

SETUP A VULNERABLE WEBSITE TO HACK!

By: AnOn Ali

What is bWAPP?

bWAPP, which stands for buggy Web Application, is an intentionally insecure web application. It contains numerous vulnerabilities and bugs typical of web applications, making it an ideal platform for security training and testing. We will be using it as our vulnerable site for practice.



What is Docker?

Docker is a platform that enables developers and administrators to easily create, deploy, and run applications in containers. Containers package up the application with all of its dependencies, ensuring that it runs consistently across different computing environments. We will use Docker to set up bWAPP (the vulnerable site).

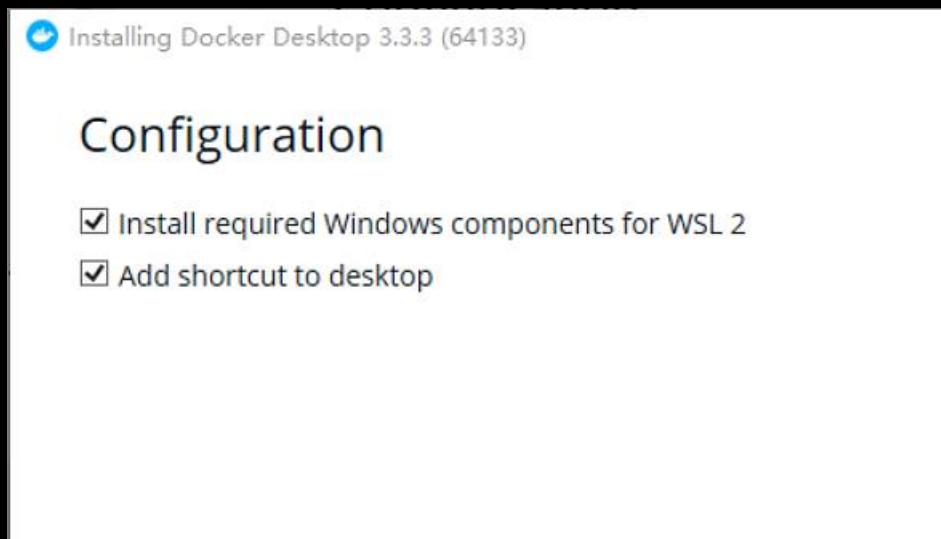


Setup Steps for Windows:

1: Install Docker

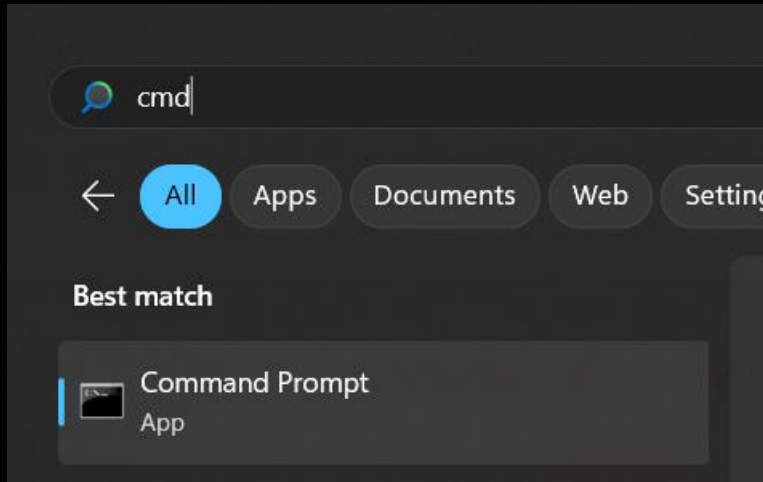
First, download and install Docker Desktop for Windows from the [Docker Hub](#).

Follow the installation instructions, and make sure to enable the WSL 2 feature and the Hyper-V when prompted, as they are required for Docker to run smoothly on Windows.



2: Download the bWAPP Docker Image:

Open your command prompt or PowerShell.



Pull the bWAPP Docker image by running the command:

```
docker pull raesene/bwapp
```

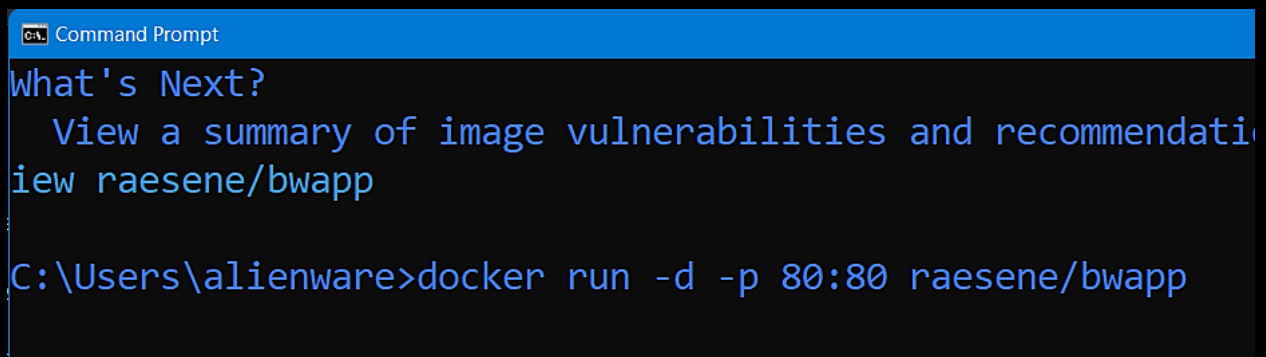
```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alienware>docker pull raesene/bwapp
Using default tag: latest
latest: Pulling from raesene/bwapp
8387d9ff0016: Pulling fs layer
3b52deaaf0ed: Pulling fs layer
4bd501fad6de: Pulling fs layer
```

3: Run the bWAPP Container:

Once the image is downloaded, you can run bWAPP in a Docker container. Use the following command to start the container:

```
docker run -d -p 80:80 raesene/bwapp
```

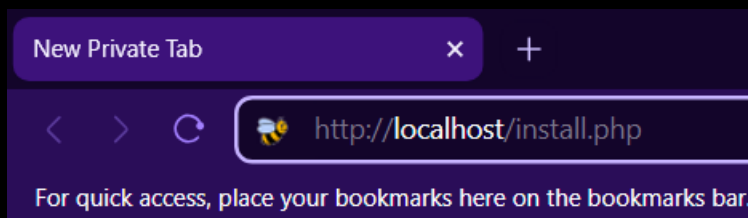


```
Command Prompt
What's Next?
  View a summary of image vulnerabilities and recommendations
  View raesene/bwapp
C:\Users\alienware>docker run -d -p 80:80 raesene/bwapp
```

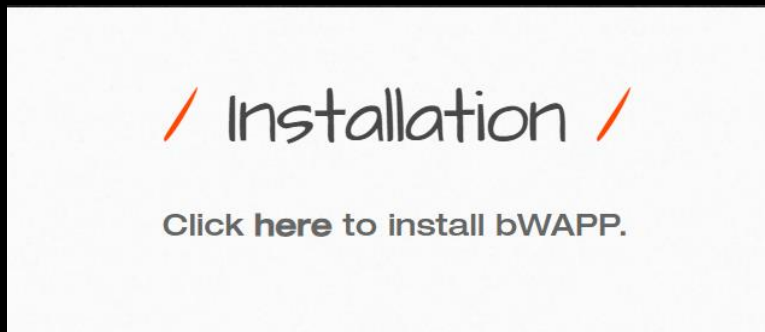
This command runs the container in detached mode (-d), maps port 80 of your local machine to port 80 of the container (-p 80:80), allowing you to access the bWAPP application by navigating to <http://localhost/> in your web browser.

4: Access bWAPP:

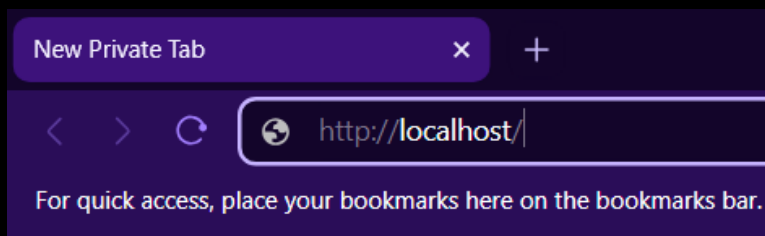
Open a web browser and go to <http://localhost/install.php>



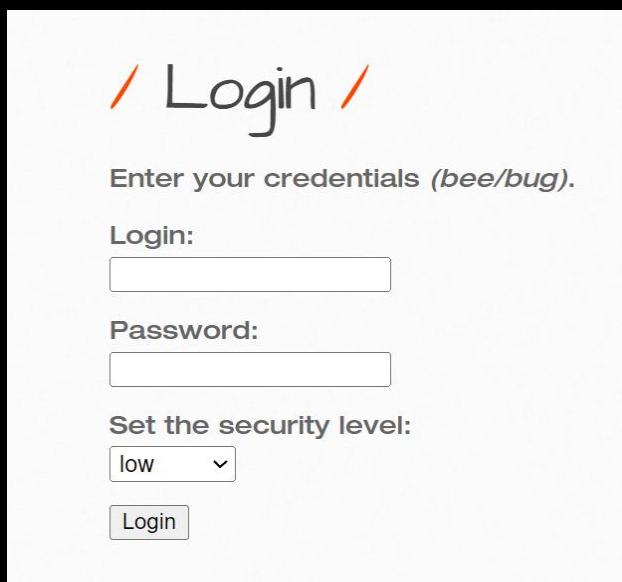
Click on the 'here' link on the page to set up the database automatically.



After the database setup, navigate to <http://localhost/>

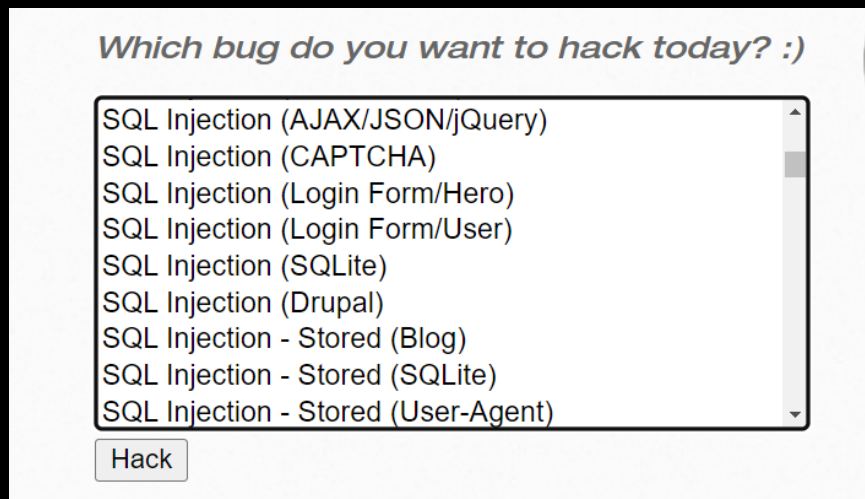


You can now log in with the default credentials
(username: bee, password: bug)

A screenshot of a web page titled "Login" in a large, handwritten-style font, flanked by two orange diagonal slashes. Below the title, the text "Enter your credentials (bee/bug)." is displayed. There are two input fields: one for "Login:" and one for "Password:". Below these fields is a label "Set the security level:" followed by a dropdown menu currently showing "low". At the bottom is a "Login" button.

Explore and Test:

Once you're logged into bWAPP, you have the opportunity to test various security vulnerabilities we've discussed in the video or watch tutorials and walkthroughs available on YouTube. This hands-on experience is invaluable for understanding and mitigating web application vulnerabilities.



To stop the Docker container running bWAPP:


Open your command prompt.

Use the following command: `docker ps`

```
C:\Users\alienware>docker ps
```

Find out the container ID of the running bWAPP container.

CONTAINER ID	IMAGE
0164ac6a	raesene/bwapp



Use the following command to stop the running container:

```
docker stop [container_id]
```

Watch The Video:

