Instituto Tecnológico Superior de Chicontepec

Ingeniería en Sistemas Computacionales

Nombre:

Camelia Bautista Hernández

Docente:

Ing. Efrén Flores Cruz

Asignatura:

Programación Web

Investigación:

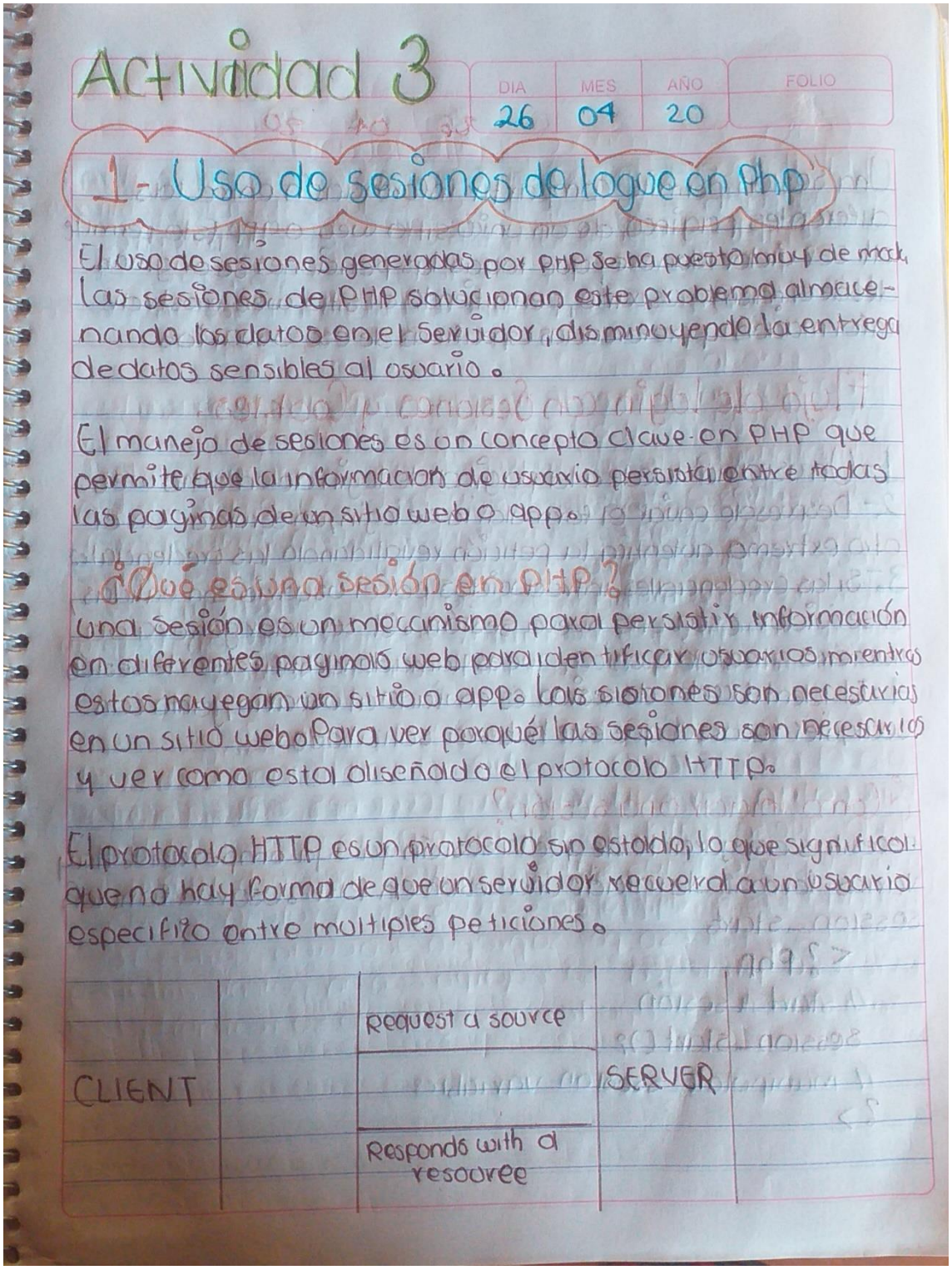
Uso de sesiones de logueo en php.

Uso de inyecciones SQL.

