УДК 004.415.53

РАЗРАБОТКА СРЕДСТВА КОМБИНИРОВАННОГО ФАЗЗИНГ-ТЕСТИРОВАНИЯ ВЕБ-ПРИЛОЖЕНИЙ

Павлов Д.Д. (Национальный исследовательский университет ИТМО)
Научный руководитель – к.т.н, доцент ФБИТ Бегаев А.Н.
(Национальный исследовательский университет ИТМО)

Основными векторами атаки на веб-приложения являются пользовательские интерфейсы, доступные потенциальному нарушителю. Средствами тестирования данных интерфейсов и анализа поведения программного обеспечения (ПО) на действия пользователя являются фаззеры. В настоящей работе разрабатывается средство комбинированного фаззинг-тестирования веб-приложений для эффективного обнаружения уязвимых мест в ПО.

Введение.

В современном мире бóльшая часть программного обеспечения имеет интерфейс взаимодействия с пользователем и, зачастую, используется его веб-представление, то есть основной точкой входа в приложение является веб-интерфейс. Данный веб-интерфейс в первую очередь должен подвергаться тестированию с целью исключения неожиданного поведения ПО после некоторых некорректных действий пользователя или ввода им некорректных данных через интерфейсы взаимодействия.

Средство, имитирующие ввод пользовательских данных во все возможные точки входа в приложение, называется фаззером. Наличие у разработчика средства фаззинг-тестирования и периодическое его использование для тестирования в рамках внедренной системы разработки безопасного программного обеспечения уменьшает возможное наличие уязвимостей в программном обеспечении и гарантирует задуманное разработчиком функционирование, способное корректно обработать любые данные пользователя.

Основная часть.

В настоящей работе предлагается разработка средства комбинированного фаззинг-тестирования веб-приложений. Данное средства совмещает в себе анализатор спецификации веб-приложения, мутатор и генератор данных по начальному входному корпусу данных, непосредственно фаззер – средство генерации и подачи запросов, и генератор отчетов. На вход средству фаззинга подаются пути до интерфейсов и первоначальные наборы данных, которые в дальнейшем мутируются по определенным правилам. На выходе получаем реакцию (выходные данные и поведение после обработки запроса) программного обеспечения на поданные данные, а также результат анализа полученной реакции с целью обнаружения неожиданных действий ПО.

Выводы.

Результат работы – разработанное средство комбинированного фаззинг-тестирования веб-приложений, возможно использовать как разработчикам программного обеспечения перед выпуском релизов для подтверждения отсутствия уязвимых интерфейсов, так и испытательным лаборатория в рамках проведения сертификационных испытаний программных средств, так как настоящее средство соответствует отдельным требованиям к средствам фаззинг-тестирования Методики выявления уязвимостей и недекларированных возможностей, разработанной ФСТЭК России.

Павлов Д.Д.

Бегаев А.Н.