

UNIVERSIDAD TECNOLÓGICA DE AGUASCALIENTES



ING. EN SISTEMAS Y DESARROLLO DE SOFTWARE

NOMBRE DEL ALUMNO:

OSCAR RENATO GARCÍA RESÉNDIZ

NOMBRE DEL(A) PROFESOR(A): AMÉRICO CUAUHTÉMOC CALZADA
DE LUNA

MATERIA: SEGURIDAD INFORMÁTICA

FECHA DE ENTREGA: 16/03/2021

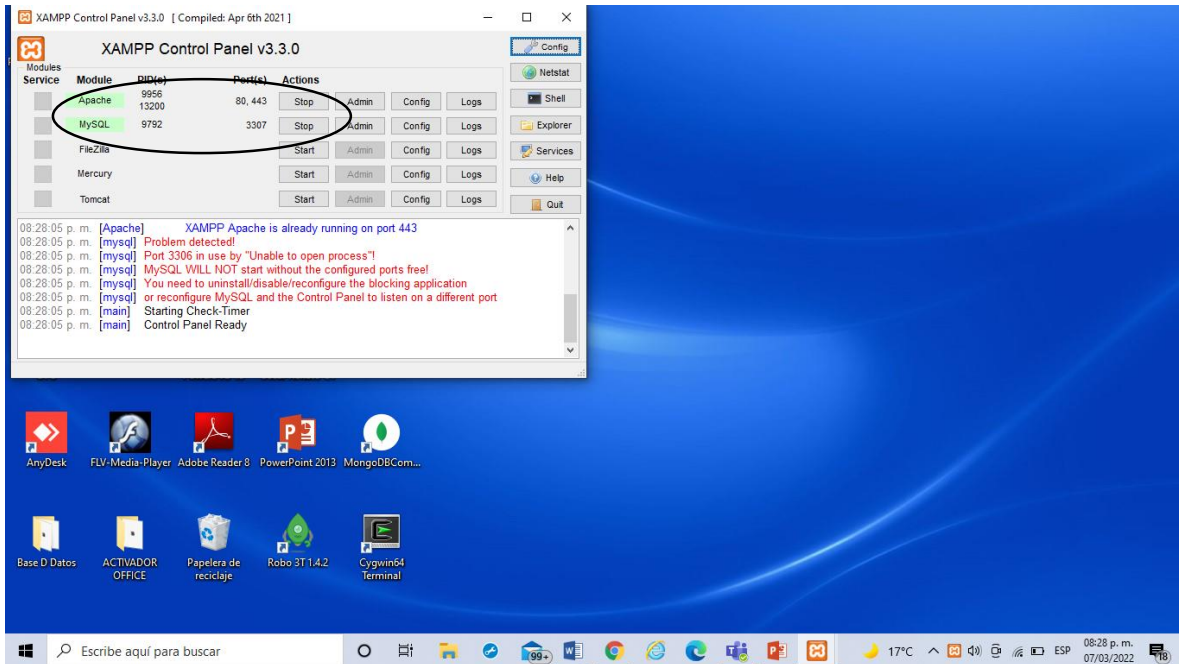
Introducción.

En esta práctica trabajaremos con diversos servicios y adentrándonos un poco a unas prácticas de lenguaje PHP. En estas prácticas usaremos los servicios de XAMPP, especialmente APACHE y MYSQL, estos son los que nos ayudaran a que nuestras prácticas sean muy buenas, en estas mostraremos el uso de algoritmo hash SHA1 y md5, de igual manera trabajaremos el cifrado de datos o contraseñas de una manera muy sencilla y eficaz, durante el desarrollo de esta práctica mostraremos evidencia y pasos a seguir por los cuales desarrollamos nuestra práctica, los pasos a seguir son los siguientes:

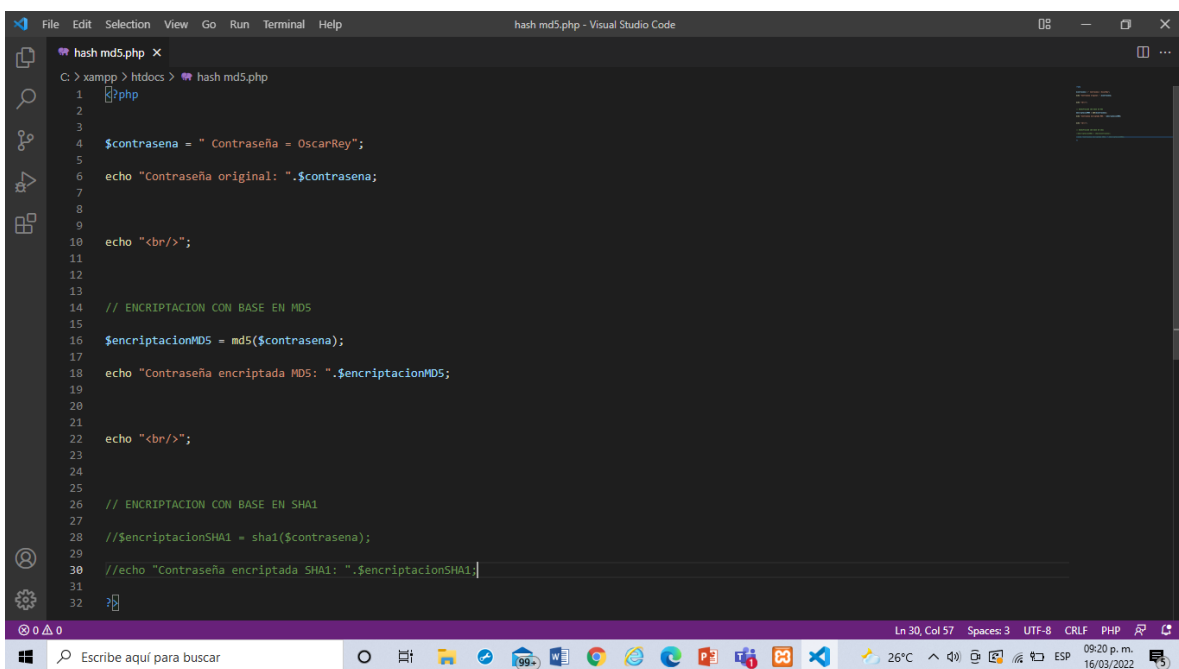
- Utilizar XAMPP , Iniciar servicio de Apache dando permisos en el Firewall de Windows.
- Crear Código que utilice hash SHA
- Crear Código que utilice hash MD5
- Colocar códigos php en C:\xampp\htdocs (DocumentRoot de Apache)

Se debe agregar pantallas de lo anterior explicando la actividad realizada.

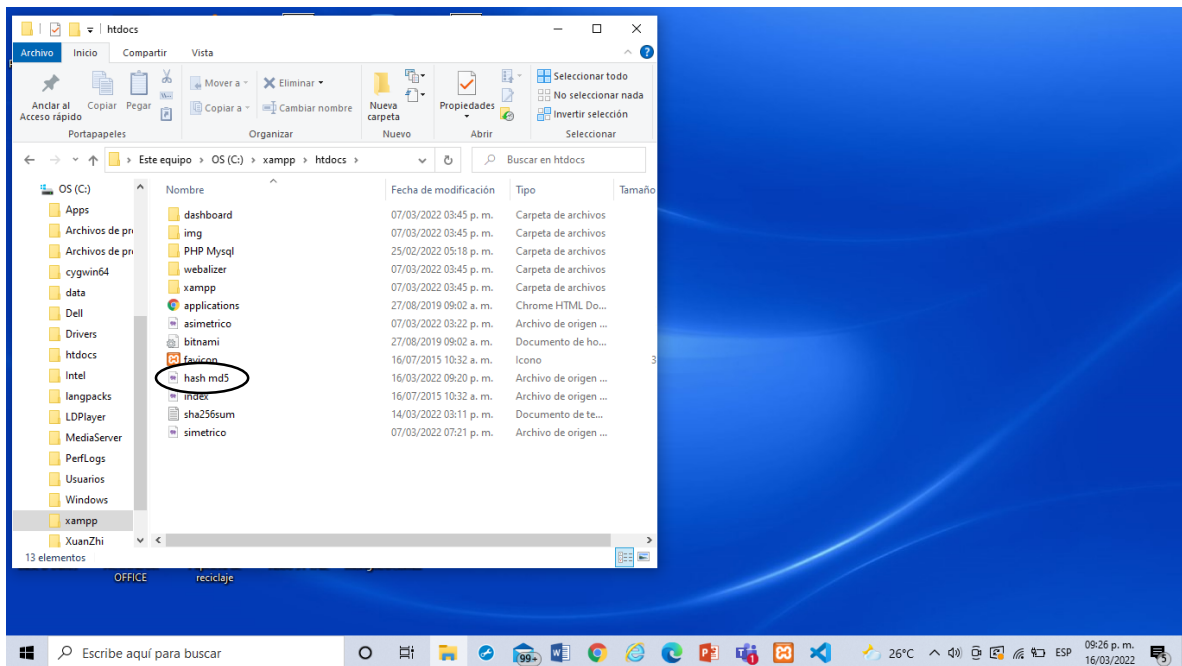
1.- Utilizar XAMPP , Iniciar servicio de Apache dando permisos en el Firewall de Windows.



