

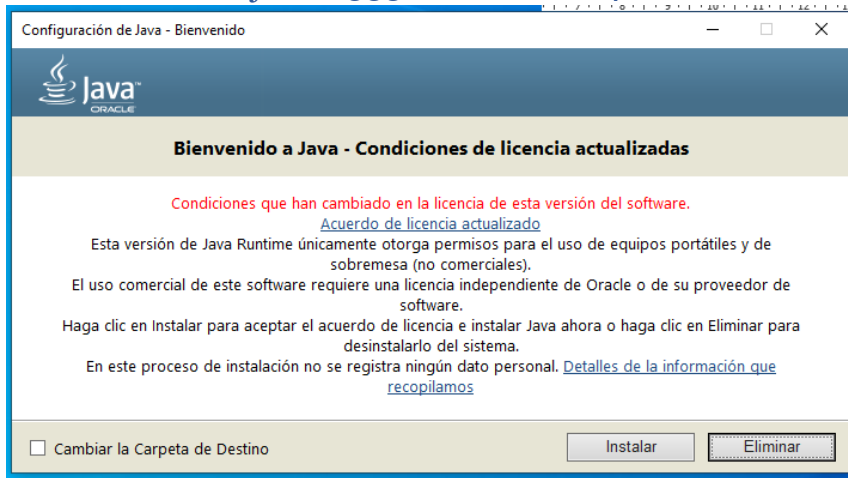
Asignatura	Datos del alumno	Fecha
Seguridad en Bases de Datos y Almacenamiento de Datos Masivos	Apellidos: Paz López	16/06/2022
	Nombre: Angel Ramón	

Contenido

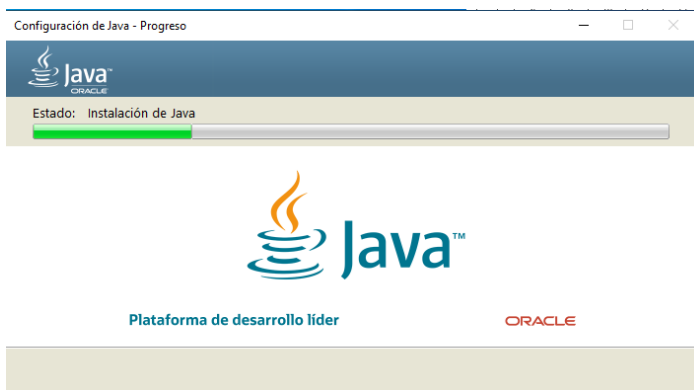
PREPARACION DEL LABORATORIO.....	2
INSTALACION jre-8u333-windows-x64	2
INSTALACION DE APACHE TOMCAT 8.5.....	2
INSTALACION DE MYSQL SERVER 5.5.....	7
INSTALACION WAVSEP	12
VULNERABILIDADES ENCONTRADAS	15
RECOMENDACIONES PARA ELIMINAR/MITIGAR LAS VULNERABILIDADES	18
MAS DETALLES	20
CONCLUSIONES.....	28
REFERENCIAS	29
ANEXOS.....	30

PREPARACION DEL LABORATORIO

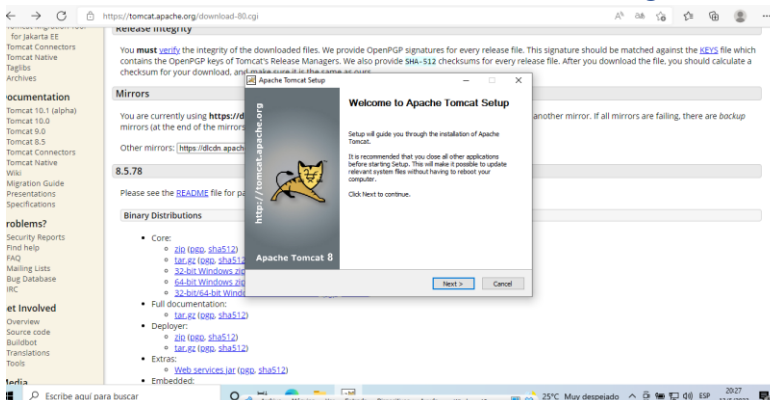
INSTALACION jre-8u333-windows-x64



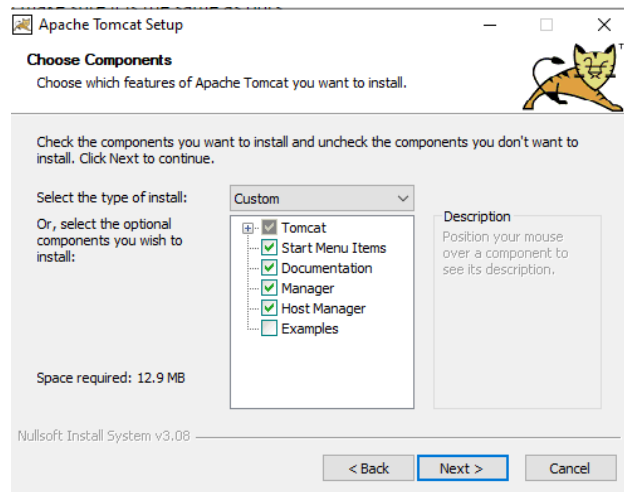
Damos clic en instalar



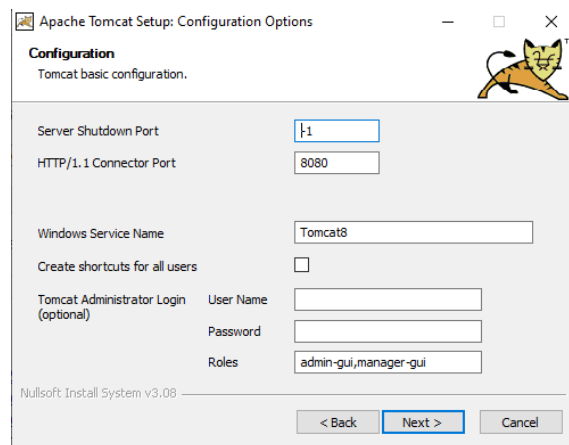
INSTALACION DE APACHE TOMCAT 8.5



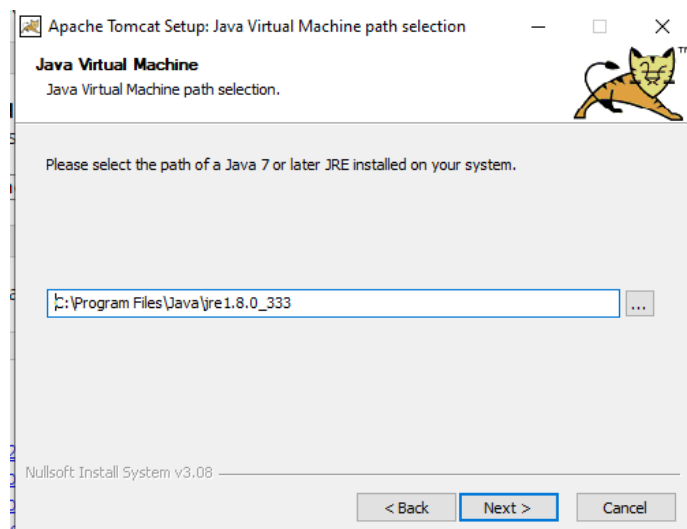
Le damos siguiente hasta llegar a la siguiente ventana



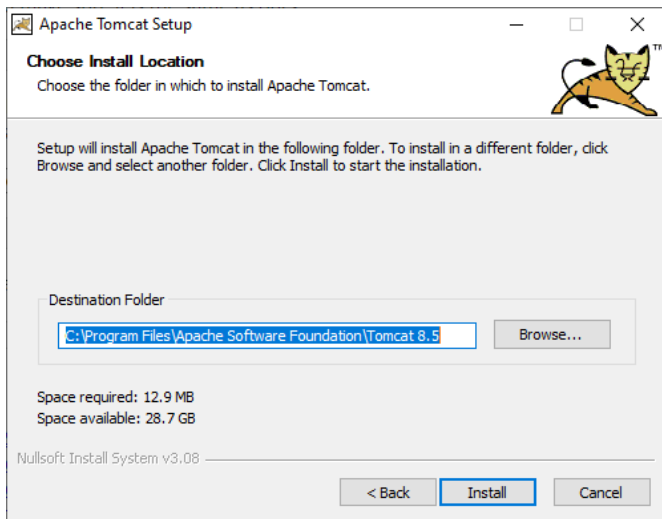
Aquí seleccionamos los componentes que queremos que se instalen y después le damos Next



Ahora nos toca configurar el servidor. Dejamos el puerto 8080, UserName colocamos el Nombre: Admin Password: UNIRBD, después le damos Next

