Azerbaijan University of Architecture and Construction
ISSN 2706-7726

Engineering Mechanics
Scientific and Technical Journal

E-mail: engineeringmechanics@azmiu.edu.az

March 2026	Issue 22	Volume 14	Number 1	Pages 25-31

APPLICATION OF MODERN METHODS AND TOOLS IN ENSURING THE SECURITY OF WEB APPLICATIONS.

NIHAT DASHDAMIRLI, SARDAR GASIMOV

Azerbaijan State Oil and Industry University
nihatdasdemirli@gmail.com, sardarkasumov1955@mail.ru

Abstract: Web applications have become an integral component of contemporary digital infrastructure and are extensively utilized across a wide range of sectors, including public administration, education, healthcare, finance, e-commerce, and defense. Their growing adoption is associated with significant advantages such as rapid access to information, enhanced service delivery, improved operational efficiency, and support for remote communication and interaction. Nevertheless, the increasing reliance on web-based platforms has simultaneously expanded the attack surface of digital systems, making web applications one of the primary targets of cyber threats. In this context, ensuring the security of web applications has emerged as a critical objective in modern cybersecurity practice.

The security of web applications is challenged by numerous vulnerabilities and sophisticated attack techniques. Common threats include unauthorized access, SQL injection, cross-site scripting, broken authentication, session hijacking, insecure data transmission, and denial-of-service attacks. The consequences of such threats may be severe, leading to data breaches, service interruptions, financial losses, reputational damage, and the compromise of sensitive or mission-critical information. Therefore, the protection of web applications must be approached as a comprehensive and continuous process that integrates technical, organizational, and analytical security measures.

This article examines the application of modern methods and tools for ensuring the security of web applications. Particular attention is devoted to authentication and authorization mechanisms, cryptographic protection methods, firewalls, intrusion detection and prevention systems, vulnerability assessment tools, secure coding practices, and continuous monitoring technologies. The study also considers the role of security testing, risk assessment, proactive threat detection, and access control mechanisms in strengthening the overall security posture of web-based systems. Furthermore, the article emphasizes the importance of applying integrated and multilayered security strategies capable of addressing both existing and emerging cyber threats.

The findings of the study indicate that no single security mechanism is sufficient to provide reliable protection for web applications operating in complex and dynamic digital environments. Effective security can only be achieved through the combined implementation of preventive, detective, and corrective measures. It is concluded that the application of modern methods and tools significantly enhances the resilience, reliability, and sustainability of web applications and contributes to the reduction of cyber risks in contemporary information systems.

Keywords: *web application security, cybersecurity, authentication, authorization, cryptographic protection, intrusion detection, intrusion prevention, vulnerability assessment, secure coding, risk assessment, cyber threats, information security*

Introduction

Web applications have become one of the most important elements of contemporary information systems and digital infrastructure. Their extensive use in public administration, finance, education, healthcare, e-commerce, and defense demonstrates their critical role in supporting data exchange, service delivery, communication, and operational management. The widespread integration of web-based platforms into organizational and institutional processes has significantly improved accessibility, efficiency, and flexibility. However, the increased reliance on web applications has also expanded the range of cybersecurity challenges associated with their development, deployment, and maintenance.

In modern digital environments, web applications are continuously exposed to a broad spectrum of security threats and vulnerabilities. Attackers frequently exploit weaknesses related to authentication, authorization, input validation, session management, data transmission, and server-side configuration. Among the most common and dangerous threats are SQL injection, cross-site scripting, cross-site request forgery, broken authentication, session hijacking, privilege escalation, and denial-of-service attacks. These threats may lead to unauthorized access, data leakage, loss of service availability, corruption of sensitive information, financial damage, and reputational loss. Consequently, web application security should be regarded as a strategic and multidimensional issue rather than merely a technical requirement.

