Вісник Тернопільського національного технічного університету
https://doi.org/10.33108/visnyk_tntu
Scientific Journal of the Ternopil National Technical University
2024, № 3 (115) https://doi.org/10.33108/visnyk_tntu2024.03
ISSN 2522-4433. Web: ***visnyk.tntu.edu.ua***

UDC 004.056.5:004.056.8:004.056.75

FRONT-END SECURITY ARCHITECTURE: PROTECTION OF USER DATA AND PRIVACY

Aleksei Chechet[1]; Maksim Chernykh[2]; Iaroslav Panasiuk[3]; Ilnur Abdullin[4]

[1]New Edge DWC-LLC, Dubai, United Arab Emirates
[2]Boom Pay, Inc, Austin, United States of America
[3]Agoda Services Co., Ltd., Bangkok, Thailand
[4]National Information Technology Center, Bishkek, Kyrgyz Republic

Abstract. *Investigation of this topic is relevant in light of the significant increase in the frequency and scale of cyber-attacks that affect various industries and organisations. The purpose of this study is to analyse existing data protection methods at the Front-end, which are able to effectively protect the confidentiality of user data in the face of modern cyber threats. Among the methods used, the analytical method, synthesis, classification, statistical and other methods should be noted. The study identified serious risks associated with storing confidential data on the client side. In particular, the use of cookies and local storage turned out to be vulnerable points that pose potential threats to data security. An analysis of existing web applications revealed the presence of cross-site scripting (XSS) vulnerabilities, which became a route for the introduction of malicious scripts. It was revealed that the generation and use of unique cross-site request forgery (CSRF) tokens for each request play a key role in preventing cross-site request forgery. The implementation of Governance as Code (GaC) technology has demonstrated potential for automating compliance with established architectural and security standards, thereby reinforcing front-end defenses against cyber threats. The findings emphasise the importance of educating end users on the basic principles of network security. The study highlights the importance of developers' active involvement in Front-end security. Thus, a comprehensive overview of the Front-end security architecture with a focus on protecting user data and ensuring privacy is provided. The practical significance of the study lies in the provision of specific recommendations and practical solutions to improve Front-end security in web applications and represents a valuable set of tools and approaches that can be applied by developers and engineers to strengthen the security of web applications. The addition of Governance as Code technology introduces an innovative layer of automated security enforcement that is particularly suited to addressing emerging cybersecurity challenges in real-time.*

Key words: *data encryption, vulnerabilities, cross-site scripting, technology development, implementation, architecture, governance as code.*

https://doi.org/10.33108/visnyk_tntu2024.03.005 *Received 18.04.2024*

1. INTRODUCTION

In the digital age, when web applications and interactive interfaces are becoming more widespread, Front-end security is becoming an integral part of ensuring high standards of data protection and privacy that meet the requirements of the user experience. The Front-end security architecture plays a crucial role in creating reliable web applications, providing not only modern and functional interfaces, but also reliable protection of data stored and processed on the client side. With the constant growth of threats in the field of cybersecurity, issues related to the protection of user data and privacy are becoming more acute and require a comprehensive approach.

The problems of this study are centred on several key aspects. The main challenges are the risks associated with storing and transferring data on the client side, and vulnerabilities and attacks aimed at the Front-end. Analysing and preventing such threats requires not only effective privacy practices, but also compliance with security standards adapted to the specifics of Front-end development.

Corresponding author: Aleksei Chechet; e-mail: A.Chechet08@gmail.com ……..…… 5

The study by M. Tsulukidze et al. [1] has determined the current level of personal data protection in Georgia to identify problems and offer recommendations to improve security. As a result, the researchers identified the strengths and weaknesses of the personal data protection system in Georgia and provided suggestions for improving legislation and control mechanisms. The purpose of the study by V. Napetvaridze and A. Chochia [2] was to investigate the development of cybersecurity strategies in Georgia in the context of policy and legal regulation to identify effective methods and recommendations for the future strengthening of cybersecurity. The researchers provided suggestions for finalising existing legislation to better meet modern challenges in cyberspace and developed practical tips and recommendations for ensuring security.

