# **XSS Detection Application**

This application is designed to detect Cross-Site Scripting (XSS) attacks using machine learning algorithms. The system is capable of identifying XSS vulnerabilities in given input data, such as URLs and other text content.

## **Prerequisites**

* Python 3.7 or higher
* pip (Python package installer)

## **Installation**

1 Download on your local machine the folder named: “XSS\_Detection\_APP”

2. Create a virtual environment (optional but recommended):

python -m venv venv

source venv/bin/activate # On Windows use `venv\Scripts\activate`

3. Install the required packages

pip install -r requirements.txt

## **Usage**

1. Prepare your data:  
   Ensure your input data is properly formatted and ready for analysis. The data should be in a format suitable for the model, such as a list of URLs or text content.
2. Run the main script:

python3 ml\_xss.py

This script will:

* + Load the pre-trained models.
  + Vectorize the input data.
  + Predict whether the input data contains XSS vulnerabilities.
  + Display the results in the console.

## **Example Output**

After running the script, you will see output similar to the following in the console:

