PROYECTO 2

BASES DE DATOS

Curso 2021-22

GESTIÓN DE ACCESOS SEGUROS SSL A UNA BASE DE DATOS

1. Objetivos Generales

- Comprensión del proceso de gestión y administración de perfiles de usuarios con acceso seguro a una Base de Datos.
- Crear la infraestructura de certificados X.509 necesaria para incorporar servicios de seguridad en el acceso a una Base de Datos.
- Configurar y establecer de forma práctica sesiones seguras SSL en MySQL.
- Captura del tráfico SSL en el acceso a la Base de Datos.

2. Objetivos específicos

El alumno será capaz de:

- Arrancar un SGBD (Sistema Gestor de Bases de Datos) con la configuración necesaria para administrar servicios de seguridad.
- Crear y administrar cuentas de usuario que requieran el protocolo SSL.
- Crear y administrar cuentas de usuario que requieran el protocolo SSL y exijan la autenticación del cliente
- Capturar y analizar tráfico SSL generado en el acceso al SGBD.

3. Metodología

El alumno dispone del software "*MÁQUINA VIRTUAL CURSO*" del enlace especificado en el apartado 4.4.

Este software contiene una *Máquina Virtual* en la cual está disponible un gestor de *Bases de Datos MySQL* a través de un paquete portable *XAMPP*. Así mismo la *Máquina Virtual* dispone de un *cliente* para acceder al *SGBD* (*Workbench*) que se debe de utilizar para hacer la práctica. El paquete XAMPP contenido en la máquina virtual está configurado y listo para ser utilizado.

El paquete *XAMPP* dispone de una herramienta administrativa denominada "*phpMyadmin*" la cual utilizaremos en determinados aspectos de la gestión de cuentas, visualización de tablas de privilegios y variables relativas a los accesos seguros.

Adicionalmente, la *MÁQUINA VIRTUAL CURSO* dispone de una herramienta de captura de tráfico denominada *Wireshark* que la utilizaremos en un apartado de esta práctica.

La ventaja de utilizar la *MÁQUINA VIRTUAL CURSO* es que el alumno no necesita instalar en su sistema ningún *SGBD MySQL*. El alumno hará las prácticas propuestas y el profesor evaluará los resultados obtenidos dentro de la máquina virtual. Adicionalmente, el profesor podrá solicitar al alumno personalmente la aclaración de algún aspecto de la entrega realizada.

4. Contenidos

Los alumnos del Grupo de Prácticas deberán crear la infraestructura necesaria en el SGDB de la *MÁQUINA VIRTUAL DEL CURSO* para que se puedan crear perfiles de usuarios con servicios de seguridad. Estos usuarios tendrán distintos privilegios relacionados con el protocolo SSL que se especificarán a continuación.

Los alumnos del Grupo de Prácticas deberán asimismo capturar el tráfico de una consulta a la Base de Datos de la *MÁQUINA VIRTUAL DEL CURSO* accediendo desde clientes de la misma máquina virtual del alumno.

4.1 Creación de la infraestructura de seguridad en el servidor (SGBS) y en el cliente (usuario)

Los alumnos del Grupo de Prácticas deberán crear la infraestructura necesaria para que el SGBD (servidor) arranque con los certificados digitales necesarios para que se puedan gestionar accesos seguros SSL. Esto significa que deberá crear los certificados digitales necesarios en el servidor y además deberá actualizar el fichero de configuración "*my.ini*" de MySQL. Además, deberán crear la infraestructura necesaria del lado del cliente (usuario que se conecta a la BD) para que disponga de los certificados digitales necesarios. En concreto, los alumnos del Grupo de Prácticas deberán:

- Crear una Autoridad de Certificación utilizando la plataforma OpenSSL: Fichero: *CACertificado.pem.* Obligatoriamente el campo "Common Name"= "**CA_GrupoX_22**". *(Siendo "Grupo" el número de grupo de prácticas del curso actual. P.e. el "Common Name" del Grupo de Prácticas 1 del curso actual sería "CA_G1_22").*