The study by A. Sivasangari et al. [3] has developed and evaluated the effectiveness of integrating blockchain technology into the security structure of medical data to ensure a high level of confidentiality and protection against threats. An integrated blockchain structure has been developed that can provide a high level of security and confidentiality of medical data. The effectiveness of using blockchain technology to solve security problems has been revealed. The main purpose of the study by D. Feldman and E. Haber [4] was to identify modern challenges and threats to privacy in the era of constant access and to develop effective methods and means of data protection. The researchers revealed an increase in the complexity of threats in the era of constant access, including attacks on personal devices, internetwork attacks, and data leaks. Methods for measuring the level of confidentiality have been developed and proposed, including analysis of the encryption level, access control, and data monitoring. The study by D. Amo et al. [5] was dedicated to the analysis and development of a plugin for Moodle, which not only increases the level of user privacy, but also provides support through the use of aliases. The researchers have developed a plugin that provides additional tools and settings for managing data privacy in Moodle. The introduction of user aliases helped to create an additional layer of anonymity, providing a level of trust for students.

These studies are valuable in the context of data security analysis, but they do not cover aspects related to the Front-end security architecture and user data protection at the web application interface level. The study focused on general data protection strategies and methods, without affecting the specifics of Front-end development and security issues at this level. The research mainly described aspects of legal regulation, the effectiveness of integrating technologies and threat analysis methods, but did not provide practical recommendations and solutions aimed at protecting user data through Front-end architecture.

The purpose of this study is to analyse the threats and risks associated with Front-end architecture. Additionally, within the framework of the study, the following tasks were set: analysis of existing security standards, such as Open Web Application Security Project (OWASP) Top Ten, and their compliance with modern security requirements for Front-end applications; development of recommendations for the use of modern encryption methods that contribute to the creation of secure web applications for effective protection of user data during their transfer and storage.

2. MATERIALS AND METHODS

Conducting a scientific study on the methods of ensuring the security and confidentiality of data in the Front-end involved the application of a certain methodology aimed at disclosing the content of the subject matter. The analytical method enabled an in-depth analysis of the topic under study, identified key aspects and principles of the Front-end security architecture, and analysed the effectiveness of these methods to ensure the security of user data and confidentiality. The synthesis provided an opportunity to combine various aspects of security and create an integrated protection system. The synthesis process involved the integration of various Front-end security approaches. This included a set of analytical methods aimed at

identifying vulnerabilities, with methods for designing secure architectural solutions. Based on the analysis of vulnerabilities identified using the analytical method, a synthesis of effective measures and protection mechanisms was carried out. This included developing recommendations to prevent cross-site scripting (XSS) attacks, improving the generation and use of unique CSRF tokens, and identifying effective end-user training methods.

The classification method helped to systematise and organise a large amount of information about security threats, vulnerabilities, and protection measures. This helped to better understand the structure and nature of the security problem. It allowed developing a structured system of data protection measures that considers different levels of threats and vulnerabilities. This provided an integrated approach to security and allowed for effective risk management. By classifying threats and vulnerabilities and determining their criticality for data security, the most significant aspects have been identified on which efforts to improve Front-end security should be focused.

The statistical method evaluated the main characteristics of the data, such as the mean, median, standard deviation and others, which facilitates understanding the data structure and identifying the security features of the Front-end. By using statistical tests such as t-tests, variance analysis (ANOVA) or correlation analysis, the statistical method helped to draw conclusions about the statistical significance of differences between data groups, evaluated the effectiveness of specific security measures. The statistical method was used to process data, calculate statistical indicators, and to build statistical models in order to predict future trends or probabilities in the field of Front-end security. This allowed making decisions based on statistically sound assumptions.

The comparative analysis in this study included the choice of data protection methods, the collection of data on the principles of operation, advantages, disadvantages, degree of protection, performance, and other parameters of each method. It allowed for a detailed analysis of the advantages and disadvantages of each method, evaluating their performance, including the execution time of operations and the impact on the overall performance of the web application. After data collection and analysis, the results of various Front-end data protection methods were compared. The strengths and weaknesses of each method were identified, and the areas of their optimal application were determined. Based on the conducted comparative analysis, general conclusions were formulated about the effectiveness and applicability of data protection methods at the Front-end, and recommendations for choosing the most appropriate methods for specific situations and tasks.

3. RESULTS

During the analysis of threats and vulnerabilities in the Front-end, a number of key aspects faced by web applications were identified. Cross-site scripting (XSS) is one of the most common types of Front-end attacks [6]. It represents a serious vulnerability when attackers inject malicious scripts into a web page, which are then executed in the user's browser. This can lead to various types of attacks, such as theft of session cookies, interception of input data, and other types of manipulation of a web page or user data. Insufficient filtering of data entry and unverified information output on the client side really create a vulnerability, allowing attackers to inject malicious scripts. In the context of Front-end web applications, where user interaction takes place directly in the browser, cross-site scripting becomes especially dangerous. In such applications, insufficient validation of input data and lack of control over the output of information on the client side can lead to serious consequences, such as theft of user data or performing unauthorised actions on their behalf.