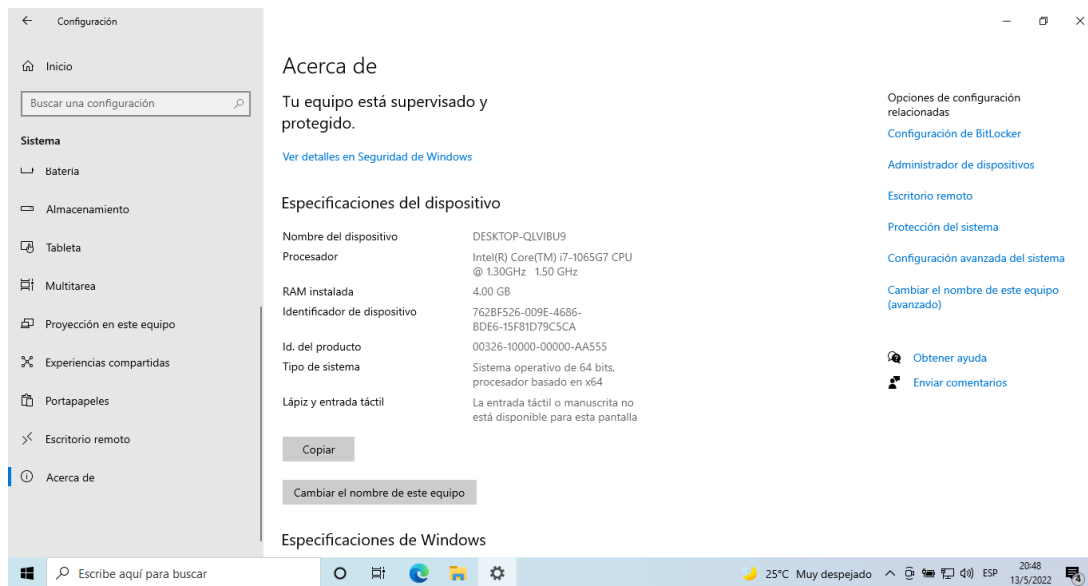


Se verifica el JDK y le damos Next

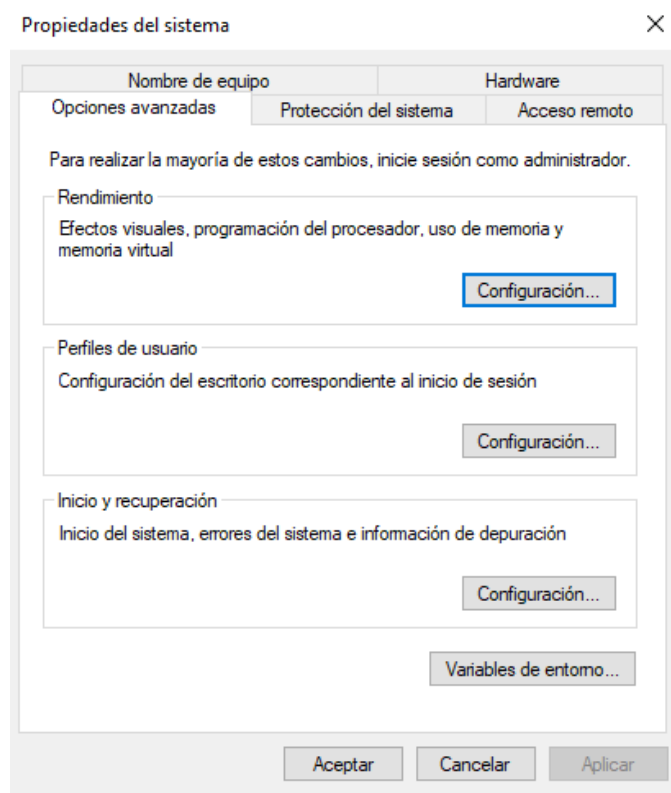


Damos clic en Install para instalar el Tomcat

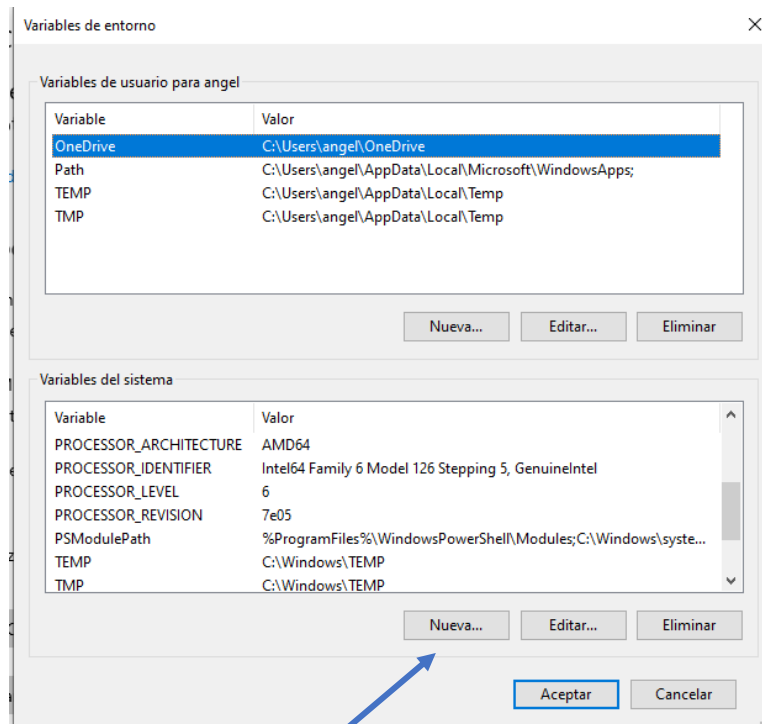
Ahora procedemos a crear las variables del Entorno del Sistema



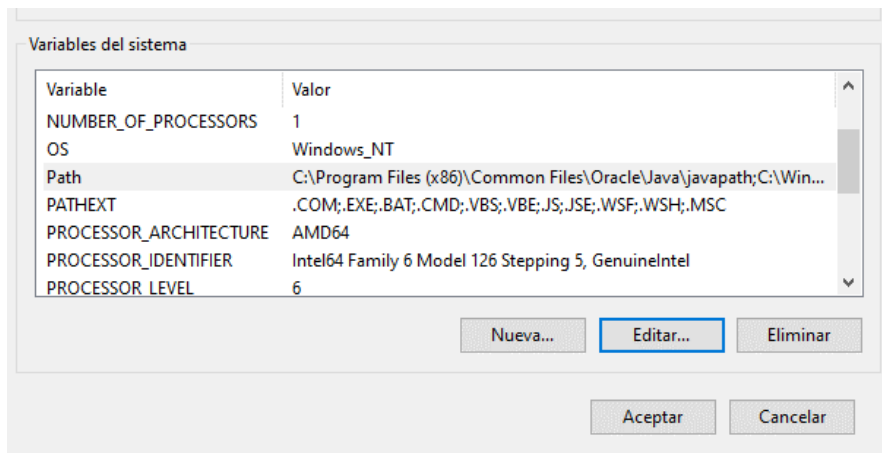
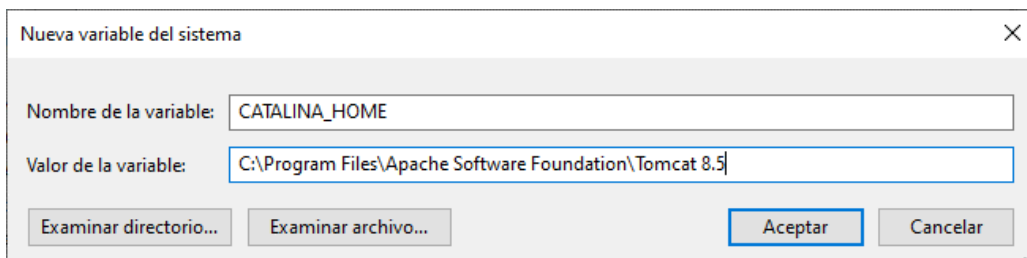
Buscamos la opción configuración avanzada del sistema, en las opciones de la columna de la parte derecha.



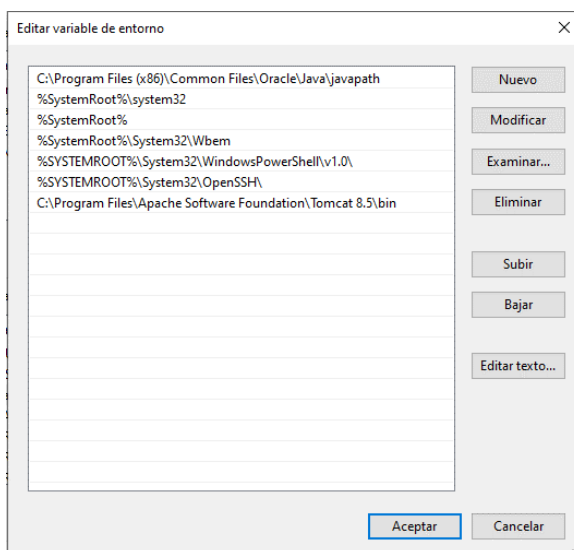
Damos clic en Variables de entorno



Damos clic en el botón Nueva... para crear una nueva variable del sistema



Ahora en Path le damos editar para pegar la dirección de la carpeta bin del Tomcat

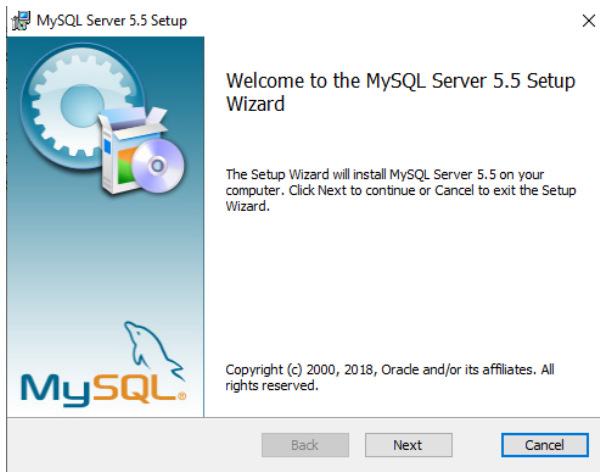


Le damos en Nuevo y pegamos la dirección donde se encuentra la carpeta bin del Tomcat 8.5. Y ya con esto podremos ejecutar el Apache Tomcat. Damos permisos y después abrimos un navegador y colocamos en la URL: <http://localhost:8080/>

