

UNIVERSIDAD TECNOLÓGICA DE AGUASCALIENTES



ING. EN SISTEMAS Y DESARROLLO DE SOFTWARE

NOMBRE DEL ALUMNO:

OSCAR RENATO GARCÍA RESÉNDIZ 7.-A

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

MATERIA: SEGURIDAD INFORMÁTICA

FECHA DE ENTREGA: 07/03/2021

Introducción.

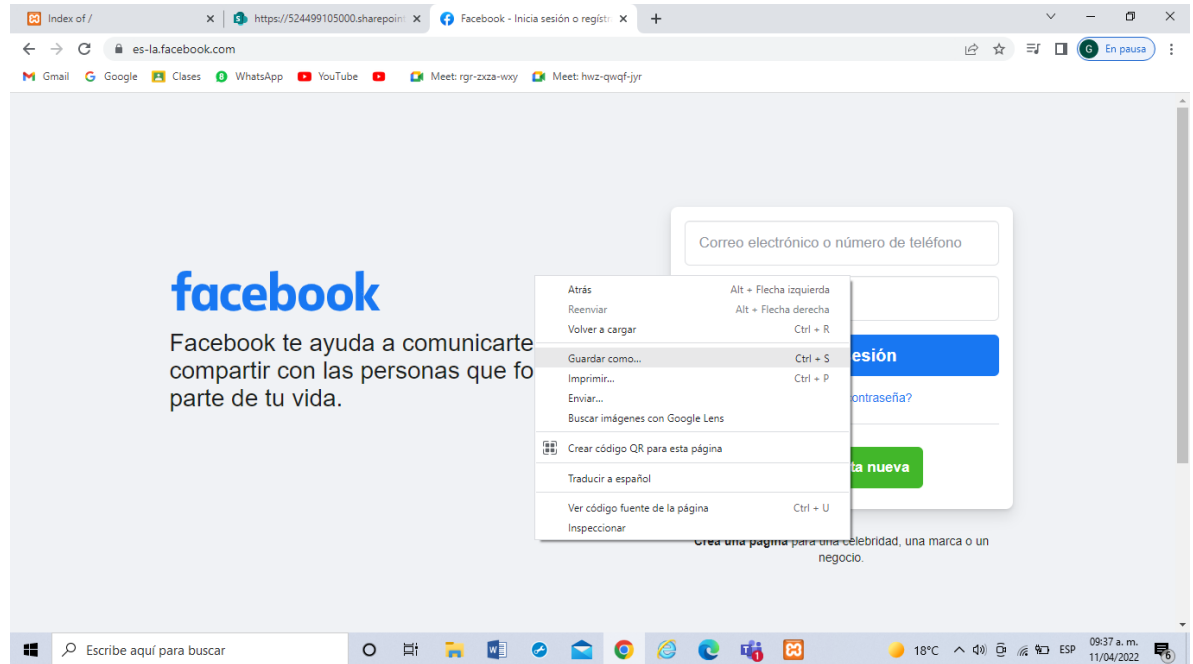
En esta práctica trabajaremos con diversos servicios y adentrándonos un poco a unas prácticas de wireshark. Además de adentrarnos al protocolo https que es importante porque es un protocolo de comunicación de Internet que protege la integridad y la confidencialidad de los datos de los usuarios entre sus ordenadores y el sitio. Además de que el Phishing es la principal estafa o fraude electrónico más común que existe que desea adquirir información privada del usuario, En estas prácticas usaremos los servicios de XAMPP, especialmente APACHE, el certificado SSL y el Sniffer wireshark, estos son los que nos ayudarán a que nuestras prácticas sean muy buenas, en esta 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.

Desarrollo.

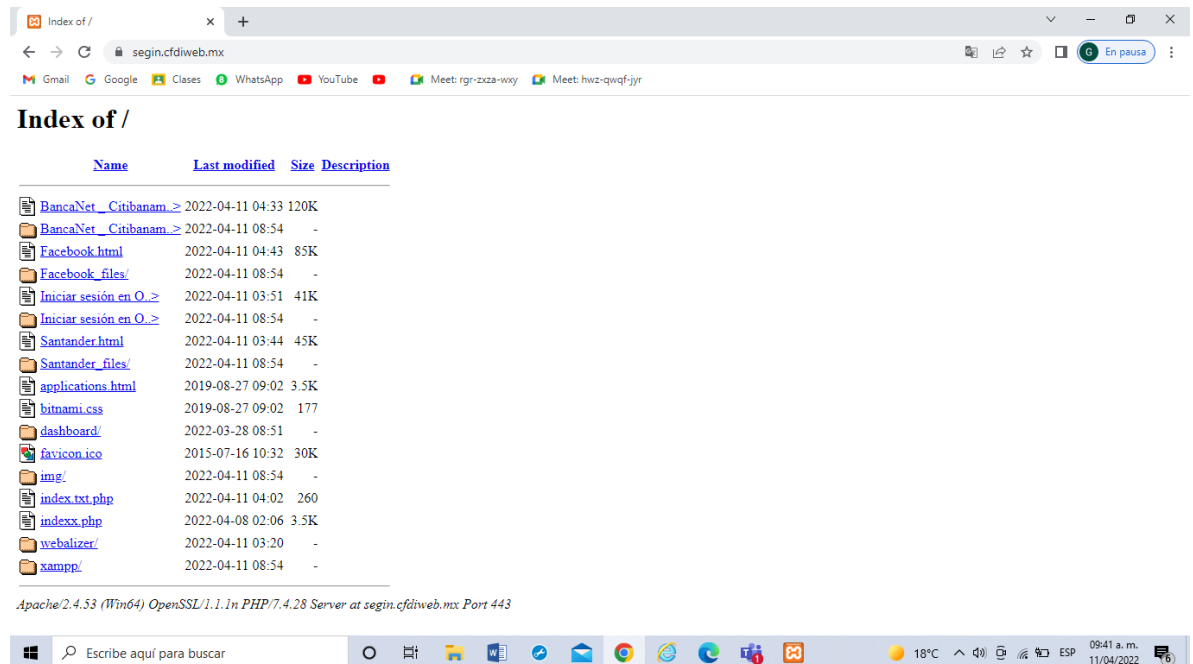
En esta práctica se analizará el protocolo HTTPS con sniffer para comprobar el cifrado, se realizará una prueba de phishing

1. En la página de su elección use la opción "Guardar como.." (clic botón derecho del mouse en la página elegida)
2. Descargue el Sniffer WireShark <https://www.wireshark.org/#download>
3. Cargue la página en el DocumentRoot de XAMPP
4. Cargue el Certificado SSL
5. Capture paquetes para el puerto 80 y 443 ¿en cual puerto se puede ver la información?

