УДК 004.056

Исследование и разработка универсальной системы управления динамическим тестированием безопасности веб-приложений

Иванов А.А. (Университет ИТМО)
Научный руководитель – кандидат технических наук, доцент Кузнецов А.Ю.
(Университет ИТМО)

Представлены результаты исследования и разработки универсальной системы управления динамическим тестированием безопасности веб-приложений. Объектом исследования является сам процесс динамического тестирования, его востребованность, сложности в построении данного процесса в организациях различного уровня и способы решения данных проблем. Разработана и протестирована система управления динамическим тестированием безопасности.

Введение. В настоящее время неотъемлемой частью жизни людей является Интернет, который, в свою очередь, представлен, по большей части, веб-сайтами. Чем больше возможностей для людей дает Интернет, тем больше угроз он может содержать в себе, а эти угрозы, потенциально, могут стать причиной потери финансов или персональных данных. В связи с этим для многих компаний, обслуживающих собственные веб-приложения, стала актуальной задача своевременного поиска и устранения потенциальных угроз безопасности. Один из методов этого достичь - динамическое тестирование безопасности, однако такое тестирование - сложный организационно-технический процесс, и не каждая компания имеет достаточно ресурсов для его реализации. Несмотря на большое количество существующих решений в области исследования безопасности веб-приложений, ни одно из них не подходит для использования в обусловленном процессе как есть.
Цель данной работы: исследовать и разработать универсальную систему динамического тестирования безопасности, которую возможно применить для построения соответствующего процесса с минимальным вложением ресурсов, тем самым повышая общий уровень информационной безопасности отдельно взятой и компании и всего Интернета в целом.

Основная часть. Основные проблемы при построении процесса динамического тестирования безопасности веб-приложений условно можно разделить на две категории: технические и организационные. В то время как организационные проблемы могут быть решены в основном только самой организацией или отделом, занимающимися построением процесса, технические проблемы могут быть решены выбором или созданием (при отсутствии существующих) подходящих программных средств. Исследование наиболее общих проблем при построении процесса показало, что система динамического тестирования должна состоять из трех независимых программных компонентов, решающих эти проблемы: обслуживающий, чья зона ответственности - доставка входных данных и получение результатов; тестирующий, суть которого заключается непосредственно в исследовании конечного веб-приложения на предмет угроз безопасности; агрегирующий, функции которого включают учет, хранение и обработку результатов.
Дальнейшее исследование выявило, что существует разнообразное количество готовых решений, которые могут выступать в качестве тестирующего и агрегирующего компонентов, однако не существует достаточно универсальных решений, способных выполнять обслуживающие функции, однако именно этот компонент является ключевым, поскольку он способен решить большую часть трудностей при организации процесса: доставку входных

данных, управление покрытием тестирования, управление сценариями тестирования, мониторинг, а также получение и подготовку результатов. Отсутствие подходящих готовых решений стало причиной создания собственного.
Разработанное решение представляет собой систему скриптов на языке программирования “Python 3”, выбор языка обусловлен достаточно низким порогом входа и высокой популярностью. Данное решение обладает гибкой модульной системой, позволяющей расширять возможности данного компонента под нужды конкретных компаний, а также легкой системой конфигурирования. В качестве тестирующего компонента была выбрана программа “Zed Attack Proxy” в виду того, что это решение с открытым исходным кодом, имеющее хорошо задокументированный программный интерфейс, различные режимы функционирования и возможность работы в виртуальной среде. В качестве агрегирующего компонента взято программное обеспечение “Defect Dojo” по следующим причинам: открытость исходного кода, большое наличие графического и программного интерфейсов, широкие возможности настройки параметров агрегирования и обработки загружаемых результатов.

Выводы. Описанные компоненты были объединены в единую систему управления процессом динамического тестирования безопасности веб-приложений, которая успешно показала себя в практических испытаниях и при внедрении в инфраструктуру компании, занимающейся разработкой собственного веб-приложения.
Данная система программных компонентов подробно задокументирована, разрабатывалась быть гибкой при внедрении и является полностью открытой, что означает возможность ее использования большинством компаний, нуждающихся в подобных решениях в области информационной безопасности.

Иванов А.А. (автор)

Кузнецов А.Ю. (научный руководитель)