WEB PHISHING DETECTION
(TEAM ID:PNT2022TMID34937)

PROJECT REPORT

Submitted by

VIJAYESH M (962819106048)
ABINESH M P (962819106002)
RAJKUMAR P (962819106031)
SANKARA NARAYANAN J (962819106037)
GUNA M P (962819106017)

In partial fulfilment for the award of degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

UNIVERSITY COLLEGE OF ENGINEERING , NAGERCOIL

ANNA UNIVERSITY-CHENNAI 600 025

NOVEMBER 2022

INDEX

1. INTRODUCTION

1.1 Project Overview

HookPhish is a website which is used to detect phishing sites to improve the customer's sense of safety whenever he/she attempts to provide any sensitive information to a site. Also, by which people won't access them which will reduce the revenue of malicious site owners. This application can be accessed online without paying instead, can be accessed via any browser of the customer's choice to detect any site with high accuracy. This system uses machine learning algorithm which implements classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy.

The design and implementation of a comprehensive web phishing detection system instils a cyber security culture which prevents the need for the deployment of targeted anti-phishing solutions in a corporate to meet industry's compliance obligations.

1.2 purpose

Web phishing is a threat in various aspects of security on the internet, which might involve scams and private information disclosure. Some of the common threats of web phishing are:

- Attempt to fraudulently solicit personal information from an individual or organization.
- Attempt to deliver malicious software by posing as a trustworthy organization or entity.
- Installing those malwares infects the data that cause a data breach or even nature's forces that takes down your company's data headquarters, disrupting access.

For this purpose, the objective of our project involves building an efficient and intelligent system to detect such websites by applying a machine-learning algorithm which implements classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy and as a result of which whenever a user makes a transaction online and makes payment through an e- banking website our system will use a data mining algorithm to detect whether the e-banking website is a phishing website or not.

2. LITERATURE SURVEY

2.1 Existing Problem

Phishing is a major problem, which uses both social engineering and technical deception to get users important information such asfinancial data, email, and other private information. phishing exploits human vulnerabilities. Malicious links will lead to a website than often steals login credentials or financial information that must be solved. These factors fall under the categories of address barbased features, domain-based features, HTML & JavaScript based features. Using these features, we build an intelligent system which can identify a phishing site with high accuracy and efficiency. It is also an open-source website which will be easily accessible to all users.

[1] A survey and classification of web phishing detection schemes Gaurav Varshney, Manoj Misra, Pradeep K ATREY: Security and Communication Phishing is a fraudulent technique that is used over the Internet to deceive users with the goal of extracting their personal information such as username, passwords, credit card, and bank account information. The key to phishing is deception. Phishing uses email spoofing as its initial medium for deceptive communication followed by spoofed

websites to obtain the needed information from the victims. Phishing was discovered in 1996, and today, it is one of the most severe cybercrimes faced by the Internet users. Researchers are working on the prevention, detection, and education of phishing attacks, but to date, there is no complete and accurate solution for thwarting them. This paper studies, analyzes, and classifies the most significant and novel strategies proposed in the area of phished website detection, and outlines their advantages and drawbacks. Furthermore, a detailed analysis of the latest schemes proposed by researchers in various subcategories is provided. The paper identifies advantages, drawbacks, and research gaps in the area of phishing website detection that can be worked upon in future research and developments. The analysis given in this paper will help academia and industries to identify the best anti-phishing technique. A survey and classification of web phishing detection schemes Gaurav Varshney, Manoj Misra, Pradeep K Atrey Security and Communication Networks 9 (18), 6266-6284, 2016 Phishing is a fraudulent technique that is used over the Internet to deceive users with the goal of extracting their personal information such as username, passwords, credit card, and bank account information. The key to phishing is deception. Phishing uses email spoofing as its initial medium for deceptive communication followed by spoofed websites to obtain the needed information from the victims. Phishing was discovered in 1996, and today, it is one of the most severe cybercrimes faced by the Internet users. Researchers are working on the prevention, detection, and education of phishing attacks, but to date, there is no complete and accurate solution for thwarting them. This paper studies, analyzes, and classifies the most significant and novel strategies proposed in the area of phished website detection, and outlines their advantages and drawbacks. Furthermore, a detailed analysis of the latest schemes proposed by researchers in various subcategories is provided. The paper identifies advantages, drawbacks, and research gaps in the area of phishing website detection that can be worked upon in future research and developments. The analysis given in this paper will help academia and industries to identify the best anti-phishing TECHNI

[2] Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future DIRECTIONS M Vijayalakshmi, S Mercy Shalinie, Ming Hour Yang, Raja Meenakshi U: Internet dragged more than half of the world's population into the cyber world. Unfortunately, with the increase in internet transactions, cybercrimes also increase rapidly. With the anonymous structure of the internet, attackers attempt to deceive the end-users through different forms namely phishing, malware, SQL injection, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Amongst them, phishing is the most deceiving attack, which exploits the vulnerabilities in the end-users. Phishing is often done through emails and malicious websites to lure the user by posing themselves as a trusted entity. Security experts have been proposing many anti- phishing techniques. Till today there is no single solution that is capable of mitigating all the vulnerabilities. A systematic review of current trends in web phishing detection techniques is carried out and a taxonomy of automated web phishing detection is presented. The objective of this study is to acknowledge the status of current research in automated web phishing detection and evaluate their performance.

This study also discusses the [3] research avenues for future investigation. Tutorial and critical analysis of phishing websites methods Rami M Mohammad, Fadi Thabtah, Lee MCCLUSKEY: Computer Science The Internet has become an essential component of our everyday social and financial activities. Internet is not important for individual users only but also for organizations, because organizations that offer online trading can achieve a competitive edge by serving worldwide clients. Internet facilitates reaching customers all over the globe without any market place restrictions and with effective use of e-commerce. As a result, the number of customers who rely on the Internet to perform procurements is increasing dramatically.

[4] Implementing a web browser with phishing detection techniques Aanchal Jain, Vineet Richariyaar Xiv preprint : Phishing is the combination

of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker. Phishing has become the most popular practice among the criminals of the Web. Phishing attacks are becoming more frequent and sophisticated. The impact of phishing is drastic and significant since it can involve the risk of identity theft and financial losses. Phishing scams have become a problem for online banking and e-commerce users. In this paper we propose a novel approach to detect phishing attacks. We implemented a prototype web browser which can be used as an agent and processes each arriving email for phishing attacks. Using email data collected over a period time we demonstrate data that our approach is able to detect more phishing attacks than existing schemes.