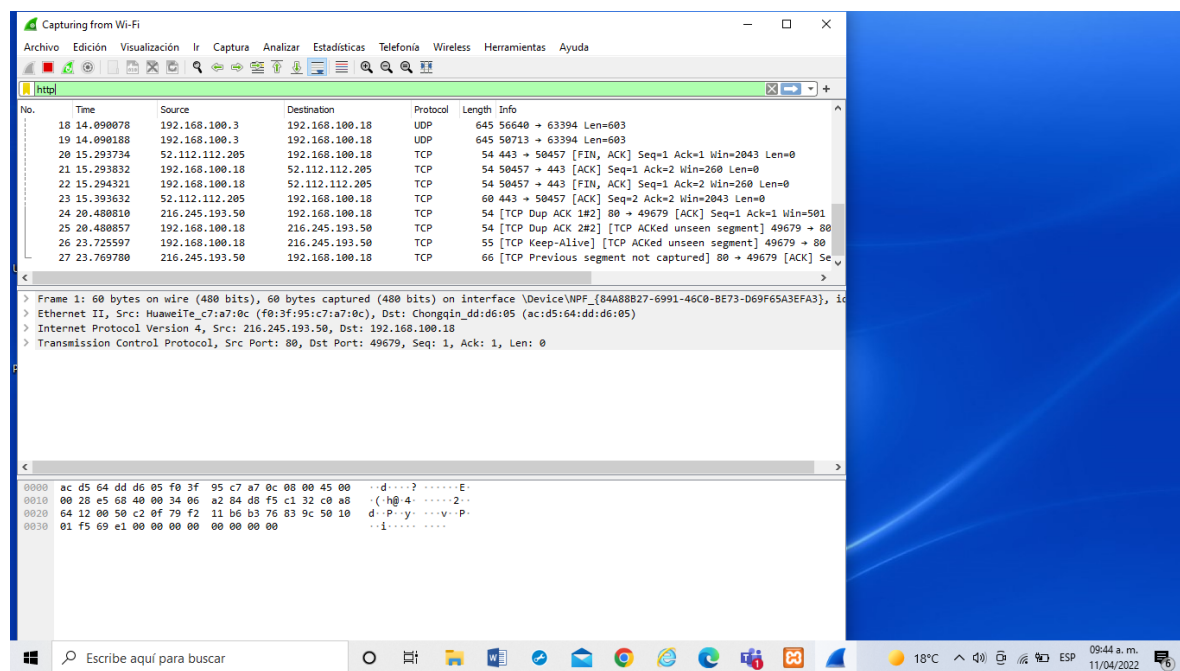
En la pagina de su elección use la opción "Guardar como.." (clic botón derecho del mouse en la pagina elegida)



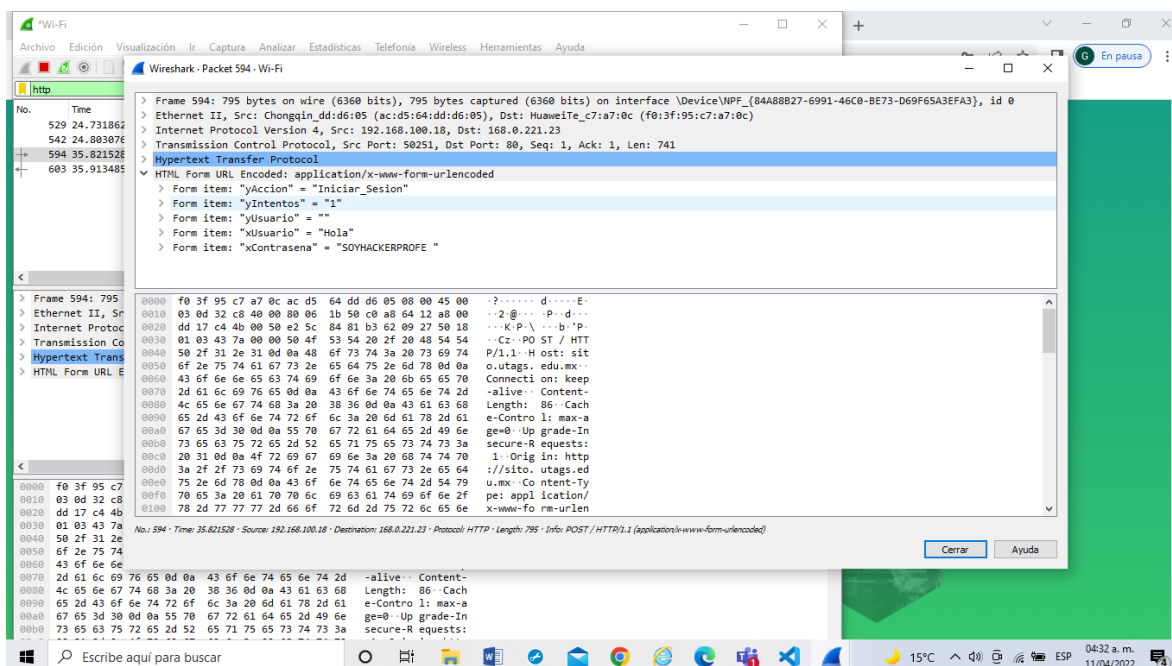
Abrir la página descargada desde nuestro XAMPP



Una vez abierta la página web desde nuestro index, procedemos a abrir nuestro Sniffer WireShark, seleccionamos el campo de búsqueda http para que filtre toda la información en tránsito con el certificado http.



