Reutilización de software

para la construcción de aplicaciones en el componente de seguridad, autenticación y administración de usuarios en la Universidad Mariana

Franklin Eduardo Jiménez Giraldo
Robinson Andrés Jiménez Toledo
Docentes del Programa de Ingeniería de Sistemas
Universidad Mariana

Jamilton Fernando Meneses Hernández
Julián Rodríguez Valenzuela
Estudiante del Programa de Ingeniería de Sistemas
Universidad Mariana

Fuente: pixabay.

Hoy en día la mayoría de la información personal o de una empresa tiene mucho valor y es necesario almacenarla en un lugar seguro y confiable, debido a que el manejo de esta puede establecer la diferencia entre el éxito y el fracaso; en muchas ocasiones la información de las empresas es manipulada o tratada por sistemas de información o aplicativos software, los cuales son confiables y seguros pero no en su totalidad. Como lo expresa Ramírez (2014), la mayoría de empresas tienen presencia en internet y esto las hace más vulnerables, porque con el avance de la tecnología también surgen nuevas formas y nuevas técnicas para vulnerar sistemas de seguridad; para Team (2008) la seguridad informática no tiene una definición única, puesto que abarca diferentes áreas con respecto a los sistemas informáticos, estas áreas van desde la protección física de uno o varios ordenadores, hasta la protección de la información que está manejada por redes que lo comunican con el exterior. Sin embargo en el entorno web, la seguridad es un elemento resultante del equilibrio conseguido entre el riesgo y las medidas establecidas para mitigarlas, con el objetivo de mantener la integridad de los datos, ya que pueden corresponder a números de tarjeta de crédito, datos de cuentas bancarias, o en otros casos, información personal como fecha de nacimiento, datos de inicio de sesión, claves, contraseñas privadas, registros médicos, códigos fuente, secretos comerciales, entre otros, que no pueden caer en manos inadecuadas porque pueden provocar daños irreparables en algunos casos.

El tema “seguridad” es muy complejo y en el aspecto de aplicativos software, es muy difícil lograr un sistema seguro; en algunos casos el desarrollar el módulo de seguridad puede ser más complejo que la funcionalidad del mismo, y la no existencia de un módulo de seguridad reutilizable con buenas técnicas y prácticas en seguridad puede llevar a los estudiantes de noveno y décimo semestre de Ingeniería de Sistemas de la Universidad Mariana a desarrollar aplicaciones poco seguras.

Al realizar el proceso de caracterización, tomando como muestra a los estudiantes de grados superiores de la Universidad Mariana de Ingeniería de Sistemas sobre el módulo de seguridad, se puede determinar cuáles son las tareas que realizan y los errores más comunes que cometen en el desarrollo de este módulo, adicional a esto, también se puede evidenciar por qué el módulo de seguridad toma tiempo y cuáles son las prácticas más comunes utilizadas

en su desarrollo; lo que se pretende, es disminuir el tiempo que toman los estudiantes en desarrollar una aplicación por completo, por ello, la finalidad de esta investigación es desarrollar un módulo de seguridad que sirva de referente a los estudiantes que requieran servicios de seguridad y administración de usuarios en el desarrollo de proyectos de grado, logrando así que los estudiantes desarrollen aplicativos con buenas medidas y prácticas en seguridad, para brindar confianza y que los usuarios tengan la certeza que sus datos están protegidos y siendo manejados de una forma segura. Al finalizar del módulo de seguridad, autenticación y administración de usuarios, se instruirá a los estudiantes sobre el proceso que se debe realizar para integrar dicho módulo a sus trabajos de investigación, para luego evaluar el aporte logrado tras su implementación.

El objetivo general de este proyecto es aportar en la reutilización de software para la construcción de aplicaciones, en el componente de autenticación y administración de usuarios en la Universidad Mariana de San Juan de Pasto, para reducir el tiempo que los estudiantes de la Universidad Mariana emplean en el desarrollo de sus aplicaciones. Para lograr este objetivo, lo primero que se debe hacer es una encuesta dirigida a estudiantes de noveno y décimo semestre de Ingeniería de Sistemas, para caracterizar los procedimientos que realizan desde el inicio hasta el final, y cuánto tiempo tardan en conseguirlo; posteriormente, se pretende realizar una investigación a fondo sobre las técnicas empleadas en los módulos de seguridad existentes, para luego crear el módulo de seguridad y administración de usuarios con base en las técnicas encontradas.

