

WEB PHISHING DETECTION

Problem Statement

There are a number of users who purchase products online and make payments through e-banking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons. This type of e-banking website is known as a phishing website. Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet.

Common threats of web phishing:

- 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.

This project mainly focuses on applying a machine-learning algorithm to detect Phishing websites.

Literature Survey On The Selected Project & Information Gathering

In this activity you are expected to gather/collect the relevant information on project use case, refer the existing solutions, technical papers, research publications etc.

H. Huang et al., (2009) proposed the 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.

S. Marchal et al., (2017) proposed this technique to differentiate Phishing website depends on the examination of authentic site server log knowledge. An application

Off-the- Hook application or identification of phishing website. Free, displays a couple of outstanding properties together with high preciseness, whole autonomy, and nice language-freedom, speed of selection, flexibility to dynamic phish and flexibility to advancement in phishing ways.

Mustafa Aydin et al. proposed a classification algorithm for phishing website detection by extracting websites' URL features and analyzing subset based feature selection methods. It implements feature extraction and selection methods for the detection of phishing websites. The extracted features about the URL of the pages and composed feature matrix are categorized into five different analyses as Alpha-numeric Character Analysis, Keyword Analysis, Security Analysis, Domain Identity Analysis and Rank Based Analysis. Most of these features are the textual properties of the URL itself and others based on third parties services.

Samuel Marchal et al. presents PhishStorm, an automated phishing detection system that can analyze in real time any URL in order to identify potential phishing sites. Phish storm is proposed as an automated real-time URL phishingness rating system to protect users against phishing content. PhishStorm provides phishingness score for URL and can act as a Website reputation rating system.

Fadi Thabtah et al. experimentally compared large numbers of ML techniques on real phishing datasets and with respect to different metrics. The purpose of the comparison is to reveal the advantages and disadvantages of ML predictive models and to show their actual performance when it comes to phishing attacks. The experimental results show that Covering approach models are more appropriate as anti- phishing solutions.

Muhemmet Baykara et al. proposed an application which is known as Anti Phishing Simulator, it gives information about the detection problem of phishing and how to detect phishing emails. Spam emails are added to the database by Bayesian algorithm.

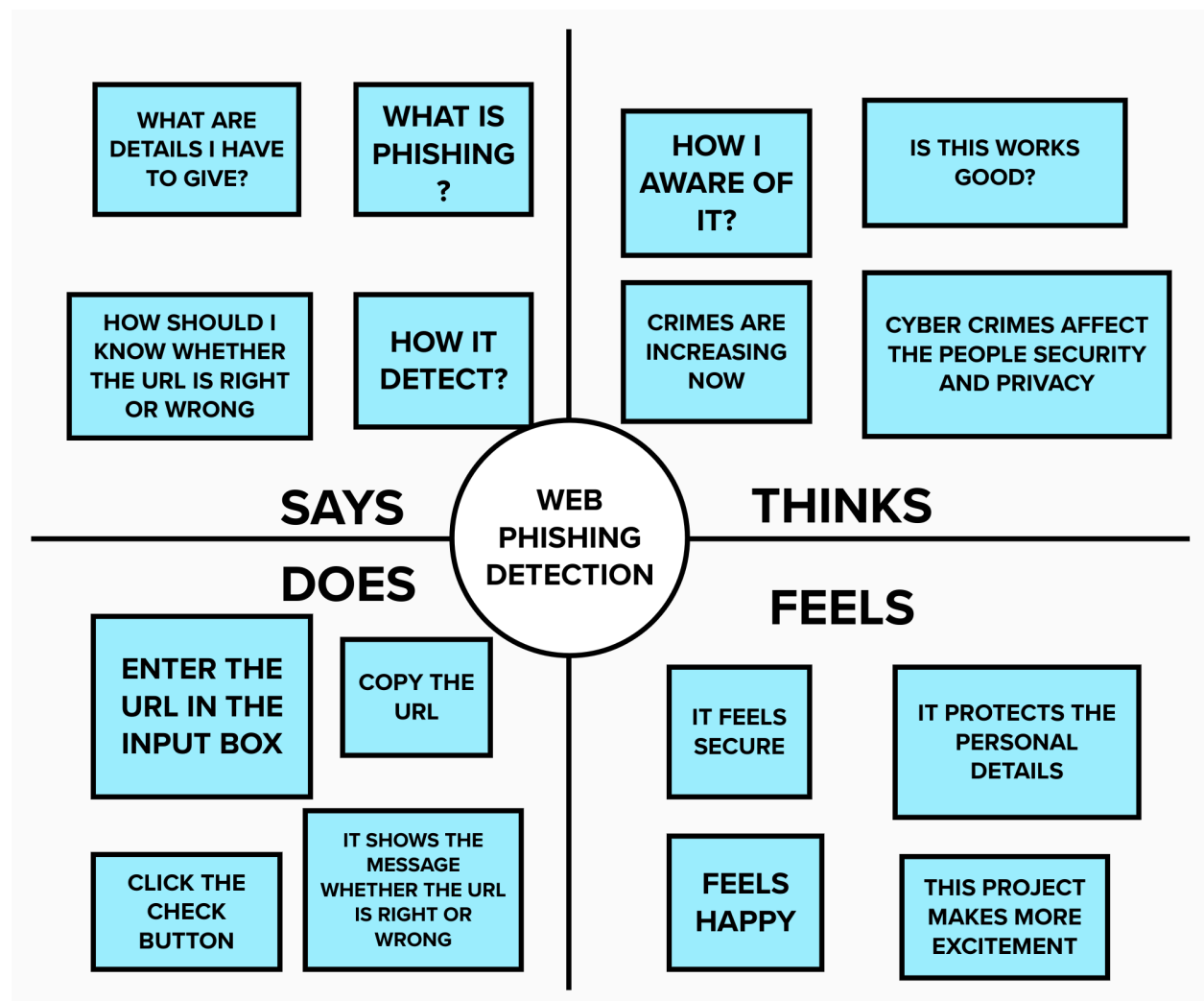
Wang et al., Jain and Gupta and Han et al. use white list-based method for the detection of suspected URL. Blacklist-based methods are widely used in openly available anti-phishing toolbars, such as Google safe browsing, which maintains a blacklist of URLs and provides warnings to users once a URL is considered as phishing. Prakash et al. proposed a technique to predict phishing URLs called Phishnet. In this technique, phishing URLs are identified from the existing

