NS
Error 404 Control

Control del Error 404 para detectar ataques hacker

Índice de contenido

1.- DESCRIPCIÓN....3
2.- VENTAJAS....4
3.- REQUERIMIENTOS Y VERSIONES....5
4.- CONFIGURACIÓN DEL PLUGIN....6
5.- CÓMO SE CLASIFICA LA PELIGROSIDAD DE LOS ATAQUES....7
6.- NOTAS Y TRADUCCIONES....8
PREGUNTAS FRECUENTES....9

1.- DESCRIPCIÓN

NS Error404 Control es un plugin para Joomla! 3.1 o superior, que controla el error 404 para:

1. poder corregir estos errores, que ayudan al SEO;
2. detectar posibles ataques hackers.

Su segunda funcionalidad -detección de ataques-, se basa en que los atacantes hackers usan programas para descubrir qué webs son vulnerables y por dónde se puede acceder a zonas delicadas o, en ocasiones, comprometidas de la web. Estos programas -normalmente spiders- realizan comprobaciones generales provocando numerosos errores 404 que pueden ser detectados de forma fácil.

El plugin envía un email con información del error 404 al email que definamos y clasifica el error 404 según su índice de peligrosidad:

- si es una equivocación de un usuario;
- si se trata de una página que ya no existe pero que se mantiene enlazada desde otra página de la web;
- si es un spider o programa que intenta descubrir vulnerabilidades de la web.

Si el plugin considera que un hacker está intentando acceder a su web, marcará el email con un aviso en el asunto. De esta forma, mediante un gestor de correo y unos filtros, es fácil clasificar las amenazas a nuestra web.

NS Error404 Control es un plugin gratuito y clasificado en el JED -Joomla! Extensions Directory-.

La página web del proyecto es: http://www.netandsoftware.es

Contacto: joomla@netandsoftware.es

Twitter: @NetAndSoftware

2.- VENTAJAS

El plugin NS Error 404 Control no genera una tabla en la base de datos de Joomla!. Esto hace que los registros diarios no se almacenen en la web ni que se llene de registros una tabla de la base de datos de la web -uno por cada error 404-, por lo que este plugin no influye en la carga de la web ni empeora el rendimiento del sitio web.

El plugin envía un email, que puede ser clasificado rápidamente por un cliente de correo.

En resumen, las características del plugin son:

- Detectar errores 404 para mejorar el SEO
- Detección de posibles ataques hackers

Las ventajas del plugin NS Error 404 Control de NetAndSoftware son:

- Bajo impacto en la carga de la web
- No existe almacenamiento de los errores en la base de datos
- Clasificación de la peligrosidad de los errores generados por su web
- Fácil instalación
- Fácil configuración
- Minimizar accesos a la web que no son visitas

3.- REQUERIMIENTOS Y VERSIONES

Los requisitos técnicos para instalar este plugin son:

- tener Joomla! 3.2 o superior, aunque puede funcionar con Joomla! 3.1.x;
- usar la reescritura de las URLs en la configuración global de Joomla! (Sistema → Configuración Global → Pestaña Configuración SEO → Reescritura de las URLs, puesto en Sí), lo que obliga a renombrar htaccess.txt a .htaccess para servidores Apache;
- el plugin de redirección de Sistema debe estar deshabilitado. Para ello: Extensiones → Gestor de Plugins → Sistema – Redirección (Deshabilitar)

La primera versión pública del plugin NS Error 404 Control -con descarga gratuita- fue la 1.0.0.

Las versiones de NS Error 404 Control se clasifican al estilo de Joomla!.

El primer número indica la versión mayor, que sólo cambiará cuando haya un cambio realmente sustancial en este plugin.

El segundo número cambiará cuando se produzca un aumento en los scripts y detecciones peligrosas de los errores 404.

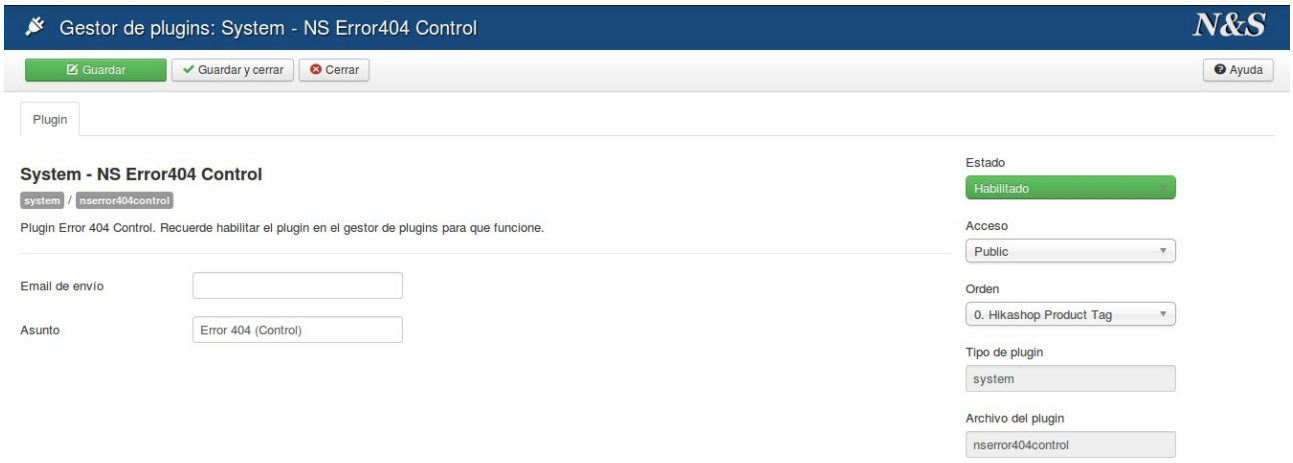
El tercer número indicará mejoras a nivel de funcionamiento o pequeños parches sin importancia.

4.- CONFIGURACIÓN DEL PLUGIN

La configuración del plugin NS Error 404 Control es muy sencilla. Sólo debe activarse el plugin y rellenar dos campos en la configuración. Para ello:

- Vaya a *Extensiones → Gestor de Plugins*
- Busque el plugin bajo el nombre “System - NS Error 404 Control” y pinche en el nombre.
- Publique el plugin seleccionando la casilla “Estado” a “Habilitado”. Se verá en color verde.
- Luego rellene los campos “Email de Envío” para indicarle al plugin dónde desea recibir los emails, y “Asunto” para indicarle un nombre al asunto del correo que se le envíe.

Para más detalles puede ver la imagen siguiente:



En el caso de no rellenar los datos de configuración, el Asunto del email enviado será “Error 404 (Control)” y la dirección donde se envían los correos será la predeterminada por su Joomla!.

IMPORTANTE: Recuerde que el plugin de redirección del sistema de Joomla! debe estar deshabilitado, y la reescritura de las URLs debe estar habilitada. Para más información vea el apartado 3 de esta documentación.

5.- CÓMO SE CLASIFICA LA PELIGROSIDAD DE LOS ATAQUES

La clasificación de la peligrosidad se realiza según la experiencia de varias webs que controlaban este error.

A través de las webs de nuestros proyectos que controlaban el error 404 mediante un script en PHP creado por N&S, se estudiaron qué accesos eran intentos ilegales a la web, qué métodos usaban, cómo averiguaban los hackers el tipo de web, y otras cuestiones algo más técnicas. Con ello se ha podido elaborar una clasificación de la peligrosidad del hacker según los accesos erróneos 404.

Con el paso del tiempo y según avancen las técnicas de hacking, el plugin se irá actualizando con mejoras en la detección de posibles ataques hackers.

Si en el plugin NS Error 404 Control se incorporasen mejoras en técnicas de detección, el segundo número de la versión de la actualización del plugin cambiaría.

Hay 6 niveles de peligrosidad en los ataques:

- **Sin riesgo**: cuando el plugin determina que es muy poco probable que el error 404 se deba a algún intento de ataque. Generalmente, cuando un error 404 se produce de forma lícita, por una equivocación de la persona al escribir la URL, o por un enlace roto, el plugin lo marca de esta forma.
- **Indeterminado**: cuando el plugin es incapaz de detectar con seguridad si el error 404 es por un error o por un intento hacker.
- **Riesgo Mínimo**: cuando se está accediendo a una URL o a extensiones que suelen ser vulnerables.
- **Riesgo Medio**: cuando parece muy probable que un hacker o un programa automático esté intentando conocer sus vulnerabilidades. El asunto del email enviado se marcará con un “Aviso”.
- **Riesgo Alto**: cuando el riesgo y peligrosidad de intento de acceso es alto y deben ponerse medidas al respecto. El asunto del email enviado se marcará con un “Aviso”.
- **Riesgo Muy Alto**: cuando, o existen varias amenazas combinadas o se produce un intento de acceso a URLs que suelen ser peligrosas. El asunto del email enviado se marcará con un “Aviso”.

6.- NOTAS Y TRADUCCIONES

Importante: Mantenga siempre actualizado este plugin.

Al igual que otras extensiones de Joomla!, éstas deben estar siempre actualizadas para no tener problemas de seguridad. Este plugin no es una excepción, y debe ser actualizado en cuanto haya una versión superior.

Este plugin no rompe la compatibilidad hacia atrás a partir de Joomla! 3.2.

Traducciones: Si desea traducir este plugin, póngase en contacto con nosotros en: joomla@netandsoftware.es

Este documento fue escrito el 30 de abril de 2014.

Última revisión del documento: 30 de abril de 2014.

Autor: Net & Software (NetAndSoftware)

PREGUNTAS FRECUENTES

Con este plugin, ¿puedo sentirme a salvo de ataques hackers?

No. Es una excelente herramienta para realizar detecciones, pero no te salva del ataque. Te recomendamos que leas el detallado artículo sobre htaccess de N&S para que puedas bloquear algunos de estos ataques: http://www.netandsoftware.es/articulos-blog/articulos-del-blog/art-para-webmasters-y-joomla/505-htaccess-en-profundidad-la-guia-completa.

¿Por qué no se implementa una herramienta para el bloqueo de los ataques en el propio plugin?

No sería difícil implementarlo, pero también es difícil asegurar cuándo se está produciendo un ataque, por lo que esta herramienta podría bloquear tráfico correcto a la web, con el consiguiente perjuicio. Por eso, la última palabra para determinar si el ataque es real o no, la debe tener siempre el webmaster o administrador del sistema Joomla!, que tiene el juicio para determinarlo con seguridad, y poseerá los conocimientos para parar de forma adecuada el intento de penetración.

¿Cómo puedo bloquear ataques?

Existen muchas formas, pero la mejor forma para un usuario medio es mediante el htaccess.

Hay que destacar que el baneo de IP no es eficaz -ya que los hackers usan proxies que cambian la IP en cada intento de acceso-, así que la mejor forma es mediante pequeños bloqueos en el htaccess según las URL, por ejemplo:

RewriteRule ^(.+)ploadify.ph(.+)$ - [F,L]

que envía un error 403 (Forbidden).

Esto provoca que se prohíba el acceso a ese spider, y posiblemente sus estadísticas de visitas sean más reales.

¿Me sirve para algo conocer si me están intentando hackear el sistema?

Le sirve para mantenerle alerta y que mantenga siempre la seguridad de su sitio web. Esto se consigue teniendo Joomla! completamente actualizado, al

igual que todas y cada una de las extensiones de Joomla!. Procure hacer esto siempre -es la estrategia de seguridad correcta-, y no sólo cuando el plugin NS Error 404 Control le avise.