Algunas de las prácticas que se pretenden implementar dentro del módulo de seguridad que pretende aportar en el componente de seguridad, autenticación y administración de usuarios en la Universidad Mariana son:

1. **Ingreso de Sesión Básico**

De acuerdo a lo anterior, el sistema de autenticación básico es aquel que consiste en realizar al usuario una prueba de conocimiento, la cual no es más que un usuario y una contraseña que puede ser asignada o personalizada a gusto del usuario; la contraseña debe ser compleja y difícil de descifrar. Quintero (2010), afirma que una contraseña debe tener algunas características como: contener 14 caracteres o más, mínimo ocho caracteres, no debe tener el nombre de usuario, el nombre real o el nombre de la empresa, no debe tener una palabra completa, debe ser diferente de las contraseñas anteriores, debe incluir caracteres especiales como: (- *? ! @ # $ / () {} = . , ; :). Y no debe tener espacios en blanco. Además de estas características, Quintero (2010) también dice que es indispensable tener en cuenta las siguientes recomendaciones:

- Cambiar las contraseñas por defecto.
- Cambiar su contraseña con regularidad.
- Evitar utilizar únicamente letras.
- Incluir números o símbolos.
- No enviar contraseña por correo electrónico.
- No escribir contraseñas en equipos que no controla.
- No guardar la contraseña en un medio virtual.
- No revelar a nadie.
- No se debe incluir secuencias ni caracteres repetidos.
- No utilizar nombres.
- Si se necesita escribir la contraseña en papel, se debe mantener en un lugar seguro.

2. **Administración de Usuarios, Roles y Permisos**

Hernández (1993) define al usuario como el personaje principal en el mundo de la informática, porque gracias a él, hay un inicio y un final en la transferencia y manejo de información, lo cual permitirá generar, desechar y modificar contenidos o documentos dentro de un sistema; otro aspecto importante que se debe tener dentro de un sistema de información son los roles. Para Juaquin (2012), un rol es el conjunto de actividades que están relacionadas a un usuario, un usuario puede tener uno o varios roles y un rol puede ser asignado a varias personas. Los roles tienen que estar definidos claramente y deben ser conocidos por todos.

Según FreeBSD (1999) en su página oficial, un permiso se utiliza para decidir quién puede realizar acciones un recurso, algunos ejemplos sobre este término son el ver, editar, eliminar, modificar de un documento o archivo dentro de un sistema informático.

Con referencia a la organización de personal y la asignación de roles, debe llevar generalmente cuatro pasos:

1. Definición de puestos.
2. Determinación de la sensibilidad del puesto.
3. Elección de personal para cada puesto.
4. Entrenamiento inicial y continuo del empleado.

Para conocer el proceso de gestión de usuarios y roles, se ha tomado de base el proceso que realiza Drupal para ello, ya que la administración de usuarios roles y permisos de un sistema de información, es similar a la de un Framework como este, Saorín (2009) define a Drupal como un gestor de contenidos web que brinda funcionalidades para la edición, almacenamiento y publicación de información, utilizando páginas web como interfaz. En Drupal los roles se pueden gestionar (crear, destruir o modificar) en “Administrar> Gestión de usuarios>Roles”. Pardo (2013) indica que para gestionar los permisos asociados a cada Rol se debe ir a “Administrar> Gestión de usuarios >Permisos”. Luego para especificar qué tareas se permitirán a cada usuario, bastará con asignar un Rol a cada uno de ellos.

Cuando se hace la modificación de un rol o de un permiso en algún sistema de información o Framework, el usuario deberá ver reflejados estos cambios en las opciones actuales de su menú, ya que para IBM (2006) los permisos son acciones dentro de un sistema y algunas de esas acciones son las de añadir, modificar, asignar, probar y suprimir, dicho de otra manera, estos permisos indican las tareas permitidas por el rol de un usuario.

