HACKNOW

Documento técnico de seguridad - ASS

Escuela de Procedencia: Universidad Politécnica Metropolitana de Hidalgo (UPMH)

Equipo: PRO08

Integrantes:

Madelin Flores García
Sandra González Reyes
Aranza Meneses Juarez
Karla Ocaña Garrido
Miguel Angel Pacheco Granillo

Pachuca, Hidalgo a 24 de Abril del 2021

Índice:

Implementación de acciones contra inyección SQL.

1. Validar las palabras que son ingresadas por los usuarios dependiendo del campo.
2. Restricciones al ingresar contraseñas para identificarse (Uso de letras mayúsculas, minúsculas y de caracteres especificados en este caso: *, ?, !, ¿, ¡) para prevenir que ingresen signos que podrían generar algún ataque.

Utilización de protocolos de comunicación seguros.

Al ser una aplicación que será utilizada en la red local de la empresa no ocupará protocolos de internet por lo que los que se utilizaran son protocolos de red que son los siguientes:

1. Protocolos de capa 1 (Física): Aquí entran las restricciones de hardware que es utilizado en la red y su calidad aparte de como fue diseñado.
2. Protocolos de capa 2 (Enlace de datos): Involucra la manera en que se contactaran los dispositivos para enviar la información.
3. Protocolos de capa 3 (Red): Involucra la manera y el espacio que conforma la red y los protocolos a seguir para configurarla.
4. Protocolos de capa 4 (Transporte):Son los protocolos que hablan de la manera en que se hará el envío y si la forma en que se protege la información.

Aseguramiento de la BD por medio de contraseñas.

Para el acceso a la base de datos se asigna una contraseña a la base y al usuario:

1. Se crearán usuarios específicos que podrán acceder a la base de datos y se colocarán contraseñas de un tamaño de mínimo 16 caracteres para asegurar un mayor grado de seguridad.
    a. La contraseña deberá de incluir caracteres especiales, no podrá incluir el nombre de la base de datos y se podrán ingresar caracteres especiales.
2. Se asignan contraseñas especiales para cada usuario que va acceder desde la aplicación, mismas que al ser transportadas se cifraran para proteger los datos.
    a. Las contraseñas se sugiere sean cambiadas de manera periódica o constante, se sugiere no seguir un patrón, además de no usar contraseñas ya utilizadas.
    b. Las contraseñas deben incluir letras mayúsculas y minúsculas, además deben de incluir algunos caracteres especificados en el manual técnico.
3. Se restringen los permisos a los usuarios que pueden acceder a la base de datos para la modificación de la estructura y de los procedimientos.

Manera en que las claves se cifran en la BD.

1. Se cifran las contraseñas con md5

Manera en que los campos de entrada son validados.

1. Se revisa la combinación de datos que se ingresan.
    a. En el caso de datos numéricos se valida que no se ingresen caracteres y que donde se ingresen tengan valor numérico.
    b. En el caso de las cadenas se evalúan los caracteres que se ingresan y se restringen el ingreso a algunos, en este caso son: (**, . “” ; ¿? ¡! % $ # : -**)
    c. En el caso de fechas se valida según el tipo en el caso de las promesas se restringe a fechas mayores a la que se está en ese momento, además se utiliza un calendario de apoyo para asignarla.

Campos de entrada de información sensible.

1. Credenciales de acceso del login (usuario y contraseña).
2. Ingreso de datos para los seguimientos (selección de la cuenta de deudores)
3. Ingreso de convenios (Selección de la cuenta de deudores , asignación de fechas y montos).

Perfiles de usuarios.

1. Gestores: cuentan con restricciones solo para ingresar seguimientos, además de la visualización de información de cuentas y convenios pudiendo modificar solo el campos de estatus y el apartado contactos validados.
2. Administrativos: podrán visualizar toda la información y modificar todos los campos de seguimientos y convenios, sin embargo solo podrán modificar de la tabla principal el campo de gestor, grupo y la celda para marcar un pre-castigo.