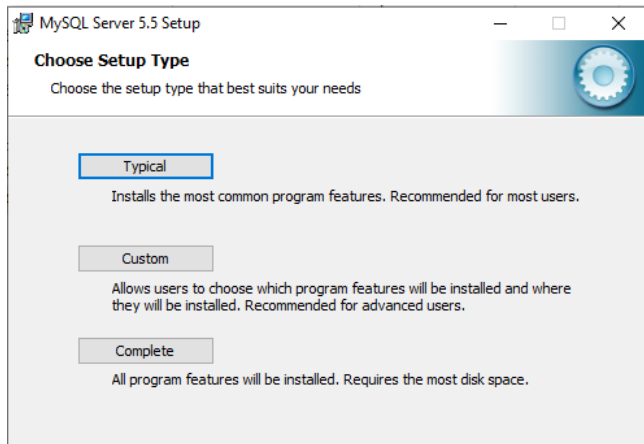
```
C:\Program Files\Apache Software Foundation\Tomcat 8.5\bin\Tomcat8.exe
13-May-2022 21:37:27.529 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Nombre de la versi|n d
del servidor: Apache Tomcat/8.5.78
13-May-2022 21:37:27.622 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Server built:
Mar 31 2022 16:05:28 UTC
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log N|mero de versi|n d
e servidor: 8.5.78.0
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:
Windows 10
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Versi|n de Sistema O
perativo: 10.0
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Arquitectura:
amd64
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:
C:\Program Files\Java\jre1.8.0_333
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:
1.8.0_333-b02
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Vededor JVM:
Oracle Corporation
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:
C:\Program Files\Apache Software Foundation\Tomcat 8.5
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:
C:\Program Files\Apache Software Foundation\Tomcat 8.5
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument
:
-Dcatalina.home=C:\Program Files\Apache Software Foundation\Tomcat 8.5
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument
:
-Dcatalina.base=C:\Program Files\Apache Software Foundation\Tomcat 8.5
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument
:
-Djava.io.tmpdir=C:\Program Files\Apache Software Foundation\Tomcat 8.5\temp
13-May-2022 21:37:27.638 INFORMATION [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument
:
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
```



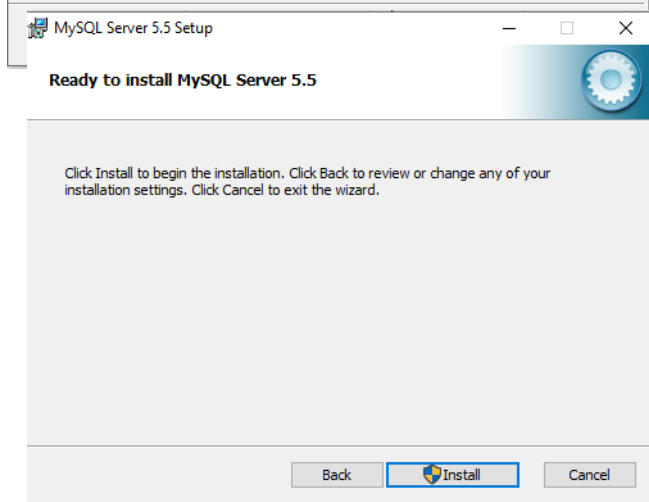
INSTALACION DE MYSQL SERVER 5.5



Una vez ejecutemos le damos clic en Next,
después Aceptamos Acuerdos

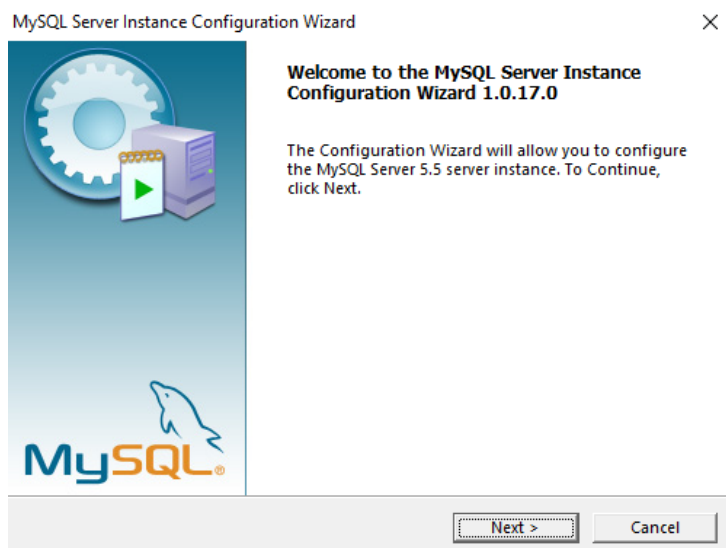


Elegimos instalación Typical

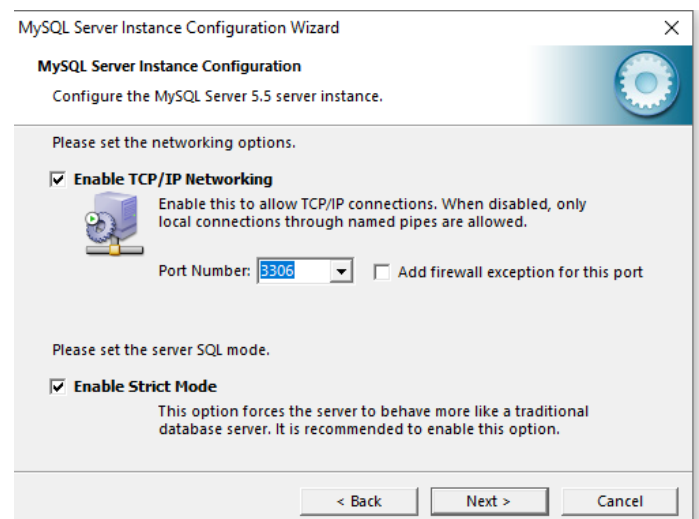
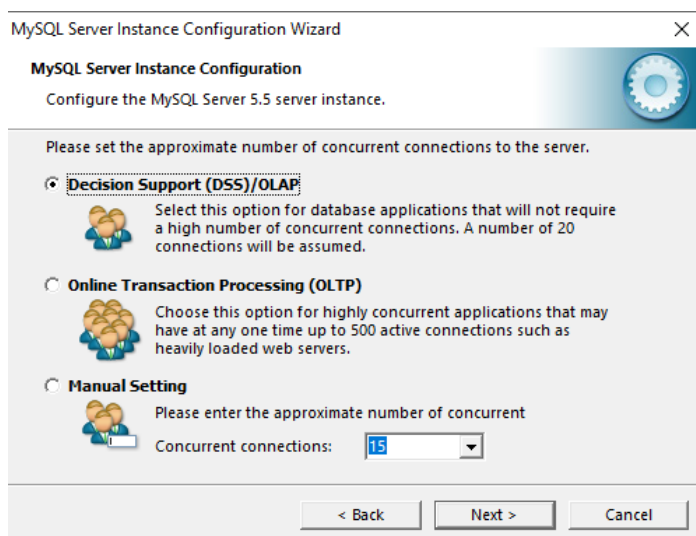
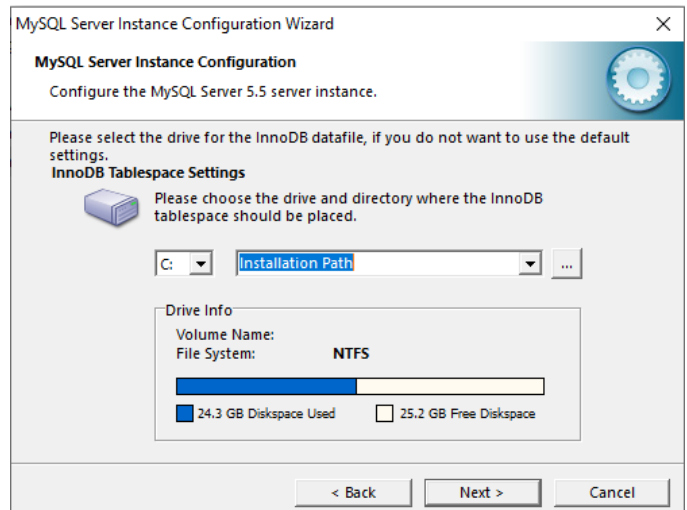
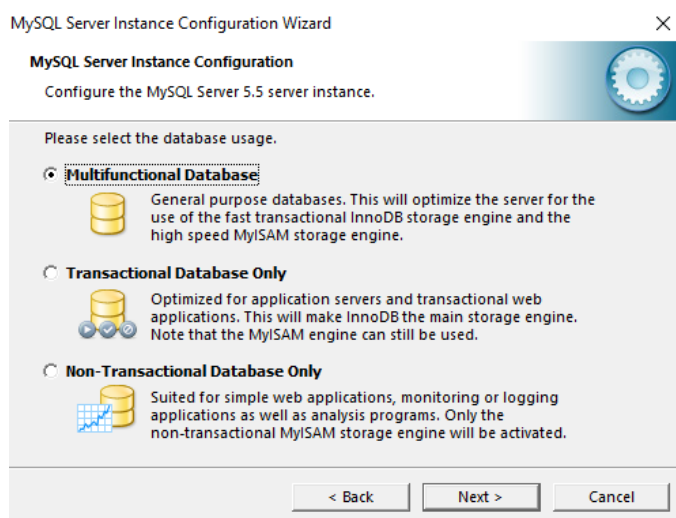
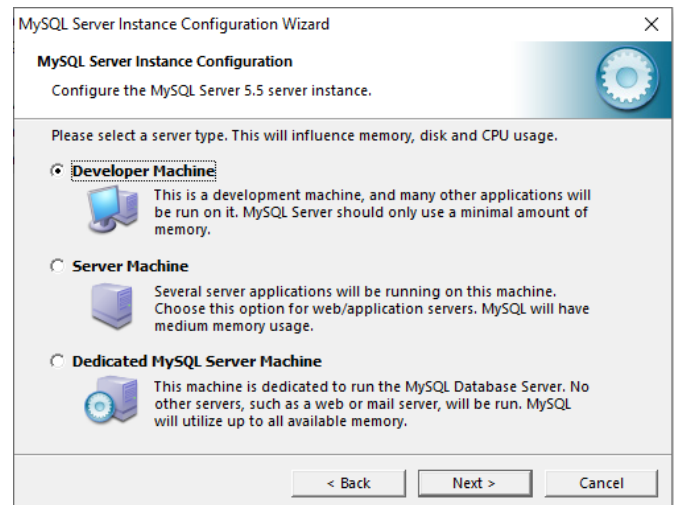
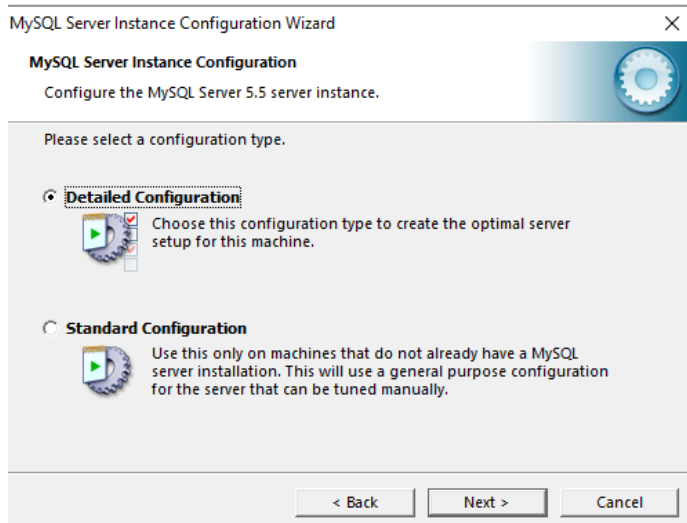


