УТВЕРЖДАЮ

Проректор по учебной работе РТУ МИРЭА

А.В. Тимошенко

«___» _____ 2024 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ
федерального государственного бюджетного образовательного учреждения высшего образования
«МИРЭА - Российский технологический университет»

на диссертацию 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

1. Оценка актуальности темы

Оценка уязвимости программного обеспечения является важным этапом его разработки и тестирования. Необходимо провести испытание на обеспечение целостности в условиях функционирования, недоступности закрытых данных, нечувствительности к разным системным настройкам и т. д. Это особенно важно для программных сервисов, реализуемых в форме веб-приложений, поскольку они имеют заданную структуру, доступность и прозрачность клиентской части кода, которые определяются браузерами, как средствами исполнения программ.

В ходе разработки программного обеспечения веб-сервисов появление ошибок и уязвимостей в создаваемых приложениях неизбежно. Отсутствие учета и устранение этих уязвимостей приводит к негативным последствиям, таким как утечки данных, недоступность приложений, нарушение качества веб-сервисов. Обнаружение максимального количества уязвимостей желательно до ввода программного обеспечения в эксплуатацию. Внедрение безопасного цикла разработки является требованием государственного стандарта по разработке безопасного программного обеспечения ГОСТ Р 56939. Одним из элементов цикла безопасной разработки, предписанных государственным стандартом, является динамический анализ программного обеспечения, включающий фаззинг-

тестирование. Для проведения фаззинг-тестирования веб-приложения необходимо выявление серверных входных точек – элементов поверхности атаки сервера веб-приложения, в которые и будут подаваться тестовые входные данные при динамическом анализе.

В этих условиях тема диссертации, посвященная разработке тестирующего программного обеспечения веб-сервисов в форме клиентского JavaScript-кода, направленного на выявление точек уязвимости по нарушению целостности и контроля доступа к данным распределенных программных систем, является актуальной задачей.

2. Оценка содержания диссертационной работы

Диссертация состоит из введения, 4 глав, заключения и 1 приложения. Полный объём диссертации составляет 133 страницы, включая 6 рисунков и 3 таблицы. Список литературы содержит 89 наименований.

Во введении обосновывается актуальность исследований, проводимых в рамках данной диссертационной работы, ставятся цели и задачи работы, формулируется научная новизна и практическая значимость представляемой работы, а также приводятся основные положения, выносимые на защиту.

В первой главе рассматривается задача выявления поверхности атаки веб-приложения при поиске в нём уязвимостей методом “чёрного ящика” и производится обзор существующих подходов. Приводится сравнение существующих методов выявления поверхности атаки. В главе отсутствуют разделы, связанные с оценкой состояния проблемы и четкие формулировки постановки решаемых задач.

Вторая глава посвящена исследованию технологических решений, применяемых разработчиками JavaScript-кода в реальных проектах разработки веб-сервисов, влияющих на возможность анализа и обнаружения серверных входных точек. Производится поиск наиболее часто применяемых решений, свойственных реальному коду, осложняющих его анализ, которые, таким образом, необходимо учитывать при разработке анализатора. Примерами выявленных технологических решений, которые требуется поддерживать, являются применение упаковщиков модулей и косвенных вызовов вкупе с передачей функций, как значений, в программе (применение так называемых “функций первого класса”). На основе характерных особенностей, выявленных в ходе исследования, в главе формулируются требования к инструментам построения поверхности атаки на основе статического анализа клиентского JavaScript-кода. Кроме того, в главе приводится описание разработанного по результатам исследования

бенчмарка, который может быть использован для автоматизированной оценки эффективности методов выявления информации о серверных входных точках.

В третьей главе содержится описание разработанной методики поиска уязвимостей веб-приложений в модели “чёрного ящика” с использованием статического анализа клиентского JavaScript-кода. Результаты апробированы в реальных системах автоматизированного поиска уязвимостей веб-приложений. Изложены действия, требуемые для проверки приложения на наличие уязвимостей с использованием собранной информации в соответствии с предложенной методикой. Приведены примеры применения описанной методики в реальных приложениях и выводы, сделанные на основе применения.

Четвёртая глава посвящена разработке программной реализации предлагаемого специализированного метода анализа клиентского кода веб-приложения для обнаружения серверных входных точек, описанию апробации реализованного метода с использованием составленного эталонного набора страниц и на наборе приложений, использовавшихся для сравнения. Приведено 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.

Текст диссертации логичен, содержит решение конкретных задач с использованием иллюстративных примеров и сопровождается вычислительными экспериментами с качественным описанием результатов.

3. Оценка научной новизны основных результатов

Автором выносятся на защиту три положения, обладающих научной новизной. Рассмотрим обоснованность каждого из выносимых положений.

«1. Проведено исследование реального кода JavaScript-приложений и выделены его наиболее существенные особенности с точки зрения статического анализа для поиска входных точек: использование упаковщиков модулей, использование непрямого объявления класса, обращение к полю объекта по вычисленному имени и другие. Учет выявленных особенностей позволил сузить задачу статического анализа и предложить более эффективный метод его выполнения.»

К сожалению, в представленной формулировке сложно выявить новизну, поскольку здесь не содержится того, что именно сделано впервые и чем отличается от альтернативных подходов. Выявление особенностей кода не является оригинальным; это довольно типовой набор, особенно в части «и

другие». В целом, это положение не является самостоятельным, а служит предварительным этапом к созданию оригинальной авторской методики или метода.

«2. Предложена методика поиска уязвимостей веб-приложений в модели “чёрного ящика”. Методика отличается от существующих повышением покрытия серверных входных точек, обращения к которым сложно вызвать через взаимодействие с пользовательским интерфейсом, за счет применения статического анализа и автоматизированного перебора имён параметров запроса, а также применением анализа кода клиентской стороны веб-приложения для обнаружения уязвимостей.»

