Секція 1

ДОСЛІДЖЕННЯ ВИНИКНЕННЯ ЛОГІЧНИХ ПОМИЛОК В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МЕТОДИК ЇХ ВИЯВЛЕННЯ

Семенець О. Ю.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Тецький А. Г.

Актуальність. Логічні помилки - це ситуації, коли код програміста успішно компілюється і виконується, але не генерує очікуваний результат для всіх можливих вхідних даних [1]. На відміну від синтаксичних помилок, логічна помилка не призводить до збоїв або аварійного завершення роботи програми. Однак вона може створити умови для експлуатації вразливості чи порушення безпеки. Загрози та вразливості виявляються під час життєвого циклу розробки програмного забезпечення, та інженер з кібербезпеки може за допомогою сучасних технік статичного та динамічного аналізу програм виявити їх. Ці техніки ефективні для виявлення заздалегідь відомих дефектів, але вони не достатньо охоплюють таку проблему, як виявлення логічних помилок [2].

Метою даної роботи є дослідження виникнення логічних помилок, причини їх виникнення в розробці програмного забезпечення та огляд розповсюджених методик їх виявлення.

Основні положення. Для своєчасного виявлення логічних помилок до команди розробки треба залучити інженера з кібербезпеки, який буде приймати активну участь в створені проекту на кожній фазі розробки. В цій роботі було проведено дослідження причин виникнення логічних помилок, для абстрактного огляду процеси розробки була приведена каскадна модель розробки програмного забезпечення. За допомогою цієї моделі процес розробки можна представити як серію послідовних фаз, через які проходить проєкт. Проведено дослідження з методик виявлення логічних помилок в залежності від етапу розробки та інструментів, які може використовувати інженер з кібербезпеки, в залежності від його доступу до проекту. Був проведений огляд таких інструментів як: SLA-generator, Microsoft Threat Modeling Tool та OWASP Threat Dragon [3]; SonarQube, Checkmarx та Fortify [4]; Burp Suite, OWASP ZAP (Zed Attack Proxy) і Wireshark [5].

Висновки. Виявлення логічних помилок є надзвичайно важливим, але й складним завданням, оскільки помилки часто не можуть бути виявлені

стандартними методами тестування. Інженер з кібербезпеки для їх виявлення може застосувати такі методи як статичний та динамічний аналіз, перевірку на проникнення, а також може використати такі інструменти набір інструментів в залежності від наявності доступу інженера до вихідного коду проекту. Запропоновані алгоритми та інструменти наведені в доповіді.

Список літератури

1. Ettles A., Luxton-Reilly A., Denny P. Common logic errors made by novice programmers. the 20th Australasian Computing Education Conference, Brisbane, Queensland, Australia, 30 January – 2 February 2018. New York, USA, 2018. DOI: https://doi.org/10.1145/3160489.3160493.
2. Stergiopoulos, G., Katsaros, P., Gritzalis, D. Source code profiling and classification for automated detection of logical errors. In 3rd International Seminar on Program Verification, Automated Debugging and Symbolic Computation, Germany. 2014. URL – https://www.infosec.aueb.gr/Publications/PAS-2014%20Logical%20Error.pdf (дата звернення: 30.10.2024).
3. Granata D., Rak M. Systematic analysis of automated threat modelling techniques: Comparison of open-source tools. Software Qual J 32. 2024. Page 125–16. DOI: https://doi.org/10.1007/s11219-023-09634-4
4. Alexandra de Barros Reigada. Generic SAST tool Comparer. URL – https://repositorium.sdum.uminho.pt/bitstream/1822/84173/1/Alexandra%20de%20Barros%20Reigada.pdf (дата звернення: 05.11.2024).
5. Ekene Joseph. Burp Suite vs OWASP ZAP – a Comparison series. *Medium*. URL – https://medium.com/@Ekenejoseph/burp-suite-vs-owasp-zap-a-comparison-series-8e34162c42e6 (дата звернення: 10.11.2024).

Відомості про авторів

Семенець Олександр Юрійович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.y.semenets@csn.khai.edu
Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskyi@csn.khai.edu