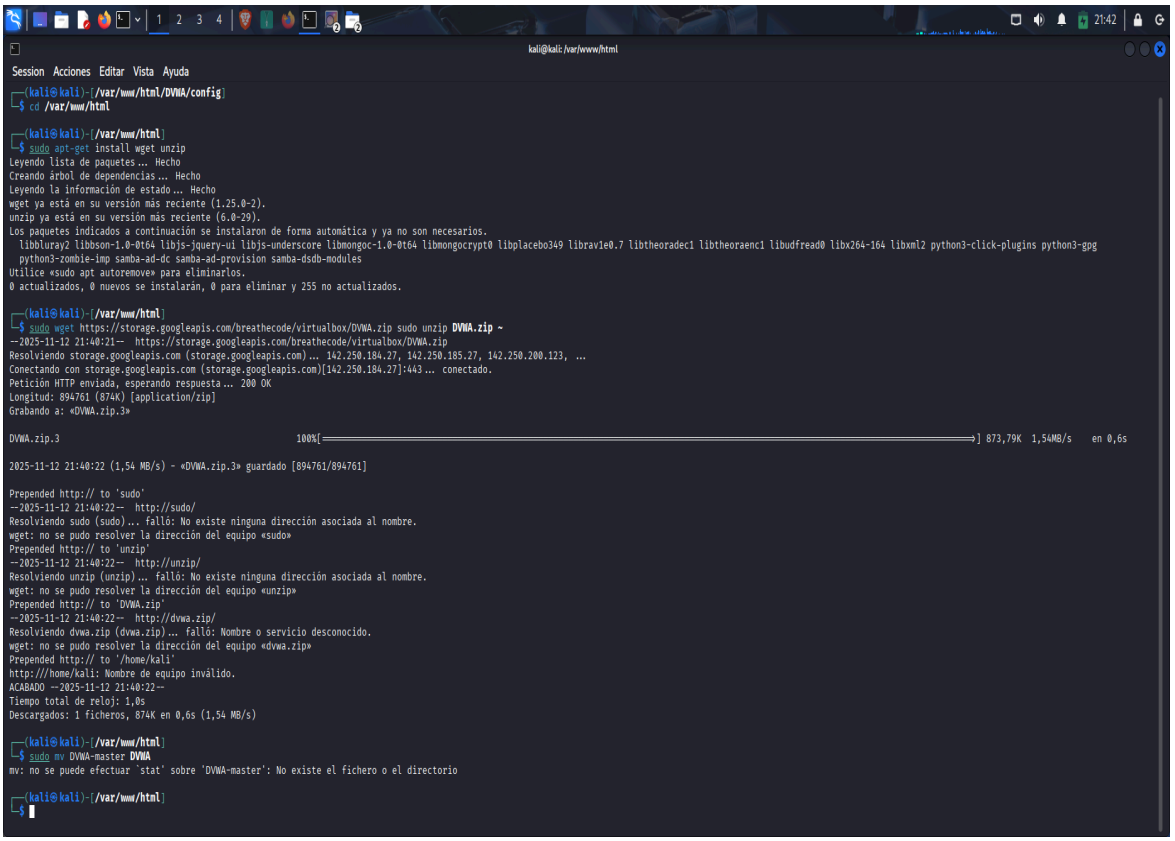
Vulnerabilidad SQL Injection

En el siguiente documento he recreado el paso a paso de como realizar una inyección SQL desde la máquina virtual Kali, recreando el paso a paso arrojando los siguientes resultados:



- Nos movemos dentro de la ruta cd /var/www/html.

.

Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
wget ya está en su versión más reciente (1.25.0-2).
unzip ya está en su versión más reciente (6.0-29).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
libbluray2 libbson-1.0-0t64 libjs-jquery-ui libjs-underscore libmongoc-1.0-0t64 libmongocrypt0 libplacebo349 librav1e0.7 libtheoradec1 libtheoraenc1 libudfread0 libx264-164 libxml2 python3-click-plugins python3-gpg
python3-zombie-imp samba-ad-dc samba-ad-provision samba-dsdb-modules
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 255 no actualizados.

- Lanzamos “sudo wget https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip sudo unzip DVWA.zip” Verificamos que resuelve el url, conectando con la api quedando OK

--2025-11-12 21:40:21-- https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip
Resolviendo storage.googleapis.com (storage.googleapis.com)... 142.250.184.27, 142.250.185.27, 142.250.200.123, ...
Conectando con storage.googleapis.com (storage.googleapis.com)[142.250.184.27]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 894761 (874K) [application/zip]
Grabando a: «DVWA.zip.3»
DVWA.zip.3
100%[==========>]
873,79K 1,54MB/s en 0,6s

2025-11-12 21:40:22 (1,54 MB/s) - «DVWA.zip.3» guardado [894761/894761]

Prepended http:// to 'sudo'
--2025-11-12 21:40:22-- http://sudo/
Resolviendo sudo (sudo)... falló: No existe ninguna dirección asociada al nombre.
wget: no se pudo resolver la dirección del equipo «sudo»
Prepended http:// to 'unzip'
--2025-11-12 21:40:22-- http://unzip/
Resolviendo unzip (unzip)... falló: No existe ninguna dirección asociada al nombre.
wget: no se pudo resolver la dirección del equipo «unzip»
Prepended http:// to 'DVWA.zip'
--2025-11-12 21:40:22-- http://dvwa.zip/
Resolviendo dvwa.zip (dvwa.zip)... falló: Nombre o servicio desconocido.
wget: no se pudo resolver la dirección del equipo «dvwa.zip»
Prepended http:// to '/home/kali'
http:///home/kali: Nombre de equipo inválido.
ACABADO --2025-11-12 21:40:22--
Tiempo total de reloj: 1,0s
Descargados: 1 ficheros, 874K en 0,6s (1,54 MB/s)

- Por último lanzamos sudo mv DVWA-master DVWA

mv: no se puede efectuar `stat' sobre 'DVWA-master': No existe el fichero o el directorio

- Nos movemos a la ruta cd DVWA/config

- Cambiamos de directorio y movemos el archivo de configuración sudo cp config.inc.php.dist config.inc.php

- Editamos el archivo nano sudo nano config.inc.php y configuramos a la configuración correcta
- Accedemos a MariaDB y creamos a la base de datos sudo mysql -u root -p
- Corregimos permisos sudo chown -R www-data:www-data /var/www/html/DVWA/
  sudo chmod -R 755 /var/www/html/DVWA/

Recomendaciones

1. Validar y sanitizar todas las entradas del usuario antes de usarlas en consultas SQL.
2. Usar consultas preparadas (prepared statements) o parámetros en lugar de concatenar variables directamente.
3. Limitar los privilegios del usuario de base de datos que usa la aplicación, para reducir el impacto de esta vulnerabilidad.
4. Implementar un firewall para realizar pruebas de seguridad de manera periodica