

Alterar todos os arquivos para 644 e todas as pastas para 755 com:

```
find . -type f -exec chmod 644 {} \;
find . -type d -exec chmod 755 {} \;
```

Depois criar algumas exceções...

```
configuration.php – 400
index.php do site – 400
index.php do template padrão – 400
Permissões de pastas:
includes e libraries – 500
```

Remover templates não usados e outras extensões também.

Adicionar ao .htaccess:

```
# Block out any script trying to set a mosConfig value through the URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z_]{1,21}(=|\%3D) [OR]

# Block out any script trying to base64_encode crap to send via URL
RewriteCond %{QUERY_STRING} base64_encode.*\(.*\) [OR]
# Block out any script that includes a <script> tag in URL
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]
# Block out any script trying to set a PHP GLOBALS variable via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\[|\%[0-9A-Z]{0,2}) [OR]
# Block out any script trying to modify a _REQUEST variable via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\[|\%[0-9A-Z]{0,2})
# Send all blocked request to homepage with 403 Forbidden error!
RewriteRule ^(.*)$ index.php [F,L]
```

Adicionar ao configuration.php:

```
   ini_set('extension', 'sourceguardian.so');
        ini_set('register_globals', 'off');
        ini_set('session.save_path', '/home/ribafs03/public_html/tmp');
        ini_set('cgi.force_redirect', 1);
        ini_set('allow_url_fopen', 0);
        ini_set('display_errors', 0);
        ini_set('allow_url_include', 0);
```

```
        ini_set('expose_php', 0);
        ini_set('magic_quotes_gpc', 0);
        ini_set('post_max_size', '262144');
        ini_set('upload_max_filesize', '262144');
        ini_set('upload_tmp_dir','/home/joao/public_html/tmp');
        $disfunctions = 'proc_open, popen, disk_free_space, set_time_limit,
leak, tempfile, exec, system, shell_exec, passthru, curl_exec, curl_multi_exec,
parse_ini_file, show_source, apache_get_modules, apache_get_version,
apache_getenv, apache_note, apache_setenv, disk_free_space, diskfreespace, dl,
highlight_file, ini_alter, ini_restore, openlog,  proc_nice, symlink, phpinfo';
        ini_set('disable_functions', $disfunctions);
        ini_set('zend_extension',
'/usr/local/php52/lib/php/extensions/ioncube.so');
        ini_set('zend_extension_manager.optimizer=',
'/usr/local/Zend/lib/Optimizer-3.3.3');
        ini_set('zend_extension_manager.optimizer_ts',
'/usr/local/Zend/lib/Optimizer_TS-3.3.3');
        ini_set('zend_optimizer.version', '3.3.3');
        ini_set('zend_extension',
'/usr/local/Zend/lib/ZendExtensionManager.so');
        ini_set('zend_extension_ts',
'/usr/local/Zend/lib/ZendExtensionManager_TS.so');
```

Adicionar ao php.ini (alternativa):

Este é para o caso do servidor permitir um php.ini no raiz que será visto por todas as partas recursivamente.

```
extension=sourceguardian.so
register_globals = off
session.save_path = "/home/ribafs03/public_html/tmp"
cgi.force_redirect = 1
allow_url_fopen= 0
display_errors = 0
expose_php = 0
magic_quotes_gpc = 0
memory_limit = 8388608
#open_basedir = 1
post_max_size = 262144
upload_max_filesize = 262144
upload_tmp_dir = "/home/ribafs03/public_html/tmp"
disable_functions = proc_open, popen, disk_free_space, set_time_limit, leak,
tempfile, exec, system, shell_exec, passthru, curl_exec, curl_multi_exec,
parse_ini_file, show_source,
apache_get_modules,apache_get_version,apache_getenv,apache_note, apache_setenv,
disk_free_space, diskfreespace, dl, highlight_file, ini_alter, ini_restore,
openlog, proc_nice, symlink, phpinfo
zend_extension=/usr/local/php52/lib/php/extensions/ioncube.so
zend_extension_manager.optimizer=/usr/local/Zend/lib/Optimizer-3.3.3
zend_extension_manager.optimizer_ts=/usr/local/Zend/lib/Optimizer_TS-3.3.3
zend_optimizer.version=3.3.3
zend_extension=/usr/local/Zend/lib/ZendExtensionManager.so
zend_extension_ts=/usr/local/Zend/lib/ZendExtensionManager_TS.so
```

Vários dos recursos acima você precisará confirmar com o suporte do seu servidor para ver se estão disponíveis.

Checklist de Segurança para Joomla

- Se possível/viável escolher a melhor hospedagem, não a mais barata;

- Utilizar sempre a última versão do CMS e das extensões;
- Efetue um backup completo de todos os arquivos e do banco e restaure localmente
- Efetuar backup completo com frfequência, especialmente antes de instalar novas extensões ou efetuar alterações como adição de conteúdo
- Ativar URLs amigáveis e mod_rewrite
- Bloquear cadastro de usuários pelo site caso não tenha necessidade: Configuração Global - Sistema - Permitir Cadastro de Usuários - Não
- Alterar metatags em Configuração Global - Configurações de Meta Dados (Trocar Joomla por outra palavra)
- Faça sempre o download do Joomla do site oficial - http://joomla.org
- Cheque o hash MD5 do arquivo baixado:

```
md5sum Joomla_3.7.5-Stable-Full_Package.zip
bd67cb02627e60bffef5e3b4ba3b2ece Joomla_3.7.5-Stable-Full_Package.zip
```

- Instalar os principais navegadores para testar o site:

Firefox, Chrome, Internet Explorer, Opera, Safari

- Mantenha os arquivos de configuração, logs e os diretórios de upload (repositórios de documentos, imagens e chache) fora do public_html.
- Remover desnecessários:

Arquivos

Extensões (se não precisa, remova e não simplesmente desabilite. Caso queira instale novamente)

- Sempre antes de instalar novas extensões:
- faça um backup completo do site e instale localmente
- Verifique se a extensão é confiável em:

https://docs.joomla.org/Archived:Vulnerable_Extensions_List

Reportar extensões vulneráveis e retirar extensão da lista

https://extensions.joomla.org/vulnerable-extensions/about/

Extensões corrigidas

https://extensions.joomla.org/index.php?option=com_content&view=category&id=10511&Itemid=1056

- Faça o download do site do criador
- Teste bastante localmente e somente então envie para o servidor
- Evite instalar extensões que tenham código criptografado

- Sempre que possível evite hospedar seu site em servidores compartilhados
- Use um servidor de SSL, pelo menos para o administrator
- Use o .htaccess
- Atualize para a versão 3 e última do Joomla