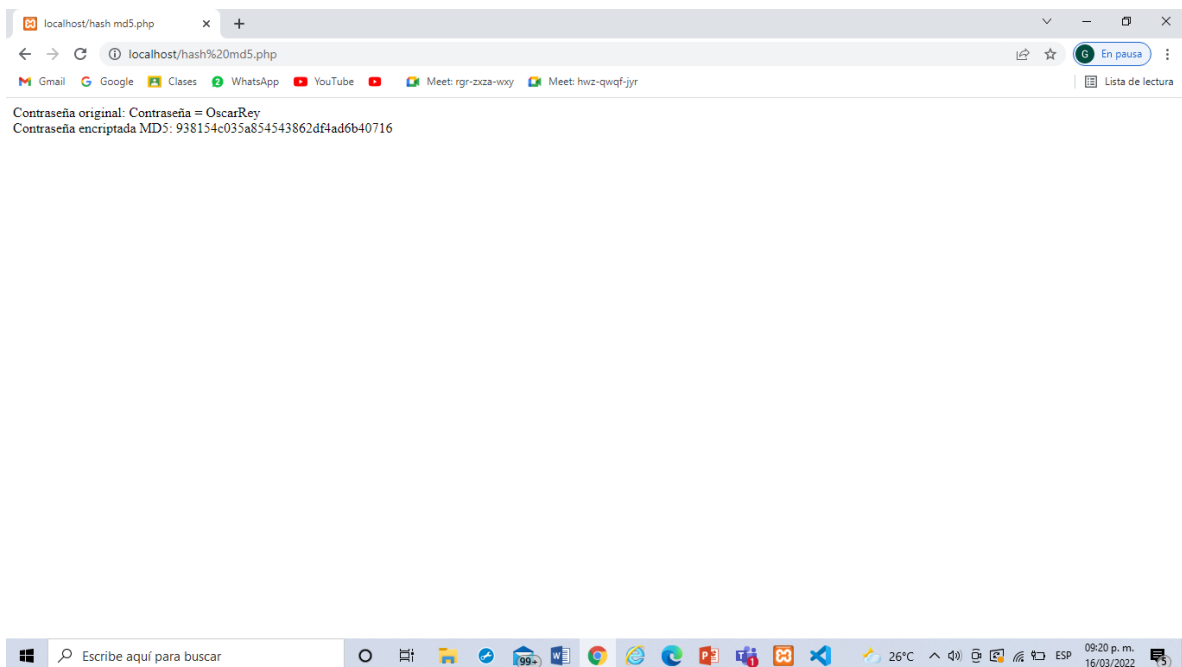
2.- Crear Código que utilice hash md5



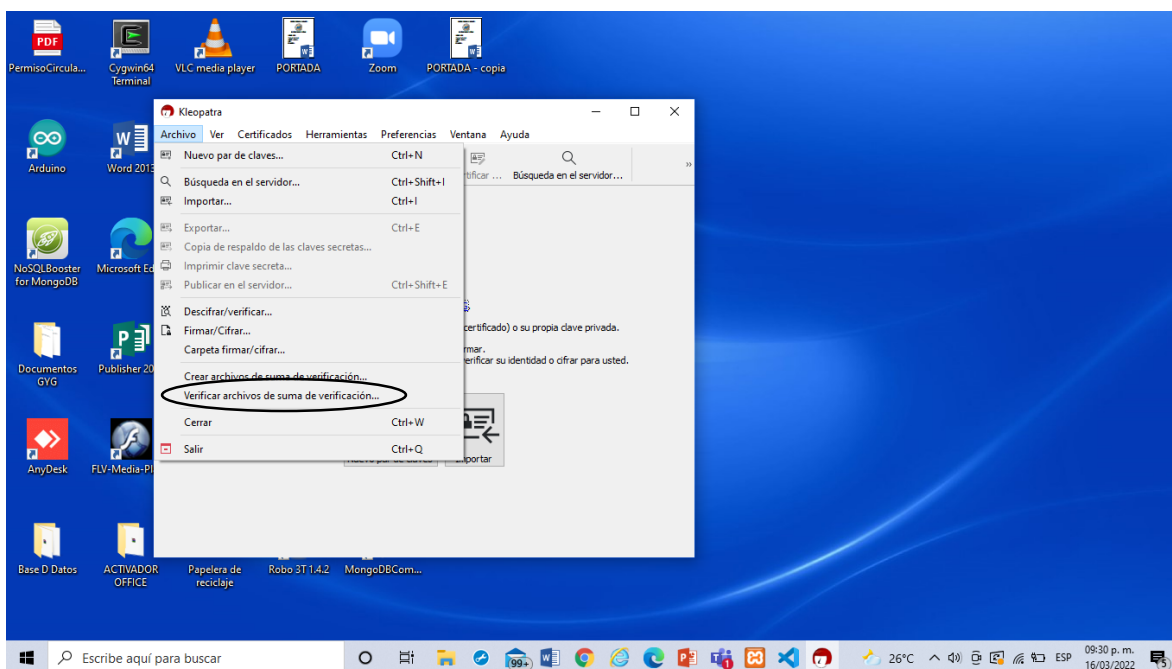
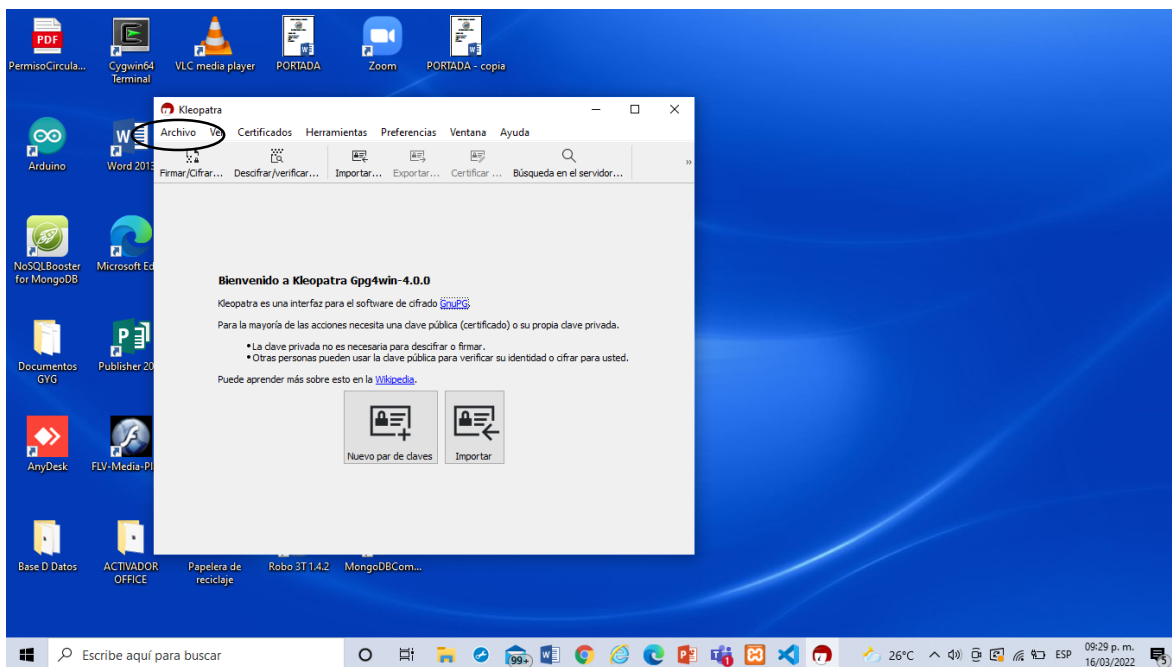
3.- Colocar Códigos PHP y carpetas en C:\xampp\htdocs

