Web Security

The main goal for these exercises is to make you aware of the top web security flaws as well as how to fix them.

We will be using an application called "WebGoat" made by OWASP as our training ground.

Installation with Docker: ***(NB only works for 64-bit systems)***

URL: https://github.com/WebGoat/WebGoat

1) Start you Ubuntu (or Kali) virtual machine.
2) Install docker with the command: *sudo apt update && sudo apt install docker.io*
3) Install the "WebGoat" docker image with the command: *docker pull webgoat/webgoat-8.0*
4) Start the service with the command: *docker run -p 8080:8080 webgoat/webgoat-8.0*
5) Open you browser and navigate to the URL: *http://localhost:8080/WebGoat*
6) Create an account and you are good to go! – Solve as many of the exercises as you can.

Running WebGoat from a jar: ***(This will work on both 32 and 64-bit systems)***

1) Navigate to a folder in your system, where you wish to download the jar file (The download folder would be a good choice)
2) Type in the command: *wget https://github.com/WebGoat/WebGoat/releases/download/7.1/webgoat-container-7.1-exec.jar*
3) Start WebGoat with the command: *java –jar webgoat-container-7.1-exec.jar*
4) Open you browser and navigate to the URL: *http://localhost:8080/WebGoat*

(In case the application does not start – make sure the machine has java installed and try again.)

Fix the Issue

In our Git repository, you will find a Web application called "SQLi", written in C#.

Unpack this solution and start it in Visual Studio. The application is a simple application, which is vulnerable to SQL Injections.

1) Try out your SQLi skills at this application.
2) Fix the code, so it is not vulnerable to SQLi anymore.