УДК 004.056.53
М. Кончак
(Тернопільський національний технічний університет імені Івана Полюя, Україна)

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД КІБЕРАТАК

UDC 004.056.53
M. Konchak

ANALYSIS OF METHODS FOR PROTECTING WEB APPLICATIONS FROM CYBER ATTACKS

З розвитком цифрових технологій веб-додатки стали важливою частиною сучасної інформаційної інфраструктури. Їх використання супроводжується ризиками кібератак, які можуть призвести до значних фінансових, репутаційних та інформаційних втрат.

Основні типи атак (згідно з рейтингом OWASP Top 10, 2024):

1. SQL-ін’єкції. Атаки, спрямовані на маніпулювання запитами до бази даних.
2. XSS-атаки (Cross-Site Scripting). Використовують уразливості для виконання шкідливих скриптів.
3. DDoS-атаки (Distributed Denial of Service). Перевантаження серверів з метою порушення їхньої роботи.

Методи захисту:

1. Валідація та фільтрація даних. Забезпечення коректної обробки вхідних даних.
2. Використання міжсайтових політик (CSP). Обмеження джерел виконання скриптів.
3. Шифрування даних. Захист переданої інформації за допомогою протоколів HTTPS.
4. Регулярні оновлення програмного забезпечення. Усунення відомих уразливостей.
5. Використання WAF (Web Application Firewall). Виявлення та блокування підозрілих запитів.

Аналіз сучасних методів захисту веб-додатків свідчить про необхідність комплексного підходу до кібербезпеки, який включає як технологічні рішення, так і організаційні заходи. Забезпечення безпеки веб-додатків є ключовим аспектом у захисті цифрових активів організацій.

Література

1. OWASP. *Top 10 Web Application Security Risks*. 2024.
2. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson, 2022.
3. Symantec. *Internet Security Threat Report*. 2023.