**Software Vulnerability Detection Tool Using Machine Learning Algorithms**

**Abstract**

Exploitable vulnerabilities in software have attracted tremendous attention in recent years because of their potentially high severity impact on computer security and information safety. Many vulnerability detection methods have been proposed to aid code inspection. Among these methods, there is a line of studies that apply machine learning techniques and achieve promising results. This paper reviews 22 recent studies that adopt deep learning to detect vulnerabilities, aiming to show how they utilize state-ofthe-art neural techniques to capture possible vulnerable code patterns. Among reviewed studies, we identify four game changers that significantly impact the domain of deep learning-based vulnerability detection and provide detailed reviews of the insights, ideas, and concepts that the game changers have brought to this field of interest. Based on the four identified game changers, we review the remaining studies, presenting their approaches and solutions which either build on or extend the game changers, and sharing our views on the future research trends. We also highlight the challenges faced in this field and discuss potential research directions. We hope to motivate the readers to conduct further research in this developing but fast-growing field.

**Existing System**

In Existing system, we are using ,machine learning algorithms like k-means, random forest and decision tree to develop vulnerability detection tool

**Disadvantages**

1.Less accuracy.

**PROPOSED SYSTEM**

In proposed system, we are using Ensemble Machine Learning algorithm which is combination of multiple algorithms such as SVM, KNN and Naïve Bayes.

Now-a-days Machine Learning algorithms are using everywhere from Medical disease prediction to road side traffic prediction as this algorithms prediction accuracy is more than 95%.

Above success of Machine Learning algorithms are migrating us to develop vulnerability detection tool using machine learning algorithms. Machine Learning algorithms get trained on past data and then can analyse new test data to predict it class of Normal or Vulnerability type.

In propose work we are using dataset to identify 3 different classes such as ‘No Vulnerability, SQL Injection, XSS or RFI.

**Advantages**

1. High Accuracy

**SYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**:

Processor - Intel i3 or higher

Speed - 1.1 GHz

RAM - 4 GB (min)

Hard Disk - 500 GB (min)

**SOFTWARE REQUIREMENTS:**

Operating System - Windows 10 or above

Programming Language - Python with Jupiter notebook