[5] Recent survey of various defense mechanisms against phishing ATTACKS Aakanksha Tewari, AK Jain, BB GUPTA: In the recent years, the phishing attack has become one of the most serious threats faced by Internet users, organizations, and service providers. In a phishing attack, the attacker tries to defraud Internet users and steal their personal information either by using spoofed emails or by using fake websites or both. Several approaches have been proposed in the literature for the detection and filtering of phishing attacks; however, the Internet community is still looking for a complete solution to secure the Internet from these attacks. This article discusses recent developments and protection mechanisms (i.e., detection and filtering) against a variety of phishing attacks (e.g., email phishing, website phishing, zero-day attacks). In addition, the strengths and weaknesses of these approaches is discussed. This article provides a better understanding of the phishing attack problem in the current solution space and also addresses the scope of future research to deal with such attacks efficiently.

[6]Implementing a web browser with phishing detection techniques Aanchal Jain, Vineet Richariyaar Xivpreprint : Phishing is the combination of social

engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker. Phishing has become the most popular practice among the criminals of the Web. Phishing attacks are becoming more frequent and sophisticated. The impact of phishing is drastic and significant since it can involve the risk of identity theft and financial losses. Phishing scams have become a problem for online banking and e-commerce users. In this paper we propose a novel approach to detect phishing attacks. We implemented a prototype web browser which can be used as an agent and processes each arriving email for phishing attacks. Using email data collected over a period time we demonstrate data that our approach is able to detect more phishing attacks than existing schemes.

[7] An integrated approach to detect phishing MAIL attacks: a case study R Suriya, K Saravanan, Arunkumar THANGAVELU: Phishing is a process of luring UNSUS in authentic looking email and messages for fraudulent purposes. Most preferred way that the phishers employ to lure victims is through a mass email, constructed to look like an authentic message from a well-known company. Phishing website has its own technical and social problem with each other and being a very complicate and complex issue to understand and analyze, to till date there exist no known single silver bullet to solve it entirely. Here an approach to create a resilient and effective method is proposed that uses fuzzy logic to quantify and qualify all the website phishing characteristics and factors in order to detect phishing websites to assess whether phishing activity is taking place or not. The approach visualizes the webpage in three layers of which the first layer, Domain Name checker, is fully based on characteristics of hyperlinks, the second, Code Script Checker which checks out for the tricks of the attackers in a way how they use JavaScript to hide information from user, and potentially launch sophisticated attacks, and the last layer of our approach, Page Content Checker, checks for phishing site based on its sub criteria. Finally if any of them (with regards to the true one) is higher than its

corresponding preset threshold then that webpage reportedas a phishing suspect.

2.2 References

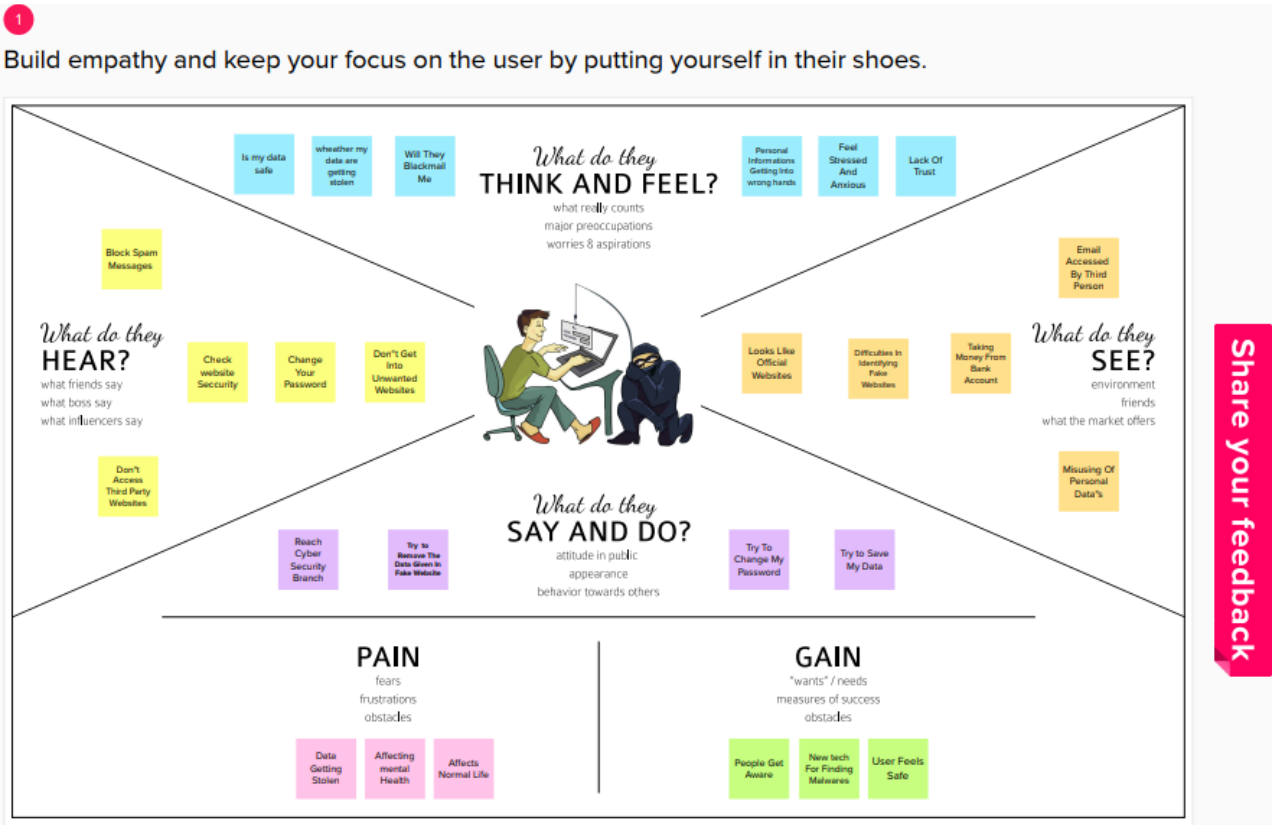
1)Gaurav Varshney, Manoj Misra, Pradeep K Atrey Security and Communication Networks 9 (18), 6266-6284, 2016
2)M Vijayalakshmi, S Mercy Shalinie, Ming Hour Yang, Raja Meenakshi U Iet Networks 9 (5), 235-246, 2020
3)Rami M Mohammad, Fadi Thabtah, Lee McCluskey Computer Science Review 17, 1-24, 2015 4)Aanchal Jain, Vineet Richariyaar Xiv preprint arXiv:1110.0360, 2011
5)R Suriya, K Saravanan, Arunkumar Thangavelu Proceedings of the 2nd International Conference on Security of Information and Networks, 193-12009
6)Aakanksha Tewari, AK Jain, BB Gupta Journal of Information Privacy and Security 12 (1), 3-13, 2016

