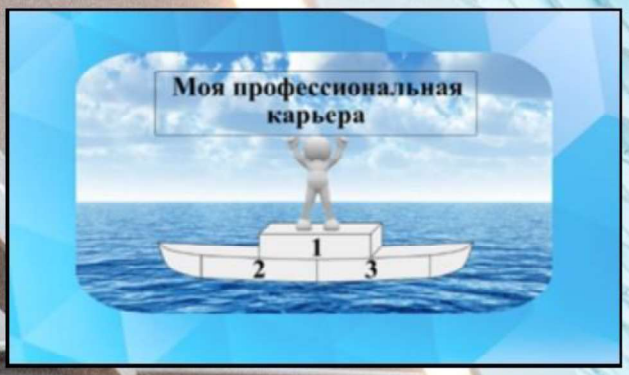

ISSN INTERNATIONAL STANDARD SERIAL NUMBER
ISSN 2782-4365
Проверить номер:

Научно-образовательный электронный журнал

ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ

Выпуск №59-4 (том 1)
(февраль, 2025)

Google Scholar
Проверить индексацию статьи. Сайт: mpcareer.ru/google

Свидетельство о регистрации СМИ №ЭЛ ФС 77-77927 от 19.02.2020 г.
РОСКОМНАДЗОР

Периодичность выпуска: 1 раз в неделю
Сайт: mpcareer.ru/oinv21veke. Почта: obrmpcareer@mail.ru

Международный научно-образовательный электронный журнал
«ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ»

ISSN 2782-4365
УДК 37
ББК 94

Международный научно-образовательный электронный журнал «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ». Выпуск №59-4 (том 1) (февраль, 2025). Дата выхода в свет: 03.03.2025.

Сборник содержит научные статьи отечественных и зарубежных авторов по экономическим, техническим, философским, юридическим и другим наукам.

Миссия научно-образовательного электронного журнала «ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ» состоит в поддержке интереса читателей к оригинальным исследованиям и инновационным подходам в различных тематических направлениях, которые способствуют распространению лучшей отечественной и зарубежной практики в интернет пространстве.

Целевая аудитория журнала охватывает работников сферы образования (воспитателей, педагогов, учителей, руководителей кружков) и школьников, интересующихся вопросами, освещаемыми в журнале.

Материалы публикуются в авторской редакции. За соблюдение законов об интеллектуальной собственности и за содержание статей ответственность несут авторы статей. Мнение редакции может не совпадать с мнением авторов статей. При использовании и заимствовании материалов ссылка на издание обязательна.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Рахматова Фотима Ганиевна	доктор философии по педагог. наукам (PhD), доцент
Рахмонов Азизхон Боситхонови	доктор педагогических наук, доцент
Таспанова Айзада Кенжебаевна	доктор философии (PhD) по экономическим наукам
Таспанова Жыгагул Кенжебаевна	доктор философии по педагог. наукам (PhD), доцент
Табашникова Ольга Львовна	кандидат экономических наук, доцент
Тўрабоева Мадинахон Рахмонжон қизи	кандидат педагогических наук, доцент
Тюрин Александр Николаевич	кандидат географических наук, доцент
Уразова Лариса Карамовна	кандидат исторических наук, доцент
Усубалиева Айнура Абдыжапаровна	кандидат социологических наук, доцент
Утегенова Жамила Джолмурзаевна	доктор философии по эконом. наукам, доцент
Фаттахова Ольга Михайловна	кандидат технических наук, доцент
Ширинов Отабек Тувалович	доктор психологических наук (PhD)
Хамдамова Ситора Сафаровна	Доктор философии в области философских наук, доцент
Ханбабаев Хакимжан Икрамович	доктор педагогических наук (DSc)
Худайкулов Хол Джумаевич	доктор педагогических наук, профессор
Худойбердиева Хурият Каримбердиевна	доктор философии (PhD) в социальной философии
Ширинов Отабек Тувалович	доктор психологических наук (PhD)
Эшназаров Журакул	кандидат педагогических наук, профессор
Эшназарова Фарида Журакуловна	доктор философии по философии (PhD)
Юнусова Бахора Ахтамжоновна	кандидат филологических наук, ассистент
Яхяева Сожида Абдурахимовна	доктор философии (PhD) в социальной философии

