##### Malicious URL Detector

##### (Using API)

**A PROJECT REPORT**

###### ***Submitted by***

**Yogendra Bijapur (20BCY10065)**

**R.P. Niranjan Surya Prasad (20BCY10129)**

**Parth Agrawal (20BCY10039)**

**Dipika Sangwan (20BCY10010)**

*in partial fulfillment for the award of the degree*

*of*

**BACHELOR OF TECHNOLOGY**

*in*

**CYBER SECURITY AND DIGITAL FORENSICS**

****

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRI KALAN, SEHORE**

**MADHYA PRADESH - 466114**

April 2022

**VIT BHOPAL UNIVERSITY, KOTHRI KALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“Malicious URL Detector (Using API)”** is the bonafide work of “**YOGENDRA BIJAPUR (20BCY10065), R.P. NIRANJAN SURYA PRASAD (20BCY10129), Parth Agrawal (20BCY10039),**

**Dipika Sangwan (20BCY10010)**” who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.



**PROGRAM CHAIR PROJECT GUIDE**

Dr. R. Rakesh, Assistant Professor Mr. Vikas Kumar Jain

School of Computer Science and Engineering School of Computer Science and Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

The Project Exhibition I Examination is held on 26-04-2022

**ACKNOWLEDGEMENT**

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. Shishir Kumar Shandilya, Head of the Department, School of Computer Science and Engineering for much of his valuable support and encouragement in carrying out this work.

I would like to thank my internal guide Mr. Vikas Kumar Jain for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Computer Science and Engineering, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**LIST OF ABBREVIATIONS**

|  |  |
| --- | --- |
| **ABBREVIATIONS** | **FULL FORM** |
| **IP** | **Internet Protocol** |
| **PHP** | **Hypertext Preprocessor** |
| **HTTP** | **HyperText Transfer Protocol** |
| **URL** | **Uniform Resource Locator** |
| **HTTPS** | **Hypertext Transfer Protocol Secure** |
| **WWW** | **World Wide Web** |
| **HTML** | **Hyper-Text Markup Language** |
| **.com** | **Dot Commercial** |
| **App** | **Application** |
| **API** | **Application Programming Interface** |

**LIST OF FIGURES AND GRAPHS**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| **1.** | **Methodology** | **7** |
| **2.** | **Prototype** | **13** |
| **3.** | **Performance Analysis (Graph)** | **14** |

**ABSTRACT**

One of the challenges faced by our research was the unavailability of reliable training datasets. In fact, this challenge faces any researcher in the field. However, although plenty of articles about predicting phishing websites using data mining techniques have been disseminated these days, no reliable training dataset has been published publicly, maybe because there is no agreement in the literature on the definitive features that characterize phishing websites, hence it is difficult to shape a dataset that covers all possible features.

In this report, we shed light on the important features that have proved to be sound and effective in predicting phishing websites. In addition, we proposed some new features, experimentally assign new rules to some well-known features, and update some other features using some research papers as a reference

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
|  | List of Abbreviations  List of Figures and Graphs  List of Tables  Abstract | iii  iv  v  vi |
| 1 | **CHAPTER-1:**  **PROJECT DESCRIPTION AND OUTLINE**  Introduction 1.2 Motivation for the Work  1.3 About Introduction to the Project  Including Techniques  1.4 Problem Statement  1.5 Objective of the work  1.6 Organization of the project  1.7 Summary | 1  1  1  1-2  2  2  2  3 |
| 2 | **CHAPTER-2:**  **RELATED WORK INVESTIGATION**  2.1 Introduction  2.2 Core Area of the project  2.3 Existing Approaches/Methods  2.4 Pros and Cons of the Stated Approaches/Methods  2.5 Issues/Observations from Investigation  2.6 Summary | 4  4  4  4  4-5  5  5 |
| 3 | **CHAPTER-3:**  **REQUIREMENT ARTIFACTS**  3.1 Introduction  3.2 Hardware and Software Requirements  3.3 Specific Project Requirements  3.3.1 Data Requirement  3.3.2 Functions Requirement  3.4 Summary | 6  6  6  6  6 |
| 4 | **CHAPTER-4:**  **DESIGN METHODOLOGY AND ITS NOVELTY**  4.1 Methodology and Goal  4.2 Functional Modules Design and Analysis  4.3 Website Architectural Designs  4.4 Subsystem Services  4.5 API Fetching  4.6 Summary | 7  7  7  7-10  11  11-12  12 |
| 5 | **CHAPTER-5:**  **TECHNICAL IMPLEMENTATION & ANALYSIS**  5.1Outline  5.2 Technical Coding and Code Solutions  5.3 Working Layout of Forms  5.4 Prototype Submission  5.5 Test and Validation  5.6 Performance Analysis (Graphs/Charts)  5.7 Summary | 13  13  13  13  13  14  14  15 |
| 6 | **CHAPTER-6:**  **PROJECT OUTCOME AND APPLICABILITY**  6.1Outline  6.2 Key Implementations Outline of the System  6.3 Significant Project Outcomes  6.4 Project Applicability on Real-World Applications  6.4 Inference | 16  16  16  16  16  16 |
| 7 | **CHAPTER-7:**  **CONCLUSIONS AND RECOMMENDATION**  7.1Outline  7.2 Limitation/Constraints of the System  7.3 Future Enhancements  7.4 Inference | 17  17  17  17  17 |
|  | RELATED WORK INVESTIGATION    References | 18  19 |

**CHAPTER-1**

**PROJECT DESCRIPTION AND OUTLINE**

# 1.1 Introduction:

# Phishing is a very common social engineering attack that is done for the main purpose of stealing important information from the victim. People are tricked by sending malicious links that steal their personal information. Phishing traditionally functions by sending forged e-mail, mimicking an online bank, auction, or payment sites, guiding users to a bogus web page that is carefully designed to look like the login to the genuine site. The project is completely based upon the address bar features for the detection of Phishing links.

1.2 Motivation for the work:

With the increasing reach of the internet, phishing URLs are also on the rise. Many websites are available that detect phishing links but we want to make a website, as most of the internet surfing takes place through smartphones. So, building a Website for this is the main motivation for the work.

1.3 Introduction to the project including techniques:

We have created a website that helps the user to get to know about the URL. On the website, the user can also get to know about the risk score and all other details

The methodology which we are using here in the implementation of this is API scanner which sends the result or found data in a JSON format.

1.4 Problem Statement:

Phishing is one of the most dangerous threats to our important data. According to a recent survey by ESET Israel, 83% of participants said that they had been targeted by phishing messages at least once. Over 57% also said that they had clicked on promotional links without first checking for red flags.

Many such surveys show the severity of the phishing attack. So, it is important to be aware and should have detection for such links.

1.5 Objective of the work:

Our goal in this project is to create a phishing URL-detecting Website that can detect whether the website accessed by a user is a phishing website or not using its URL. Our application is user-friendly and can be used by the user to be protected from ransomware, spam, and other fraudulent activities.

1.6 Organization of the project:

Our Project is organized by our team according to some split-ups of information and data. We gathered information about phishing websites and some ways to identify phishing websites through some research papers. By using the methods to identify the phishing websites we created an android app using android studio and java.

1.7 Summary:

Phishing is a social engineering attack that is used to steal personal information. Of all types of attacks like denial of service, ransomware, malware, etc phishing always stands ahead of all. Also, cybersecurity breaches that occurred in the organization in recent past years are done through phishing which accounts for more than 53% of all. Most phishing attacks are caused due to malicious links which are mainly spammed through emails. So, it is necessary to have a preventive measure against such links by which we can help ourselves to keep our valuable information safe.

**CHAPTER-2**

**RELATED WORK INVESTIGATION**

2.1 Introduction:

In this chapter, we will see about the work-related investigation we have done to develop our project. This chapter will clearly explain the core area of our project, the methods used in our project, and the pros and cons of our project.

2.2 Core area of the project:

The core area of our project is based on phishing websites detected in cybersecurity. cybersecurity or information technology security is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. Malicious Websites are created to dupe unsuspecting users into thinking they are on a legitimate site. The criminals will spend a lot of time making the site seem as credible as possible and many sites will appear almost indistinguishable from the real thing. We are trying to prevent this cybercrime phishing using our project Malicious URL Detection using Application Program Interface.

2.3 Existing Methods:

At first, we researched the methods to identify a phishing website using its URL. Then we have got some data to identify a phishing website through address bar features then we implemented it into a code that has an incrementation method. If the URL seems to be a URL of a phishing website, it gives a higher number thus the code considers the website may be phishing. Then we implemented the code to the Android studio and created an android app with a better user interface.

2.4 Pros and cons of the stated Approaches/Methods:

Pros: - There is no android application on the feature that works without the internet. Most phishing detecting websites work online for detection but this app works offline.

Cons: - The application cannot work over other applications, we always have to paste the links there for checking. Also, it only checks for address bar features, there may be a possibility that links don’t have address bar issues but maybe phishing on account of other features like domain-based and JavaScript issues.

2.5 Observations from investigation:

We have observed various online Malicious URL Detections and many research papers on how we can detect a Malicious URL in which the simple method we found to detect a Malicious website is to use their URL's so we implemented it in our project.

2.6 Summary:

In this chapter, we have seen that the core area of our project is cyber-crime Malicious Websites. Then the methods existing in our project explain the pros and cons of the project which has some cons. Then finally this chapter discusses the observations we had to develop this project.