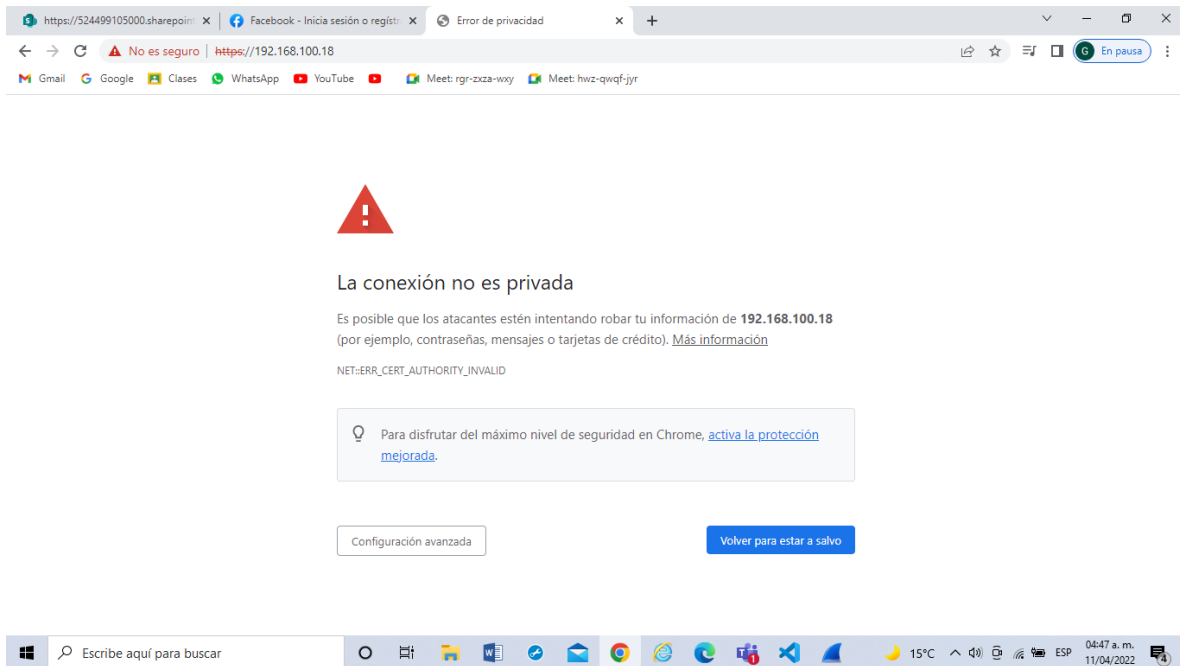
Una vez realizado lo siguiente, procedemos a desde nuestro celular o desde otra computadora diferente a la que tenemos conectada a nuestro servidor xampp, accedemos remotamente a nuestro index de Xampp, y abrimos la página descargada, una vez abierto el formulario de inicio de sesión desde nuestra otra computadora o celular, hacemos el llenado de datos de inicio de sesión y mandamos la información, una vez echo esto se puede observar que el sniffer pudo captar las credenciales usadas desde la otra computadora para verificar que el sniffer si haga la muestra de datos que se utilizó desde el otro dispositivo y como se muestra a continuación, si se realizó la muestra de datos que se le proporciono al formulario desde otro dispositivo, esto es una prueba de phishing.



Asi es como se puede observar como el sniffer capta la informacion obtenida de la pagina a travez de el inicio de sesion de el usuario, desde otra computadora a travez de el sniffer y de la coneccion que se hace entre los dos dispositivos.

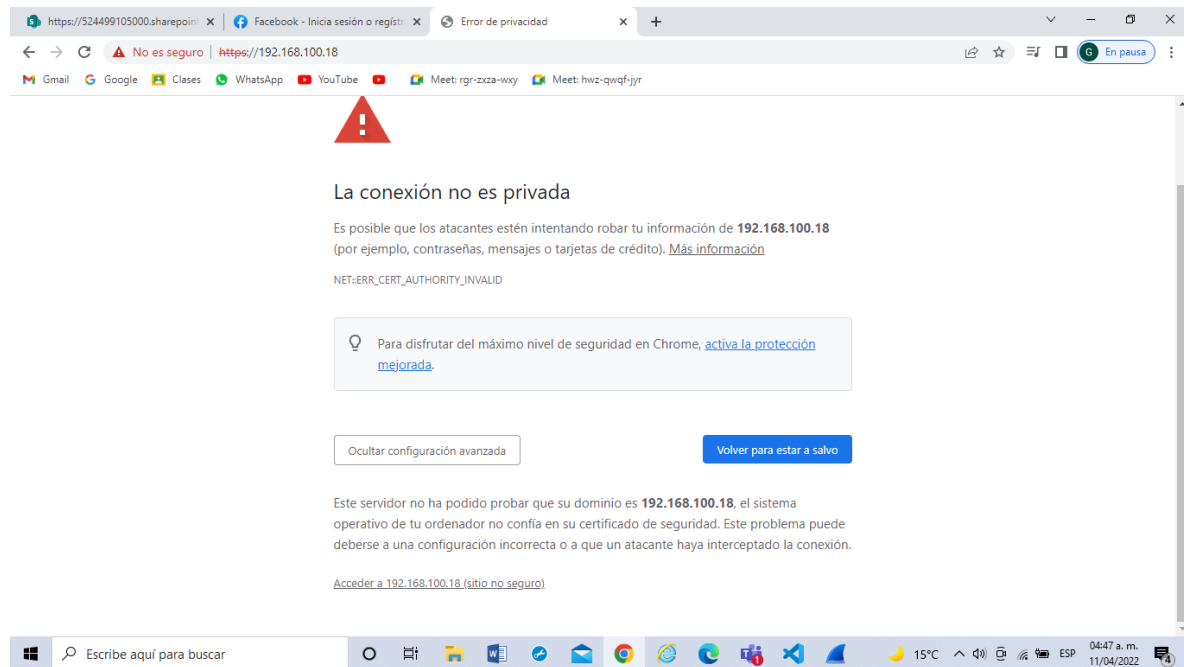
La siguiente práctica a realizar se basa en los certificados que tenemos y de la seguridad que se le brinda al usuario a la seguridad que maneja la página a la que uno está accediendo, se sabe que los certificados dados a la página son a base de la IP que se maneja, así que realizaremos una práctica donde realizaremos el cambio de certificado para acceder de manera segura.

Primero accederemos a nuestro Index o a nuestra página de Xampp a través del certificado https para darnos cuenta de lo que tenemos mal en nuestro certificado y de que nos muestra de que no es seguro pero para eso lo modificaremos y lo trabajaremos para que el certificado sea seguro y hacer una práctica correcta



Accedemos al siguiente link <https://192.168.100.18> Dónde está es nuestra ip de nuestra computadora a la que estamos conectados Al momento de ingresar como podemos vernos marca que la conexión no es privada y Qué es posible que estén atacando información

En la siguiente pantalla se muestra como nosotros podemos desglosar la información de la conexión y aún así seleccionar la opción de entrar al sitio aunque no sea seguro



Una vez ya ingresando a nuestra plataforma Index podemos observar que al costado de nuestra certificación https se encuentra un mensaje que dice que no Es segura la conexión Y esto es lo que nosotros Tratamos de arreglar

