# Setup a Vulnerable Web Server DVWA in Kali Linux localhost

# Why we need a vulnerable web server?

Attacking on a website or server in internet without legal permission will considered as crime. Practice makes perfect, but where to practice our hacking skills ?

A simple answer is on our localhost. Localhost is a locally hosted web server it can be hosted on our PC and not connected to the internet.

There is a famous quote "There is no place like 127.0.0.1". This 127.0.0.1 is our home server or local server. This is an awesome place to learn and practice our skills. That's why it is the best place. No place can better then localhost.

# How to set up?

<u>DVWA</u> stands for Damn Vulnerable Web Application. Oh yes, it is too vulnerable. In this web application security researchers, penetration testers or ethical hackers test their skills and run tools in a legal environment.



DVWA is designed for practice some most common web vulnerability. It is made with PHP and mySQL. Let's start without wasting time.

In Linux environment localhost files are stored in /var/www/html directory, so we open a terminal and change our directory to that directory using following command:

cd /var/www/html

Here we clone DVWA from it's <u>Github repository</u>. To clone it we run following command:

# git clone https://github.com/ethicalhack3r/DVWA

```
root@kali:~# cd /var/www/html
root@kali:/var/www/html# git clone https://github.com/ethicalhack3r/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 3022 (delta 3), reused 2 (delta 0), pack-reused 3011
Receiving objects: 100% (3022/3022), 1.53 MiB | 123.00 KiB/s, done.
Resolving deltas: 100% (1327/1327), done.
root@kali:/var/www/html#
```

After the cloning complete, we rename the DVWA to dvwa (it is not necessary but it will save our effort).

Then we change the permission on dvwa directory by using following command:-



Now we have to setup this web application to run properly for that we have to go into /dvwa/config directory.

Using Is command we can the list of files.





In the above screenshot we can see the config.inc.php.dist file. This file contains default configuration. We need to make a copy of this file with .php extension name, we are coping this file because in future if anything goes wrong then we have the default values. So we copy this file with .php extension name using following command:-

## cp config.inc.php.dist config.inc.php

Then we check the copied file using ls command:



Then we use nano editor to make changes on our newly created PHP file.



The screenshot is following:-

```
.
                          root@kali: /var/www/html/dvwa/config 80x24
  GNU nano 4.5
                                     config.inc.php
    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 >
    Please use a database dedicated to DVWA.
 If you are using MariaDB then you cannot use root, you must use create a dedi>
    See README.md for more information on this.
 DVWA = array();
 DVWA[ 'db_server
                         = '127.0.0.1';
 DVWA[ 'db_database' ] = 'dvwa';
 DVWA[ 'db_user' ]
                         = 'root';
 DVWA[ 'db_password' ] = 'p@ssw0rd';
# Only used with PostgreSQL/PGSQL database selection.
 DVWA[ 'db_port '] = '5432';
```

We will make changes in this part the p@ssw0rd to pass and the user from root. Watch the following screenshot:-



Then we save it using CTRL+X and press Y to save changes and Enter button to save and exit.

The next is configuring the database.

Here we have opened a new terminal window closing the previous one. We start the mysql at first using following command:-

#### service mysql start

If there are no errors that means the service is started.

Now let's login to mysql using following command:-



Here in our Kali Linux root is our superuser name, if we have something else then we need to change that user.

In the password field we press Enter without typing password; because we didn't set any password for it, now mysql will open like following screenshot:-



Now to setup a database, we start with creating a new user by applying following command:-

### create user 'user'@'127.0.0.1' identified by 'pass';

Here using this command we are creating a user called 'user' running server on 127.0.0.1(localhost) and the password is 'pass'. Remember that this username and password should exactly same as the password and username we have entered in the configuration file of dvwa web application.

```
MariaDB [(none)]> create user 'user'@'127.0.0.1' identified by 'pass';
Query OK, 0 rows affected (0.002 sec)
```

In the screenshot we can see the query is OK. That means the user is created.

Then we grant this user all the privileges over the database. For that we type following command:-

grant all privileges on dvwa.\* to 'user'@'127.0.0.1' identified by 'pass';

MariaDB [(none)]> grant all privileges on dvwa.\* to 'user'@'127.0.0.1' identified by 'pass' Query OK, 0 rows affected (0.021 sec)

MariaDB [(none)]>

Yes, we have finished the work of database, now we configure the server. For this we need to configure our apache2 server. Let's change our directory to /etc/php/7.3/apache2

Here we are using version 7.3, if we use another version then the path might be change.

## cd /etc/php/7.3/apache2

Here we configure the php.ini file using leafpad of any good text editor. We have used mousepad editor.

