Published on *Marco de Desarrollo de la Junta de Andalucía* (http://127.0.0.1/servicios/madeja)

Auditoría y Registro

Código: SEG_Auditoria

La auditoría y el registro de los eventos que suceden al ejecutar nuestras aplicaciones nos permite monitorizarlas y detectar posibles intentos de ataques o intrusiones. Además, veremos cómo mejorar la gestión de los archivos de log para que sean más seguros.

Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática se utiliza para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre en un dispositivo en particular o aplicación.

La mayoría de los logs son almacenados o desplegados en el formato estándar, el cual es un conjunto de caracteres para dispositivos comunes y aplicaciones. De esta forma cada log generado por un dispositivo en particular puede ser leído y desplegado en otro diferente.

También se le considera como aquel mensaje que genera el programador de un sistema operativo, alguna aplicación o algún proceso, en virtud del cual se muestra un evento del sistema.

Objetivos

- Garantizar la monitorización de los eventos que se producen en la aplicación
- Asegurar la información de los ficheros de registro

Código	Título	Tipo	Carácter
PAUT-0207	Archivos de registro	Directriz	Obligatoria
PAUT-0246	Denegación de servicio	Directriz	Obligatoria
LIBP-0275	Diseño del log	Directriz	Obligatoria
LIBP-0278	Información del log	Directriz	Recomendada
LIBP-0279	Manejo de los registros de auditoría	Directriz	Obligatoria

Código	Título	Tipo	Carácter
RECU-0580	Generar trazas para la depuración en PHP	Ejemplo	Obligatorio
RECU-0579	Log de errores en PHP	Manual	Obligatorio

Archivos de registro

- **Área:** Auditoría y Registro
- **Tipo de pauta:** Directriz
- **Carácter de la pauta:** Obligatoria

Código: PAUT-0207

Proteger los archivos de registro

Si no se controla el acceso de los usuarios a los archivos de registro, un atacante podría falsificar las entradas, obtener información del sistema, insertar contenido malicioso e incluso eliminar registros

LOPD | Seguridad

Source URL: http://127.0.0.1/servicios/madeja/contenido/pauta/207

Denegación de servicio

- **Área:** Auditoría y Registro
- **Tipo de pauta:** Directriz
- **Carácter de la pauta:** Obligatoria

Código: PAUT-0246

Impedir la denegación de servicio a través del log

Se debe impedir la denegación de servicio (o interrupción del sistema) a través del log. Si no se protege el log, podría incrementarse el tamaño del archivo por parte de un atacante,insertando líneas en el mismo hasta denegar el servicio.

Colocando el archivo de log en una partición separada del sistema operativo o implementando un mecanismo de monitorización de sistemas, de tal manera que pueda tener un criterio respecto al tamaño del archivo, enviando una alerta cuando se produzca un ataque de este tipo.

Disponibilidad | ENS | Seguridad

Diseño del log

- **Área:** Auditoría y Registro
- **Tipo de pauta:** Directriz
- **Carácter de la pauta:** Obligatoria

Código: LIBP-0275

Seguir las siguientes indicaciones a la hora de diseñar los archivos de log de una aplicación

Pautas

Título	Carácter
Registro de información	Obligatoria
Escritura en logs	Obligatoria
Logs seguros y confidenciales	Obligatoria
Información completa	Obligatoria
Logger único	Obligatoria

Registro de información

Registrar toda la información de errores en un log.

Toda la información de errores se debe registrar en un log, evitando el uso de trazas automáticas o manuales

Volver al índice

Escritura en logs

Escribir sólo nueva información en el log.

Los atributos del archivo de log deben permitir escribir sólo nueva información en ellos, impidiendo que los registros anteriores sean reescritos o eliminados.

Para obtener una seguridad adicional, los logs también deberían ser escritos en un soporte de escritura/múltiple lectura tal como un CD-R.

Volver al índice

Logs seguros y confidenciales

Garantizar la seguridad y confidencialidad de los logs.

Se debe asegurar la seguridad y la confidencialidad de los logs aunque la información haya sido salvada

Volver al índice

Información completa

Garantizar que la información es completa.

Se debe asegurar que la información que se registra en el log es completa y suficiente para identificar el suceso que ha ocurrido.

Volver al índice

Logger único

Utilizar sólo un logger por clase.

Debemos utilizar un logger por cada clase, de tal manera que, en el registro, pueda identificarse la clase que lo ha generado.

Volver al índice

Recursos

Área: Desarrollo » Seguridad » Auditoría y Registro

Código	Título	Tipo	Carácter

RECU-0579	Log de errores en PHP	Manual	Obligatorio
RECU-0580	Generar trazas para la depuración en PHP	Ejemplo	Obligatorio

ENS | LOPD | Seguridad | Trazabilidad

Información del log

- **Área:** Auditoría y Registro
- **Tipo de pauta:** Directriz
- **Carácter de la pauta:** Recomendada

Código: LIBP-0278

Seleccionar la información que va a contener el log de la aplicación.

