

Texto

Descripción generada automáticamente con confianza mediaTexto

Descripción generada automáticamente



# **Índice**

[Índice 2](#_Toc135871322)

[Instrucciones 3](#_Toc135871323)

[¿Qué se hizo? 11](#_Toc135871324)

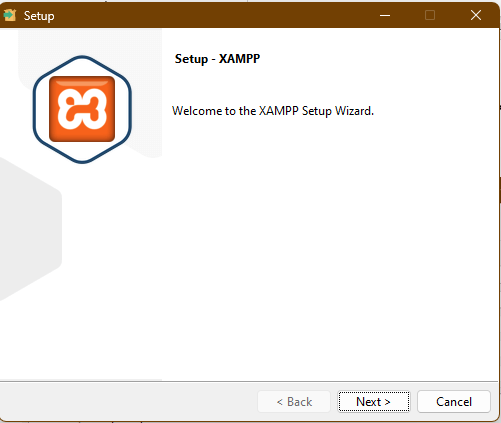
[¿Cómo se resuelve? 12](#_Toc135871325)

[¿Cómo se puede mitigar ese problema? 14](#_Toc135871326)

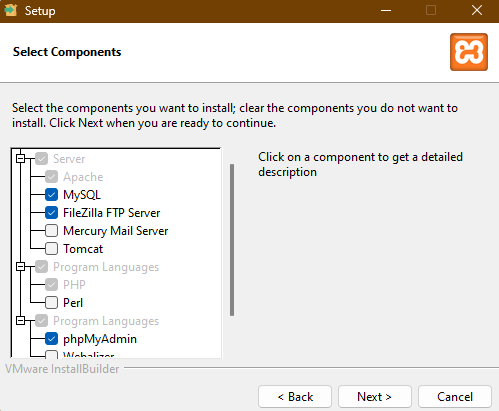
[Conclusiones 15](#_Toc135871327)

# **Instrucciones**

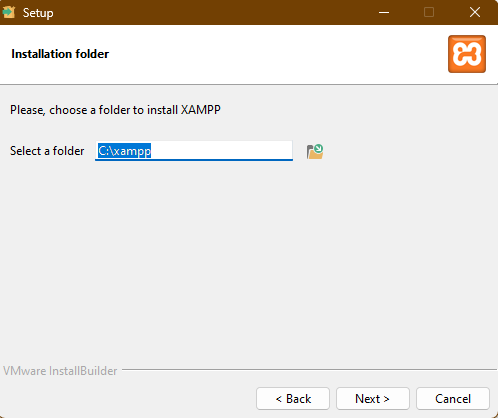
1. Clonar el repositorio <https://github.com/quintanaesc/ProyectoCokisFB.git>
2. Descargar xampp de <https://www.apachefriends.org/es/download.html>
3. Una vez descargado, comenzar la instalación.



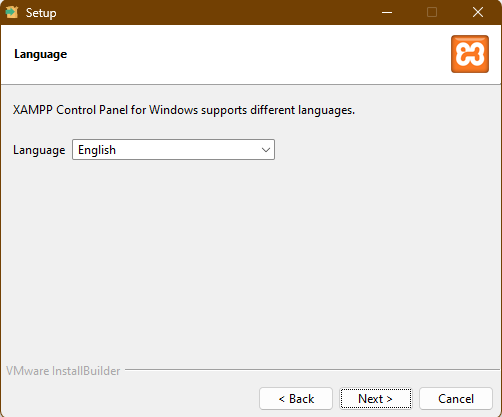
1. Seleccionar sólo lo que vamos a ocupar.



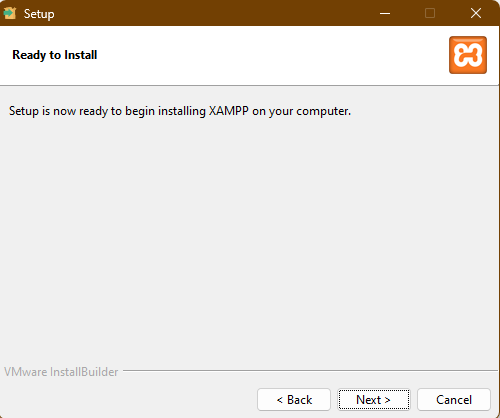
1. Seleccionar el lugar de instalación.