Index of /

Name	Last modified	Size	Description
BancaNet_Citibanam.>	2022-04-11 04:33	120K	
BancaNet_Citibanam.>	2022-04-11 04:33	-	
Facebook.html	2022-04-11 04:43	85K	
Facebook_files/	2022-04-11 04:43	-	
Iniciar sesión en O.>	2022-04-11 03:51	41K	
Iniciar sesión en O.>	2022-04-11 03:51	-	
Santander.html	2022-04-11 03:44	45K	
Santander_files/	2022-04-11 03:44	-	
applications.html	2019-08-27 09:02	3.5K	
bitnami.css	2019-08-27 09:02	177	
dashboard/	2022-03-28 08:51	-	
favicon.ico	2015-07-16 10:32	30K	
img/	2022-04-11 03:20	-	
index.txt.php	2022-04-11 04:02	260	
indexx.php	2022-04-08 02:06	3.5K	
webalizer/	2022-04-11 03:20	-	
xampp/	2022-04-11 03:20	-	

Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.28 Server at 192.168.100.18 Port 443

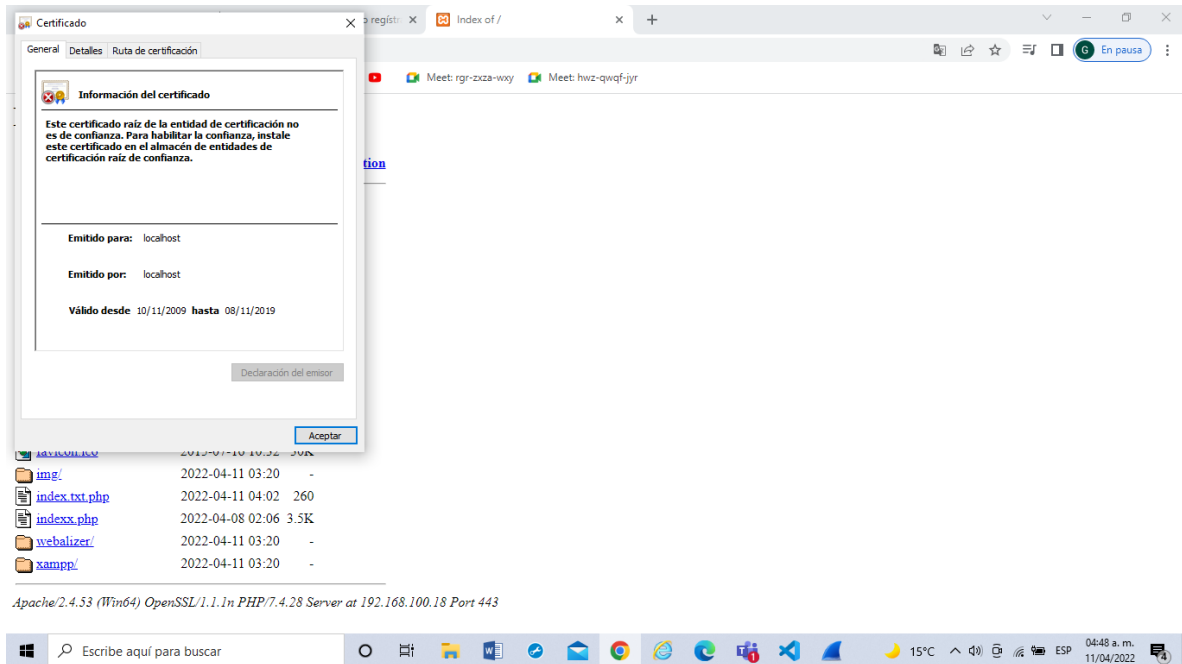
Al momento de nosotros darle click a ese mensaje de no es seguro nos va a mostrar toda la información de la conexión de el cifrado de las cookies y de la configuración que está en proceso aquí nos explica qué la conexión a nuestro Index no es segura

Index of /




Name	Last modified	Size	Description
BancaNet_Citibanam.>	2022-04-11 04:33	120K	
BancaNet_Citibanam.>	2022-04-11 04:33	-	
Facebook.html	2022-04-11 04:43	85K	
Facebook_files/	2022-04-11 04:43	-	
Iniciar sesión en O.>	2022-04-11 03:51	41K	
Iniciar sesión en O.>	2022-04-11 03:51	-	
Santander.html	2022-04-11 03:44	45K	
Santander_files/	2022-04-11 03:44	-	
applications.html	2019-08-27 09:02	3.5K	
bitnami.css	2019-08-27 09:02	177	
dashboard/	2022-03-28 08:51	-	
favicon.ico	2015-07-16 10:32	30K	
img/	2022-04-11 03:20	-	
index.txt.php	2022-04-11 04:02	260	
indexx.php	2022-04-08 02:06	3.5K	
webalizer/	2022-04-11 03:20	-	
xampp/	2022-04-11 03:20	-	

Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.28 Server at 192.168.100.18 Port 443

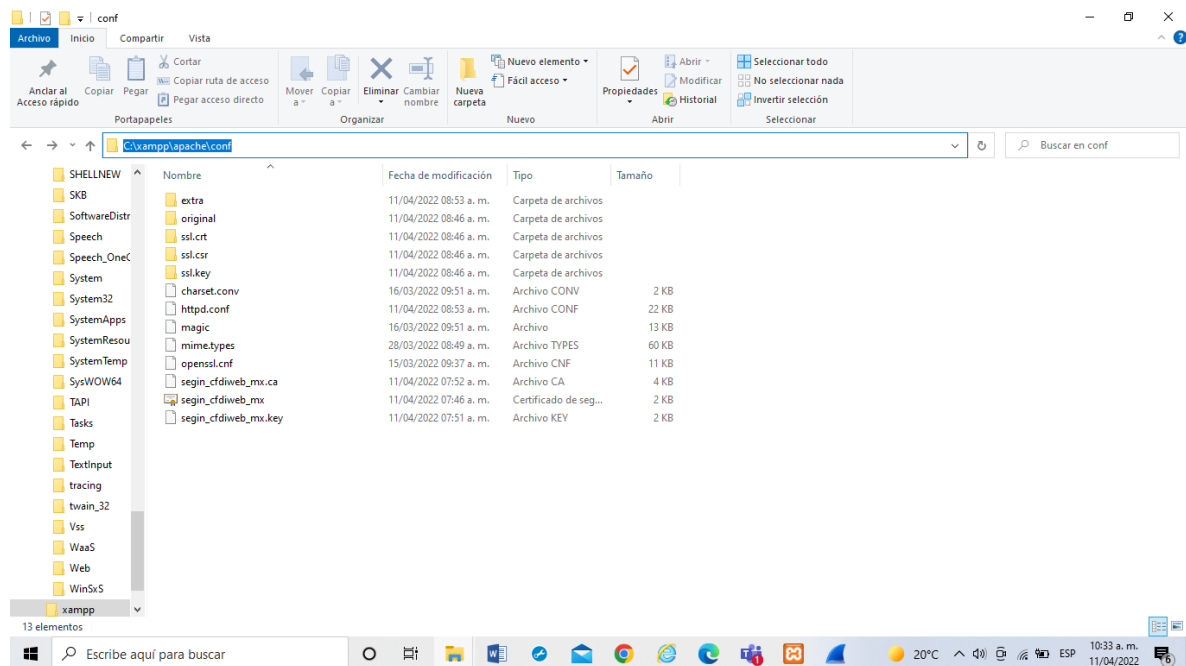
Posteriormente a nosotros al abrir más información o más detallada sobre el certificado nos muestra la siguiente pantalla dónde nos da la información del certificado para quién está estimado y para quién es válido y Hasta qué fecha es válido Así que lo que nosotros procederemos a realizar es la siguiente práctica para poder crear el certificado seguro para nuestra pantallas index



