

## ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ ПУТЕМ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ С ПОМОЩЬЮ НЕСКОЛЬКИХ СКАНЕРОВ УЯЗВИМОСТЕЙ

**Н.О. Панков**, магистрант

**МИРЭА – Российский технологический университет**  
(Россия, г. Москва)

DOI:10.24412/2500-1000-2025-3-1-221-224

***Аннотация.** Безопасность веб-приложений представляет собой комплекс действий, направленных на защиту веб-сайтов, API приложений от атак. Это достаточно широкая предметная плоскость, но в то же время ее главной целью является поддержка бесперебойного функционирования веб-приложений и защита компаний от киберпреступности, неэтичной конкуренции, кражи данных и их искажения, а также других негативных последствий. Вследствие глобального характера Интернета веб-приложения подвергаются атакам с различных направлений, они могут иметь широкий масштаб и высокую сложность. Вследствие этого поддержка безопасности веб-приложений охватывает многие звенья цепочки разработки программного обеспечения и опирается на целый ряд стратегий. В данном контексте, особого внимания заслуживает автоматизированное тестирование на проникновение с помощью нескольких сканеров уязвимостей. В статье рассмотрены различные подходы к интеграции и комбинации автоматических проверок веб-приложений.*

***Ключевые слова:** сканер, комбинация, атака, проверка, веб-приложение.*

В сегодняшнюю цифровую эпоху веб-приложения являются основой многих предприятий, компаний и государственных учреждений, поддерживая и управляя огромным массивом конфиденциальной информации, начиная от личных данных и финансовых записей до критически важных бизнес-сведений.

В свете вышеизложенного последствия нарушения безопасности веб-приложений могут быть катастрофическими. Сегодня на предприятиях и организациях лежит большая ответственность за хранение конфиденциальной личной и финансовой информации, а также интеллектуальной собственности [1]. Значение защиты таких данных трудно переоценить, поскольку их раскрытие может привести к краже персональной информации, финансовому мошенничеству и тяжелым последствиям для жертв этих атак. Кроме того, предприятие может столкнуться со штрафами и судебными исками, а также с репутационным ущербом, который неизбежно нанесет взлом, что повлияет на будущий бизнес или вовсе помешает ему. По прогнозам, среднегодовой ущерб от киберпреступности и атак на веб-приложения в 2027 году составит более

23 трлн. дол. по сравнению с 8,4 трлн. дол. в 2022 году [2].

Для защиты информации используются стандартные процедуры и структурированные, хорошо документированные подходы. Также специалисты следят за тем, чтобы при работе с веб-приложениями соблюдались правила и нормы безопасности. Тесты на проникновение, среда разработки программного обеспечения для обеспечения безопасности и процессы обеспечения безопасности – вот лишь некоторые из регламентированных процессов.

Однако, несмотря на это, злоумышленники считают веб-приложения приоритетными целями по ряду следующих причин:

- высокая стоимость вознаграждения, включая конфиденциальные частные данные, полученные в результате успешной манипуляции исходным кодом;
- простота выполнения, поскольку большинство атак можно легко автоматизировать и запускать против тысяч, десятков или сотен тысяч целей одновременно;
- сложность исходного кода, которая повышает вероятность обнаружения уязвимостей и манипулирования вредоносным кодом.

В связи с этим обнаружение уязвимостей веб-приложений до того, как произойдет кибератака, является актуальной и критически важной на сегодняшний день задачей. В контексте вышеизложенного следует отметить, что поскольку угрозы кибербезопасности становятся все более распространенными, команды разработчиков, которые полагаются только на один тип тестирования веб-приложения, делают свои программы уязвимыми для атак. Чтобы добиться успеха, целесообразно выходить за рамки наиболее распространенных методов тестирования и использовать комплексный, интегрированный подход.

Таким образом, необходимость более детального освещения данных вопросов определила выбор темы данной статьи.

Эффективность различных сканеров, которые используются для оценки уязвимостей и тестирования на проникновение веб-приложений изучают Долгачев М.В., Москвичев А.Д., Москвичева К.С., Яровой Р.В., Ashish Virendra Chandak, Niranjana Kumar Ray.

Над разработкой многофункциональных инструментов проверки безопасности приложений трудятся Ковалева О.А., Самохвалов А.В., Ляшков М.А., Пчелинцев С.Ю., Atchara Meenasantirak, Chalee Siripitakchai, Natthawut Suriya, Kavita Bhatia, Santosh K. Pandey.

Проведенный анализ позволяет отметить, что в области тестирования безопасности веб-приложений было проведено множество исследований. Однако некоторые вопросы требуют более детальной проработки и анализа. Так, например, с развитием технологий искусственного интеллекта отдельного внимания заслуживают передовые практики обеспечения безопасности приложений. Кроме того, в уточнении нуждаются критерии выбора инструментов сканирования веб-приложений на уязвимости с учетом потребностей пользователей.