Encriptación (MD5) PHP Y MySQL

Fecha de entrega

27 de Abril del 2020



Actividad 3

DIA	MES	AÑO	FOLIO
26	04	20	

1- Uso de sesiones de logue en Php

El uso de sesiones generadas por PHP se ha puesto muy de mod, las sesiones de PHP solucionan este problema almacenando los datos en el servidor, disminuyendo la entrega de datos sensibles al usuario.

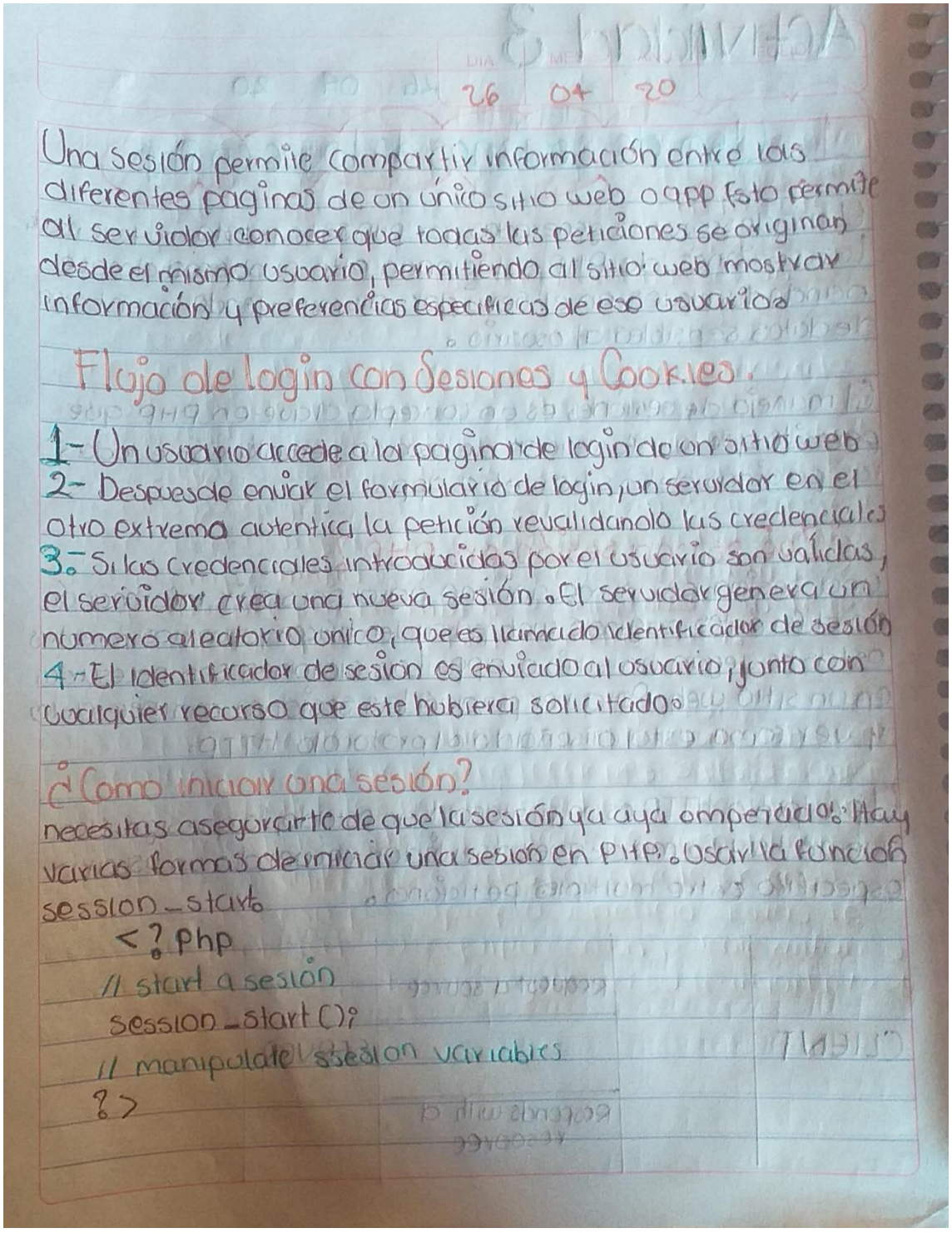
El manejo de sesiones es un concepto clave en PHP que permite que la información de usuario persista entre todas las páginas de un sitio web o app.

