# Low-Level Design Document

Low-Level Design Document: Phishing Website Detection System

1. Feature Extraction:

- Extracted 20 features from input URL including URL length, presence of '@' symbol, number of subdomains, presence of HTTPS, etc.

2. Feature Scaling:

- Applied custom min-max normalization to keep dependency light and compatible with deployment.

3. Model:

- Random Forest Classifier trained on preprocessed and normalized features. Tuned hyperparameters for optimal accuracy.

4. Backend (Flask):

- Flask app receives input URL, processes it, predicts the result using the ML model, and returns the classification (Phishing or Legitimate).

5. Hosting:

- The complete app was hosted using Render for public access.