Таким образом, цель статьи заключается в рассмотрении перспектив повышения безопасности веб-приложений путем автоматизированного тестирования на проникновение с помощью нескольких сканеров уязвимостей.

**Результаты исследования.** Сканеры для тестирования уязвимостей – это программные приложения или сервисы, призванные помочь

организациям выявить и оценить слабые места в веб-приложениях. Эти инструменты автоматизируют процесс тестирования уязвимостей, делая его более эффективным, точным и последовательным [3]. С ростом доступности современных хакерских инструментов у субъектов угроз появились мотивация, возможность и потенциал для проведения автоматизированных атак. Аналогичным образом, автоматизированный подход стал недавней тенденцией в области тестирования веб-приложений на проникновение, поскольку он исключает человеческий фактор и обеспечивает экономичное по стоимости и времени решение для создания подробных отчетов об уязвимостях.

В данном контексте актуализируется вопрос каким образом можно улучшить показатели обнаружения уязвимостей путем разработки автоматизированной системы, объединяющей результаты нескольких сканеров в единый отчет об уязвимостях. Решая эту задачу, специалисты в области кибербезопасности предлагают несколько подходов. Рассмотрим их более подробно.

#### *Распределенное тестирование*

Распределенное тестирование – это метод тестирования уязвимостей, который предполагает использование нескольких инструментов или систем тестирования, часто развернутых в разных местах, для сканирования и анализа приложения на предмет наличия уязвимостей. Такой подход позволяет получить более полное представление о состоянии безопасности объекта, поскольку помогает выявить уязвимости, которые могут быть видны только из определенных мест или при определенных условиях. Распределенное тестирование также дает возможность распределить нагрузку при тестировании уязвимостей, снижая воздействие на целевую систему и повышая эффективность процесса тестирования [4].

Примеры распределенного тестирования включают:

1. Использование нескольких сканеров уязвимостей из разных мест для сканирования веб-приложения на предмет потенциальных дефектов безопасности.

2. Координация работы группы тестировщиков в разных географических точках для

одновременного тестирования уязвимостей сети.

В качестве примера данного подхода можно привести использование нескольких сканеров уязвимостей, таких как Clair и IBM Vulnerability Advisor, в разных точках конвейера. Лучшей схемой в таком сценарии является применение сканера с открытым исходным кодом, такого как Clair, в качестве части конвейера CI/CD и использование другого сканера уязвимостей для реестра образов.

*Комбинация статического (SAST) и динамического (DAST) тестирования безопасности*

В то время как инструменты SAST анализируют код в состоянии покоя, что дает возможность обнаружить недостатки безопасности до развертывания, DAST моделирует атаки на работающие приложения. Это позволяет определить уязвимости, которые проявляются только во время выполнения. В совокупности DAST и SAST обеспечивают реализацию комплексного подхода к тестированию безопасности, который охватывает как анализ кода до его развертывания, так и оценку уязвимостей и угроз после развертывания.

Чтобы обеспечить максимальную безопасность программного приложения, целесообразным является интеграция инструментов

SAST и DAST в конвейер CI/CD. DevSecOps призван использовать обе методологии для интеграции безопасности на каждом этапе разработки. Это даст возможность командам интегрировать средства контроля в процесс проектирования без ущерба для производительности [5]. Однако SAST и DAST – не единственные методы тестирования безопасности, которые рекомендуется комбинировать в процессе анализа уязвимостей веб-приложений. Сообщество разработчиков также рекомендует использовать вариации, включающие интерактивное тестирование безопасности приложений, самозащиту приложений в процессе выполнения, тестирование безопасности гибридных приложений.

*Комбинация Arachni и OWASP ZAP*

Инструменты Arachni и OWASP ZAP широко используются в сфере кибербезопасности. Об их эффективности неоднократно упоминалось в комплексных исследованиях. Открытый исходный код Arachni и OWASP ZAP повышает прозрачность и возможности совместного использования этих инструментов [6].

При высокоуровневом обзоре архитектуры система работает на основе взаимодействия трех основных компонентов, как показано на рисунке.