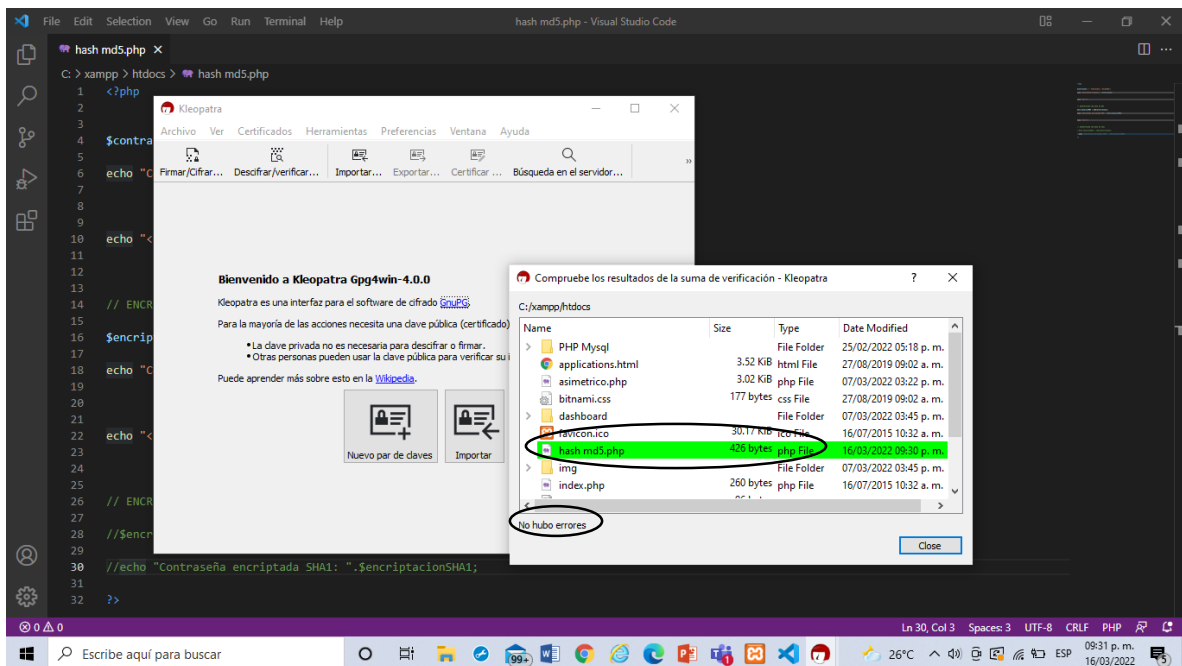
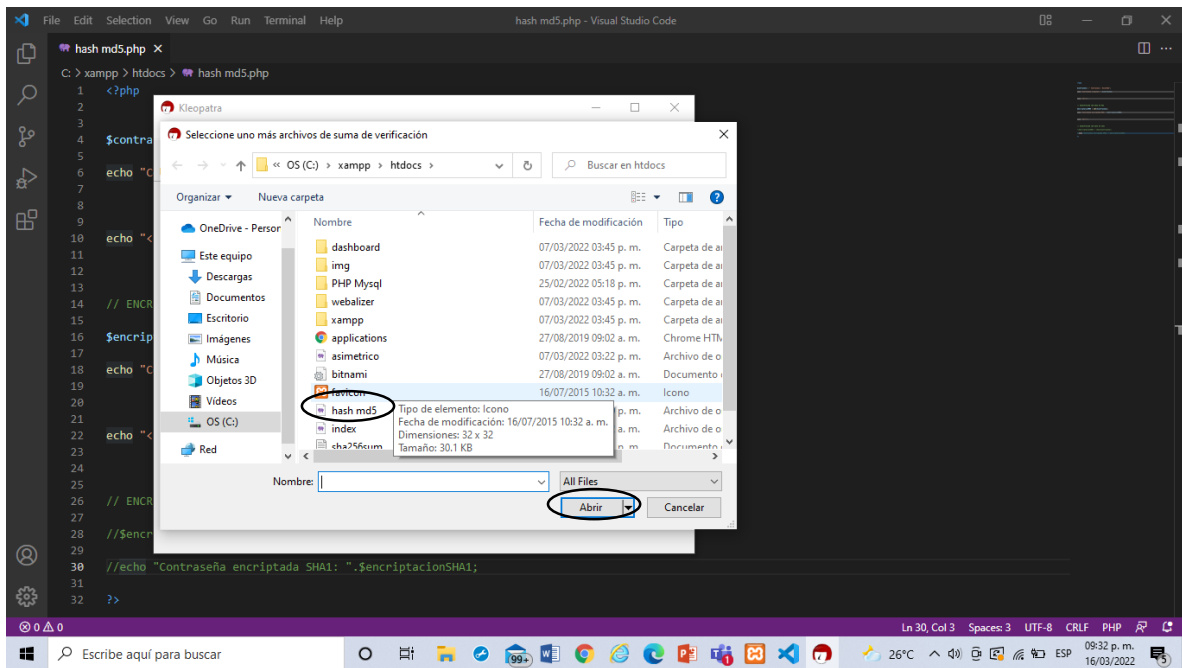


4.- Se muestra el código PHP generado en el buscador, se muestra a través de nuestro local host.

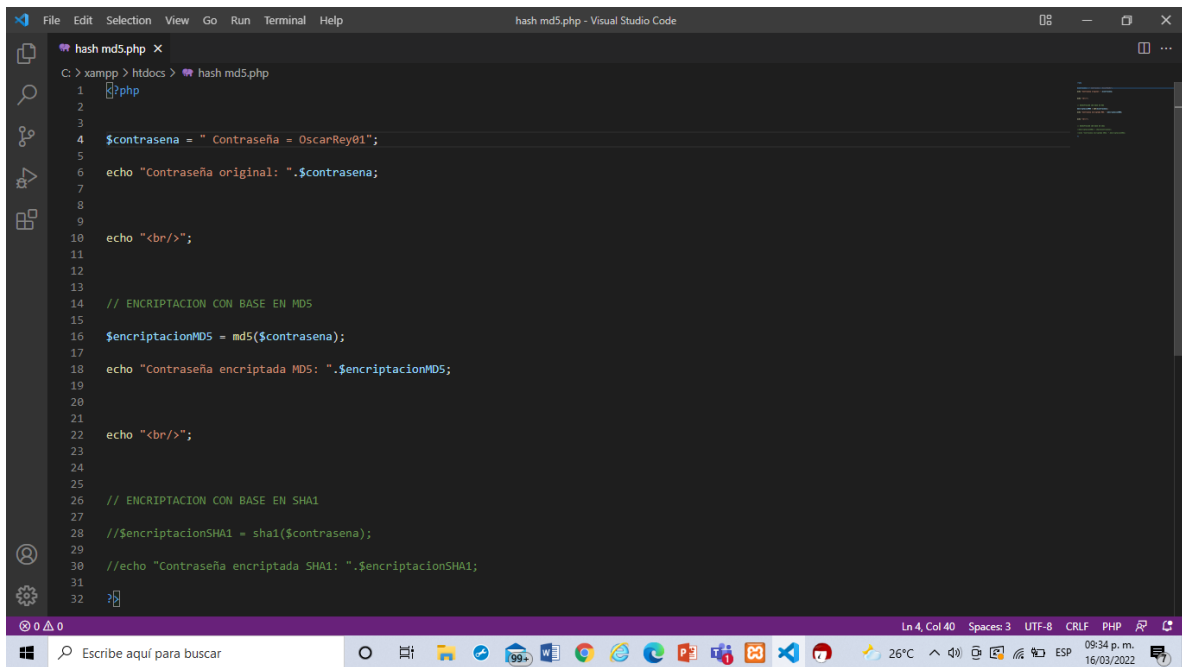


5.- Realizamos un Checksum a nuestro archivo de nuestro algoritmo desde la carpeta C:\xampp\htdocs en donde se encuentra nuestro archivo.

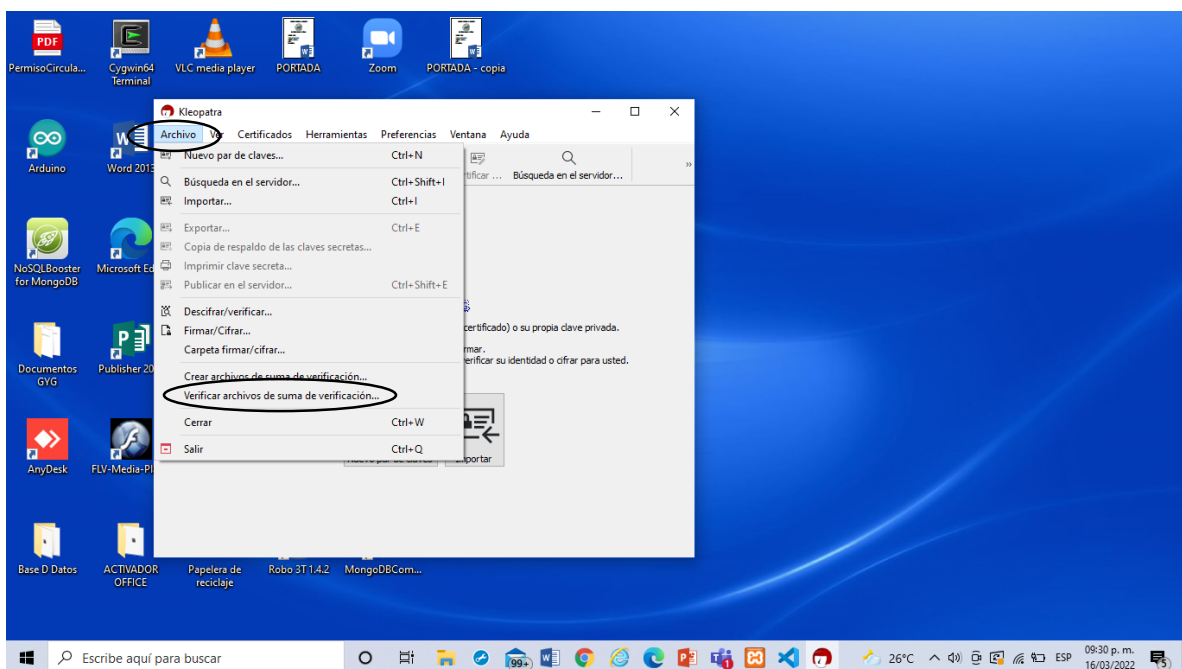


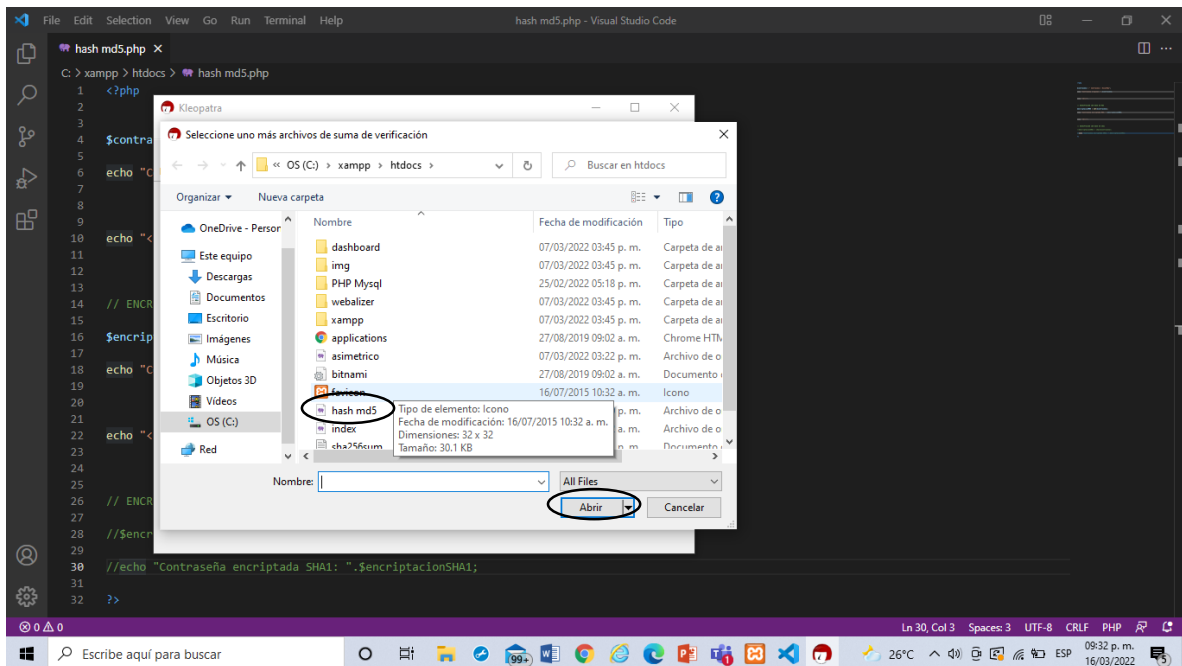


6.- Realizamos un cambio en nuestro código PHP generado par después realizar un Checksum a nuestro archivo de nuestro algoritmo desde la carpeta C:\xampp\htdocs en donde se encuentra nuestro archivo para verificar que nuestra practica y nuestro Checksum estén correctos.

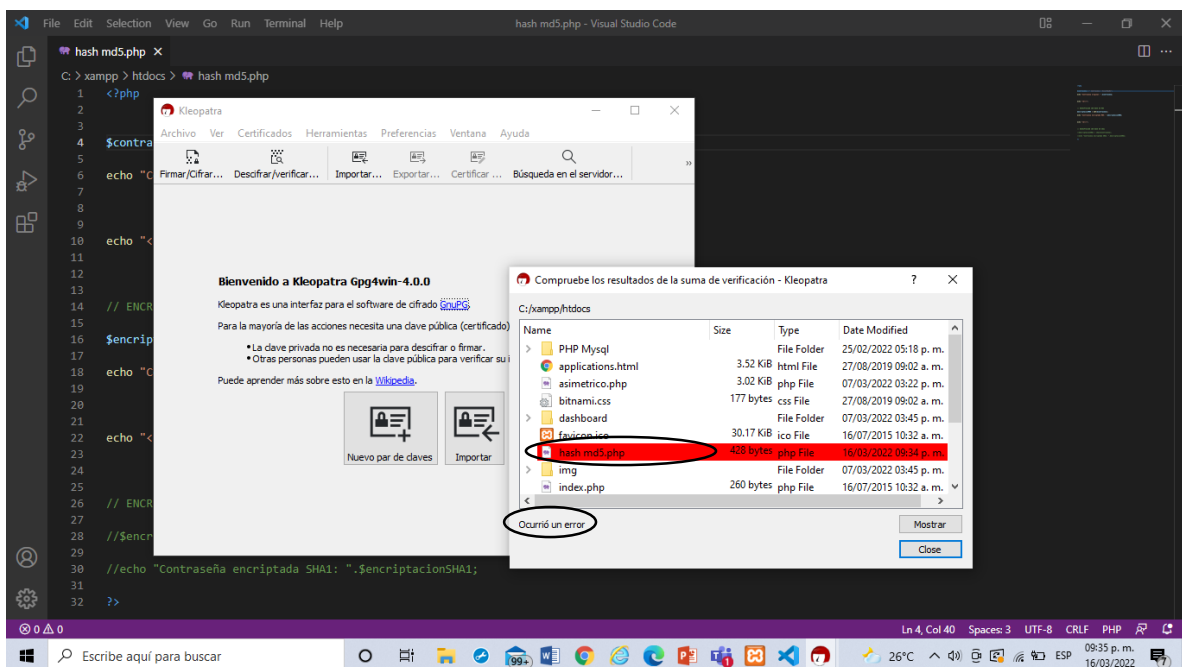


```
hash_md5.php
C:\xampp\htdocs> php hash_md5.php
1 <?php
2
3
4 $contrasena = " Contraseña = OscarRey01!";
5
6 echo "Contraseña original: ".$contrasena;
7
8
9
10 echo "<br/>";
11
12
13
14 // ENCRIPCACION CON BASE EN MD5
15
16 $encryptacionMD5 = md5($contrasena);
17
18 echo "Contraseña encriptada MD5: ".$encryptacionMD5;
19
20
21
22 echo "<br/>";
23
24
25
26 // ENCRIPCACION CON BASE EN SHA1
27
28 // $encryptacionSHA1 = sha1($contrasena);
29
30 // echo "Contraseña encriptada SHA1: ".$encryptacionSHA1;
31
32
```



