	Ministerio de Educacion Nacional República de Colombia Libertad y Orden	

Recomendaciones de Seguridad para Web sites implementados bajo Joomla!

Dirigido a:

Secretarías de Educación que hacen uso del servicio de Web Hosting proporcionado por el Ministerio de Educación Nacional de Colombia.

Publicación: Agosto-2012

Versión: 1.0

Contenido

Tabla de Modificaciones

Nº Versión	Fecha Modificación	Elaborado	Aprobado	Modificaciones
Original	Abril 2010	Ing. Johanna Quintero – Global Crossing	Gerente Proyecto MEN	Documento Original
V 1.0	Agosto 2012	Ing. Eduardo Cancino F.	Ing. Néstor Zuluaga Ing. Julio Baracaldo	Se modifica la estructura del documento, se actualiza la información y se adicionan recomendaciones.

INTRODUCCIÓN

El Ministerio de Educación Nacional, presenta a las Secretarías de Educación Departamentales y Municipales de la República de Colombia, recomendaciones básicas para disminuir las vulnerabilidades a las que pueden estar expuestas los sitios web de las Secretarías que hacen uso del ***servicio de alojamiento y soporte de sitios WEB personalizables***, que brinda el Ministerio de Educación Nacional.

El presente documento está dirigido al Secretario de Educación, a los funcionarios de las Secretarías de Educación encargados de administrar el material que se publique y, en especial al personal técnico de interno o externo que diseña, desarrolla y publica páginas web de las Secretarías de Educación que tienen convenio con el Ministerio de Educación Nacional y que usan la plataforma Joomla! para hacer uso del servicio de alojamiento y soporte de sus sitios web.

La oficina de Tecnología del Ministerio de Educación Nacional, espera que este documento adicional a ser de gran utilidad, sea de su completo agrado y comprensión. Para lo cual pone a su disposición la posibilidad de comunicarse con nuestra Mesa de ayuda y soporte a la línea gratuita 018000 113080 en Bogotá 6000258, al celular 3208557420 o a través del envío de un mensaje de correo electrónico a la cuenta mesadeayuda@tecnologia.mineducacion.gov.co, en caso de requerir aclaraciones o precisiones sobre los aspectos en él enunciados.

RECOMENDACIONES DE SEGURIDAD.

Para evitar vulnerabilidades de seguridad que se pueden presentar sobre los sitios Web implementados con plataforma Joomla!, se hace necesario que se apliquen las siguientes recomendaciones con el fin de evitar el hackeo del sitio Web de la Secretaría de Educación y así minimizar las vulnerabilidades que este pueda contener, así:

1. Recomendaciones para contraseñas de Administrador y otras consideraciones Generales.

Se recomienda, cambiar periódicamente la clave de seguridad, contraseña (password) de cada uno de los componentes del sitio web y asegurar que no se repita por lo menos en las últimas doce (12) veces. Algunas características importantes al momento de establecer una contraseña son:

1.1 La longitud de la contraseña debe ser mayor a ocho (8) caracteres.

1.2 Utilice una combinación aleatoria que incluya letras (al menos una letra en mayúscula), números (al menos un número), y caracteres especiales (al menos un carácter especial)

1.3 Evite usar nombres o palabras que puedan ser encontradas en cualquier diccionario

1.4 No se recomienda utilizar los nombres de parientes, mascotas u otras personas u objetos relacionados con el usuario y/o administrador que pudieran ser de fácil deducción

1.5 La contraseña debe cambiarse periódicamente, al menos cada cuarenta y cinco (45) días o menos si el sitio gestiona información sensible o confidencial.

Se debe tener en cuenta que la mayoría de los sistemas aceptan como caracteres válidos para contraseñas todos los caracteres ASCII desde el 33 al 126:

*! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _ ` a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~*

Mantenga siempre una copia actualizada de los archivos del sitio y de la base de datos. No es aconsejable depender de las copias de respaldo del servicio central de hosting.

2. Recomendaciones para Servidor de Desarrollo

En lo posible es recomendable, configurar un equipo que actúe como servidor local de desarrollo, y que permita realizar allí todas las actualizaciones y pruebas antes de ser publicadas en el sitio web asignado por el Ministerio. Realizar la instalación y configuración de la infraestructura de aplicaciones de manera independiente empleando el software original de cada fabricante. Por separado algunas Recomendaciones para el HTTP Server

2.1 Utilice archivos .htaccess para bloquear intentos de exploits. En la siguiente dirección se encuentra publicado un tutorial que puede servir como guía para esta implementación: http://forum.joomla.org/index.php/topic,75376.0.html

2.2 Se recomienda revisar regularmente los registros de acceso en busca de actividad sospechosa haciendo uso de los resúmenes de actividad que normalmente genera el sitio; especialmente se recomienda revisar los "raw logs" (registros en crudo) para detalles más reales de la actividad del sitio web.

2.3 Configure los filtros de Apache mod_security y mod_rewrite para que bloqueen ataques PHP.

3. Recomendaciones de Seguridad para MySQL

3.1 Se debe tener en cuenta que la cuenta MySQL de Joomla! está configurada con acceso ilimitado por defecto, razón por la cual la instalación inicial de MySQL es insegura. Por lo tanto se recomienda hacer o solicitar una configuración manual una vez finalizado el proceso de instalación. Recomendaciones asociadas a esta vulnerabilidad pueden encontrarse en el sitio de documentación de MySQL: http://dev.mysql.com/doc/refman/4.1/...rivileges.html

4. Recomendaciones de Seguridad para PhP

4.1 Sí está desarrollando su sitio por primera vez se recomienda utilizar siempre la última versión publicada de PHP. En caso de que su desarrollo exista previo a la publicación de la última versión de PHP, se recomienda en lo posible actualizar el código para que haga uso de esta versión.

4.2 Se recomienda realizar pruebas automáticas de SQL Injection en contra de la versión del Servidor de desarrollo de las aplicaciones PHP antes de ser publicadas en el sitio web. Esto se puede lograr utilizando herramientas como Paros Proxy.

4.3 Durante el ciclo de vida de desarrollo del sitio web, se recomienda seguir el principio de otorgar el menor privilegio para correr PHP sobre el servidor de desarrollo, usando herramientas como PHPsuExec, php_suexec o suPHP desde suPHP, entre otras

5. Recomendaciones de Seguridad para PhP.INI servidor de Desarrollo

5.1 Se recomienda revisar constantemente la lista oficial de directivas php.ini en www.php.net y la lista de directivas php.ini: http://us3.php.net/manual/en/ini.php#ini.list

5.2 Es recomendable solicitar/configurar la variable register_globals en OFF. Esta directiva determina si registrar o no las variables EGPCS (Environment, GET, POST, Cookie, Server) como variables globales. Para más información al respecto, puede remitirse al post: http://forum.joomla.org/viewforum.php?f=621.

5.3 Se recomienda utilizar disable_functions para desactivar funciones PHP que no son necesarias para su sitio.

5.4 Se recomienda desactivar allow_url_fopen. Esta opción habilita las envolturas fopen de tipo URL que permiten el acceso a estos objetos como archivos. Los wrappers (envolturas) son proveídos para el acceso de archivos remotos usando el ftp o el protocolo http, algunas extensiones como zlib son capaces de registrar wrappers adicionales. Nota: Esto solo puede ser configurado en php.ini por motivos de seguridad.

5.5 Solicitar/Ajustar la directiva magic_gpc_quotes a modo off para los scripts escritos en PHP 3 y PHP 4. magic_gpc_quotes configura el estado magic_quotes state para operaciones GPC (Get/Post/Cookie). Cuando magic_quotes esta on, todas las ' (single-quote/comillas-simples), " (double quote/comillas dobles), \ (backslash-barra invertida) y NUL's son evitadas con una barra invertida \ automáticamente.

5.6 Se recomienda que la directiva safe_mode esté activa y configurada correctamente. En la siguiente dirección se encuentra directivas de configuración de Seguridad PHP y Safe Mode (Modo Seguro): http://us3.php.net/manual/es/security.php.

5.7 Se recomienda solicitar/revisar la configuración de open_basedir para limitar los archivos que pueden ser abiertos por PHP a el árbol de directorios especificado, incluyendo el archivo mismo. Esta directiva no es afectada si el Safe Mode esta On u Off. La restricción especificada con open_basedir es en realidad un prefijo, no un nombre de directorio. Esto significa que "open_basedir = /dir/incl" también permite el acceso "/dir/include" y "/dir/incls" si es que existen..

6. Recomendaciones de Seguridad para CMS Joomla!

6.1 Es muy importante que siempre actualice Joomla! a la última versión estable publicada. Visite habitualmente el sitio: http://forum.joomla.org para informarse sobre la versión.

6.2 Descargue Joomla! solo del sitio oficial, de descarga: http://www.joomla.org/download.html.

6.3 En lo posible remueva todas las plantillas (templates) que no sean necesarias en su sitio. No coloque lógica de seguridad en archivos de plantillas (templates).

6.4 Edite globals.php para correr register_globals emulation off en Joomla!. Aunque la emulación Joomla! es mucho más segura que la directiva PHP register_globals, es mejor no permitir para nada register_globals.

6.5 Desde la consola de administrador, se sugiere configurar el manejo de cargue de archivos o extensiones para que se realice vía FTP y no a través de habilitar permisos de apache en las subcarpetas del sitio web.

6.6 Una vez que el sitio esté configurado y estable, proteja contra escritura la mayor cantidad de archivos y directorios que pueda, cambiando los permisos de directorios a 755, y los permisos de archivos a 644. Existe una característica de sitio --> Global Configuration (configuración global) --> que puede colocar los permisos de forma masiva por usted. Tenga en cuenta de que esta función masiva puede afectar el funcionamiento de los

componentes, si lo hace pruebe el funcionamiento de los mismos. También tenga en cuenta que es posible que no se puedan cambiar los permisos en todos los componentes o extensiones de terceros.
http://help.joomla.org/content/view/41/132/.
http://forum.joomla.org/index.php/topic,24108.0.html
Nota: Necesitará reiniciar los permisos si es que se desea instalar extensiones más tarde. Ser consciente que en algunos servidores, la opción de (Anular la protección contra escritura al guardar) puede no funcionar, aunque el aviso del sistema diga que si, por eso tendrá que cambiar las opciones de la configuración dándole permisos de escritura manualmente a su configuration.php.

7. Recomendaciones de seguridad para Extensiones (Componentes, Módulos, y Bots) de Joomla!

7.1 En lo posible elimine o renombre todas las extensiones Joomla! que requieran register_globals ON

7.2 Descargue extensiones solo de sitios de confianza.

7.3 Antes de instalar extensiones de terceros (third party extensions), revise: Lista oficial de extensiones de terceros vulnerables: http://docs.joomla.org/Vulnerable_Extensions_List.

7.4 Se recomienda probar todas las extensiones en el servidor de desarrollo antes de instalarlas en el ambiente de producción dispuesto por el MEN.

7.5 Respalde el sitio y la base de datos antes de instalar nuevas extensiones.

7.6 Remueva cualquier extensión no usada, y revise cuidadosamente que los directorios y archivos no usados hayan sido eliminados.

8. Metodología OWASP

Finalmente, se recomienda a los desarrolladores revisar el sitio web del proyecto OWASP (Open Web Application Security Project) https://www.owasp.org/index.php/Main_Page. Este proyecto provee asistencia para mejorar la seguridad de las aplicaciones. Su principal misión es difundir información sobre vulnerabilidades y fallos en su guía, para que las organizaciones y los desarrolladores puedan aplicarla para evitar riesgos reales de seguridad. Todo el material que generan se encuentra disponible bajo una licencia Open Source.

Los productos derivados de este proyecto y que deben ser observadas por los administradores son:

8.1 *Guía de Desarrollo.*

Es un **compendio de buenas costumbres y de sugerencias** a implantar en el proceso de codificación de aplicaciones web para poder generar aplicaciones de calidad en cuanto a seguridad se refiere.

8.2 *Guía de revisión de código*

Es un compendio para revisar el código que ya está generado (aplicación ya existe) en busca de vulnerabilidades y malas prácticas.

8.3 *Guía de Pruebas de aplicaciones*

La guía de pruebas resume y **muestra los posibles puntos de entrada** en las aplicaciones **y cómo explotarlos**.

8.4 *Ranking de las vulnerabilidades más activas (última actualización a la fecha Abril 2010).*

- **A1: Inyección** (SQL, OS, LDAP, etc, que suceden cuando los datos pasan sin filtrar directamente como parte de la consulta. Se pueden usar para acceder a datos sin autorización o para ejecutar comandos)
- **A2: Cross-Site Scripting** (XSS)
- **A3: Manejo de sesiones y ruptura de autentificaciones** (fallos que permiten usar cuentas de otros, listas de claves y de usuarios)
- **A4: Insecure Direct Object References** (exposición de estructura interna y de elementos de desarrollo que permita al atacante suponer métodos y datos predecibles)
- **A5: Intercepción de peticiones entre sitios** (CSRF) (permite generar peticiones falsas de forma que el usuario piense que las está realizando en el sitio correcto cuando se trata de uno falso)
- **A6: Malas configuraciones de seguridad** (a nivel de framework, sistema operativo, aplicaciones de terceros)
- **A7: Almacenamiento con fallos de encriptación** (tarjetas de crédito sin encriptar, credenciales)
- **A8: Falta de restricción de acceso a URL**
- **A9: Protección insuficiente en la capa de transporte** (uso incorrecto de certificados de seguridad)
- **A10: Redirecciones y envíos sin validación**

9. Referencias

http://co.php.net/
http://us3.php.net/manual/es/security.php
http://co.php.net/manual/es/ini.sect.safe-mode.php#ini.safe-mode
http://www.genbetadev.com/seguridad-informatica/owasp-creando-aplicaciones-seguras
http://docs.joomla.org/Vulnerable_Extensions_List
http://forum.joomla.org/viewtopic.php?f=296&t=79477
http://www.joomla.org/about-joomla/the-project/partners.html
https://www.owasp.org/index.php/Main_Page