The rapid evolution of cyber threats has demonstrated that traditional and isolated security mechanisms are no longer sufficient to provide reliable protection for web-based systems. The complexity of modern attacks requires the application of integrated, adaptive, and continuously improved security approaches. In this regard, contemporary web application security depends not only on technical controls, but also on secure software development practices, regular vulnerability assessment, real-time monitoring, effective access management, cryptographic protection, and incident response preparedness. The effective combination of these methods and tools contributes to the creation of a resilient security architecture capable of reducing cyber risks and improving the stability of digital services.

The main purpose of this article is to examine the application of modern methods and tools in ensuring the security of web applications. The study focuses on identifying major threats to web-based systems, analyzing contemporary protection mechanisms, and evaluating their importance in strengthening information security. Particular attention is given to authentication and authorization technologies, cryptographic mechanisms, firewalls, intrusion detection and prevention systems, vulnerability scanning tools, secure coding principles, and continuous monitoring solutions. The article also emphasizes the importance of adopting a comprehensive and multilayered approach to web application protection.

The scientific significance of the study lies in the systematization of modern approaches to web application security and in the analytical assessment of their role in mitigating cybersecurity risks. Its practical significance is determined by the fact that the results may be used in the design, implementation, and maintenance of secure web systems in various fields of application. The findings of the study may be beneficial for researchers, cybersecurity specialists, software developers, system administrators, and decision-makers involved in the protection of web-based environments. Therefore, the topic remains highly relevant both from theoretical and practical perspectives in the context of current cybersecurity challenges.

Main Threats to Web Applications

Web applications operate in open and highly dynamic digital environments, which makes them particularly vulnerable to a broad spectrum of cyber threats. Unlike isolated software systems, web-based platforms are continuously exposed to external interaction through browsers, application programming interfaces, network services, and distributed user sessions. This constant exposure substantially increases the probability of malicious interference, unauthorized access, and exploitation of software vulnerabilities. As a result, the identification and analysis of the main threats to web applications represent an essential stage in the development of an effective and sustainable security strategy.

Among the most common threats to web applications are SQL injection, cross-site scripting, cross-site request forgery, broken authentication, session hijacking, insecure direct object references, privilege escalation, and denial-of-service attacks. SQL injection remains one of the most dangerous attack methods because it allows attackers to manipulate database queries and gain unauthorized access to sensitive information. Cross-site scripting enables the injection of malicious scripts into trusted web pages, thereby threatening user data and session integrity, while cross-site request forgery allows unauthorized actions to be performed on behalf of legitimate users. Taken together, these threats can seriously affect the confidentiality, integrity, and availability of web-based systems.

Authentication- and session-related threats are also of critical importance in modern web environments. Weak password policies, improper session timeout settings, insecure token storage, and inadequate identity verification mechanisms may significantly increase the likelihood of unauthorized access and privilege abuse. In addition, insecure transmission channels and insufficient encryption mechanisms may expose credentials and session identifiers during data exchange. Such weaknesses may not only compromise individual accounts but may also undermine the overall trustworthiness of the system.

Another significant category of threats concerns service availability and operational continuity. Denial-of-service and distributed denial-of-service attacks are specifically designed to overload network or application resources, causing service degradation or complete interruption. Furthermore, insecure configuration, outdated software components, and weak access control policies may create favorable conditions for multi-stage attacks in which several vulnerabilities are exploited sequentially. This makes web applications especially vulnerable in environments where uninterrupted digital services are essential.

From an analytical perspective, the importance of these threats lies not only in their individual impact but also in their interdependence. Modern web attacks rarely occur in complete isolation; rather, they often emerge as interconnected stages of a broader attack chain. For this reason, web application protection should be based on an integrated and multilayered security approach rather than on fragmented technical controls. In this context, the novelty of the present study lies in the systematic treatment of web application threats as interrelated risk factors that must be addressed through the coordinated application of modern methods and tools.

Table 1. Main threats to web applications and their analytical significance

Threat	Brief description	Primary security impact	Relevance to the article's novelty
SQL injection	Manipulation of database queries through unsanitized input.	Confidentiality and integrity of stored data are compromised.	Demonstrates the need to combine secure coding, validation, and database protection measures.
Cross-site scripting (XSS)	Injection of malicious scripts into trusted web pages.	User data, browser sessions, and client-side trust are endangered.	Shows why client-side and server-side controls must be analyzed together.
Broken authentication and session hijacking	Exploitation of weak login logic, token handling, or session control.	Unauthorized access and privilege misuse may occur.	Supports the argument for integrating identity protection with monitoring and cryptographic safeguards.

Cross-site request forgery (CSRF)	Execution of unauthorized actions through forged requests in authenticated sessions.	Integrity of user actions and application workflows is threatened.	Illustrates the importance of layered request validation and access control.
Denial-of-service (DoS/DDoS)	Resource exhaustion through excessive malicious traffic.	Availability and continuity of services are reduced or lost.	Highlights that security must protect not only data, but also operational sustainability.
Insecure configuration and outdated components	Misconfiguration or obsolete software creates exploitable weaknesses.	Multiple dimensions of security can be simultaneously affected.	Reinforces the article's integrated view that technical maintenance is part of cybersecurity resilience.

Modern Methods of Ensuring Web Application Security

Ensuring the security of web applications requires the use of modern methods that address vulnerabilities across different stages of the software life cycle and multiple architectural layers. Contemporary cybersecurity practice shows that effective protection cannot be limited to post-deployment defense mechanisms alone. Security should begin at the design and development stages and continue through testing, deployment, monitoring, and incident response. Therefore, modern security methods should be understood as an interconnected system of preventive, detective, and corrective measures aimed at reducing cyber risks and strengthening the resilience of web-based systems.

One of the most fundamental methods of web application security is the implementation of strong authentication and authorization mechanisms. Authentication verifies user identity, while authorization determines access rights and privileges. The use of multi-factor authentication, role-based access control, least-privilege principles, and secure session management significantly reduces the risk of unauthorized access and privilege abuse, particularly in systems that process sensitive or mission-critical information.

Another essential method is cryptographic protection for data in transit and at rest. Secure communication protocols such as HTTPS and TLS help prevent interception, tampering, and unauthorized disclosure of transmitted information. In addition, password hashing and salting, encryption of confidential records, and secure protection of authentication tokens improve the overall security posture of web applications. These safeguards are especially important where the confidentiality and integrity of information must be preserved.

Secure coding practices also represent a central method of protection. Many cyberattacks originate from insecure code, weak input validation, inadequate error handling, and insufficient defense against common vulnerability classes. The adoption of secure software development principles, including input sanitization, parameterized queries, output encoding, dependency management, and code review, helps eliminate vulnerabilities before deployment. In this regard, security should be treated as an inherent design principle rather than as an additional control introduced after development.

Regular vulnerability assessment and security testing constitute another important method. Web applications should be continuously examined through vulnerability scanning, penetration testing, configuration analysis, and source code review in order to detect weaknesses before exploitation. This enables organizations to identify security gaps, assess cyber risks, and implement timely corrective measures. Security testing is particularly effective when integrated into the software development life cycle through continuous assessment procedures.

Continuous monitoring and threat detection are also key elements of modern web application security. Since digital environments evolve rapidly, previously secure systems may become vulnerable due to new attack techniques or configuration changes. For this reason, organizations rely on log analysis, SIEM

systems, web application firewalls, and intrusion detection or prevention systems to identify anomalous activities in real time. These methods improve the visibility of cyber events and support faster response to emerging threats.

From an analytical perspective, an important methodological improvement lies in combining these methods within an integrated and multilayered protection model. Instead of evaluating each method separately, web application security can be strengthened by linking access control, cryptographic protection, secure coding, vulnerability assessment, and continuous monitoring within a unified framework. Such an approach increases both the effectiveness of individual controls and the adaptive capacity of the overall system.

Thus, modern methods of ensuring web application security should be understood as a coordinated security architecture rather than a fragmented set of isolated mechanisms. Their effectiveness depends on consistent implementation, regular updating, and institutional support through organizational security policies.

Table 2. Modern Methods of Web Application Security and Their Functional Role

Method	Primary Security Function	Contribution to the Integrated Model
Authentication and authorization	Controls identity verification and access privileges	Provides the first defensive layer against unauthorized access
Cryptographic protection	Protects confidentiality and integrity of data	Secures sensitive information across communication and storage layers
Secure coding practices	Reduces design and implementation vulnerabilities	Prevents exploitable weaknesses before deployment
Vulnerability assessment and testing	Identifies security gaps and misconfigurations	Supports continuous improvement of security controls
Continuous monitoring and threat detection	Detects suspicious activity in real time	Strengthens adaptive response and operational visibility

Integrated Application of Modern Security Tools and Approaches in Web Application Protection

The effective protection of web applications depends not only on the selection of reliable security tools but also on the extent to which these tools are integrated into a coherent protection strategy. In contemporary cybersecurity practice, web application security is ensured through the coordinated use of technical controls, secure development approaches, testing procedures, and monitoring mechanisms. Therefore, the protection of web-based systems should be regarded as a multilayered process in which each security component performs a distinct yet complementary role.

Modern security tools used in web application protection include web application firewalls, intrusion detection and prevention systems, security information and event management platforms, vulnerability scanners, log analysis solutions, encryption mechanisms, and authentication management technologies. Each of these tools addresses a specific category of threats. Web application firewalls filter malicious requests at the application boundary, intrusion detection and prevention systems identify

suspicious behavior and support active defense, while vulnerability scanners help detect configuration weaknesses and software flaws before exploitation.

At the same time, these tools achieve greater effectiveness when combined with secure coding practices, access control policies, and regular security testing procedures. In this respect, the value of security tools lies not only in their individual technical functions but also in their ability to support prevention, detection, response, and recovery within a unified protection framework. Such coordination is particularly important in dynamic environments where attack techniques evolve rapidly and where a single defensive mechanism is rarely sufficient.

From a methodological perspective, web application security can be significantly strengthened by integrating technical tools with architectural and procedural security methods. Access control mechanisms reduce the risk of unauthorized use, cryptographic safeguards protect the confidentiality and integrity of data, secure coding practices minimize the emergence of exploitable vulnerabilities, and continuous monitoring improves visibility into abnormal behavior. When combined, these components create a stronger adaptive structure capable of resisting both conventional and emerging cyber threats.

The novelty-oriented contribution of this section lies in presenting modern security tools and methods as interacting layers of an integrated protection model rather than as independent security elements. This approach allows web application protection to be understood as a coordinated security architecture in which the effectiveness of each measure is reinforced by its relationship with the others. Thus, the combined application of modern tools and methods provides a more sustainable basis for protecting web applications than fragmented security solutions.

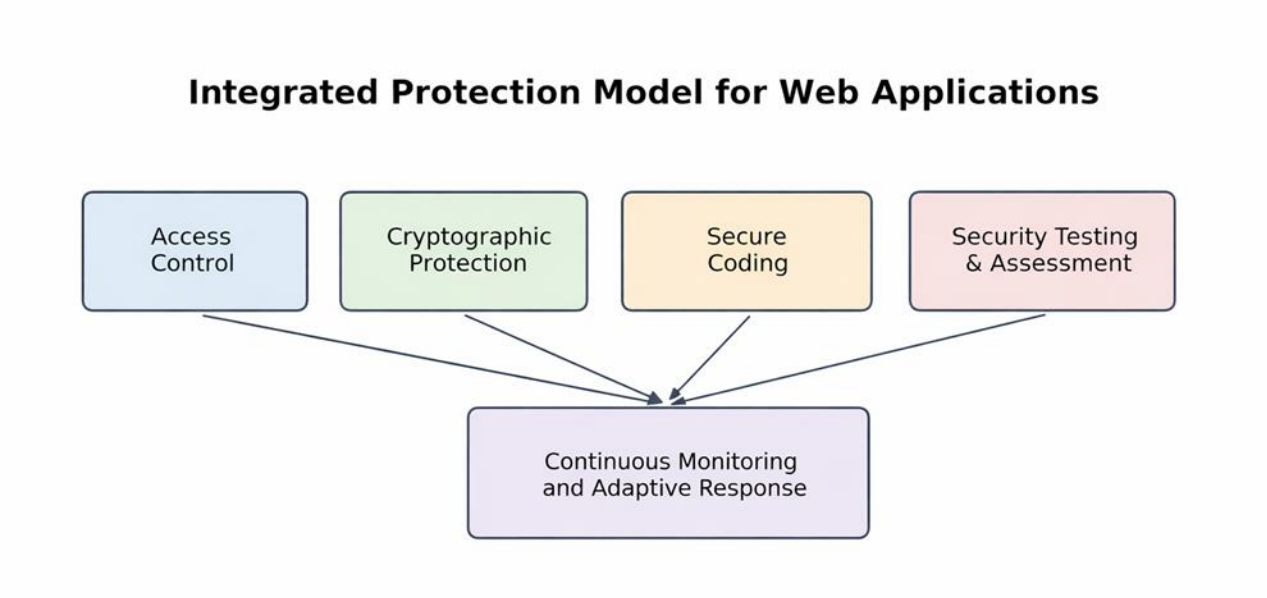

Figure 1. Integrated model of coordinated web application protection

Conclusion

Web application security remains one of the central issues of contemporary cybersecurity because organizations increasingly depend on web-based platforms for data exchange, service delivery, and operational management. The analysis presented in this study shows that web applications are exposed to a broad range of threats, including unauthorized access, injection attacks, session-related vulnerabilities, insecure configurations, and service disruption attempts. These risks demonstrate that effective protection

cannot be achieved through isolated technical measures alone, but requires a systematic and continuously updated security approach.

The study indicates that strong authentication and authorization, cryptographic protection, secure coding practices, vulnerability assessment, security testing, and continuous monitoring constitute the main components of effective web application protection. Their practical value becomes significantly greater when they are implemented in coordination rather than as separate mechanisms. In this regard, web application security should be understood as a multilayered and adaptive architecture in which preventive, detective, and corrective measures complement one another within a unified framework.

From a methodological perspective, one of the main contributions of the article lies in the integrated interpretation of modern security methods and tools. Instead of treating them as independent security elements, the study presents them as interrelated layers of a unified protection model. This approach increases both the analytical and practical value of the research and supports a more systematic understanding of how resilient web application security can be achieved in dynamic digital environments.

It can be concluded that the effective application of modern methods and tools significantly strengthens the resilience, reliability, and sustainability of web applications. Therefore, the adoption of integrated protection strategies should be regarded as one of the most effective directions for reducing cyber risks and improving the security of contemporary web-based systems.

REFERENCES

1. OWASP Foundation. OWASP Top 10: 2025. OWASP, 2025.
2. OWASP Foundation. OWASP Application Security Verification Standard (ASVS). Version 5.0. OWASP, 2025.
3. NIST. Secure Software Development Framework (SSDF), Version 1.1. NIST Special Publication 800-218, 2022.
4. NIST. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. NIST Special Publication 800-52 Revision 2, 2019.
5. NIST. Securing Web Transactions: TLS Server Certificate Management. NIST Special Publication 1800-16, 2019.
6. Stuttard, D., and Pinto, M. The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws. 2nd ed., Wiley, 2011.
7. McGraw, G. Software Security: Building Security In. Addison-Wesley, 2006.
8. Viega, J., and McGraw, G. Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley, 2001.
9. Halfond, W. G. J., Viegas, J., and Orso, A. A Classification of SQL-Injection Attacks and Countermeasures. Proceedings of the IEEE International Symposium on Secure Software Engineering, 2006.
10. Grossman, J. Cross-Site Scripting Attacks. InformIT, 2007.
11. OWASP Foundation. OWASP Web Security Testing Guide. OWASP Project Documentation.
12. OWASP Foundation. OWASP Cheat Sheet Series. OWASP Project Documentation.