



Cory Thoman, 123f

Acceso Web restringido con el Gestor de Acceso SUMO

UN AYUDANTE CACHAS

SUMO le permite añadir un módulo de gestión de usuarios repleto de funcionalidades a su aplicación web con unas cuantas líneas de código. **POR TIM SCHÜRMANN**

SUMO es una herramienta para la gestión de usuarios lista para su uso que se puede incorporar a su aplicación PHP con tan sólo añadir unas cuantas líneas de código. Una vez integrada con su aplicación web, se encargará de gestionar la autenticación y la autorización por usted. La integración de SUMO proporciona una interfaz web cómoda para la gestión de los usuarios, la asignación de los mismos a los grupos y la asignación de los derechos.

Las credenciales de los usuarios pueden residir en una base de datos MySQL, PostgreSQL u Oracle. Como alternativa, los usuarios pueden autenticarse por medio de LDAP, Active Directory, una cuenta existente de Google Mail o una cuenta del Sistema de Gestión de Contenidos Joomla!

Además del método de autenticación básico y los servicios de control de

acceso, SUMO proporciona otras funcionalidades de seguridad útiles. (Véase el cuadro titulado “Seguridad en SUMO”). Los administradores pueden configurar y

gestionar SUMO por medio de una interfaz web elegante que hace uso de la tecnología AJAX para emular un entorno de escritorio. Para un buen rendimiento

Seguridad en SUMO

SUMO proporciona varias características de seguridad para proteger un sitio web contra ataques externos. Por ejemplo, los IDs de las sesiones de los usuarios conectados se renuevan cada 10 segundos, dificultando que los atacantes puedan secuestrar y explotar las identidades de los usuarios.

Los datos enviados por el formulario de conexión tienen que pasar por un filtro. De esta forma se impiden los ataques XSS (cross-site scripting) y los intentos de inyección de código. Además, un filtro de IP cuenta los intentos de conexión fallidos. Si el número de intentos fallidos crece rápidamente en un período corto de tiempo, se supondrá que alguien está intentando realizar un ataque por fuerza bruta. En este caso, SUMO bloqueará

cualquier petición desde esa dirección IP durante un período de tiempo. Como salvaguarda adicional, se pueden definir las direcciones IP desde las cuales cada usuario tiene permiso para acceder al sistema.

Un gestor de registro interno graba cualquier mensaje importante del sistema y los errores, así como todas las acciones de los usuarios. SUMO puede almacenar los ficheros de registro en una base de datos o en ficheros de texto, o bien, puede mandarlos por correo al administrador si lo prefiere. SUMO también proporciona información detallada de los usuarios activos a los administradores, incluyendo sus direcciones IP, país de origen y las aplicaciones clientes que están utilizando.

será necesario el uso de un navegador con un intérprete JavaScript rápido.

A pesar de que el desarrollador Alberto Basso ha estado trabajando en el sistema de gestión de acceso de SUMO desde 2003, sólo va por la versión 0.5.0. Sin embargo, el número de versión tan bajo no indica nada acerca de la funcionalidad real y del estado de desarrollo de SUMO. Si está interesado en comprobar su estabilidad y rendimiento, puede probar la demo de la página web del programa [1]. SUMO se distribuye bajo licencia GPL v2.

Ingredientes

Como aplicación PHP, SUMO requiere un servidor web que incluya un intérprete de PHP 5.0 o posterior. Si posteriormente desea añadirle el sistema de autenticación basado en Google Mail, también será necesario el módulo de PHP cURL.

Desde hace unos años, SUMO ha almacenado sus propios datos en una base de datos; puede elegirse MySQL desde la versión 3.23, PostgreSQL 8.3 o SQLite versión 2, aunque perderá algunas funciones si opta por SQLite. La integración con su propia aplicación web también requiere algunos conocimientos de programación PHP.