2.3 Prblem Statement Definition

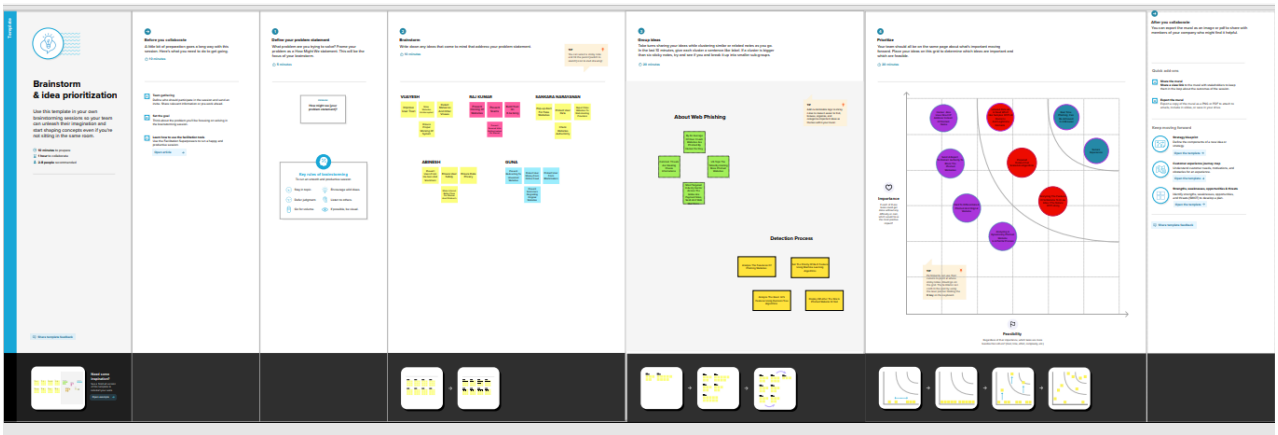
- Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity.
- It will lead to information disclosure and property damage.
- Large organizations may get trapped in different kinds of scams.

3. IDEATION & PROPOSED SOLUTION

3.1 Empathy Map



3.2 Ideation & Brainstorming



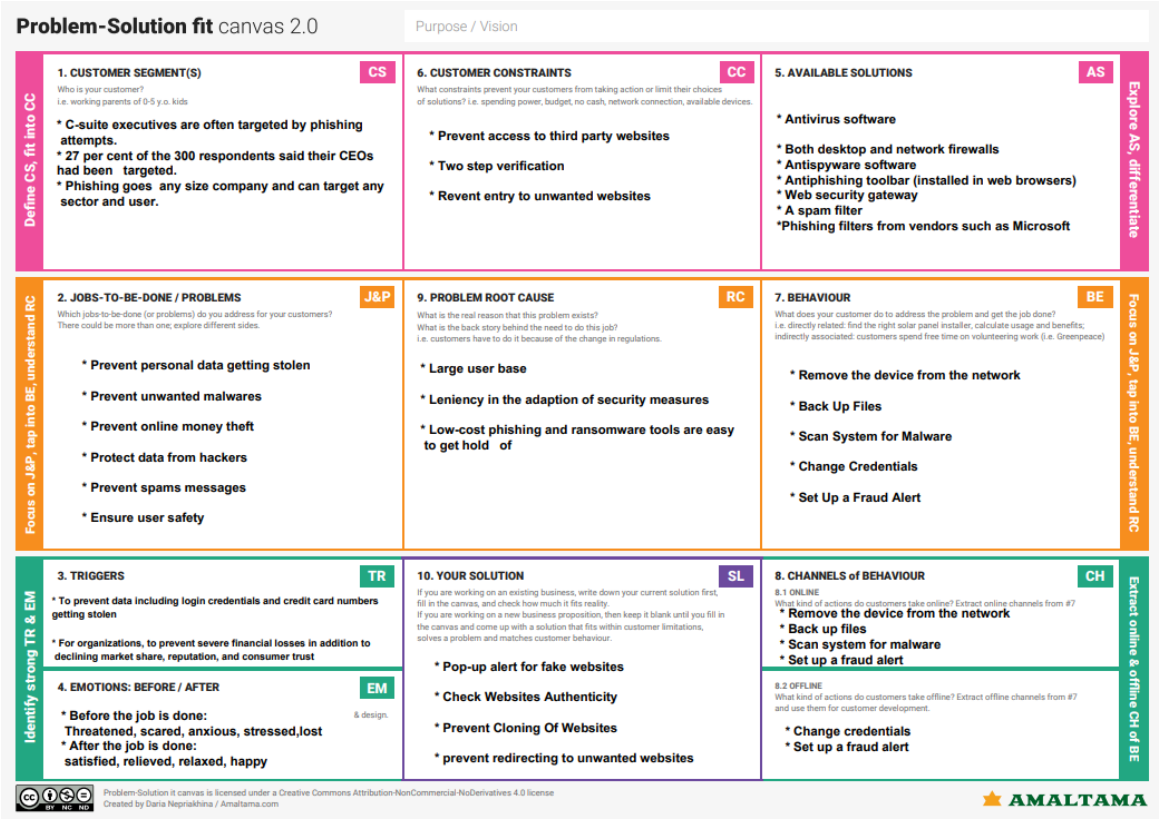
3.3 Proposed Solution

S.No	Parameter	Description
1.	Problem Statement (Problem to be solved)	Phishing is a major problem, which uses both social engineering and technical deception to get users important information such as financial data, email, and other private information. phishing exploits human vulnerabilities. Malicious links will lead to a website than often steals login credentials or financial information that must be solved
2.	Idea / Solution description	Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer. email filtering. Your first line defence against phishing is a secure email gateway.
3.	Novelty / Uniqueness	In recent times many researches have proposed the machine learning – based approach to solve phishing attacks. And web

		Address based evaluation, uniform based locators.
4.	Social Impact / Customer Satisfication	A customer Satisfaction survey is an instrument that helps Companies measure their customers level of satisfaction with their product / service. To alert the customers from preventing unwanted websites links and other things. Helps the customer to satisfied.
5.	Business Model (Revenue Model)	Nowadays, many anti-phishing systems are being developed to identify phishing contents in online communication systems. In this work, an enhanced machine leaning based predictive model is propose to improve the efficiency off anti-phishing schemes.

6.	Scalability of the Solution	The main ideas are to move the protection from end users towards the network provider and to employ the novel bad neighbourhood concept, in order to detect and isolate both phishing email senders and phishing servers.

