INSTITUTO TECNOLÓGICO SUPERIOR DE CHICONTEPEC

INGENIERÍA EN SISTEMAS COMPUTACIONALES

Producto: Usos de Logueo en php, Inyecciones SQL y Encriptación en MD5.

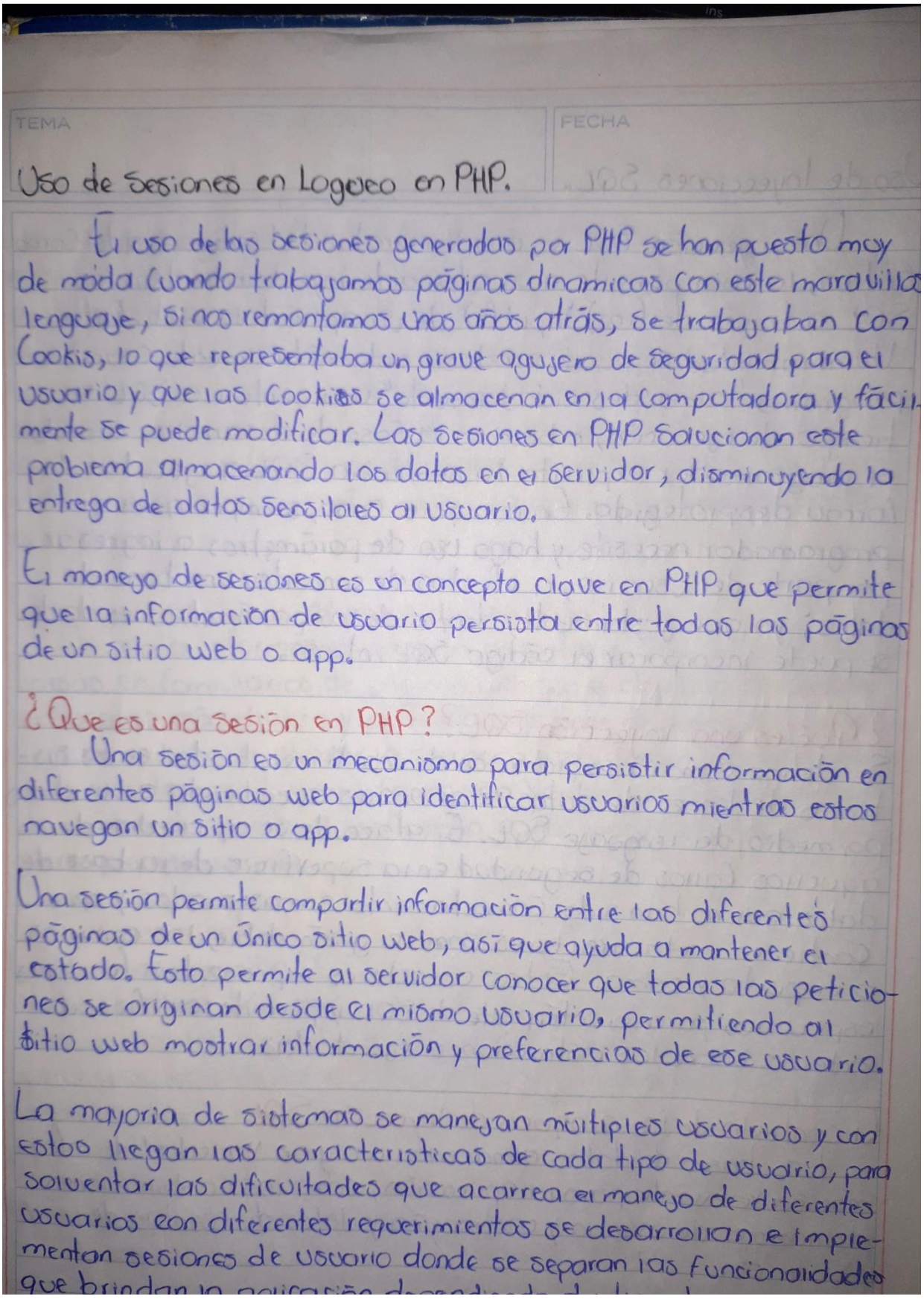
Asignatura: Programación Lógica y Funcional.

Docente: Ing. Efrén Flores Cruz.

Estudiante: Manuel Zúñiga Hernández.

