Documento Técnico de Seguridad de Sistema de Registro de Cobranzas.

Integrantes:

Mendoza Hernández Dylan Michel

Mohedano Torres Efraín

Vega Parra Marco Antonio

Sábado 24 de Abril del 2021.

a. Implementación de acciones contra inyección SQL

El riesgo más grande de sufrir un ataque por inyección SQL dentro del sistema está en el formulario de modificación de cuentas, el cual tiene campos que puede ser objetivos para vulnerar y para evitar lo anterior se recurre a la función:

htmlspecialchars($inputString);

Esta función toma un valor de entrada y convierte la cadena a valores sin semántica dentro de HTML5 para evitar que se introduzca código malicioso en los campos de entrada

A través de los formularios propuestos en el sistema se optó por utilizar el método de envío POST y no GET por la vulnerabilidad existente en la barra de direccionamiento y el conocimiento innecesario de valores y variables de parte del cliente.

b. Utilización de protocolos de comunicación seguros.

La comunicación del sistema viaja por medio del protocolo HTTP y aunque este es fácilmente vulnerado, el host en el que se encuentra tiene la facilidad de contratar un certificado SSL por lo que se podrá proteger sin dificultad todo el tráfico dentro de su información una vez que se actualice el plan de arrendamiento.

c. Aseguramiento de la BD por medio de contraseñas.

Para acceder al sistema se dispone del uso de credenciales por usuario, se requiere por medio de un formulario inicial la introducción de un nombre de usuario y su correspondiente password. Del lado del servidor se cuenta con un usuario y contraseña personalizadas para poder acceder al gestor, no se tiene ningún usuario por defecto o contraseña en blanco.

d. Manera en que las claves se cifran en la BD.

El método de autenticación requerido es por medio de credenciales, es por ello que es necesario resguardar su integridad y su privacidad en la base de datos.

Es por ello que se utiliza el algoritmo de reducción criptográfico de 128 bits **MD5** por medio de la función dentro de PHP:

```
md5($passwordunsecurity);
```

Lo anterior nos asegura que aunque se pudiesen recuperar o vulnerar las contraseñas de los usuarios, estas se encuentran cifradas.

e. Manera en que los campos de entrada son validados.

El desarrollo del sistema fue basado en capas por lo que validar el tipado e integridad de cada dato esperado es esencial, así que se realizó primeramente una validación de formularios por medio de los atributos de etiquetas de HTML 5 y evitar que se introduzcan valores con otro tipado o campos vacíos no deseados, posteriormente estos valores se vuelven a evaluar una vez llegando al servidor dentro de cada procedimiento almacenado se vuelve a rectificar su tipado y su existencia, si es necesario, dentro de la base de datos, creando una validación dual por parte de tecnologias de cliente y de servidor.

f. Los campos de entrada de información sensible deben estar enmascarados, por lo que se debe indicar cuales son esos campos y como se realizó la máscara.

No se considera la manipulación de información sensible por medio de formularios visibles por lo que el enmascarado hasta el punto de desarrollo actual del sistema es innecesario, el control de la comunicación sensible se realiza por medio de métodos no visibles al usuario.

g. Los perfiles de usuarios deben funcionar perfectamente para no comprometer información (cada usuario solamente debe poder realizar las acciones que tiene permitidas) de lo cual se debe incluir una tabla indicando cuales son dichos perfiles y a lo que tienen acceso

Los dos roles que existen en el sistema son: Administrador y Gestor. Los cuales son controlados por medio de variables de sesión que se setean una vez el usuario consigue autorizar su ingreso.

Rol	Privilegios
Administrador	Es capaz de modificar la siguiente información: ● Grupo/Zona geográfica ● El estado en el que se encuentra el celular del deudor ● El estado en el que se encuentra el contacto del trabajo del deudor ● El estado en el que se encuentra el contacto particular del deudor ● El gestor asignado a cada deudor ● El pre castigo del deudor ● Control y agregación de seguimientos ● Generación de reportes ● Filtrado de información
Gestor	Solo puede modificar los siguientes datos dentro del control de cuentas: ● El estado del contacto del trabajo: ● El estado del contacto particular ● El estado de su alta ● La fecha de alta de deudor ● Generación de reportes ● Filtrado de información