Si desea probar SUMO, los desarrolladores recomiendan la última versión de XAMPP [2], que viene con todos los componentes necesarios. Para comenzar, introduzca como root los siguientes comandos para descomprimir los paquetes en el directorio `/opt`:

```
sudo tar xvfz xampp-<versión>
.tar.gz -C /opt
```

A continuación teclee el siguiente comando para ejecutar los servidores proporcionados:

```
sudo /opt/lampp/lampp start
```

La instalación de SUMO es sumamente rápida. Primero se descomprime el

Listado 1: Configuración de la Base de Datos

```
01 $sumo_db['type'] = 'mysql'
02 $sumo_db['host'] = 'localhost'
03 $sumo_db['port'] = '3306'
04 $sumo_db['name'] = 'theaterdb'
05 $sumo_db['user'] = 'tim'
06 $sumo_db['password'] = 'secret'
```

archivo en un directorio del servidor (en el ejemplo se llama *sumo*). Si utiliza la distribución XAMPP Apache que viene con MySQL, PHP, Perl y otras herramientas ya preconfiguradas, descomprima el paquete en `/opt/lampp/htdocs`. Luego hay que darle al servidor web acceso de escritura a las carpetas de SUMO.

Si el sistema de gestión de usuarios no posee permisos de escritura, fallará posteriormente.

Almacén

El segundo paso consiste en indicarle a SUMO qué base de datos tiene que utilizar. Hay que abrir el fichero `config.database.php` que se encuentra en el directorio `config` y modificar la línea que comienza con `$sumo_db` al comienzo (línea 27). En el ejemplo mostrado en el Listado 1, MySQL (*mysql*) escucha en el puerto 3306 del mismo servidor (*localhost*). En este punto quiero que SUMO utilice la base de datos *theaterdb*, de donde puede utilizar la cuenta *tim* con la contraseña *secret*. Si tiene una instalación XAMPP, el nombre de usuario es *root*, y la contraseña no está establecida. En la parte inferior del fichero `config.database.php` se encuentran las plantillas para las bases de datos PostgreSQL y SQLite; para activarlas deben eliminarse los signos de almohadilla.

Normalmente SUMO reside en la base de datos de la aplicación web, que en este ejemplo es *theaterdb*, mostrada en el Listado 1. Las tablas que utiliza SUMO comienzan todas con el prefijo *sumo_* para impedir el solapamiento. Si su aplicación web no utiliza ninguna base de datos, tendrá que crear una. Para ello, usando XAMPP, ejecute `http://localhost/phpmyadmin`, teclee el nombre de la base de datos en *Create new database* y luego pulse *Create*.

El siguiente paso consiste en crear las tablas de la base de datos que utilizará la herramienta. De

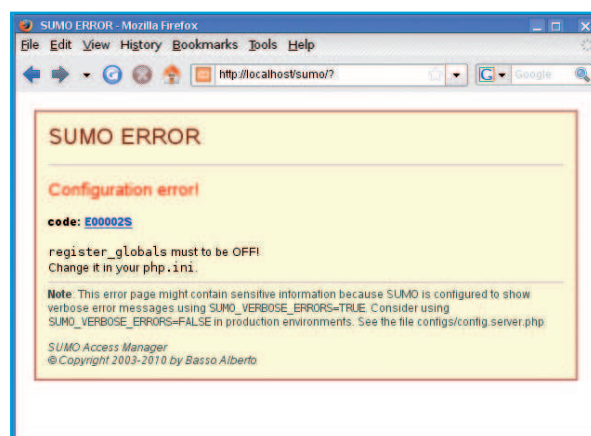


Figura 1: Si el parámetro `register_globals` está establecido en `php.ini`, aparecerá este error.

ello se encarga un script que se encuentra en el subdirectorio *install*. El directorio contiene un script para cada tipo de base de datos soportada. Por ejemplo, los usuarios de MySQL tienen que utilizar `database_mysql.sql`. Los detalles de cómo ejecutar el script SQL dependen de la elección de la base de datos. Algunos proveedores de web ofrecen una GUI en sus respectivas áreas de clientes. Los usuarios de XAMPP querrán ejecutar de nuevo phpMyAdmin en `http://localhost/phpmyadmin`. Para asegurarse de que se ha seleccionado la base de datos correcta, hay que comprobar la solapa de la izquierda, luego hay que ir a la solapa SQL, insertar el contenido del fichero `database_mysql.sql` en el cuadro de texto grande y presionar el botón *OK* para ejecutar la colección de comandos. Como resultado se obtienen 18 tablas nuevas, empezando todas ellas con *sumo_*.

