Project Design Phase-II
Solution Requirements (Functional & Non-functional)

Date	15 October 2022
Team ID	PNT2022TMID28015
Project Name	Project – Web Phishing Detection
Maximum Marks	4 Marks

Functional Requirements:

Following are the functional requirements of the proposed solution.

FR No.	Functional Requirement (Epic)	Sub Requirement (Story / Sub-Task)
FR-1	**User Input**	User inputs an URL in required field to check its validation.
FR-2	**Website Comparison**	Model compares the websites using Blacklist and Whitelist approach.
FR-3	**Feature extraction**	After comparing, if none found on comparison then it extracts feature using heuristic and visual similarity approach.
FR-4	**Prediction**	Model predicts the URL using Machine Learning algorithms such as Logistic Regression, KNN
FR-5	**Classifier**	Model sends all output to classifier and produces final result.
FR-6	**Announcement**	Model then displays whether website is a legal site or a phishing site.
FR-7	**Events**	This model needs the capability of retrieving and displaying accurate result for a website

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**High detection efficiency**	To provide high detection efficiency, incorrect classification of benign sites as phishing (false-positive) should be minimal and correct classification of phishing sites (true-positive) should be high.
NFR-2	**Real-time detection**	The prediction of the phishing detection approach must be provided before exposing the user's personal information on the phishing website
NFR-3	**Target independent**	Due to the features extracted from both URL and HTML the proposed approach can detect new phishing websites targeting any benign website (zero-day attack).