**Project Design Phase-II**

**Solution Requirements (Functional & Non-functional)**

|  |  |
| --- | --- |
| Date | 15 October 2022 |
| Team ID | PNT2022TMID02425 |
| Project Name | 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 Registration | Registration through Forms. |
| FR-2 | User Confirmation | The Registration is confirmed via Email. |
| FR-3 | User Authentication | Authentication can be done with password or 2step-verification. |
| FR-4 | User input | User need to download the extension and then inputs an URL (Uniform Resource Locator) in necessary field to check its validation. |
| FR-5 | Website Evaluation | Model evaluates the website using Blacklist and Whitelist approach |
| FR-6 | Extraction and Prediction | It retrieves features based on heuristics and visual similarities. The URL is predicted by the model using Machine Learning methods such as Logistic Regression and KNN. |
| FR-7 | Real Time monitoring | The use of Extension plugin should provide a warning pop-up when they visit a website that is phished.  Extension plugin will have the capability to also detect latest and new phishing websites |
| FR-8 | Authentication | Authentication assures secure site, secure processes and enterprise information security. |

**Non-functional Requirements:**

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

|  |  |  |
| --- | --- | --- |
| **FR No.** | **Non-Functional Requirement** | **Description** |
| NFR-1 | **Usability** | Usability is commonly considered to be the enemy of security. In general, being secure means taking extra steps to avoid falling for different attacks. This is especially true of phishing where the best ways to prevent most phishing attacks are commonly known, but cybersecurity guidance is rarely followed. Our extension helps in achieving this in an easier and affordable way |
| NFR-2 | **Security** | It guarantees that any data included within the system or its components will be safe from malware threats or unauthorised access. If you wish to prevent unauthorised access to the admin panel, describe the login flow and different user roles as system behaviour or user action |
| NFR-3 | **Reliability** | It specifies the likelihood that the system or its component will operate without failure for a specified amount of time under prescribed conditions. |
| NFR-4 | **Performance** | It is concerned with a measurement of the system's reaction time under various load circumstance |
| NFR-5 | **Availability** | It represents the likelihood that a user will be able to access the system at a certain moment in time. While it can be represented as an expected proportion of successful requests, it can also be defined as a percentage of time the system is operational within a |
| NFR-6 | **Scalability** | It has access to the highest workloads that will allow the system to satisfy the performance criteria. There are two techniques to enable the system to grow as workloads increase: Vertical and horizontal sc |