Web Applications Vulnerability Analysis

Nowadays information has become an asset to many institutions and as a result these institutions have become targets for people with malicious intents to attack these institutions. The web is now an important means of transacting business and without security, websites cannot thrive in today's complex computer ecosystem as there are new threats emerging as old ones are being tackled. Vulnerability assessment of websites is one of the means by which security can be improved on websites. According to the statistics released by the Common Vulnerabilities and Exposures (CVE) organization, the number of software vulnerabilities discovered in the year 2000 was less than 4600 while the number of vulnerabilities in the past three years from 2018 – 2020 covered nearly 200000, Which undoubtedly increases the threats faced by many computer users using any network services. Therefore, the need for automated, scalable, machine-speed vulnerability detection, vulnerability Analysis, and defect recognition techniques based on Machine Learning techniques are becoming urgent when facing severe challenges posed by network security issues.

Traditional vulnerability research methods often require security researchers to have professional knowledge and rich practical experience, which is less versatile and has limited efficiency. At present, the application of Machine learning and natural language processing technologies can intelligently process vulnerabilities. This Project will be based on Detection, Recognition and Analysis of various vulnerabilities and threats present in Websites or Web Applications so as to pre-emptively defend against the exploitation of applications, software, or networks. This can be achieved by utilizing various Machine Learning techniques and algorithms for training of the model with the help of data collected regarding various vulnerabilities present in web applications, deployment and testing of the model in order to find certain patterns, dependencies or associations in the dataset. The collection of data will be carried out using Nessus Vulnerability Scanner. Nessus is one of the many vulnerability scanners used during vulnerability assessments and malicious attacks. Nessus has the ability to classify the vulnerabilities into risk-based categories from critical to even informational which is one of the things that separates Nessus from other vulnerability scanners. The collected data will be studied, processed and an appropriate machine learning model or neural network will be implemented to analyse the data.

In the process of Web application development, it is the common goal of developers to improve quality of services and safety. Traditional vulnerabilities detection methods require domain experts to spend a lot of time and energy so as to safeguard their applications from different attacks and intrusions, and it has become vital to combine Machine learning technology to assist automated detection. In further implementations, the goal is to outline preventive maintenance against such vulnerabilities or threats and well-known techniques to secure websites owner and also educate most users which leads to better performance of web applications in terms of time, efficiency and reliability.

1RZ19MCA39 - Sanjana Suresh

1RV19MCA25 - Devyansh Saklani

Guide :

Dr. Vijayalakshmi M.N