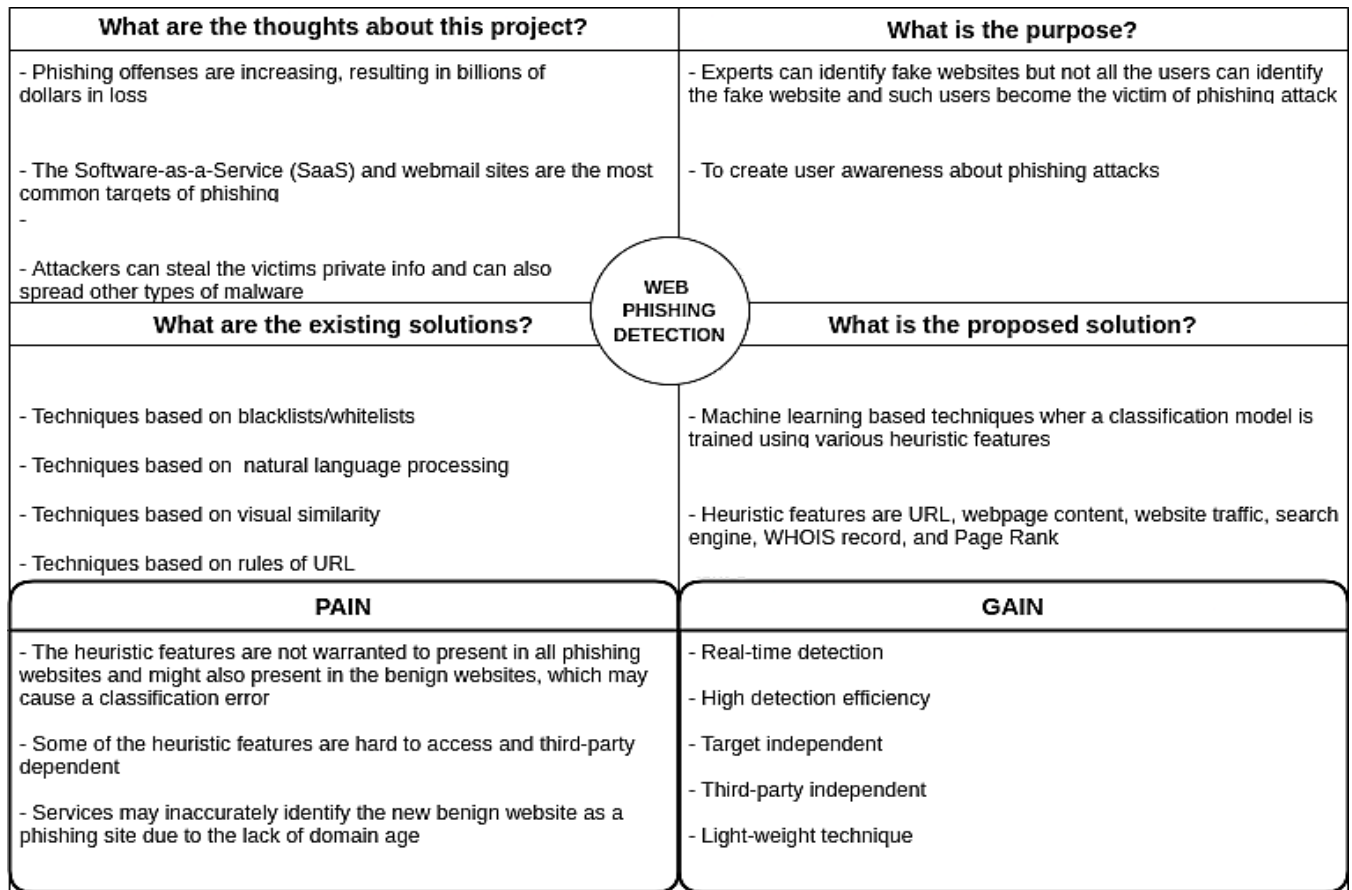
blacklisted URLs using the directory structure, equivalent IP address, and brand name.

Felegyhazi et al. developed a method that compares the domain name and name server information of new suspicious URLs to the information of blacklisted URLs for the classification process. Sheng et al. demonstrated that a forged domain was added to the blacklist after a considerable amount of time, and approximately 50–80% of the forged domains were appended after the attack was carried out.

Prepare Empathy Map

In this activity you are expected to prepare the empathy map canvas to capture the user Pains & Gains, Prepare list of problem statements.





Goal

In order to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. We implemented classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy. The e-banking phishing website can be detected based on some important characteristics like URL and domain identity, and security and encryption criteria in the final phishing detection rate. Once a user makes a transaction online when he 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.

Ideation

In this activity you are expected to list the ideas (atleast 4 per each team member) by organizing the brainstorming session and prioritize the top 3 ideas based on the feasibility & importance.

1. Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer.
2. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.
3. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.
4. The website may be used to hack and misuse others detail so to protect that Then kids nowadays are learning from online so to protect them from facing any unpleasant or bad activity. So create a extension in google which will detect the fake websites.
5. Every time you click on a link, look at the browser bar and see if matches exactly the one you would type in to go to your account.
6. All members of your executive and management team are vulnerable. If a phishing scammer acquires the email credentials of high-profile leadership, it's likely they'll target anyone they can using that very email address.
7. Almost all spam messages are malicious emails sent by unknown sources. These sources could be hackers who aim to hack into the computers of their victims.
8. Never respond to spam messages because through this, the spammer will know that the email address is active and thus, it increases the chance of your email to be constantly targeted by the spammer.
9. Do not use your personal or business email address when registering in any online contest or service such as applications, deal updates, etc. Many spammers watch these groups or emailing lists to harvest new email addresses.
10. In fact, many unsuspecting users have been dupped via text message phishing (also known as smishing) and through social media.

11. The threat of malicious messages luring users to click on a link, open a malicious webpage, download malware or provide credentials on a spoofed site proves that threat actors are getting continuously creative in their methods to hijack your assets and steal your credentials.
12. While these attacks use electronic written words to lure a user into their scam and some of the messages may be hosted in social media, a new form of messaging attacks are emerging via other cloud and SaaS (software as a service) platforms that provide in-application messaging between users.

TOP 4:

1. We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different web designing languages which include HTML, CSS, Javascript and Python.
2. It must be noted that the website is created for all users, hence it must be easy to operate with and user-friendly.
3. The website will show information regarding the services provided by us. It also contains information regarding ill- practices occurring in today's technological world.
4. The website will be created with an opinion such that people are not only able to distinguish between legitimate and fraudulent website, but also become aware of the mal-practices occurring in current world. They can stay away from the people trying to exploit one's personal information, like email address, password, debit card numbers, credit card details, CVV, bank account numbers.

PROPOSED SOLUTION:-

Problem Statement (Problem to be solved)

There are a number of users who purchase products online and make payments through ebanking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details, etc., often for malicious reasons. This type of ebanking website is known as a phishing website. Web service is one of the key communications software services for the Internet.

Idea / Solution description

Anti-spyware and firewall settings should be used to prevent phishing attacks and users should protect your mobile phone by setting software to update automatically. The website will be created with an opinion such that people are not only able to distinguish between legitimate and fraudulent websites, but also become aware of the mal-practices occurring in the current world.

Novelty / Uniqueness

The website designed will be user friendly in means for any age. Easy to detect the fraudulent website and protect the sensitive credential information.

Social Impact / Customer Satisfaction

Feel protected by using the website as the business-related credentials will be safe. Parents can be relaxed when kids explore educational website as the fraudulent website will be detected by our website.

Business Model (Revenue Model)

This can be an efficient way to help banking sector as it secures the legitimate website from other malware that are set by hacker.

Scalability of the Solution

We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different

web designing languages which include HTML, CSS, JavaScript and Python. This website is more useful to the user and it is user friendly also.

PROPOSED SOLUTION FIT:-

1. CUSTOMER SEGMENT(S)

Who is your customer? i.e. working parents of 0-5 y.o. kids

Protect yourself and your family against malicious websites with the platform for free.

With the platform, protecting your staff, data, brand, and your customer from malicious websites has never been easier.

Proactively protect multiple customers against malicious websites at once with all-in-one platform.

The platform can be used for government embeds to provide 100% security and privacy.

2. JOBS-TO-BE-DONE / PROBLEMS

Which jobs-to-be-done (or problems) do you address for your customers? There could be more than one; explore different sides.

The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions. Phishers use the websites which are visually and semantically similar to those real websites. As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing.

3. TRIGGERS

What triggers customers to act? i.e. seeing their neighbour installing solar panels, reading about a more efficient solution in the news.

Your users lack security awareness.

Criminals are (unsurprisingly) following the money.

You're not performing sufficient due diligence.

Low-cost phishing and ransomware tools are easy to get hold of.

Malware is becoming more sophisticated.

4. EMOTIONS: BEFORE / AFTER

How do customers feel when they face a problem or a job and afterwards? i.e. lost, insecure > confident, in control - use it in your communication strategy & design.

Greed- Clicking on fake successful messages.

Urgency-Hackers use fake security alerts with exclamation marks.

Helpfulness-Hackers and cybercriminals use major tragedies to appeal for help but they are only helping themselves.

Fear- Emails that spread fear and phishing links go hand in hand.

5. AVAILABLE SOLUTIONS

Which solutions are available to the customers when they face the problem or need to get the job done? What have they tried in the past? What pros & cons do these solutions have? i.e. pen and paper is an alternative to digital notetaking

Legitimate websites prevent web scraping by several techniques in respect to obfuscation using CSS sprites to display important data, replacing text with images.

Spam filtering techniques are used to identify unsolicited emails before the user reads or clicks the link.

When users visit a phishing web page that looks like a legitimate website, many people do not remember the legitimate website's domain name, particularly for some start-ups or unknown companies, so users cannot recognize the phishing website based on the URL. Some web browsers integrate a security component to detect phishing or malware sites, such as Chrome, which will display warning messages when one visits an unsafe webpage.

When the website detects that the IP address and device information of the user who is logging in does not match the commonly used information, it is necessary to verify the authenticity of the user.

6. CUSTOMER CONSTRAINTS

What constraints prevent your customers from taking action or limit their choices of solutions? i.e. spending power, budget, no cash, network connection, available devices.

The limitations of the web phishing detection approaches are explored by means of detection time, detection rate, and storage complexity to verify the level of robustness against the phishing attack.

Thus most of the recent web phishing detection approaches lag in feature selection mechanism as they use handcrafted features to detect the attack.

7. BEHAVIOUR

What does your customer do to address the problem and get the job done? i.e. directly related: find the right solar panel installer, calculate usage and benefits; indirectly associated: customers spend free time on volunteering work (i.e. Greenpeace)

Customers should take a "trust no one" approach when opening email.

Check and verify the "From" address of the email.

By carefully reading the email copy, users can typically spot something that seems “off” including:

An email with an “urgent” request or An email offering the user something that’s “too good to be true”.

Check grammar and spelling. Poor grammar and misspelled words in an email can be red flags.

Be wary of generic salutations in an email. Legitimate companies, especially those with which you have accounts or have done business typically will address you by name versus by a generic greeting,

Encourage your clients to look for any unusual or odd requests in their emails. Most fraudulent emails contain a request to respond to the email or click a link in it.

Avoid clicking links or attachments in emails from unfamiliar sources.

8. CHANNELS of BEHAVIOUR

8.1 ONLINE What kind of actions do customers take online? Extract online channels from #7

Nothing teaches like experience. When employees click on a link or an attachment in a simulated phishing email, it's important to communicate to them that they have potentially put both themselves and the organization at risk.

8.2 OFFLINE What kind of actions do customers take offline? Extract offline channels from #7 and use them for customer development.

Phishing awareness training starts with educating your employees on why phishing is harmful, and empowering them to detect and report phishing attempts.

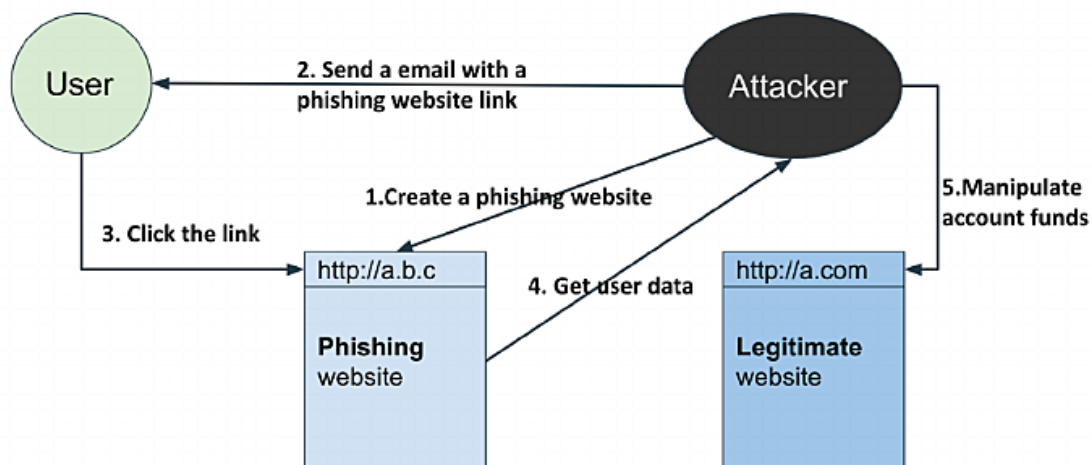
Simulated phishing campaigns reinforce employee training, and to understand risk and improve workforce resiliency as these can take many forms, such as mass phishing, spear phishing, and whaling.

9. PROBLEM ROOT CAUSE

What is the real reason that this problem exists? What is the back story behind the need to do this job? i.e. customers have to do it because of the change in regulations.

A phishing attack is a type of cybersecurity threat that targets users directly through email, text or direct messages. During one of these scams, a cybercriminal will pose as a trusted contact to steal data from an unsuspecting user such as login information, account numbers and credit card information.

While there are several types of phishing, the main purpose behind all of them is it to steal sensitive information or transfer malware.



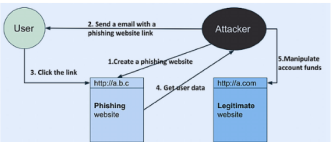
10. YOUR SOLUTION

If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality. If you are working on a new business proposition, then keep it blank until you fill in the canvas and come up with a solution that fits within customer limitations, solves a problem and matches customer behaviour.

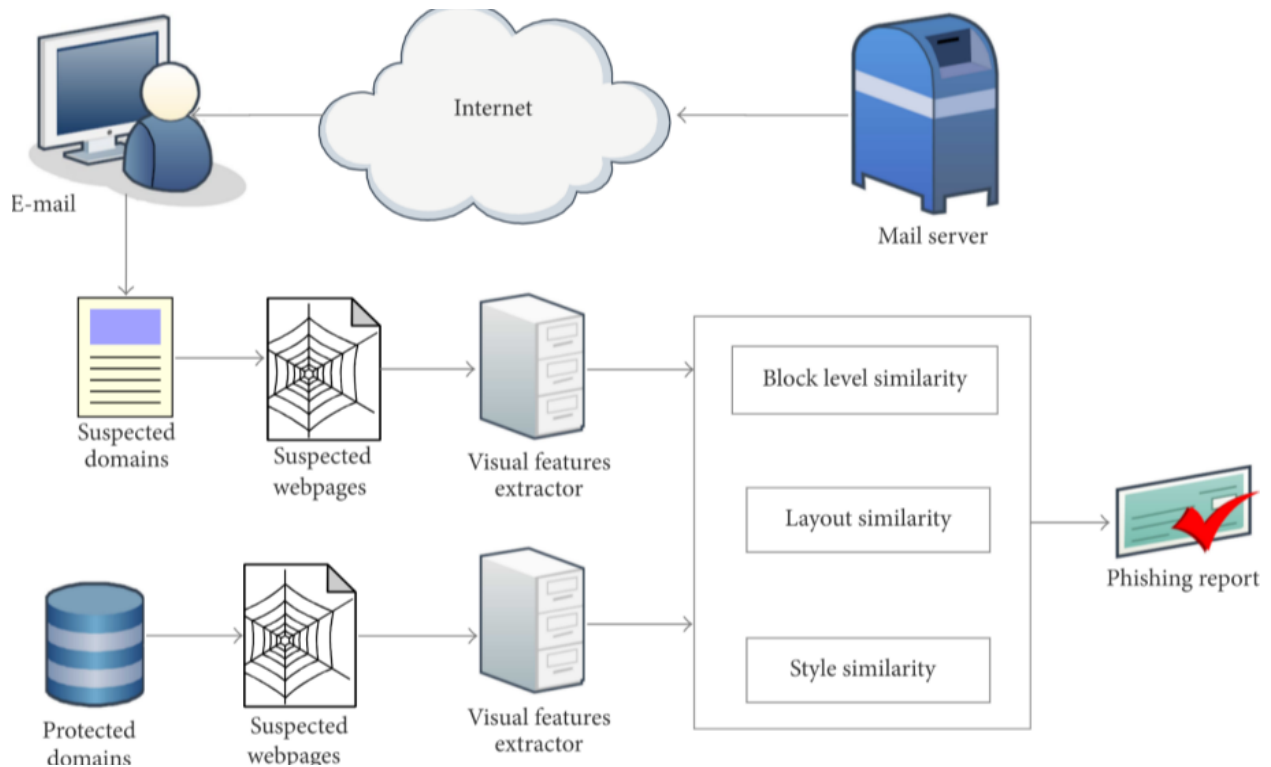
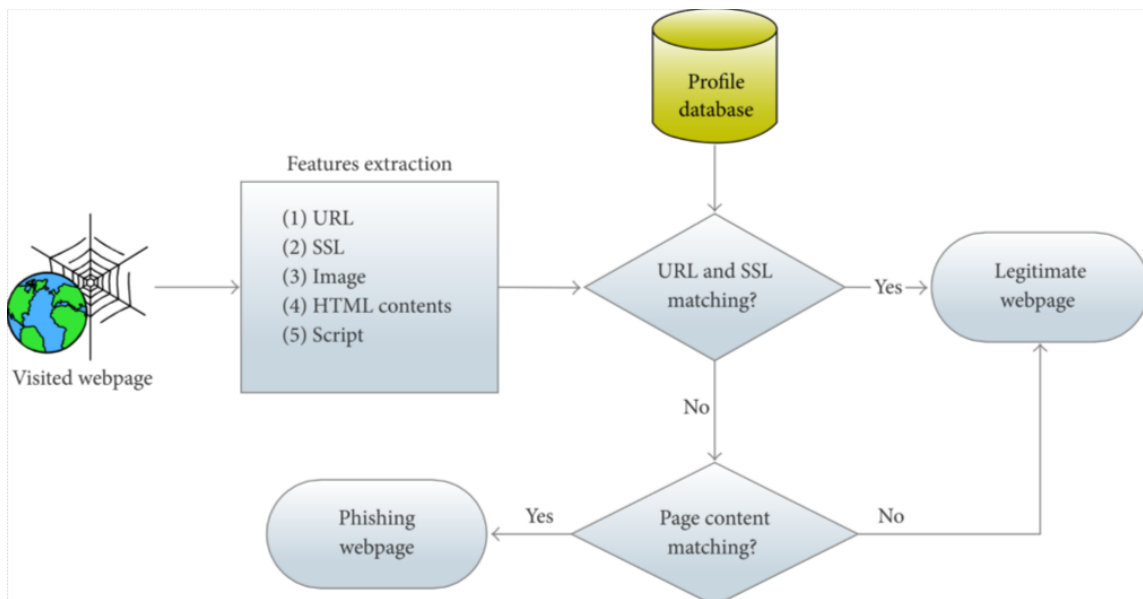
We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different web designing languages which include HTML, CSS, JavaScript and Python. This website is more useful to the user and it is user friendly also.

Problem-Solution fit canvas 2.0

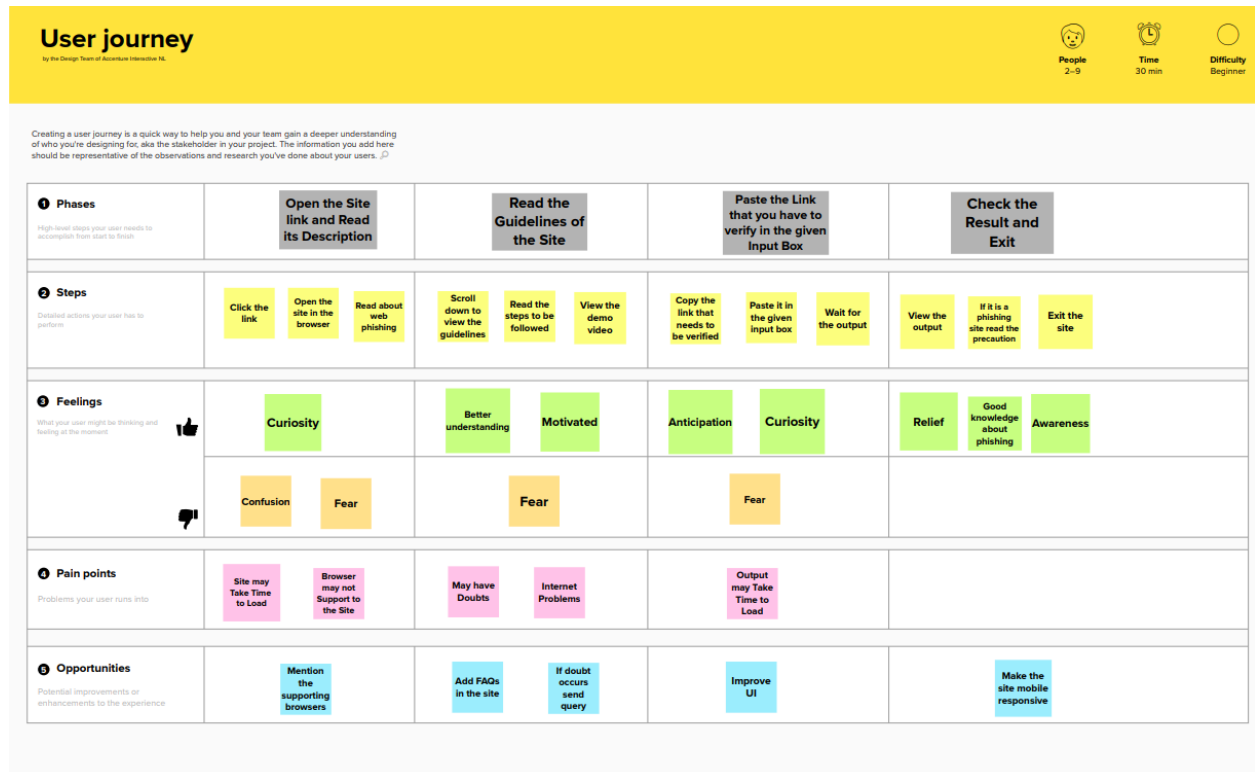
Purpose / Vision

Define CS, fit into CC	1. CUSTOMER SEGMENT(S) CS Who is your customer? <ul style="list-style-type: none"> Protect yourself and your family against malicious websites with the platform for free. With the platform, protecting your staff, data, brand, and your customer from malicious websites has never been easier. Proactively protect multiple customers against malicious websites at once with all-in-one platform. The platform can be used for government embeds to provide 100% security and privacy. 	6. CUSTOMER CONSTRAINTS CC What constraints prevent your customers from taking action or limit their choices of solutions? <ul style="list-style-type: none"> The limitations of the web phishing detection approaches are explored by means of detection time, detection rate, and storage complexity to verify the level of robustness against the phishing attack. Thus most of the recent web phishing detection approaches lag in feature selection mechanism as they use handcrafted features to detect the attack. 	5. AVAILABLE SOLUTIONS AS Which solutions are available to the customers when they face the problem or need to get the job done? What have they tried in the past? What pros & cons do these solutions have? <ul style="list-style-type: none"> Legitimate websites prevent web scraping by several techniques in respect to obfuscation using CSS sprites to display important data, replacing text with images. Spam filtering techniques are used to identify unsolicited emails before the user reads or clicks the link. When users visit a phishing web page that looks like a legitimate website, many people do not remember the legitimate website's domain name, particularly for some start-ups or unknown companies, so users cannot recognise the phishing website based on the URL. Some web browsers integrate a security component to detect phishing or malware sites, such as Chrome, which will display warning messages when one visits an unsafe web page. When the website detects that the IP address and device information of the user who is logging in does not match the commonly used information, it is necessary to verify the authenticity of the user. 	Explore AS, differentiate
	Focus on J&P, tap into BE, understand RC	2. JOBS-TO-BE-DONE / PROBLEMS J&P Which jobs-to-be-done (or problems) do you address for your customers? There could be more than one; explore different sides. <ul style="list-style-type: none"> The objective of phishing website URLs is to purloin the personal information like user name, passwords and online banking transactions. Phishers use the websites which are visually and semantically similar to those real websites. As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing. 	9. PROBLEM ROOT CAUSE RC What is the real reason that this problem exists? What is the back story behind the need to do this job?  <ul style="list-style-type: none"> A phishing attack is a type of cybersecurity threat that targets users directly through email, text or direct messages. During one of these scams, a cybercriminal will pose as a trusted contact to steal data from an unsuspecting user such as login information, account numbers and credit card information. While there are several types of phishing, the main purpose behind all of them is it to steal sensitive information or transfer malware. 	
Identify strong TR & EM		3. TRIGGERS TR What triggers customers to act? <ul style="list-style-type: none"> Your users lack security awareness. Criminals are (unsurprisingly) following the money. You're not performing sufficient due diligence. Low-cost phishing and ransomware tools are easy to get hold of. Malware is becoming more sophisticated. 	10. YOUR SOLUTION SL If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality. If you are working on a new business proposition, then keep it blank until you fill in the canvas and come up with a solution that fits within customer limitations, solves a problem and matches customer behaviour. <ul style="list-style-type: none"> We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different web designing languages which include HTML, CSS, JavaScript and Python. This website is more useful to the user and it is user friendly also. 	8. CHANNELS of BEHAVIOUR CH 8.1 ONLINE What kind of actions do customers take online? Extract online channels from #7. <ul style="list-style-type: none"> Nothing teaches like experience. When employees click on a link or an attachment in a simulated phishing email, it's important to communicate to them that they have potentially put both themselves and the organisation at risk. 8.2 OFFLINE What kind of actions do customers take offline? Extract offline channels from #7 and use them for customer development. <ul style="list-style-type: none"> Phishing awareness training starts with educating your employees on why phishing is harmful, and empowering them to detect and report phishing attempts. Simulated phishing campaigns reinforce employee training, and to understand risk and improve workforce resiliency as these can take many forms, such as mass phishing, spear phishing, and whaling.

SOLUTION ARCHITECTURE:-



CUSTOMER JOURNEY:-



FUNCTIONAL REQUIREMENT:-

Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	User Registration	Registration through Form Registration through Gmail Registration through LinkedIn
FR-2	User Confirmation	Confirmation via Email Confirmation via OTP
FR-3	Registered User - Login	Login through password (Form) Login through Gmail Login through LinkedIn
FR-4	Verify the link provided by the user	User inputs the link to be verified
FR-5	Display the result	If the site link is a phishing site, user must be aware and read the precautions displayed If the site link is legit, exit the application
FR-6	Share Queries	If any doubts, send query Read FAQs

Non-functional Requirements:

Following are the non-functional requirements of the proposed solution.

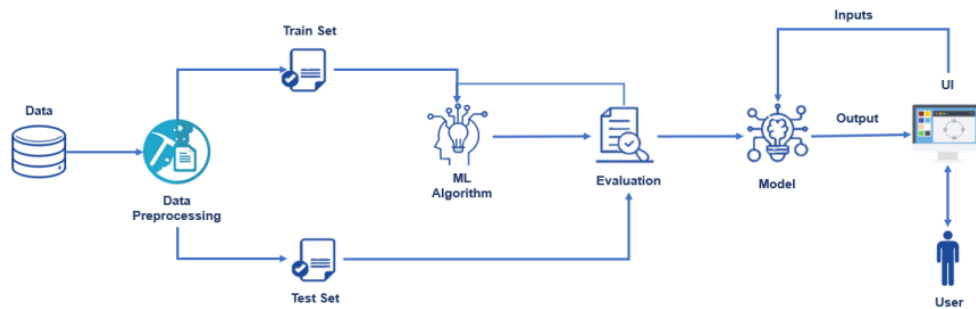
FR No.	Non-Functional Requirement	Description
NFR-1	Usability	Engage the user about the process to ensure that the functionality can meet design and usability requirements.
NFR-2	Security	It includes intrusion prevention and detection, authentication, authorization, and confidentiality of the user information.
NFR-3	Reliability	It focuses on preventing failures during the lifetime of the product or system, from commissioning to decommissioning.
NFR-4	Performance	It is the ability of the application to always run acceptably. In time-critical scenarios, even the smallest delay in processing data can be unacceptable.
NFR-5	Availability	Ensuring that the application can meet its availability targets to be resilient (fault tolerance).
NFR-6	Scalability	It is the ability for the application to scale to meet increasing demands; for example, at peak times or as the system becomes more widely adopted.

DATA FLOW DIAGRAMS:-

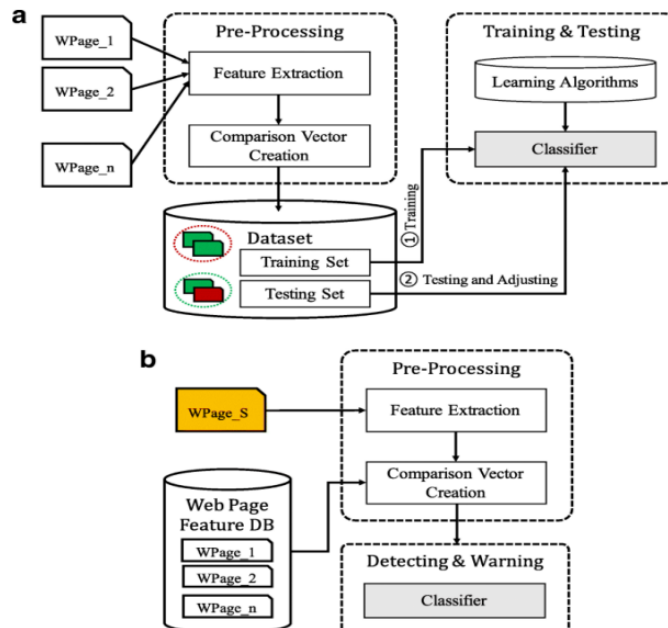
Data Flow Diagrams:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

Architecture Diagram:



DFD Diagram:



User Stories

Use the below template to list all the user stories for the product.

