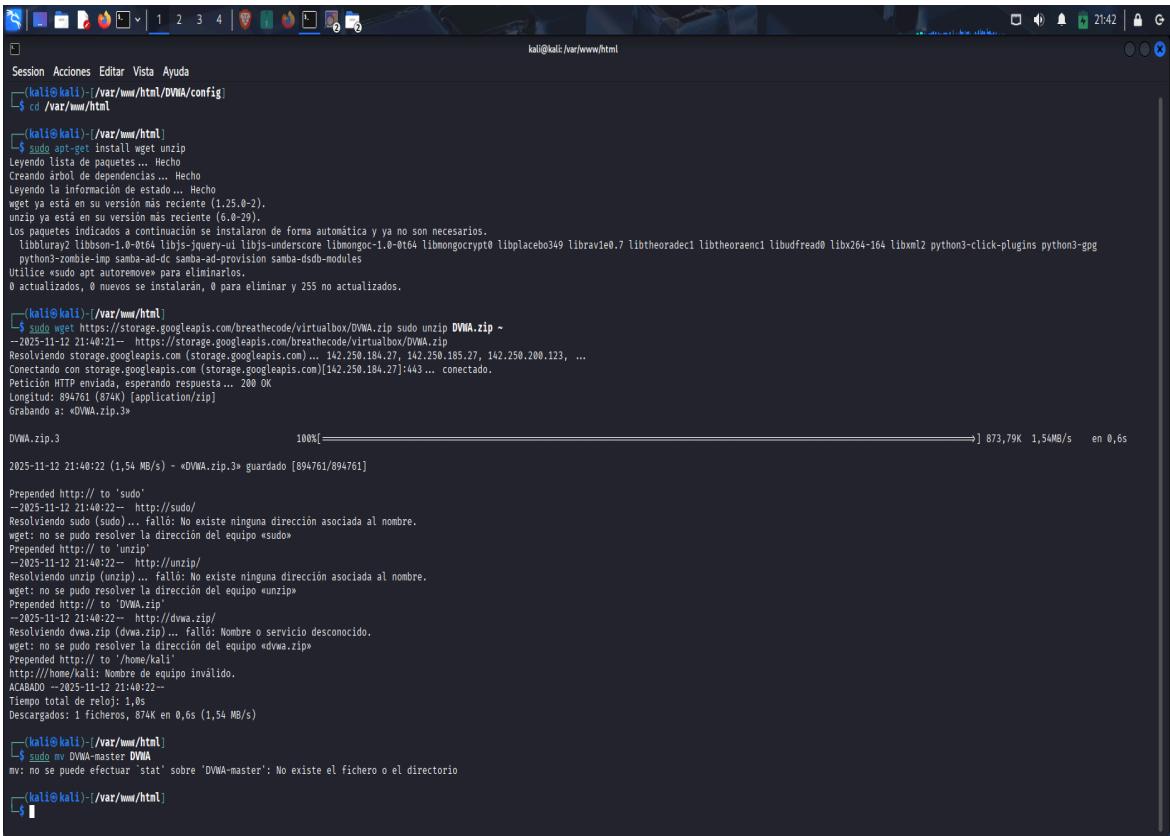


Vulnerabilidad SQL Injection

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:



```
(kali㉿kali)-[~/var/www/html]
$ cd /var/www/html
(kali㉿kali)-[~/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 (1.25.0-2).
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.
liblburay libssoray libjs-jquery-ul libjs-underscore libmongoc-1.0-0t64 libmongocrypt0 libplacebo349 libravle0.7 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.

(kali㉿kali)-[~/var/www/html]
$ sudo wget https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip -O DVWA.zip
--2025-11-12 21:40:22-- https://storage.googleapis.com/breathecode/virtualbox/DVWA.zip
Resolving storage.googleapis.com (storage.googleapis.com)... 142.250.184.27, 142.250.185.27, 142.250.200.123, ...
Conectando con 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)... Fallo: 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)... Fallo: 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)... Fallo: 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)

(kali㉿kali)-[~/var/www/html]
$ sudo mv DVWA-master DVWA
mv: no se puede efectuar 'stat' sobre 'DVWA-master': No existe el fichero o el directorio

(kali㉿kali)-[~/var/www/html]
```

- 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 libbison-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 validar las entradas del usuario antes de usarlas en consultas SQL.

 2. Usar consultas preparadas (prepared statements) o parámetros en lugar de concatenar directamente.
 3. Limitar los privilegios del usuario de base de datos que usa la aplicación, para reducir el impacto en caso de vulnerabilidad.
 4. Implementar y realizar pruebas de seguridad de manera periodica

```
Sesión Acciones Editar Vista Ayuda
[kali㉿kali]:~/var/www/html/DVWA/config
$ cd DVWA/config
[kali㉿kali]:~/var/www/html/DVWA/config
$ sudo cp config.inc.php.dist config.inc.php
[sudo] contraseña para kali:
[REDACTED] SETTING UP las entradas del usuario antes de usarlas en consultas SQL.

[kali㉿kali]:~/var/www/html/DVWA/config
$ sudo nano config.inc.php
[kali㉿kali]:~/var/www/html/DVWA/config
$ ./dvwa
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.7.29-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE dvwa;
ERROR 1007 (HY000): Can't create database 'dvwa'; database exists
MariaDB [(none)]> \q
Bye
el sistema de base de datos que usa la aplicación, para
realizar pruebas de vulnerabilidad.
[kali㉿kali]:~/var/www/html/DVWA/config
$ ./dvwa
[REDACTED]
```

```
kali㉿kali:~/var/www/html/DVWA/config
```

```
Session Acciones Editar Vista Ayuda
GNU nano 8.6 config.inc.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 @dgininfa 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';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'dvwa';
$_DVWA[ 'db_password' ] = 'tu_contraseña_de_root';
$_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' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
# Default value for the security level with each session.
# The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default locale
# Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

# Disable authentication
# Some tools don't like working with authentication and passing cookies around
# If you are getting errors, try setting this to true.
$_DVWA[ 'disable_authentication' ] = false;
```