

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

Date	16 October 2022
Team ID	PNT2022TMID33268
Project Name	Project – Web Phishing Detection
Maximum Marks	4 Marks

Functional Requirements:

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:

FR No.	Non-Functional Requirement	Description
NFR-1	Usability	It helps the users to get aware of theft of their personal information
NFR-2	Security	Refers to the security measures that individuals and organizations can take to prevent a phishing attack or to mitigate the impact of a successful attack
NFR-3	Reliability	The importance to safeguard online users from becoming victims of online fraud , divulging confidential information to an attacker among other effective uses of phishing detection tools play a vital role in ensuring a secure online experience for users.
NFR-4	Performance	<p>Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced.</p> <p>Besides, the most common technique used, blacklist- based method is inefficient in responding to emanating phishing attacks since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database.</p>
NFR-5	Availability	By developing and deploying it in online we can access any time it may help to detect the threading activities.
NFR-6	Scalability	Using Web Phishing detection move the protection from users towards the network provider and to employ the novel bad neighbourhood concept ,in order to detect and isolate both phishing e-mail senders and phishing web servers.