Flask integration with ML Model

Reading Saved ML Model

```
app = Flask(__name__)
model = pickle.load(open('model.pkl','rb'))
```

Integrating Flask

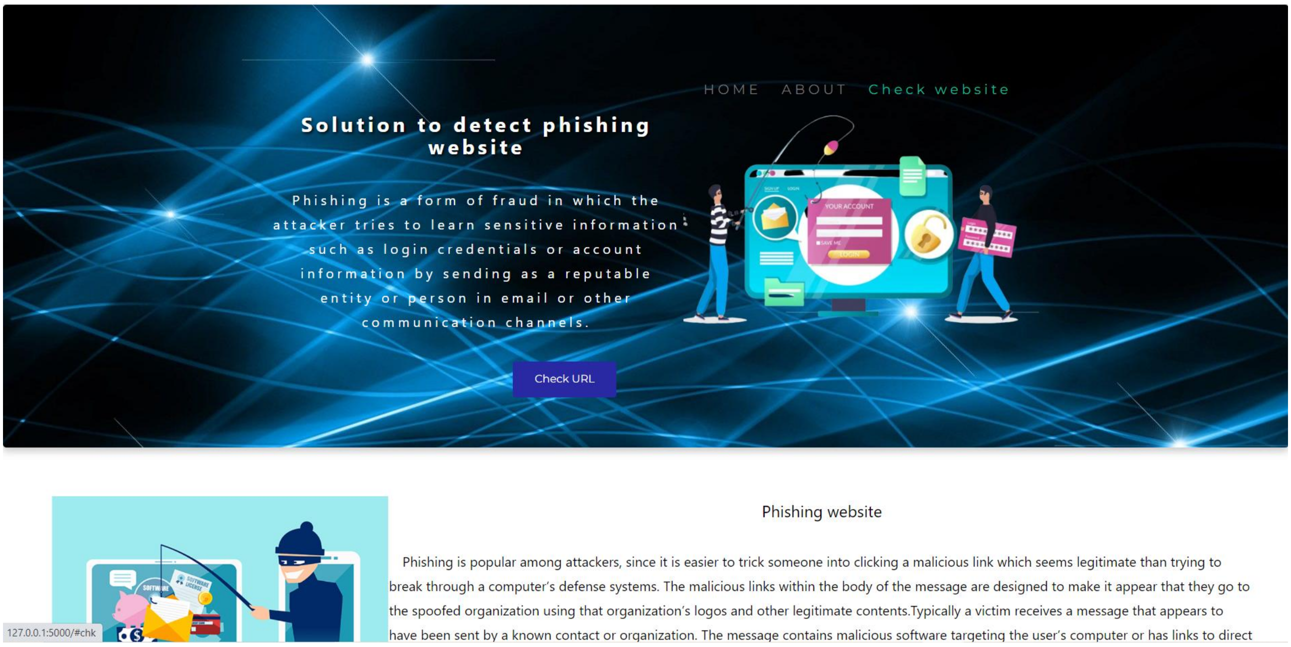
```
@app.route('/')
def home():
    return render_template('phishing.html')

@app.route('/predict',methods=['POST'])
def predict():
    return render_template('home.html')

@app.route('/result',methods=['POST'])
def result():
    #For rendering results on HTML GUI
    int_features = request.form['url']
    print(int_features)
    checkprediction = inputScript.main(int_features)
    prediction = classifier.predict(checkprediction)
    print(prediction)
    res=""
    if(prediction==1):
        res=int_features+" is not safe to enter"
    elif(prediction==-1):
        res=int_features+" is safe to enter"
    return render_template('home.html', prediction_text= res)
if __name__ == '__main__':
    app.run()
```

Website Result:

Home page



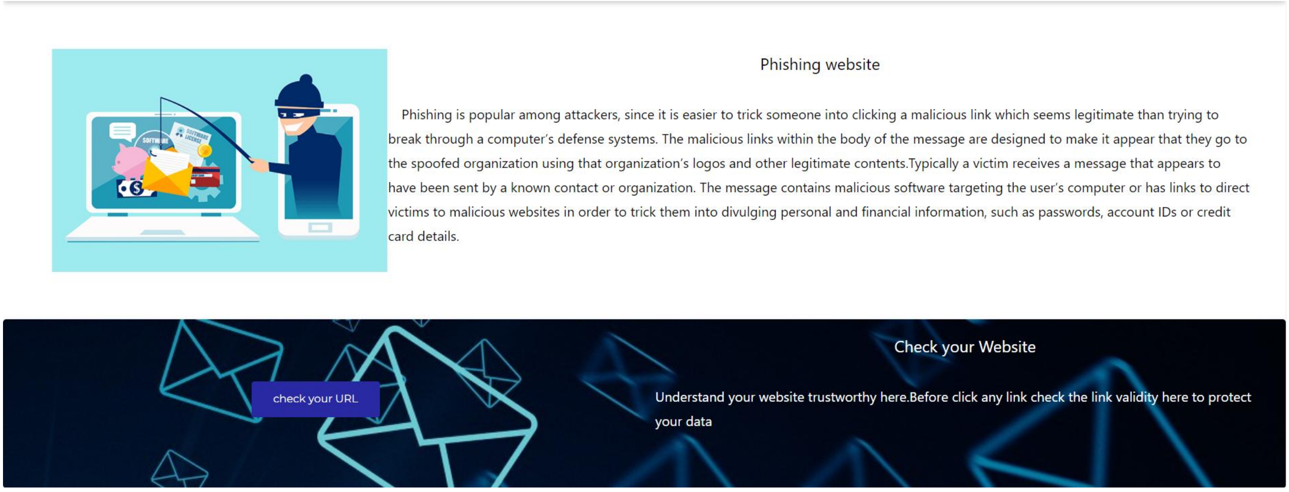
Solution to detect phishing website

Phishing is a form of fraud in which the attacker tries to learn sensitive information such as login credentials or account information by sending as a reputable entity or person in email or other communication channels.

Phishing website

Phishing is popular among attackers, since it is easier to trick someone into clicking a malicious link which seems legitimate than trying to break through a computer's defense systems. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization using that organization's logos and other legitimate contents.Typically a victim receives a message that appears to have been sent by a known contact or organization. The message contains malicious software targeting the user's computer or has links to direct

About and Check URL Section:



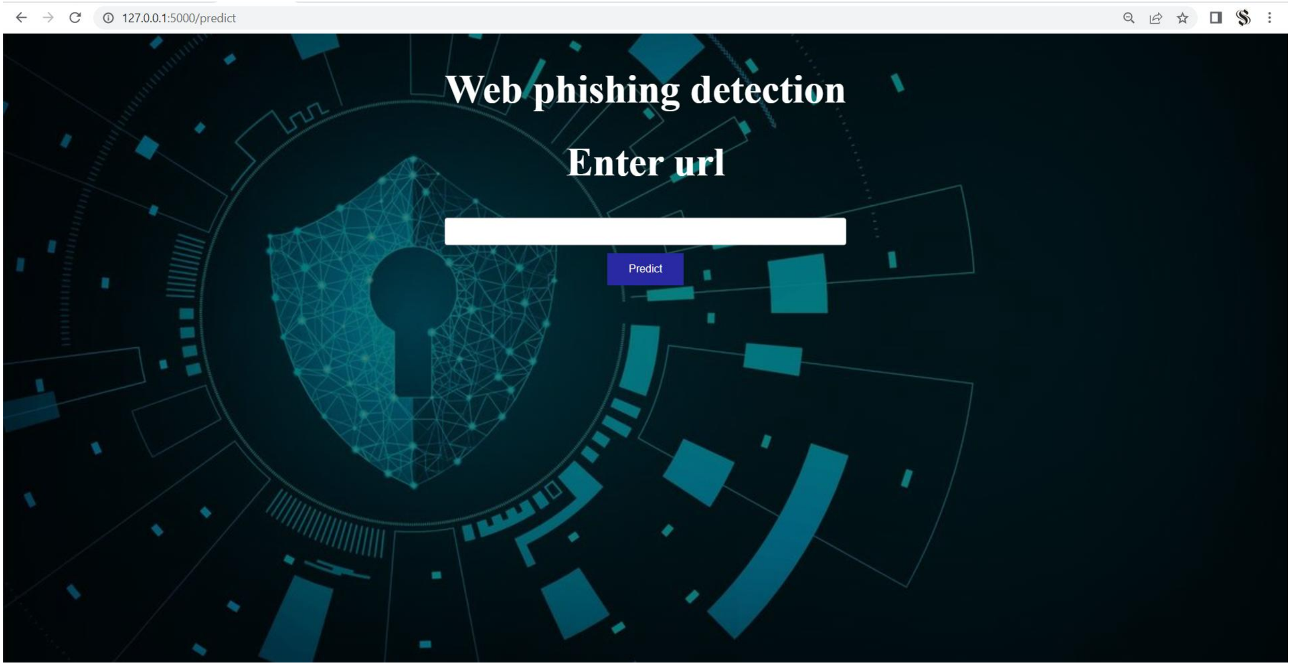
Phishing website

Phishing is popular among attackers, since it is easier to trick someone into clicking a malicious link which seems legitimate than trying to break through a computer's defense systems. The malicious links within the body of the message are designed to make it appear that they go to the spoofed organization using that organization's logos and other legitimate contents.Typically a victim receives a message that appears to have been sent by a known contact or organization. The message contains malicious software targeting the user's computer or has links to direct victims to malicious websites in order to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

