Отзыв научного руководителя

на диссертационную работу Сигалова Даниила Алексеевича

«Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода»

представленную на соискание ученой степени кандидата технических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертационная работа Сигалова Д. А. посвящена разработке нового метода выявления поверхности атаки веб-приложений при помощи анализа программного кода на языке JavaScript клиентской части веб-приложений в рамках решения более широкой задачи анализа защищенности веб-приложений в модели черного ящика.

Начиная с конца 2000-х – начала 2010-х годов веб-технологии доминируют в качестве способа публикации приложений в интернете – большинство существующих и вновь разрабатываемых приложений используют стек веб-технологий для организации как минимум интерфейсной (фронтенд) части приложения, а серверные компоненты мобильных приложений также используют HTTP API для организации интерфейса между мобильным клиентом и серверной логикой приложения. Одновременно веб-приложения остаются «слабым звеном» в вопросе обеспечения информационной безопасности компаний, пользователей и данных. Так, по данным американской компании Verizon по меньшей мере с 2015 года по настоящее время уязвимости веб-приложений являются причиной номер один утечек данных в результате инцидентов безопасности. В частности, в 2023 году в 60% инцидентов, связанных с утечками данных, веб-приложения были способом проникновения злоумышленников внутрь защищаемого контура компаний. То есть, уже по меньшей мере в течение десяти лет индустрии не удается кардинально решить проблему наличия уязвимостей в веб-приложениях. Автоматизация поиска уязвимостей веб-приложений может помочь если не решить эту проблему, то хотя бы сделать её менее острой – за счет использования автоматизированных средств обнаружения уязвимостей в рамках цикла безопасной разработки программного обеспечения. Инструменты динамического анализа защищенности приложений – это предметная область диссертационной работы Сигалова Д. А.

При использовании динамического анализа для поиска уязвимостей в приложениях одной из ключевых проблем является проблема полноты выявления поверхности атаки, то есть обнаружения серверных точек доступа для взаимодействия между инструментом и анализируемым экземпляром приложения в процессе фаззинга и тестирования на уязвимости. Задача выявления поверхности атаки в современных веб-приложениях довольно сложна из-за

того, что клиентская часть приложений давно не ограничена одним лишь языком разметки HTML, а в большинстве случаев представляет собой программу на языке программирования JavaScript, зачастую минифицированную для уменьшения размера или даже обфусцированную для затруднения анализа. Традиционные методы выявления поверхности атаки с помощью обхода интерфейса «по ссылкам» (статический краулинг) или с помощью визуального обхода интерфейса управляемым браузером (динамический краулинг) далеко не всегда эффективны – они ограничены только теми элементами, которые отображаются в интерфейсе, при этом текст клиентской программы на JavaScript может содержать большое число скрытых для такого обхода функций, которые могут отправлять запросы на сервер при совершенно конкретных пользовательских действиях, которые трудно воспроизвести автоматически в инструменте. Также клиентский код может содержать недостижимый или закомментированный программный код, содержащий информацию о серверных точках доступа и потенциально выполнимых запросах с клиента на сервер – такие функции принципиально недостижимы для любых методов обхода интерфейса.

В рамках диссертационной работы Сигалов Д. А. предложил специализированный метод выявления поверхности атаки веб-приложений на основе статического анализа программного кода на языке JavaScript клиентской части приложений. В рамках непосредственно самого исследования, и в рамках подготовки текста диссертационной работы Сигалов Д. А. системно и методично решал поставленные задачи, и провел обширное экспериментальное исследование – как особенностей современных программ на языке JavaScript, характерных для клиентской части веб-приложений, так и собственно эффективности предложенного метода для решения задачи выявления поверхности атаки и обнаружения уязвимостей в веб-приложениях. Сигалов Д. А. предложил методику использования предложенного метода выявления поверхности атаки для решения общей задачи обнаружения уязвимостей веб-приложений на основе расширения признанных в индустрии методик исследования приложений на уязвимости этапами выявления поверхности атаки с помощью статического анализа клиентских программ и фаззинга выявленных таким способом серверных точек доступа для обнаружения уязвимостей в серверной части приложений. Предложенный метод реализован и используется в составе инструмента динамического анализа защищенности веб-приложений SolidPoint DAST, который разрабатывается ООО СолидСофт, а также в составе системы динамического анализа защищенности веб-приложений на основе анализа больших данных, созданной в рамках НИР центра НТИ по технологиям хранения и анализа больших МГУ (ЦХАБД МГУ).

Таким образом, полученные Сигаловым Д. А. результаты показали свою эффективность и практическую ценность и могут быть использованы как в составе автоматизированных инструментов поиска уязвимостей веб-приложений, так и при ручном поиске уязвимостей квалифицированными специалистами по анализу защищенности приложений.

Полученные диссертантом результаты были опубликованы в авторитетных изданиях и обсуждались как на российских, так и на зарубежных профильных конференциях.

Считаю, что диссертационная работа соответствует всем требованиям, предъявляемым ВАК РФ к работам на соискание ученой степени кандидата технических наук по специальности 2.3.5 – математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей, а её автор, Сигалов Даниил Алексеевич, заслуживает присуждения ему учёной степени кандидата технических наук.

Научный руководитель:
доцент факультета ВМК МГУ, к.ф.-м.н. Гамаюнов Д. Ю.

8 июля 2025 года