

СУЧАСНІ ІНТЕРАКТИВНІ ІНСТРУМЕНТИ ТЕСТУВАННЯ БЕЗПЕКИ ЗАСТОСУНКІВ

Дика А. І.

Національний університет «Одеська юридична академія»

Україна, Одеса

ORCID: 0000-0002-4196-8734

Анотація. Для проведення тестування безпеки вебзастосунків тестувальник безпеки, в числі іншого, має розбиратися з різними інструментами тестування безпеки, вміти налаштовувати та адмініструвати відповідні інструменти. Специфіка інструментів інтерактивного тестування працювати всередині програми, зумовлює можливість безпомилково виявляти й усувати уразливості у режимі реального часу.

Ключові слова: інтерактивне тестування; тестування програмного забезпечення; тестування безпеки; інструменти тестування; безпека програми; кібербезпека; IAST.

Вступна частина. В інтерактивних інструментах безпеки (Interactive Application Security Testing, IAST) усунуто всі обмеження, які є в SAST і DAST. Інструменти IAST виявляють проблеми та повідомляють про них в режимі реального часу під час виконання програми. Агенти IAST зазвичай розгортаються на серверах застосунків.

Мета роботи – проаналізувати сучасні інтерактивні інструменти тестування безпеки застосунків.

Основна частина. IAST використовує методологію тестування сірої скриньки, може визначити рядок коду, який спричиняє проблеми з безпекою, та швидко повідомити розробника про це для негайного усунення. Наприклад, якщо дані надходять від користувача, і він хоче виконати SQL-ін'єкцію в програмі, додавши SQL-запит до запиту, запит буде позначено як небезпечний [1].

Інструменти IAST легко інтегруються у фреймворки для аналізу вихідного коду і контролю виконання програми. Їх можна легко інтегрувати в конвеєр CI/CD команди DevOps. Проводячи IAST, команди DevOps можуть виявити та виправити будь-які вразливості до того, як вебзастосунок вийде на ринок. Це означає, що виправити такі вразливості набагато легше та дешевше. Це також гарантує безпеку програми до того, як хтось її фактично розгорне, допомагаючи запобігти тому, щоб майбутні користувачі програми стали жертвами потенційного витоку даних [2].

З іншого боку, IAST залежить від мови програмування, тому якщо організація використовує не дуже популярну технологію розробки, вона може бути несумісною з інструментом IAST [3]. Суттєво, що інструменти IAST сканують код під час його виконання. Тому рекомендовано розгорнути інструмент IAST у середовищі контролю якості, яке запускає автоматизовані функціональні тести. Це може допомогти уникнути людської помилки та переконатися, що увесь функціонал програми перевірено [4].

Розглянемо декілька популярних інструментів IAST: Synopsys Seeker, Invicti, Checkmarx та Acunetix.

Synopsys Seeker (<https://www.synopsys.com/>) – інструмент IAST з активною перевіркою та відстеженням конфіденційних даних для вебзастосунків. Synopsys допомагає командам розробників, QA, DevOps і безпеки автоматизувати тестування безпеки вебзастосунків і служб. Він визначає та вразливі місця застосунків шляхом активного моніторингу їх взаємодії.

Цей динамічний підхід до безпеки робить його особливо корисним для організацій, яким потрібні ефективні та ґрунтовні рішення IAST. Synopsys Seeker здатен виявляти вразливості в режимі реального часу під час роботи програми. Він інтегрується з інструментами Jira для легкого відстеження помилок і платформами CI/CD для більш плавного робочого процесу розробки. З іншого боку, ціни Synopsys Seeker не є загальнодоступними, їх можна отримати за запитом.

Invicti (<https://www.invicti.com/>) – масштабована платформа, яка пропонує свій підхід до інтерактивного та динамічного (DAST + IAST) автоматизованого сканування безпеки. Invicti (раніше Netsparker) автоматизовано виявляє та оцінює вразливості, що допомагає розставляти пріоритети у роботі з усунення проблем. Панелі моніторингу Invicti надають інформацію у зрозумілій та стислій формі, навіть якщо у користувача є велика кількість вебресурсів. Invicti використовує масштабовані агенти сканування, які звітують перед основним застосунком та ефективно використовують кілька IT-ресурсів для скорочення часу сканування. Звіти Invicti можуть бути налаштовані відповідно до вимог користувача. Invicti можна інтегрувати з наявними системами Azure DevOps, GitLab, GitHub, Jira, а також системами керування вразливістю Metasploit або Kenna. Також можна інтегрувати Invicti з платформами CI/CD: Jenkins, TeamCity або Bamboo. Цінова політика на офіційному сайті не публікується і надається за запитом, тріал-версії не передбачено.

