ENSURING WEB SECURITY WITH OWASP METHODOLOGY

CZU: 004.056.53:004.77
DOI: https://doi.org/10.53486/csc2025.16

BRAGARU TUDOR
Moldova State University, A. Mateevici str. 60, MD-2009, Republic of Moldova
tudor.bragaru@usm.md
ORCID ID: 0000-0001-6356-2906

DARII OLGA
Moldova State University, Chisinau, A. Mateevici str. 60, MD-2009, Republic of Moldova
olga.darii@yahoo.com
ORCID ID: 0009-0001-2319-8350

Abstract. Currently, more and more companies, organizations, individuals (entities) operate online in the global virtual cyberspace, storing and processing enormous amounts of sensitive personal data. There are various ways to improve the security of web applications, many of which are proprietary, poorly accessible and difficult to implement. A thorough analysis suggests that the development of secure web applications using the OWASP methodology (The Open Worldwide Application Security Project) allows for the effective control and reduction of the values of all types of vulnerabilities. This paper is a review, synthesis that brings its small contribution to the specialized literature on awareness and promotion of the culture of web application protection with the OWASP methodology. The paper briefly describes the OWASP project, the approach to web application security based on the OWASP Top Ten vulnerabilities, which allows organizations not only to protect their data, but also their reputation and customer trust. OWASP provides a good understanding of how attackers can compromise an entity's web applications and sensitive user data. It also emphasizes the need to implement preventive, proactive measures to prevent web applications from compromising users and the host entity.

Keywords: Web applications, Web application security, OWASP, OWASP top ten vulnerabilities, Security measures, sensitive personal data.

JEL:L86, O33, I29

INTRODUCTION

The significance of web application security has grown a lot lately and continues to grow simultaneously with the development of modern digital society and electronic business. This is because the basis of e-business and the digital economy is the Internet and the web with multiple and diverse challenges and risks. Risks persist in any web application, e-government platforms, e-finance, e-insurance, etc., affecting not only individuals and/or separate organizations, but also entire industries (e.g. banking industry, e-medicine, e-government) and society as such (e.g. social networks). And a security incident, as a result of the realization of risks can lead to the loss of user trust in online e-business platforms, can have devastating consequences, such as financial, reputational losses, sanctions.

According to *recent research from Verizon, web application attacks are involved in 26% of all breaches, making them the second most common attack pattern [1].* Four of the most common attacks against web applications are SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) [11], Denial of Service & Distributed Denial of Service (DoS & DDoS).

WEB APPLICATION SECURITY: CONCEPT, VULNERABILITIES, SOLUTIONS

1. What is OWASP, OWASP values and projects, basic principles of web security

The OWASP Foundation (The Open Worldwide Application Security Project) is a non-profit organization, founded in 2001 in the USA; a dedicated open collaborative community, bringing together experts, developers, testers, who focus on the security of online web applications throughout their entire life cycle. OWASP's main mission is to provide open resources, tools, standards and guidelines to help build and maintain secure web applications, to raise awareness of critical security issues faced by developers. OWASP has over 250 local chapters worldwide, tens of thousands of members, and is a leader in education and training on the security profile of trusted web applications. For more details, see [2] (*https://owasp.org/about).*

OWASP administers hundreds of open-source projects, including code, documentation, and standards; actively participates in the formation of standards and recommendations of ISO, COBIT, NIST, PCI DSS, etc.; contributes to improving the overall security of web applications worldwide. The projects provide members with the opportunity to freely test theories and ideas with the professional support of the OWASP community. Each project has its own web page. Most projects maintain their content on GitHub. The OWASP project inventory contains over 360 objects. For more details see [6] (*https://owasp.org/projects).*

Understanding concepts, being aware of vulnerabilities, following best practice requirements, standards and industry recommendations – are vital to creating a secure online environment with web application protection based on the resources provided by the OWASP foundation.

A proactive approach to web security with the application of basic cybersecurity principles helps prevent fraud and loss; ensures confident operation in global cyberspace for all those interacting with web applications. The basic principles of ensuring web application security refer to Implementing a Web Application Firewall (WAF) [8], Defense in Depth; Prevention, Detection and Response; Security by Design; Shewhart Cycle or Deming's (quality) wheel (PDCA=Plan-Do-Check-Act); Least Privileges, etc.

For example:

- **Privilege minimization:** Limiting user and application access to strictly necessary resources reduces security risks.
- **Risk management:** Systematic risk assessments are essential to identify and remediate vulnerabilities.
- **Security by design:** Integrating security into all stages of application development helps prevent security issues before they arise.
- **Patching:** Timely application of all security updates is essential for maintaining the security of web applications [5] etc.

Lack of training, poor integration of security into design, weak security management, and inadequate access control are among the most significant factors contributing to vulnerabilities. Addressing these challenges during the development and testing phases is crucial for reducing security risks in web applications.

2. Basic web application security requirements

Web application security starts with specific policies, applied throughout the entire life cycle, from design-development to operation and decommissioning. Several dozen policy templates can be found at the SANS Institute (SysAdmin, Audit, Network, Security) [9]. At the same time, web

security is based on preserving the fundamental properties of information/CIA triad: Confidentiality, Integrity and Availability. For details, see [4].

Confidentiality in web applications refers to protecting processed data (collected, stored, transmitted) from prying eyes, but who do not have the respective rights (by hiding = steganography; by encrypting data = cryptography) and limiting access. The mechanisms used include user authentication, the use of SSL/TLS certificates. For example, to prevent unauthorized access, data leaks, ransomware attacks, etc. in a web application that stores authentication data, sensitive data (personal, medical, banking, etc.), they must be encrypted from end to end, both in transit and at rest, in databases on servers, in archives.

Integrity ensures that data is not modified/altered during the use of the application. Security measures such as input validation and hashing are recommended to prevent attacks aimed at altering data, such as SQL Injection or Cross-Site Scripting/XSS.

Availability is crucial for web applications, as users must have access to them at any time they need them. Availability is affected by DoS or DDoS attacks, which do not alter data, but block access to it by overwhelming the server by bombarding it with an excessive number of fictitious requests. Protection measures against DoS/DDoS attacks include infrastructure redundancy, backup systems, IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) [3] systems, which help prevent interruptions and ensure that the web application remains accessible even in the event of a DoS/DDoS attack or technical errors.

Based on fundamental properties, secondary aspects like non-repudiation, extended confidentiality, high availability, and accountability are ensured. Extended confidentiality secures data in storage and transit via end-to-end encryption. High availability guarantees continuous access to critical applications through disaster recovery plans and resilient architectures.

3. OWASP Top Ten Project and measures to counter vulnerabilities

Web application security is a vast and complex area related to network and Internet security, affected by numerous vulnerabilities, from SQL Injection and Cross-Site Scripting attacks to advanced phishing and ransomware techniques. The most critical security risks for web applications and methods to counter them, widely agreed upon by web application developers and users, see the OWASP Top Ten. For illustration, we reproduce only the first two of these in the 2021 version of the OWASP Top Ten [7]. Others, including the specifications for the first two vulnerabilities according to the 2025 version, follow the project status [10].

- A01. Broken access control (attacker can access resources or data they should not have access to). 61% of all breaches involve A01. There are many ways to achieve this, but one common method is to use a whitelist.
- A02. Cryptographic Failure. Insecure communications remain a major concern. Weak or unencrypted data transmission exposes sensitive information such as passwords and financial data to interception. In 2023, over 8 billion records were breached, with an average data breach cost of $4.54 million. Using HTTPS and strong cryptographic algorithms mitigates these risks by securing data in transit.

4. Results and Discussion

Ensuring the security of web applications is no longer just a technical-technological necessity of settings, usually performed once, according to the administrator's perception. It becomes a strategic responsibility, which must comply with accessible, verified and approved best practice requirements

and recommendations. In the authors' opinion, such a globally accepted and recognized practice is the OWASP Top Ten approach to web application security.

The main contribution of this bibliographic study is the review, synthesis of knowledge and recommendations of good practices for secure coding according to the OWASP Top Ten project. The main significance of web application security based on the OWASP Top Ten is the reduction of the number of reported vulnerabilities and incidents, the average severity level and the bounty payments.

Typically, the OWASP Top Ten is updated every three to four years. However, it may be updated more frequently, depending on the emergence of new threats, changes in the security landscape, and the need for updated guidance. The penultimate update was in 2021 (https://owasp.org/Top10), a new OWASP Top Ten update from 2025 [10] is expected soon. To some extent, other previous OWASP Top Ten versions, such as those from 2017, 2013, and 2010, can also be used. However, it is best to use the latest version, which considers the changes in the security landscape.

CONCLUSIONS

The most important measures to ensure web application security include data encryption, multifactor authentication, input data validation, implementation of WAF, IDS, IPS solutions, etc. These measures allow for essential risk reduction and proactive protection of web applications from potential attacks.

By implementing strict access policies, incident management, session management, backup and disaster recovery policies, etc., entities can ensure the continuity of their activities and the protection of sensitive data. Implementing appropriate security methods, such as intrusion detection and monitoring (IDS, IPS), periodic scans, the use of appropriate dynamic analysis tools and static analysis play a vital role in identifying and remediating vulnerabilities before they are exploited. All this allows organizations to react quickly to security incidents and minimize the impact of attacks.

Web application security is not a static product, goal, or one-time action, but a dynamic process, which requires constant attention and continuous adaptation to the changing threat environment. Organizations must commit to continuous improvement of web security measures, invest in staff training, and stay up to date with the latest trends and techniques in the field. A globally recognized and accepted recommendation is policy-based management and the OWASP Top Ten, with the new guidance updated in 2025 [10].

REFERENCES

1. 50 Web Security Stats You Should Know In 2025. Available at: https://expertinsights.com/insights/50-web-security-stats-you-should-know/. [Accessed 19.02.2025].
2. *About the OWASP Foundation.* Available at: *https://owasp.org/about.* [Accessed 19.02.2025].
3. *IPS/IDS - what is it?* Available at: https://www.cloud4y.ru/blog/ips-and-ids-what-is-it. [Accessed 19.02.2025].
4. *ISO/IEC 27032:2023 Cybersecurity. Guidelines for Internet security (second edition).* -34 pages
5. Laurente-Ticong. What Is Patch Management. Everything You Need to Know. Enterprise Networking Planet. Available at: https://www.enterprisenetworkingplanet.com/security/what-is-patch-management/. [Accessed 19.02.2025].
6. *OWASP projects.* Available at: *https://owasp.org/projects/.* [Accessed 19.02.2025].
7. *OWASP Top Ten. OWASP Foundation.* Available at: https://owasp.org/www-project-top-ten/. [Accessed 19.02.2025].

8. *Web Application Firewall Overview.* Available at: https://learn.microsoft.com/ro-ro/power-pages/security/web-application-firewall. [Accessed: February 19, 2025].
9. *Security Policy Templates.* Available at: https://www.sans.org/information-security-policy/. [Accessed 19.02.2025].
10. *The OWASP Top Ten.* Available at: https://www.owasptopten.org/. [Accessed 19.02.2025].
11. *What is Cross-site request forgery (CSRF)?* Available at: https://www.vectra.ai/topics/cross-site-request-forgery. [Accessed 19.02.2025].