Galandarova Aysoltan, Porrykov Dowletmyrat METHODS OF TEACHING MEDICAL BIOTECHNOLOGY	291
Agajan Myradov STATE SOVEREIGNTY IN INTERNATIONAL LAW: EVOLUTION, CHALLENGES, AND FUTURE PROSPECTS	296
Durdyyeva Enejan Geldimyradovna, Bayriyeva Selbinyaz TEACHING THE LANGUAGE OF LITERACY	301
Agayeva Suray, Annayeva Ayna THE METHODOLOGY OF TEACHING ENGLISH LANGUAGE TO CHILDREN IN PRESCHOOL	304
Ahmetyar Yusupov THE CONCEPT OF SOVEREIGNTY IN INTERNATIONAL LAW: FOUNDATIONS, IMPLICATIONS, AND CONTEMPORARY CHALLENGES	309
Mommadov Hudaynazar, Kurambayev Yoldashbay MOBILE APPLICATION FOR TEACHING ENGINEERING GRAPHICS	314
Berdiyeva Gulshat, Yazdurdyyeva Mahym THE ROLE OF MATHEMATICAL GAMES IN DEVELOPING PUPILS' LOGICAL THINKING	317
Arslan Hudayberdiyev INTERNATIONAL ORGANIZATIONS AS SUBJECTS OF INTERNATIONAL LAW	322
Suhanov Seyrangeldi, Seyitmyradov Begench THE FRANCHISING MODEL IN THE NEW ECONOMIC REALITY	327
Gayypova Shirinay, Saparova Seyyara THE PARTICULARITIES OF GUIDING STUDENTS TOWARDS A VOCATION	331
Muhammetnazar Shaliyev THE PRINCIPLE OF STATE RESPONSIBILITY IN INTERNATIONAL LAW	335
Ashyrow Ashyr, Orazdurdyyeva Gulshat AI TECHNOLOGIES IN CYBERSECURITY	340
Hommadova Bagul, Porrykov Dowletmyrat METHODOLOGY OF TEACHING CELL AND TISSUE ENGINEERING	344
Gozel Gutlyyeva PEOPLES FIGHTING FOR SELF-DETERMINATION AS SUBJECTS OF INTERNATIONAL LAW	349
Bayramova Bagul, Orazdurdyyeva Gulshat SECURITY OF WEB APPLICATIONS	354

ФИО автора(-ов): *Bayramova Bagul, student.*
Orazdurdyyeva Gulshat, teacher.
Oguzhan Engineering and Technology University of Turkmenistan.
Ashgabat, Turkmenistan
Название публикации: «SECURITY OF WEB APPLICATIONS»

Abstract: The increasing reliance on web applications for various business, financial, and personal activities has led to an escalating risk of cyberattacks targeting these platforms. Web applications are often the primary attack vectors for malicious actors, making their security a paramount concern. This paper discusses the fundamental security challenges faced by web applications, including common vulnerabilities such as cross-site scripting (XSS), SQL injection, and cross-site request forgery (CSRF). It explores the role of secure coding practices, encryption, and authentication mechanisms in mitigating these risks. Additionally, the paper reviews modern techniques for enhancing web application security, such as penetration testing, threat modeling, and the use of web application firewalls (WAFs). By analyzing current literature and case studies, the paper provides an in-depth look at best practices, tools, and strategies for securing web applications in an increasingly complex threat landscape.

Keywords: web application security, vulnerabilities, cross-site scripting, SQL injection, secure coding, encryption, authentication, penetration testing, web application firewall, threat modeling

1. Introduction:

With the rapid evolution of digital services and the increasing reliance on online platforms for communication, commerce, and social interaction, web applications have become essential to everyday life. However, this ubiquity has also made them prime targets for cyberattacks. Cybercriminals exploit various vulnerabilities in web applications to steal sensitive data, compromise system integrity, and cause significant damage to both organizations and individuals.

Web application security is a critical aspect of safeguarding sensitive information, ensuring business continuity, and maintaining user trust. As cyber threats become more sophisticated, securing web applications requires a comprehensive approach that includes secure coding practices, regular vulnerability assessments, encryption, and robust authentication mechanisms. This paper examines the key security challenges web applications face, the techniques and strategies used to mitigate these risks, and the best practices for maintaining the integrity and confidentiality of web-based services.

2. Background and Literature Review:

The security of web applications has been a focal point of research and development for over two decades. According to OWASP (Open Web Application Security Project), some of the most prevalent web application vulnerabilities include cross-site scripting (XSS), SQL injection, and cross-site request forgery (CSRF). These vulnerabilities are frequently exploited in cyberattacks, allowing attackers to steal credentials, perform unauthorized actions, and inject malicious scripts into web pages (OWASP, 2021).

Additionally, secure coding practices have been identified as one of the most effective ways to mitigate the risk of these vulnerabilities. Research by McGraw (2006) suggests that integrating security into the software development lifecycle (SDLC) is crucial for building secure applications from the ground up. Encryption techniques, such as end-to-end encryption (E2EE), also play an essential role in protecting sensitive data transmitted between clients and servers (Stallings, 2016).

Penetration testing and threat modeling have become integral in identifying and addressing potential weaknesses before they are exploited in the real world. Penetration testing simulates real-world attacks on web applications to uncover vulnerabilities, while threat modeling helps organizations understand potential threats and design security measures accordingly (Mohan et al., 2020).

3. Methodology:

This paper employs a comprehensive review methodology, analyzing existing literature, case studies, and industry reports on web application security. The study focuses on the following key areas:

1. **Common Vulnerabilities**: A review of the most frequent web application vulnerabilities such as XSS, SQL injection, and CSRF, along with examples of real-world attacks.
2. **Security Best Practices**: An exploration of secure coding practices, encryption techniques, and authentication methods for mitigating vulnerabilities.
3. **Security Tools and Techniques**: A discussion on the tools available for enhancing web application security, including web application firewalls (WAFs), penetration testing, and vulnerability scanners.
4. **Emerging Trends**: An analysis of new trends and technologies that are shaping web application security, such as AI-driven security tools and the increasing role of automated security testing.

4. Results and Discussion:

4.1 Common Web Application Vulnerabilities:

Web applications face a wide array of vulnerabilities, many of which are exploited by attackers to gain unauthorized access to systems or to execute malicious activities. For example, SQL injection occurs when user input is improperly validated, allowing attackers to execute arbitrary SQL queries that can manipulate the backend database. Similarly, XSS exploits vulnerabilities in web pages to inject malicious scripts that execute on the client side, often leading to session hijacking or data theft (OWASP, 2021).

4.2 Mitigation Techniques and Best Practices:

To mitigate these risks, secure coding practices are essential. Input validation, parameterized queries, and output encoding are some of the techniques that can help prevent SQL injection and XSS attacks. Furthermore, encryption methods such as SSL/TLS encryption should be employed to secure data in transit, ensuring that

sensitive information such as passwords and credit card numbers are not intercepted by attackers.

Authentication mechanisms, such as multi-factor authentication (MFA) and strong password policies, are crucial for ensuring that only authorized users can access sensitive data and perform critical actions within the web application. Secure session management, including session timeouts and secure cookies, can help prevent session hijacking (Stallings, 2016).

4.3 Tools for Enhancing Security:

Web application firewalls (WAFs) are essential in defending against common attacks, such as SQL injection and XSS, by filtering and monitoring HTTP traffic between the web application and the internet. Additionally, penetration testing tools, such as Burp Suite and OWASP ZAP, help identify vulnerabilities before they can be exploited in real-world attacks. Vulnerability scanning tools like Acunetix and Nessus can automate the detection of security flaws in web applications, enabling security teams to address issues promptly (Mohan et al., 2020).

4.4 Emerging Trends in Web Application Security:

As cyber threats continue to evolve, new technologies and methodologies are being introduced to enhance web application security. Artificial Intelligence (AI) and machine learning (ML) are being leveraged to detect patterns of suspicious behavior, identify anomalies, and automate threat detection. Additionally, the increasing adoption of DevSecOps practices, where security is integrated into the development process, is helping organizations build more secure web applications from the start (McGraw, 2006).

5. Conclusion:

The security of web applications is a critical aspect of protecting sensitive data and maintaining user trust in online platforms. While significant progress has been made in securing web applications, the growing complexity of cyberattacks requires organizations to adopt a proactive approach to security. By implementing secure coding practices, using encryption and authentication mechanisms, and leveraging modern tools like WAFs and penetration testing, organizations can better protect their

web applications from evolving threats. As new technologies such as AI and machine learning continue to emerge, they will further enhance the ability to detect, prevent, and respond to cyberattacks in real-time, creating more resilient web application security systems.

References

1. McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley.
2. Mohan, A., Patel, P., & Hakkim, A. (2020). Web Application Security: Penetration Testing and Ethical Hacking. Wiley.
3. OWASP Foundation. (2021). OWASP Top 10 Web Application Security Risks. https://owasp.org/www-project-top-ten/
4. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. Pearson.