3.4 Proposed Solution Fit



4. REQUIRMENT ANALYSIS

4.1 Functional Requirment

FR.No	Functional Requirment (Epic)	Sub Requirment(Story/ Sub-Task)
FR-1	Detect and predict phishing websites	Phishing website can be detected based on some important characteristics like URL and domain identity, security and criteria in the final phishing detection rate.
FR-2	Identify Fraudulent URL	A fraudulent domain or phishing domain is an URL scheme that looks suspicious. Ex: misspelled, A combination of valid and fraudulent URL , Poor rank in Alexa top 1 million websites. These characteristics helps us to distinguish it from valid URL.
FR-3	Building a data tree	We can use a Machine Learning algorithm, such as a decision tree classifier to help us to decide whether an URL is valid or not.
FR-4	Train the Model	In machine learning model , the dataset is spilted into testing data and training data. It is always better use decision

		tree because it is straight forward and generally gives the best results when trying to classify data.
FR-5	Evaluate the model	After training it is evaluated to check how it works .It helps to know the accuracy level of dectecting phished domains.
FR-6	Identify false positives & false negatives	The results of any decision tree may contain both false positives(URLs that are actually valid,but our model indicates are not) and false negatives(URLs that are actually bad, but our model indicates are fine). This should be resolved.

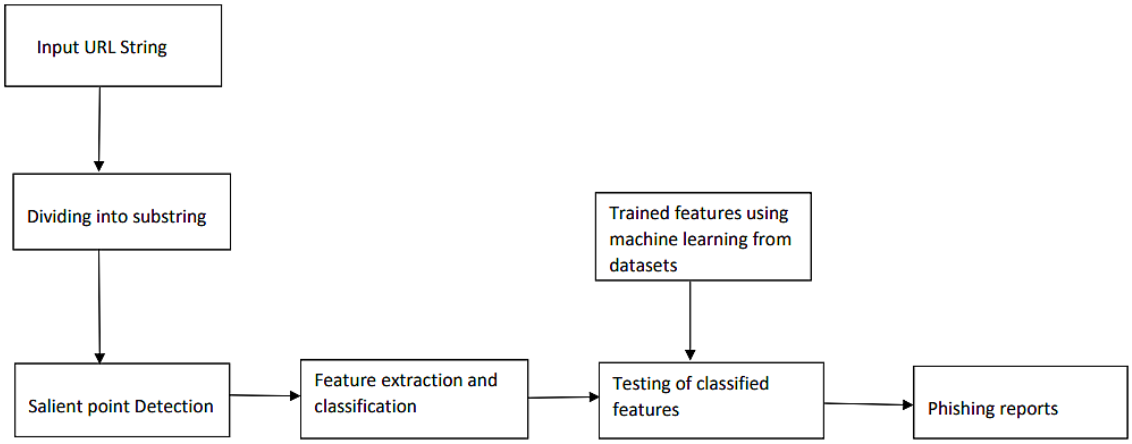
4.2 Non-Functional Requirments

FR.No	Non-Functional Requirments (Epic)	Description
NFR-1	Usability	It should be user friendly. It should constantly detect the phished domains and report to the user.
NFR-2	Reliability	It should be trustworthy and it should have more accuracy in detecting

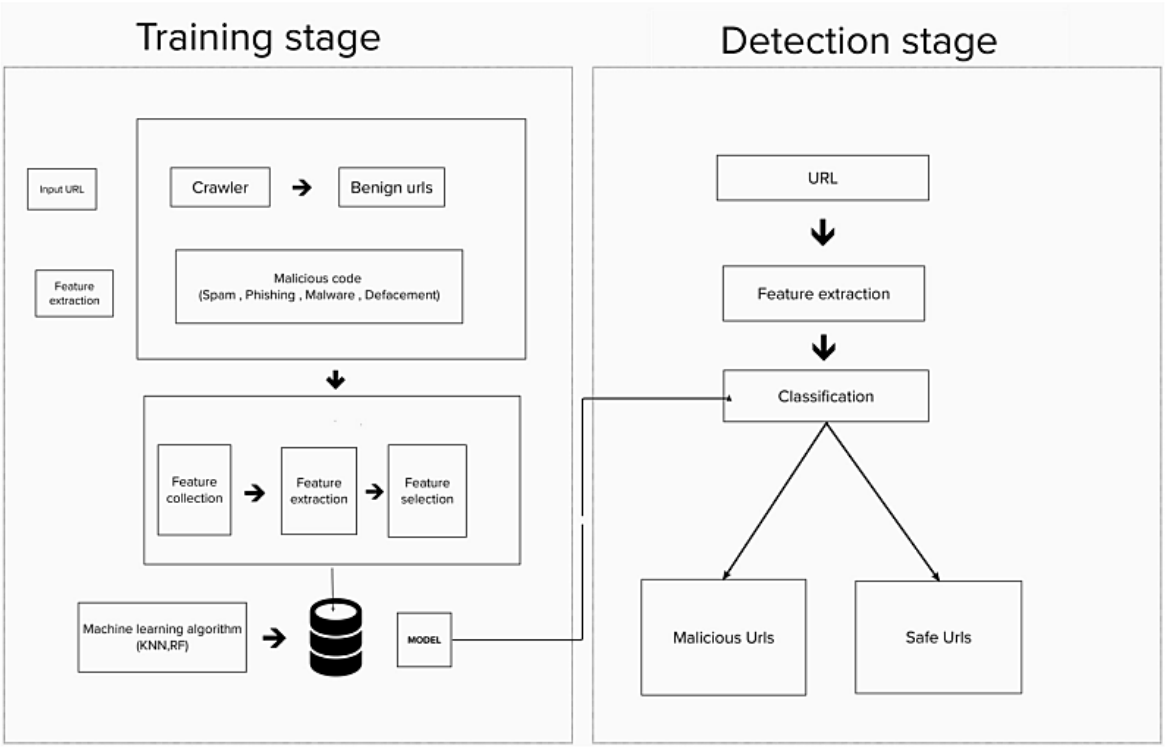
		the phished domains.
NFR-3	Scalability	It should have low maintenance cost,high user experience and should have high agility
NFR-4	Performance	The performance should be good and more accurate. It should work ceaselessly.

