ВЕБ-СЕРВИС ДЛЯ ЗАДАЧИ КЛАССИФИКАЦИИ СТЕПЕНИ КРИТИЧНОСТИ УЯЗВИМОСТИ ПО ЕЕ ТЕКСТОВОМУ ОПИСАНИЮ

А.К. Доронин

Процесс определения характеристик CVE-уязвимостей сопряжен с ручной экспертной оценкой, что может приводить к неточным или неполным данным [1], и, следовательно, к непредсказуемым последствиям. На момент появления уязвимости имеется лишь ее текстовое описание, из которого можно получить всю релевантную информацию о ее характеристиках [2]. Поэтому актуальной является разработка системы автоматического определения степени критичности уязвимости по ее текстовому описанию. В качестве ядра, производящего автоматическую оценку критичности уязвимости, предлагается использовать построенную нами модель машинного обучения с точностью предсказания 85,52 % [3]. Однако процесс практической реализации данной модели сопряжен с рядом трудностей. В частности, необходимо разработать: архитектуру системы; процесс загрузки всех необходимых для работы модели машинного обучения компонентов; процесс работы функции предсказания степени критичности по входному текстовому описанию, а также необходимо обеспечить отказоустойчивость и масштабируемость решения. В данной работе предлагается реализация такой системы в виде веб-сервиса. Разработан проект архитектуры для обращения к веб-серверу, алгоритм функции вычисления вероятностных значений модели, процесс загрузки начальных компонентов. Веб-сервис в соответствии со спроектированной архитектурой реализован на языке программирования Python 3 с использованием фреймворков Keras, Tensorflow и Flask. Проведено нагрузочное тестирование веб-сервиса на одной машине, на основе которого сделан вывод о наличии ограничения эффективной максимальной пропускной способности в 130 запросов/секунду в идеальных условиях. Веб-сервис упакован в Docker-контейнер. Среди преимуществ реализованной системы являются: масштабируемость, отказоустойчивость, легкость развертывания и взаимодействия с другими системами. Исходный код выложен в открытый доступ и доступен для дальнейших экспериментов по ссылке: https://www.github.com/teacherlex/cve_vulns_classifier/tree/master/api.

Литература

1. Massacci F., Nguyen V. H. Which is the right source for vulnerability studies? An empirical analysis on Mozilla Firefox // Proceedings of the 6th International Workshop on Security Measurements and Metrics,MetriSec'10. – 2010; 1: 4:1 – 4:8.

2. Gonzalez D., Hastings H., Mirakhorli M. Automated Characterization of Software Vulnerabilities // 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME). – 2019. – P. 135–139. – DOI:10.1109/ICSME.2019.00023.

3. Доронин А.К., Липницкий В.А. Построение модели машинного обучения для задачи классификации степени критичности CVE-уязвимостей // Вестник МГУ им. А. А. Кулешова. – 2020. – № 1 (55). – С. 51–63.