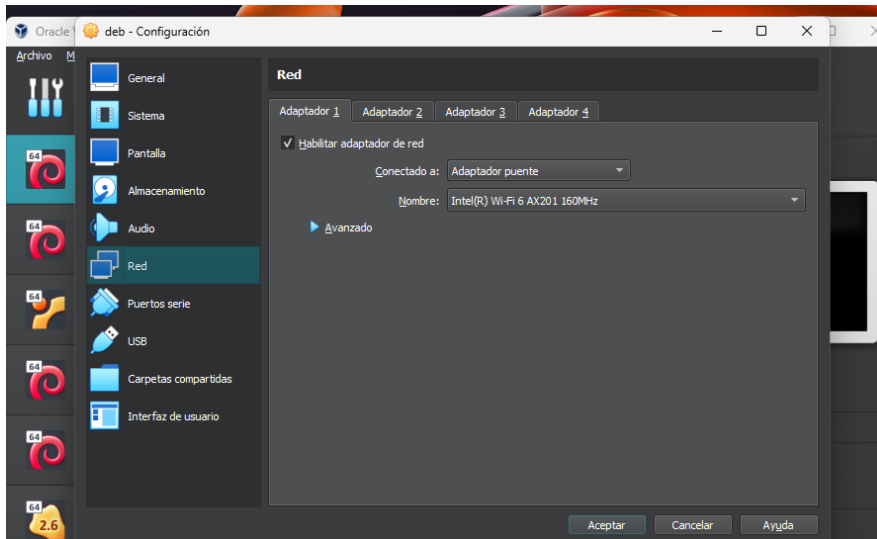


Instalación de DVWA en una Máquina Virtual para Prácticas de Inyección SQL



1.- Seleccionando 'Adaptador puente'

```
deb@debian: ~
Archivo Editar Ver Buscar Terminal Ayuda
deb@debian:~$ sudo apt update && sudo apt upgrade
[sudo] contraseña para deb:
Obj:1 http://deb.debian.org/debian bookworm InRelease
Des:2 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Des:3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
Des:4 https://packages.wazuh.com/4.x/apt stable InRelease [17,3 kB]
Des:5 http://security.debian.org/debian-security bookworm-security/main Sources [126 kB]
Des:6 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [190 kB]
Des:7 http://security.debian.org/debian-security bookworm-security/main Translation-en [116 kB]
```

2.- Actualización de sistema.

```
deb@debian:~$ sudo apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
apache2 ya está en su versión más reciente (2.4.62-1~deb12u2).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libwpe-1.0-1 libwpebackend-fdo-1.0-1 linux-headers-6.1.0-22-amd64
  linux-headers-6.1.0-22-common linux-headers-6.1.0-23-amd64
  linux-headers-6.1.0-23-common linux-image-6.1.0-18-amd64
  linux-image-6.1.0-22-amd64 linux-image-6.1.0-23-amd64
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

3.- Servicio apache.

```

• apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-11-01 03:03:26 -04; 8min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 33521 (apache2)
     Tasks: 6 (limit: 9452)
    Memory: 16.3M
       CPU: 132ms
   CGroup: /system.slice/apache2.service
           └─33521 /usr/sbin/apache2 -k start
             └─33523 /usr/sbin/apache2 -k start
               └─33524 /usr/sbin/apache2 -k start
                 └─33525 /usr/sbin/apache2 -k start
                   └─33526 /usr/sbin/apache2 -k start
                     └─33528 /usr/sbin/apache2 -k start

nov 01 03:03:26 debian systemd[1]: Starting apache2.service - The Apache HTTP Server...
nov 01 03:03:26 debian apachectl[33520]: AH00558: apache2: Could not reliably determine the server's fully qualified
nov 01 03:03:26 debian systemd[1]: Started apache2.service - The Apache HTTP Server.
~

```

3.1.- Confirmando estatus de servicio.