Semestre: Octavo

Chicontepec, Veracruz, a 01 de Mayo 2020.



TEMA

Uso de Sesiones en Logeeo en PHP.

FECHA

El uso de las sesiones generadas por PHP se han puesto muy de moda cuando trabajamos páginas dinamicas con este maravilloso lenguaje, si nos remontamos unos años atrás, se trabajaban con Cookis, lo que representaba un grave agujero de seguridad para el usuario y que las Cookies se almacenan en la computadora y fácilmente se puede modificar. Las Sesiones en PHP solucionan este problema almacenando los datos en el servidor, disminuyendo la entrega de datos sensibles al usuario.

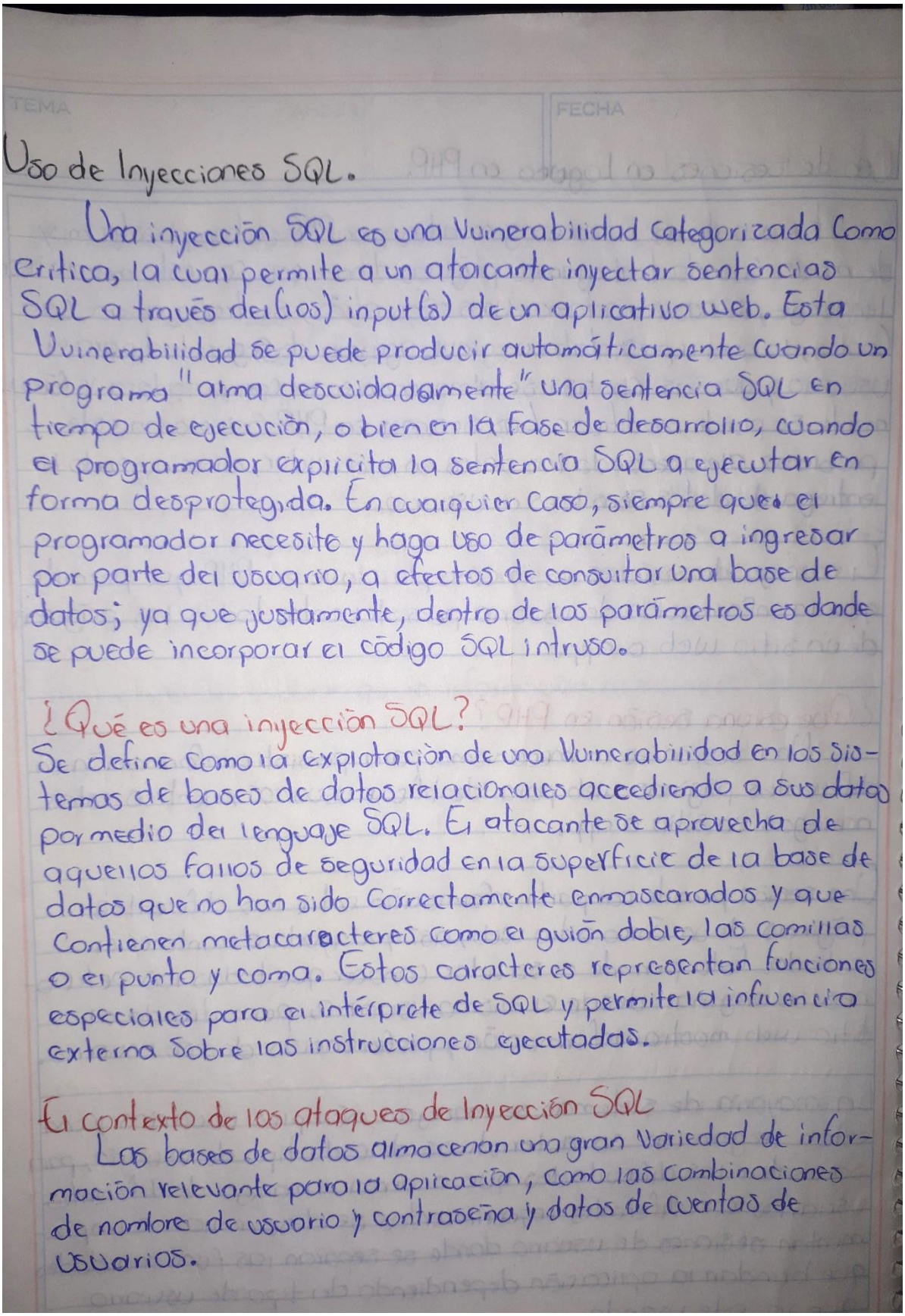
El manejo de sesiones es un concepto clave en PHP que permite que la información de usuario persista entre todas las páginas de un sitio web o app.