5. PROJECT DESIGN

5.1 Data Flow Diagrams



5.2 Solution & Technical Architecture



5.3 User Stories

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Csuite executive, CEO, mobile user,	Detect and predict phishing websites	USN-1	As a user, I to detect phishing websites	I can protect my personal data getting stolen	High	Sprint-1

web user)						
Customer (Csuite executive, CEO, mobile user, web user)	Identify Fraudulent URL	USN-2	As a user, I need to identify the URL that looks suspicious	I can protect my data from hackers	High	Sprint-2
Customer (Csuite executive, CEO, mobile user, web user)	Identify Fraudulent URL	USN-3	As a user, I need to identify whether a URL is valid or not	I can prevent online money theft	High	Sprint-2
Customer (Csuite executive, CEO, mobile user, web user)	Identification of accuracy level of of detected phished domains	USN-4	As a user, I need to know the accuracy level of detected phished domains	I can ensure safety	Medium	Sprint-3
Custom	Identify	USN-5	As a	I can	Low	Sprint-4

er (Csuite executive, CEO, mobile user, web user)	false positives and false negatives		user, I need to identify false positives and false negatives	prevent unwanted malware		

6. PROJECT PLANNING & SCHEDULING

6.1 Sprint Planning & Estimation

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	Home page	USN-1	As a user, first have an good impression upon the homepage and I can explore and view	20	Medium	Vijayesh, Sankaranarayanan

			the funtioning of the website			
Sprint-2	Registration	USN-2	As a user, I will receive confirmation email once I have registered for the application	10	High	Abinesh, Rajkumar
Sprint-2		USN-3	As a user, I can register for the application through google	10	Medium	Guna
Sprint-2	Login	USN-4	As a user, I can register	10	Medium	Abinesh

			for the application through Gmail			
Sprint-2		USN-5	As a user, I can log into the application by entering email & password		low	Rajkumar, Vijayesh
Sprint-3	Dashboard	USN-6	User would go through the funtionalities and the uses of the website	5	low	Sankaranarayanan
Sprint-3	Prediction	USN-7	User would able to analyze whether the website	15	High	Guna, Abinesh

			is a real website or a phishing website			
Sprint-3	Result page	USN-8	User can able to see the results web page of the analysis		low	Vijayesh
Sprint-4	User query	USN-9	User can able to reply any queries regarding the results of the analysis	10	High	Sankaranarayanan, Rajkumar

sprint-4	contact	USN-10	User can able to contact the developer directly for any other queries	10	Medium	Vijayesh

6.2 Sprint Delivery Schedule

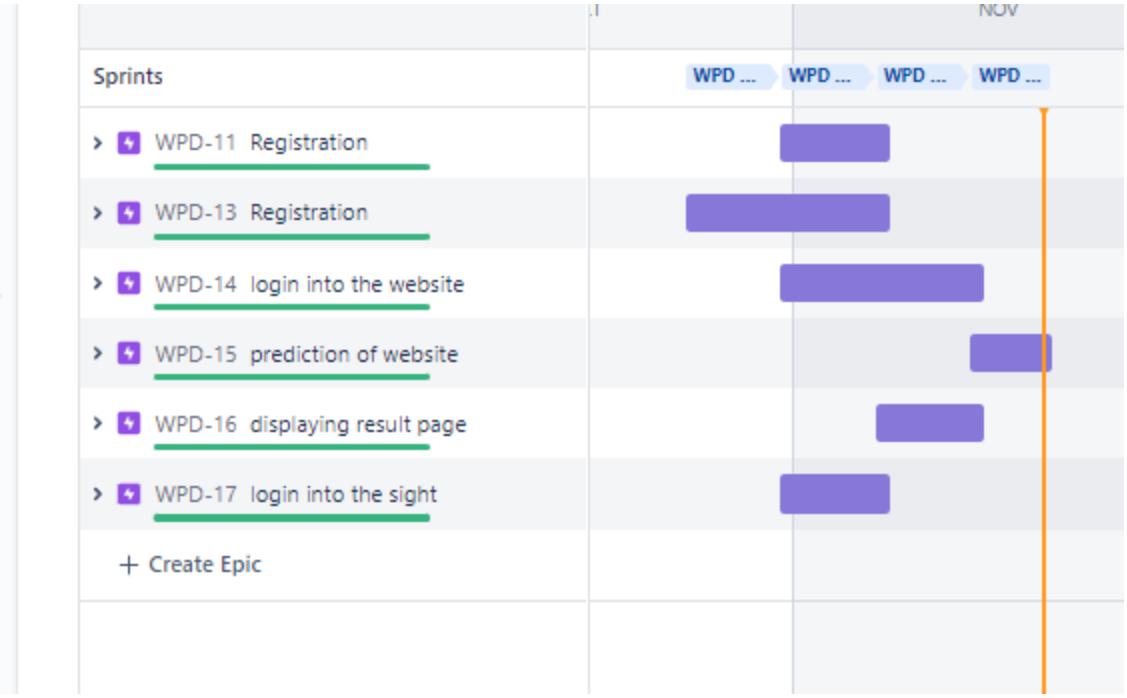
TITLE	DESCRIPTION	COMPLETION DATE
Literature survey	Literature survey on the selected project & gathering information by referring the, technical papers, research publications etc	Aug 29, 2022 - Sep 3, 2022
Empathy Map	Prepare Empathy Map Canvas to capture the user Pains & Gains, Prepare list of problem statements	Sep 5, 2022 - Sep 10, 2022
Problem Statement	Prepare the problem statement document	Sep 5, 2022 - Sep 10, 2022
Brainstorming Idea Generation Prioritization	List them by organizing the brainstorming session and prioritize the top 3 ideas based on the feasibility & importance.	Sep 12, 2022 - Sep 17, 2022
Problem Solution Fit	Prepare problem - solution fit document.	Sep 26, 2022 - Oct 1, 2022
Proposed Solution	Prepare the proposed solution document, which includes the novelty, feasibility of idea, business model,	Sep 19, 2022 - Sep 24, 2022

	social impact, scalability of solution, etc.	
Solution Architecture	Prepare a solution architecture document.	Sep 19, 2022 - Sep 24, 2022

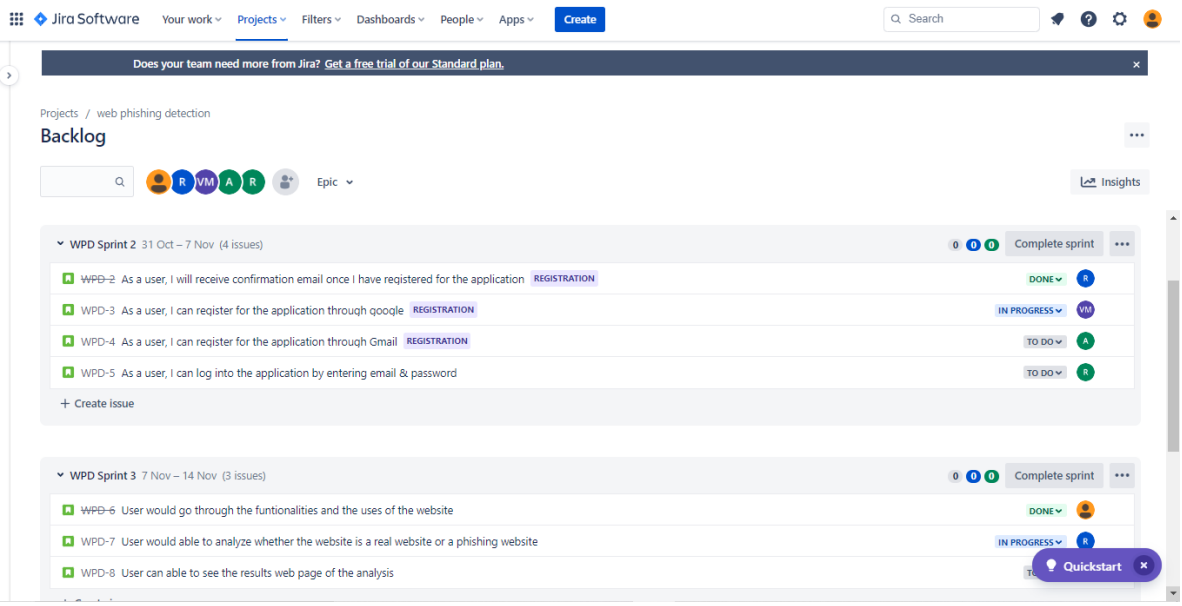
Functional Requirements	Prepare the functional requirement document.	Oct 10, 2022 - Oct 15, 2022
Customer Journey Map	Prepare the customer journey maps to understand the user interactions & experiences with the application (entry to exit).	Oct 3, 2022 - Oct 8, 2022
Data Flow Diagrams and User Stories	Draw the data flow diagrams and submit for review.	Oct 10, 2022 - Oct 15, 2022
Technology Stack	Prepare the technology architecture diagram	Oct 10, 2022 - Oct 15, 2022

