ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Сигалова Даниила Алексеевича
по теме «**Методы выявления поверхности атаки веб-приложений при помощи анализа клиентского JavaScript-кода**»,
представленную к защите на соискание ученой степени кандидата технических наук по научной специальности 2.3.5 – «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей»

Актуальность темы

Возрастающая сложность и размеры программ неизбежно приводят к появлению в них ошибок. Последствия возникновения ошибок особенно серьёзны в случаях, когда вследствие возникновения ошибки в программе возникает уязвимость. Борьба с уязвимостями является важной задачей, и отдельного внимания заслуживают уязвимости веб-приложений. Помимо их широкого распространения, веб-приложения часто публично доступны для взаимодействия через сеть Интернет, в то время как их серверная часть находится внутри инфраструктуры организации, которой принадлежит приложение. Зачастую именно компрометация веб-приложения являлась первым шагом в успешной атаке злоумышленников на компанию. Кроме того, веб-приложения пропускают через себя и хранят большие объёмы пользовательских данных, включая личные данные, такие, как номера банковских карт. При этом задача своевременного выявления и исправления уязвимостей веб-приложений остаётся нерешённой, в результате чего даже такие давно известные, классические уязвимости, как SQL-инъекции, по сей день встречаются в реальных веб-приложениях (что подтверждается и экспериментами, проведёнными в диссертационной работе). Таким образом, работа Сигалова Д. А., имеющая своей целью повысить качество работы методов выявления уязвимостей веб-приложений путём повышения полноты выявления анализируемых на наличие уязвимостей серверных функций, *является актуальной*.

Структура работы

Диссертация содержит 133 страницы текста, который состоит из введения, четырёх глав, заключения, списка литературы (89 источников), а также приложения. Текст работы содержит 6 рисунков и 3 таблицы.

Во введении обосновывается актуальность диссертационной работы, формулируются цели, задачи работы, научная новизна и практическая значимость, а также приводятся основные положения, выносимые на защиту.

Первая глава посвящена исследованию задачи и обзору литературы и программных средств, имеющих непосредственное отношение к теме диссертации. Глава содержит сравнение существующих методов выявления поверхности атаки.

Вторая глава посвящена изучению особенностей реального JavaScript-кода, которые влияют на возможность его анализа для выявления серверных входных точек.

Рассматриваются распространённые особенности, присущие реальному коду, которые затрудняют его анализ и требуют особого внимания при создании инструментов для анализа. На основе выявленных особенностей в главе определяются требования к инструментам, предназначенным для построения поверхности атаки с использованием статического анализа клиентского JavaScript-кода. Кроме того, в главе описывается созданный по результатам исследования бенчмарк, который может быть применён для автоматизированной оценки эффективности методов обнаружения серверных входных точек.

Третья глава описывает методику поиска уязвимостей веб-приложений в модели «чёрного ящика» с использованием статического анализа клиентского JavaScript-кода. Методика основана на OWASP Web Security Testing Guide (WSTG) версии 4.2 и охватывает как сбор информации об анализируемом приложении, так и проверку приложения на наличие уязвимостей. На этапе сбора информации выполняется статический и динамический анализ для поиска серверных входных точек, а также анализ HTML-разметки и некоторые другие методы. Далее обнаруженные входные точки проверяются на уязвимости, такие как SQL injection, Reflected XSS и другие. Предлагается также анализировать клиентский JavaScript-код для выявления проблем, включая DOM-based XSS и утечки данных. Методика успешно применена на реальных веб-приложениях в рамках Bug Bounty программ, где обнаружен ряд уязвимостей. Выводом по итогам главы стало то, что использование статического анализа клиентского кода повышает эффективность поиска уязвимостей, позволяя выявить новые серверные входные точки.