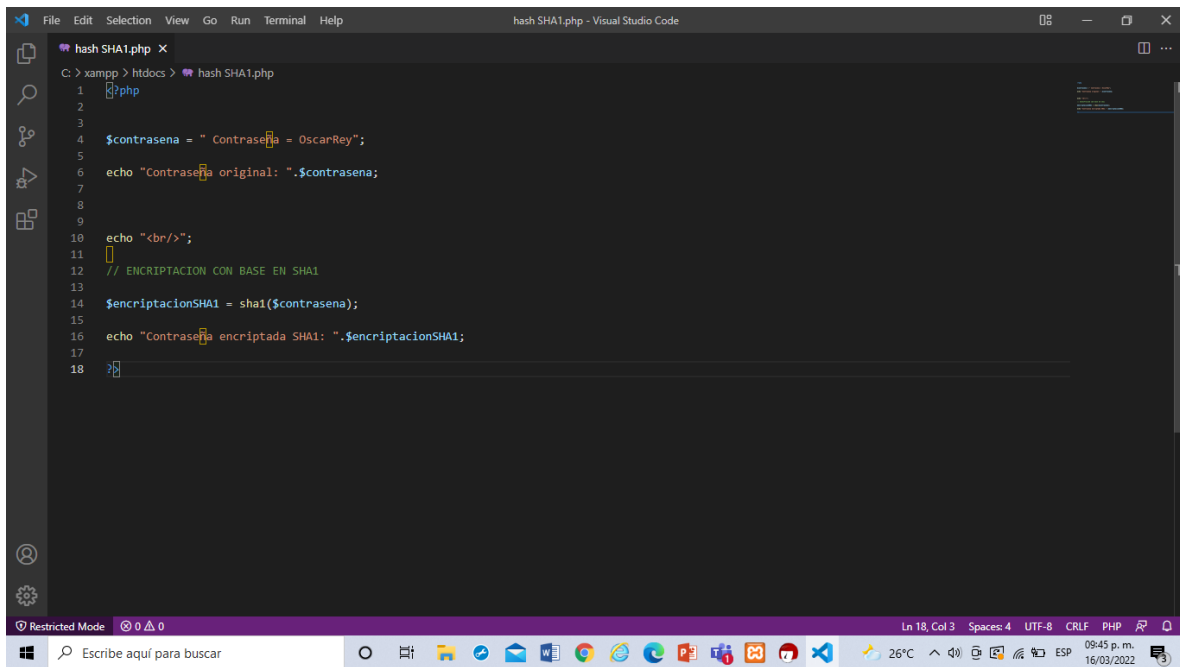


7.- Y al momento de hacer un cambio en el código y realizar esta acción en la pantalla nos mostrara un mensaje de error en la operación, así nuestra practica está completa y para regresar a lo anterior solo es volver a corregir el código a como se encontraba antes.