- Crear un certificado de servidor (SGBD) a utilizar en las conexiones SSL firmado por la Autoridad de Certificación anterior utilizando la plataforma OpenSSL: Fichero *SR_Certificado.pem*. Obligatoriamente el campo "Common Name"= "**SR_GrupoX_22**". A su vez, el protocolo SSL del SGBD deberá disponer de la clave privada asociada a dicho certificado. Fichero: *SR_ClavePrivada.pem. (Siendo "Grupo" el número de grupo de prácticas del curso actual. P.e. el "Common Name" del Grupo de Prácticas 1 del curso actual sería "SR_G1_22").*

- Crear un certificado de cliente a utilizar en las conexiones SSL con autenticación de cliente firmado por la Autoridad de Certificación anterior utilizando la plataforma OpenSSL: Fichero *CL_Certificado.pem*. Obligatoriamente el campo "Common Name"= "**CL_GrupoX_22**". A su vez, el protocolo SSL del cliente (usuario) deberá disponer de

la clave privada asociada a dicho certificado. Fichero: *CL_ClavePrivada.pem. (Siendo "Grupo" el número de grupo de prácticas del curso actual. P.e. el "Common Name" del Grupo de Prácticas 21 del curso actual sería "CL_G1_22").*

- Incorporar en el fichero de configuración de MySQL ("*my.ini*") los *paths* en los que se encuentran los certificados del servidor. Todos los alumnos utilizarán la misma ubicación para colocar los certificados digitales del servidor (SGBD). Esta ubicación será:
  "C:/xampp/mysql/CONFIGURACION_MYSQL_SSL/SERVER/"

El alumno dispondrá de la documentación contenida en el fichero "*BD_ACCESO_SSL.pdf*" que se encuentra en el enlace del material de la asignatura para la realización de esta parte de la práctica. Además, dispone de videos que se pueden descargar de los enlaces contenidos en el apartado 7.

4.2 Creación de usuarios con privilegios de seguridad

El alumno deberá crear en el SGBD y utilizando las sentencias SQL necesarias los usuarios que se especifican a continuación con los privilegios indicados:

- ***clssl0_GrupoX_22/ssl (login/password):*** Cliente al que se le exige el protocolo SSL sin Autenticación de usuario. *(Siendo "Grupo" el número de grupo de prácticas del curso actual. P.e. el usuario/pass que deberá crear el Grupo de Prácticas 1 del curso actual sería "clssl0_G1_22/ssl").*

- ***clssl_GrupoX_22/ssl (login/password):*** Cliente al que se le exige el protocolo SSL con Autenticación de usuario. *(Siendo "Grupo" el número de grupo de prácticas del curso actual. P.e. el usuario/pass que deberá crear el Grupo de Prácticas 1 del curso actual sería "clssl_G1_22/ssl").*

El alumno deberá asimismo crear en el cliente (*Workbench*) los perfiles de los usuarios anteriores para la posterior verificación de los privilegios otorgados. Nótese que hay que configurar el *path* de los certificados del cliente, en el menú del *Workbench*.

El lugar en el que todos los alumnos deberán ubicar los certificados del cliente deberá ser:

C:\Archivos de programa\MySQL\CONFIGURACION_MYSQL_SSL\CLIENTE_SSL

El alumno dispondrá de la documentación contenida en el fichero "*BD_ACCESO_SSL.pdf*" que se encuentra en el enlace del material de la asignatura para la realización de esta parte de la práctica. Además, dispone de videos que se pueden descargar de los enlaces contenidos en el apartado 7.

4.3 Capturas de tráfico SSL

El alumno deberá capturar el tráfico originado por una conexión SQL desde un *cliente_SSL0* (sin autenticación) al SGBD y desde un *cliente_SSL* (con autenticación) al SGDB. Todo ello se

hará dentro de la Máquina Virtual. El procedimiento para realizar esta captura de tráfico está explicado en la documentación contenida en el fichero "*BD_ACCESO_SSL.pdf*" que se encuentra en el enlace del material de la asignatura para la realización de esta parte de la práctica y en los videos que se pueden descargar de los enlaces contenidos en el apartado 7. En concreto, en el *video 9*.