**CHAPTER-3**

**REQUIREMENT ARTIFACTS**

3.1 Introduction:

We have previously discussed the main idea of the project. Here we will be discussing the requirements in the successful completion of this project and what all the data and knowledge we need to put into this project.

3.2 Hardware and Software requirements:

For this project we require a laptop/pc with some average config to work in and we will be needing an IDE to code and any online platform to design the front end of our project. But we used nicepage.com to design our website. we also need a hosting provider to host our website.

3.3 Specific Project requirements:

Some specific requirements needed for this project are basic understanding of JAVA and JavaScript for the code implementation and designing the front end of the website java coding, and project algorithm developing skills.

3.3.1 Data requirement:

We require a key set for checking our urls in the API. And we will also be needing the codes for connecting the URL Reputation API in the backend of our website. We need some set of codes for the working of API.

3.4 Summary:

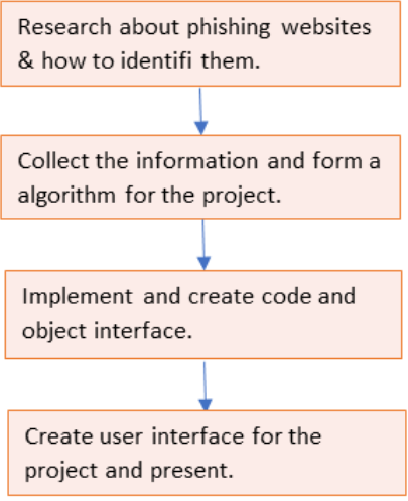
We can summarize as the requirements for the implementations of the code are Java, Javascript, IDE and a web page designing platform . And the most important thing is the codes for connecting the URL Reputation API and the key sets.

**CHAPTER-4**

**DESIGN METHODOLOGY AND ITS NOVELTY**

4.1 Methodology and goal:

Methodology:



Goal:

Our main goal is to create a threat-free friendly cyber network using our project as our first step.

4.2 Functional modules design and analysis:

The main functional module used in our project is the Application Programming Interface(API). It plays an important role in our project to detect the given URL is a Malicious URL or not using50+ security checks like phishing\_heuristics.

4.3 Website Architectural designs:

For the development of the Website.

<!DOCTYPE html>

<html style="font-size: 16px;">

<head>

<meta name="viewport" content="width=device-width, initial-scale=1.0">

<meta charset="utf-8">

<meta name="keywords" content="​Library Education, ​Meet our Principal, ​Helping each child find and follow their best learning path.">

<meta name="description" content="">

<meta name="page\_type" content="np-template-header-footer-from-plugin">

<title>Home</title>

<link rel="stylesheet" href="nicepage.css" media="screen">

<link rel="stylesheet" href="Home.css" media="screen">

<script class="u-script" type="text/javascript" src="jquery-1.9.1.min.js" defer=""></script>

<script class="u-script" type="text/javascript" src="nicepage.js" defer=""></script>

<meta name="generator" content="Nicepage 4.8.2, nicepage.com">

<link id="u-theme-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:100,100i,200,200i,300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i|Open+Sans:300,300i,400,400i,500,500i,600,600i,700,700i,800,800i">

<link id="u-page-google-font" rel="stylesheet" href="https://fonts.googleapis.com/css?family=Raleway:100,100i,200,200i,300,300i,400,400i,500,500i,600,600i,700,700i,800,800i,900,900i|Lobster:400">

<link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3" crossorigin="anonymous">

<style>

.risk\_score{

font-size: xx-large

}

.style{

font-style: italic;

}

</style>

<script type="application/ld+json">{

"@context": "http://schema.org",

"@type": "Organization",

"name": "",

"url": "/",

"sameAs": []

}</script>

<meta name="theme-color" content="#2799b1">

<meta property="og:title" content="Home">

<meta property="og:type" content="website">

<link rel="canonical" href="/">

</head>

<body class="u-body u-xl-mode"><header class="u-clearfix u-header u-header" id="sec-9c34"><div class="u-clearfix u-sheet u-sheet-1">

<nav class="u-menu u-menu-dropdown u-offcanvas u-menu-1" data-responsive-from="XL">

<div class="menu-collapse" style="font-size: 1rem; letter-spacing: 0px; font-weight: 500;">

<a class="u-button-style u-custom-active-color u-custom-border u-custom-border-color u-custom-hover-color u-custom-left-right-menu-spacing u-custom-padding-bottom u-custom-text-active-color u-custom-text-color u-custom-text-hover-color u-custom-top-bottom-menu-spacing u-nav-link u-text-active-palette-1-base u-text-hover-palette-2-base" href="#">

<svg class="u-svg-link" viewBox="0 0 24 24"><use xlink:href="#menu-hamburger"></use></svg>

<svg class="u-svg-content" version="1.1" id="menu-hamburger" viewBox="0 0 16 16" x="0px" y="0px" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns="http://www.w3.org/2000/svg"><g><rect y="1" width="16" height="2"></rect><rect y="7" width="16" height="2"></rect><rect y="13" width="16" height="2"></rect>

</g></svg>

</a>

</div>

<div class="u-nav-container">

<ul class="u-nav u-spacing-2 u-unstyled u-nav-1"><li class="u-nav-item"><a class="u-active-grey-5 u-button-style u-hover-grey-10 u-nav-link u-text-active-grey-90 u-text-grey-90 u-text-hover-grey-90" href="Home.html" style="padding: 10px 20px;">Home</a>

</li><li class="u-nav-item"><a class="u-active-grey-5 u-button-style u-hover-grey-10 u-nav-link u-text-active-grey-90 u-text-grey-90 u-text-hover-grey-90" href="About.html" style="padding: 10px 20px;">About</a>

</li><li class="u-nav-item"><a class="u-active-grey-5 u-button-style u-hover-grey-10 u-nav-link u-text-active-grey-90 u-text-grey-90 u-text-hover-grey-90" href="Contact.html" style="padding: 10px 20px;">Contact</a>

</li></ul>

</div>

<div class="u-nav-container-collapse">

<div class="u-black u-container-style u-inner-container-layout u-opacity u-opacity-95 u-sidenav">

<div class="u-inner-container-layout u-sidenav-overflow">

<div class="u-menu-close"></div>

<ul class="u-align-center u-nav u-popupmenu-items u-unstyled u-nav-2"><li class="u-nav-item"><a class="u-button-style u-nav-link" href="Home.html" style="padding: 10px 20px;">Home</a>

</li><li class="u-nav-item"><a class="u-button-style u-nav-link" href="About.html" style="padding: 10px 20px;">About</a>

</li><li class="u-nav-item"><a class="u-button-style u-nav-link" href="Contact.html" style="padding: 10px 20px;">Contact</a>

</li></ul>

</div>

</div>

<div class="u-black u-menu-overlay u-opacity u-opacity-70"></div>

</div>

</nav>

</div></header>

<section class="u-align-center u-clearfix u-image u-valign-middle-md u-valign-middle-sm u-valign-middle-xs u-section-1" id="carousel\_c62e" data-image-width="1980" data-image-height="1114">

<div class="u-clearfix u-gutter-0 u-layout-wrap u-layout-wrap-1">

<div class="u-layout" style="">

<div class="u-layout-row" style="">

<div class="u-container-style u-layout-cell u-left-cell u-shape-rectangle u-size-60 u-size-xs-60 u-layout-cell-1" src="">

<div class="u-container-layout u-container-layout-1">

<h1 class="u-align-left u-text u-text-body-alt-color u-text-1" data-animation-name="fadeIn" data-animation-duration="1000" data-animation-direction="Left" data-animation-delay="250"> Malicious URL Detector</h1>

<div class="u-form u-form-1">

<form action="//publish.nicepage.com/Form/Process" method="POST" class="u-clearfix u-form-spacing-15 u-form-vertical u-inner-form" style="padding: 15px;" source="email" name="form">

<input type="hidden" id="siteId" name="siteId" value="1768619">

<input type="hidden" id="pageId" name="pageId" value="1768631">

<div class="u-form-email u-form-group u-label-none u-form-group-1">

<label for="email-6797" class="u-label">Email</label>

<input type="email" placeholder="Enter URL" id="email-6797" name="URL" class="u-border-1 u-border-grey-30 u-input u-input-rectangle u-radius-50 u-white u-input-1" required="">

</div>

<div class="u-align-center u-form-group u-form-submit u-form-group-2">

<a href="#" class="u-border-2 u-border-grey-75 u-btn u-btn-round u-btn-submit u-button-style u-palette-1-base u-radius-50 u-btn-1">Submit</a>

<input id="SubBtn" type="submit" value="submit" class="u-form-control-hidden">

</div>

<div class="u-form-send-message u-form-send-success">Thank you! Your message has been sent.</div>

<div class="u-form-send-error u-form-send-message">Unable to send your message. Please fix errors then try again.</div>

<input type="hidden" value="" name="recaptchaResponse">

</form>

</div>

<div id="urlcheck" class="m-4 p-4">

</div>

<a href="https://nicepage.com/html-templates" class="u-border-none u-btn u-btn-round u-button-style u-palette-3-base u-radius-10 u-text-palette-1-base u-btn-2" data-animation-name="fadeIn" data-animation-duration="1000" data-animation-direction="Up" data-animation-delay="500">learn more</a>

<img class="u-image u-image-round u-opacity u-opacity-25 u-radius-50 u-image-1" src="images/403.png" alt="" data-image-width="833" data-image-height="586">

<p class="u-align-justify u-text u-text-body-alt-color u-text-2" data-animation-name="fadeIn" data-animation-duration="1000" data-animation-direction="Up" data-animation-delay="250"> &nbsp; &nbsp; &nbsp;<span class="u-text-palette-3-base">Malicious URL Detector</span>&nbsp;scans links in real-time to detect suspicious URLs. Accurately identify phishing links, malware URLs and viruses, parked domains, and suspicious URLs with real-time risk scores.

</p>

</div>

</div>

</div>

</div>

</div>

</section>

<section class="u-align-center u-clearfix u-valign-middle u-white u-section-2" id="carousel\_2f1f">

<div class="u-expanded-width u-gradient u-opacity u-opacity-55 u-shape u-shape-rectangle u-shape-1" data-animation-name="rollIn" data-animation-duration="1000" data-animation-direction=""></div>

<div class="u-clearfix u-gutter-40 u-layout-spacing-vertical u-layout-wrap u-layout-wrap-1">

<div class="u-gutter-0 u-layout">

<div class="u-layout-row">

<div class="u-size-31 u-size-60-md">

<div class="u-layout-col">

<div class="u-container-style u-hidden-md u-hidden-sm u-hidden-xs u-layout-cell u-right-cell u-size-20 u-layout-cell-1" wfd-invisible="true">

<div class="u-container-layout u-container-layout-1"></div>

</div>

<div class="u-align-center u-container-style u-layout-cell u-radius-20 u-right-cell u-shape-round u-size-40 u-white u-layout-cell-2" data-animation-name="fadeIn" data-animation-duration="1000" data-animation-direction="Left" data-animation-delay="250">

<div class="u-container-layout u-container-layout-2">

<img class="u-expanded-width u-image u-image-round u-radius-20 u-image-1" src="images/bn.jpg" alt="" data-image-width="800" data-image-height="800" data-animation-name="fadeIn" data-animation-duration="2000" data-animation-direction="Left" data-animation-delay="250">

<h5 class="u-text u-text-1" spellcheck="false">STEP-1</h5>

<p class="u-text u-text-2" spellcheck="false"> Enter your URL&nbsp;</p>

</div>

</div>

</div>

</div>

<div class="u-size-29 u-size-60-md">

<div class="u-layout-col">

<div class="u-align-center u-container-style u-layout-cell u-left-cell u-radius-20 u-size-40 u-layout-cell-3" data-animation-name="zoomIn" data-animation-duration="2000" data-animation-direction="">

<div class="u-container-layout u-valign-middle-md u-valign-middle-sm u-valign-middle-xs u-valign-top-lg u-valign-top-xl u-container-layout-3" src="">

<img class="u-image u-image-round u-radius-20 u-image-2" src="images/kj.jpg" data-image-width="1200" data-image-height="1002" data-animation-name="fadeIn" data-animation-duration="1000" data-animation-direction="Right" data-animation-delay="250">

</div>

</div>

<div class="u-align-center u-container-style u-layout-cell u-left-cell u-size-20 u-white u-layout-cell-4">

<div class="u-container-layout u-container-layout-4">

<h3 class="u-text u-text-default u-text-3" spellcheck="false">STEP-2</h3>

<p class="u-text u-text-4" spellcheck="false">

<span style="font-weight: 700; font-size: 1.25rem;"> You will get the RESULT whether your given URL is malicious or not &amp;<br>some information of that website.

</span>

<br>

</p>

</div>

</div>

</div>

</div>

</div>

</div>

</div>

</section>

<section class="u-clearfix u-section-3" id="carousel\_08cf">

<div class="u-clearfix u-sheet u-valign-middle u-sheet-1">

<div class="u-expanded-width-lg u-expanded-width-md u-expanded-width-sm u-expanded-width-xs u-gradient u-shape u-shape-rectangle u-shape-1"></div>

<img class="u-align-left u-image u-image-round u-radius-20 u-image-1" data-image-width="900" data-image-height="900" src="images/5178414.jpg">

<div class="u-container-style u-grey-5 u-group u-radius-20 u-shape-round u-group-1">

<div class="u-container-layout u-container-layout-1">

<h3 class="u-align-left u-text u-text-default u-text-1" spellcheck="false"> What is Malicious URl?</h3>

<p class="u-align-justify u-text u-text-2" spellcheck="false"> Malicious URL is&nbsp;<b>a link created with the purpose of promoting scams, attacks, and frauds</b>. By clicking on an infected URL, you can download ransomware, virus, trojan, or any other type of malware that will compromise your machine or even your network, in the case of a company.

</p>

</div>

</div>

<div class="u-gradient u-shape u-shape-circle u-shape-2"></div>

</div>

</section>

<section class="u-align-center u-clearfix u-grey-5 u-section-4" id="sec-686e">

<div class="u-clearfix u-sheet u-valign-middle u-sheet-1">

<h2 class="u-text u-text-default u-text-1"> Meet our Principal</h2>

<div class="u-list u-list-1">

<div class="u-repeater u-repeater-1">

<div class="u-container-style u-custom-item u-gradient u-list-item u-radius-20 u-repeater-item u-shape-round u-list-item-1">

<div class="u-container-layout u-similar-container u-container-layout-1">

<h4 class="u-align-left u-custom-item u-text u-text-black u-text-default u-text-2">Why it is so important</h4>

<p class="u-align-justify u-custom-item u-text u-text-body-alt-color u-text-default u-text-3" spellcheck="false"> Using Malicious URLs can threaten your sensitive data. so every person should aware about malicious things in URL.</p>

</div>

</div>

<div class="u-container-style u-custom-item u-list-item u-radius-20 u-repeater-item u-shape-round u-video-cover u-white u-list-item-2">

<div class="u-container-layout u-similar-container u-container-layout-2">

<h4 class="u-align-left u-custom-item u-text u-text-default u-text-4">---&gt;</h4>

<p class="u-align-justify u-custom-item u-text u-text-default u-text-5" spellcheck="false"> URLs allow Internet users to navigate from one website to another. They comprehensively represent access to content that it is stored in servers, somewhere in the world.&nbsp;</p>

</div>

</div>

<div class="u-container-style u-custom-item u-list-item u-radius-20 u-repeater-item u-shape-round u-video-cover u-white u-list-item-3">

<div class="u-container-layout u-similar-container u-container-layout-3">

<h4 class="u-align-left u-custom-item u-text u-text-default u-text-6">---&gt;</h4>

<p class="u-align-justify u-custom-item u-text u-text-default u-text-7" spellcheck="false"> Our objective is to classify URLs given as inputs to predict if they are dangerous or inoffensive</p>

</div>

</div>

<div class="u-container-style u-custom-item u-gradient u-list-item u-radius-20 u-repeater-item u-shape-round u-video-cover u-list-item-4">

<div class="u-container-layout u-similar-container u-container-layout-4">

<h4 class="u-align-left u-custom-item u-text u-text-black u-text-default u-text-8">Goals</h4>

<p class="u-align-justify u-custom-item u-text u-text-body-alt-color u-text-default u-text-9" spellcheck="false"> In this tech era, everyone is using technology and somehow directly or indirectly connected with URLs. so it is very important that every single person uses safe URLs only.&nbsp;</p>

</div>

</div>

</div>

</div>

</div>

</section>

<section class="u-clearfix u-section-5" id="carousel\_33aa">

<div class="u-clearfix u-sheet u-valign-middle u-sheet-1">

<div class="u-clearfix u-expanded-width-md u-expanded-width-sm u-expanded-width-xs u-layout-wrap u-layout-wrap-1">

<div class="u-layout">

<div class="u-layout-row">

<div class="u-container-style u-layout-cell u-left-cell u-size-15 u-size-60-md u-layout-cell-1">

<div class="u-container-layout u-container-layout-1">

<!-- <h4 class="u-align-left u-text u-text-1"> Online learning</h4> -->

<p class="u-align-justify u-text u-text-2" spellcheck="false"> Throughout the years, cybercriminals have become more skilled at

escaping discovery by lurking within benign things and attacking their

targets. They essentially utilize URLs that lead targets to genuine yet

compromised websites or have safe-looking redirectors that ultimately

redirect targets to a phishing plot.</p>

</div>

</div>

<div class="u-align-justify u-container-style u-layout-cell u-size-18-lg u-size-18-xl u-size-21-sm u-size-21-xs u-size-60-md u-layout-cell-2">

<div class="u-container-layout u-container-layout-2"><span class="u-icon u-icon-circle u-text-palette-3-base u-icon-1"><svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 95.333 95.332" style=""><use xlink:href="#svg-cbee"></use></svg><svg class="u-svg-content" viewBox="0 0 95.333 95.332" x="0px" y="0px" id="svg-cbee" style=""><g><g><path d="M30.512,43.939c-2.348-0.676-4.696-1.019-6.98-1.019c-3.527,0-6.47,0.806-8.752,1.793 c2.2-8.054,7.485-21.951,18.013-23.516c0.975-0.145,1.774-0.85,2.04-1.799l2.301-8.23c0.194-0.696,0.079-1.441-0.318-2.045 s-1.035-1.007-1.75-1.105c-0.777-0.106-1.569-0.16-2.354-0.16c-12.637,0-25.152,13.19-30.433,32.076 c-3.1,11.08-4.009,27.738,3.627,38.223c4.273,5.867,10.507,9,18.529,9.313c0.033,0.001,0.065,0.002,0.098,0.002 c9.898,0,18.675-6.666,21.345-16.209c1.595-5.705,0.874-11.688-2.032-16.851C40.971,49.307,36.236,45.586,30.512,43.939z"></path><path d="M92.471,54.413c-2.875-5.106-7.61-8.827-13.334-10.474c-2.348-0.676-4.696-1.019-6.979-1.019 c-3.527,0-6.471,0.806-8.753,1.793c2.2-8.054,7.485-21.951,18.014-23.516c0.975-0.145,1.773-0.85,2.04-1.799l2.301-8.23 c0.194-0.696,0.079-1.441-0.318-2.045c-0.396-0.604-1.034-1.007-1.75-1.105c-0.776-0.106-1.568-0.16-2.354-0.16 c-12.637,0-25.152,13.19-30.434,32.076c-3.099,11.08-4.008,27.738,3.629,38.225c4.272,5.866,10.507,9,18.528,9.312 c0.033,0.001,0.065,0.002,0.099,0.002c9.897,0,18.675-6.666,21.345-16.209C96.098,65.559,95.376,59.575,92.471,54.413z"></path>

</g>

</g></svg></span>

<p class="u-text u-text-3" spellcheck="false"> According to the statistics in the 2018 Keepnet Phishing

Trends Report dataset,<span class="u-text-palette-3-base">

<span style="font-weight: 700;">49.32%</span>

</span> of phishing messages were

opened by the target across all organizations,&nbsp; <span class="u-text-palette-3-base" style="font-weight: 700;">33.10 %</span> went on to click the malicious attachment or link, <span class="u-text-palette-3-base" style="font-weight: 700;">12.87 %</span> handed over the information.

</p>

</div>

</div>

<div class="u-align-center-sm u-align-center-xs u-container-style u-layout-cell u-right-cell u-size-24-sm u-size-24-xs u-size-27-lg u-size-27-xl u-size-60-md u-layout-cell-3">

<div class="u-container-layout u-valign-middle-md u-container-layout-3">

<div class="u-expanded-width u-gradient u-shape u-shape-rectangle u-shape-1"></div>

<img src="images/ggg.jpg" alt="" class="u-align-left u-image u-image-default u-image-1" data-image-width="900" data-image-height="946">

</div>

</div>

</div>

</div>

</div>

</div>

</section>

<section class="u-align-center u-clearfix u-grey-5 u-section-6" id="carousel\_6405">

<div class="u-clearfix u-sheet u-valign-middle u-sheet-1">

<div class="u-clearfix u-expanded-width u-gutter-20 u-layout-wrap u-layout-wrap-1">

<div class="u-layout">

<div class="u-layout-row">

<div class="u-align-center u-container-style u-layout-cell u-size-60 u-layout-cell-1">

<div class="u-container-layout u-valign-middle-lg u-valign-middle-md u-valign-middle-xl u-container-layout-1">

<div class="u-form u-form-1">

<form action="//publish.nicepage.com/Form/Process" method="POST" class="u-clearfix u-form-spacing-15 u-form-vertical u-inner-form" style="padding: 0;" source="email" name="form">

<input type="hidden" id="siteId" name="siteId" value="1768619">

<input type="hidden" id="pageId" name="pageId" value="1768631">

<div class="u-form-email u-form-group u-form-partition-factor-2 u-form-group-1">

<label for="email-f2a8" class="u-label u-label-1">E-mail</label>

<input type="email" placeholder="Enter a valid email address" id="email-f2a8" name="email" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle" required="">

</div>

<div class="u-form-group u-form-name u-form-partition-factor-2 u-form-group-2">

<label for="name-f2a8" class="u-label u-label-2">Name</label>

<input type="text" placeholder="Enter your Name" id="name-f2a8" name="name" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle" required="">

</div>

<div class="u-form-group u-form-select u-form-group-3">

<label for="select-8e9d" class="u-form-control-hidden u-label u-label-3">Select</label>

<div class="u-form-select-wrapper">

<select id="select-8e9d" name="select" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle">

<option value="Item 1">Item 1</option>

<option value="Item 2">Item 2</option>

<option value="Item 3">Item 3</option>

</select>

<svg xmlns="http://www.w3.org/2000/svg" width="14" height="12" version="1" class="u-caret"><path fill="currentColor" d="M4 8L0 4h8z"></path></svg>

</div>

</div>

<div class="u-form-date u-form-group u-form-partition-factor-2 u-form-group-4">

<label for="date-4441" class="u-label u-label-4">Date</label>

<input type="date" placeholder="MM/DD/YYYY" id="date-4441" name="date" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle" required="">

</div>

<div class="u-form-group u-form-partition-factor-2 u-form-phone u-form-group-5">

<label for="phone-447e" class="u-label u-label-5">Phone</label>

<input type="tel" pattern="\+?\d{0,2}[\s\(\-]?([0-9]{3})[\s\)\-]?([\s\-]?)([0-9]{3})[\s\-]?([0-9]{2})[\s\-]?([0-9]{2})" placeholder="Enter your phone (e.g. +14155552675)" id="phone-447e" name="phone" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle" required="">

</div>

<div class="u-form-group u-form-message u-form-group-6">

<label for="message-f2a8" class="u-label u-label-6">Message</label>

<textarea placeholder="Enter your message" rows="4" cols="50" id="message-f2a8" name="message" class="u-border-2 u-border-grey-75 u-border-no-left u-border-no-right u-border-no-top u-input u-input-rectangle" required=""></textarea>

</div>

<div class="u-align-left u-form-group u-form-submit u-form-group-7">

<a href="#" class="u-active-palette-1-base u-border-none u-btn u-btn-rectangle u-btn-submit u-button-style u-hover-palette-1-base u-palette-3-base u-text-active-white u-text-hover-white u-text-palette-1-base u-btn-1">Submit</a>

<input type="submit" value="submit" class="u-form-control-hidden">

</div>

<div class="u-form-send-message u-form-send-success"> Thank you! Your message has been sent. </div>

<div class="u-form-send-error u-form-send-message"> Unable to send your message. Please fix errors then try again. </div>

<input type="hidden" value="" name="recaptchaResponse">

</form>

</div>

</div>

</div>

</div>

</div>

</div>

</div>

</section>

<footer class="u-align-center-md u-align-center-sm u-align-center-xs u-clearfix u-footer u-grey-80" id="sec-90c0"><div class="u-clearfix u-sheet u-sheet-1">

<p class="u-align-center u-text u-text-1" spellcheck="false">Follow us on</p>

<p class="u-align-center-lg u-align-center-md u-align-center-xl u-custom-font u-font-lobster u-text u-text-2" spellcheck="false">Thank you</p>

<div class="u-align-left u-social-icons u-spacing-10 u-social-icons-1">

<a class="u-social-url" title="facebook" target="\_blank" href=""><span class="u-icon u-social-facebook u-social-icon u-icon-1"><svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 112 112" style=""><use xlink:href="#svg-4736"></use></svg><svg class="u-svg-content" viewBox="0 0 112 112" x="0" y="0" id="svg-4736"><circle fill="currentColor" cx="56.1" cy="56.1" r="55"></circle><path fill="#FFFFFF" d="M73.5,31.6h-9.1c-1.4,0-3.6,0.8-3.6,3.9v8.5h12.6L72,58.3H60.8v40.8H43.9V58.3h-8V43.9h8v-9.2

c0-6.7,3.1-17,17-17h12.5v13.9H73.5z"></path></svg></span>

</a>

<a class="u-social-url" title="twitter" target="\_blank" href=""><span class="u-icon u-social-icon u-social-twitter u-icon-2"><svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 112 112" style=""><use xlink:href="#svg-d30f"></use></svg><svg class="u-svg-content" viewBox="0 0 112 112" x="0" y="0" id="svg-d30f"><circle fill="currentColor" class="st0" cx="56.1" cy="56.1" r="55"></circle><path fill="#FFFFFF" d="M83.8,47.3c0,0.6,0,1.2,0,1.7c0,17.7-13.5,38.2-38.2,38.2C38,87.2,31,85,25,81.2c1,0.1,2.1,0.2,3.2,0.2

c6.3,0,12.1-2.1,16.7-5.7c-5.9-0.1-10.8-4-12.5-9.3c0.8,0.2,1.7,0.2,2.5,0.2c1.2,0,2.4-0.2,3.5-0.5c-6.1-1.2-10.8-6.7-10.8-13.1

c0-0.1,0-0.1,0-0.2c1.8,1,3.9,1.6,6.1,1.7c-3.6-2.4-6-6.5-6-11.2c0-2.5,0.7-4.8,1.8-6.7c6.6,8.1,16.5,13.5,27.6,14

c-0.2-1-0.3-2-0.3-3.1c0-7.4,6-13.4,13.4-13.4c3.9,0,7.3,1.6,9.8,4.2c3.1-0.6,5.9-1.7,8.5-3.3c-1,3.1-3.1,5.8-5.9,7.4

c2.7-0.3,5.3-1,7.7-2.1C88.7,43,86.4,45.4,83.8,47.3z"></path></svg></span>

</a>

<a class="u-social-url" title="instagram" target="\_blank" href=""><span class="u-icon u-social-icon u-social-instagram u-icon-3"><svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 112 112" style=""><use xlink:href="#svg-50f4"></use></svg><svg class="u-svg-content" viewBox="0 0 112 112" x="0" y="0" id="svg-50f4"><circle fill="currentColor" cx="56.1" cy="56.1" r="55"></circle><path fill="#FFFFFF" d="M55.9,38.2c-9.9,0-17.9,8-17.9,17.9C38,66,46,74,55.9,74c9.9,0,17.9-8,17.9-17.9C73.8,46.2,65.8,38.2,55.9,38.2

z M55.9,66.4c-5.7,0-10.3-4.6-10.3-10.3c-0.1-5.7,4.6-10.3,10.3-10.3c5.7,0,10.3,4.6,10.3,10.3C66.2,61.8,61.6,66.4,55.9,66.4z"></path><path fill="#FFFFFF" d="M74.3,33.5c-2.3,0-4.2,1.9-4.2,4.2s1.9,4.2,4.2,4.2s4.2-1.9,4.2-4.2S76.6,33.5,74.3,33.5z"></path><path fill="#FFFFFF" d="M73.1,21.3H38.6c-9.7,0-17.5,7.9-17.5,17.5v34.5c0,9.7,7.9,17.6,17.5,17.6h34.5c9.7,0,17.5-7.9,17.5-17.5V38.8

C90.6,29.1,82.7,21.3,73.1,21.3z M83,73.3c0,5.5-4.5,9.9-9.9,9.9H38.6c-5.5,0-9.9-4.5-9.9-9.9V38.8c0-5.5,4.5-9.9,9.9-9.9h34.5

c5.5,0,9.9,4.5,9.9,9.9V73.3z"></path></svg></span>

</a>

<a class="u-social-url" title="linkedin" target="\_blank" href=""><span class="u-icon u-social-icon u-social-linkedin u-icon-4"><svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 112 112" style=""><use xlink:href="#svg-9a01"></use></svg><svg class="u-svg-content" viewBox="0 0 112 112" x="0" y="0" id="svg-9a01"><circle fill="currentColor" cx="56.1" cy="56.1" r="55"></circle><path fill="#FFFFFF" d="M41.3,83.7H27.9V43.4h13.4V83.7z M34.6,37.9L34.6,37.9c-4.6,0-7.5-3.1-7.5-7c0-4,3-7,7.6-7s7.4,3,7.5,7

C42.2,34.8,39.2,37.9,34.6,37.9z M89.6,83.7H76.2V62.2c0-5.4-1.9-9.1-6.8-9.1c-3.7,0-5.9,2.5-6.9,4.9c-0.4,0.9-0.4,2.1-0.4,3.3v22.5

H48.7c0,0,0.2-36.5,0-40.3h13.4v5.7c1.8-2.7,5-6.7,12.1-6.7c8.8,0,15.4,5.8,15.4,18.1V83.7z"></path></svg></span>

</a>

</div>

</div></footer>

<section class="u-backlink u-clearfix u-grey-80">

<a class="u-link" href="https://nicepage.com/html-templates" target="\_blank">

<span>HTML Website Templates</span>

</a>

<p class="u-text">

<span>created with</span>

</p>

<a class="u-link" href="" target="\_blank">

<span>WYSIWYG Web Builder</span>

</a>.

</section><span style="height: 64px; width: 64px; margin-left: 0px; margin-right: auto; margin-top: 0px; background-image: none; right: 20px; bottom: 20px" class="u-back-to-top u-icon u-icon-circle u-opacity u-opacity-85 u-palette-1-base u-spacing-15" data-href="#">

<svg class="u-svg-link" preserveAspectRatio="xMidYMin slice" viewBox="0 0 551.13 551.13"><use xmlns:xlink="http://www.w3.org/1999/xlink" xlink:href="#svg-1d98"></use></svg>

<svg class="u-svg-content" enable-background="new 0 0 551.13 551.13" viewBox="0 0 551.13 551.13" xmlns="http://www.w3.org/2000/svg" id="svg-1d98"><path d="m275.565 189.451 223.897 223.897h51.668l-275.565-275.565-275.565 275.565h51.668z"></path></svg>

</span>

</body>

</html>

4.4 Subsystem services:

The Visual Studio Code is the subsystem service used in our project. Visual Studio Code is a streamlined code editor with support for development operations like debugging, task running, and version control.

4.5 API Fetching

For fetching API with the Website is used:

<script>

let SubBtn = document.querySelector('#SubBtn')

SubBtn.addEventListener('click',generate);

console.log("Hello")

function generate(){

let email = document.getElementById('email-6797').value;

url = "https://endpoint.apivoid.com/urlrep/v1/pay-as-you-go/?key=09d2414e22a102405a6ecee3d96954874ae0c966&url="+email;

console.log(url);

fetch(url,{"method":"GET"})

.then((response) => {

return response.json();

}).then((data) => {

console.log('Hii')

console.log(data.data.report);

let res = `<div class="m-4 p-4 h-50 border border-warning border-3 rounded-3">

<h2 class="text-center">Result-:</h2>

<p class="style risk\_score"><b>risk-score-: ${data.data.report.risk\_score.result}</b></p>

<p class="style"><b>is\_phishing\_heuristic-: ${data.data.report.security\_checks.is\_phishing\_heuristic}</b></p>

<p class="style"><b>hostname-: ${data.data.report.server\_details.hostname}</b></p>

<p class="style"><b>ip-: ${data.data.report.server\_details.ip}</b></p>

<p class="style"><b>city\_name-: ${data.data.report.server\_details.city\_name}</b></p>

<p class="style"><b>country\_name-: ${data.data.report.server\_details.country\_name}</b></p>

<p class="style"><b>continent\_name-: ${data.data.report.server\_details.continent\_name}</b></p>

<p class="style"><b>host-: ${data.data.report.url\_parts.host}</b></p>

<p class="style"><b>scheme-: ${data.data.report.url\_parts.scheme}</b></p>

</div>`

let urlcheck = document.getElementById('urlcheck').innerHTML = res;

});

}

</script>

4.6 Summary:

In this chapter, we have very elaborately discussed about the methodology and goal of our project. Then we have explained the functional modules, we have then discussed the Website Architectural Design and API Fetching of our project.

**CHAPTER-5**

**TECHNICAL IMPLEMENTATION & ANALYSIS**

5.1Outline:

In this chapter will look into the application’s performance; success rates, tests, prototypes, etc.

5.2 Technical coding and code solutions:

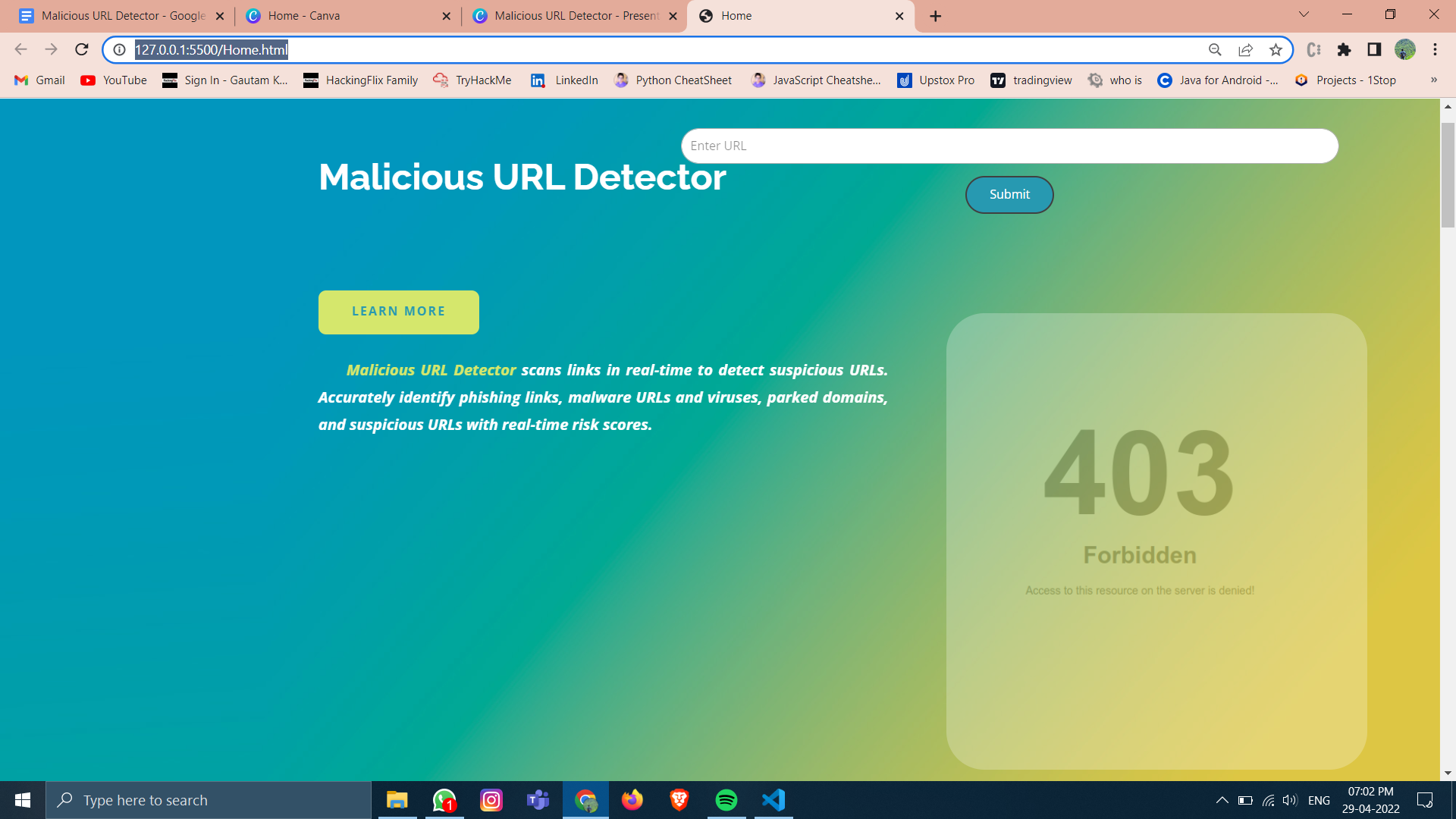
Java Script and HTMLcoding are used in our project;

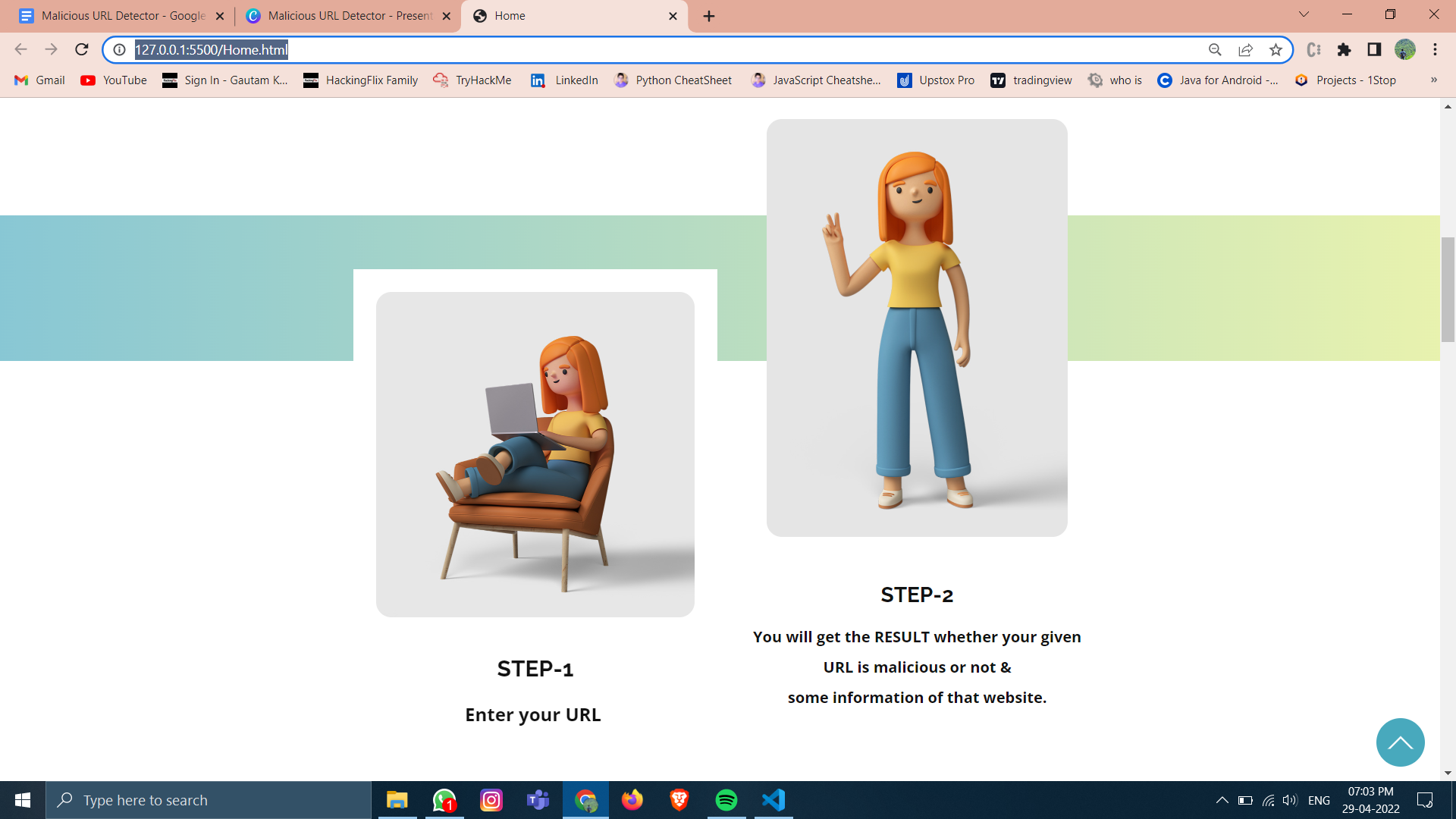
5.3 Working Layout of Forms:

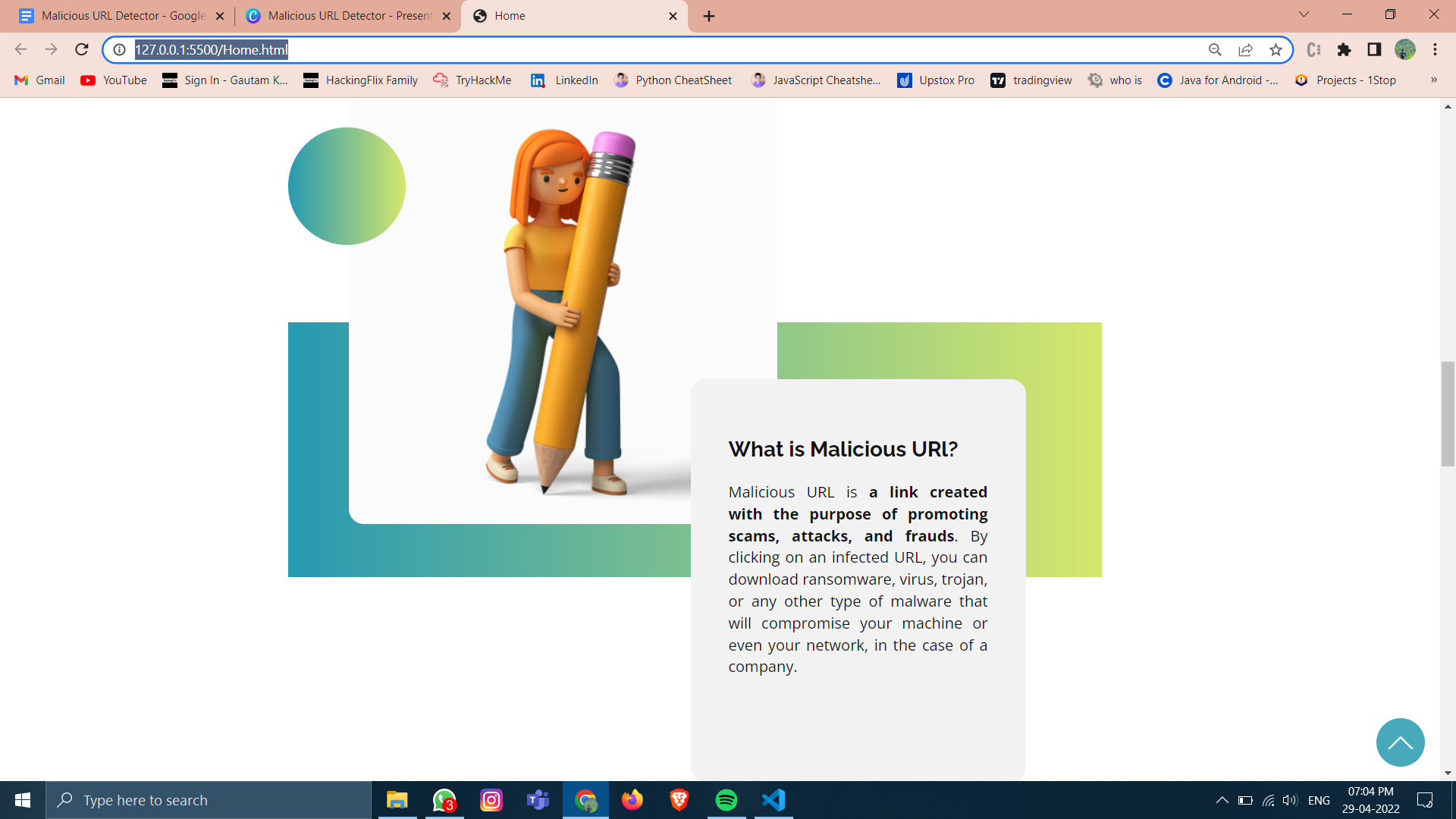
We have first found various ways of detecting phishing sites then implemented the most appropriate one in the application. So, the working layout is somewhat like