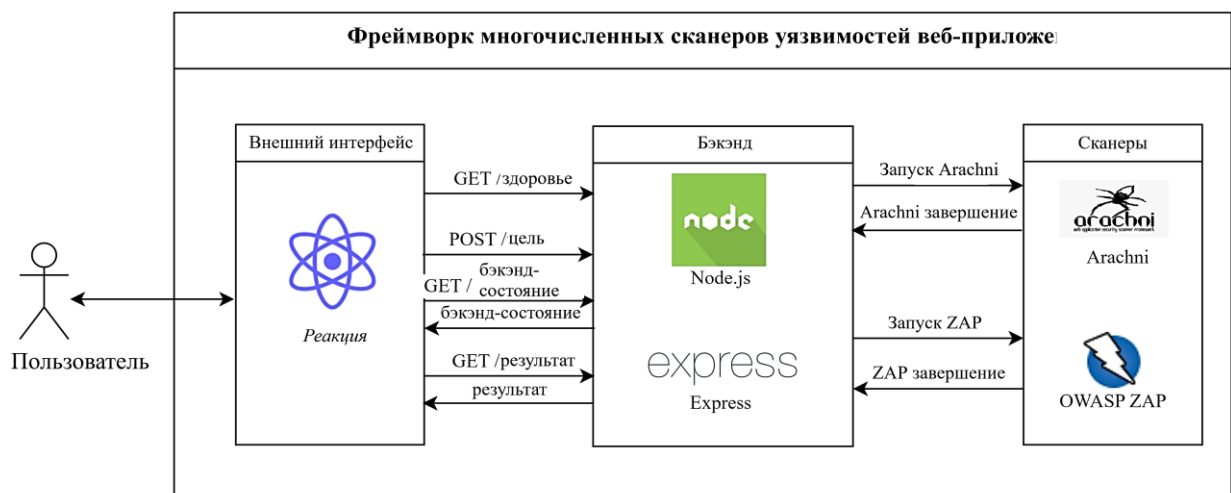


Рисунок. Схема структуры автоматизированного тестирования веб-приложений с помощью нескольких сканеров уязвимостей

Пользователь связывается с внешним веб-приложением, которое позволяет ему взаимодействовать с внутренними API с помощью внешнего интерфейса. Пользователю не нужно понимать, как запустить Arachni или

OWASP ZAP, поскольку вся эта логика управляется фреймворком. Ему необходимо только заполнить поле ввода для цели и нажать кнопку запуска.

Получив HTTP-запросы от внешнего сервера, внутренний сервер запускает сканеры уязвимостей веб-приложений для выполнения необходимых задач сканирования. Затем внутренний модуль запускает сканеры для проверки указанной цели и генерирует результаты. После этого бэкэнд возвращает эту информацию на фронтэнд, позволяя пользователям просматривать и анализировать результаты. Такое взаимодействие между внешним и внутренним модулями и сканерами уязвимостей веб-приложений обеспечивает удобство работы.

**Заключение.** Таким образом, большинство инцидентов безопасности, связанных с веб-приложениями, возникают из-за неисправленных ошибок, которые эксплуатируются современной сложной средой ИТ-угроз. Для повышения уровня защиты и предупреждения утечки данных целесообразным является применение автоматизированного тестирования на проникновение с помощью нескольких сканеров уязвимостей. В статье рассмотрено несколько вариантов совмещения и комбинации автоматических проверок.

### Библиографический список

1. Юдова Е.А. Анализ возможностей использования технологий машинного обучения для выявления атак на веб-приложения // International Journal of Open Information Technologies. – 2022. – Т. 10, № 1. – С. 61-68.
2. Bing Song. Design of Web Security Penetration Test System Based on Attack and Defense Game // Scientific Programming. – 2022. – Iss. 1. – P. 20-29.
3. Jesús-Ángel Román-Gallego, María-Luisa Pérez-Delgado. Artificial Intelligence Web Application Firewall for advanced detection of web injection attacks // Expert Systems. – 2023. – Vol. 42, Iss. 1. – P. 65-73.
4. Зегжда Д.П. Обнаружение атак на веб-приложения с использованием межсетевого экрана на базе сетей с долгой краткосрочной памятью // Методы и технические средства обеспечения безопасности информации. – 2023. – № 32. – С. 105-106.
5. Aref Shaheed. Web Application Firewall Using Machine Learning and Features Engineering // Security and Communication Networks. – 2022. – Iss. 1. – P. 87-93.
6. Bailin Xie. Application-Layer DDoS Attack Detection Using Explicit Duration Recurrent Network-Based Application-Layer Protocol Communication Models // International Journal of Intelligent Systems. – 2023. – Vol. 2023. – P. 23-29.

## INCREASING WEB APPLICATION SECURITY USING MULTI-VULNERABILITY SCANNER BASED AUTOMATED PENETRATION TESTING

**N.O. Pankov**, Graduate Student  
MIREA – Russian Technological University  
(Russia, Moscow)

**Abstract.** Web application security is a broad spectrum of methods for protecting websites, applications and APIs from attacks. Despite the fact that this is a very broad subject area, its main task is to implement and guarantee the smooth operation of web applications. Which will generally protect companies from cybercrime, data corruption and theft, unethical competition and other negative consequences. Due to the fact that the Internet has a global nature, web applications are confirmed to be attacked by various documents at different levels of complexity and scale. In this context, automated penetration testing using multiple vulnerability scanners deserves special attention. The paper discusses different approaches to integrating and combining automated web application scans.

**Keywords:** scanner, combination, attack, inspection, web application.