Finalmente, hay que asegurarse de que la variable PHP `register_globals` tenga el valor *off*. En caso contrario, SUMO rehusará cooperar (Figura 1). Hay que editar el fichero `php.ini` (en XAMPP se encuen-

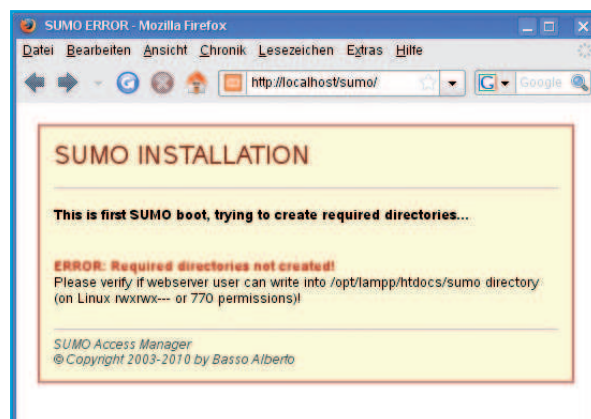


Figura 2: SUMO quejándose por no tener acceso de escritura.

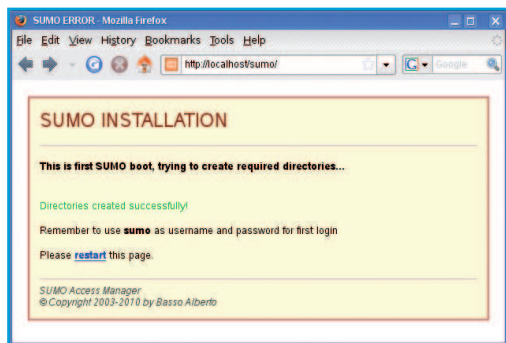


Figura 3: Si ve este mensaje, la instalación habrá concluido satisfactoriamente.

tra en el directorio `/opt/lampp/etc`, buscar la línea que comienza con `register_globals =` y reemplazarla, si es necesario, con lo siguiente:

```
register_globals = Off
```

En XAMPP, además hay que reiniciar el servidor web:

```
sudo /opt/lampp/lampp restart
```

Ahora ya se puede acceder a la interfaz del gestor en `http://ejemplo.com/sumo`, donde `ejemplo.com` es el nombre de dominio y `sumo` el directorio en el que reside SUMO: En XAMPP sería `http://localhost/sumo`.

Cuando se ejecuta por primera vez, SUMO crea un par de directorios temporales en su propia carpeta. Esto sólo sucede si el servidor web posee permiso de escritura. Si no fuese así, aparecería el mensaje mostrado en la Figura 2. Si ve este mensaje, habrá que modificar los permisos correspondientes para `sumo`.

Tras crear las carpetas, podrá ver el mensaje de éxito mostrado en la Figura 3. Pulse `restart` y aparecerá la página de inicio de sesión a la espera de que se introduzca `sumo` como nombre de usuario y `sumo` como contraseña (Figura 4).

La Consola

La consola de SUMO mostrada en la Figura 5 generará un par de noticias y de avisos. Las ventanas amarillas desaparecen tras unos segundos, pero hay que confirmar el mensaje rojo de forma explícita. Especialmente cuando SUMO se esté ejecutando en un servidor en Internet, sería muy buena idea seguir las sugerencias por razones de seguridad. Una sugerencia, por ejemplo, consiste en la modificación de la contraseña `sumo`

que viene por defecto en la cuenta del administrador. Para ello es preciso pulsar el aviso rojo *Change now* y teclear una contraseña segura en los dos cuadros de texto que aparecen. Por otro lado, se puede acceder a esta función por medio de *Console | Users & Groups*; hacer doble clic sobre *Users*, hacer clic en *sumo*, pulsar en *Edit* y luego en

Security Options.

