

официального оппонента, доктора технических наук, профессора
МАЗИНА Анатолия Викторовича на диссертационную работу соискателя
ученой степени кандидата технических наук СИГАЛОВА Даниила Алексеевича,
выполненную на тему: «Методы выявления поверхности атаки веб-приложений
при помощи анализа клиентского JavaScript-кода» по специальности 2.3.5 —
«Математическое и программное обеспечение вычислительных систем,
комплексов и компьютерных сетей»

Актуальность диссертации

Автоматическое обнаружение серверных точек входа веб-приложений -
задача, активно исследуемая в области безопасности информационных систем.
Существующие подходы, как правило, опираются на динамический анализ,
используя технику динамического краулинга.

Эта методология, реализованная в инструментах вроде BackREST и Gelato
(Oracle Labs), XIEv и CHIEv (SBA Research), а также в разработках совместной
группы Университета Британской Колумбии и Делфтского технического
университета, подразумевает автоматизированное взаимодействие с веб-
интерфейсом при помощи управляемого браузера. Система имитирует действия
пользователя, записывая все HTTP-запросы, отправляемые на сервер.

Полученные данные затем анализируются для выявления уникальных URL-
адресов и API-эндпоинтов, представляющих собой точки входа.

Однако, динамический краулинг имеет существенные ограничения.

Во-первых, сложность веб-приложения может быть настолько высока, что
полный перебор всех возможных пользовательских действий станет
непрактичным из-за экспоненциального роста числа комбинаций.

Времени на анализ может потребоваться неприемлемо много, особенно для
крупных и сложных приложений с динамически генерируемым контентом,
использованием AJAX-запросов и интенсивным взаимодействием с JavaScript.
Вторая проблема связана с наличием "недостижимого" кода.

Часть JavaScript-функций, отправляющих запросы к серверным точкам
входа, может быть вызвана не через пользовательский интерфейс, а, например,

через события, таймеры, или внутренние механизмы приложения.

Такой код может быть критически важным с точки зрения безопасности, ведь он может содержать уязвимости, не обнаруживаемые при поверхностном анализе интерфейса.

Например, функция, активирующаяся при определенном событии в фоновом режиме или при выполнении специфического условия, может обходить стандартные механизмы авторизации и допускать несанкционированный доступ.

Поэтому актуальна разработка методов, выходящих за рамки чисто динамического анализа. Перспективным направлением является статический анализ клиентского JavaScript-кода.

Диссертационная работа Сигалова Даниила Алексеевича, 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., является, несомненно, актуальной.

Характеристика научных результатов диссертации

На основе глубокого понимания состояния и перспектив проблематики в области автоматизации выявления поверхности атаки и инструментов динамического анализа защищенности приложений соискатель верно сформулировал научную задачу диссертации, цель исследования и аргументировано выстроил ряд частных, логически связанных исследовательских задач, обеспечивающих достижение цели.

В ходе проведения исследований по теме диссертационной работы автор получил ряд результатов, обладающих научной новизной и практической значимостью и выдвигаемых для публичной защиты.

Во-первых, это требования к инструментам построения поверхности атаки на основе статического анализа клиентского JavaScript-кода и методика использования разработанного метода для обнаружения уязвимостей в веб-приложениях.

Методика апробирована в реальных системах автоматизированного анализа защищенности приложений.

Во-вторых, это специализированный метод анализа клиентского кода веб-приложения для обнаружения серверных входных точек для последующего поиска в них уязвимостей.

Метод разработан с учётом особенностей реального кода, отправляющего запросы на сервер, выявленных в ходе проведённого исследования.

Проведена апробация реализованного метода с использованием составленного эталонного набора страниц, а также на наборе приложений, использовавшихся для сравнения в предыдущих работах.

Кроме того, проведены эксперименты с реализацией метода на сайтах в сети Интернет, в результате которых были обнаружены реальные уязвимости.

В целом, теоретическая значимость диссертации заключается в развитии методов автоматического выявления набора серверных входных точек посредством анализа клиентской части веб-приложения, основанного на специализированном статическом анализе клиентского JavaScript-кода.

Практическая значимость результатов диссертационных исследований обусловлена возможностью применения её результатов в анализе защищенности реальных систем, метод позволяет более полно выявлять элементы поверхности атаки — анализируемые наличие уязвимостей серверные входные точки, — тем самым, увеличивая количество обнаруживаемых уязвимостей.

Достоверность и обоснованность разработанного научно-методического аппарата подтверждается корректностью и логической обоснованностью рассмотренных вопросов, принятых допущений и ограничений, кроме того, подтверждается экспериментальными результатами, успешным внедрением результатов работы, что отражено в акте внедрения.

В диссертационной работе Сигалов Даниил Алексеевич предложил специализированный метод выявления поверхности атаки веб-приложений на основе статического анализа программного кода на языке JavaScript клиентской части приложений.

Замечания по диссертации

1. Кроме веб-страниц, использующих JavaScript-код, в качестве клиентов для веб-приложений выступают мобильные приложения (прежде всего это

приложения для операционных систем "Android" и "iOS").

Мобильные приложения зачастую реализованы не на JavaScript, а на Java, Objective-C, Swift и ряде других.

В работе не упоминается этот вид клиентских приложений, а также вопрос возможности и целесообразности анализа мобильных приложений с целью выявления поверхности атаки.

2. Страницы веб-приложений часто содержат сторонний JavaScript- код, который может отправлять запросы к сторонним веб-сервисам, не принадлежащим владельцам основного веб-приложения (часто это вебаналитика).

С точки зрения анализа, на предмет наличия уязвимостей, сторонние сервисы могут быть неинтересны, более того, передача информации о сторонних сервисах сканирующим модулям и фаззинг этих сервисов может быть нежелателен.

В работе не упоминается такой "лишний" код и вопрос об обеспечении того, чтобы сторонние сервисы не сканировались.

3. В работе не указано, какие ресурсы необходимы для реализации поставленных задач.

4. В работе не приводится экономическое обоснование применения разработанной методики.

В целом, отмеченные недостатки не носят принципиального характера и не наносят существенного ущерба значимости результатам диссертационной работы, выполненной на хорошем научном уровне.

Основные выводы и результаты диссертационного исследования достаточно широко опубликованы в научных изданиях и докладывались на представительных научно-технических конференциях, где получили одобрение научной общественности, признающей авторитет автора в разработке вопросов, положенных в основу диссертационной работы.

Соискатель по теме диссертации имеет 14 опубликованных научных работ, в том числе: 9 научных статьи (4 статьи индексируемых Web of Science и Scopus, 5 статей в изданиях из Перечня ВАК,) 5 докладов на конференциях.

Получено 1 свидетельство о регистрации программы для ЭВМ.

Содержание автореферата соответствует основным результатам работы и позволяет вынести обоснованное представление обо всей диссертации в целом.

Содержание диссертации полностью соответствует паспорту специальности 2.3.5 - «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

ВЫВОДЫ

1. Представленная диссертация является законченной научно-квалификационной работой, содержащей решение актуальной научной задачи - разработка метода автоматического выявления поверхности атаки вебприложений с динамической клиентской частью, реализованной на языке программирования JavaScript.

2. По актуальности тематики, глубине проводимых исследований и значимости полученных результатов диссертация полностью удовлетворяет требованиям п.п. 9 (абз.2), 10, 11, 13, 14 «Положения о присуждении ученых степеней», а её автор, Сигалов Даниила Алексеевича, 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:

заведующий кафедрой «Защита информации» Калужского филиала Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана» (национальный исследовательский университет), доктор технических наук, профессор

А.В. Мазин

2 сентября 2025 года

Сведения об оппоненте: Анатолий Викторович Мазин, д.т.н., профессор,

Калужский филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Московский

государственный университет имени Н.Э. Баумана» (национальный технический исследовательский университет). Юридический адрес: 248000, г. Калуга, ул. Баженова, д. 2. Телефон: (4842) 74-40-32, Факс: (4842) 56-30-45

E-mail организации: mail@bmstu-kaluga.ru Сайт организации: <http://bmstu-kaluga.ru>