Procedure

┌──(kali㉿kali)-[~]

└─$ cd /var/www/html

┌──(kali㉿kali)-[/var/www/html]

└─$ git clone https://github.com/digininja/DVWA.git

fatal: could not create work tree dir 'DVWA': Permission denied

┌──(kali㉿kali)-[/var/www/html]

└─$ sudo git clone https://github.com/digininja/DVWA.git

[sudo] password for kali:

Cloning into 'DVWA'...

remote: Enumerating objects: 3934, done.

remote: Counting objects: 100% (43/43), done.

remote: Compressing objects: 100% (21/21), done.

remote: Total 3934 (delta 21), reused 37 (delta 21), pack-reused 3891

Receiving objects: 100% (3934/3934), 1.74 MiB | 7.74 MiB/s, done.

Resolving deltas: 100% (1836/1836), done.

┌──(kali㉿kali)-[/var/www/html]

└─$ ls

DVWA index.html index.nginx-debian.html

┌──(kali㉿kali)-[/var/www/html]

└─$ mv DVWA dvwa

mv: cannot move 'DVWA' to 'dvwa': Permission denied

┌──(kali㉿kali)-[/var/www/html]

└─$ sudo mv DVWA dvwa

┌──(kali㉿kali)-[/var/www/html]

└─$ ls

dvwa index.html index.nginx-debian.html

┌──(kali㉿kali)-[/var/www/html]

└─$ sudo chmod -R 777 dvwa/

┌──(kali㉿kali)-[/var/www/html]

└─$ cd dvwa

┌──(kali㉿kali)-[/var/www/html/dvwa]

└─$ ls

about.php dvwa instructions.php README.fr.md security.php

CHANGELOG.md external login.php README.md setup.php

config favicon.ico logout.php README.tr.md tests

COPYING.txt hackable phpinfo.php README.zh.md vulnerabilities

database ids\_log.php php.ini robots.txt

docs index.php README.ar.md SECURITY.md

┌──(kali㉿kali)-[/var/www/html/dvwa]

└─$ cd config

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ ls

config.inc.php.dist

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo cp config.inc.php.dist config.inc.php

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo nano config.inc.php

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo service mysql start

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo mysql -u root -p

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 31

Server version: 10.6.8-MariaDB-1 Debian buildd-unstable

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;

Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user 'admin'@127.0.0.1 identified by 'password';

Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> grant all on dvwa.\* to 'admin'@127.0.0.1;

Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit;

Bye

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ cd /etc/php/8.1/apache2

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ ls

conf.d php.ini

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ sudo nano php.ini

┌──(kali㉿kali)-[/etc/php/8.1/apache2]

└─$ cd /var/www/html/dvwa/config/

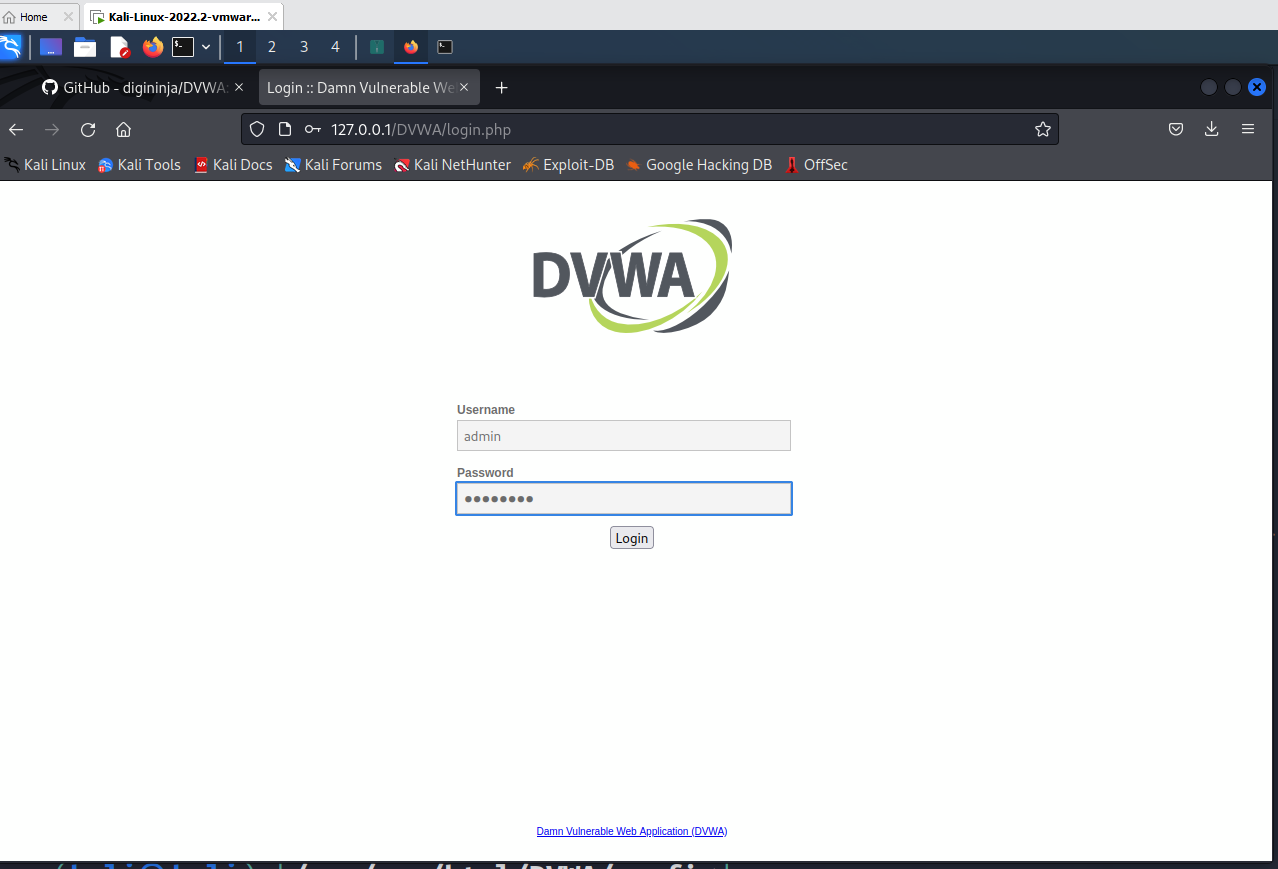
┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo service apache2 start

┌──(kali㉿kali)-[/var/www/html/dvwa/config]

└─$ sudo service mysql start

observation



Use % ‘or’ 1=1