El siguiente paso consiste en borrar el subdirectorio `install`. Si esta es su primera experiencia con SUMO, probablemente desee mantener el directorio `examples` (del que hablaremos un poco más adelante); si no, puede borrar este directorio, ya que es una posible vulnerabilidad. Luego se deben comprobar nuevamente los permisos de los ficheros. Los desarrolladores recomiendan el uso del comando `chmod` con `640` para los ficheros y `750` para los subdirectorios.

Al fin ya podrá echarle un vistazo a la consola de SUMO con la barra de menú en la parte superior. En el lado izquierdo puede utilizar *Console* para cambiar los parámetros. Como alternativa, puede hacer doble clic en el icono del escritorio. La ayuda no le lleva a un sistema de ayuda en línea, sino al típico *Acerca de...* Windows. La documentación [1] del sitio web contiene un manual incompleto.

Si se pulsa *Exit* se sale de la sesión actual. En el lado derecho, se puede acceder rápidamente al perfil de un usuario haciendo clic sobre su nombre; el icono que se encuentra junto a esta opción limpia el escritorio, y la bandera permite el cambio de idioma, al final de la lista se encuentra la configuración de la fecha y hora.

Usuarios y Grupos

El primer paso para el administrador consiste en indicarle a SUMO



Figura 4: La página de registro de la consola de SUMO.



Figura 5: La consola de SUMO le ayuda a configurar a los usuarios. Algunos parámetros aparecen en pequeños cuadros de diálogo, como el de ayuda mostrado aquí.

qué usuarios tienen permiso para acceder a la aplicación web. Al igual que en la mayoría de los sistemas de gestión de usuarios, cada usuario posee un nombre de usuario único y puede pertenecer a uno o varios grupos. Como experimento inicial, un único usuario perteneciente a un único grupo propio es suficiente. Para crear el grupo, vaya a *Console | Users & Groups*; haga doble clic en *Groups* y presione *Add*: Hace falta un nombre para el grupo, digamos `clientes` y, opcionalmente, una descripción. Tras pulsar en *OK* para crear el grupo, se puede crear el usuario de pruebas y añadir el usuario a este grupo. Para ello, haga doble clic en *Users* que se encuentra en la ventana *Console |*

Tabla 1: El Significado de los Niveles de Acceso

Nivel de Acceso	Significado
1	Actualmente no se utiliza en SUMO.
2	Actualmente no se utiliza en SUMO.
3	El usuario puede ver el recurso.
4	El usuario puede ver y editar el recurso.
5	El usuario puede ver, editar y crear el recurso.
6	Actualmente no se utiliza en SUMO; aunque el usuario puede ver, editar y crear el recurso.
7	El usuario puede hacer lo que quiera con el recurso (ver, editar, crear y borrar).

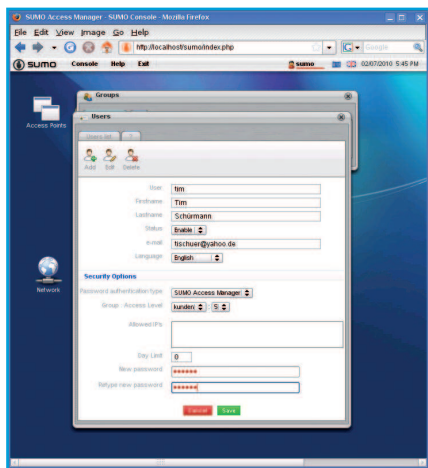


Figura 6: Creando un usuario nuevo, tim.

Users and Groups y presione Add para obtener el formulario que se muestra en la Figura 6.