¿Qué 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. Las sesiones son necesarias en un sitio web. Para ver porqué las sesiones son necesarios y ver como está diseñado el protocolo HTTP.

El protocolo HTTP es un protocolo sin estado, lo que significa que no hay forma de que un servidor recuerde a un usuario especifico entre multiples peticiones.

CLIENT	Request a source	SERVER
	Responds with a resource	



26 04 20

Una sesión permite compartir información entre las diferentes paginas de un único sitio web o app Esto permite al servidor conocer que todas las peticiones se originan desde el mismo usuario, permitiendo al sitio web mostrar información y preferencias especificas de ese usuario.

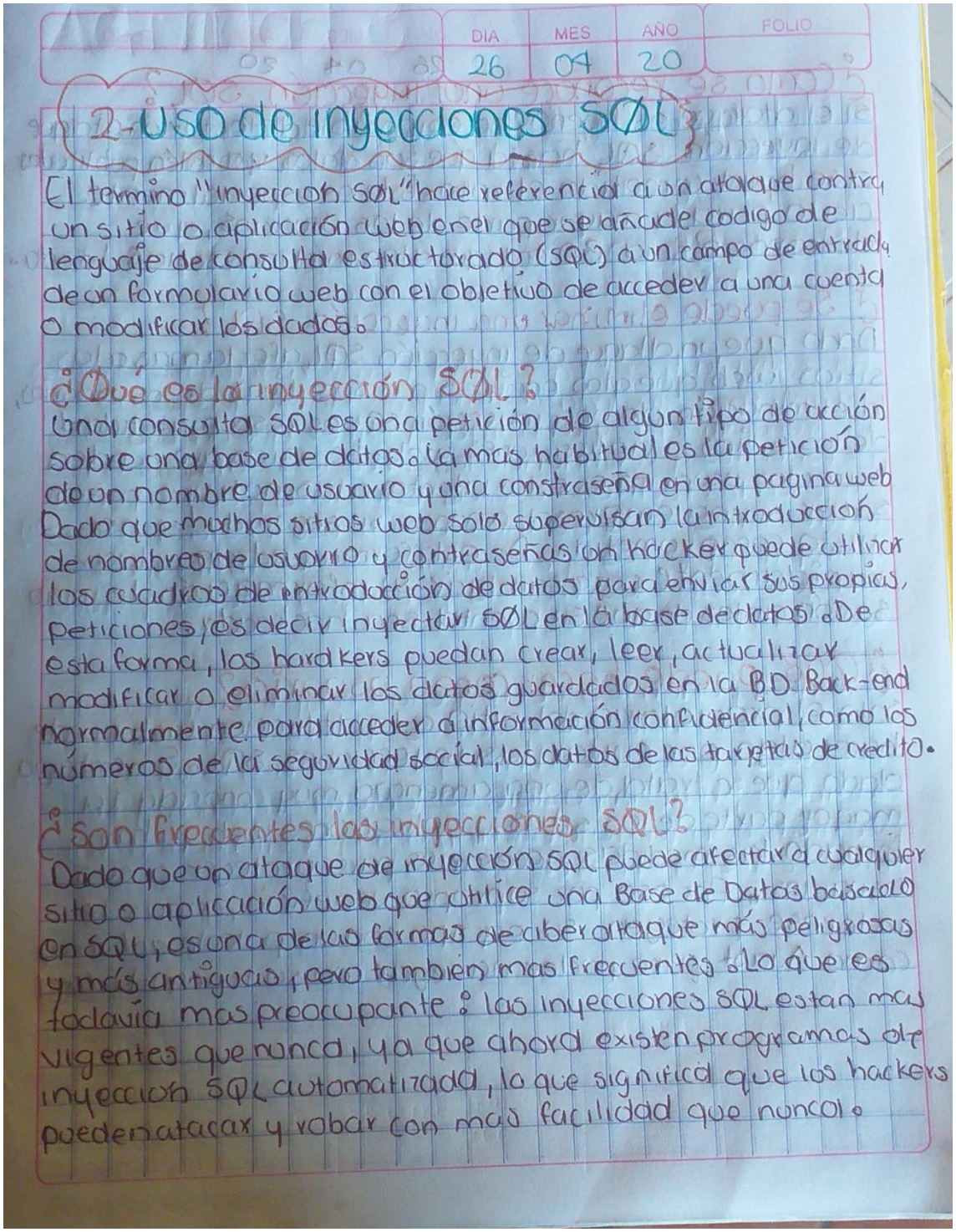
Flujo de login con Sesiones y Cookies.

