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

Date	17October 2022
Team ID	PNT2022TMID31980
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	**Features Extraction**	Lexical Features. Hyperlink Features. URL Features. Textual content Features.
FR-2	**Data Base Collection**	Phishing URL's. Non-Phishing URL.
FR-3	**Machine Learning Classifier Training**	Identify the Criteria. Build a decision tree. Train our model. Evaluate our model. Check for false positives/negatives.
FR-4	**Features Set Classification**	Address Bar based Features. Abnormal Based Features. Domain Based Features. HTML & JavaScript Based Features.
FR-5	**Algorithm**	Data Mining Algorithm. PhishDekt Algorithm.
FR-6	**Techniques**	Whitelist & Blacklist Techniques. Layout Based Detection Schemes.

Non-functional Requirements:

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

FR No.	Non-Functional Requirement	Description
NFR-1	**Usability**	The internet users can assist antiphishing tools and technology which provide essential information, such as warning of spoofed pages.
NFR-2	**Security**	The list-based detection will alert the users before entering into the phishing websites.
NFR-3	**Reliability**	Provide warning message to the users when it fails to detect the blacklisted URL are encountered with minor changes
NFR-4	**Performance**	The phishing websites can be detected with 97.95% accuracy
NFR-5	**Availability**	Users can utilize the ML algorithm to detect attacks based on features extracted from URL
NFR-6	**Scalability**	ML based models is able to detect 0-day attacks which is scalable and accurate