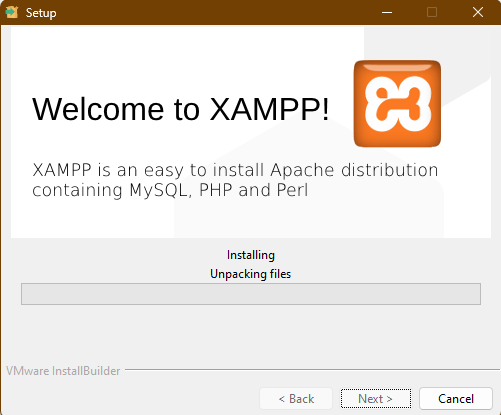
1. Seleccionar el idioma.



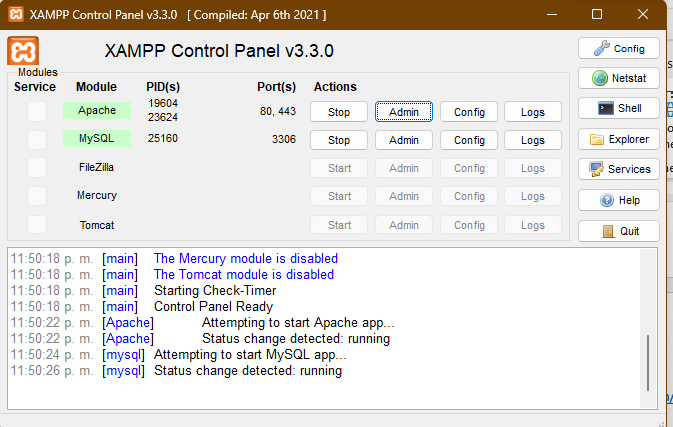
1. Una vez acabada la configuración, comenzar con la instalación.



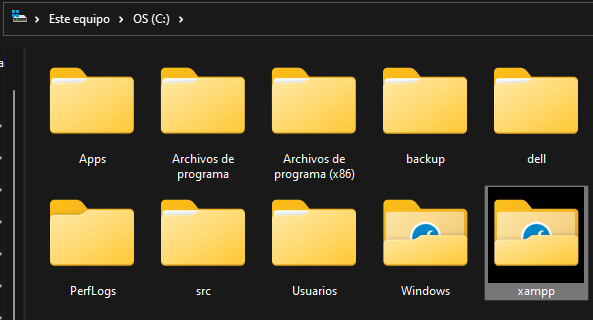
1. Esperar a que acabe la instalación.



1. Si hay algún problema en la instalación o no corre correctamente, se puede usar el siguiente vídeo de guía: <https://www.youtube.com/watch?v=xXkKeojOb1A&t=231s>
2. Una vez instalado, podemos comenzar nuestra configuración para abrir el servidor.



1. Ubicamos la carpeta donde se instaló Xampp



1. Buscamos la carpeta llamada “htdocs”

Interfaz de usuario gráfica, Aplicación

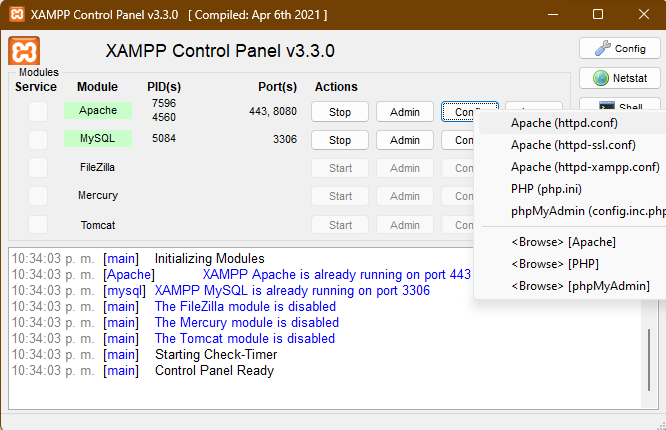
Descripción generada automáticamente

1. Copiamos los archivos que descargamos del repositorio y los pegamos en esa carpeta:

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Ya teniendo los archivos ahí, nos dirigimos a Xampp y apretamos el botón “Config” de “Apache”.