¿Que es una Sesión en PHP?

Una sesión es un mecanismo para persistir información en diferentes páginas web para identificar usuarios mientras estos navegan un sitio o app.

Una sesión permite compartir información entre las diferentes páginas de un único sitio web, así que ayuda a mantener el estado. Esto permite al servidor conocer que todas las peticiones se originan desde el mismo usuario, permitiendo al sitio web mostrar información y preferencias de ese usuario.

La mayoria de sistemas se manejan múltiples usuarios y con esto llegan las caracteristicas de cada tipo de usuario, para solventar las dificultades que acarrea el manejo de diferentes usuarios con diferentes requerimientos se desarrollan e implementan sesiones de usuario donde se separan las funcionalidades que brindan la aplicación dependiendo de [illegible]



TEMA

FECHA

Uso de Inyecciones SQL.

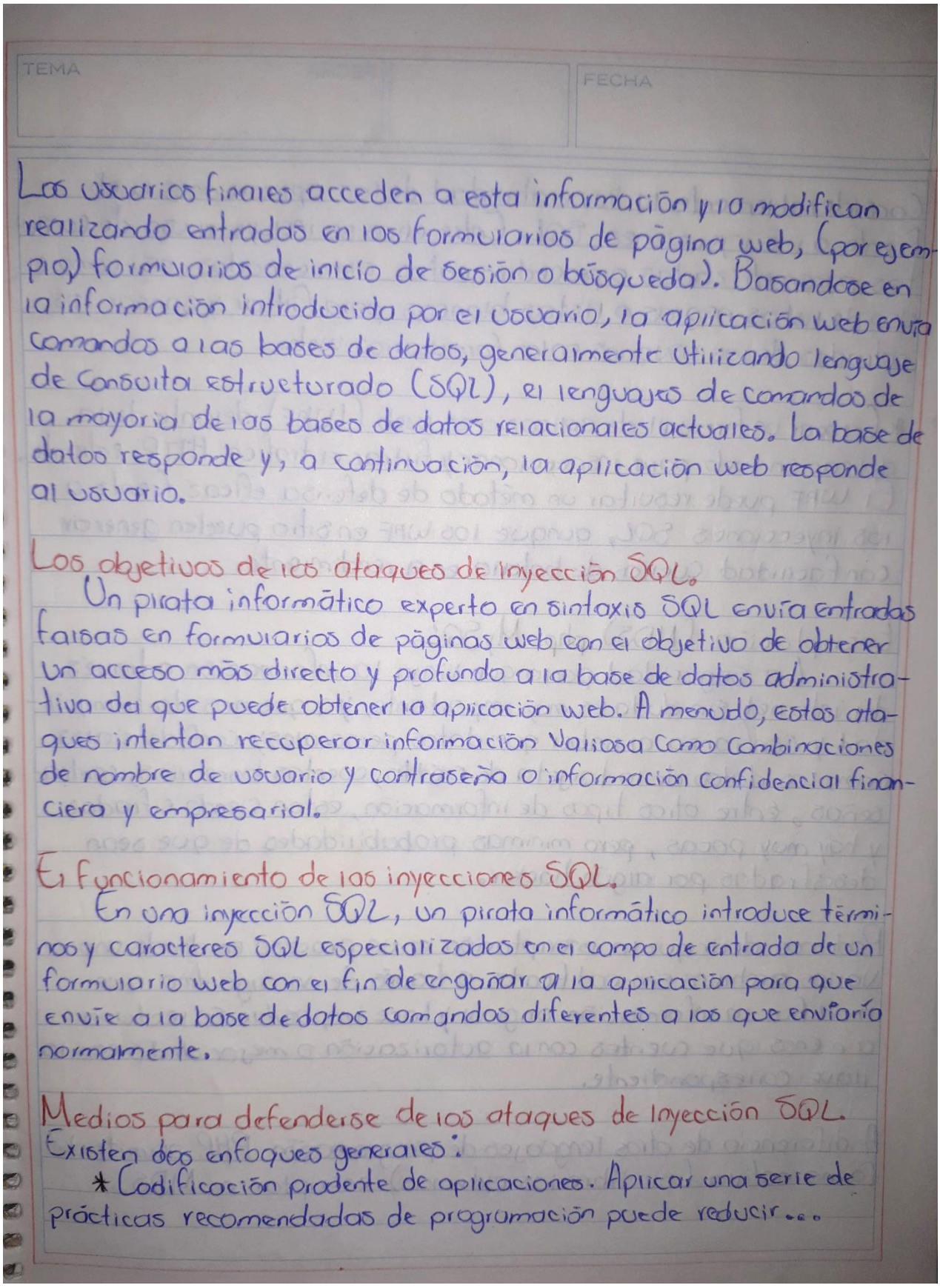
Una inyección SQL es una Vulnerabilidad categorizada como crítica, la cual permite a un atacante inyectar sentencias SQL a través del(los) input(s) de un aplicativo web. Esta Vulnerabilidad se puede producir automáticamente cuando un programa "alma descuidadamente" una sentencia SQL en tiempo de ejecución, o bien en la fase de desarrollo, cuando el programador explicita la sentencia SQL a ejecutar en forma desprotegida. En cualquier caso, siempre que el programador necesite y haga uso de parámetros a ingresar por parte del usuario, a efectos de consultar una base de datos; ya que justamente, dentro de los parámetros es donde se puede incorporar el código SQL intruso.