4.4 Enlace Descarga Software

http://www.personal.fi.upm.es/~lmengual/bases_datos/descargas_mv_bd.html

5. Entrega de la Práctica

El responsable en cada Grupo de Prácticas deberá subir OBLIGATORIAMENTE a la *plataforma Moodle* **en una tarea habilitada para ello un único fichero comprimido (*.zip, *.rar, o *.7z) cuyo nombre sea (Grupo_X_Proyecto2.rar) que contenga:**

1. **Los ficheros:** CACertificado.pem, SR_Certificado.pem, SR_ClavePrivada.pem, CL_Certificado.pem, CL_ClavePrivada.pem.
2. **El fichero de configuración de MySQL"*my.ini*"** con el *path* en los que se encuentran los certificados del servidor.
3. **Dos ficheros de capturas.** Uno que contenga las capturas de tráfico obtenidas con la herramienta *Wireshark* de una conexión SQL-SSL de un cliente sin autenticación (**captura*_clssl0_GrupoX_22.pcapng***) y otro fichero de capturas que contenga las capturas de una conexión de un cliente con autenticación (**captura*_clssl_GrupoX_22.pcapng***).
4. **Un fichero de texto conteniendo el número de grupo de prácticas y, de todos los miembros del grupo**, los nombres, apellidos, direcciones de correo electrónico, número de matrícula y grupo de matriculación.

En el proceso de evaluación de la práctica se puede exigir a un grupo de prácticas que demuestren el funcionamiento de su configuración. Para ello el profesor se pondrá en contacto con el grupo de Prácticas.

La fecha tope de subida OBLIGATORIA de los ficheros al Moddle se establecerá en una nota en la página de la asignatura.

6. Consultas acerca del desarrollo del ejercicio práctico

Cualquier duda acerca del desarrollo del ejercicio práctico se podrá resolver en el despacho 4303 (Luis Mengual) o alternativamente en la dirección de correo lmengual@fi.upm.es o utilizando la plataforma *Moodle* de la asignatura.

7. Enlaces descarga Videos

- VIDEO 1: CREAR CERTIFICADO CA

https://drive.upm.es/index.php/s/gdKiSm7SkioBJZH

- VIDEO 2: CREAR CERTIFICADO SR (SGBD)

https://drive.upm.es/index.php/s/gSAEM9hae53kiJp

- VIDEO 3: CREAR CERTIFICADO CL

https://drive.upm.es/index.php/s/5yHkUcLVFEivdCR

- VIDEO 4: PRUEBA HAVE_SSL

https://drive.upm.es/index.php/s/zOGxMOXOcGsmk2P

- VIDEO 5: CONEXION SSL-CONFIGURACION MANUAL

https://drive.upm.es/index.php/s/2B2VLlpGGl5u3LT

- VIDEO 6: CONEXION SSL-CONFIGURACION AUTOMATICA

https://drive.upm.es/index.php/s/qjrmDSJDssb9PXT

- VIDEO 7: CONFIGURACION CLIENTE_SSL0

https://drive.upm.es/index.php/s/PXiAa94b6mUOQQr

- VIDEO 8: CONFIGURACION CLIENTE_SSL

https://drive.upm.es/index.php/s/6szxlz94c7wUJtG

- VIDEO 9: CAPTURA TRÁFICO SSL

https://drive.upm.es/index.php/s/888HFILEosdogwv

8. Enlace Documentación

http://www.personal.fi.upm.es/~lmengual/bases_datos/BD_ACCESO_SSL.7z

http://www.personal.fi.upm.es/~lmengual/bases_datos/BD_ACCESO_SSL_PN.7z

Paquete XAMPP*

*Versión paquete portable XAMPP descargada de http://www.apachefriends.org/en/xampp-windows.html#641 con fines docentes

A1. 1 Paquete XAAMP

Con el fin de facilitar la tarea de la realización de las prácticas propuestas en la asignatura de Bases de Datos se proporciona el software "*PAQUETE XAMPP PRÁCTICAS SQL*". Este paquete es una versión del software *XAMPP* de libre distribución (GNU General Public License).

Este paquete software contiene un gestor de *Bases de Datos Mysql* que se propone para hacer las prácticas de la asignatura. La ventaja de utilizar este paquete es que el alumno no tiene que instalar ningún servicio ni ninguna aplicación en su sistema.

Este paquete aparece integrado en la Máquina Virtual del curso. En este caso el paquete ya está configurado y listo para ser usado.

