

Forum:[Hack Forums](#)

Thread: [How to setup DVWA for penetration testing \(Damn Vulnerable Web Application\)](#)

Revelations - November 14, 2019, 4:03 pm

What is DVWA?

According to google. 'DVWA is a DAMN VULNERABLE WEB APP coded in PHP/MYSQL. Seriously it is too vulnerable. In this app security professionals, ethical hackers test their skills and run this tools in a legal environment. ... The aim of DVWA is to practice some of the most common web vulnerability, with various difficulties levels.'

DVWA has a number of vulnerabilities that allow you to test your skills; Brute forcing, command injections, CSRF, file inclusion, file uploading, captchas, SQLi, XSS, CSP, and Java Script. There are different levels of security to test your skills. Low, medium, and high.

What you need.

Basic knowledge of how to use Kali Linux

Latest version of Kali Linux, either in a Virtual machine. (VMware, Virtualbox) or a bootable usb.

Setting up DVWA for the first time.

Before we start be sure not to copy and paste commands! You need repetition so that one day you will be able to do this on your own!

Start by booting into Kali Linux and opening a terminal. We are going to setup DVWA on our own local system. So firstly we need to change to the directory that has all the appropriate files for running a web application.

Code `cd /var/www/html/`

Now we need to clone into DVWA.

Code `git clone https://github.com/ethicalhack3r/DVWA.git`

The output should look like this.

Code Coning into 'DVWA'...

remote: Enumerating objects: 2986, done.

remote: Total 2986 (delta 0), reused 0 (delta 0), pack-reused 2986

Recieving objects: 100% (1322/1322), done.

Now we need to give this directory permissions.

Code `chmod -R 777 DVWA/`

Now we need to setup the application. Change directories.

Code `cd DVWA/config/`

In this directory there is a file with all the default configurations for DVWA, we need to make a copy of this file so that we can edit the new one to our specific needs.

Code `cp config.inc.php.dist config.inc.php.dist`

Now we will open this file in nano.

Code `nano config.inc.php`

The next part is completely optional but it makes it easier for us in the future. After you open the file in our nano text editor scroll down, you should see a line that says.

Code `$_DVWA[ 'db_password' ] = 'p@ssw0rd';`

We want to change p@ssw0rd, to pass. Other wise things could get complicated in the near future. Now ctrl + x to save.

Now clear the screen to return back to the default directory we started in.

Next we will configure the database,

Code `service mysql start`

we will be using username root.

Code `mysql -u root -p`

Now enter you password and you will see an output like this.

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

Your MariaDB connection id is 150

Server version: 10.3.12-MariaDB-2 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)]>

Now, we will start by creating a new user. We will be referring back to the config.inc.php for our username and password. enter the following command into your MariaDB prompt.

Code `create user 'root'@'127.0.0.1' identified by 'pass';`

Now we will be granting all the privileges to our new user, enter the following.

Code `grant all privileges on dvwa.* to 'root'@'127.0.0.1' identified by 'pass';`

Now type exit and clear. We have successfully sat up the web application and the database. Next we will configure the server. In order to configure it we need to start it first. We will be using Apache2. Type in

Code `service apache2 start`

Now we have to make some changes in the configuration file for apache2. Type in

Code `cd /etc/php/7.3/apache2/`

In this directory you should see the file php.ini, we will open it with gedit.

Code `gedit php.ini`

Now you should see a whole giant file full of codes and mumbo jumbo. What you want to do is scroll down about mid way and look for these..

Code `allow_url_fopen = Off`

and

Code allow_url_include = Off

In some cases these may be set to On. This is good. If not then switch them to On and click save.

Now start the apache2 server again.

Code service apache2 start

Done!

Now all that's left is to access the DVWA application on your local server!

Open your web browser and type in

Code 127.0.0.1/DVWA

You should see the web application!

Now the very last step, scroll down to the bottom and click create. You've just successfully set up the DVWA to practice your pentesting skills.

I will be making more tutorials focusing on the basics just like this in the future. Enjoy