Technology Bucket: Software - Web App development
Ministry: Ministry of External Affairs
Team Leader: Rajshree Gavel

Category: Software
Problem Code:
College Code: u-0092

Abstract Idea:

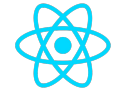
SQL Injection is around 19 years old technique yet many web applications are prone to it. OWSAP is an organisation which provides top 10 security vulnerabilities. To make the internet a more secure place, we need to work more on the security and fix these vulnerabilities.

There are many tools available to scan if a particular website is vulnerable. But the problem is not everyone can easily use them. Most of them are command line tools and the developers aren't the happiest people using them.
There will be an easy to use vulnerability scanner which can help out the developers to scan their websites in two modes viz., External Scan Mode and Source Code Mode.

While the External Scan Mode will tell us what vulnerabilities are there, Source Code Mode will tell us where exactly the problem is and how we can fix it. The latter will be done with the use of Deep Learning (Neural Networks), while the vulnerabilities will be told using the algorithms. We can convert the code base into embeddings with the models such as Word2Vec, Code2Vec, and BERT and then train the model on labeled data which could determine what vulnerabilities are present in the codebase and then we can find out where they lie.

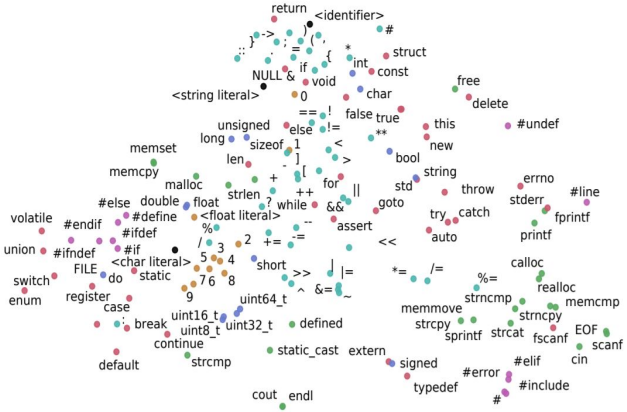
Tech Stack:

- React.js for frontend GUI.
- Tensorflow serving to serve APIs from deep learning model.
- Keras library in python for building deep learning models.
- Node.js for VSCode extension.
- HTML, CSS and JS for Chrome extension.
- Electron for a cross-platform desktop application.
- Docker for build pipeline.

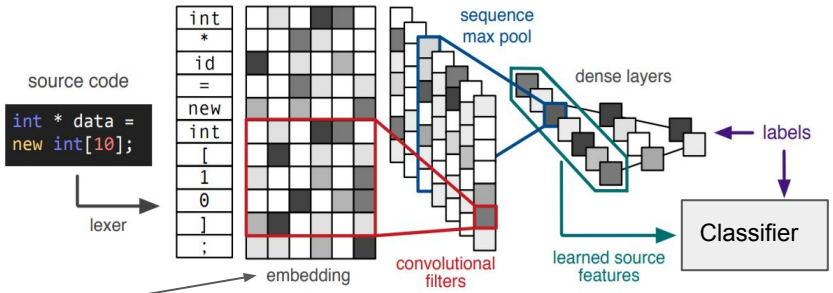


VSCode Extension

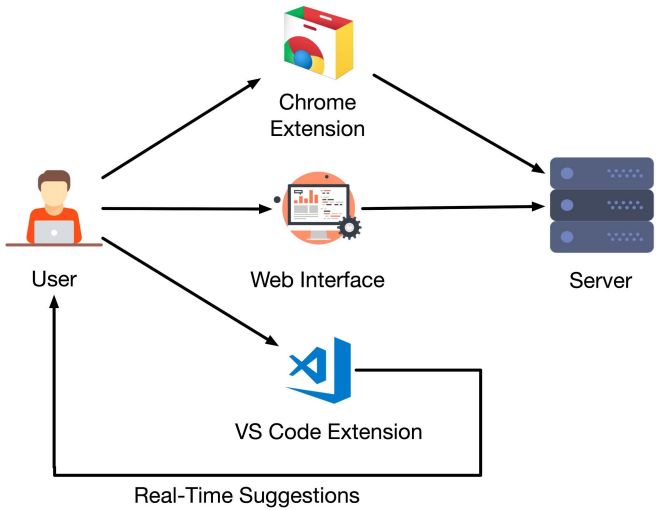
Chrome Extension



C/C++ embeddings



Architecture of deep learning model



Use Case:

Expected users are Developers, Hackers and Website owners who want to see if a website is vulnerable to attacks, especially coming from OWASP top 10 vulnerabilities.

Show Stopper:

A real-time vulnerability detection assistant integrated with VSCode which allows developers to address security issues as they code.