1. Presionamos la primera opción (Apache (httpd.conf))
2. Nos va a abrir un bloc de notas, en el cual con el buscador (Ctrl + b), ubicaremos la palabra “htdocs”.

Captura de pantalla de un celular

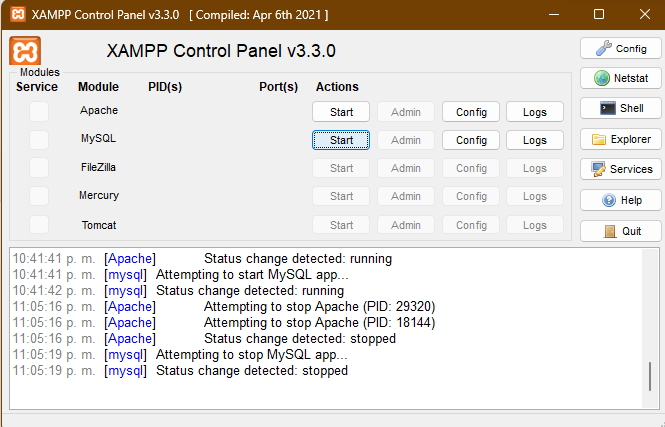
Descripción generada automáticamente

1. Le agregamos el nombre de nuestro directorio y guardamos.

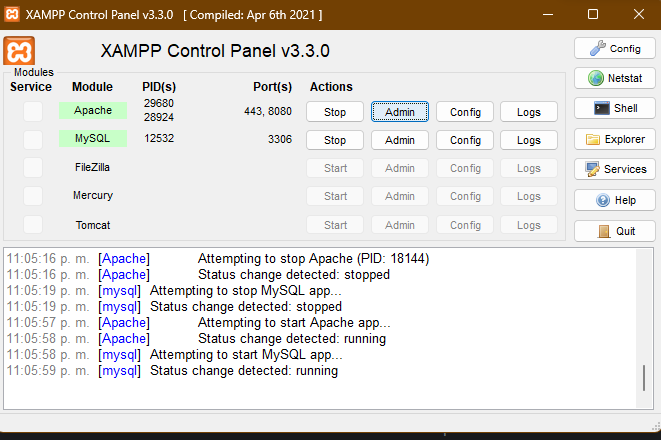
Texto

Descripción generada automáticamente

1. Reiniciamos Apache y MySQL.



1. Y ya tendremos listos nuestros servicios. Podemos entrar de varias maneras:
2. Dando click en “Admin” de “Apache”

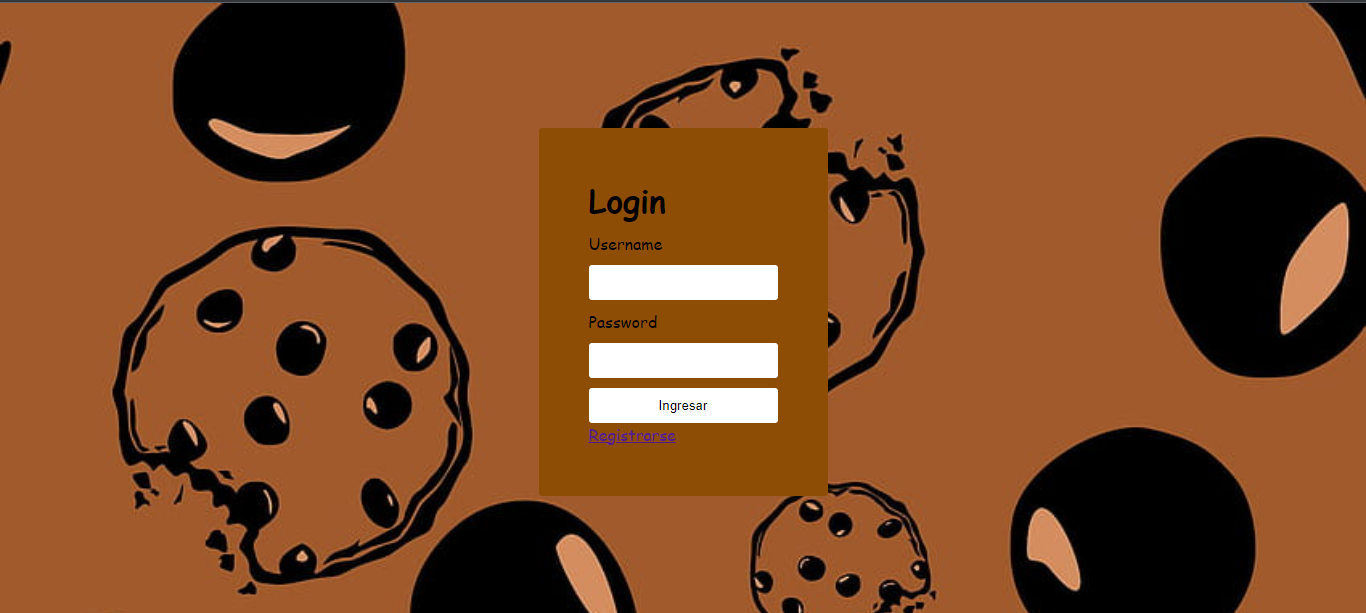


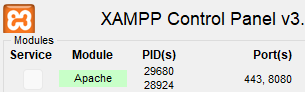
Y nos va a abrir el localhost

Interfaz de usuario gráfica, Texto, Correo electrónico

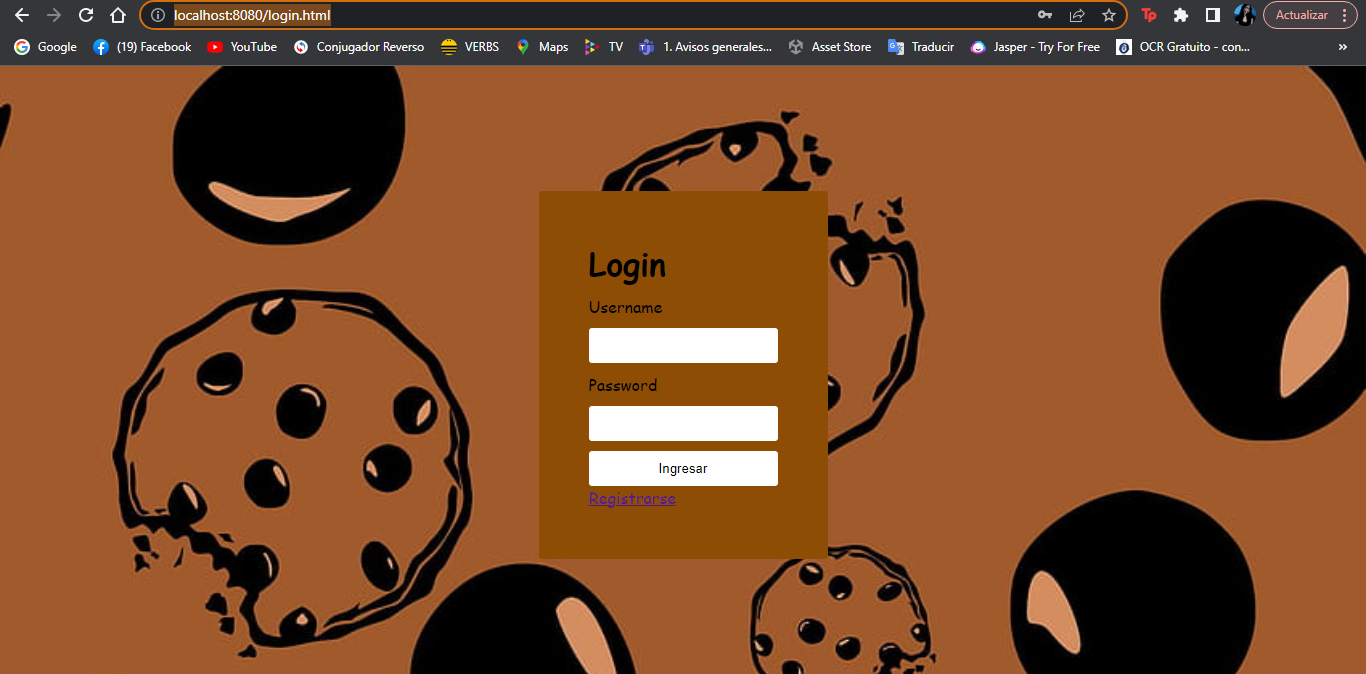
Descripción generada automáticamente

Ya sólo seleccionamos el html de login y ya tenemos acceso a la página de ingreso.



1. Nos vamos directamente al navegador de su preferencia y colocamos en el buscador “localhost”, el cual nos va a volver a dirigir a la página que muestra los archivos, seleccionamos el html de login y accedemos.
2. En el mismo navegador colocamos en el buscador “localhost” acompañado del puerto, el cual lo va a indicar Xampp: 

En éste caso, colocamos “localhost:8080” para que nos rediriga directamente a la página de login.