Los logs pueden contener diferentes tipos de información. La selección de la información se relaciona normalmente con la motivación que conduce al loggeo de la misma.

Esta sección contiene información sobre los diferentes tipos de información de log y las razones por las cuales podríamos querer loggearlas.

En general, las características de loggeo incluyen información de depuración de errores tal como la fecha y hora del evento, procesos iniciados o dueño del proceso, y una descripción detallada del evento, así como acciones consideradas críticas en la lógica de negocio.

Pautas

Título	Carácter
Acceso al archivo de información	Recomendada
Estructura de los logs	Recomendada
Información significativa	Recomendada
Funciones administrativas y de configuración	Recomendada
Depuración de errores	Recomendada
Intentos de autorización	Recomendada
Eliminación de información	Recomendada
Comunicaciones de red	Recomendada
Eventos de Autenticación	Recomendada

Acceso al archivo de información

Escribir en el log los accesos al archivo de información.

Podemos escribir en el log los accesos al archivo de información de manera que, posteriormente, podamos ver qué tipo de información es leída, cuándo fue leída y el usuario que la leyó.

Volver al índice

Estructura de los logs

Crear una estructura para los logs de información.

Debemos establecer una estructura para los logs de información indicando dónde y cómo se escribe la información. De este modo podemos ver si la información fue sobreescrita o si el programa está escribiendo en un momento determinado.

Volver al índice

Información significativa

Incluir información significativa en los logs

Se recomienda que el log muestre sólo información significativa y relevante, para facilitar su lectura por parte del administrador de la aplicación.

Volver al índice

Funciones administrativas y de configuración

Registrar las funciones administrativas y de configuración

Se recomienda registrar las funciones administrativas y los cambios de configuración (actividades de manejo de cuenta, visualización de información de usuario, habilitación o deshabilitación de loggeo, etc.).

Volver al índice

Depuración de errores

Incluir información de depuración de errores.

Se recomienda incluir información de depuración de errores, permitiendo que ésta pueda ser activada o desactivada.

Volver al índice

Intentos de autorización

Registrar los intentos de autorización.

En aplicaciones de con un alto nivel de seguridad se debe registrar en el log todos los intentos de autorización, mostrando: el usuario, la fecha, la hora, el tipo de acceso y si ha sido aceptado o rechazado.

Con esto podemos detectar intentos para forzar las contraseñas e incluso alimentar un sistema de detección de intrusos que detectará anomalías.

Volver al índice

Eliminación de información

Registrar la información que se va a eliminar

Se recomienda registrar la eliminación de cualquier tipo de información (objeto).

Volver al índice

Comunicaciones de red

Escribir en los logs las comunicaciones de red

Se recomienda escribir en los logs las comunicaciones de red (asociación, conexión, aceptación, etc). Con esta información un sistema de detección de intrusos puede detectar escaneos de puertos y ataques de fuerza bruta.

Volver al índice

Eventos de Autenticación

Incluir en los logs los eventos de autenticación

Es recomendable incluir todos los eventos de autenticación (inicio de sesión, cierre de sesión, intento de acceso fallido, etc.) en los logs de modo que permita detectar ataques de fuerza bruta y también ataques por adivinación.

Volver al índice

ENS | LOPD | Seguridad | Trazabilidad

Manejo de los registros de auditoría

- **Área:** Auditoría y Registro
- **Tipo de pauta:** Directriz
- **Carácter de la pauta:** Obligatoria

Código: LIBP-0279

Almacenar los registros de auditoría en lugares con alta integridad.

Los registros de auditoria se encuentran legalmente protegidos en muchos países y deben ser guardados en lugares con alta integridad para prevenir modificaciones y eliminaciones casuales o motivadas. Para ello se deben seguir las siguientes indicaciones:

Pautas

Título	Carácter
Auditoría de eventos	Obligatoria
Centralización de logs	Obligatoria
Revisión de logs	Obligatoria
Repositorios confiables	Obligatoria
Confianza de punta a punta	Obligatoria
Revisión de las entradas de logs	Recomendada
Vigencia del log	Obligatoria

Auditoría de eventos

Auditar eventos realmente importantes.

Debemos auditar solamente aquellos eventos que son realmente importantes ya que los registros de auditoría se tienen que mantener por un tiempo prolongado, lo que podría ocasionar una pérdida importante de recursos si registramos los mensajes de debug o mensajes que contienen sólo información del sistema.

Volver al índice

Centralización de logs

Centralizar los logs en sistemas seguros.