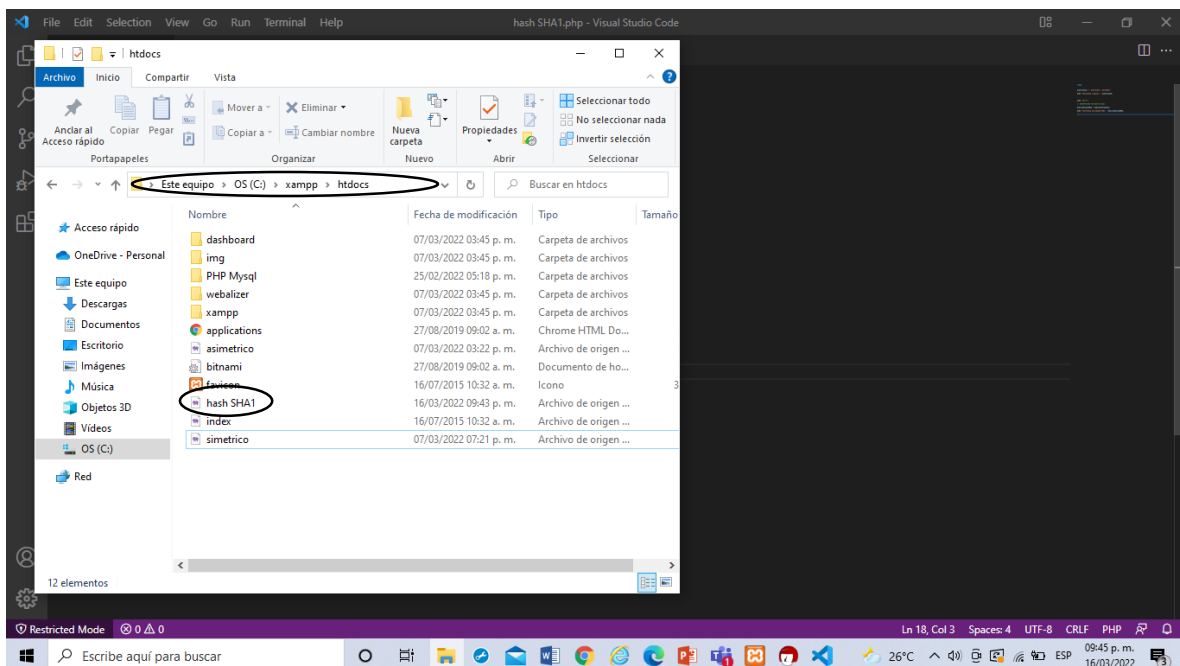
CODIGO SHA1

1.- Crear Código que utilice hash SHA1

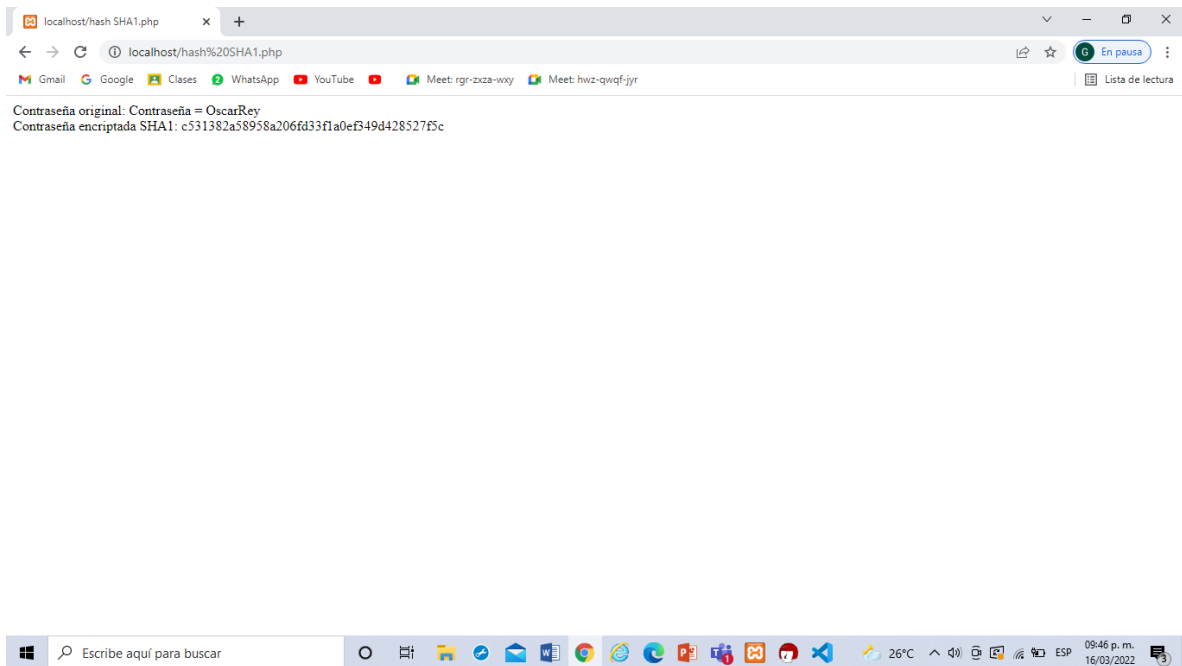


```
hash SHA1.php X
C: > xampp > htdocs > hash SHA1.php
1  #?php
2
3
4  $contrasena = " Contraseña = OscarRey";
5
6  echo "Contraseña original: ".$contrasena;
7
8
9
10 echo "<br/>";
11
12 // ENCRYPTACION CON BASE EN SHA1
13
14 $encriptacionSHA1 = sha1($contrasena);
15
16 echo "Contraseña encriptada SHA1: ".$encriptacionSHA1;
17
18
```

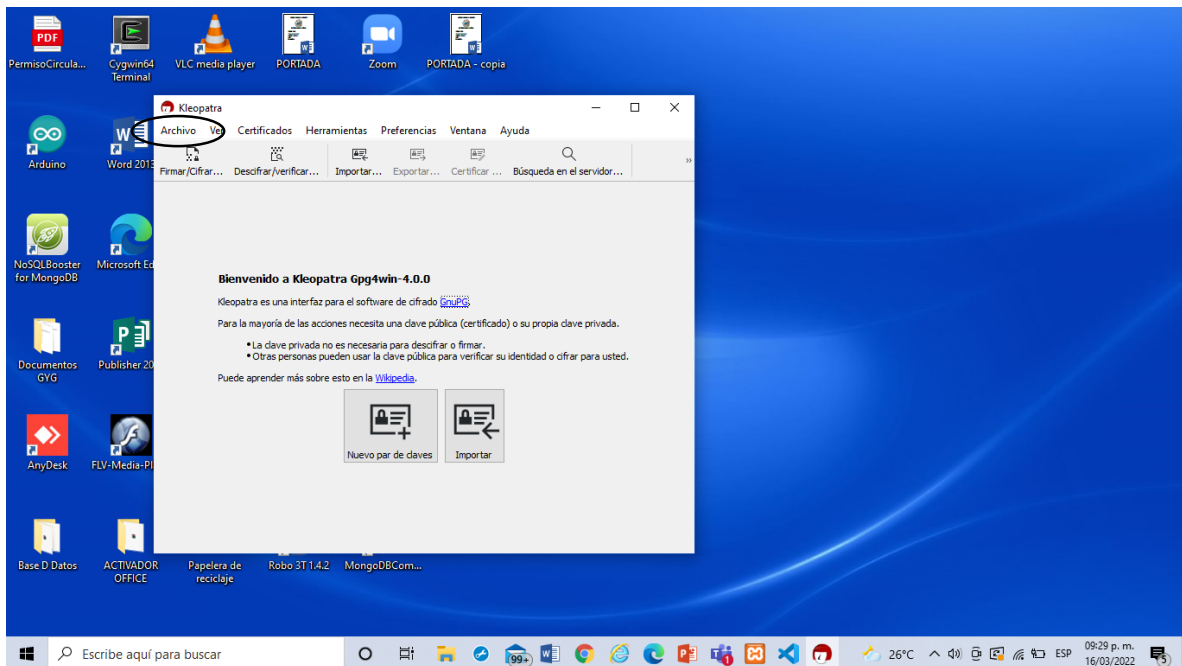
2.- Colocar Códigos PHP y carpetas en C:\xampp\htdocs

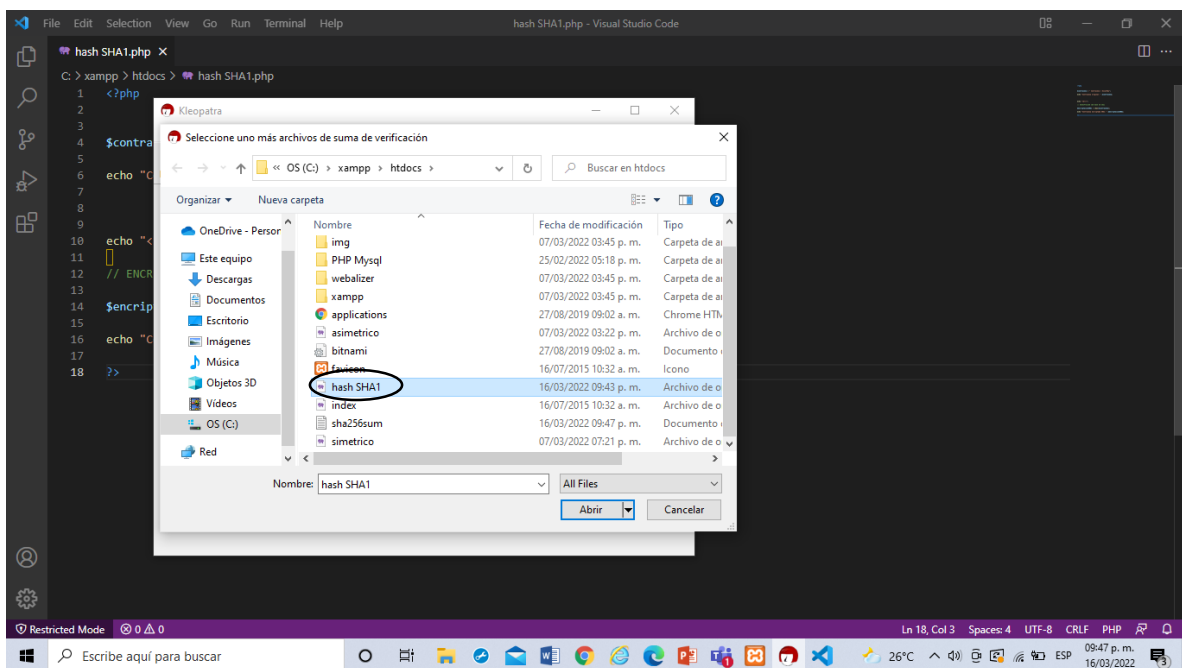
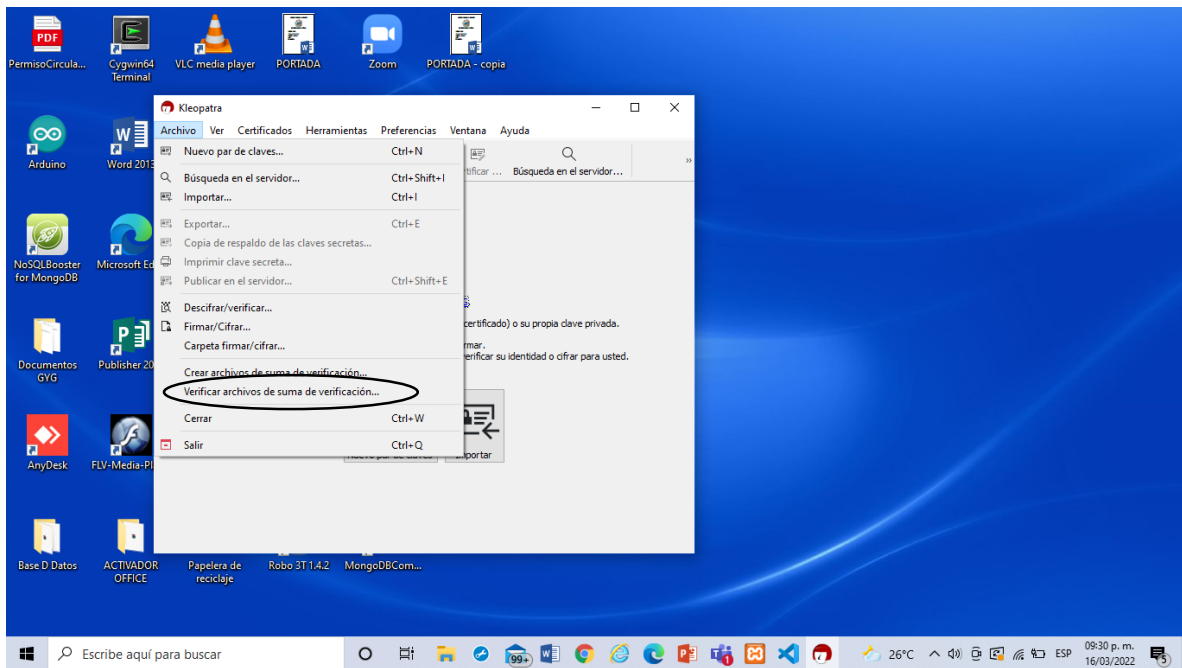