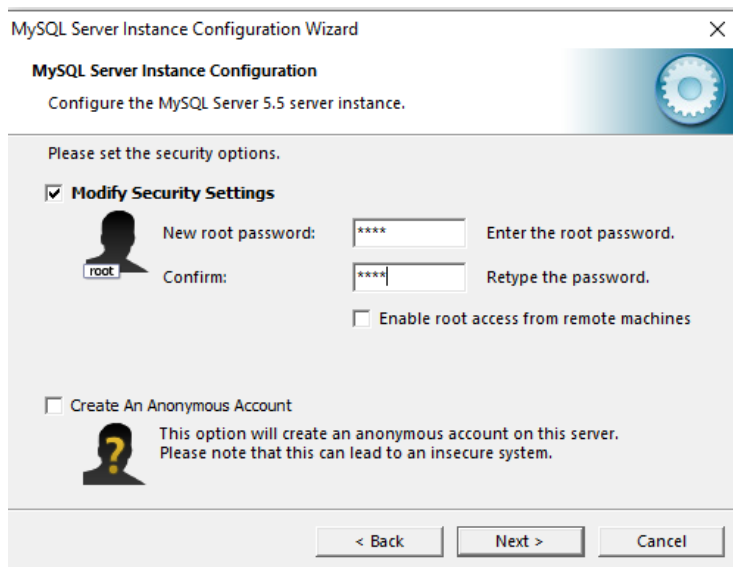
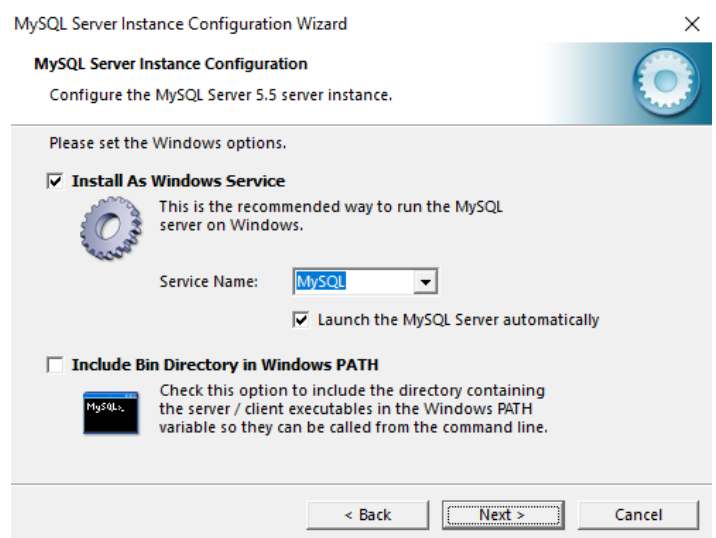
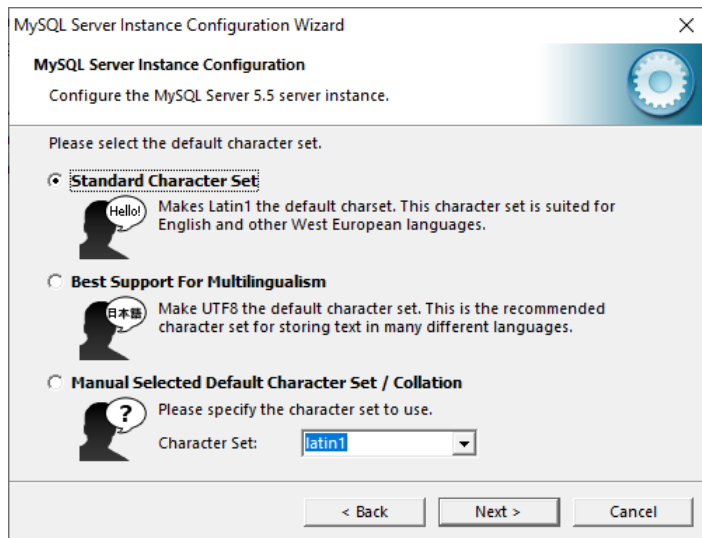
Damos clic en Install y damos
Finish a la última ventana que
aparecera

CONFIGURACION MYSQL

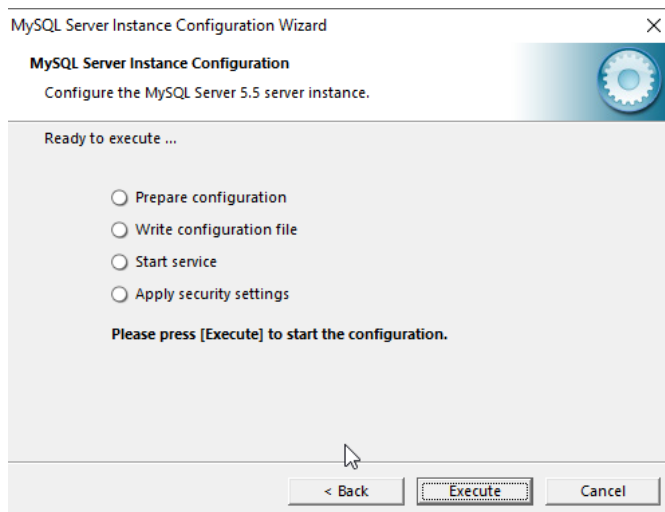


Clic en Next y seleccionaremos
las siguientes configuraciones
y después dando Next a cada
ventana