Para crear un usuario hay que rellenar el nombre de usuario (User); especificar el nombre real del usuario, sus apellidos y su correo electrónico; y establecer el idioma, en la mayoría de los casos Inglés. Para que el usuario pueda iniciar sesión, hay que establecer su Status a Enable. El Password authentication type (tipo de autenticación) define el tipo de credenciales y la forma de autenticación (véase el cuadro titulado “Métodos de Accesos Alternativos”). Si desea que SUMO gestione los datos de la cuenta,

tiene que introducir una contraseña en los dos cuadros de texto de la parte inferior.

Cada usuario posee ciertos privilegios. En un portal de noticias, por ejemplo, algunos usuarios tendrán derechos para leer los mensajes y otros para crearlos. El nivel de acceso, un valor numérico, decide qué derechos posee un usuario. La Tabla 1 muestra qué niveles de acceso poseen los usuarios para realizar varias tareas.

El grupo especial *sumo* permite a sus miembros acceder a los recursos del resto de los grupos. Dicho de otro modo, el grupo *sumo* es el de los administradores. Un miembro que adicionalmente posea el nivel 5 o superior podrá crear, modificar y borrar grupos por medio de la consola de SUMO.

Para añadir el nuevo usuario al grupo *clientes*, seleccione el grupo en la lista desplegable junto a Group: Acces Level (Figura 6). La Tabla 1 muestra los niveles de acceso disponibles para los usuarios. Si el usuario de prueba tiene permiso para acceder al sitio web desde cualquier dirección IP, deje el cuadro de texto Allowed Ips vacío. Para restringir el acceso, teclee la dirección IP desde la

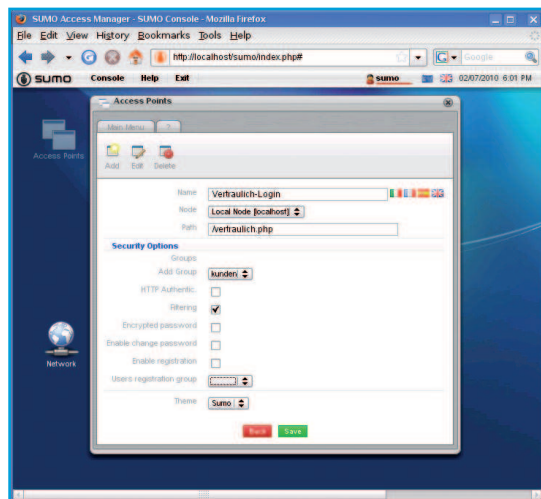


Figura 7: El punto de acceso a la página confidencial.php.

ejemplo, el sitio será *confidential.php*, que se encuentra directamente en el directorio raíz del sitio web, por simplicidad (es decir, en */opt/lampp/htdocs* si tiene XAMPP). Siguiendo el ejemplo del Listado 2, primero hay que activar *sumo.php*.

Desde la línea segunda hasta la última del Listado 2 se habilita la opción de cierre de sesión. Si quiere que SUMO proteja múltiples páginas o ficheros PHP, cada uno de ellos tendrá que integrar *sumo.php*, como se muestra aquí.

Punto de Acceso

Finalmente, hay que indicarle a SUMO qué páginas usarán los usuarios para iniciar la sesión. SUMO se refiere a esta página como *access point* (punto de acceso). Este ejemplo sólo tiene una página, *confidential.php*, así que además será el punto de acceso. Para utilizar la página de la consola de SUMO como el punto de acceso, debería abrir el menú de la consola *Console*, hacer doble clic en *Access Points* y presionar *Add*. En el formulario que se muestra en la Figura 7, se introduce un nombre para el punto de acceso; el nombre se mostrará en la página de inicio de sesión de su propia aplicación web más adelante. La página que se desea proteger se encuentra en el mismo servidor que SUMO; de modo que habrá que dejar el parámetro *Node* como *Local Node* (véase el cuadro titulado “Uno para Todos”). La ruta a *confidential.php* es */confidential.php* en este ejemplo. El acceso a esta página le será permitido a todos los *clientes*; para que esto suceda hay que seleccionar el grupo en *Add Group*. Tras hacer clic en *Save*

cual tiene permiso para acceder.