User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Web user)	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	I can access my account / dashboard	High	Sprint-1
		USN-2	As a user, I will receive confirmation email once I have registered for the application	I can receive confirmation email & click confirm	High	Sprint-1
		USN-3	As a user, I can register for the application through LinkedIn	I can register & access the dashboard with LinkedIn Login	Low	Sprint-3
		USN-4	As a user, I can register for the application through Gmail	I can register & access the dashboard with Gmail Login	Medium	Sprint-2
	Login	USN-5	As a user, I can log into the application by entering email & password	I can access my account / dashboard	High	Sprint-1
	Dashboard	USN-6	As a user, I paste the Link that needs to be Verified as a Phishing site or not	I can paste the Link into the Textbox	High	Sprint-2
		USN-7	As a user, I can see the Result	I can view that it is a Safe Site	High	Sprint-2
Customer Care Executive	Help	USN-8	As a user, I can Share my Queries in the Help Textbox	I can send my Doubts through it	Medium	Sprint-3
Administrator	Contact	USN-9	As a Administrator, I can Answer the User Queries	I sent the Solution through User provided Email	Low	Sprint-4
		USN-10	As a Administrator, I can Improve the Accuracy	I can update the Website	High	Sprint-4

TECHNOLOGY ARCHITECTURE:-

Technical Architecture:

The Deliverable shall include the architectural diagram as below and the information as per the table1 & table 2

Web Phishing Detection Diagram

Reference: [What is phishing? | IBM](#)

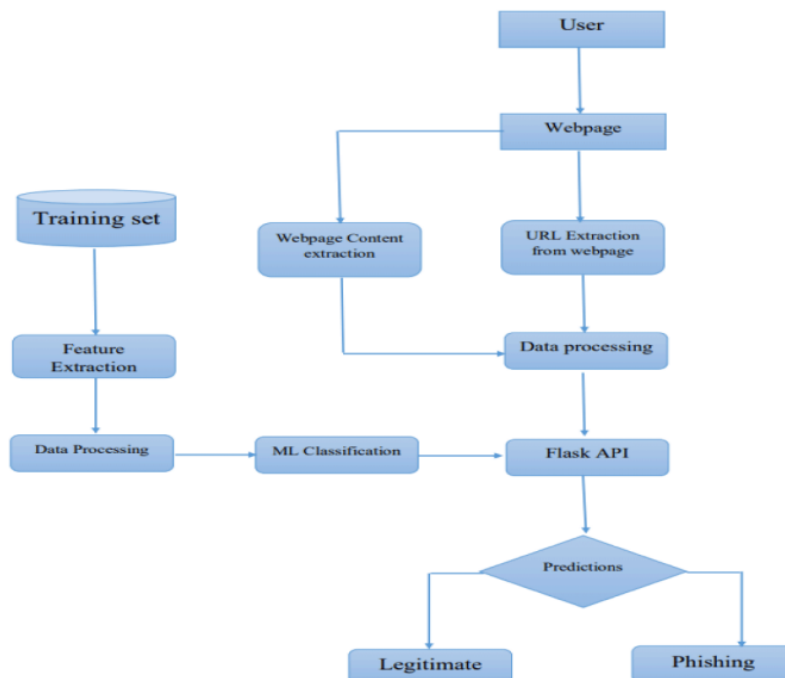
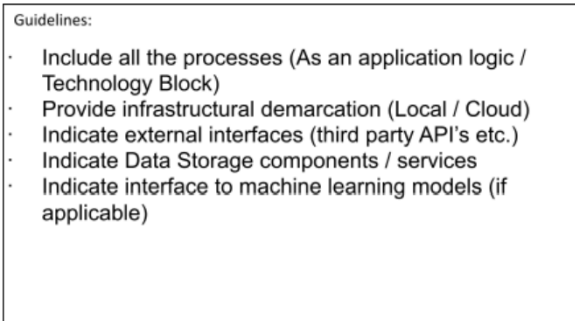


Table-1 : Components & Technologies:

S.No	Component	Description	Technology
1.	User Interface	Dynamic Web UI	HTML, CSS, JavaScript, Bootstrap
2.	Application Logic-1	User Registration/Login	IBM API Connect Service, Gmail API, LinkedIn API
3.	Application Logic-2	Web app that predicts if the link is a phishing site or not	Flask API, Python
4.	Database	Store user input links in the database	MongoDB
5.	Cloud Database	Database Service for storing user profile	IBM DB2, IBM Cloudant etc.
6.	File Storage	Store the datasets used for prediction	Local Filesystem
7.	External API-1	User Registration/Login using email and password	IBM API Connect
8.	External API-2	User Registration/Login using external apps	Gmail API, LinkedIn API
9.	Machine Learning Model	Machine Learning Model for web phishing detection	Logistic Regression Model
10.	Infrastructure (Server / Cloud)	Application Deployment on Local System / Cloud	Local, Render, IBM Cloud

