

ІНСТРУМЕНТИ СТАТИЧНОГО ТЕСТУВАННЯ БЕЗПЕКИ

Трофименко О.Г., к.т.н., доцент

Національний університет «Одеська юридична академія»

Україна, Одеса

ORCID: 0000-0001-7626-0886

Анотація. Інструменти SAST необхідні для раннього виявлення вразливості. У топ-5 таких засобів нині входять: PMD, Code Climate Quality, Snyk, Codacy, Veracode Static Analysis. Для ефективного вибору того чи іншого засобу для тестування безпеки застосунків варто враховувати специфіку відповідного програмного засобу.

Ключові слова: статичне тестування; SAST; тестування безпеки; інструменти тестування; кібербезпека.

Вступна частина. Інструменти статичного тестування безпеки застосунків (Static Application Security Testing, SAST) аналізують вихідний код і допомагають розробникам виявляти недоліки ще під час кодування. Процес SAST ще відомий як тестування білої скриньки [1]. Цей підхід тестувальники використовують, щоб перевірити внутрішню структуру програмного забезпечення та побачити, як воно інтегрується із зовнішніми системами.

Мета роботи – проаналізувати специфіку застосування інструментів статичного тестування безпеки застосунків на прикладі популярних на сьогодні інструментів безпеки.

Основна частина. Інструменти статичного аналізу коду використовують такі методи: аналіз синтаксису, аналіз потоку даних і аналіз безпеки. Синтаксичний аналіз перевіряє вихідний код на наявність синтаксичних помилок, подібно до того, як редактори документів, наприклад Microsoft Word, виділяють граматичні помилки. Аналіз потоку даних програмно аналізує потік даних на виявлення проблем зациклення. Нарешті, аналіз безпеки перевіряє вихідний код на наявність вразливостей у безпеці, якими можуть скористатися атаки [2].

Інструменти статичного аналізу коду допомагають у створенні якісного коду для будь-якого програмного проекту. Низька якість коду може спричинити зниження ефективності, проблеми з масштабованістю, вразливості безпеки тощо. Якщо ці проблеми не вирішити на етапі розробки, це може спричинити величезні проблеми надалі. З іншого боку, на практиці, хоча інструменти SAST корисні для раннього виявлення вразливостей, вони можуть генерувати помилкові спрацьовування та пропускати вразливості [3].

Наразі на ринку є десятки різних інструментів безпеки, які пропонують різні набори послуг безпеки програмних продуктів. Більшість наявних на ринку інструментів безпеки за різну абонплату намагаються надавати комплексні набори засобів для розробників і команд безпеки та не обмежуються наданням інструментів SAST, DAST чи то інших. Для розуміння можливої специфіки та відмінностей розглянемо п'ять популярних на сьогодні інструментів безпеки, які дозволяють безплатно аналізувати відкритий код на виявлення можливих проблем або надають безплатну тріал-версію, а саме: PMD, Code Climate Quality, Snyk, Codacy та Veracode Static Analysis.

PMD (<https://pmd.github.io/>) – розширюваний багатомовний статичний аналізатор відкритого коду, який підтримує загалом 16 мов, але переважно стосується Java та Apex. PMD доступний для Windows, macOS і Linux. На відміну від більшості інших аналізаторів коду, які вимагають платної ліцензії або пропонують обмежену функціональність у своїх безплатних

планах, PMD є програмним забезпеченням з відкритим вихідним кодом, що робить його економічно ефективною, безплатною альтернативою платним варіантам. PMD виявляє типові недоліки програмування, як-от: невикористані змінні, порожні блоки catch, створення непотрібних об'єктів тощо. Він має 400+ вбудованих правил, які можна розширювати. Вбудовані перевірки дозволяють налаштовувати правила для різних мов, щоб забезпечити дотримання стандартів кодування. Інструмент також містить детектор копіювання/вставлення (CPD), який допомагає ідентифікувати повторюваний код у кодовій базі. Інтеграція через плагіни доступна з такими популярними IDE, як Eclipse, JDeveloper і Gradle. Щодо недоліків PMD, то налаштування правил аналізу може бути складним, а зворотний зв'язок щодо кодування не надається в режимі реального часу.

Code Climate Quality (<https://codeclimate.com/quality>) – є інструментом аналізу коду, що здатен забезпечити статичний аналіз для таких мов: PHP, Java, JavaScript, Python і Ruby. Code Climate Quality має вбудовану інтеграцію з GitHub і GitLab. Інструмент також інтегрується з такими системами обміну заявками та повідомленнями, як Asana, Trello та Slack. Особливістю, які відрізняє Code Climate Quality, є наявна 10-бальна оцінка (від A до F) коду на основі його ремонтпридатності та покриття тестами. Він також оцінює, скільки часу може знадобитися для розв'язання проблеми. Ці показники та візуальні звіти про прогрес допомагають краще визначити пріоритети проблем з обслуговування або недостатнє покриття, тим самим допомагає командам розробників створювати кращий код. Пропонується безплатна версія для проєктів з відкритим кодом.