# **Imagen en blanco y negro Descripción generada automáticamente con confianza media¿Qué se hizo?**

# **¿Cómo se resuelve?**

**¿Qué tecnologías se usaron?**

# **¿Cómo se puede mitigar ese problema?**

Para mitigar el problema de la modificación no autorizada de cookies y el acceso no autorizado a datos, es importante seguir las mejores prácticas de seguridad en la gestión de cookies:

* Utilizar el atributo HttpOnly: Configurar las cookies con el atributo HttpOnly, lo que evita que sean accesibles mediante scripts del lado del cliente. Esto ayuda a prevenir ataques de secuestro de cookies a través de scripts maliciosos.
* Establecer tiempos de expiración adecuados: Configurar tiempos de expiración razonables para las cookies. Evitar que las cookies tengan tiempos de vida demasiado largos, lo que reducirá la ventana de oportunidad para posibles ataques.
* Validar y sanitizar los datos de las cookies: Antes de utilizar los datos almacenados en las cookies, asegurar de validarlos y sanitizarlos adecuadamente para prevenir inyecciones de código malicioso o manipulación no autorizada.
* Mantener las aplicaciones y servidores actualizados: Mantener las aplicaciones y servidores actualizados, con los últimos parches de seguridad. Esto ayuda a mitigar posibles vulnerabilidades conocidas que podrían ser explotadas para manipular cookies o acceder a datos no autorizados.
* Realizar pruebas de seguridad: Realizar pruebas de seguridad periódicas en la aplicación para identificar posibles vulnerabilidades y corregirlas antes de que sean aprovechadas por atacantes.

# **Imagen en blanco y negro Descripción generada automáticamente con confianza mediaConclusiones y experiencias**

En conclusión, la realización del CTF es una excelente manera de reforzar y poner a prueba nuestras habilidades y conocimientos en la asignatura, y crear un desafío propio agrega un nivel adicional a nuestra creatividad y personalización.

En este caso, el desafío se centró en automatizar cookies por fuerza para encontrar el usuario.

Bajo el contexto de un CTF donde realizamos pruebas en un entorno controlado, el uso de fuerza bruta puede ser una técnica que nos puede ayudar a resolver desafíos y aprender sobre las vulnerabilidades que existen con medidas adecuadas de seguridad.

Es importante destacar que el objetivo principal de nuestro CTF es promover el aprendizaje y mejorar nuestras habilidades en esta área. Al diseñar y realizar este desafío propio, no comprometemos la seguridad o privacidad de otros sistemas o personas fuera de nuestro entorno controlado del CTF.

En general, nuestra experiencia fue

* Paola:
* Ricardo:
* Diana:
* Roberto: