CHROME EXTENSION FOR DETECTING PHISHING WEBSITES

A PROJECT REPORT

submitted By

MUBEENA NAZAR
TVE20MCA2041

to

the APJ Abdul Kalam Technological University
in partial fullfilment of the requirements for the award of the degree

of

Master of Computer Applications

Department of Computer Applications
College of Engineering
Trivandrum-695016

MARCH 2022

Declaration

I undersigned hereby declare that the project report titled ”Chrome Extension for Detecting Phishing Websites” submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Smt. Minu R Nath, Assistant Professor. This submission represents my ideas in my words and where ideas or words of others have been included. I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity as directed in the ethics policy of the college and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and/or University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title.

Place : Trivandrum **MUBEENA NAZAR**
Date : 05/03/2022

DEPARTMENT OF COMPUTER APPLICATIONS

COLLEGE OF ENGINEERING
TRIVANDRUM

CERTIFICATE

This is to certify that the report entitled **CHROME EXTENSION FOR DETECTING PHISHING WEBSITES** submitted by **MUBEENA NAZAR (TVE20MCA2041)** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications is a bonafide record of the project work carried out by her under my guidance and supervision. This report in any form has not been submitted to any University or Institute for any purpose.

Minu R Nath	Deepa S S
Internal Supervisor	Head of the Dept

Acknowledgement

If words are considered as symbols of approval and tokens of acknowledgement, then let words play the heralding role of expressing our gratitude.

First and for most I thank **GOD** almighty and to my parents for the success of this project. I owe a sincere gratitude and heart full thanks to everyone who shared their precious time and knowledge for the successful completion of my project.

I am extremely thankful to **Dr Jiji C V**, Principal, College of Engineering Trivandrum for providing me with the best facilities and atmosphere which was necessary for the successful completion of this project.

I am extremely grateful to **Assoc.Prof. Deepa S S**, HOD, Dept of Computer Applications, for providing me with best facilities and atmosphere for the creative work guidance and encouragement.

I express our sincere thanks to **Smt. Minu R Nath**, Asst. Professor, Department of Computer Applications, College of Engineering Trivandrum for her valuable guidance, support and advice that aided in the successful completion of my project.

I profusely thank other teachers in the department and all other staffs of CET, for their guidance and inspirations throughout my course of study.

I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this project. No words can express my humble gratitude to my beloved parents and relatives who have been guiding me in all walks of my journey.

MUBEENA NAZAR

Abstract

A phishing attack is the act of sending fraudulent communications that appear to come from a valid source. Today, phishing is one of the most common forms of online fraud. The goal is to steal sensitive data like user id, password, and financial information, login information, or to install malware on the victim's machine. 'Phishing sites' are a sort of safety troubles that particularly focuses on the human vulnerabilities as compared to software vulnerabilities. Phishing techniques are visual and semantically similar to those used by legitimate websites. 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 computers defence system.

Phishing websites can be detected using a database that contains blacklisted websites and the phishing links associated with them, which can be compared to the entered suspicious link to determine whether it is a URL of a phishing website or not. There is a risk of the user visiting the website if the link is not in the user's database. The goal of this research project is to create a Google Chrome extension that will detect phishing websites by connecting to the databases of several online phishing detectors that will be regularly updated . Due to its connections to multiple databases, it significantly reduces the risk of visiting illegitimate websites. In addition to giving an alert to the user, this extension also provides a detailed report on demand , from multiple databases , about why the corresponding website was blacklisted.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chrome extensions are programs that can be installed into Chrome to improve its functionality. By combining existing browser features, the extension can offer new functionality and allow users to perform many tasks simultaneously. A few of the functions that Google Chrome extensions have include blocking ads, managing passwords, and translating web pages.

Phishing imitates the features and characteristics of a website and makes it look the same as the original. These phishing websites are made to mock the appearance of an original organisation website. The user thinks that this is a genuine company or an organisation. By clicking on the links, the user is involuntarily visiting the phishing website. Phishing is a cyber crime, the reason behind the phishers doing this crime is that it is very easy to do this, it does not cost anything and is effective. In phishing attacks, phishers (attackers) manipulate their victims into providing sensitive information under false pretences. There are several types of phishing scams, including SMS messages, email, and fake websites. The purpose of this project is to build an extension that detects phishing sites and alerts users accordingly.The purpose of this project is to build an extension for Google Chrome that detects phishing sites and alerts users accordingly.

Chapter 2

Problem Definition and Motivation

Phishing is a very common social engineering attack these days. There are a lot of phishing detection websites that use their own strategies to detect phishing attacks, so an integrated platform incorporating the techniques used by websites can be more effective in detecting phishing attacks.

Google Chrome extension is suitable as a platform for development of such a system for many reasons. Firstly, the Google Chrome Extension is based on and installed inside the Chrome browser, which has a minimal effect on the use of the computer system resources.Secondly, the extension will be small in size and easy to install inside the browser. Google Chrome extension is safe and user-friendly because it just needs one click to install. When users want to stop it, they need one click to disable the extension.These are the driving force behind the development of this system.

Chapter 3

Literature Review

Phishing is a fraudulent attempt where attackers trick the victims into disclosing sensitive information under pretenses. This research project aims to develop a Google Chrome extension to detect phishing websites. As a part of my literature review I went through various papers and presentations on this topic. The quick summary of my findings are specified in this chapter.

'Detection and classification of phishing websites' [**1**] by Manoj P, Bhuvan Kumar, Rajshitha and Megha discussed the development of a machine learning classifier that analyzes phishing sites and picks appropriate combinations of systems for training the machine learning classifier

Hongkai Chen and Mohammad Hossain [**2**] proposed the Google extension frameworks that distinguish the phishing utilizing page section similitude that breaks down universal resource locator tokens to create forecast preciseness phishing pages normally keep its CSS vogue like their objective pages.

A paper on 'Chrome Extension for Detecting Phishing Websites ' [**3**] by Bhavya Shah, Karan Dharamshi, Mihir Patel and Dr. Vaishali Gaikwad proposed a chrome plugin that automates the job of detecting and overcoming traditional methods by using a machine learning algorithm. The paper utilises the Random Forest discriminative classifier for detection of phishing website.

Samuel Marchal [**4**] presents Phish Storm, an automated phishing detection system that can analyze in real time any URL in order to identify potential phishing sites. Phish Storm provides phishingness score for URL and can act as a Website reputation rating system.

In light of these papers' analysis, a Chrome extension can be developed that detects phishing websites by using all the methods and techniques described in these papers.

Chapter 4

Requirement Analysis

4.1 Purpose

The purpose of this project is to develop a chrome extension that detects phishing websites by connecting to an updated database. This system makes browsing more secure.
The main functions of the proposed system are:

- Sending an alert
- Providing report
- Comparison of result from multiple databases
- Cross-checking between multiple databases

4.2 Hardware Requirements

- Computers equipped with a Pentium 4 processor or higher
- Approximately 100MB of free hard drive space
- 128MB of RAM
- Web Browser
- Internet Connection

4.3 Software Requirements

- WINDOWS 7 or higher
- Python 3.6.0 or higher
- Visual Studio Code
- Django
- HTML
- JavaScript

4.4 Functional Requirements

The chrome extension warns the user whether website is phishing or not. The extension should adhere to the following requirements:

- It should be able to alert the user of the website's safety.
- It should be faster and easier to use.
- It should provide a report that specifies the reasons for categorizing a website as blacklisted.
- It should be able to detect newly created phishing sites, and keep up with emerging phishing techniques.

4.5 Non-Functional Requirements

4.5.1 User Interface

There must be a simple and easy to use user interface where the user should be able to quickly identify the phishing website. Input should be provided by the user, and output should be easily recognizable. The user should also receive a report regarding the results.

4.5.2 Performance

The chrome extension should be always available and should make fast detection with low false negatives. When a url of suspecting website is entered it will detect whether that website is phishing or not in quick time.

4.6 Constraints And Assumptions

4.6.1 Constraints

Data and reports are taken from external websites. Heavy techniques can't used considering the processing power of client machines and the page load time of the website. Only JavaScript can be used to develop chrome extension.

4.6.2 Assumption

The chrome extension is provided with the needed permissions in the chrome environment. The user has a basic knowledge about phishing and extensions

Chapter 5

Design And Implementation

5.1 Overall Design

The system warns the user about the safety of the website. In addition, users can also request reports about the security status of these from multiple websites. The system also provides a shorthand version of the virus total report.

This system provides a web interface for its users. It is added as a chrome extension. As a chrome extension, it is more user-friendly and efficient.

5.2 System Design

The proposed application can run in any browser in any Operating system . User can add it to their chrome extensions . Users can enter the url of a suspicious website and get alert , request for report from multiple websites and a report notably from virustotal .The tool is easily integrated into users context menus once added as an extension.

5.3 Data Flow Diagram

This diagrams gives a clear picture about the privileges of user.Also the entire working flow was specified in this.

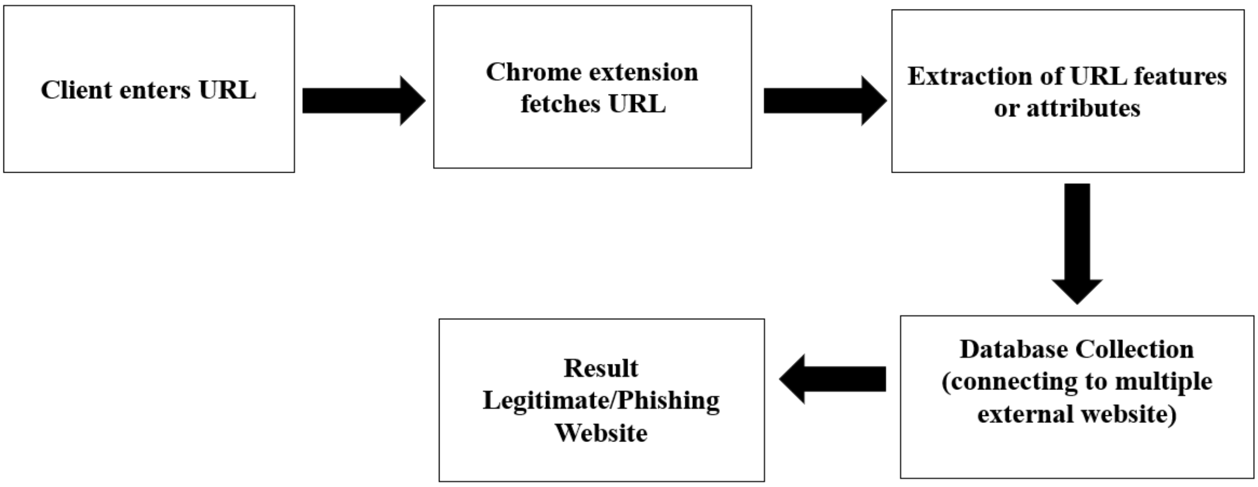

Client enters URL
Chrome extension fetches URL
Extraction of URL features or attributes
Database Collection (connecting to multiple external website)
Result Legitimate/Phishing Website

Figure 5.1: Data Flow diagram

5.4 User Case Diagram

This diagram gives a graphical depiction of a user's possible interactions with a system

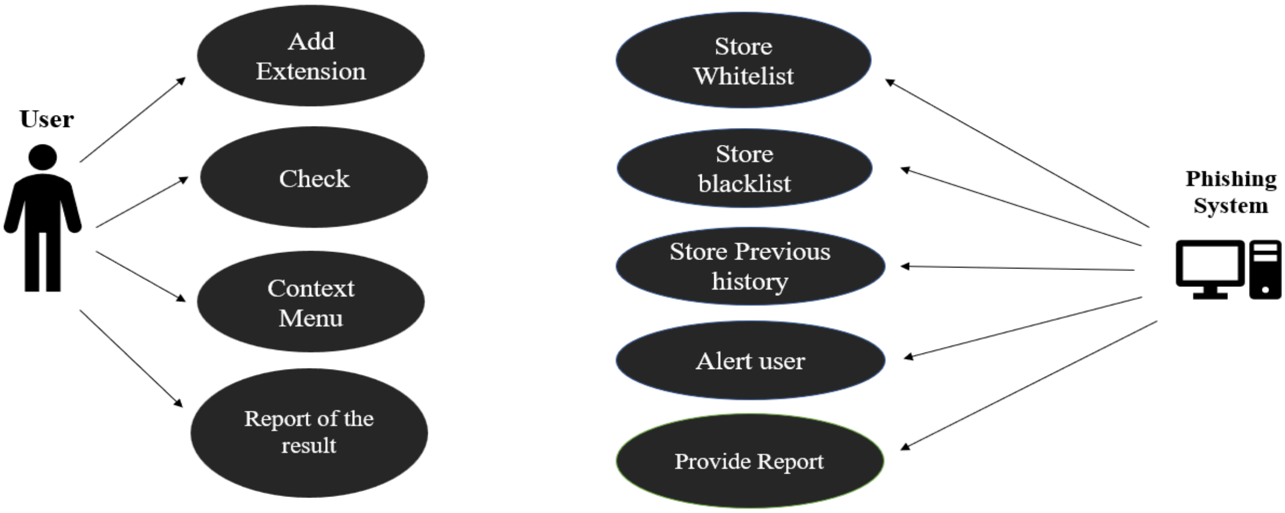


Figure 5.2: Use case diagram

5.5 User Interface Design

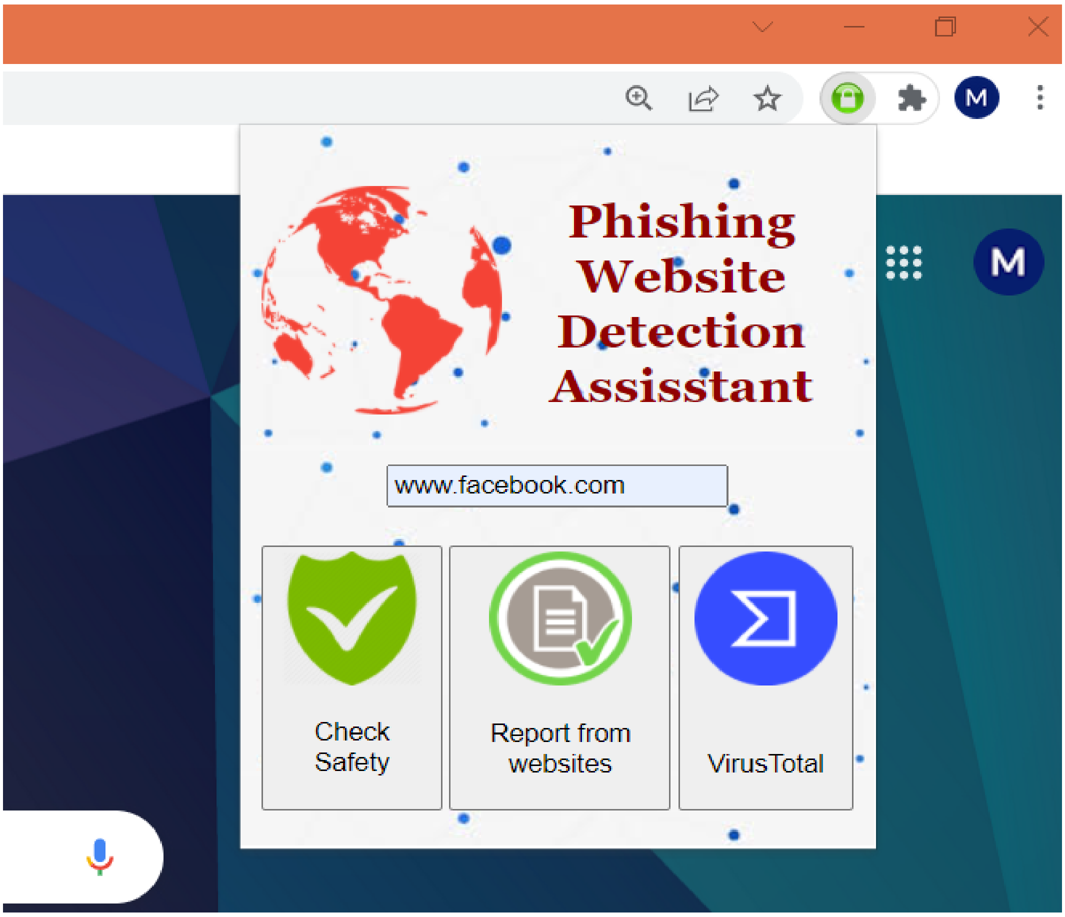


Figure 5.3: Google chrome extension for detecting phishing website

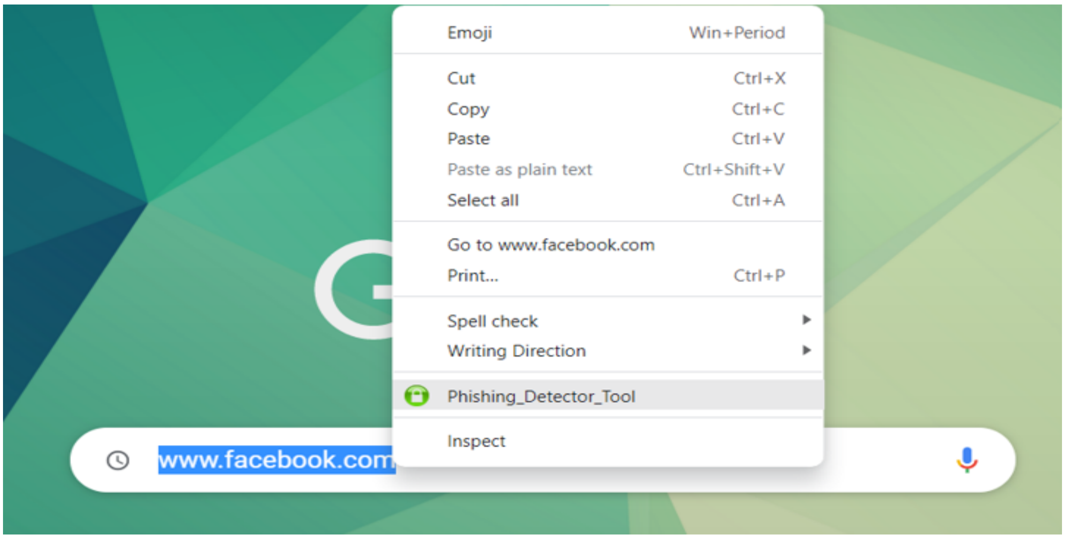
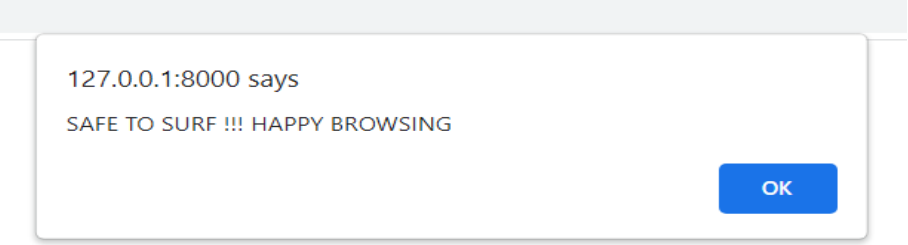


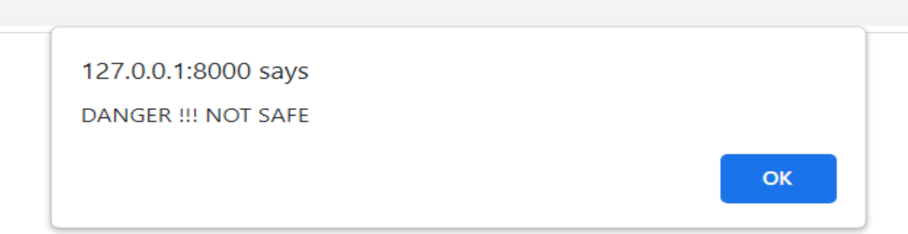
Figure 5.4: Context Menu with phishing detection tool



127.0.0.1:8000 says

SAFE TO SURF !!! HAPPY BROWSING

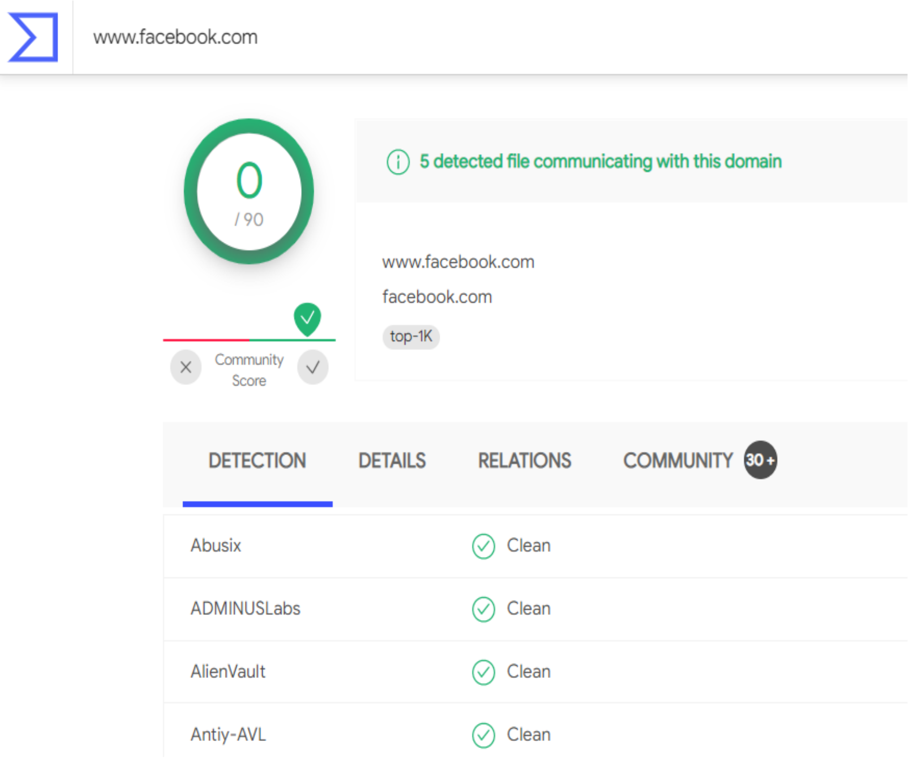
Figure 5.5: Alert box



127.0.0.1:8000 says

DANGER !!! NOT SAFE

Figure 5.6: Alert box



www.facebook.com

0 / 90

Community Score

5 detected file communicating with this domain

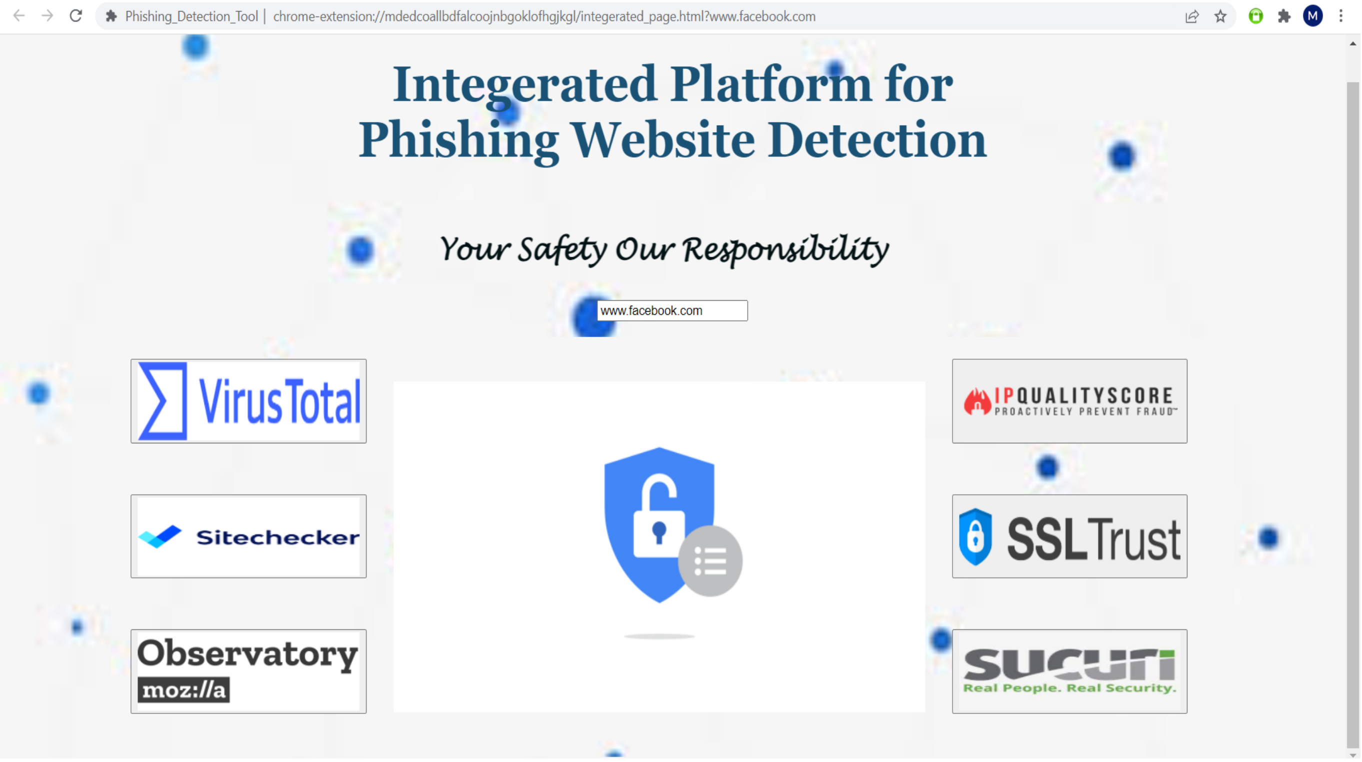
www.facebook.com

facebook.com

top-1K

Abusix	✓ Clean
ADMINUSLabs	✓ Clean
AlienVault	✓ Clean
Antiy-AVL	✓ Clean

Figure 5.7: Report from virus total



Phishing_Detection_Tool | chrome-extension://mdedcoallbdfalcoojnbgoklofhgjkgl/integerated_page.html?www.facebook.com

Integerated Platform for Phishing Website Detection

Your Safety Our Responsibility

www.facebook.com

VirusTotal
Sitechecker
Observatory moz://a
IPQUALITYSCORE PROACTIVELY PREVENT FRAUD™
SSLTrust
sucuri Real People. Real Security.

Figure 5.8: Integrated page to get the report

Chapter 6

Testing

6.1 Testing and various types of testing used

System testing is the period of time during which the structure is used to ensure that it functions correctly and efficiently before live development begins. Testing is the process of putting the software into action with the goal of finding errors and missing tasks. Check to see if the objectives have been reached and the client's needs have been addressed. Attestation of quality is a key element. The tests are completed, the results are segregated, and the standard record is kept. Everything that was thought to be incorrect turned out to be correct, and the research was completed. A test plan is created for each module using point-by-point testing approaches. The test plan depicts the unit, integration, and framework testing methods. The following are intertwined in the test scope: One of the most important goals of application framework testing is to ensure that the system meets the full functional requirements, including quality requirements (Non functional prerequisites). At the end of the project development cycle, the user should find that the project has met or exceeded all their expectation as detailed in requirements. Any changes, additions, or deletions to the requirements document,functional specification or design specification will be documented an tested at the higher level of quality allowed within the remaining time of the project and within the abiity of the test team.The secondary objective of testing application systems will be do: identity in expose all issues and associated risks,communicate all known issues are addressed in an appropriate matter before release.This test approach document describes the appropriate strategies,process,work flows and methodologies used to plan,organize,execute and manage testing to software project “Chrome extension for detecting phishing website”

6.1.1 System Testing

Text Cases and Result

Sl No	Procedures	Expected result	Actual result	Pass or Fail
1	Adding as a chrome extension	Succesfully added to the browser	Same as expected	Pass
2	Checking a suspicious URL	User get alert regarding the safety of the website	Same as expected	Pass
3	Demand for report regarding the security of the website from multiple websites	User gets a detailed report	same as expected	Pass
4	Detailed report from virus total	User get report from virus total	Same as expected	Pass
5	Automatically added in context menu for getting alert	User receives the alert	Same as expected	Pass

Table 6.1: System test cases and results

Chapter 7

Results and Discussion

It is observed that the system performs all the functionalities as expected. The primary objective is to safeguard the users from the threat of phishing via alerts about the security of the website and the provision of a report upon request. This way, they will be able to compare results across multiple websites and draw conclusions. Adding this feature to the context menu makes it more accessible for the users.

7.1 Advantages

- Reduces security risks
- The computation time is very short, and it is more user-friendly
- Using multiple databases for better results
- Detailed site report
- Detection by hiding the users identity from phishers.

7.2 Limitations

- Results are not 100
- Relies on external websites
- Working offline is not possible

Chapter 8

Conclusion

Phishing attacks have been found to be very problematic, and a mechanism to detect them is vital in order to protect the personal information of users. Because the personal information of users can be leaked through phishing websites, it is imperative to take care of this issue. We proposed a chrome extension with more accuracy and precision when detecting phishing websites as it uses online databases in order to detect phishing websites. Meanwhile, it has a relatively low false positive rate. The extension shows a good ability to distinguish between phishing websites and non-phishing websites. By notifying users of phishing websites, our extension also provides them with the report of these sites on demand, which reduces the risk of users being scammed.

Chapter 9

Future Extension

We intend to integrate the IP address, email ... in the detection process in the future. Furthermore, we prefer to automate the detection process. In the future, we will build the phishing detection system as a scalable web service, integrating online learning so that new phishing attack patterns can be easily learned and improve our model accuracy with more information about the phishing attacks.

Bibliography

[1] Manoj P, ” Detection and Classification of Phising Website,” July 2021. [Online].Available: https://www.peertechzpublications.com/articles/TCSIT-6-140.php.

[2] Hongkai Chen and Mohammad Hossain, ” Developing a Google Chrome Extension for Detecting Phishing Emails,” 2021. [Online].Available: https://easychair.org/publications/paper/RJLM.

[3] Bhavya Shah, Karan Dharamshi, Mihir Patel, Dr.Vaishali Gaikwad, ” Chrome Extension for Detecting Phishing Websites,” March 2020. [Online].Available: https://www.irjet.net/archives/V7/i3/IRJET-V7I3590.pdf.

[4] Samuel Marchal, J´erˆome Franc¸ois, Radu State and Thomas Engel, ” PhishStorm: Detecting Phishing with StreamingAnalytics,” 2021. [Online].https://www.researchgate.net/publication/273169788 PhishStorm Detecting Phishing With StreamingAnalytics.

[5] Ms. Sophiya Shikalgar , Dr. S. D. Sawarkar , Mrs. Swati Narwane, ” Detection of URL based Phishing Attacks using Machine Learning,” November 2019. [Online].Available: https://www.ijert.org/detection-of-url-based-phishing-attacks-using-machine-learning.

[6] Atharva Deshpande , Omkar Pedamkar , Nachiket Chaudhary , Dr. Swapna Borde, ” Detection of Phishing Websites using Machine Learning,”May 2021. [Online].Available: https://www.ijert.org/detection-of-phishing-websites-using-machine-learning.

[7] Khan A, Vuong T, Gresty D and Ahamed Khan MKA, ” Phishing Detection on URLs Using Machine Learning,” December 2020. [Online].Available: https://crimsonpublishers.com/nrs/fulltext/NRS.000634.php.