¿Qué es una inyección SQL?

Se define como la explotación de una Vulnerabilidad en los sistemas de bases de datos relacionales accediendo a sus datos por medio del lenguaje SQL. El atacante se aprovecha de aquellos fallos de seguridad en la superficie de la base de datos que no han sido correctamente enmascarados y que contienen metacaracteres como el guión doble, las comillas o el punto y coma. Estos caracteres representan funciones especiales para el intérprete de SQL y permite la influencia externa sobre las instrucciones ejecutadas.

El contexto de los ataques de Inyección SQL

Las bases de datos almacenan una gran variedad de información relevante para la aplicación, como las combinaciones de nombre de usuario y contraseña y datos de cuentas de usuarios.



TEMA

FECHA

Los usuarios finales acceden a esta información y la modifican realizando entradas en los formularios de página web, (por ejemplo) formularios de inicio de sesión o búsqueda). Basandose en la información introducida por el usuario, la aplicación web envía comandos a las bases de datos, generalmente utilizando lenguaje de consulta estructurado (SQL), el lenguajes de comandos de la mayoria de las bases de datos relacionales actuales. La base de datos responde y, a continuación, la aplicación web responde al usuario.

Los objetivos de los ataques de inyección SQL.

Un pirata informático experto en sintaxis SQL envía entradas falsas en formularios de páginas web con el objetivo de obtener un acceso más directo y profundo a la base de datos administrativa de que puede obtener la aplicación web. A menudo, estos ataques intentan recuperar información valiosa como combinaciones de nombre de usuario y contraseña o información confidencial financiera y empresarial.