```

deb@debian:~$ sudo systemctl status mariadb
• mariadb.service - MariaDB 10.11.6 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-11-01 02:58:54 -04; 18min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 916 (mariadb)
  Status: "Taking your SQL requests now..."
     Tasks: 9 (limit: 9452)
    Memory: 236.2M
       CPU: 11.405s
   CGroup: /system.slice/mariadb.service
           └─916 /usr/sbin/mariadb

```

4.- Confirmando estatus de servicio MariaDB.

```

deb@debian:~$ sudo apt install php
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
php ya está en su versión más reciente (2:8.2+93).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libwp6-1.0-1 libwp6backend-fdo-1.0-1 linux-headers-6.1.0-22-amd64 linux-headers-6.1.0-22-common
  linux-headers-6.1.0-23-amd64 linux-headers-6.1.0-23-common linux-image-6.1.0-18-amd64 linux-image-6.1.0-22-amd64
  linux-image-6.1.0-23-amd64
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.

```

5.- Instalación de PHP.

```

Aplicaciones Lugares Sistema
deb@debian: /var/www/html

Archivo Editar Ver Buscar Terminal Ayuda
deb@debian: /var/www/html$ sudo apt-get install wget unzip
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
wget ya está en su versión más reciente (1.21.3-1+b2).
unzip ya está en su versión más reciente (6.0-28).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libwp6-1.0-1 libwp6backend-fdo-1.0-1 linux-headers-6.1.0-22-amd64 linux-headers-6.1.0-22-common
  linux-headers-6.1.0-23-amd64 linux-headers-6.1.0-23-common linux-image-6.1.0-18-amd64 linux-image-6.1.0-22-amd64
  linux-image-6.1.0-23-amd64
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
deb@debian: /var/www/html$ sudo wget https://storage.googleapis.com/breathcode/virtualbox/DVWA.zip sudo unzip DVWA.zip
--2024-11-01 03:20:52-- https://storage.googleapis.com/breathcode/virtualbox/DVWA.zip
Resolviendo storage.googleapis.com (storage.googleapis.com)... 2687:f8b0:4012:81c::201b, 2687:f8b0:4012:822::201b, 2687:f8b0:4012:823::201b, ...
Conectando con storage.googleapis.com (storage.googleapis.com)[2687:f8b0:4012:81c::201b]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 894761 (874K) [application/zip]
Grabando a: «DVWA.zip.1»

DVWA.zip.1 100%[=====] 873,79K 5,53MB/s en 0,2s

2024-11-01 03:20:52 (5,53 MB/s) - «DVWA.zip.1» guardado [894761/894761]

--2024-11-01 03:20:52-- http://sudo/
Resolviendo sudo (sudo)... falló: Nombre o servicio desconocido.
wget: no se pudo resolver la dirección del equipo «sudo»
--2024-11-01 03:20:52-- http://unzip/
Resolviendo unzip (unzip)... falló: Nombre o servicio desconocido.
wget: no se pudo resolver la dirección del equipo «unzip»
--2024-11-01 03:20:52-- http://dwa.zip/
Resolviendo dwa.zip (dwa.zip)... falló: Nombre o servicio desconocido.
wget: no se pudo resolver la dirección del equipo «dwa.zip»
ACABADO --2024-11-01 03:20:52--

```

6.- Descarga, Instalación y extracción de DVWA.

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 7.2                                config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server']   = getenv('DB_SERVER') ? '127.0.0.1' : 'localhost';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user']     = 'root';
$_DVWA['db_password'] = '123456';
$_DVWA['db_port']     = '3306';

# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';

```

7.- Configuración de credenciales de la base de datos.

```

MariaDB [(none)]> CREATE DATABASE dvwa;
ERROR 1007 (HY000): Can't create database 'dvwa'; database exists
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| dvwa     |
| information_schema |
| mysql    |
| performance_schema |
| sys      |
+-----+

