

# Wireframe

## PHISHING DOMAIN DETECTION

Document Version: 0.1

Last Revised Date: 15-May-2023

Parvej alam Ansari

Document Version Control:

Version	Date	Author	Description
0.1	15-05-2023	Parvej alam	Abstarct, UserInterface
0.1	15-05-2023	Parvej alam	User Input, Result Page

Contents

1    **Abstract**-----3

2    **Web Interface**-----4

3    **User Input**-----4

4    **Result Page**-----4

## 1. Abstract

Phishing stands for a fraudulent process, where an attacker tries to obtain sensitive information from the victim. Usually, these kinds of attacks are done via emails, text messages, or websites. Phishing websites, which are nowadays in a considerable rise, have the same look as legitimate sites. However, their backend is designed to collect sensitive information that is inputted by the victim. Discovering and detecting phishing websites has recently also gained the machine learning community's attention, which has built the models and performed classifications of phishing websites. This model uses full variation that consist of 88,647 websites labeled as legitimate or phishing and allow the researchers to train their classification models, build phishing detection systems, and mining association rules. Now, for that purpose classification type supervised machine learning model will be created. This model will takes 111 inputs and produces output in terms of whether the Website URL is phishing or genuine.

## 2. Web Interface

The web interface or web-page is single interface where input from the user side and the predicted output is displayed.



The wireframe shows a dark-themed web interface. At the top, there are two icons of a person wearing a hat and sunglasses, flanking the title **PHISHING DOMAIN DETECTION** in large, bold, orange letters. Below the title, a green text prompt reads: **Let's Check Whether URL is a Legitimate Website or a Phishing Website!**. Underneath this, a blue instruction line says: **Enter Suspicious URL Below**, with a small blue arrow pointing up on each side. Below the instruction is a long, empty, dark gray rectangular input field. At the bottom left of the input field, there is a green button with the word **Check** in white text.

## 3. User-Input

Whenever the user hits provided url, the user input page appears where the user is required to provide the information like:

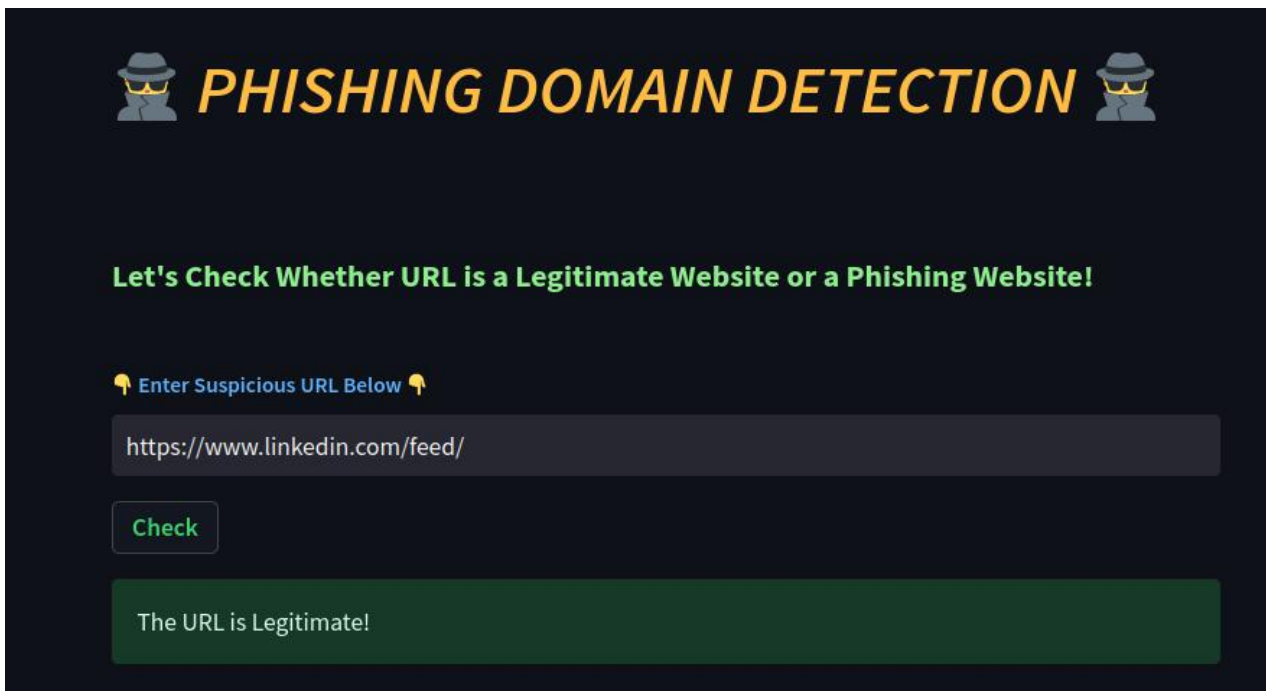
- Text-Box where the person can enter suspicious website link to check whether it is legitimate or phishing.

## 4. Result Page

After the user hits the submit/check button the page gets refreshed and the results are being displayed in the highlighted area in the above frame.

The user can refill the input URL in same page and can get the result in the sameway.

## ◆ Example of Legitimate Website Link:



The screenshot shows the 'PHISHING DOMAIN DETECTION' interface. At the top, the title is flanked by two hacker icons. Below the title, a green instruction reads: 'Let's Check Whether URL is a Legitimate Website or a Phishing Website!'. A prompt 'Enter Suspicious URL Below' is followed by a text input field containing the URL 'https://www.linkedin.com/feed/'. A green 'Check' button is positioned below the input field. At the bottom, a dark green message box states: 'The URL is Legitimate!'.

## ◆ Example of Phishing Website Link:



The screenshot shows the same 'PHISHING DOMAIN DETECTION' interface. The title and instructions are identical. The text input field now contains the URL 'https://antai-services-public.com/app/pages/index.php'. The 'Check' button is highlighted with a red border. At the bottom, a dark red message box states: 'The URL is a Phishing Attempt!'.