1- Un usuario accede a la pagina de login de un sitio web
2- Despues de enviar el formulario de login, un servidor en el otro extremo autentica la petición revalidando las credenciales
3- Si las credenciales introducidas por el usuario son validas, el servidor crea una nueva sesión. El servidor genera un numero aleatorio unico, que es llamado identificador de sesión
4- El identificador de sesión es enviado al usuario, junto con cualquier recurso que este hubiera solicitado.

¿Como iniciar una sesión?

necesitas asegurarte de que la sesión ya aya emperado. Hay varias formas de iniciar una sesión en PHP. Usar la función session_start

```
<? php
// start a sesión
session_start ();
// manipulate session variables
?>
```



DIA 26 MES 04 AÑO 20 FOLIO

2-Uso de inyecciones SQL

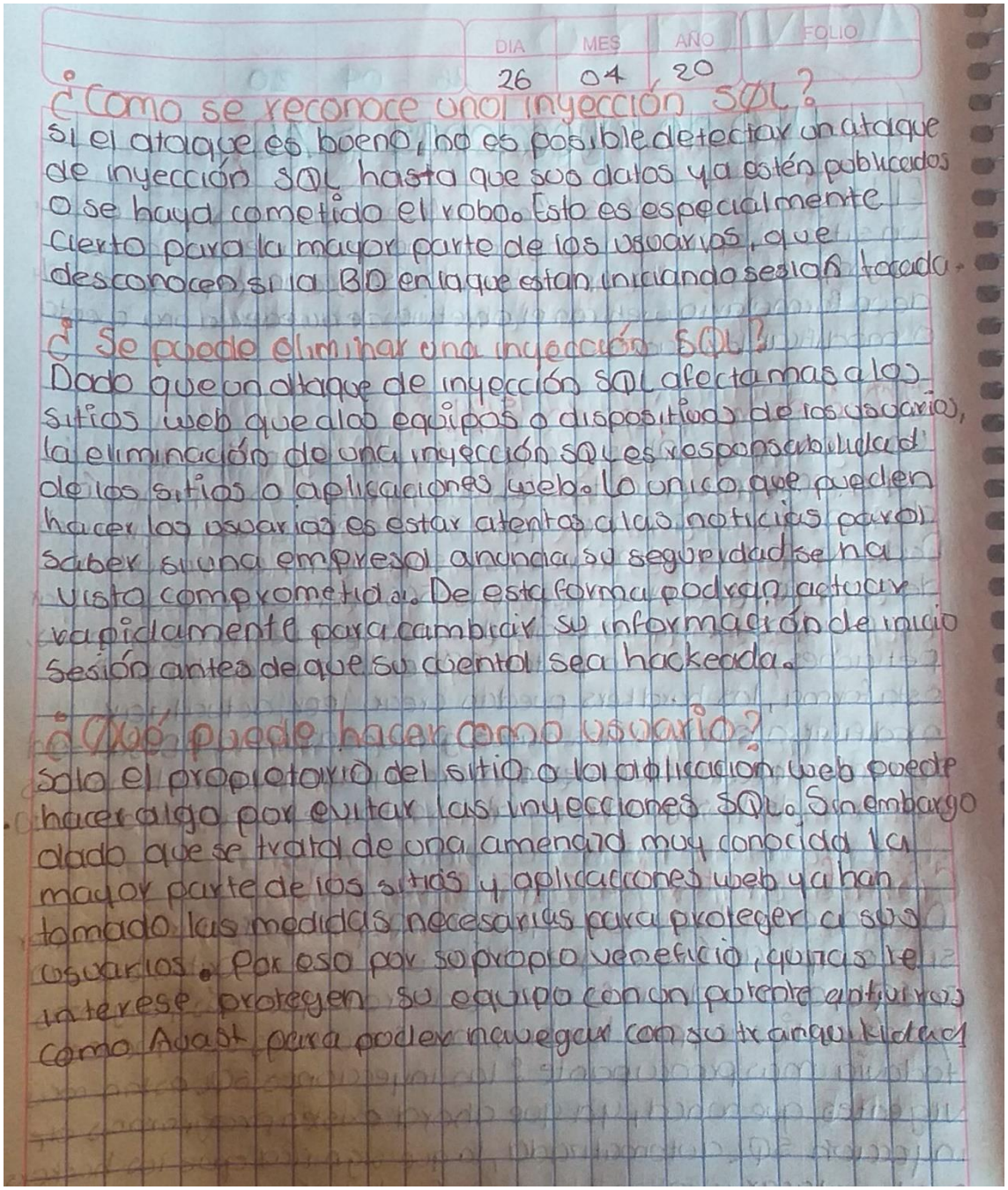
El termino "inyección SQL" hace referencia a un ataque contra un sitio o aplicación web en el que se añade codigo de lenguaje de consulta estructurado (SQL) a un campo de entrada de un formulario web con el objetivo de acceder a una cuenta o modificar los datos.

