

возможности журналирования Windows и Linux соответственно, обеспечивая детализированную регистрацию событий, критичных для обнаружения атак. Практическое использование описанных инструментов в комплексе с системами SIEM позволяет автоматизировать выявление подозрительных паттернов и значительно сократить время реагирования на инциденты.

СПИСОК ЛИТЕРАТУРЫ

1 **Chuvakin, A.** Logging and Log Management: The Authoritative Guide / A. Chuvakin, K. Schmidt, C. Phillips. – Syngress, 2012. – 460 p.

2 **Russinovich, M.** Sysinternals Suite Documentation: Sysmon / M. Russinovich. – Microsoft Learn. – URL: <https://learn.microsoft.com/sysinternals/downloads/sysmon> (date of access: 03.04.2026).

3 Red Hat Enterprise Linux Security Guide: System // Red Hat Inc. – URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/ (date of access: 05.04.2026).

4 **Sanders, C.** Applied Network Security Monitoring: Collection, Detection, and Analysis / C. Sanders, J. Smith. – Syngress, 2014. – 496 p.

Получено 11.06.2026

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 31. Гомель, 2026

УДК 004.056.5

И. В. ЗАГОРЦЕВ (ЭМ-31)

Научный руководитель – ст. пр. *В. Е. МИНИН*

УЧЕБНЫЙ СТЕНД ПО ИЗУЧЕНИЮ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ

Рассмотрены методология и практика тестирования безопасности web-приложений на основе специализированной учебной платформы OWASP Juice Shop. На реальных сценариях атак проанализированы типичные уязвимости: межсайтовое выполнение скриптов (XSS), SQL-инъекции, атаки на JWT-токены, нарушения контроля доступа (Broken Access Control). Для каждого класса угроз представлены конкретные векторы эксплуатации с входными данными и ожидаемыми результатами.

Подготовка специалистов в области информационной безопасности требует практических навыков работы с реальными уязвимостями в контролируемой среде. OWASP Juice Shop – намеренно уязвимое web-приложение, представляющее собой полнофункциональный интернет-магазин, – является де-факто стандартом для обучения пентесту [1]. Все уязвимости класси-

фицированы по методологии OWASP Top 10, что обеспечивает соответствие учебного процесса актуальной отраслевой номенклатуре угроз.

Развертывание стенда выполняется единственной командой Docker: `docker run -d -p 3000:3000 bkimminich/juice-shop`. После запуска приложение доступно по адресу `localhost:3000`. Среда включает встроенную систему задач (Score Board) с более чем 100 заданиями различной сложности, автоматически фиксирующую факт успешной эксплуатации каждой уязвимости.

В таблице 1 приведены исследуемые классы уязвимостей.

Таблица 1 – Исследуемые уязвимости OWASP Juice Shop

Уязвимость	Описание
XSS	Внедрение вредоносных JavaScript-скриптов в страницы, просматриваемые другими пользователями
SQLi	Манипуляция запросами к БД через поля ввода, нарушающая логику SQL-запроса
NoSQLi	Атака на нереляционные БД (MongoDB) путем внедрения операторов запросов в формате JSON
JWT	Некорректная работа с токенами аутентификации: слабые секреты, отсутствие валидации подписи
Broken Access Control	Некорректная работа механизмов ограничения прав, позволяющая выполнять несанкционированные действия

XSS представляет собой класс уязвимостей, при которых злоумышленник внедряет выполняемый JavaScript-код в контент, отображаемый другим пользователям [2]. В OWASP Juice Shop атака реализована через строку поиска ввод `payload <iframe src="javascript:alert('xss')">` вызывает выполнение произвольного скрипта в контексте браузера жертвы.

Механизм атаки заключается в том, что приложение не выполняет очистку пользовательского ввода перед его отображением на странице, что позволяет встроить `iframe` с JavaScript URI. В результате отображается диалоговое окно с сообщением «xss», подтверждающее успешное выполнение инъекции. Практические последствия включают кражу сессионных cookie, перенаправление пользователей и фишинговые атаки.

SQL-инъекция позволяет манипулировать запросами к реляционной базе данных путем внедрения управляющих конструкций в поля ввода [3]. Классический вектор атаки на форму аутентификации Juice Shop: в поле email вводится `' OR 1=1--`, пароль – произвольный.

На стороне сервера формируется запрос `SELECT * FROM Users WHERE email=" OR 1=1--" AND password='...'`. Условие `OR 1=1` всегда истинно, а комментарий `--` нейтрализует проверку пароля. В результате атакующий получает доступ к учетной записи первого пользователя в базе данных – в данном случае администратора (`admin@juice-sh.op`).

NoSQL-инъекция направлена на нереляционные СУБД, использующие

JSON-подобный синтаксис запросов. В OWASP Juice Shop атака применяется для массового изменения отзывов, а после регистрации аккаунта и публикации легитимного отзыва злоумышленник перехватывает PATCH-запрос к конечной точке `/rest/products/reviews`.