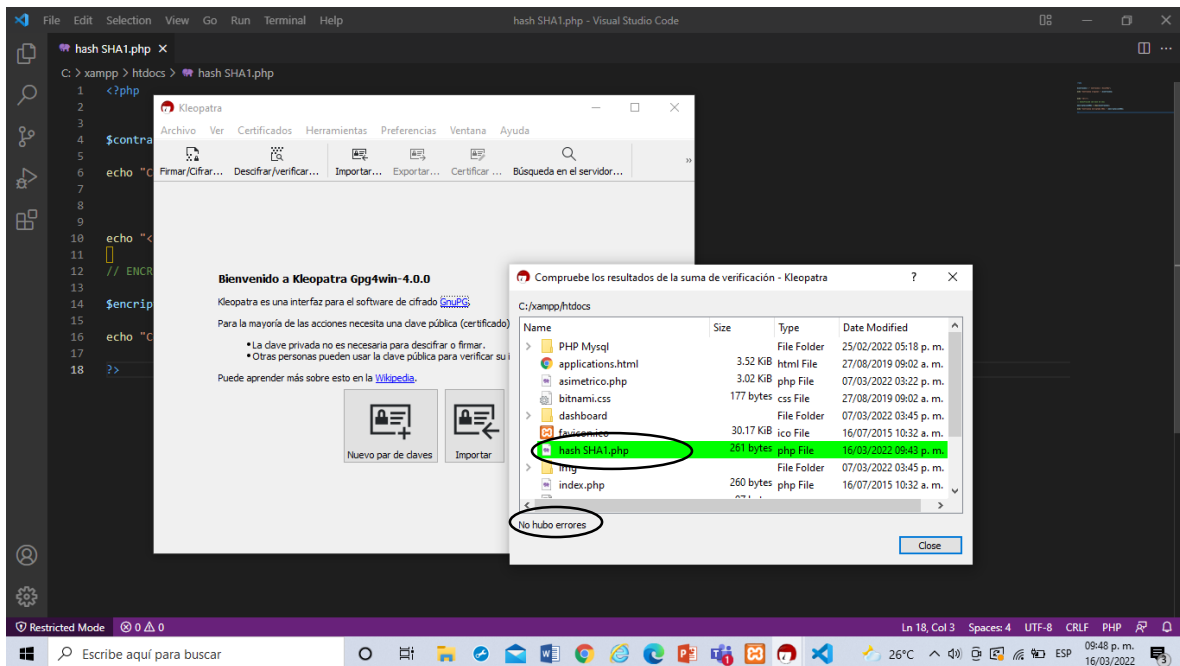
3.- Se muestra el código PHP generado en el buscador, se muestra a través de nuestro local host.



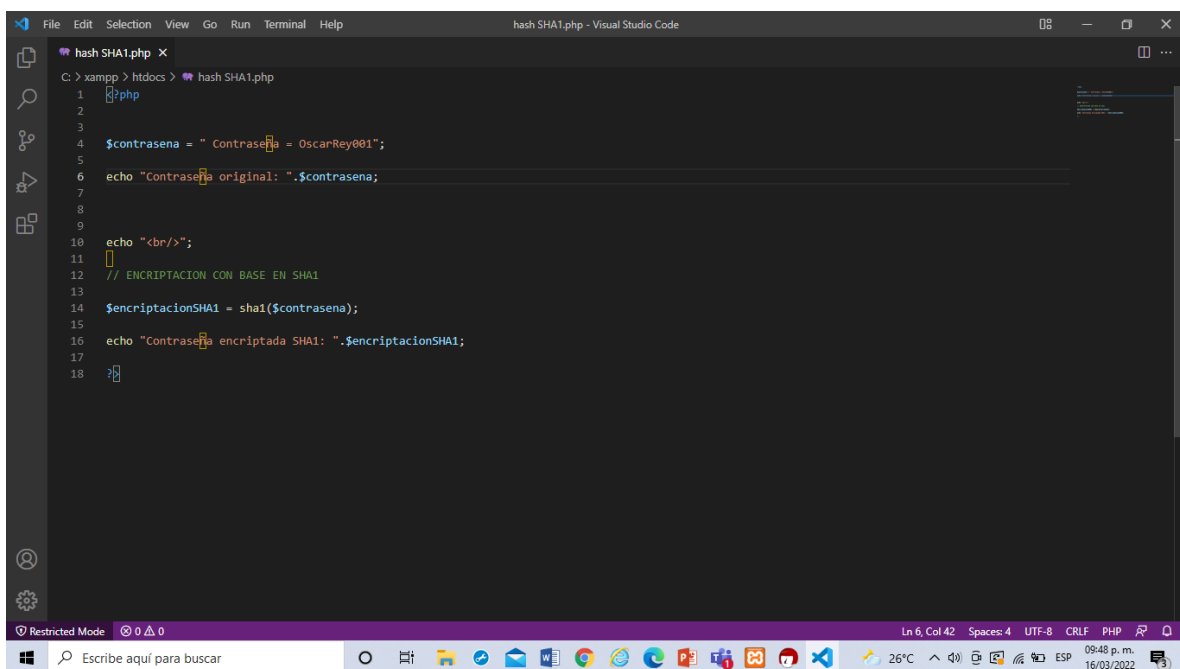
4.- Realizamos un Checksum a nuestro archivo de nuestro algoritmo desde la carpeta C:\xampp\htdocs en donde se encuentra nuestro archivo.