В четвёртой главе описан предлагаемый метод анализа клиентского кода веб-приложения для обнаружения серверных входных точек. Глава содержит высокоуровневое описание метода и графическую схему его устройства, описание предлагаемого алгоритма статического анализа клиентского JavaScript-кода, приведены особенности его программной реализации. Кроме того, в главе описаны несколько экспериментов с разработанным методом. Проведены два эксперимента на тестовых данных: один эксперимент на бенчмарке, разработанном в рамках диссертационной работы, и один на тестовых приложениях, которые были известны ранее и использовались в экспериментах, описанных в существующих работах. Также в главе содержится описание проведённых экспериментов с сайтами из сети Интернет, в результате которых были обнаружены реальные уязвимости.

В заключении диссертации приводятся основные результаты и выводы проведенной работы.

Основные результаты работы

К основным результатам, полученным Сигаловым Д. А. в ходе выполнения диссертационного исследования, следует отнести:

1. Особенности реального JavaScript-кода, выделенные по результатам исследования, а также требования к средствам статического анализа клиентского JavaScript-кода и разработанный бенчмарк, позволяющий тестировать инструменты статического анализа клиентского кода в автоматическом режиме.

2. Методика поиска уязвимостей в веб-приложениях, при применении которой повышение полноты выявления серверных входных точек обеспечивается за счет статического анализа клиентской части приложения.
3. Метод анализа клиентского кода веб-приложения для выявления серверных входных точек. Метод использует алгоритм статического анализа, при разработке которого учтены выявленные особенности реального кода.
4. Инструмент, представляющий собой реализацию предложенного метода, внедрённый в реальные системы автоматизированного поиска уязвимостей. С разработанным инструментом были проведены эксперименты на сайтах в сети Интернет, в результате которых были обнаружены реальные уязвимости.

Научная новизна

Научная новизна результатов, представленных в диссертационной работе Сигалова Д.А., заключается в разработке алгоритма статического анализа клиентского JavaScript кода для выявления серверных входных точек с целью поиска в них уязвимостей, а также в выявлении характерных особенностей реального клиентского кода, которые необходимо учитывать при его статическом анализе, и в разработке на основе этих особенностей требований к средствам статического анализа клиентского кода для выявления поверхности атаки сервера. Результаты экспериментов показывают адекватную эффективность разработанного подхода, а также пригодность его для использования в составе систем автоматизированного поиска уязвимостей. Кроме того, новой является предложенная методика поиска уязвимостей веб-приложений, отличающаяся от существующих более полным обнаружением серверных входных точек, отправку к которым сложно вызвать через взаимодействие с пользовательским интерфейсом.

Замечания

1. При сравнении результатов работы инструментов на тестовых приложениях помимо сравнения количества найденных входных точек в тексте диссертации хотелось бы видеть оценку того, насколько совпадают наборы точек, найденных разными средствами. Для этого можно было бы сделать попарное сравнение наборов найденных точек с подсчётом количества точек, уникальных для каждого из инструментов в паре. Таким образом можно было бы получить представление о том, в какой степени результаты сравниваемых средств дублируют друг друга, а в какой - дополняют (что говорило бы о потенциальной пользе от использования сочетания из обоих средств).
2. Помимо JavaScript и HTML, существуют и другие способы реализации клиентов, взаимодействующих с сервером веб-приложения по протоколу HTTP. Клиентом может быть не только браузер, но и другое приложение, а в современных браузерах может выполняться код в формате WebAssembly (в этот формат может компилироваться код на языках C, C++, Rust и ряде других). В работе не указывается, применим ли разработанный метод для других технологий выполнения клиентского кода.

Заключение

Отмеченные замечания не снижают общей научной и практической ценности диссертационной работы и не влияют на её положительную оценку. Содержание диссертационной работы полно и правильно отражено в автореферате. Диссертация Д.А. Сигалова является законченной научно-исследовательской работой. Она отвечает всем требованиям ВАК РФ, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а Сигалов Даниил Алексеевич заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Официальный оппонент
кандидат физико-математических наук,
ведущий научный сотрудник отдела компиляторных технологий
Федерального государственного бюджетного учреждения науки
Институт системного программирования им. В.П.Иванникова
Российской академии наук

Курмангалеев Шамиль Фаимович

«8» сентября 2025 г.