Секція 1

АНАЛІЗ ВРАЗЛИВОСТЕЙ OWASP TOP TEN ТА ЗАХИСТ ЗА ДОПОМОГОЮ БРЕНДМАУЕРУ

Лісних О. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Морозова О. І.

Актуальність. З ростом кіберзагроз та інтернет-економіки, вразливість веб-додатків є критичною. Зловмисники постійно шукають нові способи атак та вразливості для втручання в системи та крадіжки даних. Регулярний аналіз вразливостей, які з'являються, допомагає підвищити безпеку веб-додатків та запобігти можливим загрозам. Саме некомерційний фонд OWASP і їх списки найпопулярніших вразливостей надає можливості захистити свій додаток [1]. OWASP (Open Web Application Security Project) – це проєкт, спрямований на підвищення безпеки веб-додатків.

Метою даної роботи є аналіз вразливостей веб-додатків за результатами дослідження OWASP Top Ten та досягання надійної системи, яка може ефективно контролювати та фільтрувати мережевий трафік, запобігаючи проникненню шкідливих даних і атак за допомогою брандмауеру [2]. Брандмауери – це системи безпеки, які контролюють вхідний і вихідний мережевий трафік на основі заздалегідь визначених правил безпеки. Вони можуть бути апаратними, програмними або комбінацією обох.

Основні положення. В роботі буде проаналізовано вразливості зі списку OWASP Top Ten, серед них:

1. Порушений котроль доступу – контроль доступу застосовує політику таким чином, що користувачі не можуть діяти поза межами своїх передбачуваних дозволів [3].
2. Криптографічні збої – проблеми, пов'язані з криптографією, так як слабке шифрування [4].
3. Ін'єкції – вставка та виконання злоякісного ПЗ або коду на стороні додатку [5].

На основі аналізу вразливостей в веб-додатках, буде відображено схему, алгоритм та принцип роботи брандмауеру, який буде мати за ціль захистити додаток від найпопулярніших вразливостей. Брандмауер повинен бути здатним адаптуватися до нових загроз, забезпечувати гнучкість у налаштуванні правил безпеки та інтегруватися з іншими системами безпеки для забезпечення комплексного захисту. Основні функції брандмауера включають:

1. Фільтрація пакетів: аналіз і контроль мережевих пакетів, що проходять через брандмауер.
2. Інспекція стану: відстеження стану активних з'єднань і визначення, які пакети можуть проходити через брандмауер.
3. Захист від DDoS-атак: виявлення та блокування розподілених атак відмови в обслуговуванні.
4. VPN підтримка: забезпечення безпечного віддаленого доступу через віртуальні приватні мережі.

Висновки. Ефективний брандмауер повинен бути інтегрованим у загальну стратегію безпеки організації, забезпечуючи захист від сучасних загроз. Розробка та впровадження брандмауерів, які відповідають потребам організації, є важливим кроком у забезпеченні безпеки даних та систем. Враховуючи актуальність і постійний розвиток кіберзагроз, інвестиції в сучасні рішення для брандмауерів є необхідними для захисту бізнесу.

Список літератури

1. OWASP Top Ten. *OWASP*. URL – https://owasp.org/about (дата звернення: 05.11.2024).
2. OWASP Top Ten 2025. *OWASP*. URL – https://owasp.org/www-project-top-ten (дата звернення: 05.11.2024).
3. A1:2021 – Broken Access Control. *OWASP*. URL – https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).
4. A2:2021 – Cryptographic Failures. *OWASP*. URL – https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).
5. A3:2021 – Injection. *OWASP*. URL – Available at: https://owasp.org/Top10/A01_2021-Broken_Access_Control (дата звернення: 06.11.2024).

Відомості про авторів

Лісних Олександр Ігорович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.lisnykh@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп’ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., професор, o.morozova@khai.edu