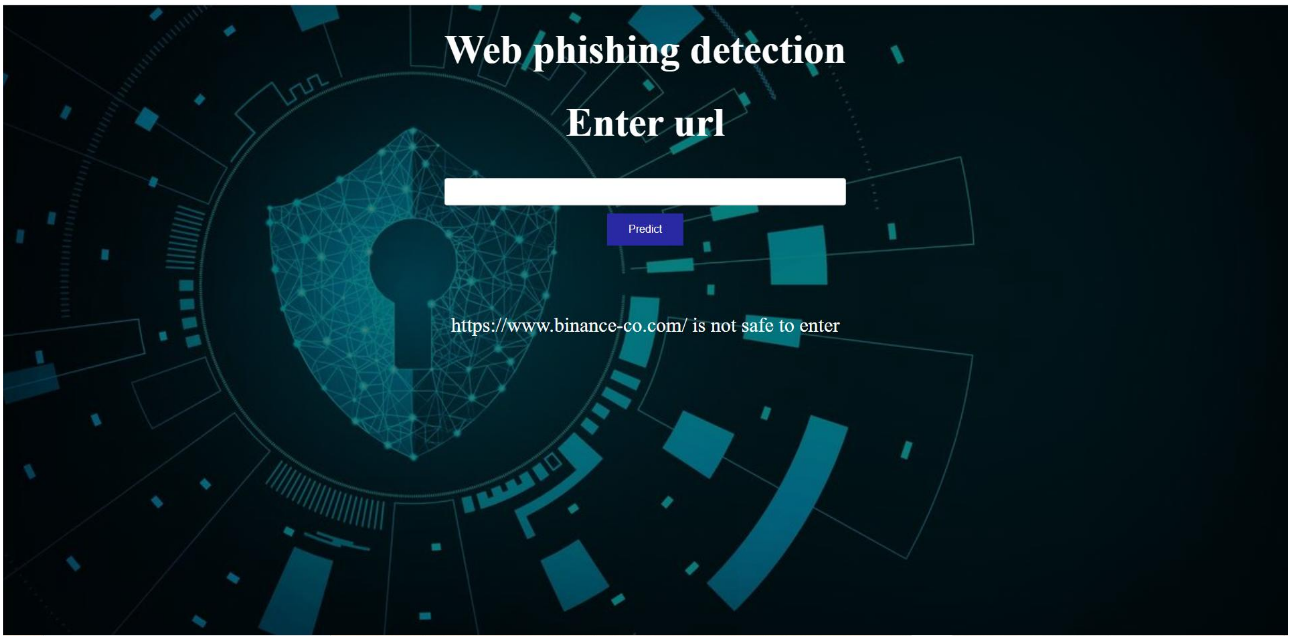
Check your Website

Understand your website trustworthy here.Before click any link check the link validity here to protect your data

Prediction Page

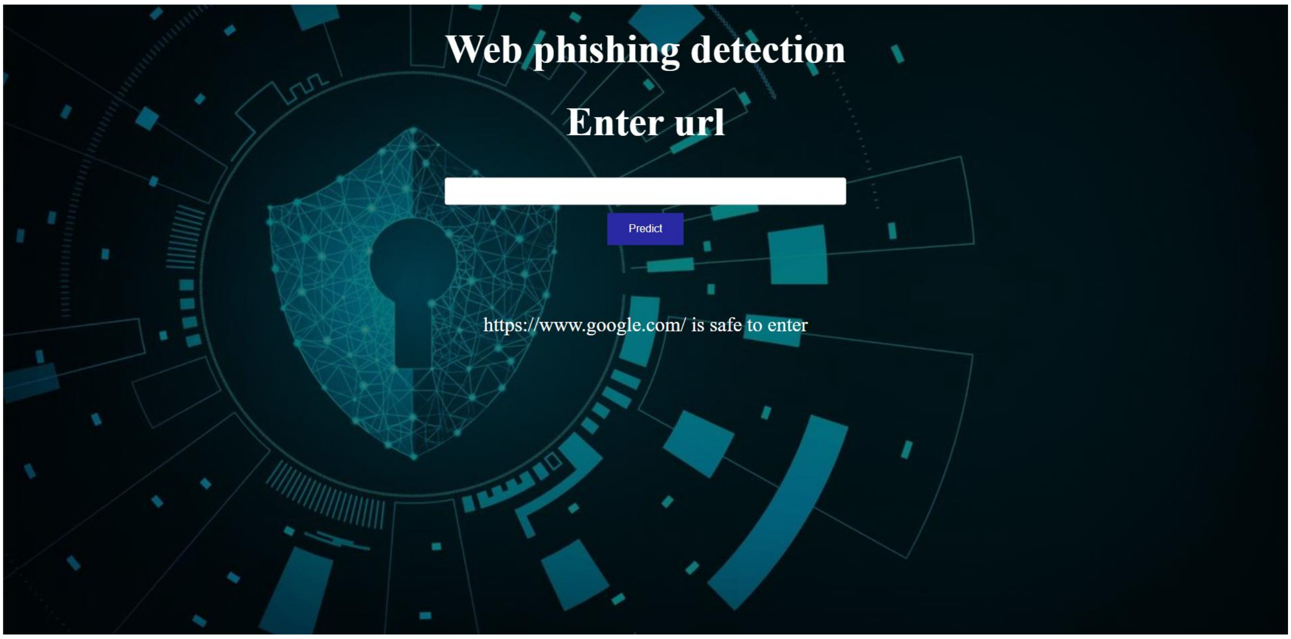


Output for Safe URL Prediction



https://www.binance-co.com/ is not safe to enter

Output for detection for phishing URL



Web phishing detection

Enter url

https://www.google.com/ is safe to enter