JOOMLA

CHECKLIST DE SEGURANÇA

[ ] BLOQUEAR O ACESSO AO PAINEL DE ADMINISTRADOR

[ ] APAGAR EXTENSÕES DESNECESSÁRIAS

[ ] NÃO UTILIZAR USUÁRIO PADRÃO “ADMIN” OU “ROOT”, RENOMEAR O MESMO

[ ] MUDAR A SENHA DE ADMINISTRADOR PARA UMA SENHA FORTE (EXEMPLO PK!%15Ojw33$ - UTILIZANDO PELO MENOS 12 CARACTERES)

[ ] CRIAR UM “NOVO” USUÁRIO E ATRIBUIR À ESTE AS PERMISSÕES DE ADMINISTRADOR

[ ] APAGAR A CONTA DE ADMINISTRADOR *

[ ] RENOMEAR O ARQUIVO HTACCESS.TXT PARA .HTACCESS E DEIXAR A OPÇÃO “REWRITEENGINE” EM “ON”

[ ] VERIFICAR SE A PASTA DO WEBSITE POSSUI ARQUIVOS DESNECESSÁRIOS, TAIS COMO: ARQUIVOS .PSD, ARQUIVOS DE PROJETO, ETC... E APAGAR

[ ] VERIFICAR SE O ÚLTIMO PATH DO JOOMLA FOI APLICADO

[ ] VERIFICAR AS CONFIGURAÇÕES DE PERMISSÃO DOS ARQUIVOS .PHP, SE ESTÃO SETADAS PARA 644 (rw-r-r) OU PREFERENCIALMENTE 444 (r-r-r - SOMENTE LEITURA).

[ ] NÃO UTILIZAR O PREFIXO DE TABELA PADRÃO “jos_table”, ALTERAR IMEDIATAMENTE.

[ ] REMOVER NOME OU NÚMERO DE VERSÃO DAS EXTENSÕES. **

[ ] REMOVER NÚMERO DE VERSÃO DO JOOMLA **

[ ] REMOVER O GERADOR META TAG DO JOOMLA **

*** Cerca de 90% dos ataques, baseiam-se em scripts e trojans que exploram contas/usuários padrão do sistema.**

**** Remover o nome, número de versão e tag´s, dificulta que hacker´s utilizem programas de motor de buscas e identifiquem facilmente as páginas e possíveis brechas de segurança envolvidas.**

Ricardo Silveira - 16/11/2016