Debemos centralizar los logs y asegurar que los registros de auditoría más importantes no son almacenados en sistemas vulnerables, particularmente servidores web.

Volver al índice

Revisión de logs

Revisar las copias de los logs

Debemos revisar solamente las copias de los logs, evitando revisar logs originales

Volver al índice

Repositorios confiables

Proveer repositorios confiables a largo tiempo

Debemos proveer repositorios confiables a largo tiempo para los sistemas altamente protegidos mediante la utilización de dispositivos de escritura única o similar.

Volver al índice

Confianza de punta a punta

Garantizar la confianza de punta a punta en los mecanismos de log

Debemos asegurar que existe una confianza de punta a punta en los mecanismos de log en sistemas altamente protegidos.

Volver al índice

Revisión de las entradas de logs

Disponer de herramientas para la lectura de logs

Es recomendable disponer de herramientas de auditoría para leer logs de errores, que puedan reducir la mayor parte del ruido que suele estar basado en la repetición de eventos o se origina de la misma fuente. También puede ser muy útil si el visualizador de log puede desplegar los eventos ordenados por nivel de severidad en lugar de mostrar sólo la hora en la que ocurrió.

Volver al índice

Vigencia del log

Establecer un periodo mínimo de vigencia del log

En aplicaciones con alto nivel de seguridad es obligatorio por ley conservar los datos del registro durante, al menos, dos años.

Volver al índice

LOPD | Seguridad

Generar trazas para la depuración en PHP

- **Área:** Auditoría y Registro
- **Carácter del recurso:** Obligatorio
- **Tecnologías:** PHP

Código: RECU-0580
Tipo de recurso: Ejemplo

Descripción

Es recomendable crear una traza de la ruta de ejecución desde la que se inicia el sistema hasta que se produce una excepción. Esta traza debe contener todas las invocaciones que van sucediendo, en qué línea salta la ejecución, hasta terminar en el lugar exacto donde falló el sistema. PHP aporta una función que le permite realizar esto, como en el ejemplo siguiente

```
<?php
// filename: /tmp/a.php

function a_test($str)
{
    echo "\nHi: $str";
    var_dump(debug_backtrace());
}

a_test('friend');
?>

<?php
// filename: /tmp/b.php
include_once '/tmp/a.php';
?>
```

Pautas

Área: Desarrollo » Seguridad » Auditoría y Registro

Código	Título	Tipo	Carácter
LIBP-0275	Diseño del log	Directriz	Obligatoria

ENS | LOPD

Source URL: http://127.0.0.1/servicios/madeja/contenido/recurso/580

Log de errores en PHP

- **Área:** Auditoría y Registro
- **Carácter del recurso:** Obligatorio
- **Tecnologías:** PHP

Código: RECU-0579
Tipo de recurso: Manual

Descripción

Es necesario crear un log de errores que permita controlar cuando se ha producido un error, de tal manera que permita corregirlo y evitar que se repita en el futuro.

En PHP necesitamos indicar, al abrir el archivo, el modo de utilización del mismo. Para crear un log, abriremos el archivo en modo 'a' (escritura al final) y escribiremos el error indicando la fecha, para simplificar el trabajo lo podemos incluir todo en una función:

```
<?php
function error($numero,$texto){
 $ddf = fopen('error.log','a');
 fwrite($ddf,"[".date("r")."] Error $numero: $texto\r\n");
 fclose($ddf);
}
?>
```

Una vez declarada la función, sólo es necesario llamarla de la siguiente manera cuando se produzca un error php para que se guarde en error.log:

```
<?php
// Si no existe la cookie sesion
if(!isset($_COOKIE['sesion'])){
// Guardamos un error
error('001','No existe la cookie de sesion');
}
?>
```

De esta manera, cada vez que un usuario entra a esta página sin la cookie sesión, se almacena una nueva línea en el fichero indicado:

[fecha] Error 001: No existe la cookie de sesión

Vamos a ver ahora como podemos mejorar esto de manera que además de poder grabar los errores Php, nos almacene los errores Php producidos durante la ejecución del script php. Esto lo conseguiremos indicando al interprete Zend que llame a la función error() cada vez que el código Php contenga un error con la función set_error_handler:

```
<?php
set_error_handler('error');
?>
```

Entonces, el código completo del log de error Php queda de la siguiente manera:

```
<?php
function error($numero,$texto){
$ddf = fopen('error.log','a');
fwrite($ddf,"[".date("r")."] Error $numero:$texto\r\n");
fclose($ddf);
}
set_error_handler('error');
?>
```

Pautas

Área: Desarrollo » Seguridad » Auditoría y Registro

Código	Título	Tipo	Carácter
LIBP-0275	Diseño del log	Directriz	Obligatoria

ENS | LOPD