Данное положение является основным результатом, обоснованным в диссертационном исследовании и имеющим научную новизну. Здесь совершенно справедливо не используется неудачное определение «атак», используемое в название диссертации, а говорится об «уязвимости». Однако некоторые термины могут быть скорректированы. Как правило, под «черным ящиком» понимают кибернетические динамические модели, а здесь используется «статический анализ». В диссертации на с. 15 указано, что «Статические методы способны анализировать весь код программы, независимо от того, достижим ли он, и насколько сложно добиться достижения того или иного участка кода при реальном запуске.».

«3. Предложен метод обнаружения информации о серверных входных точках для задачи анализа защищенности приложений методом “черного ящика” с помощью статического анализа клиентского кода. Для типичной страницы реального веб-приложения разработанный алгоритм анализа позволяет решить задачу обнаружения входных точек за несколько минут, что делает его пригодным для практического использования. Это достигается за счёт ограничения числа проходов по коду и добавления встроенной поддержки популярных JavaScript-библиотек, отправляющих запросы на сервер (позволяет не анализировать собственный код библиотек). Разработанный алгоритм анализирует весь код страницы, включая недостижимый код.»

В целом можно признать данный пункт обоснованным в диссертации и обладающим новизной. Формулировки требуют уточнений: 1) если «предложен метод», то откуда взялся «разработанный алгоритм»; 2) насколько ограничения по числу проходов влияют на качество выявленных уязвимостей; 3) каким образом анализируется «недостижимый код»; 4) что такое «типичная страница»; 5) чем метод отличается от аналогов; 6) почему в названии

диссертации «методы» во множественном числе, а в работе предлагается один метод?

Оценивая работу в целом, можно признать в положениях и выводах наличие научной новизны.

4. Значимость результатов для развития соответствующей отрасли науки

Результаты, выводы и рекомендации диссертации имеют существенное значение для развития математического и программного обеспечения веб-сервисов, в части автоматизации выявления уязвимостей клиентской части кода на этапе разработки программного обеспечения.

Теоретическая значимость заключается в разработке методики поиска уязвимостей веб-приложений на основе анализа серверных входных точек, обращения к которым сложно вызвать через взаимодействие с пользовательским интерфейсом, а также применением анализа кода клиентской стороны веб-приложения для обнаружения уязвимостей.

Практическая значимость результатов, изложенных в работе, состоит в том, что для веб-страниц с целью тестирования и обнаружения скрытых уязвимостей создается клиентский JavaScript-код со встроенной поддержкой популярных JavaScript-библиотек, отправляющих запросы на сервер.

5. Рекомендации по использованию результатов и выводов диссертации

Целесообразно продолжить теоретическую и практическую работу по совершенствованию тестирующего программного обеспечения веб-сервисов в форме клиентского JavaScript-кода, направленного на выявление точек уязвимости по нарушению целостности и контроля доступа к данным распределенных программных систем

Рекомендуется использовать результаты и выводы диссертации при создании информационного обеспечения веб-сервисов государственных служб и частных компаний, а также продолжить работу в направлении повышения универсальности с целью их широкого применения при тестировании программного обеспечения.

Результаты работы могут быть внедрены в коммерческие и государственные компании, использующие веб-интерфейсы для информационно-технологических и вычислительных систем.

6. Замечания по диссертационной работе

1. Пункт 1 Положений, выносимых на защиту (с. 8 диссертации), сформулированный как «требования к инструментам *построения* поверхности атаки», не соответствует заявленным в теме разработке *методам выявления* поверхности атак.

2. В автореферате работы, представленной по специальности 2.3.5 Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей не уделяется существенного внимания математическому обеспечению, хотя автор использует специализированные нотации и формализованные описания (с. 57-67 диссертации).

3. Предложенные алгоритмы не содержат оценок сходимости и принятых оценок сложности и ресурсной эффективности.

7. Заключение о соответствии диссертации критериям, установленным Положением о присуждении ученых степеней

Представленная диссертационная работа выполнена на высоком научно-техническом уровне и представляет собой законченную научно-квалификационную работу, в которой содержится решение научной задачи по разработке программного обеспечения веб-сервисов в форме клиентского JavaScript-кода, выявляющего скрытые уязвимости приложения, имеющей значение для развития соответствующей отрасли знаний — математического и программного обеспечение вычислительных систем, комплексов и компьютерных сетей. Что удовлетворяет требованиям п. 9. Положения о присуждении ученых степеней.

Положения, выносимые на защиту, апробированы и в достаточной мере освещены в научной печати, в том числе в изданиях из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени кандидата наук, обсуждены на международных научных конференциях. Автореферат отражает основные научные положения и выводы, сделанные в диссертации.

В целом, диссертационная работа соответствует критериям, предъявляемым к диссертациям на соискание ученой степени кандидата наук, установленным пп. 9-14 «Положения о присуждении ученых степеней», а ее автор, Сигалов Даниил Алексеевич, заслуживает присуждения ученой степени кандидата технических наук по научной специальности

2.3.5 «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей» на основании защиты.

Диссертационная работа и отзыв рассмотрены и утверждены на заседании кафедры КБ-14 «Цифровые технологии обработки данных» Федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА - Российский технологический университет» (протокол № 04/24-25 от 05 ноября 2024 года).

Заведующий кафедрой КБ-14
«Цифровые технологии обработки данных»
РТУ МИРЭА
кандидат технических наук, доцент И.А. Иванова

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет»
Адрес: 119454, ЦФО, г. Москва, Проспект Вернадского, д. 78
Телефон: +7 (499) 600-80-80
E-mail: rector@mirea.ru
Веб-сайт: https://www.mirea.ru/