En el Fondo de la Cuestión

Tras crear el usuario de prueba, es el momento para integrar SUMO con la aplicación Web. Para ello, primero hay que localizar el fichero *sumo.php*, que se encuentra en el directorio *sumo*; en XAMPP, la ruta debería ser */opt/lampp/htdocs/sumo/sumo.php*. El siguiente paso consiste en encontrar el sitio web que SUMO debe proteger. En este

Métodos de Accesos Alternativos

Por defecto, SUMO comprobará si la contraseña del usuario se encuentra en su base de datos cuando un usuario intente conectarse. Si se desea que los usuarios puedan utilizar otros servicios, como una cuenta Google Mail, habrá que añadir esta opción de forma explícita. Para ello hay que hacer doble clic en *Data Sources* en *Console | Network*, y luego pulsar en *Add*. En *Data source name* hay que introducir una descripción (por ejemplo, *Conexión basada en Google Mail*) y escoger el tipo de autenticación requerida en *Password Authentication type* – en este ejemplo sería *Google Mail Accounts*. A continuación hay que rellenar los campos de la parte inferior. SUMO normalmente tiene que acceder en este punto a los datos de una base de datos. Tras presionar *Save*, debe asignarse el nuevo método para el usuario abriendo el perfil del usuario *Console | Users and Groups | Users*; luego, hay que pulsar sobre el usuario y presionar *Edit* y seleccionar la entrada requerida en *Password authentication type*. El usuario sólo tendrá esta única opción para autenticarse; la versión actual de SUMO no le permitirá elegir.

Listado 2: Ejemplo de Fichero *confidential.php*

```
01 <?php
02 require "/opt/lampp/htdocs/sumo/sumo.php";
03 echo "This text is confidential!<br />";
04 echo "<a href='?sumo_action=logout'>Logout</a>";
05 ?>
```



Figura 8: El punto de acceso modificado de la pantalla de registro, Confidential-Login.

para guardar el punto de acceso, se puede cerrar la consola de SUMO pulsando *Exit*. Si no lo hace, seguirá trabajando como el administrador *sumo*, y el administrador siempre tiene acceso a *confidential.php*. Ahora entre en *confidential.php* desde su navegador como un usuario anónimo. La dirección para ello en la instalación XAMPP es <http://localhost/confidential.php>.

SUMO muestra la familiar página de inicio, pero esta vez presenta el nombre del punto de acceso (Figura 8). Inicie la sesión con las credenciales de su usuario de prueba, y debería ser capaz de acceder a la página confidencial (Figura 9). Haga clic en *Logout* para cerrar la sesión del usuario de prueba.

Hágalo Usted Mismo

A los usuarios de foros y redes sociales se les permiten crear sus propias cuentas. Para indicarle a SUMO que permita esto, hay que acceder a la consola e ir a los parámetros globales, *Console | Settings*; pulsar *Edit* para que aparezca el cuadro de diálogo *Accounts*; marcar *User registration* y presionar *Save*. Luego vaya a la lista de puntos de acceso (por medio del menú de la consola) y abra la configuración de su punto de acceso. que será *confidential-Login*, si ha ido

siguiendo los pasos de este ejemplo. Presione *Edit* para activar los cambios y marque *Enable registration* en la zona *Security Options*. Tras guardar los cambios, la pantalla de inicio de sesión poseerá dos opciones nuevas: *User registration* y *Unregister user*, que los usuarios pueden utilizar para crear cuentas nuevas o borrar las existentes.