Snyk (<https://snyk.io/>) – платформа безпеки для розробників, яка пропонує сканування та аналіз коду в реальному часі. Snyk підтримує такі мови для аналізу коду: Python, Java, JavaScript, TypeScript, C++, Kotlin, Ruby, Go, Apex, .NET, PHP, Scala, Swift і VB NET. Він пропонує інтеграцію зі сховищем Git, що дозволяє визначати пріоритетність проблем у проєктах. Доступна інтеграція для таких інструментів CI/CD: Jenkins, Azure Pipelines і Bitbucket Pipelines. Є також плагіни для інструментів IDE: Eclipse, JetBrains Visual Studio і PhpStorm. Зручною функцією Snyk є надання кожній проблемі оцінки ризику, тож можна визначити пріоритетність проблем і зробити свій код більш безпечним. Інструменти аналізу коду Snyk включають сканування контейнерів, яке перевіряє наявність вразливостей у зображеннях контейнерів, і відстеження коду в реальному часі, яке перевіряє код під час роботи. Його інструмент DeepCode AI відкриває список швидких виправлень, які можна переглянути та застосувати ці виправлення у своєму інтегрованому середовищі розробки (IDE). Хоча повний функціонал Snyk є платним (25\$ на місяць), доступний безплатний план з обмеженням у 100 тестів на місяць.

Codacy (<https://www.codacy.com/>) – інструмент перевірки коду, який автоматизовано аналізує вихідний програмний код і висвітлює виявлені проблеми, дозволяючи розробляти більш ефективне програмне забезпечення. Платформа підтримує понад 40 мов програмування та фреймворків, добре інтегрується з робочими процесами CI і DevOps. Проста інтеграція Codacy з GitHub, GitLab, Bitbucket, Jira та Slack дозволяє отримувати миттєві відгуки про код, стандартизувати якість коду, автоматично блокуючи невідповідні запити, тобто вирішувати будь-які виявлені негаразди з кодом. В Codacy є зручна можливість, крім наявних сотень доступних правил, встановлювати ще й власні набори правил. Передбачена 14-денна безплатна пробна версія. До мінусів можна віднести відсутність інтеграції з Lombok, бібліотекою Java, яка скорочує шаблонний код, та неможливість експортувати шаблони коду.

Veracode Static Analysis (<https://www.veracode.com/>) – платформа статичного тестування безпеки, яка підтримує понад 100 мов програмування і фреймворків, забезпечуючи широке

покриття. Можлива інтеграція з понад 40 платформами, серед яких: Azure DevOps, Bitbucket, Eclipse, Jenkins, Visual Studio тощо. Veracode забезпечує зворотний зв'язок у режимі реального часу, сканує та визначає вразливості протягом усього циклу розробки, пропонує конвеєрні інтеграції CI/CD. Рекомендації щодо виправлення в режимі реального часу допомагають визначити пріоритетність виправлень, які становлять найбільшу загрозу. Особливостями Veracode Static Analysis є його швидка продуктивність сканування та низький рівень хибнопозитивних результатів (<1,1%) [4]. Доступна 14-денна безплатна пробна версія Veracode. Щодо можливих недоліків, то в деяких областях бракує документації, крім того, характерним є крута крива навчання.

Висновки. Загалом інструменти SAST необхідні для раннього виявлення вразливості. Для них не потрібна працююча програма і таке тестування може відбуватися без виконання коду. Це допомагає розробникам виявляти вразливості на початкових етапах розробки та швидко вирішувати проблеми, не порушуючи збірки та не передаючи вразливості до остаточного випуску програми. Деякі інструменти вказують на точне розташування вразливостей і виділяють ризикований код. Інструменти SAST також можуть надавати доволі докладні вказівки щодо вирішення проблем і підказувати найкраще місце в коді для їх вирішення, не вимагаючи глибоких знань у сфері безпеки [5]. Тому важливо запускати інструменти SAST в програмі на регулярній основі, наприклад, під час щоденних/щомісячних збірок, кожного разу, коли перевіряється код, або під час випуску коду.

З іншого боку, інструменти SAST можуть генерувати помилкові спрацьовування та пропускати вразливості під час виконання. Тому рекомендованим є багаторівневий підхід до безпеки, що поєднує різні інструменти (SAST, DAST, IAST і RASP) тестування для досягнення комплексної безпеки застосунків.

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., Соколов, А. В., Чикунів, П. О., Ахметьєва, Г. В., Атанасевич, А. О. (2024). Аналіз ролі фахівців із тестування та забезпечення якості. *Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова*, 3(496), 106-113. [https://doi.org/10.15589/znp2024.3\(496\).16](https://doi.org/10.15589/znp2024.3(496).16).
- [3] Fernandes, A.A. (2024). Evaluating the top application security tools: from static analysis to runtime protection. *Asian Journal of Research in Computer Science*, 17(7), 119-27. <https://doi.org/10.9734/ajrcos/2024/v17i7483>
- [4] Gardini, P.M. (2024). *20 Best Code Analysis Tools in 2024*. <https://thectoclub.com/tools/best-code-analysis-tools/>
- [5] Black Duck. (2024). *Static Application Security Testing*. <https://www.blackduck.com/glossary/what-is-sast.html>

Trofymenko Olena

Static security testing tools

Abstract. SAST tools are essential for early vulnerability detection. The top 5 such tools are: PMD, Code Climate Quality, Snyk, Codacy, Veracode Static Analysis. In order to effectively choose a tool for testing the security of applications, it is necessary to take into account the specifics of the corresponding software tool.

Keywords: static application security testing; SAST; security testing; testing tools; cybersecurity.