En este momento alumno podrá utilizar las aplicaciones incluidas en el paquete *XAMPP*. Para la práctica propuesta el alumno deberá pinchar en primer lugar el botón "*start*" de la aplicación "*Apache*". Si todo ha ido bien deberá aparecer la palabra "*running*" resaltada de color verde a la altura del nombre de la aplicación como se aprecia en la figura A4. A continuación deberá pinchar el botón "*start*" de la aplicación "*Mysql*". Si todo ha ido bien deberá también aparecer la palabra "*running*" resaltada de color verde a la altura del nombre de la aplicación como se aprecia en la figura A1.1.

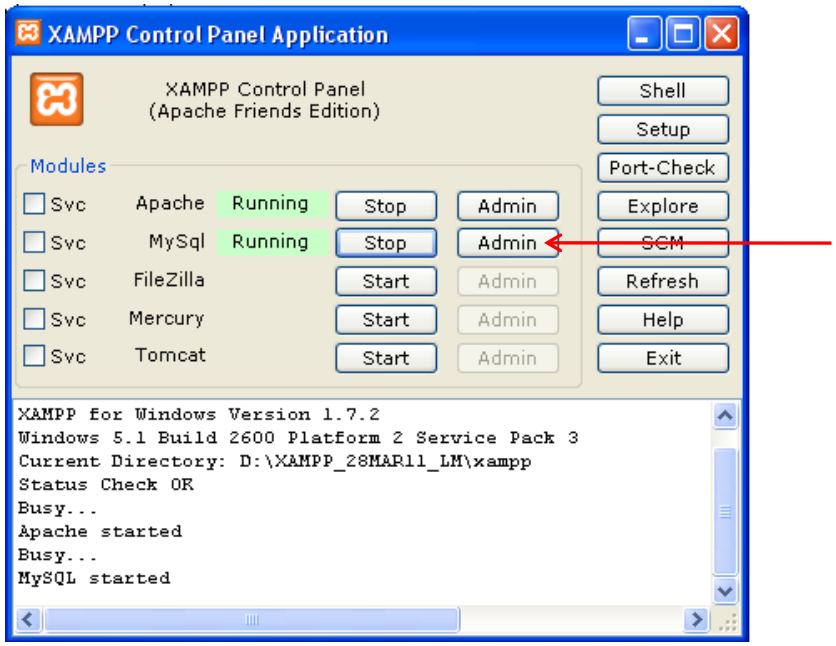

Figura A1.1

Ahora, el alumno puede pinchar el botón "*Admin*" del panel de control del paquete *XAMPP* (ver Figura A4). De este modo el alumno accede al entorno denominado "*phpMyAdmin*" el cual es una aplicación web de acceso administrativo al gestor de Base de Datos *MySQL* . Desde este entorno (ver Figura A1.2) el alumno puede por ejemplo exportar una Base de Datos, ver el diagrama de esquema de una Base de Datos, crear tablas, consultar el estado de las variables de *MySQL*, etc ….

