

Gestión de seguridad en tus proyectos Joomla!



Seguridad. Principios de diseño (Saltzer y Schroeder¹)

Mínimo privilegio	Cada sujeto ha de tener el mínimo de privilegios para realizar sus funciones
Separación de privilegios	Procurar que tengan que satisfacerse varias condiciones para realizar una función
Mínimo mecanismo común	Minimizar los recursos compartidos
Simplicidad de mecanismo	Evitar complicaciones innecesarias
Mediación completa	Hacer la comprobación de acceso siempre
Valores predeterminados seguros	La opción por omisión debería ser denegar el acceso al recurso
Diseño público	La eficacia del sistema de seguridad no debe basarse en el secreto del diseño
Aceptabilidad por los usuarios	El sistema de seguridad debe ser fácil de cumplir y poco molesto



Gestión de seguridad en tus proyectos Joomla!

I. Checklist para la configuración del servidor, preparación del alojamiento y cómo conseguir un alojamiento *Joomla Friendly*

II Buenas prácticas en la configuración de tu instalación antes de la entrada en producción

1. Permisos; Grupos, usuarios y privilegios de ejecución.
2. Securización de directorios
3. Copias de seguridad; desde tu alojamiento y desde componentes Joomla adhoc
4. Filtro para script kiddies. Activando el .htaccess

III Buenas prácticas en el seguimiento de instalaciones y parques de instalaciones Joomla

1. Seguimiento de vulnerabilidades y actualizaciones de seguridad.
2. Seguimiento, rastreo y neutralización de actividad hostil
 - A) Identificación desde el NOC y desde Joomla (Componentes de seguridad)
 - B) Neutralización de actividad hostil y limpieza de una instalación comprometida



I. Checklist para la configuración del servidor, preparación del alojamiento y cómo conseguir un alojamiento *Joomla Friendly*

CSF Firewall + LFD Login Failure Daemon

MySQL 5

Apache mod_security → Personaliza tus reglas
.htaccess → Personaliza tus reglas

PHP 5, con Suhosin Patch

magic_quotes_gpc ON

disable_functions

show_source, system, shell_exec, passthru, exec,
phpinfo, popen, proc_open

safe_mode OFF

register_globals OFF

allow_url_fopen OFF



II Buenas prácticas en la configuración de tu instalación antes de la entrada en producción

Si bien la instalación Base de Joomla! Es segura cuando ha sido instalada correctamente, las extensiones de terceros pueden ser completamente heterogéneas en cuanto a su edad, calidad o su trazabilidad.

No confíes ciegamente en todas las extensiones de terceros. Lee las opiniones de otras personas que ya han utilizado la extensión, asegúrate también de que es una extensión que se ha ido actualizando periódicamente, y que descargas la versión más reciente.

Si tienes conocimientos avanzados, revisa el código y asegúrate de que cumple con los requisitos de seguridad.

Copias de seguridad MUY frecuentes, de ficheros, y BBDD



Permisos; Grupos, usuarios y privilegios de ejecución.

Atendiendo a un criterio de mínima disponibilidad, es importante ajustar al máximo detalle posible el nivel de permisos

Permisos en carpetas y directorios

r = Read permiso de lectura
w = Write permiso de escritura
x = Execute permiso de ejecución

Propietario	Grupo	Otros
r w x	r w x	r w x
4 2 1	4 2 1	4 2 1

4+2+1	4+2+1	4+2+1
= 7	= 7	= 7

```
find . -type f -exec chmod 644 {} \;  
find . -type d -exec chmod 755 {} \;  
chmod 707 images  
chmod 707 images/stories  
chown apache:apache cache
```



Filtro para script kiddies. Activando el .htaccess

Limitar la ejecución de procesos o permisos dentro del directorio público es una primera y básica medida de seguridad que puede suponer un medio muy efectivo ante meros lammers y script kiddies entre otros.

Joomla incorpora por defecto un fichero .htaccess listo para renombrar y que no sólo permite reescribir las URL.

