

УДК 004.056.5

Э. К. СВИСТОВИЧ (ЭМ-21)

Научные руководители: старшие преподаватели *В. Е. МИНИН*,
С. С. ТАТУР

ИНСТРУМЕНТЫ ДЛЯ ПЕНТЕСТА ВЕБ-ПРИЛОЖЕНИЙ – BURP SUITE И OWASP ZAP

Проведён сравнительный анализ двух наиболее популярных инструментов для тестирования на проникновение веб-приложений: Burp Suite и OWASP ZAP. Рассмотрены их ключевые функциональные возможности, преимущества и ограничения. Обоснована целесообразность использования данных инструментов в зависимости от целей, задач и бюджета организации.

В условиях стремительной цифровизации веб-приложения становятся основным вектором кибератак. Согласно отчету OWASP Top 10, уязвимости на уровне приложений, такие как инъекции, ошибки криптографии и нарушения контроля доступа, остаются критическими угрозами информационной безопасности [1]. Для выявления и устранения данных уязвимостей на этапах разработки и эксплуатации широко применяется тестирование на проникновение (пентест). Ключевую роль в этом процессе играют специализированные программные комплексы, среди которых лидирующие позиции на рынке занимают Burp Suite и OWASP ZAP.

Burp Suite, разработанный компанией PortSwigger, является де-факто отраслевым стандартом для тестирования безопасности веб-приложений. Его архитектура построена вокруг прокси-сервера, который перехватывает и модифицирует HTTP/HTTPS-трафик между браузером тестировщика и целевым сервером. Ключевые компоненты Burp Suite включают:

- Proxu: основной инструмент для перехвата, просмотра и изменения запросов и ответов в реальном времени;
- Intruder: автоматизированный инструмент для подбора параметров (например, брутфорс паролей или фаззинг полей ввода);
- Repeater: позволяет вручную изменять и многократно отправлять отдельные HTTP-запросы для детального анализа реакции сервера;
- Scanner (в версии Professional): мощный автоматизированный сканер уязвимостей, способный выявлять широкий спектр проблем безопасности с минимальным количеством ложных срабатываний.

Важным аспектом является наличие двух версий: бесплатной Community Edition с ограниченным функционалом (например, отсутствие

автоматического сканера и искусственное ограничение скорости работы Intruder) и платной Professional Edition, предоставляющей полный набор возможностей для коммерческого использования [2].

OWASP ZAP (Zed Attack Proxy) – это инструмент с открытым исходным кодом, разрабатываемый и поддерживаемый международным фондом OWASP. Он позиционируется как доступная и мощная альтернатива коммерческим решениям, идеально подходящая как для начинающих специалистов по безопасности, так и для интеграции в процессы непрерывной интеграции и доставки (CI/CD). Основные возможности OWASP ZAP:

- автоматический сканер: выявляет известные уязвимости (например, XSS или SQL-инъекции) с минимальным вмешательством пользователя;
- Fuzzer: инструмент для отправки модифицированных данных в различные части запроса с целью выявления ошибок обработки ввода;
- HUD (Hears Up Display): инновационный интерфейс, позволяющий использовать возможности ZAP (перехват запросов, сканирование) непосредственно в браузере во время ручного тестирования;
- поддержка скриптов: возможность написания собственных скриптов на языках JavaScript, Python, Zest и других для расширения функциональности и автоматизации рутинных задач [3]. Главным преимуществом ZAP является его полная бесплатность, отсутствие ограничений по скорости сканирования и активное сообщество разработчиков, регулярно выпускающее обновления и новые плагины (add-ons).

Для выбора оптимального инструмента в рамках конкретной организации необходимо провести их сравнительный анализ по ключевым параметрам (таблица 1).

Таблица 1 – Сравнительный анализ Burp Suite Professional и OWASP ZAP

Критерий сравнения	Burp Suite (Professional)	OWASP ZAP
Тип лицензии	Проприетарная (платная)	Открытая (бесплатная, Open Source)
Автоматическое сканирование	Высокая точность, минимум ложных срабатываний, глубокий анализ	Хорошая базовая точность, но требует дополнительной тонкой настройки
Интеграция в CI/CD	Возможна через API, но требует приобретения дорогостоящей лицензии	Отличная, нативная поддержка, наличие готовых плагинов для Jenkins, GitLab и др.
Порог вхождения	Средний/высокий (требует понимания HTTP и логики приложений)	Низкий/средний (интуитивно понятный интерфейс, наличие режима обучения)
Расширяемость	VApp Store (огромная библиотека проверенных расширений)	Маркетплейс дополнений (активно развивается сообществом)

Таким образом, выбор между Burp Suite и OWASP ZAP зависит от конкретных задач, уровня подготовки специалистов и бюджета организации. Burp Suite Professional незаменим для глубокого ручного аудита, расследования сложных инцидентов и коммерческих пентестов благодаря своему удобному интерфейсу, стабильности и мощному автоматическому сканеру. В свою очередь, OWASP ZAP является идеальным решением для организаций с ограниченным бюджетом, государственных структур, а также для автоматизации проверок безопасности (DAST) в конвейерах CI/CD.

На практике наиболее эффективным подходом является использование комбинации обоих инструментов: OWASP ZAP для первичного автоматизированного сканирования и интеграции в процесс разработки и Burp Suite для углубленного ручного анализа выявленных аномалий и сложных бизнес-логик приложения. Такой комплексный подход позволяет обеспечить максимально полный охват потенциальных уязвимостей и повысить общий уровень защищенности веб-ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1 OWASP Top 10:2021. – URL: <https://owasp.org/www-project-top-ten/> (дата обращения: 10.05.2025).

2 Портсвиггер. Официальная документация Burp Suite. – URL: <https://portswigger.net/burp/documentation> (дата обращения: 10.05.2025).

3 OWASP ZAP. Официальный сайт проекта. – URL: <https://www.zaproxy.org/> (дата обращения: 10.05.2025).

4 Стоун, Д. Тестирование на проникновение веб-приложений: полное руководство / Д. Стоун. – М. : ДМК Пресс, 2023. – 415 с.

Получено 29.05.2026

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 338.32

Д. В. СЕДАЯ (ГБ-31)

Научный руководитель – ст. преп. *Т. В. ШОРЕЦ*

ОСОБЕННОСТИ ВЛИЯНИЯ АМОРТИЗАЦИОННОЙ ПОЛИТИКИ НА ПОКАЗАТЕЛИ ЭФФЕКТИВНОСТИ РАБОТЫ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Рассматриваются проблемы эффективности использования долгосрочных активов транспортными организациями Республики Беларусь. Предложен интегральный подход, объединяющий гибкую амортизационную политику, оценку эффективности