Изменение `payload` запроса на `{"id":{"$ne":-1},"message":"Injected text"}` с использованием оператора MongoDB `$ne` (не равно) обновляет все отзывы одновременно. Условие `"$ne":-1` соответствует всем записям, поскольку идентификатор `-1` заведомо отсутствует в базе данных.

JWT – открытый стандарт передачи данных аутентификации в клиент-серверных приложениях [4]. Токен содержит три Base64-кодированных компонента: заголовок (алгоритм подписи), полезную нагрузку (данные пользователя) и подпись. В OWASP Juice Shop исследованы два вектора атаки.

Первый вектор – раскрытие конфиденциальных данных. Перехват ответа при авторизации предоставляет JWT, декодирование которого на `jwt.io` обнажает email, хеш пароля, роль и другие атрибуты учетной записи. Второй вектор – подмена идентификатора пользователя. С помощью JWT Editor в Burp Suite удаляется параметр `alg` из заголовка, а значение `id` в полезной нагрузке изменяется с 1 на 2. Измененный токен успешно аутентифицирует атакующего от имени другого пользователя.

Broken Access Control объединяет уязвимости, при которых механизмы ограничения прав функционируют некорректно. В OWASP Juice Shop исследованы два сценария на основе функции корзины покупателя.

Просмотр чужих корзин (IDOR). Подмена идентификатора в URL с `/rest/basket/1` на `/rest/basket/2` через Burp Suite Repeater предоставляет полное содержимое корзины другого пользователя без какой-либо проверки прав.

Добавление товаров в чужую корзину. Прямая замена параметра `BasketId` блокируется сервером, однако дублирование параметра в теле запроса (передача двух полей `BasketId` с разными значениями) обходит проверку: сервер использует второе значение, размещая товар в целевую корзину.

Тестирование продемонстрировало эффективность OWASP Juice Shop как инструмента для обучения вопросам кибербезопасности. Исследованные уязвимости – XSS, SQLi, NoSQLi, атаки на JWT и Broken Access Control – воспроизводимы при минимальном инструментарии (браузер, Burp Suite, Postman) и наглядно демонстрируют последствия отсутствия базовых механизмов защиты: очистки ввода, валидации токенов и проверки прав доступа на стороне сервера.

СПИСОК ЛИТЕРАТУРЫ

1 OWASP Juice Shop Project // OWASP Foundation. – URL: <https://owasp.org/www-project-juice-shop/> (date of access: 01.04.2026).

2 **Stuttard, D.** The Web Application Hacker's Handbook / D. Stuttard, M. Pinto. – 2nd ed. – Wiley, 2011. – 912 p.

3 **Clarke, J.** SQL Injection Attacks and Defense / J. Clarke. – 2nd ed. – Syngress, 2012. – 561 p.

4 **Jones, M.** JSON Web Token (JWT) / M. Jones, J. Bradley, N. Sakimura // RFC 7519. – IETF, 2015. – URL: <https://www.rfc-editor.org/rfc/rfc7519> (date of access: 02.04.2026).

Получено 69.003.2:658.14/.17

ISSN 2227-1155. Сборник студенческих научных работ.

Вып. 31. Гомель, 2026

УДК 69.003.2:658.14/.17

Я. А. ЗЕЛЕНКО (ПСм-32), Д. С. ЗЕМЛИН (ПСм-31)

Научный руководитель – канд. техн. наук *З. Н. ЗАХАРЕНКО*

ФИНАНСИРОВАНИЕ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ

Строительный комплекс традиционно выступает одним из ключевых драйверов экономического роста Республики Беларусь, обеспечивая воспроизводство основных средств и создание комфортной среды для жизни граждан. Однако специфика строительной деятельности (высокая капиталоемкость, длительные сроки окупаемости и значительные риски незавершенного производства) выдвигает проблему финансирования на первый план.

Финансирование строительной отрасли Республики Беларусь представляет собой сложный многоуровневый механизм, сочетающий рыночные инструменты с доминирующей ролью государственного регулирования и прямых бюджетных вливаний. Для понимания логики инвестиционных потоков в строительстве необходимо четко разграничивать источники по их происхождению и целевому назначению.

Традиционно в экономике строительства выделяют три ключевых блока: собственные средства организаций, привлеченные (заемные) средства и бюджетное финансирование.

Детальная классификация направлений финансирования в рамках Государственной инвестиционной программы ГИП-2025.

1 Транспортная инфраструктура (более 80 % вложений через госпрограммы – наиболее капиталоемкое направление. Государство финансирует проекты, которые бизнес не может осилить самостоятельно из-за длительных сроков окупаемости.

Конкретные примеры из Указа № 49: мостовые переходы: строительство