```

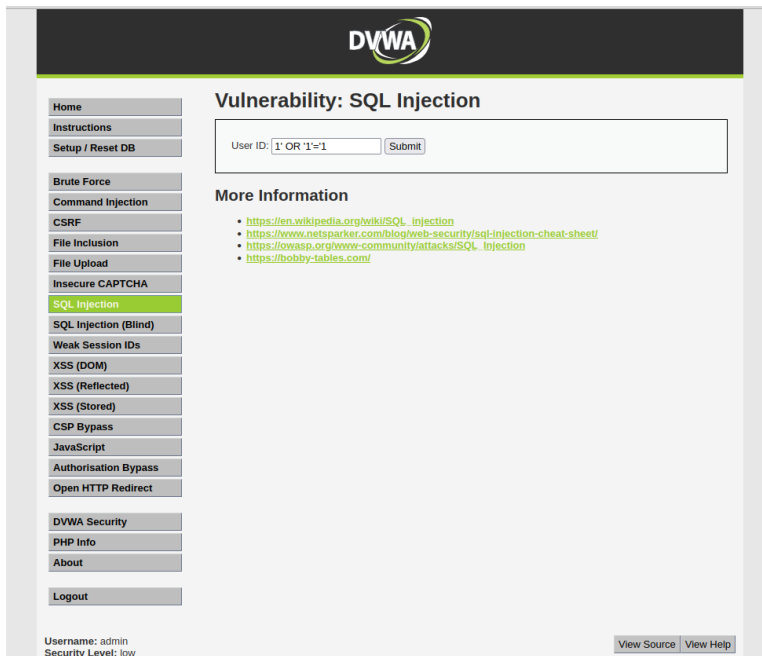
8.- Confirmando base de datos creada.

```

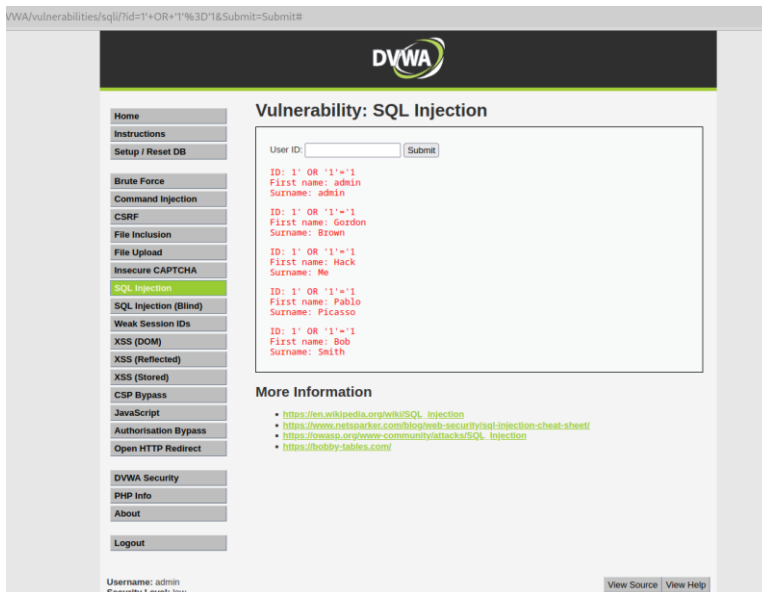
deb@debian:/var/www/html/DVWA/config$ ls -l
total 12
-rw-r--r-- 1 www-data www-data 2192 nov  1 03:26 config.inc.php
-rw-r--r-- 1 www-data www-data 2192 sep 25 23:09 config.inc.php.bak
-rwxr-xr-x 1 www-data www-data 2194 jun 11  2023 config.inc.php.dist
deb@debian:/var/www/html/DVWA/config$ sudo chown -R www-data:www-data /var/www/html/DVWA/
deb@debian:/var/www/html/DVWA/config$ sudo chmod -R 755 /var/www/html/DVWA/
deb@debian:/var/www/html/DVWA/config$ ls -l
total 12
-rwxr-xr-x 1 www-data www-data 2192 nov  1 03:26 config.inc.php
-rwxr-xr-x 1 www-data www-data 2192 sep 25 23:09 config.inc.php.bak
-rwxr-xr-x 1 www-data www-data 2194 jun 11  2023 config.inc.php.dist
deb@debian:/var/www/html/DVWA/config$

```

9.- Configuración de permisos de archivos config.



