

Phishing Attack Domain Detection

10 Jan, 2022

Overview

This project focuses on solving the most common cyber attack called phishing. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.

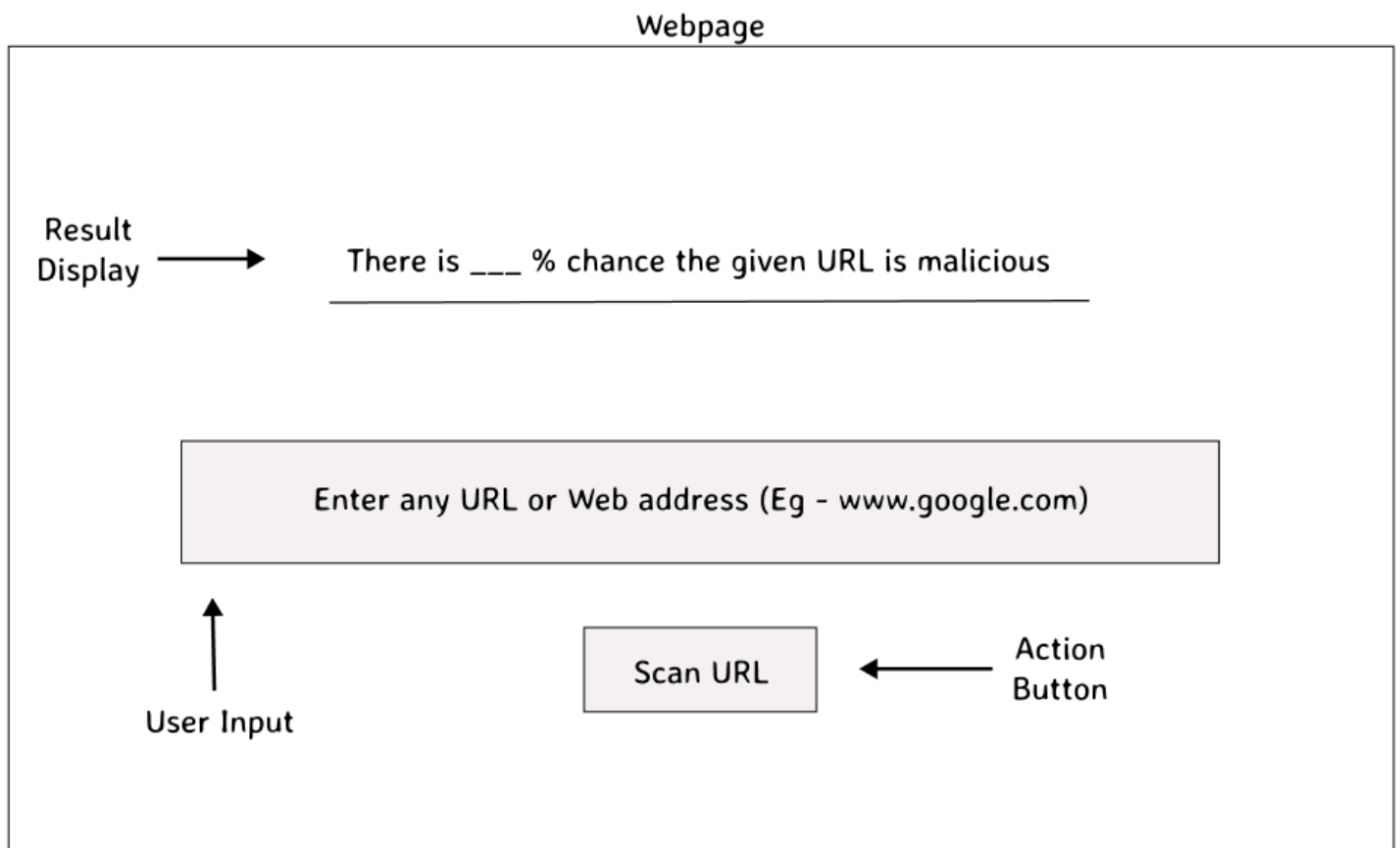
This document describes the wireframe for the schematic design of the web interface created for the ML model. We'll also discuss how the Web Interface will be connected to the ML model.

Made by Deepesh Mhatre

1.Web Interface Wireframe

A wireframe is a two-dimensional illustration of a page's interface that specifically focuses on space allocation and prioritization of content, functionalities available, and intended behaviors.