#### mousepad php.ini

We need to change the *allow\_url\_fopen* and *allow\_url\_include* values. We set both of them 'On'. In some cases when we are first time configuring it, we might find that one of this or both of this configuration is set to 'Off'. We have turned both of these configuration to 'On', as the following screenshot:-



Then we save and close the file.

Then we start the apache2 server using following command:-

#### service apache2 start

Let's open the browser and navigate to 127.0.0.1/dvwa/ first open will open the setup.php as shown in the screenshot.



Here we scroll down and click on "Create/Reset Database".

 MySQL username: user

 MySQL password: \*\*\*\*\*\*

 MySQL database: dvwa

 MySQL host: 127.0.0.1

 reCAPTCHA key: Missing

 [User: root] Writable folder /var/www/html/dvwa/hackable/uploads/: Yes

 [User: root] Writable folder /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: Yes

 [User: root] Writable folder /var/www/html/dvwa/config: Yes

 Status in red, indicate there will be an issue when trying to complete some modules.

 If you see disabled on either allow\_url\_fopen or allow\_url\_include, set the following in your php.ini file and restart Apache.

 allow\_url\_fopen = 0n

 allow\_url\_include = 0n

 These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Then it will create and configure the database and we redirected to DVWA login page.

	Login I	Dama Vulnerable Web Application (DVWA) v1.10 *Development* - Mozilla Firefox		_ = ×
Login :: Damn Vulnerable W 🗙	+			
( → ℃ @	③ 127.0.0.1/dvwa/login.php		🖂 🏠	i\ 00 40 ≣
🔨 Kali Linux 🚿 Kali Training 🚿	Kali Training 💊 Exploit-DB 💊	GHDB		
		DIMAIA		
		DV(WA)		
		Username		
		Pwssword		
		Login		
		Denn, Valverable, Web Application (DVWA)		

The default login is

- Username:- admin
- Password:- password

After login we are in Damn Vulnerable Web Applications main page. Here is some general information and warnings.



On the left side we can see lots of vulnerable pages are available we can practice here.

DVWA have different security levels to change those we navigate to DVWA security. There are some security levels low, medium, high, impossible. We can choose difficulty as we need.

	DY/WA Security II Damn Yulinerable Web Application (DY/WA) v1.10 *Development* - Neažla Firefox											
DVWA Security :: Damn X	+											
← → @ ŵ	③ 127.0.0.1/dvwa/secu	© 127.0.0.1/dvwa/security.php					E … ⊠ ☆		IIA CC		=	
🔨 Kali Linux 🔨 Kali Training 🗎	Kali Training 👛 Exploit-0	B 💊 GHDB										
			D	<b>WA</b>								
	Home	DVWA Se	ecurity									
	Instructions											
	Setup / Reset DB	Security Le	evel									
	Brute Force Command Injection	Security level is currently: <b>Impossible</b> . You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:										
	CSNP	1. Low - This a as an exam	ecurity level is ple of how web	completely vulnerable a application vulnerabilitie	nd has no security meas a manifest through bad co	ures at all. It ding practices	's use is s and to	serve				
	File Inclusion	as a platform 2. Medium - Ti	n to teach or le	am basic exploitation technical and example	chriques. to the user of had securi	ty practices.	where th	10				
	Hie Opidad	c. Indexter has being to many to get an example to one size on the second point operating processing index the developer has the dot bill all be secure an application. It is also acts as a challenge to users to refine the exploitation techniques. 3. High -This option is an extension to the medium difficulty, with a mixture of harder or alternative bad										
	SOL Injection							bad				
	SQL Injection (Rind)	exploitation.	similar in vari	cure the code. The vulne ous Capture The Flags (C	rability may not allow the s CTFs) competitions.	same extent o	of the					
	Weak Session IDs	<ol> <li>Impossible source code</li> </ol>	This level sho to the secure	uld be secure against a source code.	Il vulnerabilities. It is use	ed to compare	the vul	nerable				
	XSS (DOM)	Prior to DVN	WA v1.9, this is	wel was known as 'high'.								- 1
	XSS (Reflected)	High 🛩	Submit									
	XSS (Stored)	Low										
	CSP Bypass	Medium										
	JawaScript	High M <sup>1</sup> Impossible	-Intrusion Det	ection System) is a secu	rity layer for PHP based w	veb applicatio	nsi.					
	OVWA Security PHP Into	PHPIDS works by DVWA to serve as some cases how V	filtering any us a live example WAFs can be c	er supplied input against of how Web Application icumvented.	a blacklist of potentially n Firewalls (WAFs) can hel	alicious code p improve sec	outly an	sed in d in				

Now we can run penetration testing tools and techniques in our localhost.

This is how we can setup **DVWA**, Damn Vulnerable Web Application in our **Kali Linux** system. This is very helpful for beginners to advanced users, because of it multilayered security levels.