13.- Ejecutando SQL Injection en DVWA.



14.- Procesado de inyección y resultados de la base de datos.

1. Título del Reporte

Reporte de Incidente de Seguridad: Pruebas de Inyección SQL en DVWA (Damn Vulnerable Web Application)

2. Introducción

Este reporte documenta el proceso de instalación, configuración y pruebas de vulnerabilidades en la aplicación web DVWA instalada en una máquina virtual para simular prácticas de inyección SQL. DVWA es una herramienta diseñada para permitir a los estudiantes y profesionales de seguridad informática probar diferentes tipos de ataques en un entorno seguro, facilitando la comprensión de los vectores de ataque y las posibles soluciones para proteger aplicaciones web.

3. Descripción del Incidente

El incidente consiste en la ejecución de prácticas de inyección SQL en la aplicación DVWA. La inyección SQL es una técnica de ataque que permite a un usuario malintencionado manipular las consultas SQL realizadas por una aplicación, accediendo o modificando información confidencial en la base de datos. En este caso, la aplicación vulnerable DVWA fue utilizada intencionalmente para realizar ataques de prueba y obtener información de la base de datos mediante esta técnica.

4. Proceso de Reproducción

1. **Instalación de DVWA en una Máquina Virtual:** Se configuró un entorno en una máquina virtual utilizando un adaptador puente para la conexión de red.
2. **Actualización del Sistema y Configuración de Servicios:** Se actualizaron los paquetes del sistema y se iniciaron los servicios necesarios, como Apache y MariaDB, verificando su estado para asegurar que estuvieran activos.
3. **Instalación de PHP y DVWA:** Se instaló PHP y se descargó DVWA, extrayendo los archivos en el servidor web y configurando las credenciales de la base de datos.
4. **Configuración de Permisos y Revisión de la Configuración:** Se otorgaron los permisos adecuados al archivo de configuración de DVWA, y se verificó la correcta creación de la base de datos.
5. **Pruebas de Inyección SQL:** Después de iniciar sesión en DVWA, se estableció un nivel de seguridad bajo para facilitar las pruebas de inyección SQL, permitiendo la manipulación de consultas para extraer datos.

5. Impacto del Incidente

El impacto de este incidente es limitado debido a que se realizó en un entorno de pruebas controlado. Sin embargo, en un entorno de producción, una inyección SQL exitosa podría tener consecuencias graves, tales como:

- Acceso no autorizado a información confidencial almacenada en la base de datos.

- Modificación o eliminación de datos sensibles.
- Exposición de credenciales y otra información de los usuarios.
- Potencial escalamiento de privilegios en el sistema afectado.

6. Recomendaciones

Para mitigar el riesgo de inyección SQL en entornos reales, se recomienda implementar las siguientes medidas:

- **Validación y Saneamiento de Entrada:** Asegurarse de que todos los datos ingresados por el usuario sean validados y sanitizados antes de utilizarlos en consultas SQL.
- **Uso de Consultas Preparadas:** Emplear consultas preparadas con parámetros en lugar de concatenar entradas de usuario directamente en las consultas SQL.
- **Restricción de Permisos en la Base de Datos:** Limitar los privilegios de los usuarios de base de datos para evitar accesos innecesarios.
- **Monitoreo y Auditoría:** Implementar sistemas de monitoreo y auditoría para detectar actividades sospechosas en la base de datos.
- **Establecimiento de Niveles de Seguridad Adecuados:** Configurar correctamente los niveles de seguridad en aplicaciones y bases de datos para minimizar la superficie de ataque.

7. Conclusión

La práctica de inyección SQL en DVWA permitió simular un escenario común de ataque en aplicaciones web, proporcionando una oportunidad de aprendizaje sobre cómo funcionan las inyecciones SQL y sus posibles consecuencias. Las pruebas realizadas demuestran la importancia de implementar controles de seguridad adecuados en el desarrollo de software. Aplicar las recomendaciones descritas puede ayudar a mitigar los riesgos y proteger mejor los datos almacenados en aplicaciones de producción.