Con el desarrollo de roles se podría decir que estos ayudan a la creación de un menú dinámico, entendiendo que para Blackboard (2004), los roles se definen para restringir que los usuarios que no tienen relación con algunas funciones de un sistema, causen errores o alteraciones dentro de él; en la gran mayoría de sistemas de información los usuarios se dividen en dos grupos fundamentalmente. Maldonado (2015) afirma que el primer grupo está diseñado para los gerentes y altos ejecutivos que son los usuarios que pueden controlar y monitorear que todos los procesos dentro de un sistema de información o aplicación web se

estén realizando correctamente y sin ninguna anomalía, mientras que el segundo grupo es para los operarios que son los encargados de distribuir y manipular la información crítica del sistema. En todo sistema se debe mantener estos dos grupos, ya que pueden ser de mucha ayuda a la hora de realizar una toma de decisiones.

Con un gestor de roles, permisos y usuarios se limitará las acciones de cada uno de los usuarios, para evitar que estos accedan a opciones dentro del sistema que no les corresponden y provoquen daños dentro del mismo.

3.**Recuperar contraseña**

Cuando un sistema auténtica a sus usuarios por medio de un usuario y una contraseña, es muy común que los usuarios olviden el texto asignado para su contraseña, cuando un usuario olvida la contraseña de algún sistema lo primero que debe hacer es recuperarla; para el proceso de recuperación existen varios métodos que pueden ser automáticos, o que requieran de una tercera persona. Los métodos automáticos son aquellos que al realizar el proceso, no necesitan la aprobación de un tercero para realizar su recuperación y, por otro lado, están los que sí necesitan la aprobación del administrador o la persona encargada del sistema.

En la interfaz gráfica, la opción de recuperación de contraseña, en la mayoría de casos, se encuentra cerca al inicio de sesión; Facil (2011) muestra que la opción "Recuperar Contraseña" llevará al usuario a un formulario aparte, donde se debe ingresar el nombre de usuario o el E-mail con el cual se encuentre registrado ese usuario, esto depende del gusto y de la facilidad del mismo; el formulario debe contar con un Captcha para verificar que el cambio de contraseña que se está realizando por una persona y no por una aplicación o programa malicioso.

Cuando los datos del formulario de recuperación de contraseña son completados y enviados, tanto el usuario como el administrador del sistema recibirán una notificación de que se está efectuando el cambio de contraseña, en el caso de que el sistema haga este procedimiento automático; Ventanilla (2011) dice que el usuario deberá ingresar al correo con el cual fue registrado en el sistema y revisar en su bandeja de entrada el correo de confirmación enviado por el sistema, este correo debe contener un texto informativo acerca de lo que se está haciendo y lo que sucederá al completar el proceso. Adicionalmente, el correo mostrará un Token de confirmación, el cual no será más que un link que solo funcionará durante cierto tiempo y una sola vez, para evitar que se vuelva a realizar el cambio de contraseña con el mismo Token; el Token lleva al usuario a un nuevo formulario con dos campos donde él debe ingresar la nueva contraseña, esta contraseña también deberá cumplir con los requisitos que se le pidió cuando se creó la contraseña por primera vez, cuando el usuario confirma el cambio de contraseña, el sistema deberá comprobar que el texto introducido en los dos campos coincidan para evitar que el usuario se equivoque al ingresar su nueva contraseña en alguno de estos campos, luego de que el sistema haya verificado que todo esté bien, se le informará al usuario que el cambio ha sido exitoso

4. **Cajas de Texto**

Las cajas de texto para Martínez (2002), son etiquetas y herramientas que brinda HTML para el desarrollo de páginas y plataformas virtuales, es tal vez una de las más indispensables y utilizadas en la programación, ya que esta herramienta está diseñada para la interacción entre el usuario y un aplicativo web. Esto debido a que usualmente, el sistema toma la información almacenada en cada una de estas etiquetas para realizar algún tipo de acción internamente, estas acciones pueden variar desde el ingreso de sesión hasta la realización de un pago o una compra en línea. Esta etiqueta se distingue por tener tres tipos de uso en función de la longitud y de la seguridad que necesite emplearse:

Cuadro de texto

- Tipo numérico.
- Tipo contenido.
- Tipo obligatorio.
- Sin carácter.

Cuadro de contraseña

- Tipo escritura.

Área de texto

- Tipo semántica.

5. **Subir archivos.**

En muchos sistemas de información o páginas web existe la posibilidad de subir archivos en determinadas opciones del sistema, estos archivos pueden ser documentos, imágenes, PDF, archivos comprimidos, entre otros. La UNAM (2013) nos dice que estos archivos se almacenan generalmente en el servidor en una carpeta temporal, para luego ser almacenado en una carpeta permanente y ser leído en memoria; en el traspaso hay que ser claros y precisos al ingresar el parámetro que referencie al nombre del archivo y la ruta de acceso, ya que pueden ser truqueadas para que apunten a archivos de configuración del sistema como /etc/passwd en sistemas Unix.

Cuando un sistema tiene la opción para adjuntar archivos se debe limitar las extensiones de los archivos que se van a subir, por ejemplo, en el caso de una galería de imágenes, que los archivos sean de tipo png, jpg, jpeg o gif y si es el caso de un archivo plano que su extensión sea .doc, docx, pdf, txt, entre otros. Existe la posibilidad de que un ataque se realice cambiando la extensión de un archivo malicioso a conveniencia, al respecto, wikibooks (2015) afirma que se puede cambiar la extensión de un archivo manualmente desde el sistema operativo Windows. Un ejemplo de esto puede ser que un archivo ejecutable se le haya cámbialo la extensión y tenga una de tipo png o docx para poder subirla a un dominio o servidor. Para evitar este sipo de casos, los archivos que se pretenden subir deben pasar por un análisis de extensión, lo que hace es informar de la extensión original de un archivo, así haya sido cambiada; existe un método para lograr la transformación de cualquier archivo en números, que serán distintos dependiendo de la extensión que haya tenido originalmente, con lo cual se evitará que los usuarios adjunten archivos maliciosos al servidor.

6. **Registro de actividades**

Un registro de actividades es un registro de los procesos que se hacen en un determinado tiempo, para Pinales (2007) un registro de actividades es un fichero de texto, al que se le añaden líneas de manera automática a medida que se realizan acciones dentro del sistema. En todo sistema de información o aplicación web es recomendable que este tipo de registro se implementen como medidas de seguridad para poder llevar un control sobre las

mismas, el registro de actividades se ejecuta inmediatamente un usuario se autentique y este dentro del sistema; en algunos framework se tiene la posibilidad de instalar plugins para realizar el monitoreo y registro de las actividades de los usuarios. Optimbyte (2015) muestra las actividades que comúnmente se deberían llevar a en un registro de actividades de un framework o, en este caso, un sistema de seguridad aplicación software.

- Hora de Ingreso y cierre de sesión.
- Inserción, actualización, eliminación de registros o archivos.
- Salidas de sistema como impresiones, envíos por correo, entre otros.
- Modificaciones del perfil.
- Cambios de contraseña.

Al integrar el registro de actividades en un sistema basado en usuarios, se puede minimizar el riesgo de presentar ataques internos, ya que se pueden hacer llamados de atención si se llega a notar comportamientos fuera de lo común por parte de algún usuario.

7. **Copias de seguridad**

Realizar copias de seguridad es una de las medidas más importantes que hay que tener en cuenta a la hora de proteger información. Apolonio (2015) recomienda tener una buena copia de seguridad para restaurar los datos en caso que haya eliminación accidental de archivos, fallas en el disco duro, robo o extravío de dispositivos, o infección por malware.

Cuando se realiza una copia de seguridad hay que definir qué se va a incluir y que no, para ello, hay que realizar un previo análisis de la información para luego seleccionar la más frágil y de más importancia para realizar la copia de seguridad sobre esos archivos; en seguida, se puede escoger a conveniencia el lapso de tiempo entre copia y copia de seguridad, puede variar entre horas, días, semanas y meses, pero lo más recomendable es que se realicen en un periodo de tiempo corto, ya que si sucede algún imprevisto la pérdida de información sería menos.

