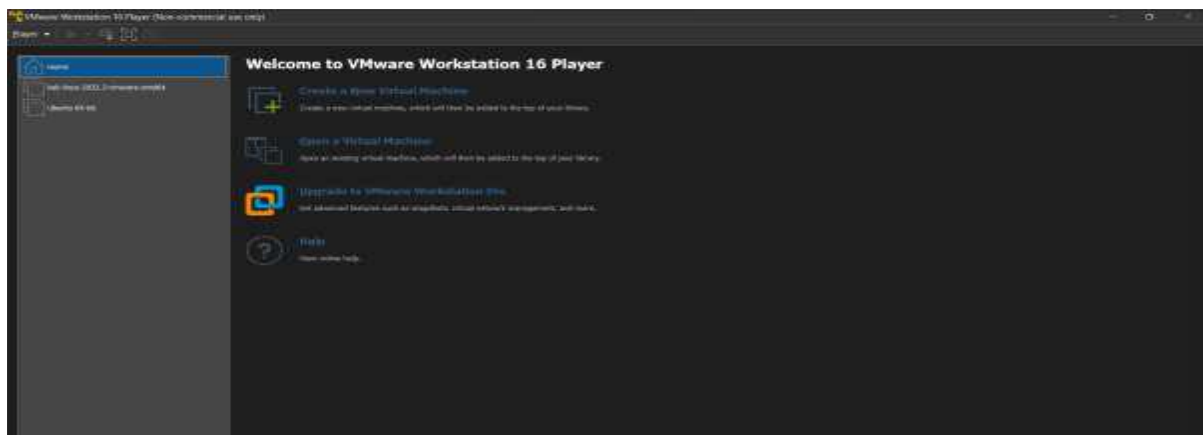


Download VMWare Workstation Player and Load Kali Linux OS into it.



Open Kali Linux, with default user name and password as 'Kali' and 'Kali'.

- Open Terminal and Download DVWA application from GitHub using command: '**sudo git clone https://www.github.com/digininja/DVWA**'
- Change the permissions to the folder DVWA using 'chmod' command.

```
(kali㉿kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
^[[B^[[B^[[B^[[B^[[Bremote: Enumerating objects: 3990, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 3990 (delta 0), reused 3 (delta 0), pack-reused 3986
Receiving objects: 100% (3990/3990), 1.79 MiB | 1.31 MiB/s, done.
Resolving deltas: 100% (1858/1858), done.

(kali㉿kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Navigate to 'DVWA/Config/config.inc.php.dist' and make a copy with name 'config.inc.php'

- Now, Open 'config.inc.php' file in Nano Editor.

```
(kali㉿kali)-[/var/www/html]
$ cd DVWA/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
```

After opening the file, check the username and password of DVWA application , Edit if you want.

```
File Actions Edit View Help
GNU nano 6.3 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 @diglinja 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'] = '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'dvwa';
$_DVWA['db_password'] = 'dvwapw';
$_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'] = '';
```

Now, install MySQL Server using following command:

‘sudo apt install default-mysql-server’

○ Now, start the service and check the status in SystemCTL.

```
File Actions Edit View Help
$ sudo apt install default-mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
default-mysql-server is already the newest version (1.0.8).
0 upgraded, 0 newly installed, 0 to remove and 1319 not upgraded.

kali@kali:~/var/www/html/DVWA/config$ sudo service mysql start

kali@kali:~/var/www/html/DVWA/config$ systemctl status mysql
● mariadb.service - MariaDB 10.6.8 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 05:56:35 EST; 2s ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Process: 3239 ExecStartPre=/usr/bin/install -w 755 -o mysql -g root -d /var/run/mysql (code=exited, status=0/SUCCESS)
   Process: 3241 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 3245 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR= cd /usr/bin/..; /usr/bin/galera_recovery; [ $? -eq 0 ] && s=
   Process: 3291 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 3291 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 3274 (mariadb)
   Status: "Taking your SQL requests now..."
   Tasks: 14 (limit: 2283)
   Memory: 98.7M
   CPU: 1.733s
   OGroup: /system.slice/mariadb.service
          └─3274 /usr/sbin/mariadbd
```

Now, Open MySQL Terminal and Create a DVWA user with past credentials and Grant him all privileges on DVWA folder.

○ Now, Install PHP using following command: **‘sudo apt install php’** Now,

```

(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 builddd-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 user 'dvwau'@'127.0.0.1' identified by 'dvwap';
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> grant all privileges on DVWA.* to 'dvwau'@'127.0.0.1' identified by 'dvwap';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
Bye

```

Now, Install PHP using following command:

‘sudo apt install php’

○ Now, Install PHP extensions required.

‘sudo apt install php-{extension1,extension2,...}’

```

(kali@kali)-[/var/www/html/DVWA/config]
$ sudo apt install php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
php is already the newest version (2:8.1+92+nmu1).
0 upgraded, 0 newly installed, 0 to remove and 1319 not upgraded.

(kali@kali)-[/var/www/html/DVWA/config]
$ sudo apt install php-{imap,bcmath,bz2,intl,gd,mbstring,mysql,zip}
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
php-imap is already the newest version (2:8.1+92+nmu1).
php-bcmath is already the newest version (2:8.1+92+nmu1).
php-bz2 is already the newest version (2:8.1+92+nmu1).
php-intl is already the newest version (2:8.1+92+nmu1).
php-gd is already the newest version (2:8.1+92+nmu1).
php-mbstring is already the newest version (2:8.1+92+nmu1).
php-mysql is already the newest version (2:8.1+92+nmu1).
php-zip is already the newest version (2:8.1+92+nmu1).
0 upgraded, 0 newly installed, 0 to remove and 1319 not upgraded.

(kali@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.1

(kali@kali)-[/etc/php/8.1]
$ ls
apache2  cli  mods-available

```

Now, Navigate to **‘php/8.1/apache2’** folder and Open **‘php.ini’** file in Nano editor.

○ In that file, Make sure these two fields are set to be **On**.

allow_url_fopen

allow_url_include

```
#####
; Fopen wrappers ;
#####

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
;user_agent="PHP"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
^C Location  ^_ Go To Line
```

Now, Start the apache2 server and Check the status in systemCTL.

```
kali@kali:~/etc/php/8.1/apache2$ sudo nano php.ini
kali@kali:~/etc/php/8.1/apache2$ sudo service apache2 start
kali@kali:~/etc/php/8.1/apache2$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 06:01:19 EST; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4619 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 4636 (apache2)
       Tasks: 6 (limit: 2283)
      Memory: 22.4M
         CPU: 249ms
    CGroup: /system.slice/apache2.service
            └─636 /usr/sbin/apache2 -k start
              638 /usr/sbin/apache2 -k start
              639 /usr/sbin/apache2 -k start
              640 /usr/sbin/apache2 -k start
              641 /usr/sbin/apache2 -k start
              642 /usr/sbin/apache2 -k start

Nov 24 06:01:19 kali systemd[1]: Starting The Apache HTTP Server...
Nov 24 06:01:19 kali apachectl[4635]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive dynamically to determine the server's name.
Nov 24 06:01:19 kali systemd[1]: Started The Apache HTTP Server.
lines 3-20/20 (END)
```

Now, Open any browser and Go to Local Host:

'http://127.0.0.1/dvwa.login.php'

○ Enter the Credentials, **admin** as username and **password** as password.