6.3 Reports from JIRA

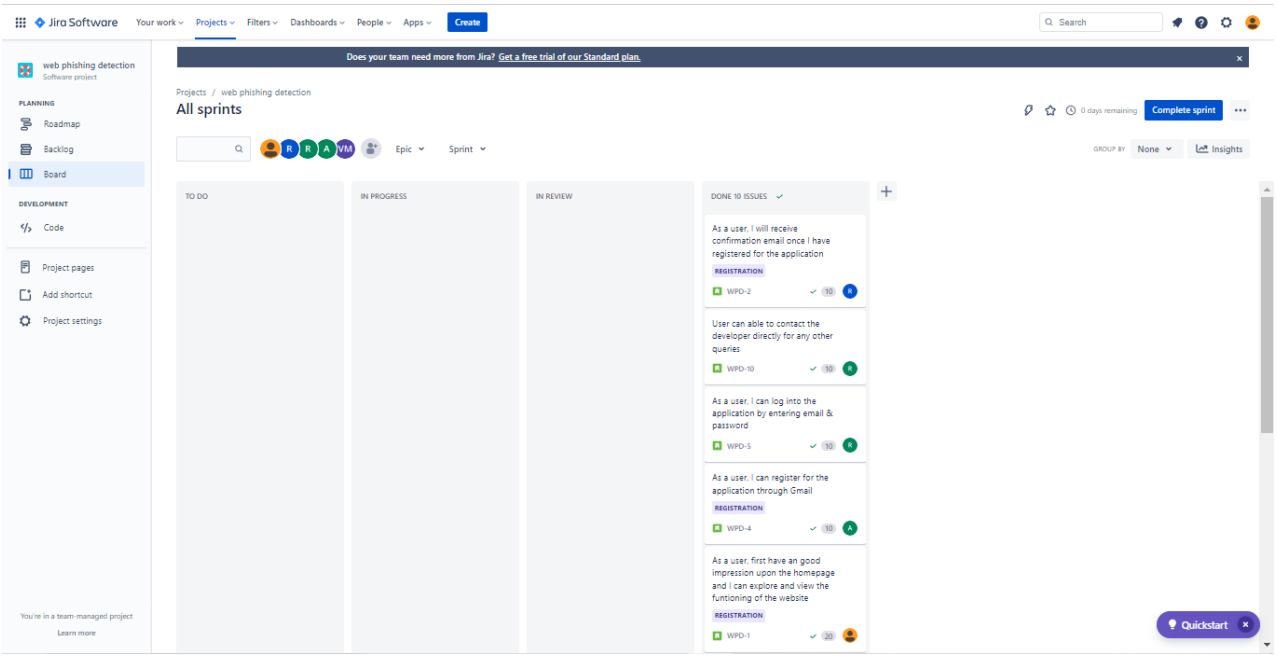
ROAD MAP IN JIRA



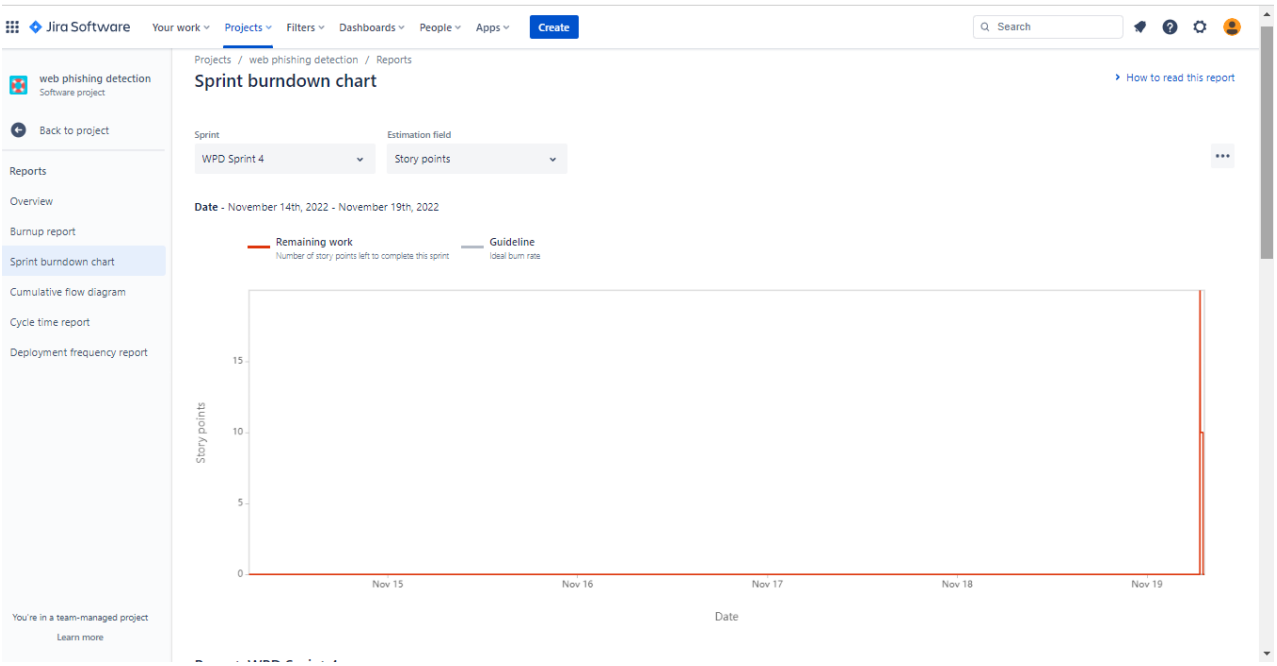
BACKLOG IN JIRA



BOARD IN JIRA



BURNDOWN CHART



7. CODING & SOLUTIONING

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
     <meta name="description" content="This website is develop for identify the safety of url.">
          <meta name="keywords" content="phishing url,phishing,cyber security,machine learning,classifier,python">

   <!-- BootStrap -->
                                                <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
                                                integrity="sha384-9aIt2nRpC12Uk9gS9baDl411NQApFmC26EwAOH8WgZl5MYYxFfc+NcPb1dKGj7Sk" crossorigin="anonymous">

   <link href="static/styles.css" rel="stylesheet">
   <title>URL detection</title>
   <link rel="stylesheet" href="style.css">

</head>

<body>

<div class=" container">
   <div class="row">
```

```
<div class="form col-md" id="form1">
    <h2>PHISHING SITE DETECTION TOOL</h2>

    <br>
    <form action="/" method ="post">
                <input type="text" class="form__input" name ='url' id="url" placeholder="Enter URL" required="" />
        <label for="url" class="form__label">URL</label>
            <a href="show.html"><button class="button" role="button" >Check here</button></a>
    </form>

  </div>

  <div class="col-md" id="form2">

    <br>
    <h6 class = "right "><a href= {{ url }} target="_blank">{{ url }}</a></h6>

    <br>
    <h3 id="prediction"></h3>
                <button class="button2" id="button2" role="button" onclick="window.open('{{url}}')" target="_blank" >Still want to Continue</button>
                <button class="button1" id="button1" role="button" onclick="window.open('{{url}}')" target="_blank">Continue</button>
  </div>
</div>
<br>
<h1>Project Team ID : PNT2022TMID34937</h1>
```

```
</div>

    <!-- JavaScript -->
    <script src="https://code.jquery.com/jquery-3.5.1.slim.min.js"
                                                                integrity="sha384-
DfXdz2htPH0lsSSs5nCTpuj/zy4C+OGpamoFVy38MVBnE+IbbVYUew+OrCXa
Rkfj"
        crossorigin="anonymous"></script>
                                                                <script
src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"
                                                                integrity="sha384-
Q6E9RHvbIyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfoo
Ao"
        crossorigin="anonymous"></script>
                                                                <script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.j
s"
                                                                integrity="sha384-
OgVRvuATP1z7JjHLkuOU7Xw704+h835Lr+6QL9UvYjZE3Ipu6Tp75j7Bh/kR0
JKI"
        crossorigin="anonymous"></script>


    <script>

            let x = '{{xx}}';
            let num = x*100;
            if (0<=x && x<0.50){
                num = 100-num;
            }
            let txtx = num.toString();
            if(x<=1 && x>=0.50){
```

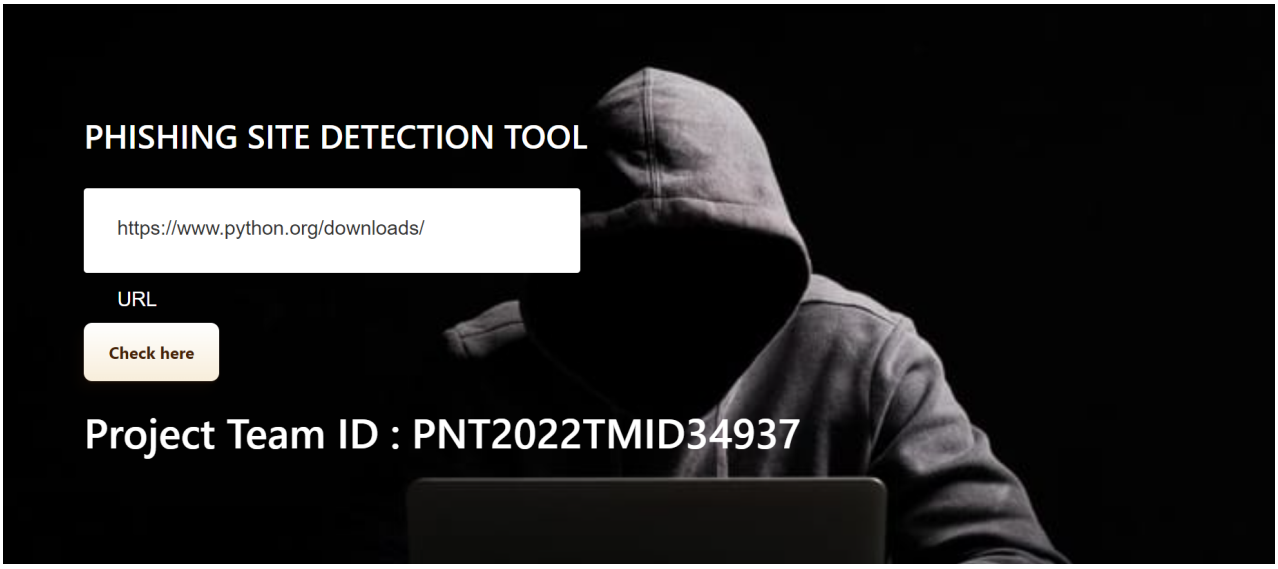
```
            var label = "Website is "+txtx +"% safe to use...";
            document.getElementById("prediction").innerHTML = label;
            document.getElementById("button1").style.display="block";
        }
        else if (0<=x && x<0.50){
             var label = "Website is "+txtx +"% unsafe to use..."
            document.getElementById("prediction").innerHTML = label ;
            document.getElementById("button2").style.display="block";
        }