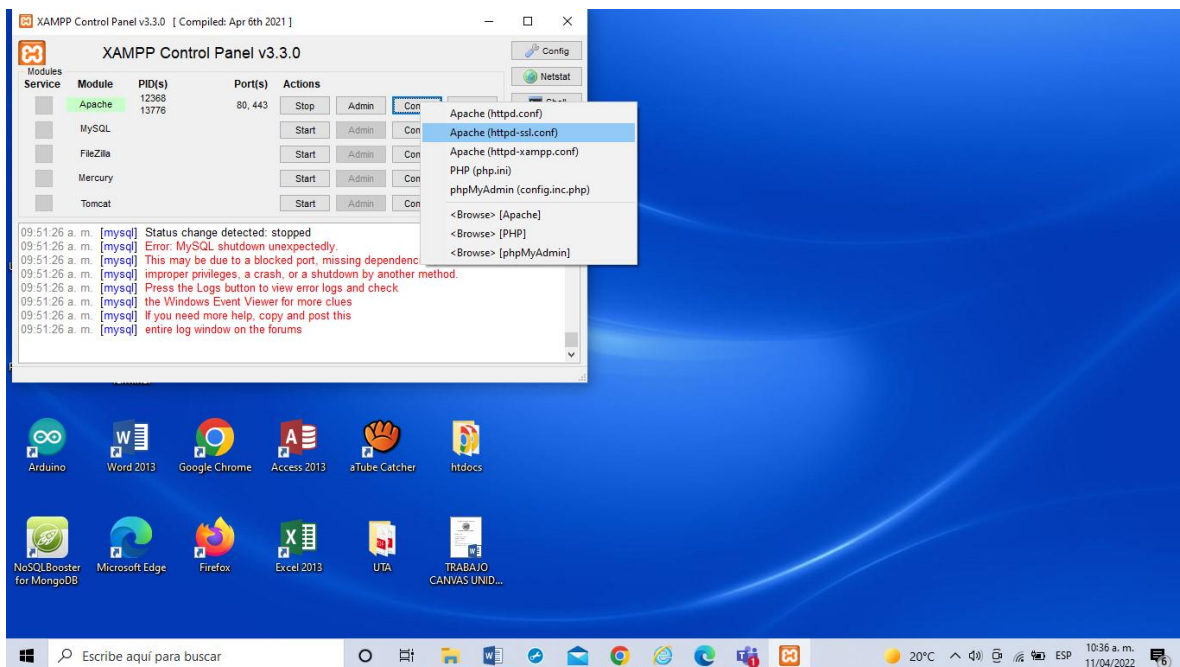
Lo primero que tendremos que hacer para esta práctica será crear o realizar el certificado que nosotros vamos a querer aplicarle a nuestra página o a nuestro servidor para proceder a validarlo y aplicarlo

 segin_cfdiweb_mx.ca	11/04/2022 07:52 a. m.	Archivo CA	4 KB
 segin_cfdiweb_mx	11/04/2022 07:46 a. m.	Certificado de seg...	2 KB
 segin_cfdiweb_mx.key	11/04/2022 07:51 a. m.	Archivo KEY	2 KB

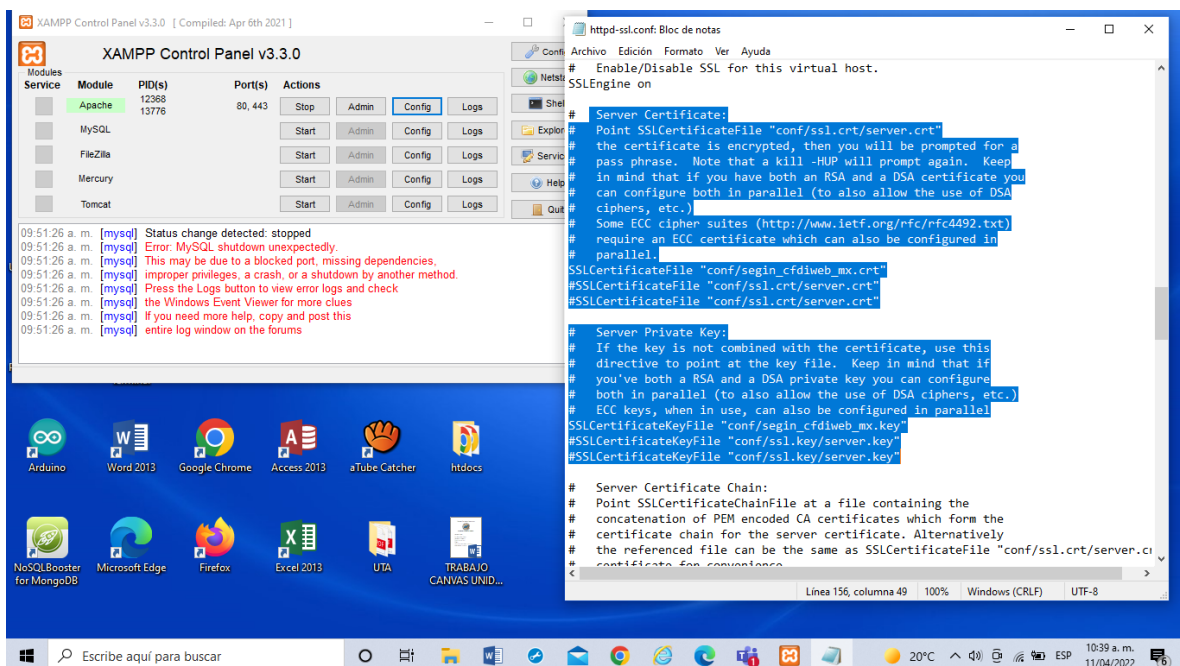
Una vez teniendo ya listo nuestros certificados que el profesor e hizo favor de pasarnos procederemos a los tres archivos Qué nos pasó el profe nos moveremos a la carpeta llamada disco local C:\xampp\apache\config Ahí es donde nosotros procederemos a pegar nuestros archivos de certificado



