UDC 004.056.5

A. V. Pavlovska
V. V. Chopliak

ANALYSIS AND REMEDIES TO CRITICAL WEB APPLICATION VULNERABILITIES ACCORDING TO OWASP TOP 10 CLASSIFICATION

Vinnytsia National Technical University

Анотація

У роботі розглянуто актуальні загрози веббезпеки відповідно до класифікації OWASP Top 10 та проаналізовано сучасні методи захисту від кожної з них. Запропоновано комплексний підхід до забезпечення безпеки вебзастосунків, що охоплює технічні, організаційні та процедурні заходи.

Ключові слова: вебзастосунки, аналіз, OWASP, кібербезпека, захист інформації, вразливості, SQL-ін'єкція, XSS, автентифікація.

Abstract

The paper examines current web security threats according to the OWASP Top 10 classification and analyses modern protection methods for each of them. A comprehensive approach to web application security is proposed, encompassing technical, organisational, and procedural measures.

Keywords: web applications, analysis, OWASP, cybersecurity, information security, vulnerabilities, SQL injection, XSS, authentication.

Introduction

The rapid development of web technologies and the large-scale implementation of web applications in critical business processes have led to a significant increase in the number of cyberattacks directed against them. According to statistics from the OWASP (Open Web Application Security Project), more than 80% of successful attacks on web resources exploit vulnerabilities included in the OWASP Top 10 list [1]. This makes the task of comprehensive protection of web applications one of the priority areas of modern cybersecurity.

OWASP Top 10 Threat Analysis

The OWASP Top 10 list (2021 edition) identifies the ten most critical categories of web application vulnerabilities [1]. The most common are: A01 – Broken Access Control; A02 – Cryptographic Failures; A03 – Injection (including SQL and NoSQL); A05 – Security Misconfiguration; A07 – Identification and Authentication Failures.

SQL injection remains one of the most dangerous attacks: an attacker injects arbitrary SQL code into a database query, gaining unauthorized access to or modification of data. Cross-site scripting (XSS) allows malicious JavaScript code to be executed in the victim's browser, leading to session cookie theft or redirection to phishing resources [3].

Web application security methods

Web Application Firewall (WAF). Using a WAF allows you to filter out malicious HTTP traffic at the rule level, blocking known attack patterns before they reach the application. Popular solutions include ModSecurity, AWS WAF, and Cloudflare WAF.

To counter the OWASP Top 10 threats, a set of technical and organizational measures is proposed.

Injection protection. The main method of countering SQL injections is the use of parameterized queries (Prepared Statements) and ORM frameworks, which make it impossible to execute arbitrary SQL code. It is additionally recommended to apply the principle of least privileges for database accounts and regularly perform static code analysis [2].

XSS protection. An effective measure is to escape all data displayed in the HTML context, as well as implement the Content Security Policy (CSP) policy – an HTTP header that limits the sources of loading scripts and styles. In addition, data input sanitization libraries should be used, in particular DOMPurify [3].

Access control. Access control violation (OWASP A01) is eliminated by implementing the RBAC (Role-Based Access Control) model, where each user is assigned a role with a minimum set of rights. All requests to protected resources must be checked on the server side regardless of client logic [1].

Cryptographic protection. To eliminate category A02, it is necessary to use up-to-date encryption algorithms (AES-256, RSA-2048 and higher), the TLS 1.3 protocol for the transport layer, as well as modern hash functions for storing passwords (bcrypt, Argon2). The use of outdated algorithms MD5, SHA-1 and DES is prohibited [4].

Authentication and session management. The implementation of multi-factor authentication (MFA), limiting the number of unsuccessful login attempts (rate limiting), generating cryptographically strong session tokens and their timely revocation significantly reduce the risk of unauthorized access [2].

Web Application Firewall (WAF). Using a WAF allows you to filter malicious HTTP traffic at the rules level, blocking known attack patterns before they reach your application. Popular solutions include ModSecurity, AWS WAF, and Cloudflare WAF.

Conclusion

An analysis of the OWASP Top 10 threats and corresponding mitigation techniques shows that no single measure can ensure the complete security of a web application. Effective protection can only be achieved through the comprehensive use of parameterized queries, CSP, RBAC, modern cryptography, MFA, and WAF. Further research should focus on automating vulnerability detection using machine learning and integrating DevSecOps practices into the web application development process.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OWASP Top Ten 2021. *Open Web Application Security Project*. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 09.05.2026).
2. OWASP API Security Top 10 2023. *Open Web Application Security Project*. 2023. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (дата звернення: 09.05.2026).
3. Cross Site Scripting (XSS) Prevention Cheat Sheet. *Open Web Application Security Project*. 2024. URL: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (дата звернення: 09.05.2026).
4. Guideline for Using Cryptographic Standards in the Federal Government: NIST Special Publication 800-175B Rev. 1. *National Institute of Standards and Technology*. 2020. URL: https://doi.org/10.6028/NIST.SP.800-175Br1 (дата звернення: 09.05.2026).
5. Nykyporets S. S., Kot S. O., Sabadosh J. H., Chopliak V. V., Piddubchak S. Y. Leveraging digital technologies in English phraseology research. *Bulletin of Science and Education. Series «Philology»*. 2025. № 10(40). С. 83-95. DOI: https://doi.org/10.52058/2786-6165-2025-10(40)-83-95.

Павловська Анастасія Вячеславівна – студентка групу 1БС-24б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail : nastyapav2006@gmail.com.

Науковий керівник: ***Чопляк Вікторія Володимирівна*** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Pavlovska Anastasiia Vyacheslavivna – student group 1SS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nastyapav2006@gmail.com.

Scientific Supervisor**: Victoriia V. Chopliak** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.