Phishing attacks have become a prevalent threat in today's digital landscape, posing significant risks to individuals and organizations. To combat this issue, this project presents a novel approach to detecting phishing URLs using machine learning classification algorithms. The project leverages a comprehensive dataset comprising various parameters such as UsingIP, LongURL, ShortURL, Symbol@, Redirecting//, PrefixSuffix-, SubDomains, HTTPS, DomainRegLen, Favicon, NonStdPort, HTTPSDomainURL, RequestURL, AnchorURL, LinksInScriptTags, ServerFormHandler, InfoEmail, AbnormalURL, WebsiteForwarding, StatusBarCust, DisableRightClick, UsingPopupWindow, IframeRedirection, AgeofDomain, DNSRecording, and WebsiteTraffic.Multiple classification algorithms, namely K-Nearest Neighbors (KNN), Support Vector Machine (SVM), Logistic Regression, XGBoost, and Gradient Boosting, were employed to predict the safety of a given URL. Evaluation of these algorithms was conducted using precision, recall, and F1-score metrics. Among the algorithms tested, the Gradient Boosting algorithm exhibited superior performance, achieving an accuracy of 97% in correctly identifying phishing URLs.Based on the successful development and evaluation of the machine learning models, a web application was developed to provide real-time phishing detection. The application accepts input URLs and provides an instant determination of their safety status, assisting users in making informed decisions and protecting their systems from potential harm. The findings of this project demonstrate the effectiveness of machine learning algorithms in detecting phishing URLs and emphasize the importance of proactive measures to counter phishing attacks. The developed web application holds great potential in enhancing the security posture of individuals and organizations by enabling prompt identification of phishing attempts.