1. Renombrar el fichero .htaccess
2. Personaliza tus reglas .htaccess
 - [http://docs.joomla.org/Htaccess_examples_\(security\)](http://docs.joomla.org/Htaccess_examples_(security))
 - <http://perishablepress.com/press/tag/htaccess>



Securización de directorios y ficheros críticos

Protege los directorios que por su naturaleza o circunstancialmente requieran disponer de permisos 777 (images, docman, ...)

Añade un fichero .htaccess específico dentro del directorio restringiendo la posibilidad de ejecutar ficheros dentro de él:

```
AddHandler cgi-script .php .pl .py .jsp .asp .htm .shtml .sh .cgi
Options -ExecCGI

<Files .htaccess>
order allow,deny
deny from all
</Files>

<Files configuration.php>
order allow,deny
deny from all
</Files>
```



III Buenas prácticas en el seguimiento de instalaciones y parques de instalaciones Joomla.

Control de actualizaciones y versiones de componentes instalados.

Existen algunas herramientas que pueden suponer una importante ayuda para controlar y actualizar en bloque:

Joomla Mass Updater

Joomla Upgrade Notifier

Joomla Diagnostics

Joomla system tool

OWASP Joomla Vulnerability Scanner Project

Seguimiento de registros de incidencia y reportes de seguridad

Copias de seguridad regulares



Seguimiento de vulnerabilidades y actualizaciones de seguridad

Lugares de referencia para el seguimiento de vulnerabilidades y actualizaciones de Joomla

<http://developer.joomla.org/security.html>

<http://feeds.joomla.org/JoomlaSecurityNews>

Las extensiones y complementos de terceros suponen el porcentaje más importante de las quiebras de seguridad en Joomla. Es importante tener muy presente éste feed:

<http://feeds.joomla.org/JoomlaSecurityVulnerableExtensions>

Pero también las actualizaciones de los propios componentes y sistema operativo.



Seguimiento, rastreo y neutralización de actividad hostil

- A. Identificación desde el NOC y desde Joomla
(Componentes de seguridad)
- B. Neutralización de actividad hostil y limpieza de una
instalación comprometida



Identificación desde el NOC

Reportes de actividad sospechosa

```
Time: Thu Feb 11 15:47:12 2010 +0100
IP: 77.92.139.74 (TR/Turkey/datacenter-74-139-92-77.sadecehosting.net)
Hits: 11
Blocked: Temporary Block

Sample of block hits:
Feb 11 15:45:24 orix-1 kernel: Firewall: *TCP_IN Blocked*
IN=eth0 OUT= MAC=00:1c:c0:d4:45:94:00:24:c3:84:04:00:08:00 SRC=77.92.139.74 DST=94.23.154.250 LEN=52
TOS=0x00 PREC=0x00 TTL=56 ID=26905 DF PROTO=TCP SPT=3082 DPT=81 WINDOW=65535 RES=0x00 SYN URGP=0
Time: Thu Feb 11 13:37:56 2010 +0100
IP: 94.198.53.66 (RU/Russian Federation/-)
Hits: 11
Blocked: Temporary Block

Feb 11 15:45:24 orix-1 kernel: Firewall: *TCP_IN Blocked*
IN=eth0 OUT= MAC=00:1c:c0:d4:45:94:00:24:c3:84:04:00:08:00
SRC=77.92.139.74 DST=94.23.154.250 LEN=52
TOS=0x00 PREC=0x00 TTL=56 ID=26905 DF PROTO=TCP SPT=3082 DPT=81 WINDOW=65535 RES=0x00 SYN URGP=0
```

Sistematización y análisis de los reportes en tiempo real
24x7x365 desde el NOC (por ejemplo mediante SPLUNK)



Neutralización de actividad hostil y limpieza de una instalación comprometida

Comprueba si hay ficheros que han sido modificados en el ataque, y dedica tiempo a buscar cual ha sido el punto por el que han entrado (versión obsoleta de Joomla!, extensiones que habías instalado), y corrige el punto débil para que no vuelva a ocurrir.

Controla los archivos logs del servidor

Cambia la contraseña de FTP y MySQL

Guarda el fichero de configuración, imágenes y archivos particulares

Borra todo el directorio y vuelve a construir el sitio partiendo de una instalación nueva o copias de seguridad limpias.



¡Gracias!

Daniel Rodríguez Merino
d.rodriguez@occentus.net