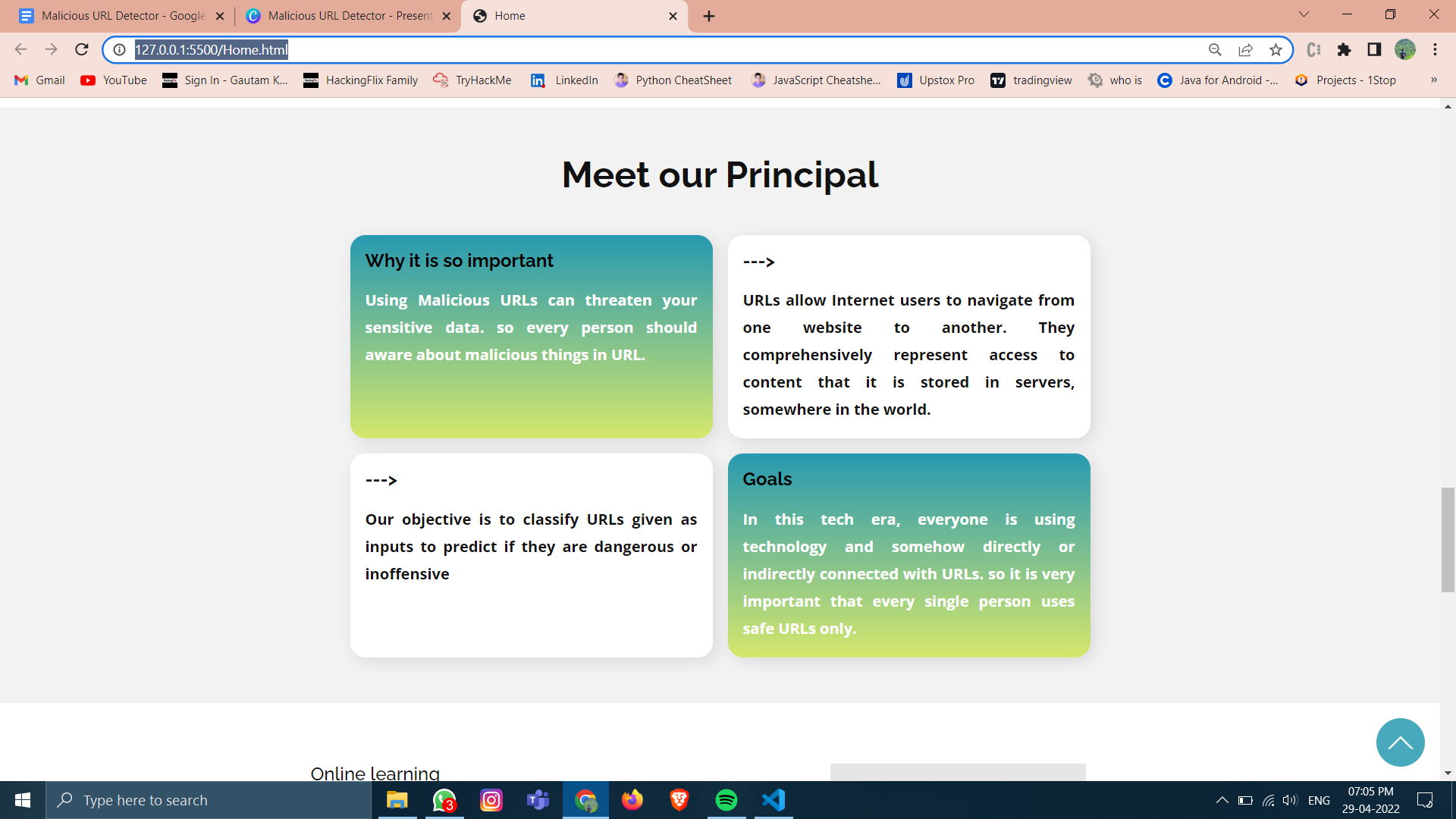
API Details --------> website

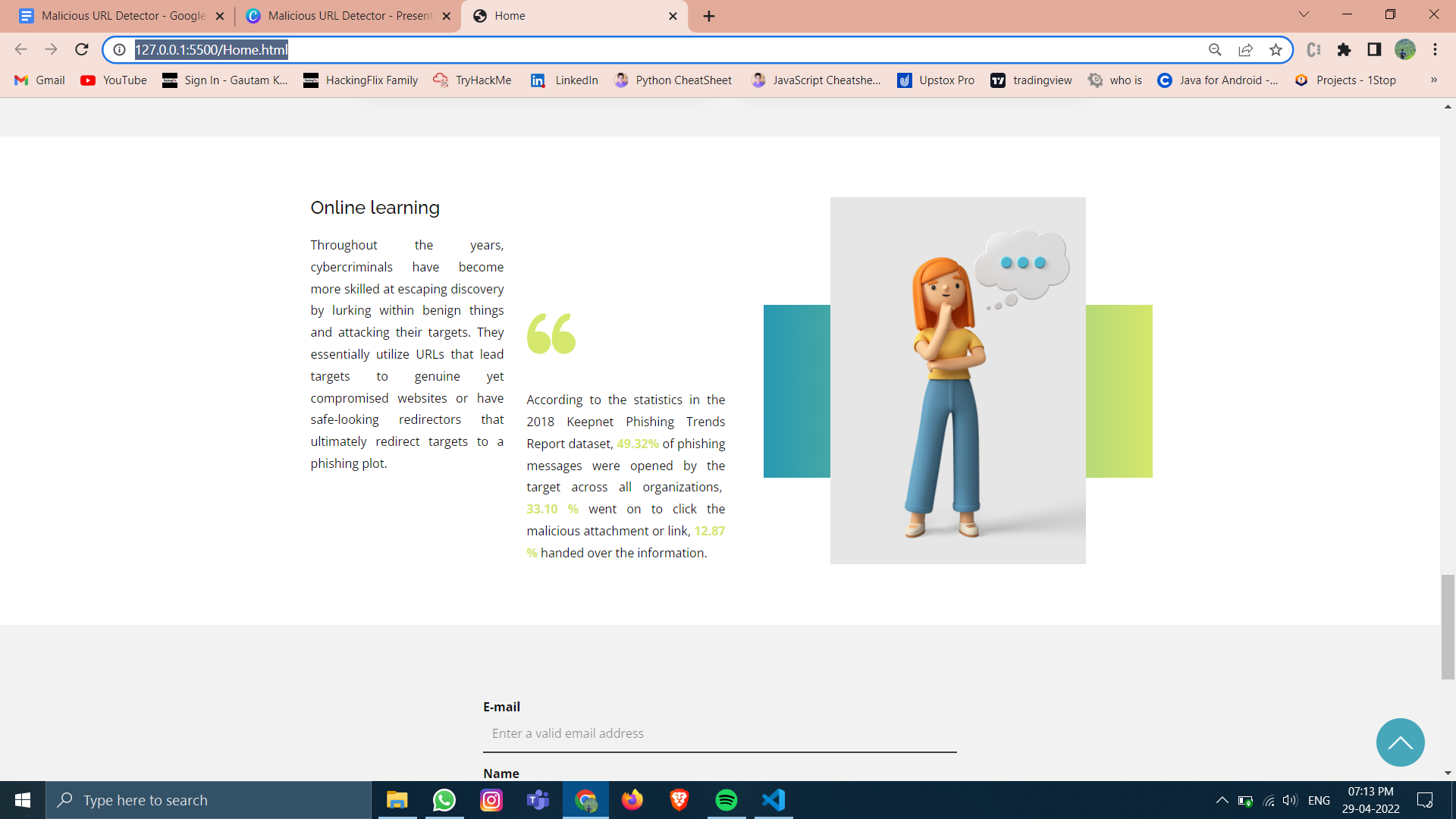
5.4 Prototype submission:



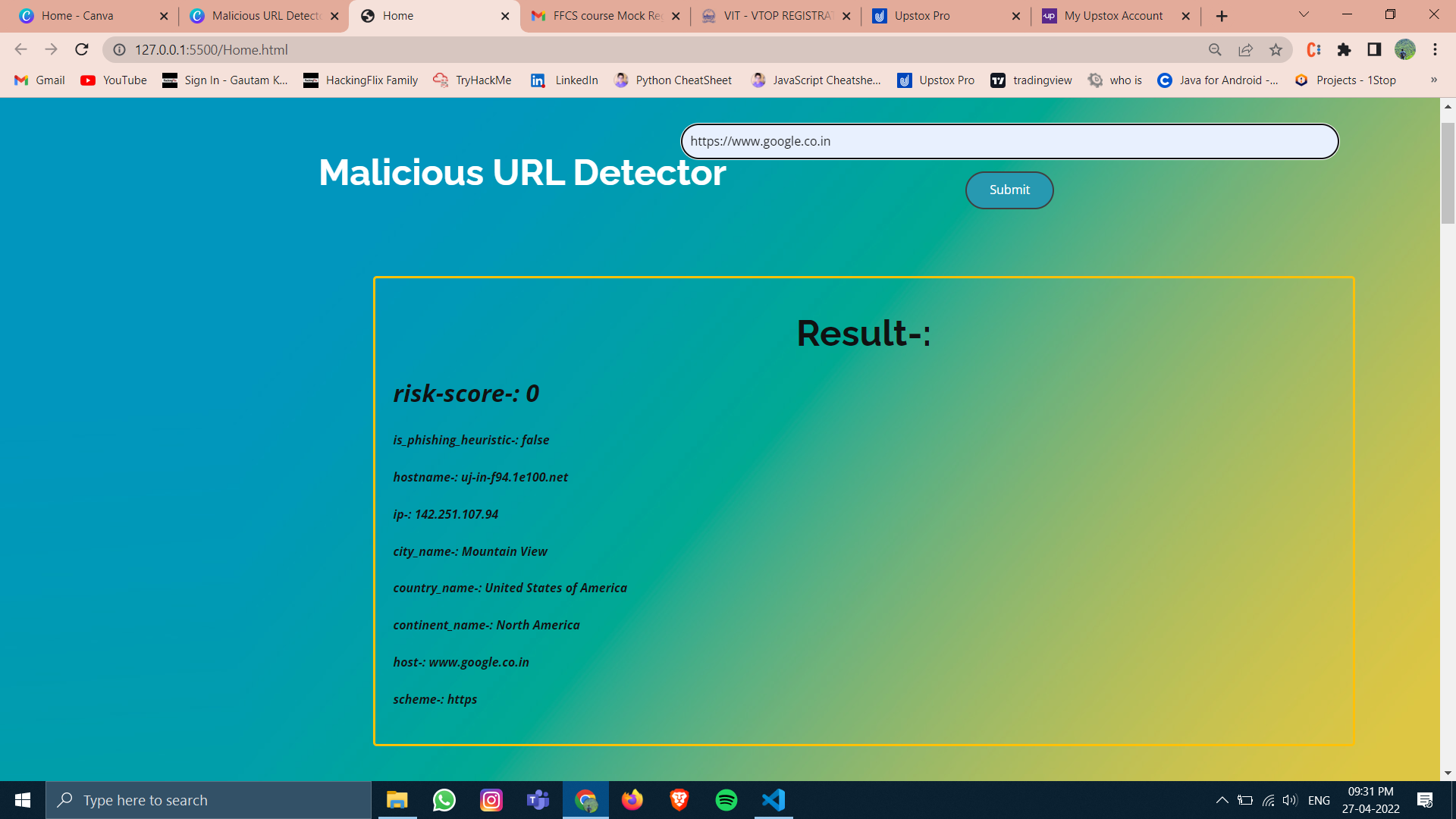


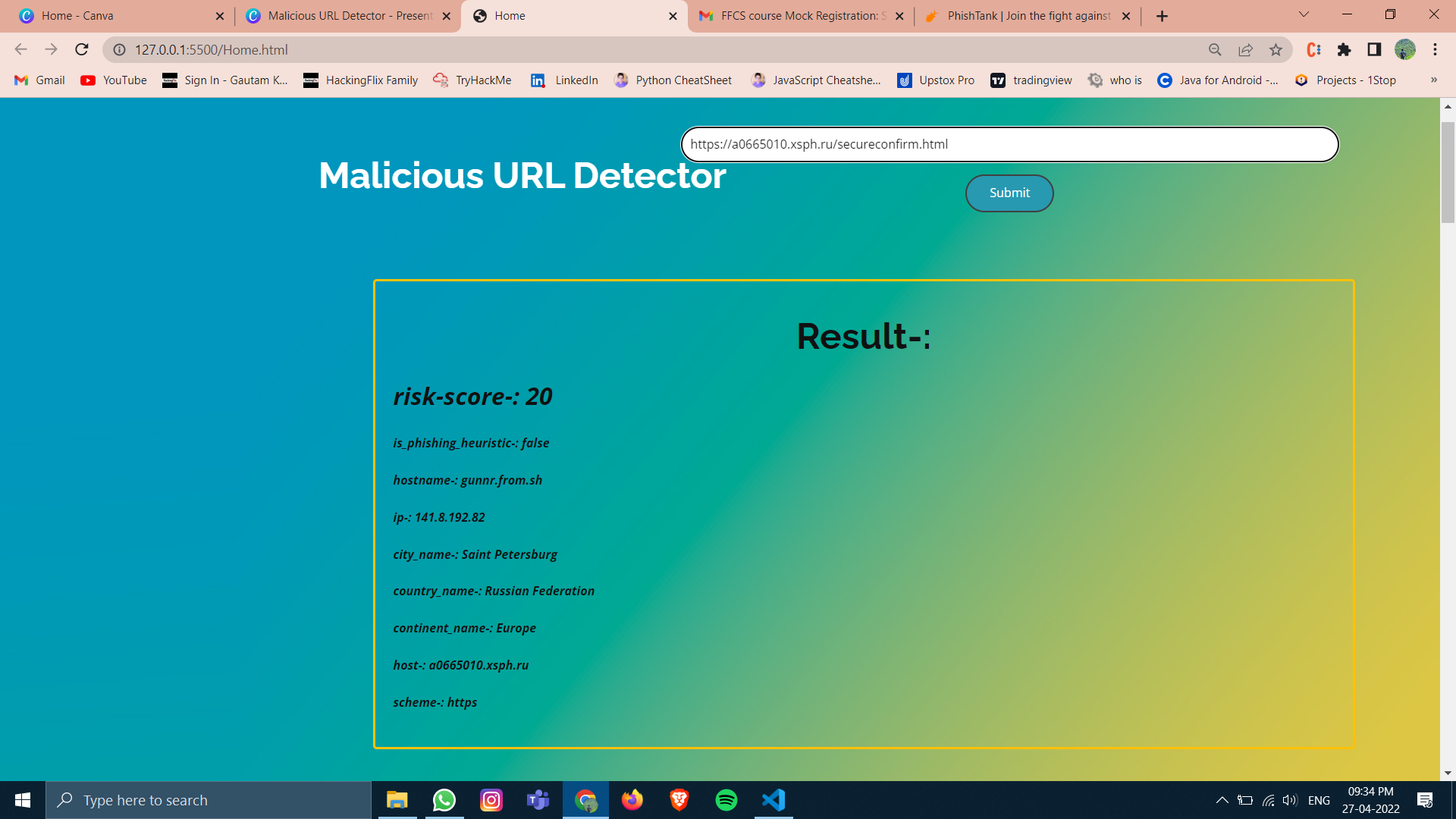






5.5 Test and validation:





5.7 Summary:

In this chapter we have explained technical coding, working layout of our project, prototype of our project, then we have shown the test analysis and performance analysis of our project.

**CHAPTER-6**

**PROJECT OUTCOME AND APPLICABILITY**

6.1Outline:

The project is successfully implemented by us. It works well, smooth and fine. The outcome is the same as we expected, it successfully detects the urls, and it also gives the complete details about the url like timestamp, hostname,location,ip,http scheme,risk score.

6.2 Key implementations outline of the System:

The main part of the project is the implementation of the code and connecting the API to the website. We managed to achieve it and next to it hosting our website and making it secure to use.

6.3 Significant project outcomes:

The project is successfully implemented and works for all types of urls. It successfully detects malicious urls and vulnerable urls using the API and lets us know beforehand.

6.4 Project applicability on Real-world applications:

This project is just singly purposed to detect the malicious urls and give its risk score based upon its vulnerabilities. It can be merged into multi-function applications like mobile antivirus programs. It can also be made to detect suspicious links and viruses automatically as most desktop antivirus programs do.

6.4 Inference:

Here in the chapter, we discussed how we implemented and also tried for what purpose it can be used in the real world. It can work well as a single-purpose website or can be further enhanced and clubbed with other advanced security applications which gives us the future extension.

**CHAPTER-7**

**CONCLUSIONS AND RECOMMENDATION**

7.1Outline:

We can conclude that phishing links are not the same as ordinary links, they can be judged and we can find whether they are phishing or not.

7.2 Limitation/Constraints of the System:

The limitation of phishing detection is that most detectors are not accurate; they sometimes give false results. Also, some may even ask for signing up for detection and the limitation of the project is it works only on address bar features.

7.3 Future Enhancements:

The website is purely based upon some address bar features for the detection of phishing links. We can also move on using many more complex features like domain-based features, Html/JavaScript-based features, and abnormal features which can link more potentially phishing ones. It can be further made more advanced by adding more features like we don’t have to put links for detections. It automatically detects the link and shows them in green if they are safe or in red if they are doubtful ones.

7.4 Inference:

As discussed, phishing can be dangerous, so we must have prevention against them. Most phishing links have Address bar-based issues; they are not like ordinary links. So, we can infer from this that phishing links are not like ordinary links, they can be judged on various parameters to know whether they are phishing or not.

**RELATED WORK INVESTIGATION**

Anderson, J. R., A. T. Corbett, K. Koedinger, and R. Pelletier in 1995 they identified Phishing attacks, in which criminals lure Internet users to websites that impersonate legitimate sites, are occurring with increasing frequency and are causing considerable harm to victims. They have described in a paper the design and evaluation of an embedded training email system that teaches people about phishing during their normal use of email. They have conducted lab experiments contrasting the effectiveness of standard security notices about phishing with two embedded training designs they developed. They found that embedded training works better than the current practice of sending security notices which was used before 1995. They also derived sound design principles for embedded training systems.

**REFERENCES**

1. M. Mohammad School of Computing and Engineering University of Huddersfield Huddersfield, UK.rami.mohammad@hud.ac.uk
2. Fadi Thabtah E-Business Department Canadian University of Dubai Dubai, UAE. fadi@cud.ac.ae
3. Lee McCluskey School of Computing and Engineering University of Huddersfield Huddersfield, UK. t.l.mccluskey@hud.ac.uk
4. <https://www.sciencedirect.com/topics/computer-science/phishing-detection>
5. <https://www.israeldefense.co.il/en/node/52989>
6. <https://docs.apivoid.com/>