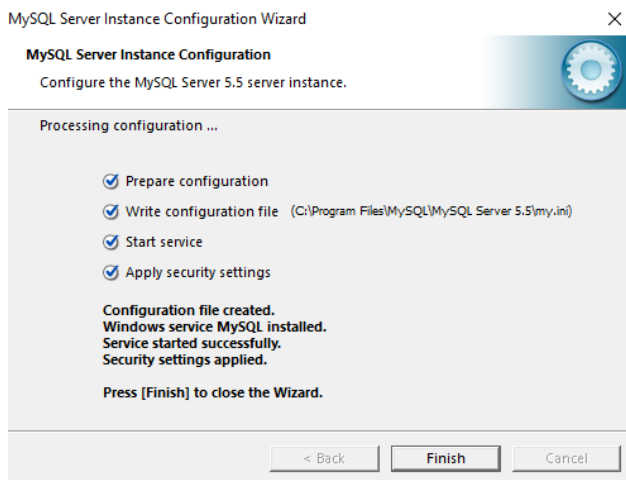




Colocamos una contraseña y la confirmamos y después damos Next

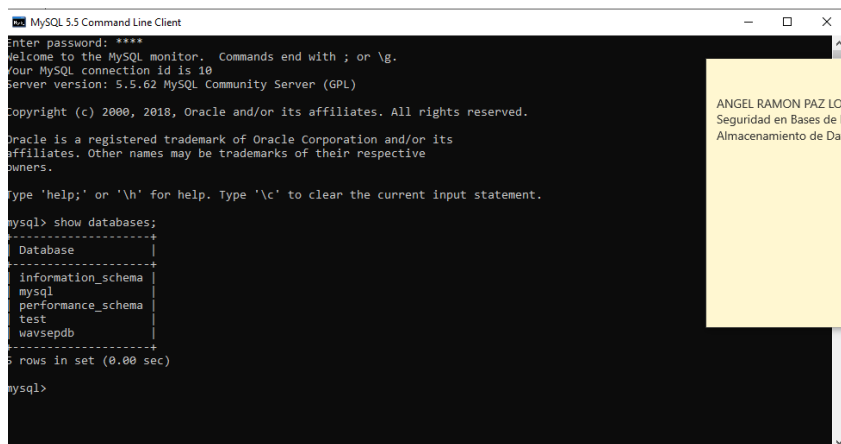


Clic en Execute



Damos en Finish

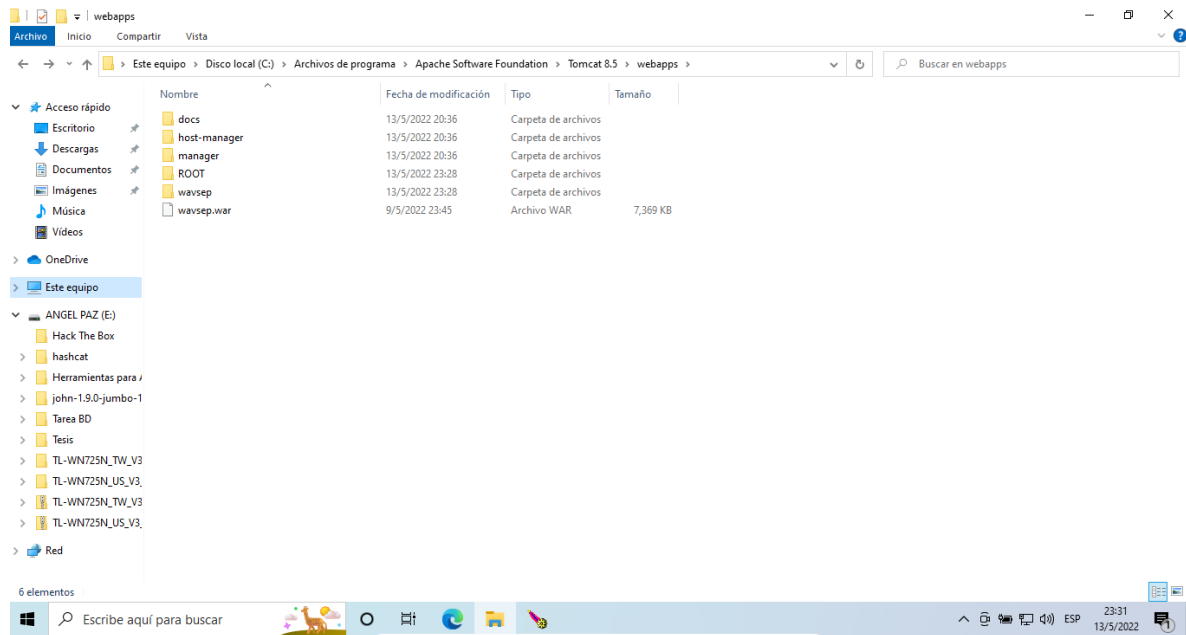
Nos aseguramos que existe la base de datos.



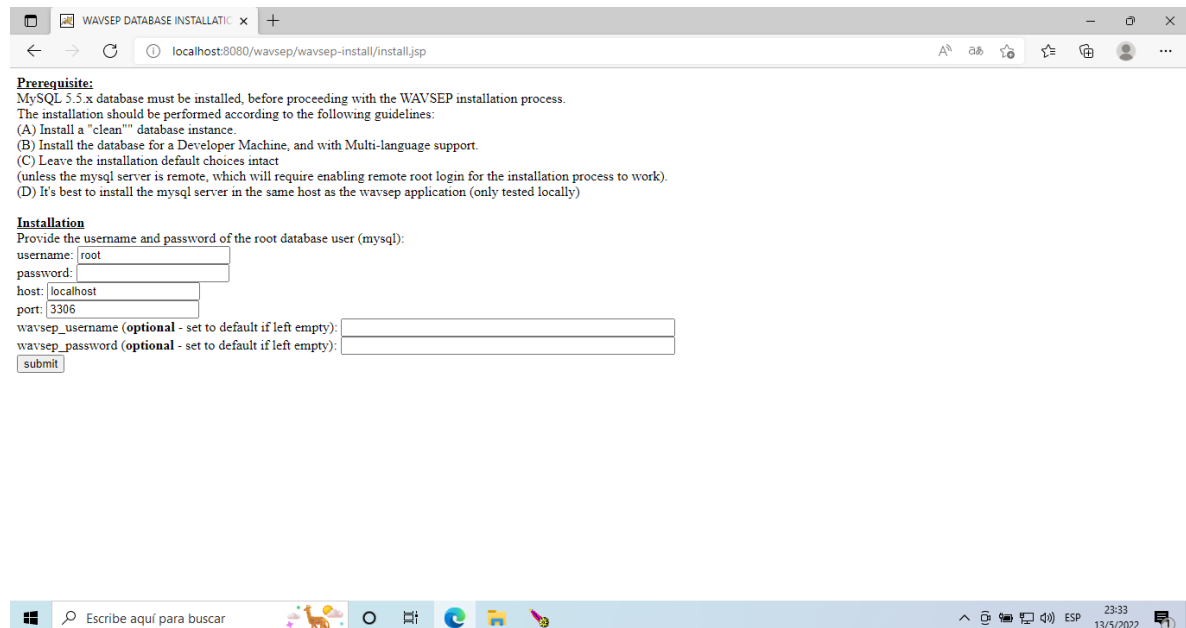
ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

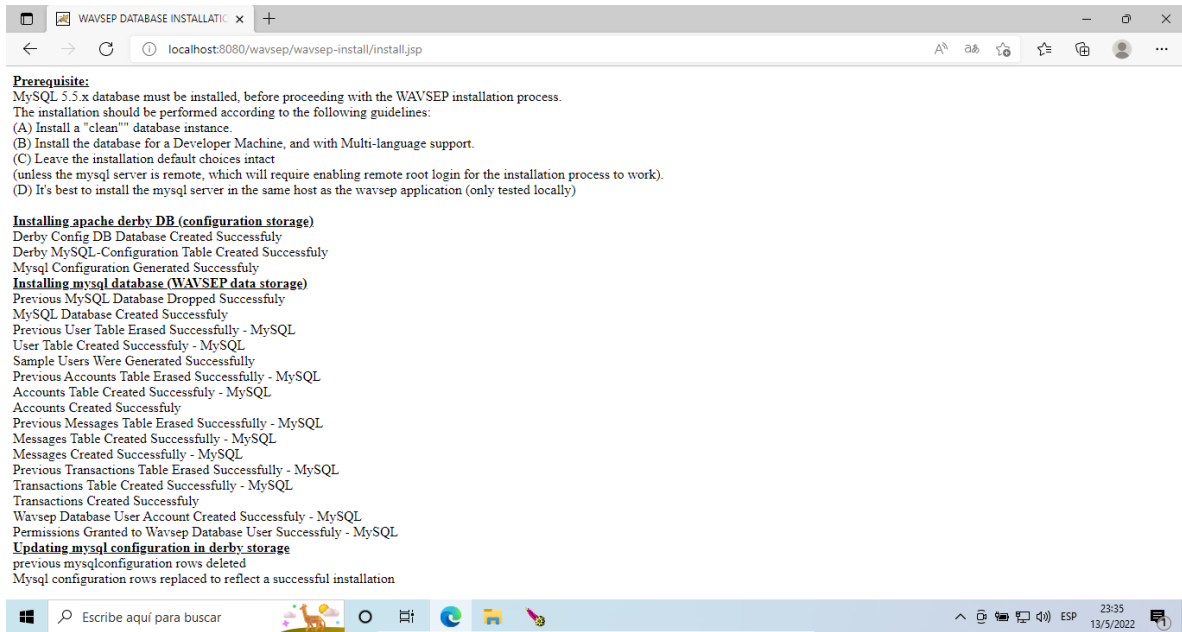
INSTALACION WAVSEP

Tenemos que tener ejecutado el Apache Tomcat, colocar en C:\Program Files\Apache Software Foundation\Tomcat 8.5\webapps el archivo wavsep.war

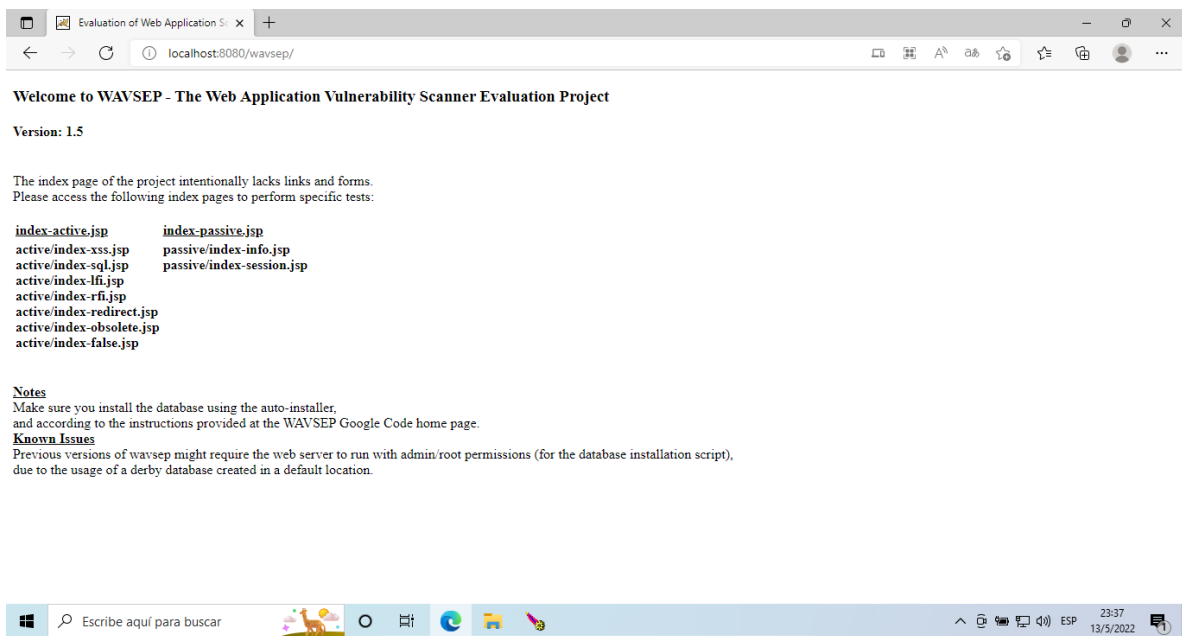


Abrimos en el navegador <http://localhost:8080/wavsep/wavsep-install/install.jsp>, colocamos la contraseña y le damos submit





Ya acá tenemos ya instalado y volvemos a <http://localhost:8080/wavsep/>



Y con esto estamos listo para trabajar con Wavsep

Iniciar Scuba

The screenshot shows the IMPERVA Scuba web interface. On the left, there is a welcome message and a note about scanning supported databases. On the right, there is a form to enter database details. A yellow sticky note is placed over the form, containing the text: "ANGEL RAMON PAZ LOPEZ Seguridad en Bases de Datos y Almacenamiento de Datos Masivos".