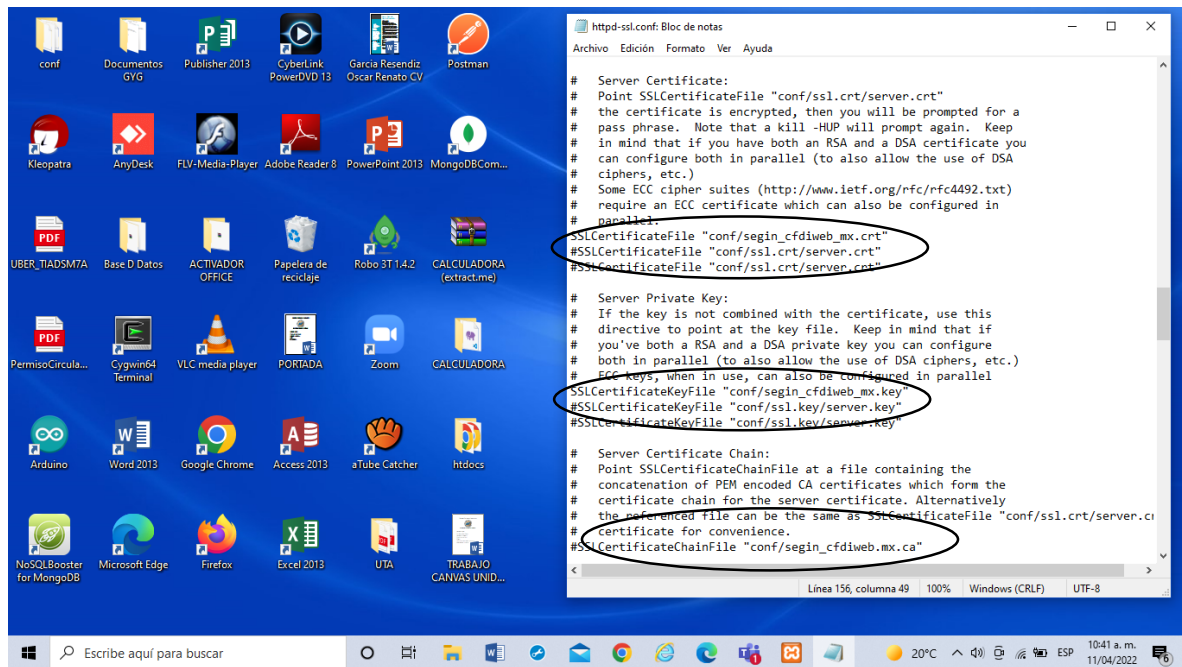
A continuación procederemos a abrir nuestra página principal del xampp O Nuestro panel de control seleccionamos Apache config y aplicamos la opción que tenemos seleccionada



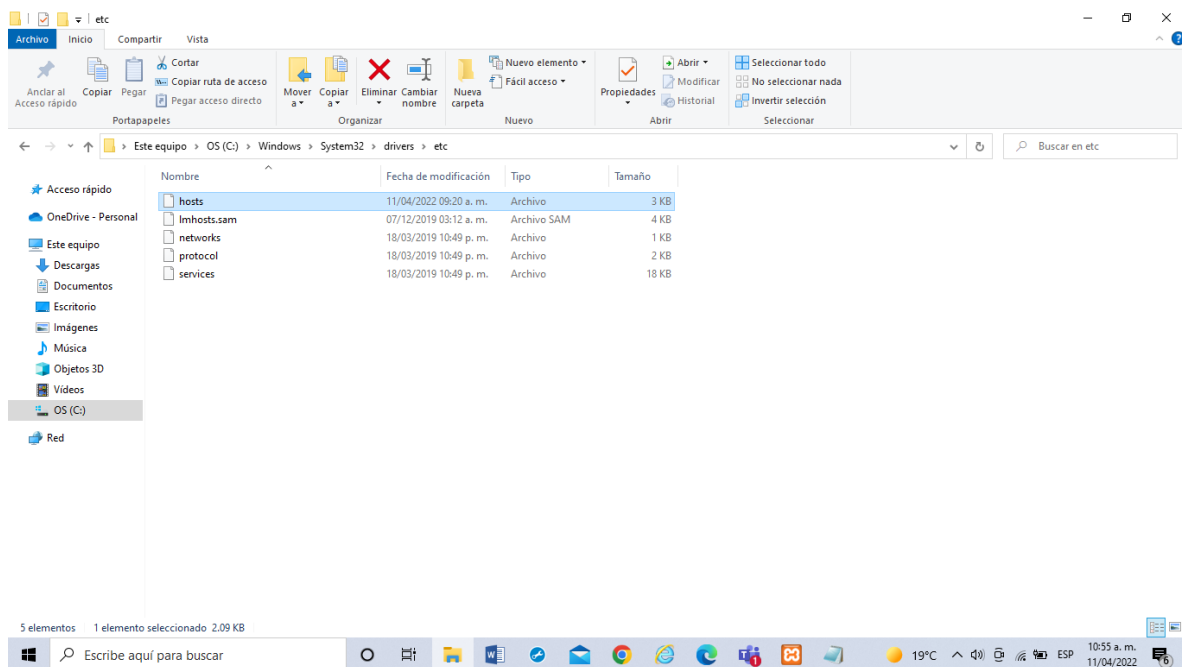
Una vez abierta nuestra página de configuración procederemos a buscar la parte de las llaves donde se muestran nuestros certificados y la configuración para ellos