Sistemas Individuales

SUMO pasa los datos del inicio de sesión del usuario a la aplicación PHP por medio del array `$SUMO['user']`; el nombre de usuario se almacena en `$SUMO['user']['user']`, por ejemplo. La función `sumo_verify`

`_permissions($level, $group, $user)` se asegura de que el usuario de la cadena `$user` posee el nivel de seguridad `$level`, y es miembro del grupo `$group`. Si es así, la función devolverá un valor de *true*. También se pueden dejar en blanco algunos parámetros. Las instrucciones de esta construcción *if* sólo se ejecutan si el usuario posee el nivel de acceso 5 y es miembro del grupo *clientes*:

```
if (sumo_verify_permissions(2
5, "customers"))
{
/* ... */
}
```

El directorio *examples* de SUMO proporciona algunos ejemplos simples y otros

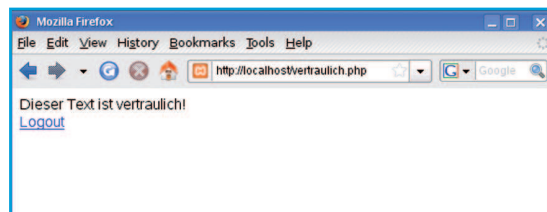


Figura 9: Intento de acceso con éxito a l.confidential.php.

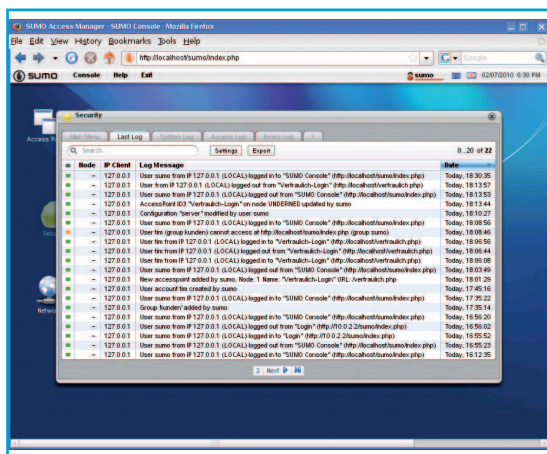


Figura 10: SUMO informa de cada detalle en sus ficheros de registro..

más prácticos. Por medio de los ejemplos, los usuarios pueden suplir la carencia de documentación de SUMO. Si desea personalizar la apariencia de la ventana de inicio de sesión, el directorio *themes* será un buen punto de partida.

Una vez que los usuarios comiencen a trabajar con su aplicación web, puede acceder a la consola de SUMO. En *Console | Security*, haga doble clic en *Security* para encontrar los ficheros de registro (Figura 10). Si pulsa *Export*, podrá descargarlos en formato Excel o CSV. En *Console | Sessions* se muestra la actividad actual.

Conclusiones

SUMO le permite instalar un módulo de gestión de usuarios basado en PHP en una pequeña aplicación web. Sin embargo, el modelo de nivel de acceso muestra rápidamente sus limitaciones a la hora de utilizarlo en proyectos más complejos. Los siete niveles por defecto no son suficientes si se desea un sistema de gestión más granular.

Uno para Todos

Como diferentes aplicaciones web que confían en SUMO para la gestión del acceso pueden usar la misma base de datos, los usuarios pueden mantener las mismas credenciales para acceder, por poner un ejemplo, a una tienda, a un foro y a un sitio web de una empresa con sede en Internet. La red de SUMO puede ser gestionada y mantenida desde cualquier servidor que ejecute SUMO. Si fuera necesario, cada nodo podrá pasar los datos de la sesión de los usuarios al resto de los nodos. Dicho de

otra forma, un cliente sólo tiene que autenticarse una única vez para utilizar cualquiera de los servicios conectados. Desde el punto de vista técnico, el nodo crea un ID de sesión que es único para la red de SUMO y lo almacena en una tabla especial de la base de datos. Para registrar un nodo y anunciarlo al resto de los nodos es preciso ejecutar la consola de SUMO e ir a *Console | Network*; seguidamente, hacer doble clic en *Nodes*, presionar *Add* y rellenar el formulario.

RECURSOS

- [1] Gestor de acceso SUMO: <http://sumoam.sourceforge.net>
- [2] XAMPP: <http://www.xampp.org>