PREPARE MILESTONE AND ACTIVITY LIST:-

TITLE	DESCRIPTION	DATE
Literature Survey & Information Gathering	Literature survey on the selected project & gathering information by referring to technical papers, research publications etc.	3 September '22
Prepare Empathy Map	Prepare Empathy Map Canvas to capture the user Pains & Gains and prepare a list of problem statements.	10 September '22
Ideation	List the ideas (at least 4 per each team member) by organizing the brainstorming session and prioritize the top 3 ideas based on the feasibility & importance	17 September '22
Proposed Solution	Prepare the proposed solution document, which includes the novelty, feasibility of idea, business model, social impact, scalability of solution, etc.	24 September '22
Proposed Solution Fit	Prepare problem - solution fit document.	01 October '22
Solution Architecture	Prepare a solution architecture document.	01 October '22
Customer Journey Map	Prepare the customer journey maps to understand the user interactions & experiences with the application (entry to exit).	08 October '22
Data Flow Diagrams	Prepare the Data-Flow Diagrams.	15 October '22
Solution Requirements	Prepare the Functional Requirement Document.	15 October '22
Technology Architecture	Prepare Technology Architecture of the solution.	15 October '22
Project Planning	Prepare Milestone & Activity List, Sprint Delivery Plan.	22 October '22
Project Development - Delivery of Sprint-1, 2, 3 & 4	Develop & submit the developed code by testing it.	In Progress

SPRINT DELIVERY PLAN:-

Product Backlog, Sprint Schedule, and Estimation (4 Marks)

Use the below template to create product backlog and sprint schedule

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	Registration	USN-1	As a user, I can register for the application by entering my email, password, and confirming my password.	5	High	Harini, Febi
Sprint-1		USN-2	As a user, I will receive confirmation email once I have registered for the application	5	High	Harini, Febi
Sprint-3		USN-3	As a user, I can register for the application through LinkedIn	10	Low	Harini, Febi
Sprint-2		USN-4	As a user, I can register for the application through Gmail	5	Medium	Ana,Beautsmin
Sprint-1	Login	USN-5	As a user, I can log into the application by entering email & password	10	High	Harini, Febi
Sprint-2	Dashboard	USN-6	As a user, I paste the Link that needs to be Verified as a Phishing site or not	5	High	Ana,Beautsmin, Harini, Febi
Sprint-2		USN-7	As a user, I can see the Result	10	High	Ana,Beautsmin, Harini, Febi
Sprint-3	Help	USN-8	As a user, I can Share my Queries in the Help Textbox	10	Medium	Ana,Beautsmin
Sprint-4	Contact	USN-9	As a Administrator, I can Answer the User Queries	10	Low	Ana,Beautsmin
Sprint-4		USN-10	As a Administrator, I can Improve the Accuracy	10	High	Ana,Beautsmin

Project Tracker, Velocity & Burndown Chart: (4 Marks)

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	20	6 Days	24 Oct 2022	29 Oct 2022	20	29 Oct 2022
Sprint-2	20	6 Days	31 Oct 2022	05 Nov 2022	15	05 Nov 2022
Sprint-3	20	6 Days	07 Nov 2022	12 Nov 2022	10	12 Nov 2022
Sprint-4	20	6 Days	14 Nov 2022	19 Nov 2022	20	19 Nov 2022

Velocity:

Imagine we have a 10-day sprint duration, and the velocity of the team is 20 (points per sprint). Let's calculate the team's average velocity (AV) per iteration unit (story points per day)

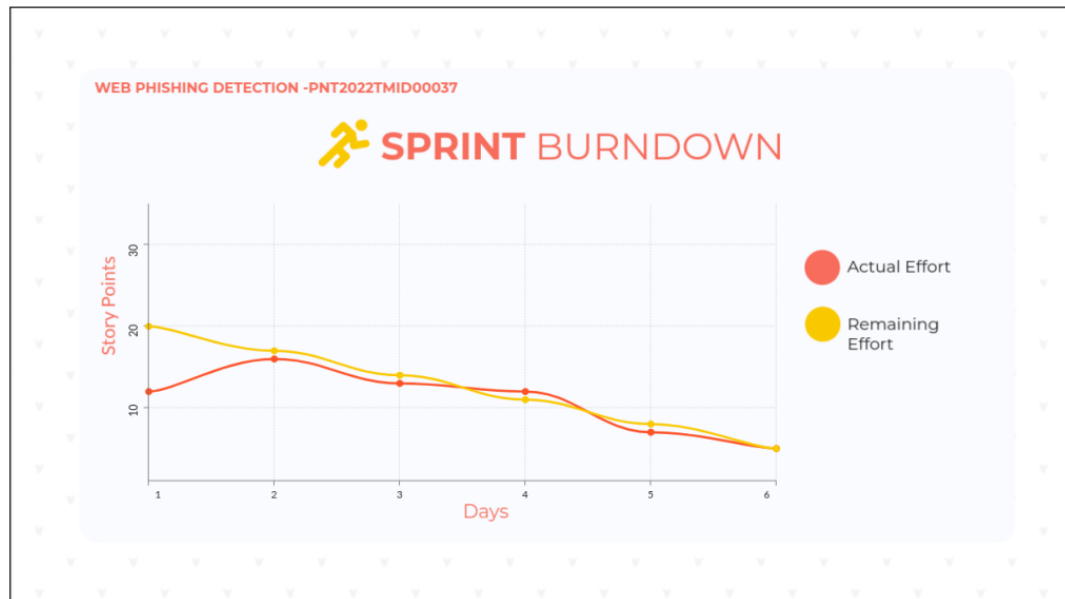
$$AV = \frac{\text{sprint duration}}{\text{velocity}} = \frac{20}{10} = 2$$

We have a 6-day sprint duration, and the velocity of the team is 20 (points per sprint). So our team's average velocity (AV) per iteration unit (story points per day)

$$AV = (\text{Sprint Duration} / \text{Velocity}) = 20 / 6 = 3.33$$

Burndown Chart:

A burndown chart is a graphical representation of work left to do versus time. It is often used in agile software development methodologies such as Scrum. However, burn down charts can be applied to any project containing measurable progress over time.



Reference:

<https://www.visual-paradigm.com/scrum/scrum-burndown-chart/>

<https://www.visme.co/templates/charts/sprint-burndown-chart-1425285230/>

USER ACCEPTANCE TESTING(UAT) REPORT TEMPLATE:-

1. Purpose of Document

The purpose of this document is to briefly explain the test coverage and open issues of the Web Phishing Detection 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
Print Engine	7	0	0	7
Client Application	51	0	0	51
Security	2	0	0	2
Outsource Shipping	3	0	0	3

Exception Reporting	9	0	0	9
Final Report Output	4	0	0	4
Version Control	2	0	0	2