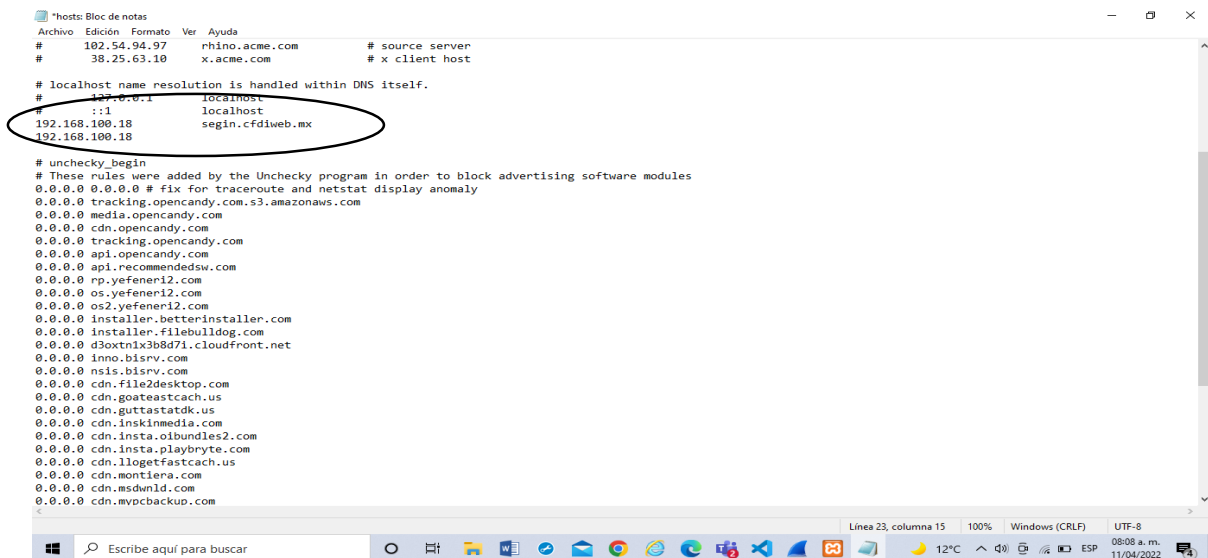


Una vez teniendo seleccionada nuestra pantalla donde haremos el cambio a los certificados procederemos a hacer las siguientes modificaciones que se muestran a continuación y a guardar los resultados



Una vez realizados estos cambios a nuestro código procederemos a dirigirnos a la siguiente carpeta C:\Windows\system32\drivers\etc\host dónde En esta carpeta Y en este archivo llamado Host realizaremos unos cambios y agregaremos nuestra ip de nuestra computadora y la enlazaremos con nuestro certificado para que así tenga la validación correcta





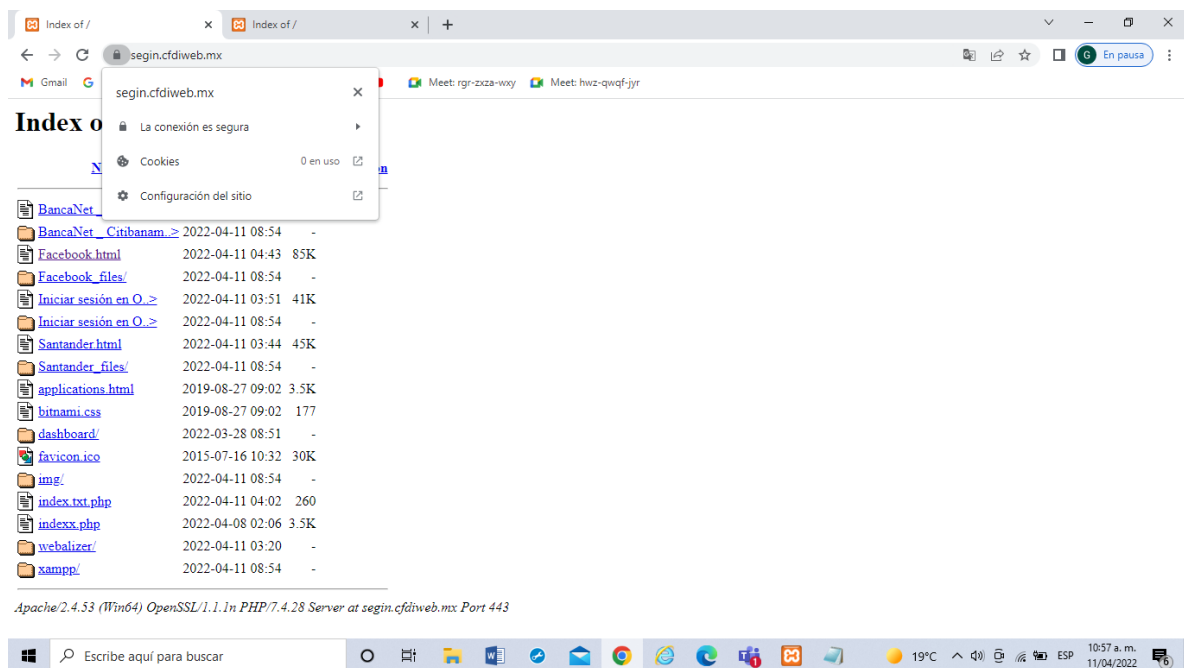
```
#hosts: Bloc de notas
Archivo Edición Formato Ver Ayuda
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host

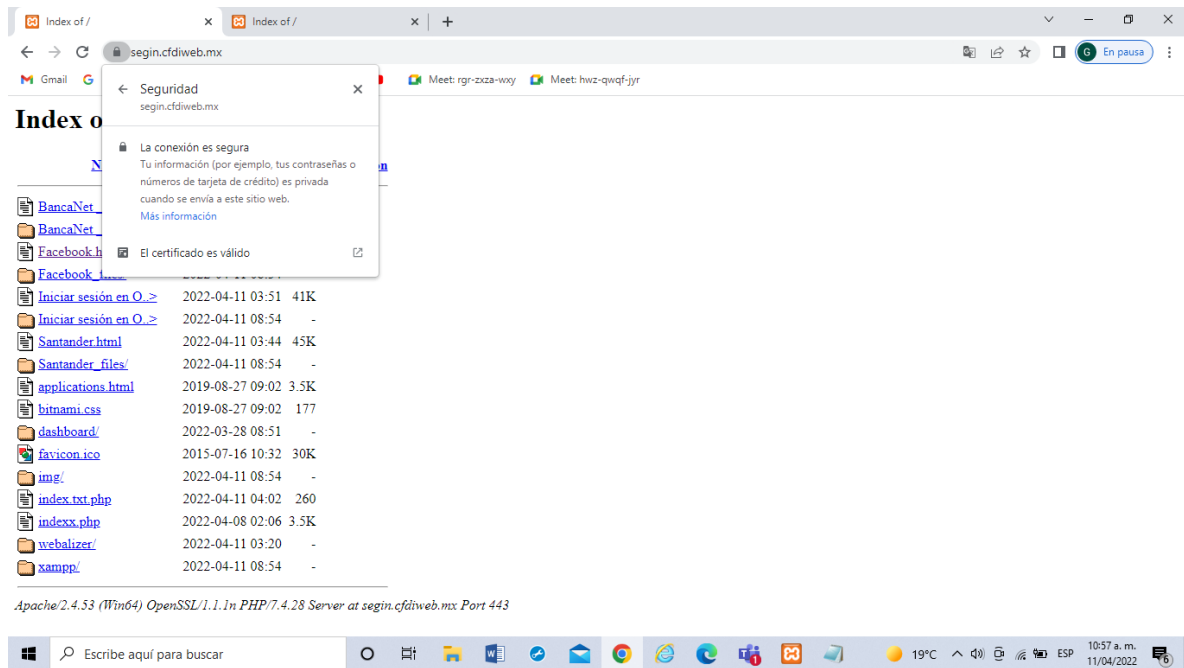
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
192.168.100.18 segin.cfdiweb.mx
192.168.100.18

# unchecky_begin
# These rules were added by the Unchecky program in order to block advertising software modules
0.0.0.0 0.0.0.0 # fix for traceroute and netstat display anomaly
0.0.0.0 tracking.opencandy.com.s3.amazonaws.com
0.0.0.0 media.opencandy.com
0.0.0.0 cdn.opencandy.com
0.0.0.0 tracking.opencandy.com
0.0.0.0 api.opencandy.com
0.0.0.0 api.recommendedsw.com
0.0.0.0 rp.yefener12.com
0.0.0.0 os.yefener12.com
0.0.0.0 os2.yefener12.com
0.0.0.0 installer.betterinstaller.com
0.0.0.0 installer.filebulldog.com
0.0.0.0 d3oxtnix3b8d71.cloudfront.net
0.0.0.0 inno.bisrv.com
0.0.0.0 nsis.bisrv.com
0.0.0.0 cdn.file2desktop.com
0.0.0.0 cdn.goateastcach.us
0.0.0.0 cdn.guttastatdk.us
0.0.0.0 cdn.inskinmedia.com
0.0.0.0 cdn.insta.oibundles2.com
0.0.0.0 cdn.insta.playbryte.com
0.0.0.0 cdn.llogetfastcam.us
0.0.0.0 cdn.montiera.com
0.0.0.0 cdn.msduin1d.com
0.0.0.0 cdn.mvpcbackup.com
```