Por su parte Cole (2013) da a conocer las dos maneras más comunes para almacenar las copias de seguridad, la primera es empleando medios físicos como DVD, memorias USB o discos duros externos, la segunda forma de almacenamiento es en la nube (en alguna parte de Internet). Si se utiliza cualquiera de estos métodos se debe tener en cuenta que las copias de seguridad no deben estar en el mismo lugar donde se encuentren los archivos originales.

Referencias

Apolonio, J. (2015). ¿Aún vale la pena comprar computadores con Windows 7 para la empresa?. Recuperado de http://www.apolodata.cl/blog/?cat=3&paged=2

Blackboard. (2004). Administración de usuarios. Recuperado de https://es-es.help.blackboard.com/Learn/9.1_2014_04/Administrator/060_Application_Management_and_Support/User_Management

Borghello, C. (2002). Seguridad Lógica - Administración de Seguridad. Recuperado de http://www.segu-info.com.ar/logica/administracion.htm

Cole, E. (2013). Copias de seguridad y recuperación personal. Recuperado de https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201309_sp.pdf

Facil, B. (2011). Recuperar la contraseña de Twitter. Recuperado de https://basicoyfacil.wordpress.com/2011/11/27/recuperar-la-contrasena-de-twitter/

FreeBSD. (1999). Manual de FreeBSD. Recuperado de https://www.freebsd.org/doc/es/books/handbook/index.html

Hernández, P. (1993). Hablemos de Biometría. Recuperado de https://s3.amazonaws.com/umanick.public.docs/es/umanick_cuaderno01_introduccionbiometria.pdf

IBM Knowledge Center. (2006). Roles & permissions. Recuperado de http://www.ibm.com/support/knowledgecenter/STFS69_3.3.0/ts7740_ua_roles_permissions.html?lang=es

Juaquin, J. (2012). Administración de los recursos y función informática. Recuperado de http://es.slideshare.net/cotorrito/roles-y-funciones-12849484

Maldonado, G. (2015). Análisis y diseño de Sistemas. Recuperado de http://analistasdsistemas.blogspot.com.co/2015_05_01_archive.html

Martínez, Á. (2002). MANUAL PRÁCTICO DE HTML. Recuperado de http://bioinf.ibun.unal.edu.co/servicios/electiva/man-htlm/HTML.pdf

Optimbyte. (2015). Monitorear la actividad de los usuarios en wordpress. Recuperado de http://www.optimbyte.com/actividad-de-los-usuarios-en-wordpress/

Pardo, M. (2013). CMS - Gestores de Contenidos. Recuperado de http://cmsgestoresuned.blogspot.com.co/2013/06/mas-terredes-sociales-y-aprendizaje.html

Pinales, M. (2007). LOGS. Recuperado de http://www.ur.mx/Default.aspx?tabid=3804&language=en-US

Quintero, J. (2010). Recomendaciones de uso de contraseñas seguras. Recuperado de http://secorreo.impsat.net.co/documentos/RecomendacionesUsoContrasenas.pdf

Saorín, T. (2009). Guía básica de gestión de contenidos web con Drupal: instalación, configuración y extensión. Recuperado de https://digitum.um.es/xmlui/bitstream/10201/3300/6/digitum_2009_guiabasicaDrupal.pdf

Team, H. (2008). SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN. Recuperado de http://tecno.unsl.edu.ar/redes%202008/seguridadinformatica.pdf

UNAM-CERT. (2013). Aspectos Básicos de la Seguridad en Aplicaciones Web. Recuperado de http://www.seguridad.unam.mx/descarga.dsc?arch=2430

Ventanilla, U. (2011). RECUPERACIÓN DE CONTRASEÑA PARA SERVICIOS WEB. Recuperado de https://www.ventanillaunica.gob.mx/cs/groups/public/documents/contenidovu/mdaw/mdex/~edisp/vucem012981.pdf

wikibooks. (2015). Recuperado de https://es.wikibooks.org/wiki/Aprende_de_Windows/Cambia_las_extensiones_de_los_archivos