ФГБОУ ВО «Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Кафедра информационной безопасности

«Моделирование автоматизированной системы тестирования безопасности WEB приложений на основе методики OWASP»

Выполнил: студент группы УИБ25-2м факультета информационных технологий и анализа больших данных Финансового университета при Правительстве Российской Федерации

Матевосян Гурген Арменович

Научный руководитель: доцент, кандидат технических наук

Бонч-Бруевич Андрей Михайлович

АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Актуальность исследования

В условиях стремительной цифровизации экономики и общества веб-приложения становятся критически важной инфраструктурой для бизнеса, государственных услуг и коммуникаций. Параллельно с этим наблюдается экспоненциальный рост количества и изощренности кибератак, нацеленных на уязвимости прикладного уровня. По данным последних отчетов, такие атаки, как инъекции, межсайтовый скриптинг и нарушения контроля доступа, десятилетиями остаются в топе угроз, нанося многомиллиардный ущерб.

ОБЪЕКТ И ПРЕДМЕТ ИССЛЕДОВАНИЯ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Объект исследования – процесс тестирования безопасности веб-приложений на предмет наличия уязвимостей.

Предмет исследования – методы и средства автоматизации тестирования безопасности веб-приложений на основе методики OWASP с применением больших языковых моделей

ЦЕЛИ И ЗАДАЧИ ИССЛЕДОВАНИЯ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Цель исследования – разработать модель и программный прототип автоматизированной системы тестирования безопасности веб-приложений, интегрирующей методику OWASP Testing Guide, инструменты анализа и генеративные возможности LLM для повышения эффективности и полноты проверок.

Задачи исследования

- Анализ OWASP Testing Guide Checklist
  - Сравнение подходов OWASP с Российскими нормативными документами и методическими рекомендациями
- Выбор инструментов анализа и тестирования WEB приложений
  - Разработка промтов для LLM, обеспечивающих автоматизацию выполнения анализа
  - Разработка программного комплекса и агентной модели для тестирования уязвимостей
- Тестирование разработанной системы, определение степени полноты анализа уязвимостей

ФИНУНИВЕРСИТЕТ
Кафедра информационной безопасности
(наименование кафедры)

УТВЕРЖДАЮ
Руководитель ВКР
Доцент, кандидат технических наук
(должность, уч. степень, уч.звание)
_____ А.М. Бонч-Бруевич
(подпись) (И.О. Фамилия)
«____» _____2025 г.

ПЛАН – ЗАДАНИЕ
на выпускную квалификационную работу[1]

обучающегося Матевосяна Гургена Арменовича
(фамилия, имя, отчество)

Тема выпускной квалификационной работы «Моделирование автоматизированной системы тестирования безопасности WEB приложений на основе методики OWASP»

закреплена приказом Финуниверситета от «17» декабря 2025 г. №3152/о.

Целевая установка:[2]
Разработать автоматизированную систему тестирования безопасности WEB-приложений на основе методики OWASP

План ВКР (основные вопросы, подлежащие исследованию и разработке):
1. Анализ OWASP Testing Guide Checklist
1.1. Сравнение подходов OWASP с Российскими нормативными документами и методическими рекомендациями
2. Выбор инструментов анализа и тестирования WEB приложений
2.1. Разработка промптов для LLM, обеспечивающих автоматизацию выполнения анализа
2.2. Разработка программного комплекса и агентной модели для тестирования уязвимостей
3. Тестирование разработанной системы, определение степени полноты анализа уязвимостей

Дополнительные рекомендации руководителя ВКР по проведению исследования:

_____ Г.А. Матевосян
подпись обучающегося И.О. Фамилия обучающегося

[1] План-задание согласовывается руководителем с обучающимся и размещается обучающимся в личном кабинете на платформе не позднее 15 календарных дней с даты издания приказа о закреплении темы ВКР.
[2] Руководитель ВКР совместно с обучающимся может конкретизировать целевую установку задачами.

НАУЧНАЯ ГИПОТЕЗА

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Научная гипотеза исследования заключается в том, что использование агентной модели на базе LLM для координации тестирования безопасности позволяет достичь более высокого покрытия проверок OWASP и снизить уровень ложных срабатываний по сравнению с использованием изолированных инструментов автоматизированного сканирования

ТЕОРЕТИЧЕСКАЯ И ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Теоретическая значимость заключается в формализации процесса интеграции международной методики тестирования (OWASP) и требований российского регулирования, а также в разработке модели агентно-управляемой системы автоматизированного тестирования с применением LLM.

Практическая значимость состоит в создании прототипа программного комплекса, который может быть использован разработчиками, тестировщиками безопасности и аудиторами для повышения эффективности и скорости проверок веб-приложений, формирования отчетов, соответствующих как техническим стандартам OWASP, так и российским нормативным требованиям.

РАЗРАБОТКА ПО

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

В рамках выпускной квалификационной работы планируется разработка мульти-агентной системы автоматизированного тестирования безопасности WEB-приложений на языке программирования c# в среде MS Visual Studio

Что предлагается

«MAOI» — Мульти-агентный OWASP Иммунитет

Windows-приложение на C#, объединяющее MITM-прокси + браузерную автоматизацию + локальную LLM для реального поиска уязвимостей без ложных срабатываний

Ключевые особенности

- Родной .exe-файл — не нужны Java, Docker, Python
- Графический интерфейс — удобный и понятный
- Локальная LLM — код приложения не уходит в облако
- Автоматическая генерация PoC-эксплойтов

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СПАСИБО ЗА ВНИМАНИЕ!