УДК 004.4

РАЗРАБОТКА АНАЛИЗАТОРА УЯЗВИМОСТЕЙ .NET-ПРИЛОЖЕНИЙ

Дерябин А. (Университет ИТМО)
Научный руководитель – ассистент факультета ПИиКТ, Логинов И.П.
(Университет ИТМО)

В настоящее время многие приложения используют функциональность сторонних библиотек. При этом каждая из библиотек потенциально содержит уязвимости, которые могут сделать уязвимой приложение, в котором данные библиотеки используются. При обнаружении уязвимости обычно вносятся в общедоступную базу данных и, если библиотека всё ещё поддерживается, выпускается новая версия, устраняющая проблемы безопасности. Чтобы минимизировать риск наличия уязвимых зависимостей, имеет смысл регулярно обновлять их до самой последней стабильной версии, однако это не всегда возможно, так как каждое обновление создает риск нарушения совместимости с существующей кодовой базой, и, следовательно, вызывает необходимость её изменения, что, в свою очередь, может требовать существенных трудозатрат. Частичным решением этой проблемы является обновление только тех библиотек, об уязвимостях которых уже известно – несмотря на то, что остаются проблемы, связанные с изменением кодовой базы, количество и частота обновлений становится существенно ниже, за счёт чего существенно уменьшаются трудозатраты. Такой подход, однако, требует своевременного отслеживания публикаций об уязвимостях в используемых библиотеках. Разработанное ПО решает эту задачу для приложений на основе .NET Framework и .NET Core, осуществляя поиск используемых зависимостей в актуальной базе CVE.

Основной уклон при разработке анализатора уязвимостей был направлен на практическую применимость разрабатываемого решения. Конечный продукт должен быть удобен для пользователя, а также выполнять поиск по базе уязвимостей как можно точнее. Для удобства использования реализован графический интерфейс, а также поддержка использования через интерфейс командной строки. Извлечение базы уязвимостей автоматизировано, а способ хранения записей был подобран таким образом, чтобы было удобно дописывать дополнительные записи при необходимости. Для реализации поиска по базе был реализован алгоритм, учитывающий возможные различия записи версий между базой уязвимостей и извлекаемыми версиями из .NET-сборки, а также позволяющий выполнять поиск по диапазону версий. Извлечение данных о зависимостях из .NET-сборки реализовано при помощи механизма рефлексии.

Результатом работы является приложение – анализатор, а также скрипт для составления базы уязвимостей, реализованные на C# и Python соответственно. Разработанное программное обеспечение уже зарегистрировано в едином реестре российских программ для ЭВМ и в дальнейшем будет эксплуатироваться компаниями на практике.

Дерябин А. (автор) _____

Логинов И.П. (научный руководитель) _____