¿Qué es la inyección SQL?

Una consulta SQL es una petición de algun tipo de acción sobre una base de datos. La mas habitual es la petición de un nombre de usuario y una constraseña en una pagina web Dado que muchos sitios web solo supervisan la introduccion de nombres de usuario y contraseñas un hacker puede utilizar los cuadros de introducción de datos para enviar sus propias, peticiones, es decir inyectar SQL en la base de datos. De esta forma, los hardkers puedan crear, leer, actualizar modificar o eliminar los datos guardados en la BD. Back-end normalmente para acceder a información confidencial, como los números de la seguridad social, los datos de las tarjetas de credito.

¿Son frecuentes las inyecciones SQL?

Dado que un ataque de inyección SQL puede afectar a cualquier sitio o aplicación web que utilice una Base de Datos basada en SQL, es una de las formas de aber ataque más peligrosas y más antiguas, pero tambien mas frecuentes. Lo que es todavia mas preocupante: las inyecciones SQL estan mas vigentes que nunca, ya que ahora existen programas de inyección SQL automatizada, lo que significa que los hackers pueden atacar y robar con mas facilidad que nunca.



DIA 26 MES 04 AÑO 20 FOLIO

¿Como se reconoce una inyección SQL?

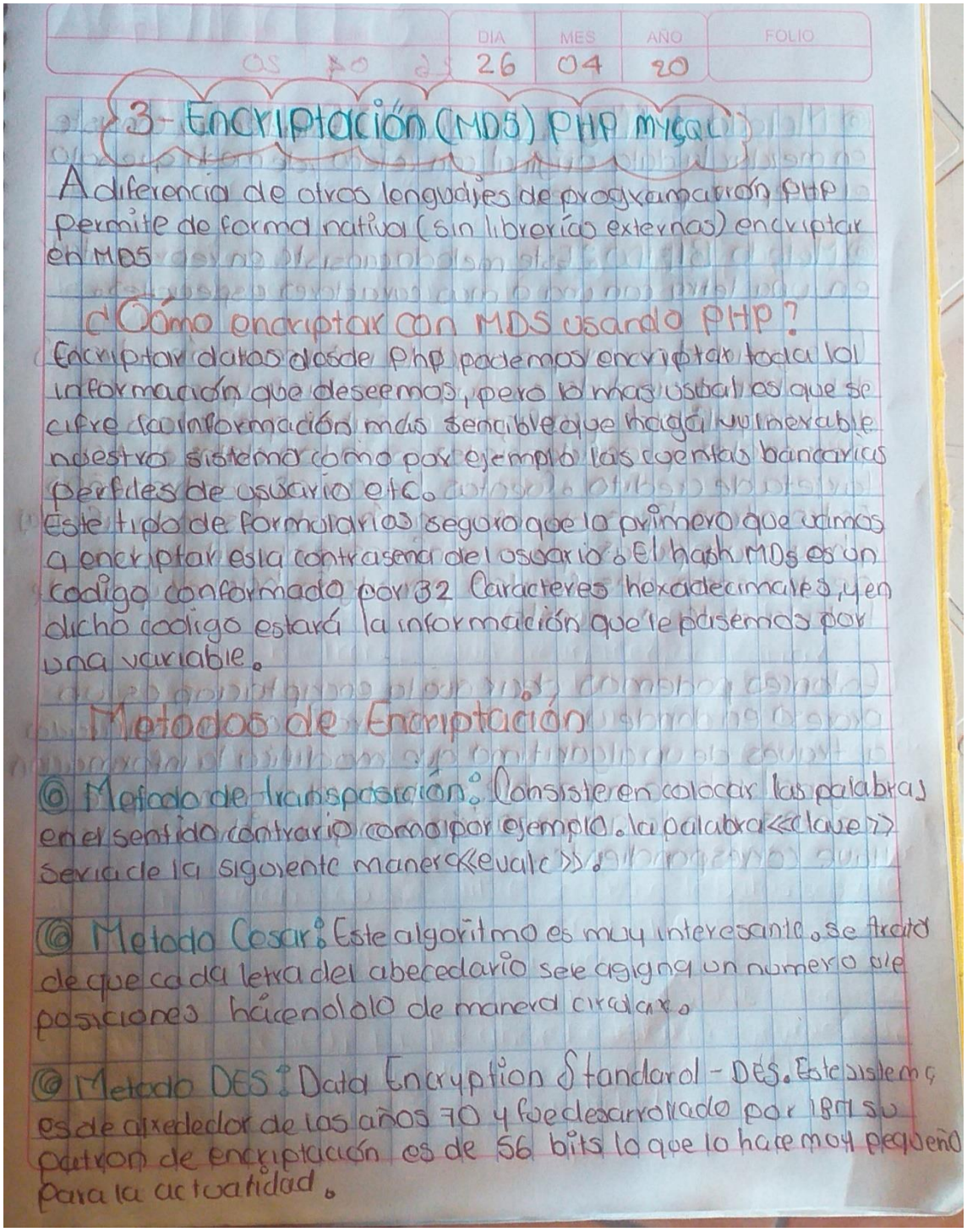
Si el ataque es bueno, no es posible detectar un ataque de inyección SQL hasta que sus datos ya estén publicados o se haya cometido el robo. Esto es especialmente cierto para la mayor parte de los usuarios, que desconocen si la BD en la que están iniciando sesión fue hackeada.

¿Se puede eliminar una inyección SQL?

Dado que un ataque de inyección SQL afecta más a los sitios web que a los equipos o dispositivos de los usuarios, la eliminación de una inyección SQL es responsabilidad de los sitios o aplicaciones web. Lo único que pueden hacer los usuarios es estar atentos a las noticias para saber si una empresa anuncia su seguridad se ha visto comprometida. De esta forma podrán actuar rápidamente para cambiar su información de inicio sesión antes de que su cuenta sea hackeada.

¿Qué puede hacer como usuario?

Solo el propietario del sitio o la aplicación web puede hacer algo por evitar las inyecciones SQL. Sin embargo dado que se trata de una amenaza muy conocida la mayor parte de los sitios y aplicaciones web ya han tomado las medidas necesarias para proteger a sus usuarios. Por eso por su propio beneficio, quizás le interese protegen su equipo con un potente antivirus como Avast para poder navegar con su tranquilidad



DIA 26 MES 04 AÑO 20 FOLIO

3- Encriptación (MD5) PHP MySQL

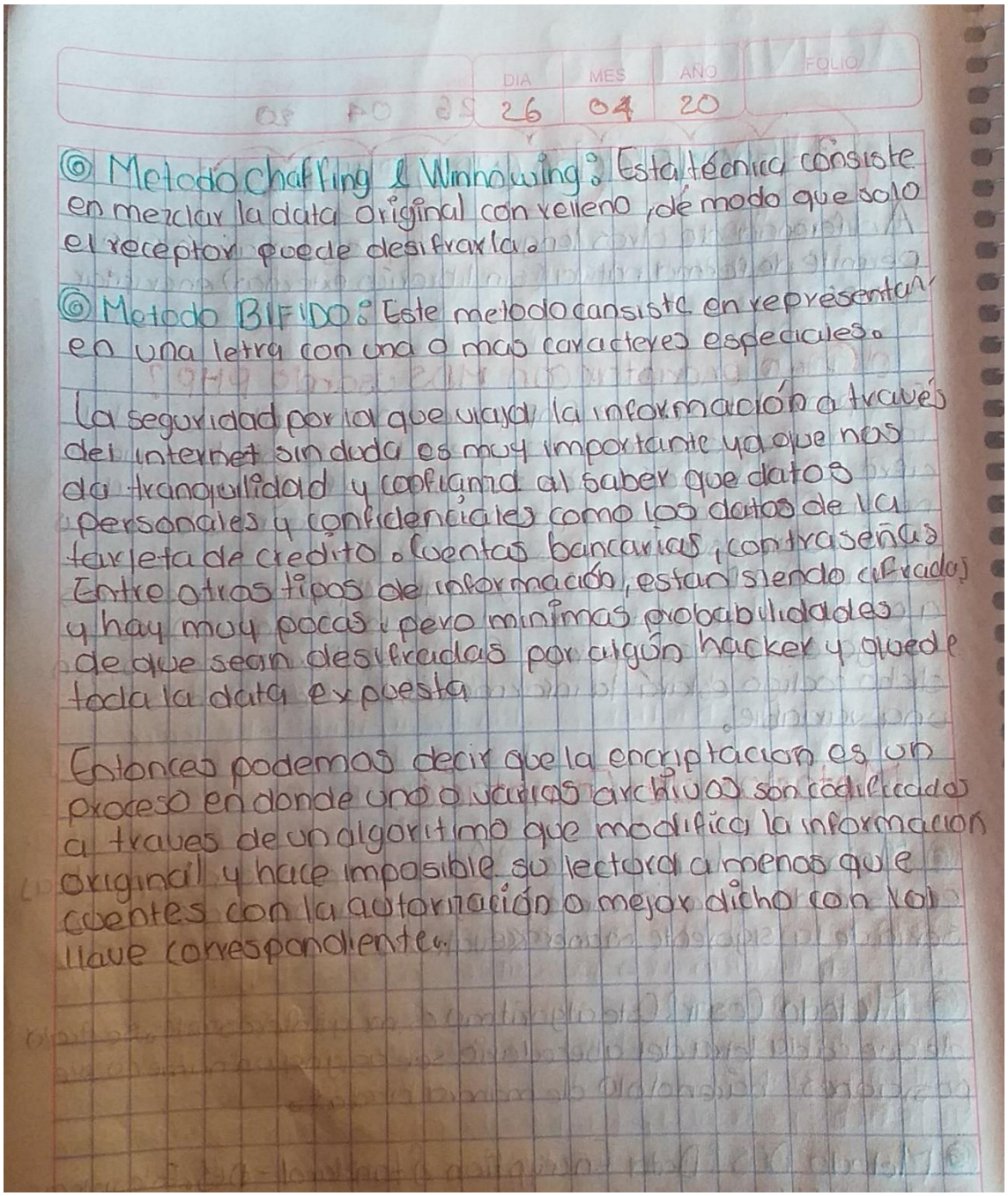
A diferencia de otros lenguajes de programación PHP permite de forma nativa (sin librerías externas) encriptar en MD5

¿Cómo encriptar con MD5 usando PHP?

Encriptar datos desde Php podemos encriptar toda la información que deseemos, pero lo mas usual es que se cifre la información mas sensible que haga vulnerable nuestro sistema como por ejemplo las cuentas bancarias perfiles de usuario etc.