Cloud (SSH Tunnel)

SSH Host:

SSH Username:

SSH Private Key:

MYSQL

127.0.0.1

3306

root

wavsepdb

Go!

***NEW* Scuba now supports scanning of the supported databases when installed in AWS, Azure and GCP!**

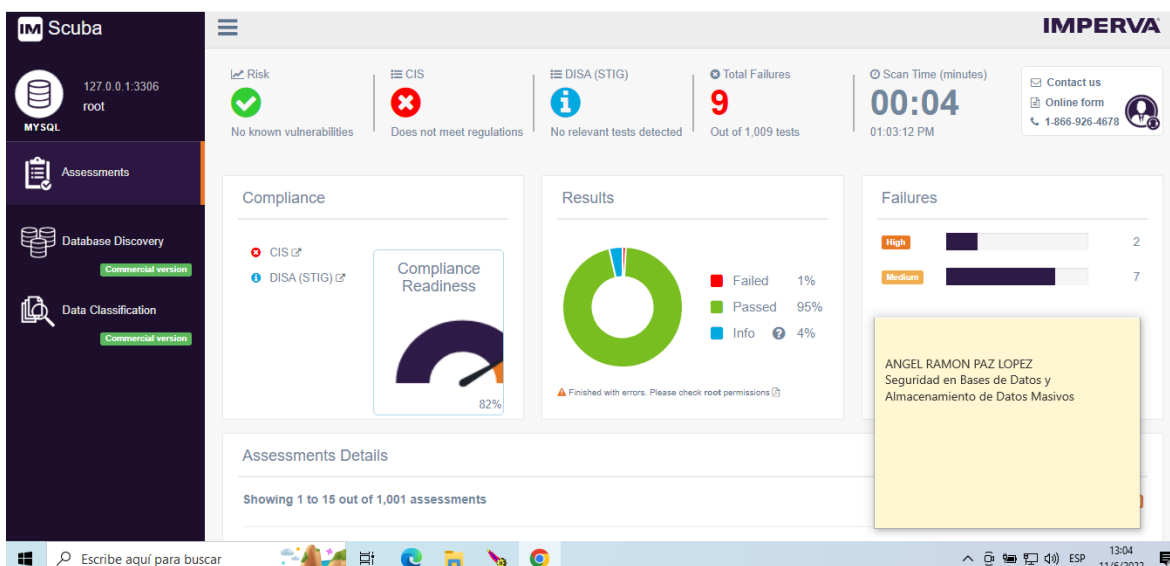
[Click to learn more](#)

Note: Scuba does not support scanning database as a service. To scan RDS databases please use [Imperva Snapshot](#)

Please fill in your database details and click "Go!"

Sales@imperva.com
www.imperva.com
1-866-926-4678

¡Se colocan las credenciales y nombre de base de datos y dar clic en Go!



Teniendo como pantalla principal donde podemos observar que la aplicación WAVSEP tiene un total de 9 vulnerabilidades encontradas entre ellas 2 vulnerabilidades de nivel alto y 7 vulnerabilidades de nivel medio

VULNERABILIDADES ENCONTRADAS

<i>TEST</i>	<i>CATEGORIA</i>	<i>DETALLES</i>	<i>DESCRIPCION</i>	<i>NIVEL DE RIESGO</i>
<i>Cuenta 'root' existente</i>	Autenticación y Gestión de Usuarios	Deshabilitar la capacidad del usuario root para interactuar con MySQL limita el uso de esta cuenta confidencial para fines administrativos no operativos del sistema. Además, evitar la cuenta 'root' para las interacciones de MySQL reduce la posibilidad de comprometer el sistema a través de una vulnerabilidad creada por el cliente de MySQL.	Comprobar si la cuenta de administrador ha cambiado de a configuración predeterminada 'root'	Alto
<i>Usuarios existentes en la base de datos con contraseñas en blanco (CIS MySQL 5.7)</i>	Autenticación y Gestión de Usuarios	Sin una contraseña, solo conocer el nombre de usuario y la lista de hosts permitidos permitirá que alguien se conecte al servidor y asuma la identidad del usuario.	Comprueba si existen usuarios de la base de datos con contraseñas en blanco.	Alto

		Esto, en efecto, elude los mecanismos de autenticación.		
<i>Usuarios no obligados a usar SSL</i>	Control de Acceso	SSL garantiza la confidencialidad e integridad de la información confidencial a medida que atraviesa redes no confiables.	Comprueba que el campo de usuario ssl_type esté establecido en ANY, X509 o SPECIFIED.	Medio
<i>Opción local_infile establecida en ON</i>	Control de Acceso	La carga local permite cargar archivos desde la máquina cliente. Esta función se usa a veces para realizar la carga de datos desde máquinas remotas. En un entorno web donde los clientes se conectan desde un servidor web, un atacante podría usar una vulnerabilidad de inyección SQL para leer archivos del servidor web.	Comprueba si la opción local_infile está activada.	Medio
<i>local_infile Option Is Not Disabled</i>	Control de Acceso	Deshabilitar local_infile reduce la capacidad de un atacante para leer archivos confidenciales del afectado servidor a través de una vulnerabilidad de inyección SQL.	Comprueba si la opción local_infile está activada	Medio

<i>Base de datos de 'test' existente</i>	Información general de la base de datos	La eliminación de componentes no utilizados eliminará la capacidad de un atacante para usarlos.	Comprueba si existe una base de datos de 'test'.	
<i>Opción have_symlink establecida en SÍ</i>	Integridad del Sistema Operativo	Evita que se utilicen enlaces simbólicos para archivos de bases de datos. Esto es especialmente importante cuando MySQL se ejecuta como root, ya que se pueden sobrescribir archivos arbitrarios.	Comprueba si la opción have_symlink está establecida en SÍ.	Medio
<i>La opción sql_mode no está establecida en 'STRICT_ALL_TABLES'</i>	Control de recursos	Sin el modo estricto, el servidor intenta continuar con la acción cuando puede ocurrir un error. ha sido una opción más segura. Por ejemplo, por defecto, MySQL truncará los datos si lo hace. no encaja en un campo, lo que puede conducir a un comportamiento desconocido, o ser aprovechado por un atacante para eludir la validación de datos.	Comprueba si la opción 'sql_mode' no contiene el valor 'STRICT_ALL_TABLES'.	Medio

<i>Opción have_openssl establecida en DESHABILITADA</i>	Control de Acceso	SSL garantiza la confidencialidad e integridad de la información confidencial a medida que atraviesa redes no confiables.	Comprueba si la opción have_openssl está configurada como DESHABILITADA	Medio
---	----------------------	--	---	-------

RECOMENDACIONES PARA ELIMINAR/MITIGAR LAS VULNERABILIDADES

TEST	RECOMENDACION
<i>Cuenta 'root' existente</i>	Cambie la cuenta de administrador de forma predeterminada ("root") a otra cosa mucho más segura y lo recomendable es eliminar la cuenta root
<i>Usuarios existentes en la base de datos con contraseñas en blanco (CIS MySQL 5.7)</i>	<p>Para cada fila devuelta del procedimiento de auditoría, establezca una contraseña para el usuario dado utilizando la siguiente declaración (como ejemplo):</p> <p>ESTABLECER CONTRASEÑA PARA <usuario>@'<host>' = '<borrar contraseña>'</p> <p>NOTA: Reemplace <usuario>, <host> y <borrar contraseña> con los valores apropiados. Se debe establecer una contraseña de manera obligatoria para cada usuario creado.</p>

<i>Usuarios no obligados a usar SSL</i>	Verifica que el campo de usuario ssl_type esté establecido en ANY, X509 o SPECIFIED.
<i>Opción local_infile establecida en ON</i>	Verifique que el valor de local_infile esté "APAGADO"
<i>La opción local_infile no está deshabilitada</i>	Agregue la siguiente línea a la sección [mysqld] del archivo de configuración de MySQL y reinicie el servicio MySQL: local-infile=0
<i>Base de datos de 'test' existente</i>	Remover la base de datos 'test'
<i>Opción have_symlink establecida en SÍ</i>	Verifique que el valor have_symlink esté "DESHABILITADO"
<i>La opción sql_mode no está establecida en 'STRICT_ALL_TABLES'</i>	Realice las siguientes acciones para remediar esta configuración: Agregue STRICT_ALL_TABLES a sql_mode en el archivo de configuración del servidor
<i>Opción have_openssl establecida en DESHABILITADA</i>	Cuando trabaje con redes no confiables (Internet) o cuando se transfiera PII restringida, use SSL

MAS DETALLES

1. Usuarios existentes en la base de datos con contraseñas en blanco (CIS MySQL 5.7)

Un usuario puede crear una contraseña en blanco. Tener una contraseña en blanco es arriesgado ya que cualquiera puede simplemente asumir la identidad del usuario, ingresar el ID de inicio de sesión del usuario y conectarse al servidor. Esto pasa por alto la autenticación, lo cual es malo.

dominio:

```
SELECT User,host FROM mysql.user WHERE authentication_string='';
```

```
mysql> SELECT User,host
-> FROM mysql.user
-> WHERE authentication_string='';
Empty set (0.04 sec)
```

2. Usuarios no obligados a usar SSL

SSL/TLS debe configurarse por usuario. Esto evita aún más el espionaje de atacantes malintencionados.

dominio:

```
SELECT user, host, ssl_type FROM mysql.user WHERE NOT HOST IN ('::1',
'127.0.0.1', 'localhost');
```

```
mysql> SELECT user, host, ssl_type FROM mysql.user
-> WHERE NOT HOST IN ('::1', '127.0.0.1', 'localhost');
+-----+-----+-----+
| user  | host | ssl_type |
+-----+-----+-----+
| clarkngo | 3306 |          |
+-----+-----+-----+
1 row in set (0.02 sec)
```

3. Base de datos de 'test' existente

Una vez instalada la base de datos MySQL, y establecida la contraseña del usuario “root”, de forma predeterminada MySQL tiene dos usuarios definidos y una base de datos 'test'. Los usuarios no tienen predefinida ninguna contraseña y las tablas de la base de datos, que comienzan por 'test', tienen permisos de escritura para todo el mundo. Para deshabilitar estos usuarios y eliminar las tablas mencionadas se recomienda escribir:

```
DELETE FROM user WHERE User = '';  
DELETE FROM db WHERE Host = '%'
```

4. Opción have_symlink establecida en SÍ

Se recomienda deshabilitar los enlaces simbólicos en MySQL porque pueden introducir múltiples riesgos de seguridad diferentes. Los enlaces podrían apuntar potencialmente a directorios con diferentes permisos que podrían causar problemas de seguridad.

