Web Application Lab Setup

Today we are going to show you how you can set up a vulnerable web application server in a Windows system using Xampp. Here we will be configuring the most popular web applications (DVWA, bwapp, SQLI, Mutillidae). So, let's do that.

Table of Content

Requirement

- Web application
- Xampp Server Installation in Windows
- DVWA
- bWAPP
- Sqli
- Mutillidae

Requirement-Xampp server (Windows-X64)

Web Application

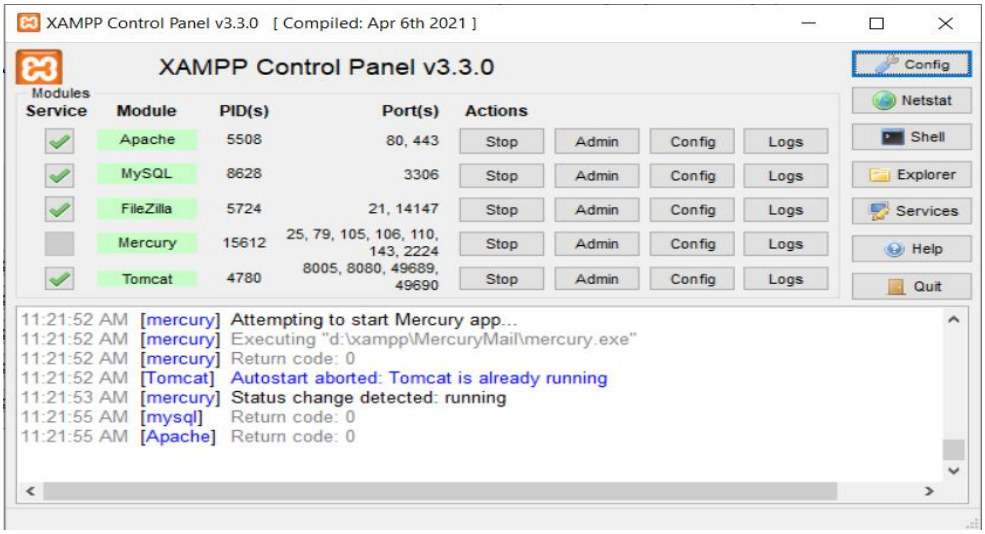
A web application is a computer program that utilizes web browsers and web technology to perform tasks over the Internet. Web apps can be built for a wider use which can be used by anyone; from an enterprise to an entity for a variety of reasons. Frequently used Web applications can include webmail.

Xampp Server Installation

XAMPP stand for Apache + MariaDB + PHP + Perl
XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible. (read more from Wikipedia)
Download from here

https://www.apachefriends.org/download.html

Once the installation is done, we need to start the service of Mysql and Apache service in Xampp server.



DVWA

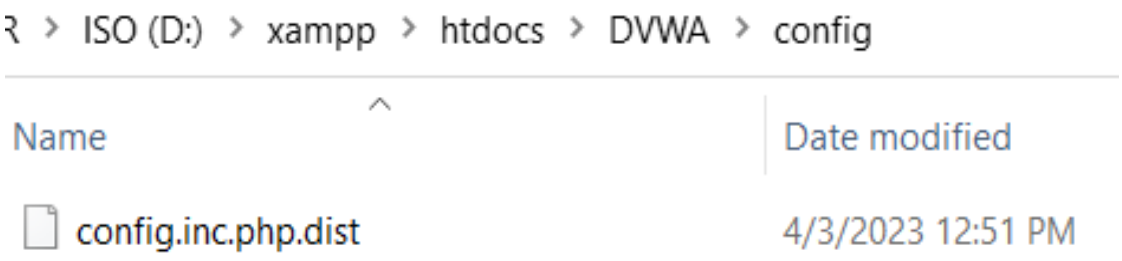
DVWA is a web application that is damn sensitive to PHP / MySQL. The main objectives are to provide security professionals with assistance to test their skills and resources in a legal environment, enable web developers to better understand the processes of protecting web applications and assist teachers/students to teach/learn protection in the classroom.

Download from here

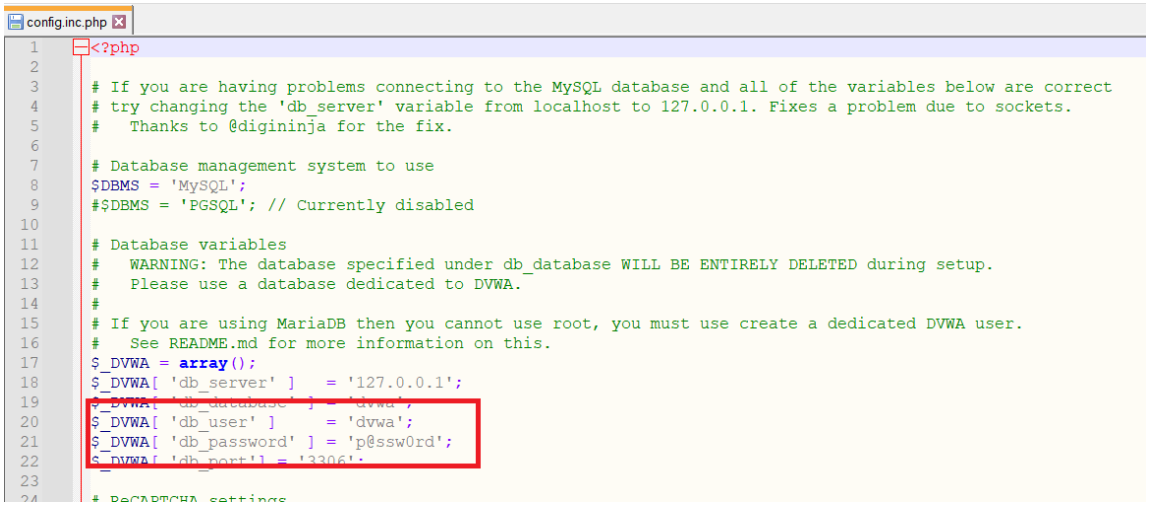
https://github.com/digininja/DVWA

Once the dvwa is installed completely then we will navigate to C:/Xampp/htdocs/dvwa/config.inc.php.dist to change the username and password for the database.

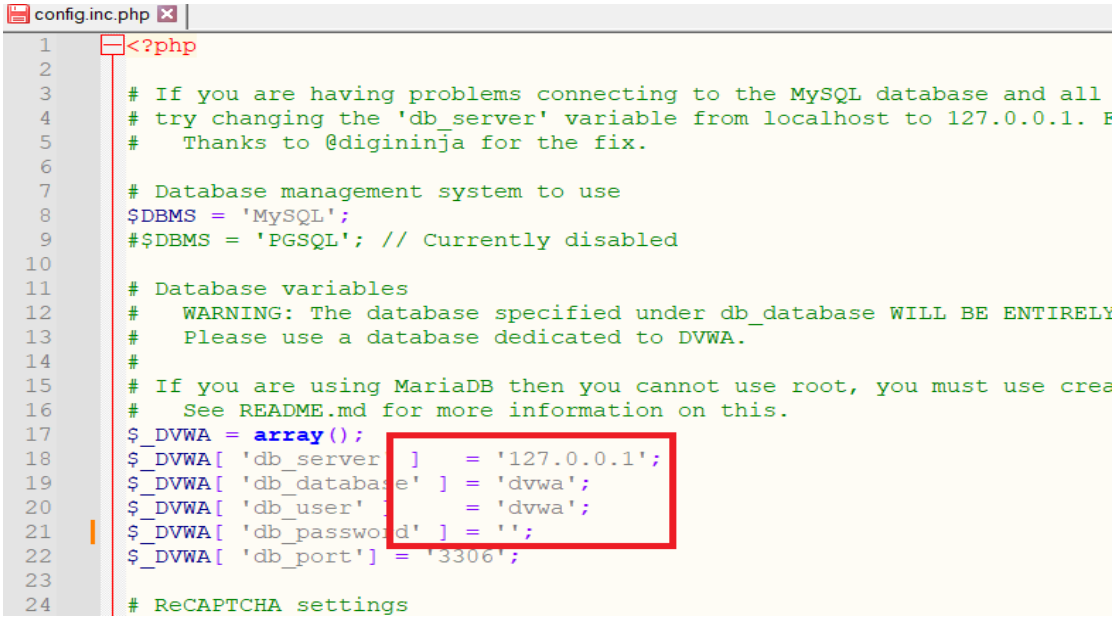
Open the configuration file to set the Username and Password.



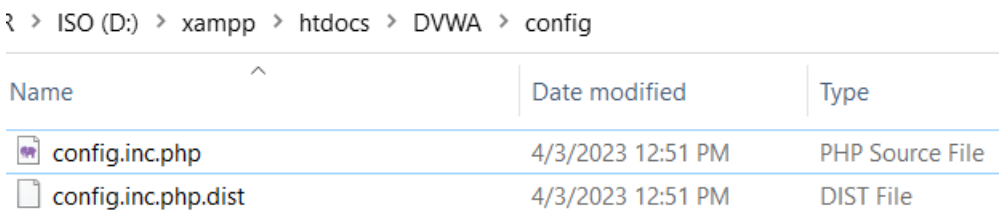
Here, you can notice that the default username is root and password is password which we will modify.



Now here you may notice that we have set the password “blank” for user “root”. Now save these settings and quit.



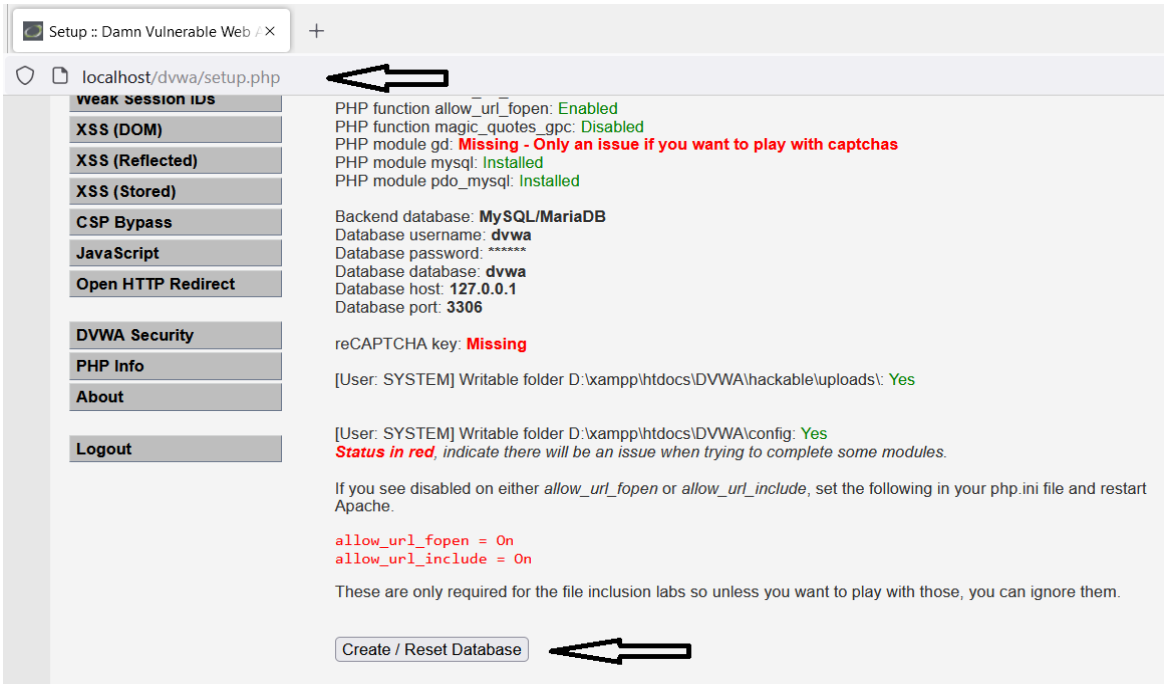
Rename the file as “config.inc.php” after making above changes and save it.



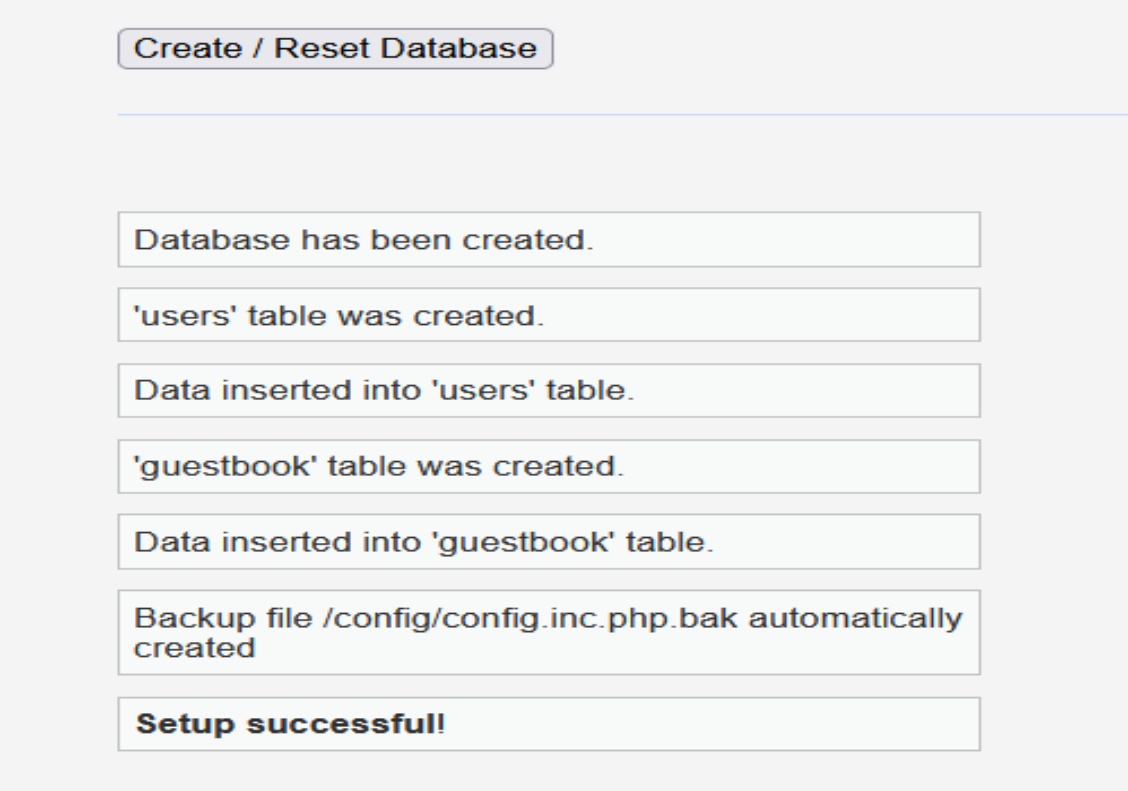
Now we need to open the DVWA application in our localhost to create the database

http://localhost/dvwa/setup.php

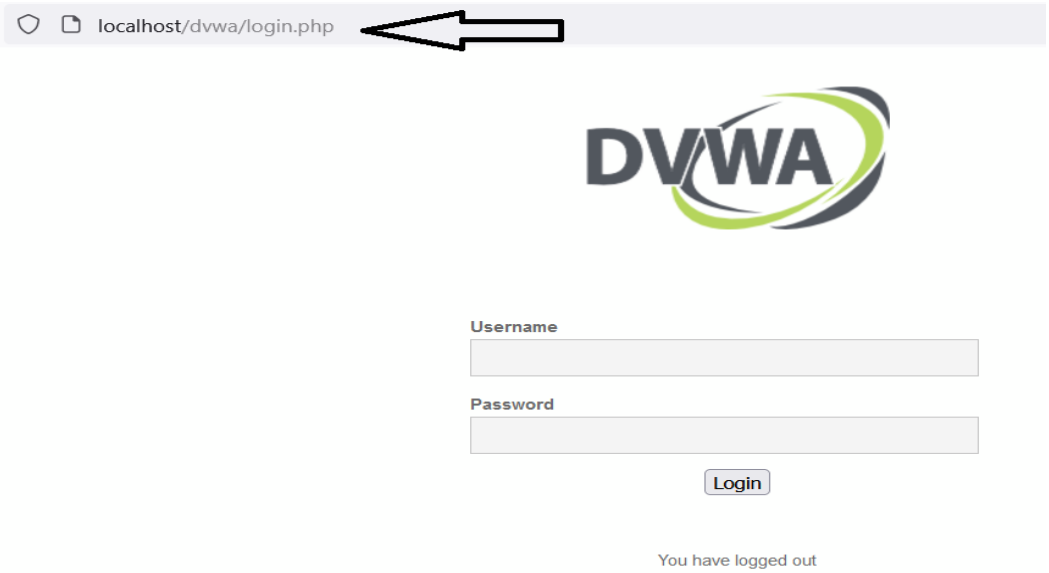
Now click on create database and database is created.



Now click on login and you are done with the setup.



For login, we will use the DVWA username which is **admin** and **password** which is DVWA password by default



Bwapp

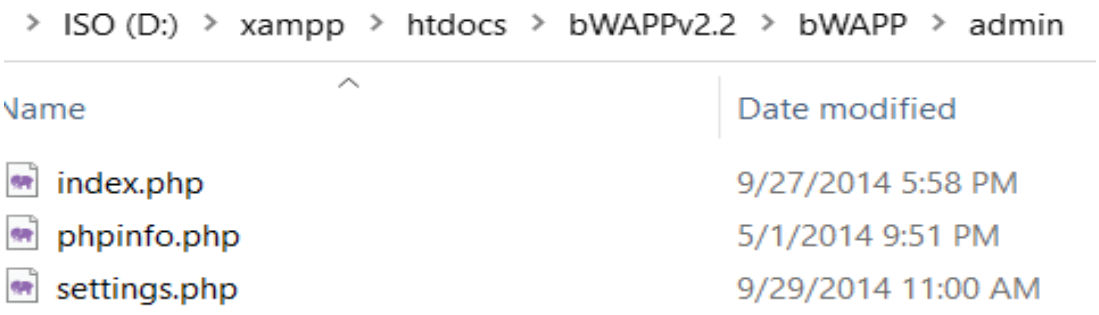
BWAPP is a free, open-source and intentionally unreliable web application, or a web buggy program. It helps security enthusiasts, designers and students discover Web bugs and stop them from doing so. BWAPP plans for positive penetration tests and cyber ethics initiatives.

Download it from here.

http://www.itsecgames.com/

https://sourceforge.net/projects/bwapp/files/bWAPP/

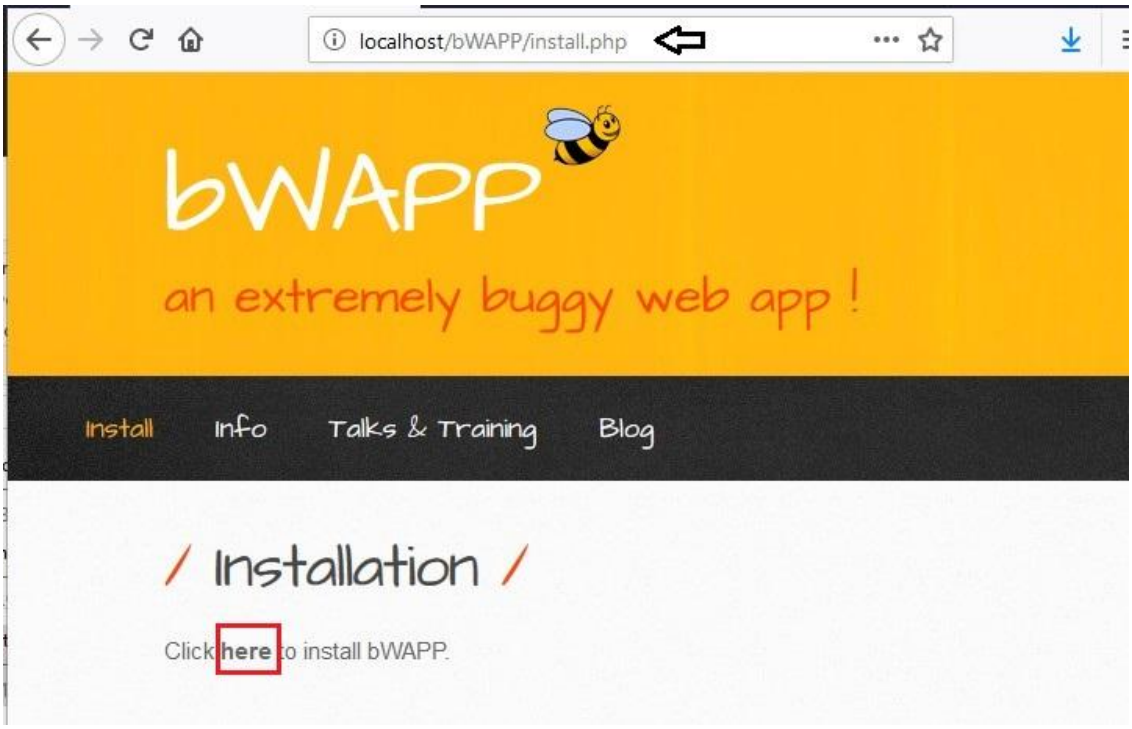
Now navigate to “C:/Xampp/htdoc/bwapp/admin” folder to change the default username and password for the database.



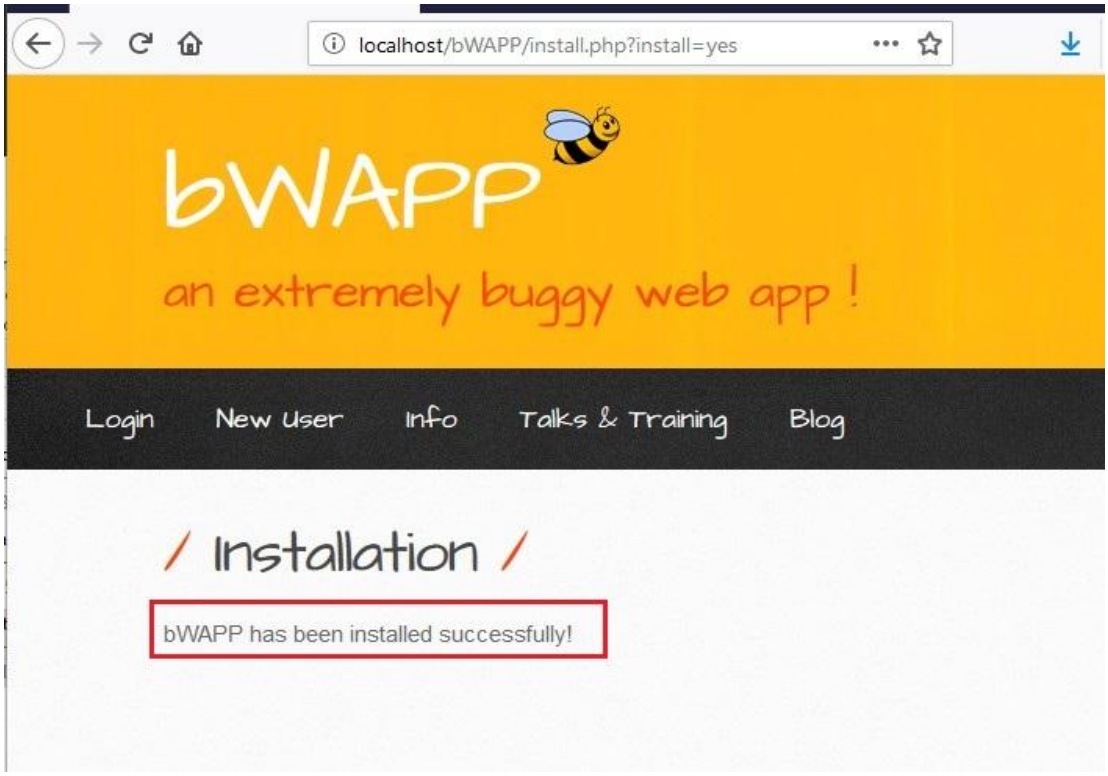
Now you can see that the default username is root and password is bug which we will modify.

Now here the username is root and password we have set blank. Now save the settings and quit.

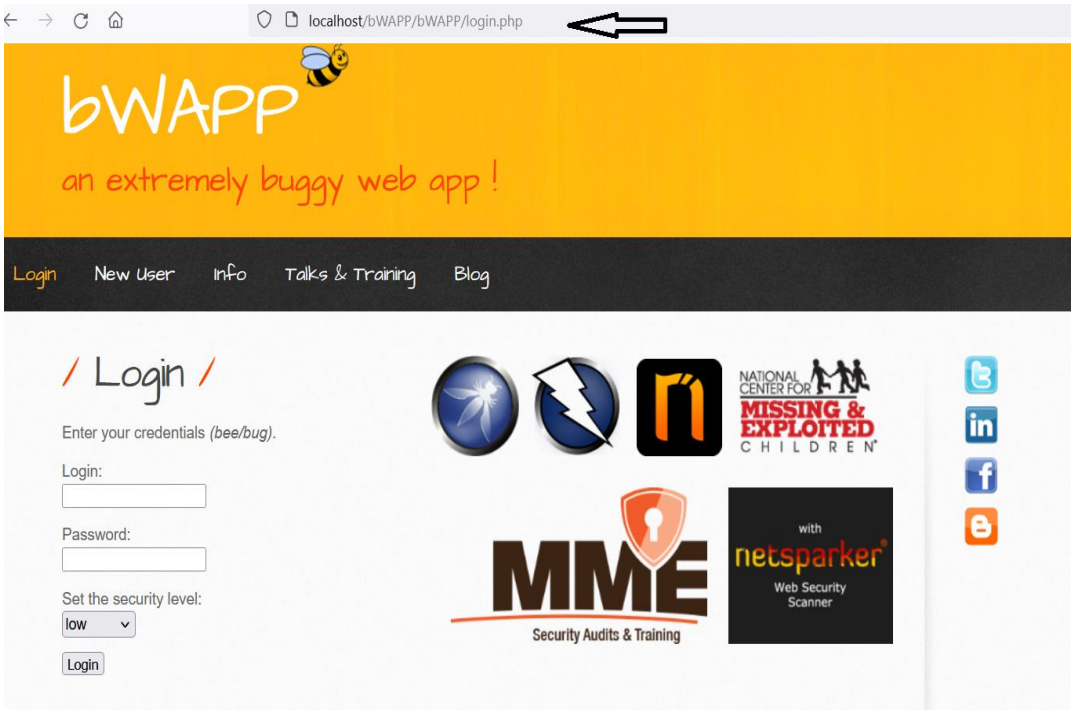
Now let’s open “bwapp/install.php” in the localhost and click on “here” to complete the installation.



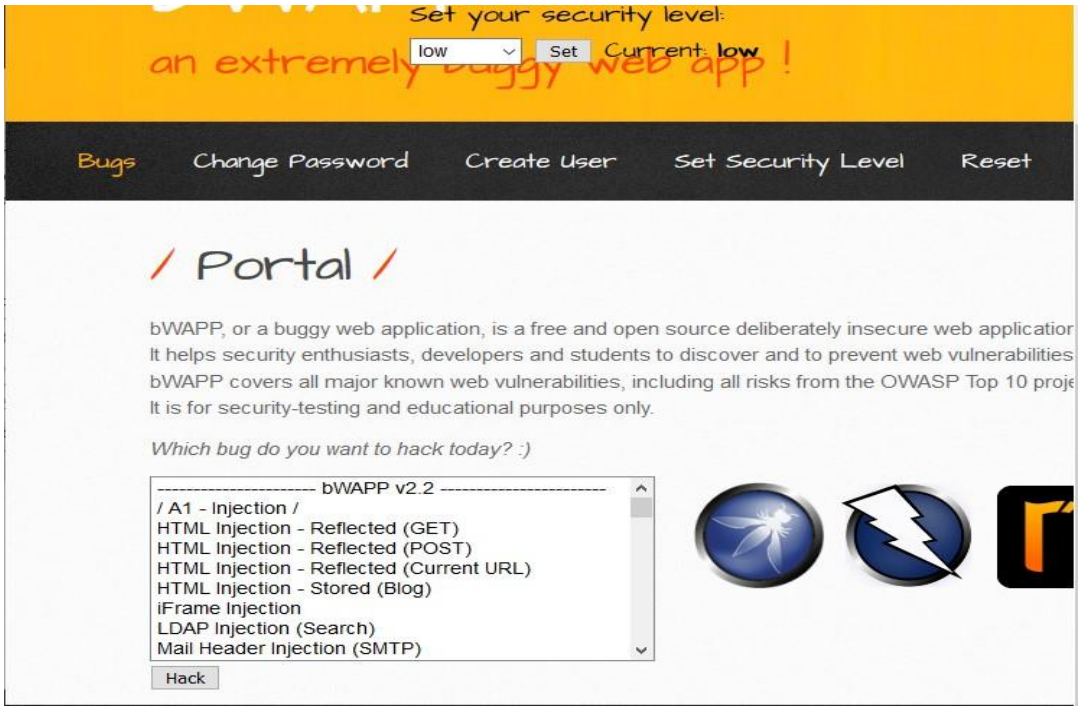
Now the installation is complete.



When you will login as bee:bug; you will get the portal to test your penetration testing skill



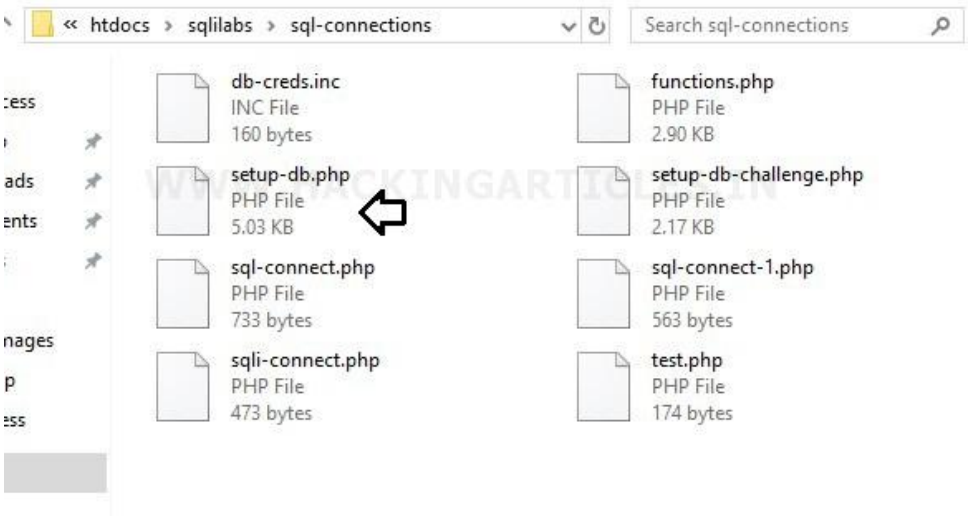
Here you can click on bugs and all bugs will be displayed to you which are there in bwapp web application.



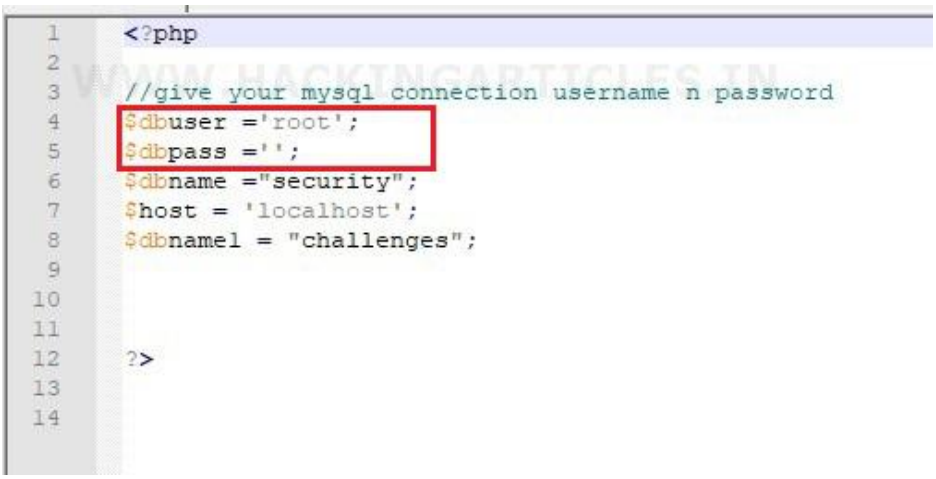
SQLI

SQLi: A facility that provides a robust testing environment for those involved in SQL injection acquisition and enhancement. Let’s start. First, we will download the SQLI lab through GitHub.

Now we will navigate to C:/htdocs/sqlilabs/sqli-connections to edit the setup-db.php.

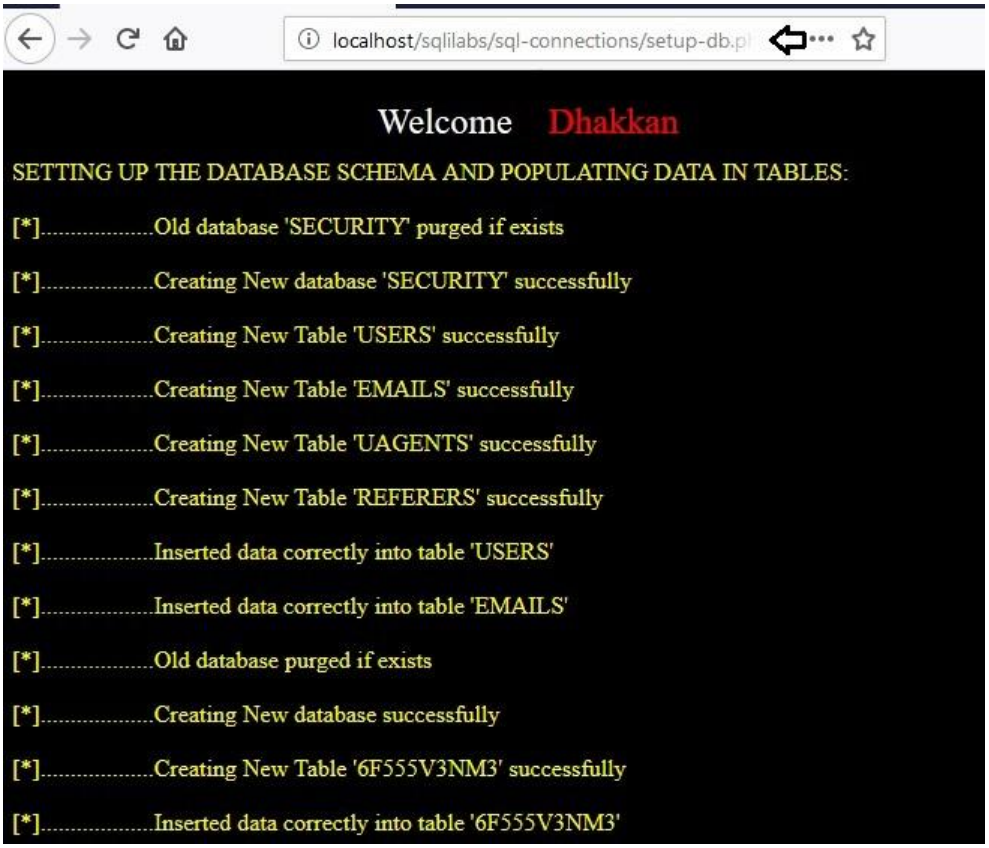


Now here we will set the password “blank” and save the changes and then quit.



Now browse this web application from through this URL: localhost/sqli and click on Setup/reset Databases for labs.

Now the sqli lab is ready to use. Now a page will open up in your browser which is an indication that we can access different kinds of Sqli challenges

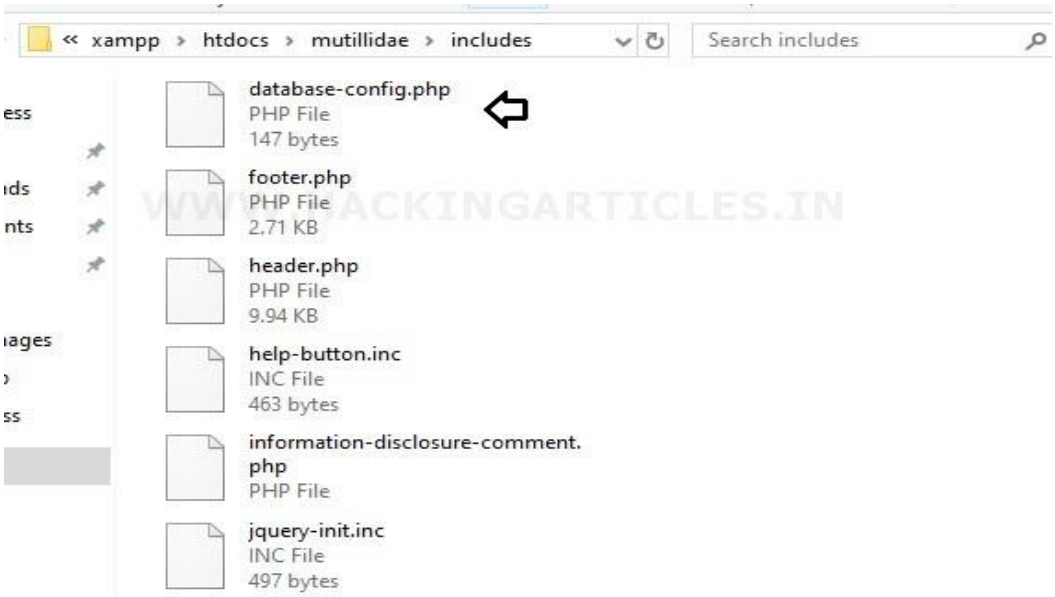


Now you can see that we have opened lesson 1. So, we have successfully set Sqli labs for practice.

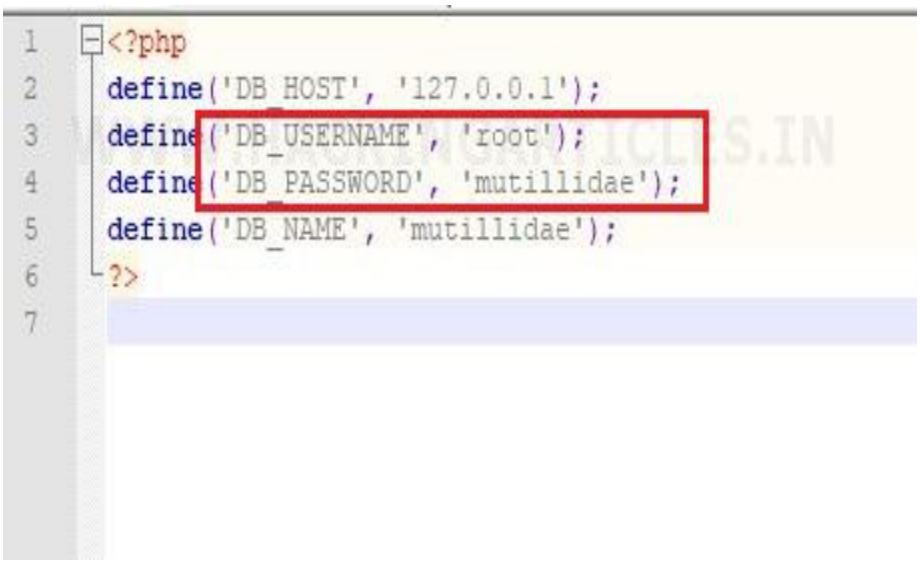
Mutillidae

OWASP Mutillidae is an open-source web application that is intentionally vulnerable and actively aims at web security. It's a laboratory for those involved in SQL injection acquisition and development, which offers a full test environment. This internet hacking framework is simple to use and is designed for labs, safety lovers, schools, CTFs and vulnerability assessments.

First, we will navigate to "C:/Xampp/htdocs/mutillidae/includes" to edit the "database-config.php" as shown below.

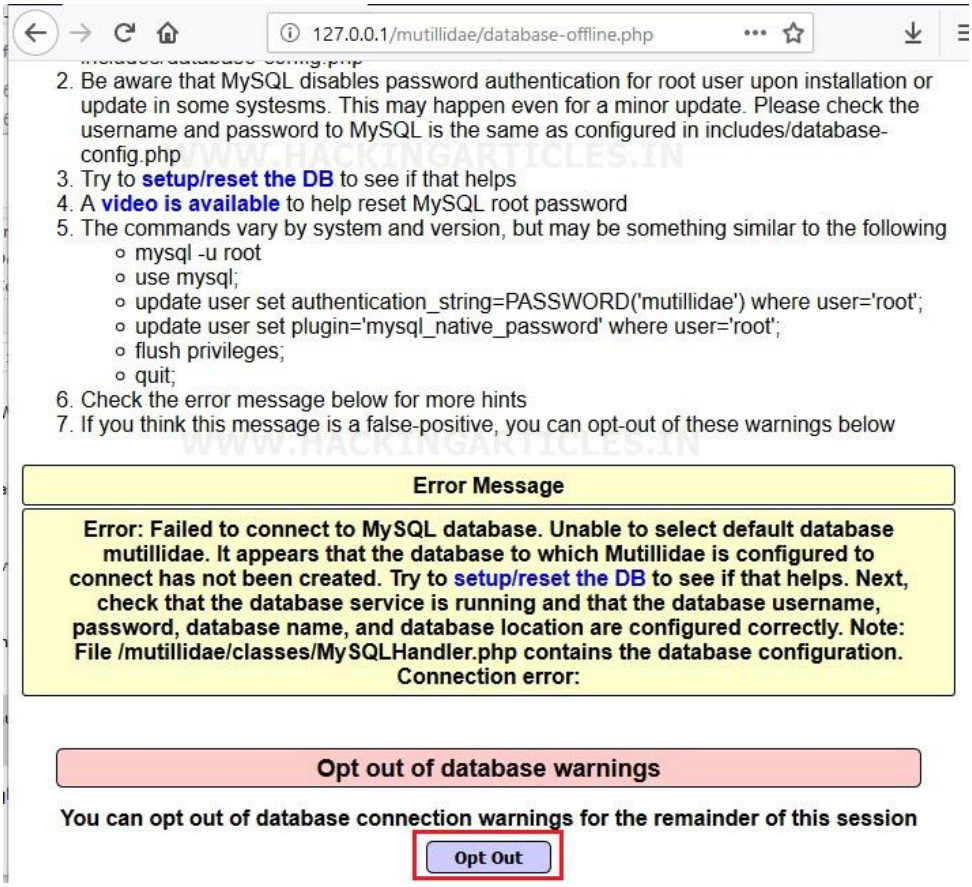


Here we can see that password is set mutillidae which we will replace with blank.



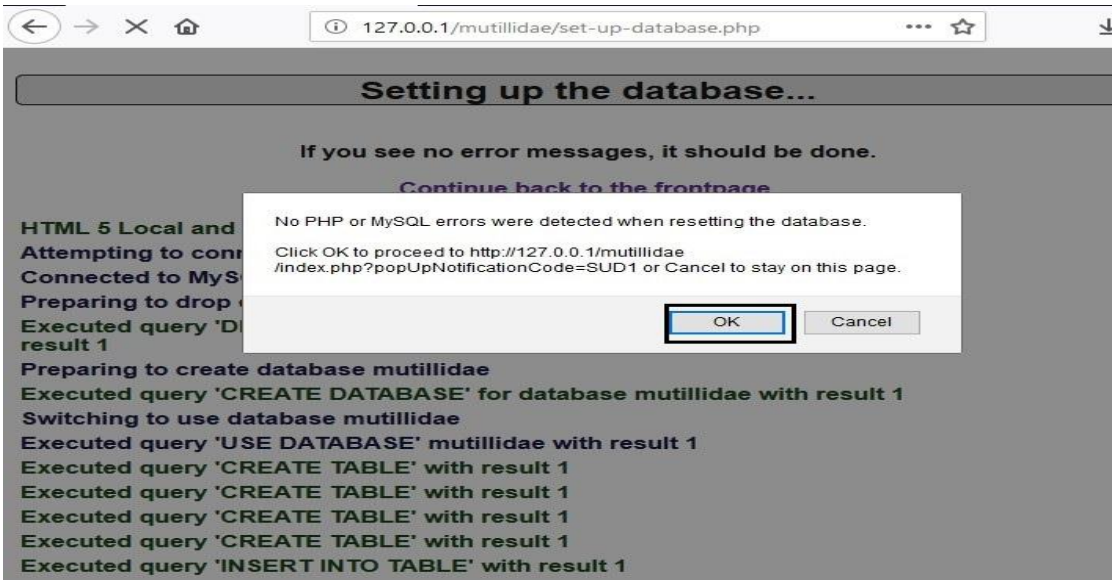
You can view that we have set the password "blank". Now save the settings and quit.

Now you can see the page where you need to click on opt out tap.



Now we will open this our local browser by the following URL: localhost/mutillidae where we will find an option of reset database. Just click on it to reset the database. So, In this way, we can setup our vulnerable web application lab for penetration testing.

Now you will be redirected to a page which will ask you to click ok to proceed. Here you need to click on OK and you are done with the configuration of the Mutillidae lab.



We have successfully set all the web applications in Xampp server in Windows.

Author: Geet Madan is a Certified Ethical Hacker, Researcher and Technical Writer at Hacking Articles on Information Security. Contact here

Now click on login and you are done with the setup.

For login, we will use the DVWA username which is admin and password which is DVWA password by default.

Bwapp

Now let’s set up a new lab which is BWAPP.

BWAPP is a free, open-source and intentionally unreliable web application, or a web buggy program. It helps security enthusiasts, designers and students discover Web bugs and stop them from doing so. BWAPP plans for positive penetration tests and cyber ethics initiatives.

Download it from here.

Now navigate to “C:/Xampp/htdoc/bwapp/admin” folder to change the default username and password for the database.

Now you can see that the default username is root and password is bug which we will modify.