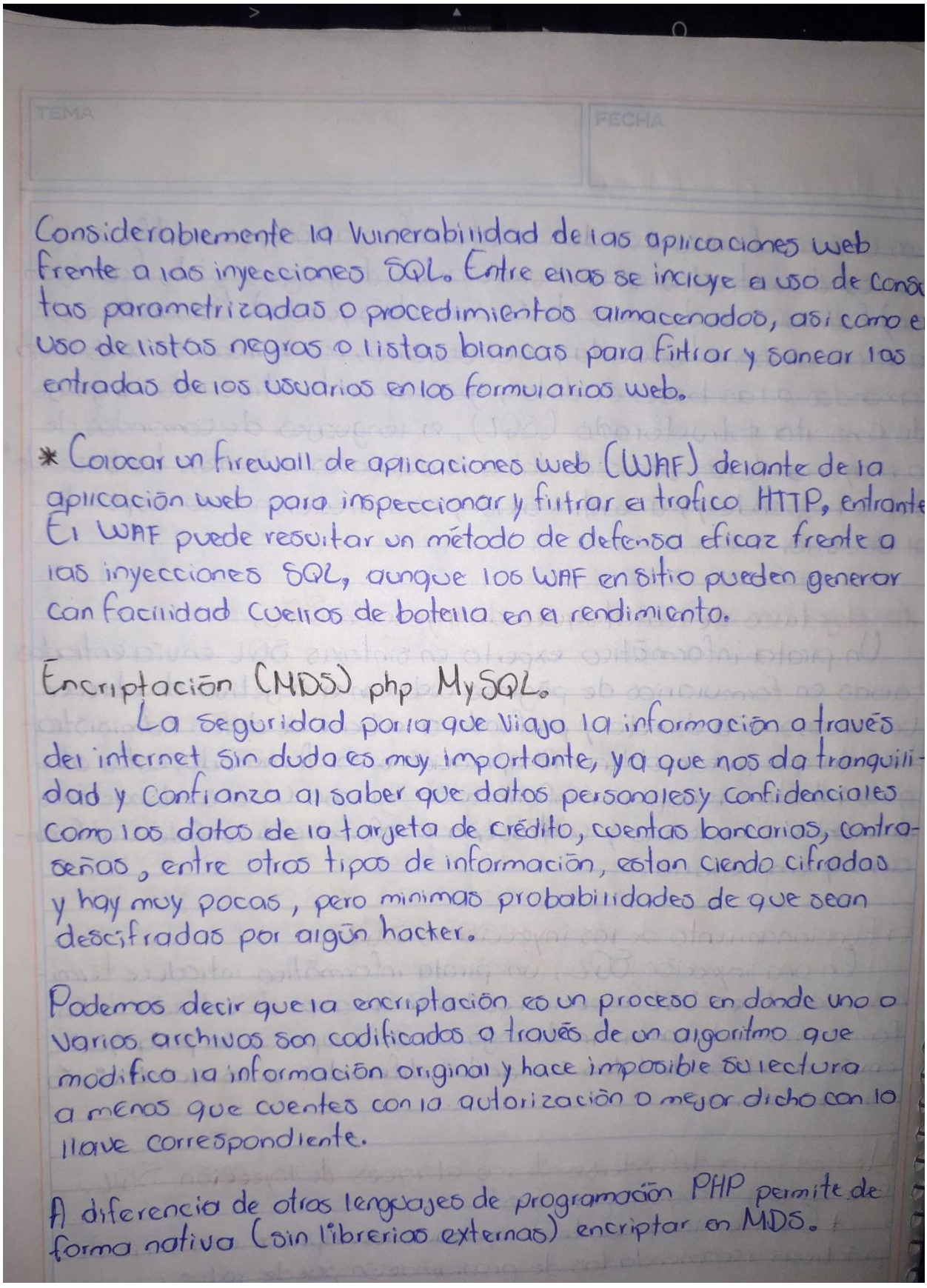
El funcionamiento de las inyecciones SQL.

En una inyección SQL, un pirata informático introduce términos y caracteres SQL especializados en el campo de entrada de un formulario web con el fin de engañar a la aplicación para que envíe a la base de datos comandos diferentes a los que enviaría normalmente.

Medios para defenderse de los ataques de inyección SQL.

Existen dos enfoques generales:

* Codificación prodente de aplicaciones. Aplicar una serie de prácticas recomendadas de programación puede reducir...



TEMA

FECHA

Considerablemente la vulnerabilidad de las aplicaciones web frente a las inyecciones SQL. Entre ellas se incluye el uso de consultas parametrizadas o procedimientos almacenados, así como el uso de listas negras o listas blancas para filtrar y sanear las entradas de los usuarios en los formularios web.

* Colocar un firewall de aplicaciones web (WAF) delante de la aplicación web para inspeccionar y filtrar el trafico HTTP, entrante. El WAF puede resultar un método de defensa eficaz frente a las inyecciones SQL, aunque los WAF en sitio pueden generar con facilidad cuellos de botella en el rendimiento.

Encriptación (MD5) php MySQL.

La seguridad para que viaja la información a través del internet sin duda es muy importante, ya que nos da tranquilidad y confianza al saber que datos personales y confidenciales como los datos de la tarjeta de crédito, cuentas bancarias, contraseñas, entre otros tipos de información, estan siendo cifrados y hay muy pocas, pero minimas probabilidades de que sean descifradas por algún hacker.

Podemos decir que la encriptación es un proceso en donde uno o varios archivos son codificados a través de un algoritmo que modifica la información original y hace imposible su lectura a menos que cuentes con la autorización o mejor dicho con la llave correspondiente.

A diferencia de otros lenguajes de programación PHP permite de forma nativa (sin librerias externas) encriptar en MD5.