Esta es la línea que verá en el archivo de configuración justo encima de la línea que le permite habilitar/deshabilitar enlaces simbólicos:

"Se recomienda deshabilitar los enlaces simbólicos para evitar una variedad de riesgos de seguridad"

Mientras tengas cuidado, probablemente deberías estar bien. Esto no es mucho más peligroso que especificar un directorio de datos alternativo. Solo asegúrese de que los permisos de sus archivos se administren correctamente y probablemente debería estar bien.

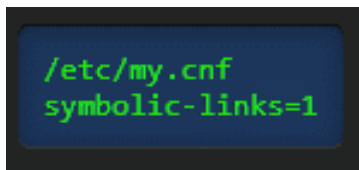
Cómo deshabilitar enlaces simbólicos en MySQL

Los enlaces simbólicos se pueden utilizar para almacenar una base de datos en una ubicación alternativa además de la predeterminada. Es posible que desee que su

base de datos esté en un directorio diferente o en una unidad diferente, todos juntos. Esto te permite hacerlo.

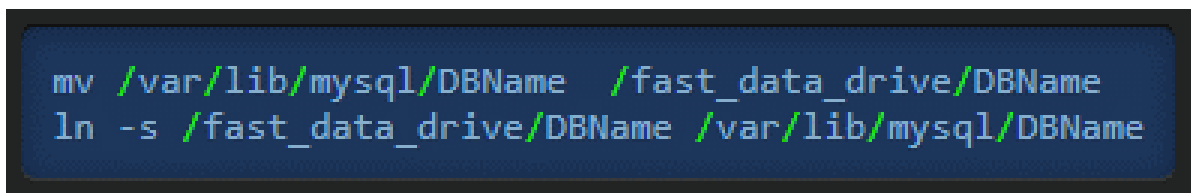
Asegúrese de detener el servicio MySQL antes de mover el directorio y crear el enlace.

Puede habilitar enlaces simbólicos para MySQL en la configuración de esta manera:



```
/etc/my.cnf
symbolic-links=1
```

Puede mover un directorio de base de datos como este:



```
mv /var/lib/mysql/DBName /fast_data_drive/DBName
ln -s /fast_data_drive/DBName /var/lib/mysql/DBName
```

Puede encontrarse con problemas de permisos o problemas de selinux. Asegúrese de que se está ejecutando como el usuario correcto y que todos los directorios tienen los permisos correctos. Puede deshabilitar selinux o incluso configurarlo potencialmente correctamente si así lo desea.

5. Opción `have_openssl` establecida en DESHABILITADA

Para utilizar conexiones SSL entre el servidor MySQL y los programas cliente, su sistema debe tener la capacidad de ejecutar OpenSSL y su versión de MySQL debe ser la 4.0.0 o superior.

Para conseguir que las conexiones seguras funcionen con MySQL, debe hacer lo siguiente:

1. Instale la librería OpenSSL. MySQL ha sido comprobado con OpenSSL 0.9.6. Si necesita OpenSSL, visite <http://www.openssl.org>.
2. Cuando configure MySQL, ejecute el script **configure** con las opciones **--with-vio** y **--with-openssl**.
3. Asegúrese de que ha actualizado sus tablas grant para que las columnas relacionadas con SSL de la tabla **mysql.user** se hayan agregado. Esto es necesario si las tablas grant provienen de una versión de MySQL anterior a la 4.0.0.
4. Para comprobar si un servidor **mysqld** que se está ejecutando tiene soporte para OpenSSL, examine el valor de la variable de sistema **have_openssl**:

```
mysql> SHOW VARIABLES LIKE 'have_openssl';
```

```
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_openssl | YES   |
+-----+-----+
```

Si el valor es **YES**, el servidor tiene soporte para conexiones OpenSSL.

Aquí tiene un ejemplo para configurar certificados SSL para MySQL:

```
DIR=`pwd`/openssl
PRIV=$DIR/private

mkdir $DIR $PRIV $DIR/newcerts
cp /usr/share/ssl/openssl.cnf $DIR
replace ./demoCA $DIR -- $DIR/openssl.cnf

# Create necessary files: $database, $serial and $new_certs_dir
# directory (optional)

touch $DIR/index.txt
echo "01" > $DIR/serial

#
# Generation of Certificate Authority(CA)
#

openssl req -new -x509 -keyout $PRIV/cakey.pem -out
$DIR/cacert.pem \
```

```

-config $DIR/openssl.cnf

# Sample output:
# Using configuration from /home/monty/openssl/openssl.cnf
# Generating a 1024 bit RSA private key
# .....++++++
# .....++++++
# writing new private key to
# '/home/monty/openssl/private/cakey.pem'
# Enter PEM pass phrase:
# Verifying password - Enter PEM pass phrase:
# -----
# You are about to be asked to enter information that will be
# incorporated into your certificate request.
# What you are about to enter is what is called a Distinguished
Name
# or a DN.
# There are quite a few fields but you can leave some blank
# For some fields there will be a default value,
# If you enter '.', the field will be left blank.
# -----
# Country Name (2 letter code) [AU]:FI
# State or Province Name (full name) [Some-State]:.
# Locality Name (eg, city) []:
# Organization Name (eg, company) [Internet Widgits Pty Ltd]:MySQL
AB
# Organizational Unit Name (eg, section) []:
# Common Name (eg, YOUR name) []:MySQL admin
# Email Address []:

#
# Create server request and key
#
openssl req -new -keyout $DIR/server-key.pem -out \
    $DIR/server-req.pem -days 3600 -config $DIR/openssl.cnf

# Sample output:
# Using configuration from /home/monty/openssl/openssl.cnf
# Generating a 1024 bit RSA private key
# ..++++++
# .....++++++
# writing new private key to '/home/monty/openssl/server-key.pem'
# Enter PEM pass phrase:
# Verifying password - Enter PEM pass phrase:
# -----
# You are about to be asked to enter information that will be
# incorporated into your certificate request.
# What you are about to enter is what is called a Distinguished
Name
# or a DN.
# There are quite a few fields but you can leave some blank
# For some fields there will be a default value,

```



```

# If you enter '.', the field will be left blank.
# -----
# Country Name (2 letter code) [AU]:FI
# State or Province Name (full name) [Some-State]:.
# Locality Name (eg, city) []:
# Organization Name (eg, company) [Internet Widgits Pty Ltd]:MySQL
AB
# Organizational Unit Name (eg, section) []:
# Common Name (eg, YOUR name) []:MySQL server
# Email Address []:
#
# Please enter the following 'extra' attributes
# to be sent with your certificate request
# A challenge password []:
# An optional company name []:

#
# Remove the passphrase from the key (optional)
#

openssl rsa -in $DIR/server-key.pem -out $DIR/server-key.pem

#
# Sign server cert
#
openssl ca -policy policy_anything -out $DIR/server-cert.pem \
    -config $DIR/openssl.cnf -infiles $DIR/server-req.pem

# Sample output:
# Using configuration from /home/monty/openssl/openssl.cnf
# Enter PEM pass phrase:
# Check that the request matches the signature
# Signature ok
# The Subjects Distinguished Name is as follows
# countryName             :PRINTABLE:'FI'
# organizationName        :PRINTABLE:'MySQL AB'
# commonName               :PRINTABLE:'MySQL admin'
# Certificate is to be certified until Sep 13 14:22:46 2003 GMT
# (365 days)
# Sign the certificate? [y/n]:y
#
#
# 1 out of 1 certificate requests certified, commit? [y/n]y
# Write out database with 1 new entries
# Data Base Updated

#
# Create client request and key
#
openssl req -new -keyout $DIR/client-key.pem -out \
    $DIR/client-req.pem -days 3600 -config $DIR/openssl.cnf

```

```

# Sample output:
# Using configuration from /home/monty/openssl/openssl.cnf
# Generating a 1024 bit RSA private key
# .....++++++
# .....++++++
# writing new private key to '/home/monty/openssl/client-key.pem'
# Enter PEM pass phrase:
# Verifying password - Enter PEM pass phrase:
# -----
# You are about to be asked to enter information that will be
# incorporated into your certificate request.
# What you are about to enter is what is called a Distinguished
Name
# or a DN.
# There are quite a few fields but you can leave some blank
# For some fields there will be a default value,
# If you enter '.', the field will be left blank.
# -----
# Country Name (2 letter code) [AU]:FI
# State or Province Name (full name) [Some-State]:.
# Locality Name (eg, city) []:
# Organization Name (eg, company) [Internet Widgits Pty Ltd]:MySQL
AB
# Organizational Unit Name (eg, section) []:
# Common Name (eg, YOUR name) []:MySQL user
# Email Address []:
#
# Please enter the following 'extra' attributes
# to be sent with your certificate request
# A challenge password []:
# An optional company name []:

#
# Remove a passphrase from the key (optional)
#
openssl rsa -in $DIR/client-key.pem -out $DIR/client-key.pem

#
# Sign client cert
#

openssl ca -policy policy_anything -out $DIR/client-cert.pem \
    -config $DIR/openssl.cnf -infiles $DIR/client-req.pem

# Sample output:
# Using configuration from /home/monty/openssl/openssl.cnf
# Enter PEM pass phrase:
# Check that the request matches the signature
# Signature ok
# The Subjects Distinguished Name is as follows
# countryName             :PRINTABLE:'FI'
# organizationName        :PRINTABLE:'MySQL AB'