    </script>

</body>

</html>
```

SOLUTION



8. TESTING

8.1 Test Cases Report

Date	19-Nov-22
Team ID	PNT2022TMID34937
Project Name	Project - Web Phishing Detection
Maximum Marks	4 marks

Test case ID	Feature Type	Component	Test Scenario	Pre-Requisite	Steps To Execute	Test Data	Expected Result	Actual Result	Status	Comments	TC for Automation(Y/N)	BUG ID	Executed By
strationPage_TC_	UI	Login page	Verify user is able to see the submit button		1.Open the web app 2.verify username test box is displayed 3.Verify password textbox is displayed 4.Verify submit button is displayed	Username: webphish@gmail.com password: Testing123	Application should show submit button	Working as expected	Pass		No		
strationPage_TC_	Functional	Login page	Verify user is able to register to the application using valid credentials		1.Enter valid username in username test box 2.Enter valid email in email textbox 3.Enter valid password in password textbox 4.Click submit	Username: webphish@gmail.com password: Testing123	User should navigate to next page	Working as expected	Pass		No		

8.2 User Acceptance Testing

1. Purpose of Document

The purpose of this document is to briefly explain the test coverage and open issues of the [ProductName] project at the time of the release to User Acceptance Testing (UAT).

2. Defect Analysis

This report shows the number of resolved or closed bugs at each severity level, and how they were resolved

Resolution	Severity 1	Severity 2	Severity 3	Severity 4	Subtotal
By Design	10	4	2	3	20
Duplicate	1	0	3	0	4
External	2	3	0	1	6
Fixed	11	2	4	20	37
Not Reproduced	0	0	1	0	1
Skipped	0	0	1	1	2
Won't Fix	0	5	2	1	8
Totals	24	14	13	26	77

3. Test Case Analysis

This report shows the number of test cases that have passed, failed, and untested

Section	Total Cases	Not Tested	Fail	Pass
Home Page	7	0	0	7
Registration	8	0	0	8
Login	10	0	0	10
Dashboard	5	0	0	5
Prediction	5	0	0	5
Result Page	3	0	0	3
User Query	4	0	0	4
Contact	2	0	0	2
Final Report Output	10	0	0	10
Version Control	2	0	0	2

9. RESULTS

9.1Performance Metrics

1. METRICS:
CLASSIFICATION REPORT:

```
In [52]: #computing the classification report of the model

         print(metrics.classification_report(y_test, y_test_gbc))
```

	precision	recall	f1-score	support
-1	0.99	0.96	0.97	976
1	0.97	0.99	0.98	1235
accuracy			0.97	2211
macro avg	0.98	0.97	0.97	2211
weighted avg	0.97	0.97	0.97	2211

10. ADVANTAGES & DISADVANTAGES

10.1 ADVANTAGES

- ★ Prevent Personal Data Getting Stolen
- ★ Protect Data from Hackers
- ★ Protect Spam Messages

- ★ Prevent Online Money Theft

10.2 DISADVANTAGES

- ★ Time consuming
- ★ Huge number of features
- ★ Consuming Memory

11. CONCLUSION

We can conclude that this detection software can protect innocent users from hackers. This helps to resist phishers from acquiring sensitive informations such as user name, password and bank account details.

12. FUTURE SCOPE

In future hybrid technology will be implemented to detect phishing websites more accurately, for which random forest algorithm of machine learning technology and blacklist method will be used

13. APPENDIX

13.1 SOURCE CODE

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta http-equiv="X-UA-Compatible" content="IE=edge">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
     <meta name="description" content="This website is develop for identify the safety of url.">
          <meta name="keywords" content="phishing url,phishing,cyber security,machine learning,classifier,python">

   <!-- BootStrap -->
                                                <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
                                                integrity="sha384-9aIt2nRpC12Uk9gS9baDl411NQApFmC26EwAOH8WgZl5MYYxFfc+NcPb1dKGj7Sk" crossorigin="anonymous">

   <link href="static/styles.css" rel="stylesheet">
   <title>URL detection</title>
   <link rel="stylesheet" href="style.css">

</head>

<body>
```

```
<div class=" container">
   <div class="row">
      <div class="form col-md" id="form1">
         <h2>PHISHING SITE DETECTION TOOL</h2>

         <br>
         <form action="/" method ="post">
                        <input  type="text"  class="form__input"  name  ='url'  id="url"
placeholder="Enter URL" required="" />
            <label for="url" class="form__label">URL</label>
               <a href="show.html"><button class="button" role="button" >Check
here</button></a>
         </form>

   </div>

   <div class="col-md" id="form2">

      <br>
      <h6 class = "right "><a href= {{ url }} target="_blank">{{ url }}</a></h6>

      <br>
      <h3 id="prediction"></h3>
                        <button    class="button2"    id="button2"    role="button"
onclick="window.open('{{url}}')"       target="_blank"       >Still       want       to
Continue</button>
                        <button    class="button1"    id="button1"    role="button"
onclick="window.open('{{url}}')" target="_blank">Continue</button>
   </div>
</div>
<br>
<h1>Project Team ID : PNT2022TMID34937</h1>
```

```
</div>

    <!-- JavaScript -->
    <script src="https://code.jquery.com/jquery-3.5.1.slim.min.js"
                                                                integrity="sha384-
DfXdz2htPH0lsSSs5nCTpuj/zy4C+OGpamoFVy38MVBnE+IbbVYUew+OrCXa
Rkfj"
        crossorigin="anonymous"></script>
                                                                <script
src="https://cdn.jsdelivr.net/npm/popper.js@1.16.0/dist/umd/popper.min.js"
                                                                integrity="sha384-
Q6E9RHvbIyZFJoft+2mJbHaEWldlvI9IOYy5n3zV9zzTtmI3UksdQRVvoxMfoo
Ao"
        crossorigin="anonymous"></script>
                                                                <script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/js/bootstrap.min.j
s"
                                                                integrity="sha384-
OgVRvuATP1z7JjHLkuOU7Xw704+h835Lr+6QL9UvYjZE3Ipu6Tp75j7Bh/kR0
JKI"
        crossorigin="anonymous"></script>


    <script>

            let x = '{{xx}}';
            let num = x*100;
            if (0<=x && x<0.50){
                num = 100-num;
            }
            let txtx = num.toString();
```

```
        if(x<=1 && x>=0.50){
            var label = "Website is "+txtx +"% safe to use...";
            document.getElementById("prediction").innerHTML = label;
            document.getElementById("button1").style.display="block";
        }
        else if (0<=x && x<0.50){
            var label = "Website is "+txtx +"% unsafe to use..."
            document.getElementById("prediction").innerHTML = label ;
            document.getElementById("button2").style.display="block";
        }

    </script>

</body>

</html>
```

13.2 GitHub & Project Demo Link