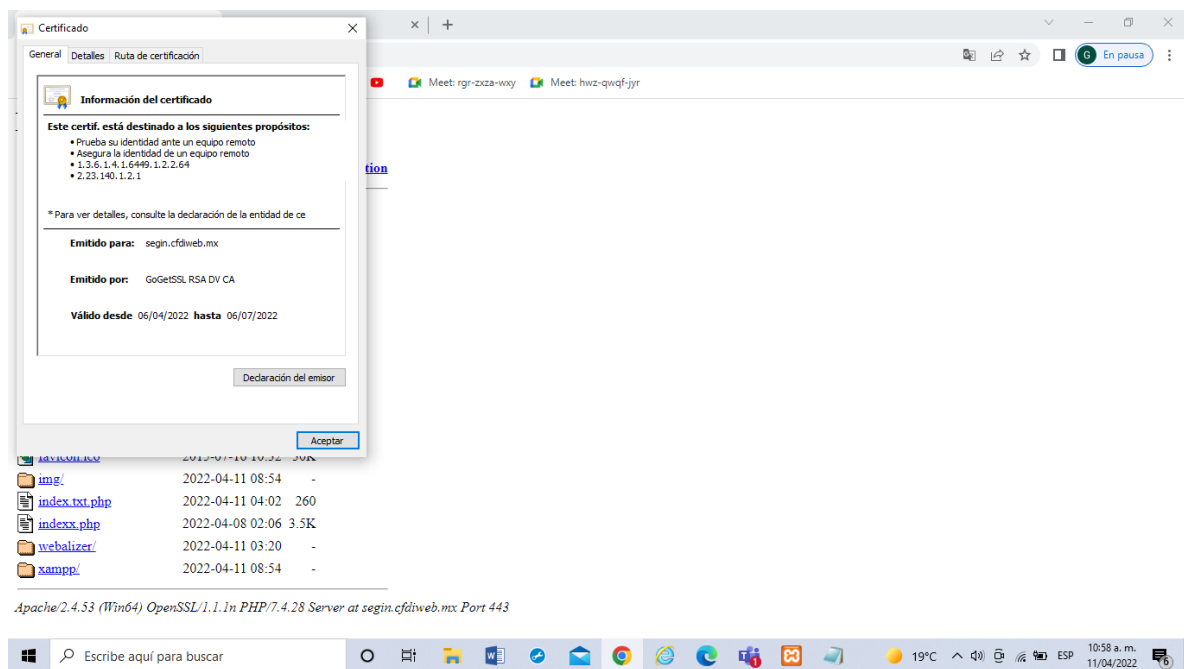
Una vez realizados estos cambios seleccionamos guardar todos los cambios provenientes y ahora procederemos a realizar una pequeña revisión sobre nuestra práctica para ver si esto nos fue de utilidad

Cómo se puede observar en las siguientes pantallas ya se muestra que nuestra página principal index se muestra que la conexión Es segura qué la configuración del sitio Es segura y que el certificado Está correcto y está funcionando de una manera segura





También a continuación se muestran los detalles y la información general sobre el certificado sobre cual fue emitido desde cuándo es válido la ruta y los detalles que manejan y así es como podemos hacer el cambio de certificación válida en una página para nuestro correcta seguridad.



Conclusión: Personalmente para mí trabajar esta actividad fue un poco complicada ya que hubieron muchos errores y muchas contratiempos que atravesé para lograr realizar esta actividad, De igual forma me gustó mucho porque así pude saber cómo hacer una buena práctica la relacionada a los certificados de seguridad, a los sniffers y también sobre la importancia de la seguridad informática y el uso de los certificados de seguridad, también así poder conocer sobre todo lo que está relacionado a las certificaciones y a los ataques por sniffer, también lo que está relacionado el xampp siento que aprender Esto me ayudó mucho ya que conocí temas que desconocía y también aprendí más cosas de las que ya sabía poco refuerzo mis conocimientos Además de que tuve que realizar un amplio trabajo de investigación para poder solucionar los temas que tenía pendientes y los errores que me provocaba el realizar esta práctica para mí de verdad que fue un alivio cuándo por fin pude acceder a la correcta certificación desde mi navegador ya que tuve que proseguir muchos pasos y bastantes horas de tiempo para poder lograrlo me gustó mucho conocer de este tema y siento que es de mucho conocimiento del que pueda abarcar.

