МЕТОДОЛОГІЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-ДОДАТКІВ

Дорофєєва К.І., Сєвєрінов О.В., Сидоренко З.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Забезпечення інформаційної безпеки веб-додатків залишається критично важливим завданням для організацій різного масштабу. Одним із прийнятних підходів для систематичної оцінки безпеки є тестування на проникнення, яке дозволяє імітувати дії зловмисника з метою виявлення слабких місць у захисті додатка. Аналіз актуальних загроз, що постають перед сучасними веб-додатками в умовах стрімкого розвитку технологій показує постійне зростання кількості кібератак. Основні категорії з них - ін'єкційні атаки (SQL/NoSQL Injection), міжсайтовий скриптинг (XSS), підробка запитів (CSRF), атаки на автентифікацію та управління сесіями, зокрема brute force, credential stuffing та викрадення токенів. Особлива увага необхідно приділяти вразливостям у контролі доступу, сучасним атакам на API та ризикам, пов'язаним із використанням сторонніх бібліотек і компонентів у ланцюгах постачання [1, 2].

Метою доповіді є дослідження та формалізація методології проведення тестування на проникнення веб-додатків, а також формування чіткої послідовності дій, метрик і шаблонів звітності для етичних тестувань на проникнення.

Послідовність проведення тестування на проникнення передбачає такі етапи [3, 4].

1. Підготовчий етап. Визначення об'єкта тестування, меж і правил, отримання письмового дозволу від власника системи і узгодження часових вікон для виконання активних перевірок;

2. Планування та конфігурація інструментів. Налаштування проксі, визначення політик сканування, імпорт сценаріїв аутентифікації, підготовка довірених сертифікатів для HTTPS-трафіку та інтеграція із засобами автоматизації;

3. Збір інформації. Реєстрація всіх HTTP/HTTPS-запитів і відповідей, ідентифікація точок введення даних, карта сторінок і перечислення функціональних API. Пасивний збір дозволяє мінімізувати ризик впливу на продуктивне середовище; активний – застосовується тільки в узгоджені вікна й за наявності дозволу;

4. Аналіз вразливостей. Застосування правил виявлення OWASP ZAP та власних тестів для виявлення класичних категорій вразливостей. Тут описується як проводити верифікацію виявлень вручну або із застосуванням скриптів, щоб уникнути хибнопозитивних спрацьовувань;

5. Перевірка експлуатації. Документоване відтворення виявлених пробілів у безпеці з максимально обережними діями, що не завдають шкоди системі;

6. Формування звіту та рекомендацій. Стандартизований шаблон звіту: опис вразливості, кроки відтворення, рівень критичності, можливі наслідки,

короткострокові та довгострокові рекомендації, пріоритети усунення та запропоновані заходи з моніторингу;

7. Післятестові дії. Перевірка усунення вразливостей, оновлення документації з безпеки, передача знань команді розробки та налаштування автоматичного моніторингу для виявлення регресій.

У доповіді представлено структурований підхід до реалізації кожного з етапів методології. Акцент зроблено на узгодженні меж перевірки, документуванні дій та стандартизації процесу звітування, що забезпечує відтворюваність результатів і можливість інтеграції методології в корпоративні процеси управління безпекою. Описано методику збору метрик, умови експериментів і вимоги до середовища для забезпечення достовірності результатів.

Завдяки запропонованій методології забезпечується не лише систематичний і формалізований підхід до виявлення та аналізу вразливостей веб-додатків, але й створюється основа для побудови комплексного процесу управління безпекою веб-додатків [1]. Розроблена послідовність дій дозволяє поєднати теоретичні принципи тестування на проникнення з практичними аспектами його реалізації в реальних умовах експлуатації. Це забезпечує відтворюваність результатів, точність виявлення вразливостей і можливість їх подальшого усунення без шкоди для продуктивного середовища [5].

Отже, розроблена методологія проведення тестування на проникнення веб-додатків є гнучким, масштабованим і практично орієнтованим інструментом, який може бути впроваджений як у невеликих організаціях, так і у великих корпоративних середовищах. Її застосування сприяє формуванню культури безпечної розробки (SDLC), підвищенню рівня обізнаності персоналу щодо сучасних загроз і створює основу для побудови стійкої та адаптивної системи захисту, здатної ефективно реагувати на динамічні зміни кіберсередовища.

Список літератури

1. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (date of access: 21.10.2025).

2. Сєвєрінов, О. В., Шевцов, В. О., & Сокол-Кутиловська, А. С. (2017). Аналіз сучасних методів атак на електронні ресурси органів управління. *Системи озброєння і військова техніка*, (1), 65-68.

3. Qiu, X.; Wang, S.; Jia, Q.; Xia, C.; Xia, Q. An automated method of penetration testing. In Proceedings of the 2014 IEEE Computers, Communications and IT Applications Conference, Beijing, China, 20–22 October 2014; pp. 211–216.

4. Д'якова, Н. Є., & Сєвєрінов, О. В. (2022). Тестування вразливостей сучасних веб-ресурсів.

5. Zhou, T.-Y.; Zang, Y.-C.; Zhu, J.-H.; Wang, Q.-X. NIG-AP: A new method for automated penetration testing. Front. Inf. Technol. Electron. Eng. 2019, 20, 1277–1288.