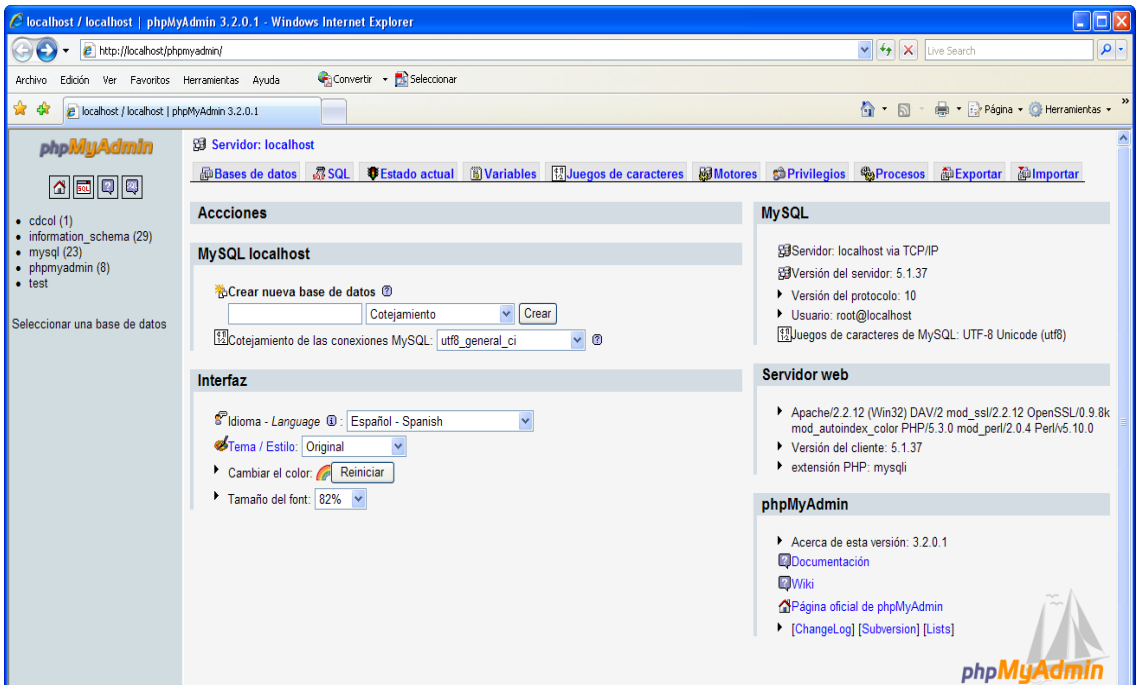

Figura A1.2: Entorno Administración "*phpMyAdmin*"

Se recomienda, no obstante, que el alumno utilice un cliente, por ejemplo, el *"MySQL Workbench"* para conectarse al Servidor *MySQL* y realizar consultas *DDL (Data Definition Language)* y *DML (Data Manipulation Language),* dejando el entorno "*phpMyAdmin*" para tareas de administración (P.e. exportar una Base de Datos, ver el diagrama de esquema de una Base de Datos o consultar las variables de estado o los usuarios creados. (ver Figura A1.3).

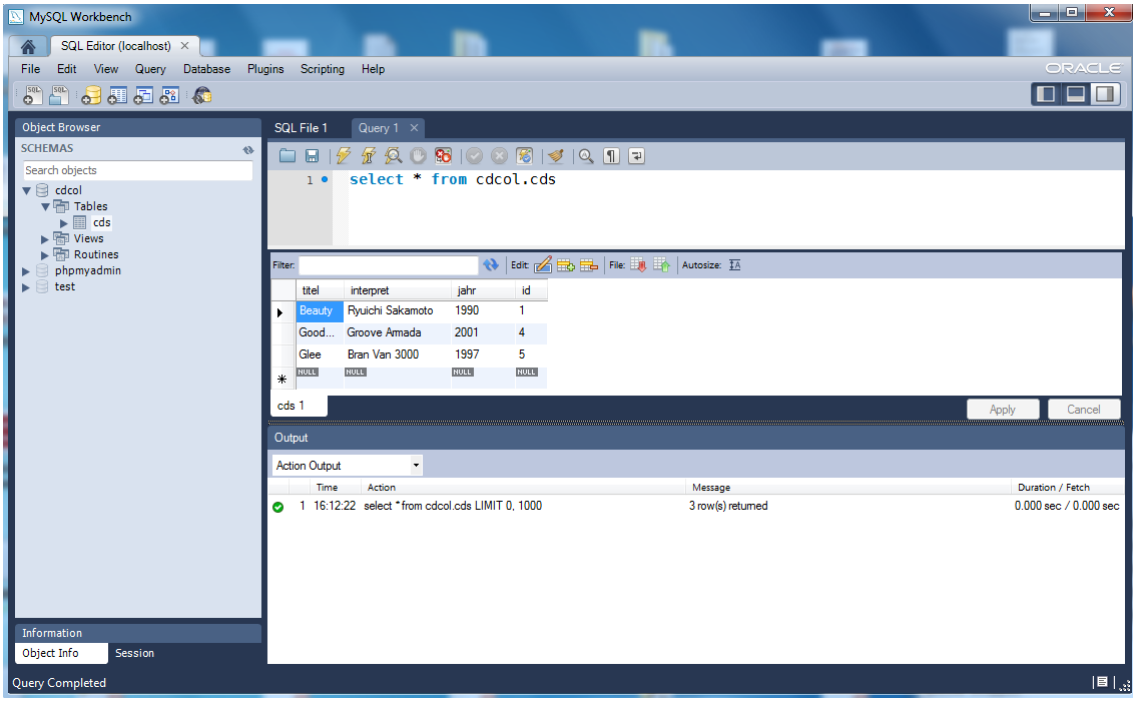

Figura A1.3: Cliente *Workbench*