The interface we have created consists of only a single page through which the user interacts with the Machine learning model,below is the wireframe for our phishing attack domain project :



2.Component Functions

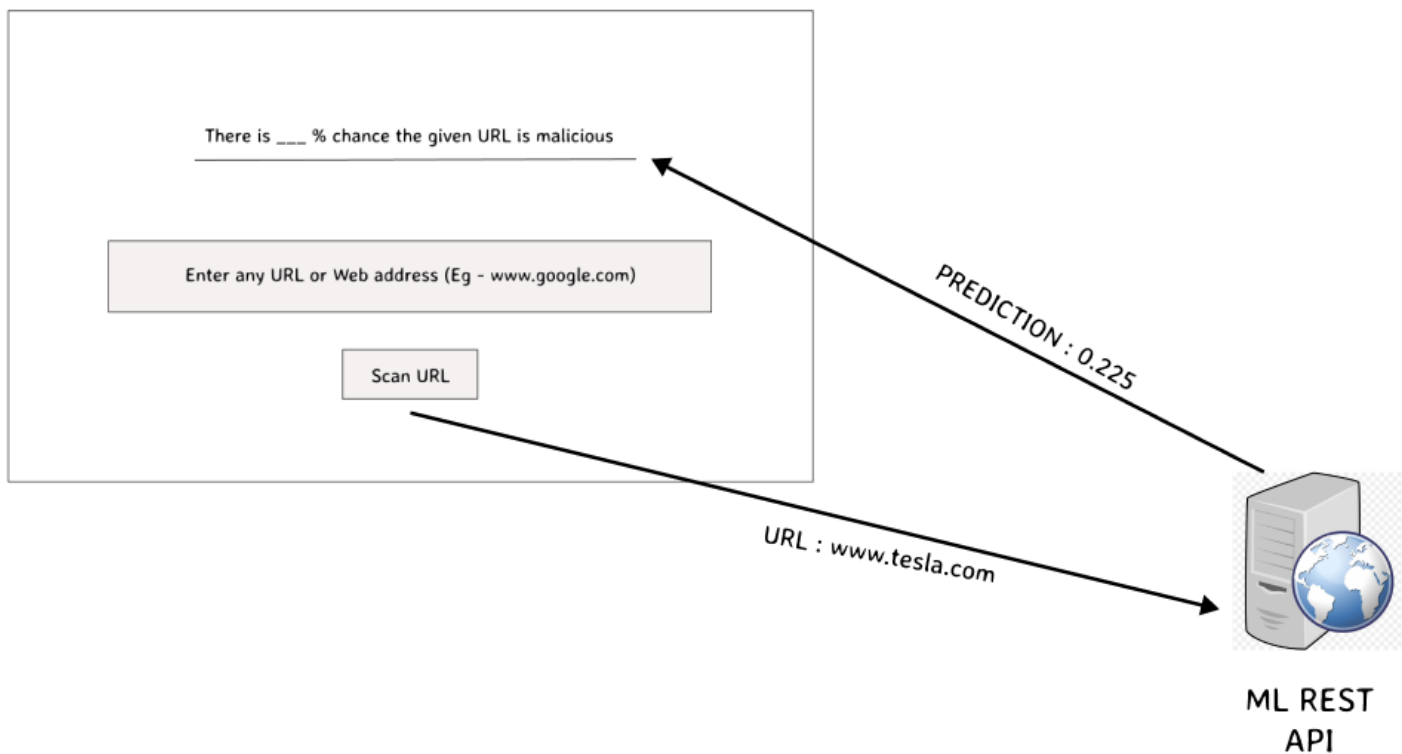
Below are the roles that each component in the wireframe performs :

1. **User-Input** : Takes the user input (in our case a URL) from the user and prepares for transmission to ML API
2. **Action-Button** : When clicked, it sends the user input to the Rest API as a POST request.
3. **Result-Display** : This component is responsible for displaying the result received from the POST request to the ML model.

Made by Deepesh Mhatre

3.User Interaction

Previously we saw what function each component inside the wireframe performs, now we'll see how these components work together to facilitate communication between user and the model.



The sequence in which the communication happens :

1. User enters the URL inside the input box
2. User clicks the action button and sends a POST request to API
3. The display receives the output from the API and updates the result