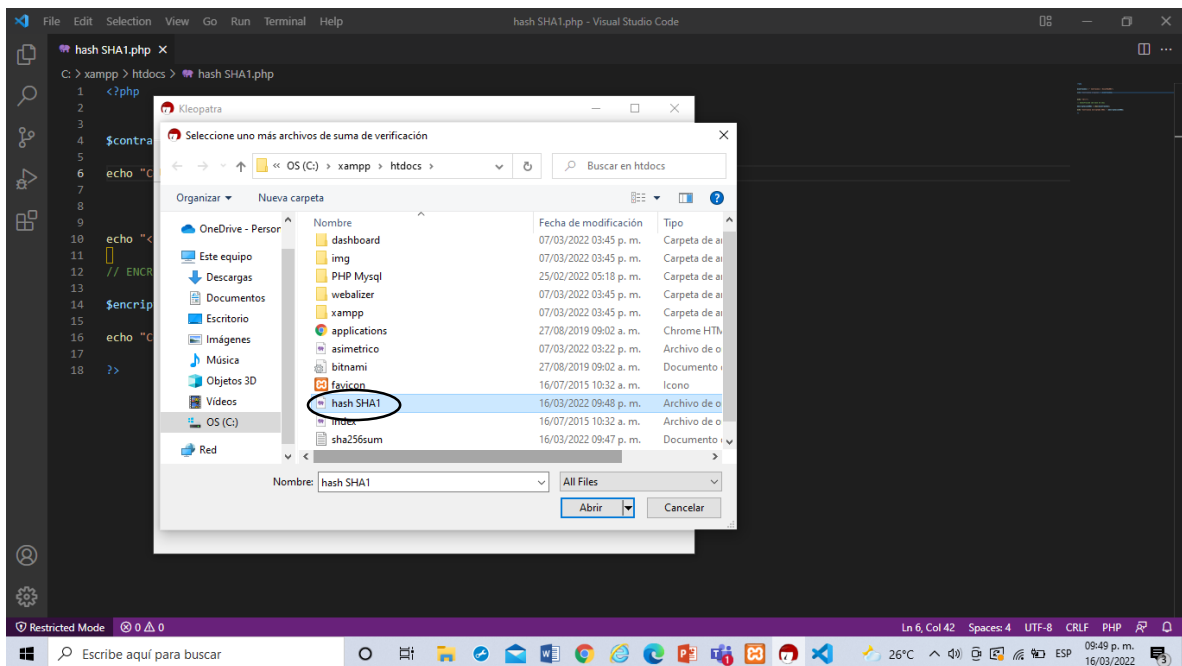
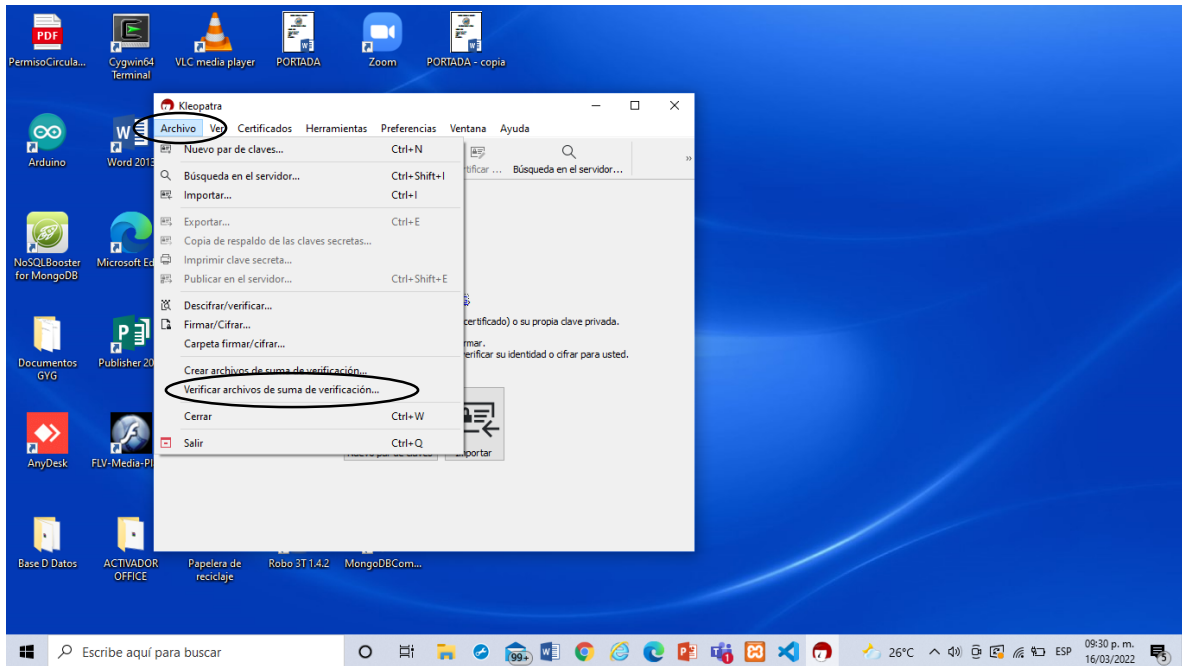




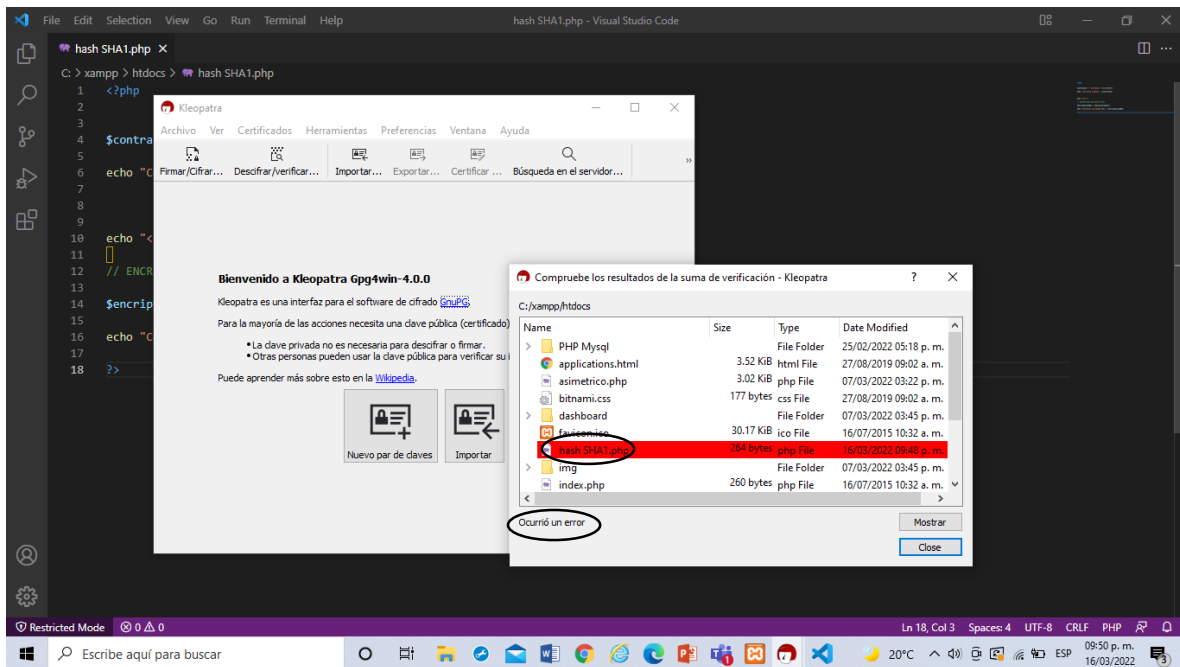


5.- Realizamos un cambio en nuestro código PHP generado par después realizar un Checksum a nuestro archivo de nuestro algoritmo desde la carpeta C:\xampp\htdocs en donde se encuentra nuestro archivo para verificar que nuestra practica y nuestro Checksum estén correctos.





6.- Y al momento de hacer un cambio en el código y realizar esta acción en la pantalla nos mostrara un mensaje de error en la operación, así nuestra practica está completa y para regresar a lo anterior solo es volver a corregir el código a como se encontraba antes.



Conclusión: Personalmente para mí trabajar esta actividad me gustó mucho porque así pude saber cómo hacer una buena práctica la relacionada al php, al cifrado de contraseñas con md5 y SHA1 , también aprendí como hacer un checkzoom, Esto me ayudó mucho ya que conocí temas que desconocía y también aprendí más cosas, de igual forma aprendi que SHA-1 transforma un mensaje a una larga ristra de números y letras que sirven como huella criptográfica (hash) para ese mensaje y que md5 es una función hash de 128 bits, que toma como entrada un mensaje de tamaño arbitrario y produce como salida un resumen del mensaje de 128 bits. El MD5 no sirve para cifrar un mensaje ya que lo destruye completamente, la información no es recuperable de ninguna manera ya que hay pérdida de información.