Este tipo de formularios seguro que lo primero que vamos a encriptar es la contraseña del usuario. El hash MD5 es un codigo conformado por 32 caracteres hexadecimales, y en dicho codigo estará la información que le pasemos por una variable.

Metodos de Encriptación

- Metodo de transposición: Consiste en colocar las palabras en el sentido contrario como por ejemplo. la palabra «clave» sería de la siguiente manera «evalc».
- Metodo Cesar: Este algoritmo es muy interesante. se trata de que cada letra del abecedario se le asigna un numero de posiciones hácenlolo de manera circular.
- Metodo DES: Data Encryption Standard - DES. Este sistema es de alrededor de los años 70 y fue desarrollado por IBM su patron de encriptación es de 56 bits lo que lo hace muy pequeño para la actualidad.



DIA 26 MES 04 AÑO 20 FOLIO

- Metodo chaffing & Winnowing: Esta técnica consiste en mezclar la data original con relleno, de modo que solo el receptor puede desifrarla.
- Metodo BIFIDO: Este metodo consiste en representar en una letra con una o mas caracteres especiales.

La seguridad por la 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 credito, cuentas bancarias, contraseñas Entre otros tipos de información, estan siendo cifrados y hay muy pocas pero mínimas probabilidades de que sean desifradas por algún hacker y quede toda la data expuesta

Entonces podemos decir que la encriptacion es un proceso en donde uno o varios archivos son codificados a traves de un algoritmo que modifica la información original y hace imposible su lectora menos que e cuentes con la autorización o mejor dicho con la llave correspondiente.