```

```
# commonName          :PRINTABLE:'MySQL user'
# Certificate is to be certified until Sep 13 16:45:17 2003 GMT
# (365 days)
# Sign the certificate? [y/n]:y
#
#
# 1 out of 1 certificate requests certified, commit? [y/n]y
# Write out database with 1 new entries
# Data Base Updated

#
# Create a my.cnf file that you can use to test the certificates
#

cnf=""
cnf="$cnf [client]"
cnf="$cnf ssl-ca=$DIR/cacert.pem"
cnf="$cnf ssl-cert=$DIR/client-cert.pem"
cnf="$cnf ssl-key=$DIR/client-key.pem"
cnf="$cnf [mysqld]"
cnf="$cnf ssl-ca=$DIR/cacert.pem"
cnf="$cnf ssl-cert=$DIR/server-cert.pem"
cnf="$cnf ssl-key=$DIR/server-key.pem"
echo $cnf | replace " " '
' > $DIR/my.cnf
```

Para comprobar las conexiones SSL, inicie el servidor de la siguiente manera, donde **\$DIR** es la ruta a el directorio donde está el archivo de opciones de ejemplo **my.cnf**:

```
shell> mysqld --defaults-file=$DIR/my.cnf &
```

Entonces ejecute un programa cliente utilizando el mismo archivo de opciones:

```
shell> mysql --defaults-file=$DIR/my.cnf
```

Si tiene una distribución de código fuente de MySQL, usted puede tambier comprobar su configuración modificando el archivo **my.cnf** precedente para que se refiera al certificado y los archivos de claves en el directorio **SSL** de la distribución.

CONCLUSIONES

Se realizo una auditoria a la Instancia de BD WAVSEP preparamos su debida instalación de laboratorio e instalamos una herramienta para el escaneo y análisis de la base de datos Mysql con la herramienta SCUBA el cual ayudara a todo auditor en su labores de auditoría a base de datos, en nuestro caso encontramos un total de 9 vulnerabilidades en la base de datos de WAVSEP con su respectivo nivel de riesgo, la herramienta SCUBA nos brinda la información necesaria, desde su descripción de las vulnerabilidades y recomendaciones de como poder resolverlas, lo cual hace a SCUBA una herramienta idónea para el escaneo de vulnerabilidades a Instancias de Base de Datos.

REFERENCIAS

- Paz, A. (20 de 05 de 2022). *Explotación de vulnerabilidades de inyección de SQL en la BD WAVSEP*. Obtenido de UNIR:
<https://micampus.unir.net/courses/29353/assignments/449583>
- *Why is It Recommended to Disable Symbolic Links in MySQL | Low Orbit Flux*. (s. f.). Recuperado 16 de junio de 2022, de <https://low-orbit.net/why-is-it-recommended-to-disable-symbolic-links-in-mysql>
- *How to make sure your MySQL database is secured*. (2018, octubre 28). freeCodeCamp.org. <https://www.freecodecamp.org/news/cjn-is-your-mysql-secured-7793e5444cf5/>
- *Capítulo 5. Administración de bases de datos*. (s. f.). Recuperado 16 de junio de 2022, de <https://manuales.guebs.com/mysql-5.0/mysql-database-administration.html#secure-requirements>
- *[PDF] Télématique ISSN: Universidad Privada Dr. Rafael Bellosó Chacín Venezuela - Free Download PDF*. (s. f.). Recuperado 16 de junio de 2022, de <https://silo.tips/download/telematique-issn-universidad-privada-dr-rafael-belloso-chacin-venezuela-13>
- Scuba Database Vulnerability Scanner

ANEXOS

Test	Category	Compliance	Result
Existing 'root' Account	Authentication and User Management	CIS	High

DETAILS

Disabling the root user's ability to interact with MySQL limits the use of this sensitive account for non-operating system administrative purposes. Additionally, avoiding the 'root' account for MySQL interactions reduces the possibility of compromising the system via a MySQL client-born vulnerability.

DESCRIPTION

Checks if admin account has changed from default ('root').

DATA

User	Host
root	localhost

REMEDATION

Change admin account from default ("root") to something else

ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

7.1

08:06
16/6/2022

Cuenta 'root' existente

Test	Category	Compliance	Result
Existing Database Users with Blank Passwords (CIS MySQL 5.7)	Authentication and User Management	CIS	High

DETAILS

Without a password only knowing the username and the list of allowed hosts will allow someone to connect to the server and assume the identity of the user. This, in effect, bypasses authentication mechanisms.

DESCRIPTION

Checks if database users with blank passwords exist.

DATA

User	Host
root	localhost

REMEDATION

For each row returned from the audit procedure, set a password for the given user using the following statement (as an example):

SET PASSWORD FOR <user>@<host> = '<clear password>'

NOTE: Replace <user>, <host>, and <clear password> with appropriate values

ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

6.5

08:08
16/6/2022

Usuarios existentes en la base de datos con contraseñas en blanco (CIS MySQL 5.7)

Users not Forced to Use SSL

2

Access Control

CIS

Medium

DETAILS

SSL ensures the confidentiality and integrity of sensitive information as it traverses untrusted networks.

DESCRIPTION

Checks that the user field ssl_type is set to ANY, X509 or SPECIFIED.

DATA

User	Host
root	localhost
wavsep	localhost

REMEDIATION

When working with untrusted networks (Internet) or when restricted PII is transferred, SSL must be used

ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

4.9

08:18

16/6/2022

Usuarios no obligados a usar SSL

local_infile Option Set to ON

1

Access Control

CIS

Medium

DETAILS

Local loading allows loading files from the client machine. This feature is sometimes used to perform data loading from remote machines. In a web environment where clients are connecting from a web server an attacker could use a SQL Injection vulnerability to read files from the web server.

DESCRIPTION

Checks if local_infile option is set to ON.

DATA

VARIABLE_NAME	VARIABLE_VALUE
LOCAL_INFILE	ON

REMEDIATION

Verify value is "OFF"

ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

4.9

08:24

16/6/2022

Opción local_infile establecida en ON

local_infile Option Is Not Disabled

1

Access Control

CIS

Medium

DETAILS

Disabling local_infile reduces an attacker's ability to read sensitive files off the affected server via an SQL injection vulnerability.

DESCRIPTION

Checks if the local_infile option is set to ON

DATA

VARIABLE_NAME	VARIABLE_VALUE
LOCAL_INFILE	ON

REMEDIATION

Add the following line to the [mysqld] section of the MySQL configuration file and restart the MySQL service:
local-infile=0

3.5

La opción local_infile no está deshabilitada

Existing 'test' Database

General Database Info

CIS

Medium

DETAILS

Removing unutilized components will eliminate an attacker's ability to use them.

DESCRIPTION

Checks if 'test' database exists.

REMEDIATION

Remove test database

4.6

ANGEL RAMON PAZ LOPEZ
Seguridad en Bases de Datos y
Almacenamiento de Datos Masivos

Base de datos de 'test' existente

have_symlink Option Set to YES

1

OS Integrity

CIS

Medium

DETAILS

Prevents sym links from being used for database files. This is especially important when MySQL is executing as root, as arbitrary files may be overwritten.

DESCRIPTION

Checks if have_symlink option is set to YES.

DATA

VARIABLE_NAME	VARIABLE_VALUE
HAVE_SYMLINK	YES

REMEDIATION

Verify value is "DISABLED"

ANGEL RAMON PAZ LOPEZ

Seguridad en Bases de Datos y

Almacenamiento de Datos Masivos

4.9

08:40
16/6/2022

Opción have_symlink establecida en SÍ

sql_mode Option is not set to 'STRICT_ALL_TABLES'

1

Resource Control

CIS

Medium

DETAILS

Without strict mode the server tries to do proceed with the action when an error might have been a more secure choice. For example, by default MySQL will truncate data if it does not fit in a field, which can lead to unknown behavior, or be leveraged by an attacker to circumvent data validation.

DESCRIPTION

Checks if the 'sql_mode' option does not contain 'STRICT_ALL_TABLES' value.

DATA

VARIABLE_NAME	VARIABLE_VALUE
sql_mode	STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION

REMEDIATION

Perform the following actions to remediate this setting:
Add STRICT_ALL_TABLES to the sql_mode in the server's configuration file

ANGEL RAMON PAZ LOPEZ

Seguridad en Bases de Datos y

Almacenamiento de Datos Masivos

4.6

La opción sql_mode no está establecida en 'STRICT_ALL_TABLES'

have_openssl Option Set to DISABLED

1

Access Control

CIS

Medium

DETAILS

SSL ensures the confidentiality and integrity of sensitive information as it traverses untrusted networks.

DESCRIPTION

Checks if have_openssl option is set to DISABLED.

DATA

VARIABLE_NAME	VARIABLE_VALUE
HAVE_OPENSSL	DISABLED

REMEDIATION

When working with untrusted networks (internet) or when restricted PII is transferred, use SSL

super_priv Privilege Granted to Replication Users

1

Access Control

CIS

Info

ANGEL RAMON PAZ LOPEZ

Seguridad en Bases de Datos y

Almacenamiento de Datos Masivos

4.9

Opción have_openssl establecida en DESHABILITADA