Acunetix (<https://www.acunetix.com/>) – платформа сканування вразливостей у програмах, написаних на Node.js, PHP, Java (включаючи Spring framework) і ASP.NET. Acunetix поєднує сканування DAST + IAST і забезпечує перевірку широкого спектра вразливостей: топ-10 OWASP і топ-10 API, SQL-ін'єкції, XSS, неправильні конфігурації, викриті бази даних, позадіапазонні вразливості тощо. Acunetix IAST з AcuSensor сканує кожен файл, у тому числі приховані та незв'язані, забезпечуючи користувачам кращу видимість серверної частини їхніх вебзастосунків. Acunetix також може імпортувати файли визначення API та посилання для тестування API за допомогою архітектури REST, SOAP або GraphQL.

Checkmarx (<https://checkmarx.com/>) – корпоративна хмарна платформа безпеки вебзастосунків, яке допомагає організаціям виявляти, керувати та пом'якшувати вразливі місця веббезпеки. підходить для статичного та інтерактивного тестування безпеки застосунків. Checkmarx IAST сумісний із застосунками на основі мікросервісів і забезпечує зворотний зв'язок у реальному часі та комплексний аналіз спеціального коду, бібліотек, фреймворків і потоку даних під час виконання. Checkmarx приділяє значну увагу безпеці API, забезпечуючи охоплення топ-10 вразливостей API OWASP. Він виявляє, класифікує та документує API, а також відстежує їх використання та авторизацію. Розроблений з урахуванням розробників Checkmarx пропонує детальний аналіз вихідного коду для швидкого усунення потенційних вразливостей. Checkmarx має автоматизоване сканування SCA та відображення вразливостей сторонніх розробників під час сканування IAST. Checkmarx IAST можна розгорнути як локально в приватному центрі обробки даних, так і розмістити в приватному клієнті в AWS, пропонуючи гнучкі варіанти розгортання. Платформа має широкі можливості налаштування, що дозволяє створювати та налаштовувати користувацькі запити для оптимізації результатів, а її повна інтеграція в наявні робочі процеси забезпечує безпечний процес розробки без збоїв.

Висновки. Проведений аналіз сучасних інтерактивних інструментів тестування вебзастосунків виявив наявність різних підходів і розмаїття засобів для захисту програмних продуктів. Не існує ідеального універсального інструмента тестування безпеки.

Усі інтерактивні інструменти тестування безпеки мають свої переваги й недоліки через специфіку їх організації. Комбінування та використання переваг кожного чи то більшості з них може забезпечити високий рівень безпеки програмного вебпродукту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Трофименко, О.Г., Дика, А.І., Лобода, Ю.Г. (2023). Аналіз інструментів тестування вебзастосунків. *Кібербезпека: освіта, наука, техніка*, 4(20), 62-71. <https://doi.org/10.28925/2663-4023.2023.20.6271>.
- [2] Трофименко, О.Г., Дика, А.І. (2024). *Тестування та забезпечення якості програмних систем*: навч. посібник. Одеса: Фенікс. 195 с.
- [3] Harris, C., Iannini, L. (2024). *The Top 7 Interactive Application Security Testing (IAST) Tools*. <https://expertinsights.com/insights/the-top-interactive-application-security-testing-iaست-tools/>
- [4] Contrast. (2024). *Interactive Application Security Testing*. <https://www.contrastsecurity.com/glossary/interactive-application-security-testing>

Dyka Anastasiia

Analysis of project management software

Abstract. A security tester for testing web application security, among other things, must know various security testing tools, configure and administer them. The specificity of interactive testing tools to work inside the program determines the ability to accurately identify and eliminate vulnerabilities in real time.

Keywords: interactive application security testing; software testing; security testing; testing tools; application security; cybersecurity; IAST.