Cross-site request forgery (CSRF) attacks are among the most common and dangerous threats to web applications [7]. In this type of attack, attackers use the user's trust in the website

to perform unwanted actions on their behalf. The attacker creates a fake request that is sent to the web server using the user's authentication data, for example, cookies. This request may contain commands to modify the data executed on the server. An example would be a malicious script embedded on another website or sent via a malicious email. When a user visits this site or opens an email, the script executes a request to the target website on behalf of the user. If the website is not protected from CSRF, it can execute this request without even suspecting that it was not initiated by the user. Such attacks lead to various consequences, including changing the user's password, performing financial transactions, sending malicious messages, etc. Therefore, CSRF protection is an important aspect of securing web applications.

The use of cookies and local storage are the main methods of storing data on the client side in web applications [8]. One of the identified risks is the possibility of unauthorised access to data stored in cookies and local storage. Insufficient protection of this data can lead to leaks of confidential information, which is a serious threat to user privacy. An additional aspect of the analysis is the risk of data manipulation on the client side. Attackers may try to change the data stored in cookies or local storage, affecting the operation of the application or even provoking erroneous actions on behalf of the user. In addition, the risk of vulnerability to various forms of attacks, such as data interception and request forgery, has been identified. Unauthorised access to user data or the possibility of introducing malicious scripts through cookies and local storage become paths for potential attacks.

Typical risks such as XSS, and CSRF attacks, together with potential threats related to data storage on the client side, represent important security aspects of Front-end web applications [9]. Figure 1 shows the distribution of threats in Front-end web applications, indicating the importance of each of them in the security context. In the process of creating the diagram, specific characteristics are considered, which makes it an informative tool for making security decisions.

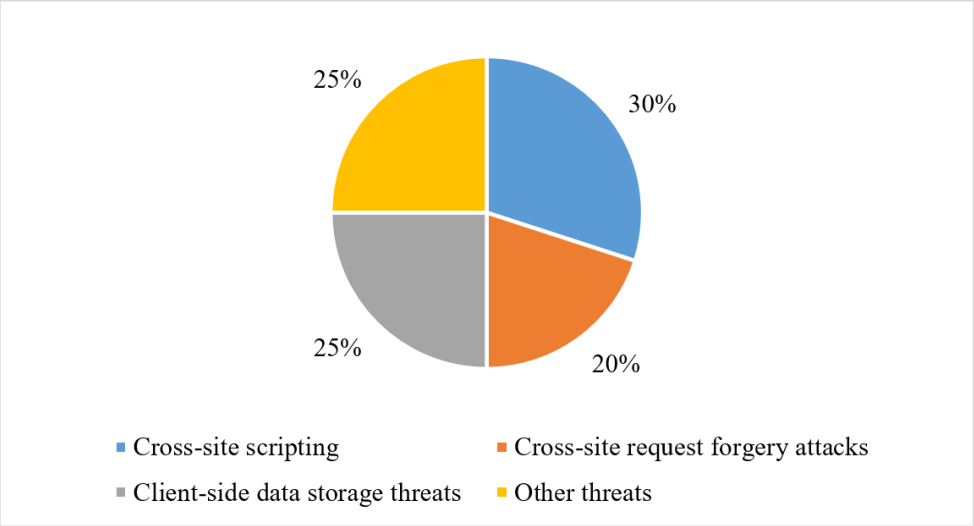

Figure 1. Threat distribution in Front-end web applications

Source: compiled by the authors.

The concept of security in Front-end development is becoming increasingly critical in the face of ever-increasing cyber threats [10]. In this regard, the development of effective data encryption mechanisms at the stages of their transmission and storage plays an important role. When choosing the appropriate encryption algorithms to ensure the security of the Front-end

architecture, various aspects must be considered, including the security and performance requirements of the application. Asymmetric algorithms such as Rivest-Shamir-Adleman (RSA) or Error Correction Code (ECC) can be used to exchange keys and sign data, providing a high level of security when transferring information between the client and the server.

Symmetric algorithms such as Advanced Encryption Standard (AES) provide effective encryption of data on the client side, considering the limited computing resources of the browser [11]. In addition, the use of hash functions such as SHA-256 can ensure data integrity and protect against information substitution during transmission. Evaluating each algorithm in the context of a specific application will help to choose the optimal combination of encryption methods, ensuring a balance between security and performance. Figure 2 demonstrates the importance of these encryption methods.

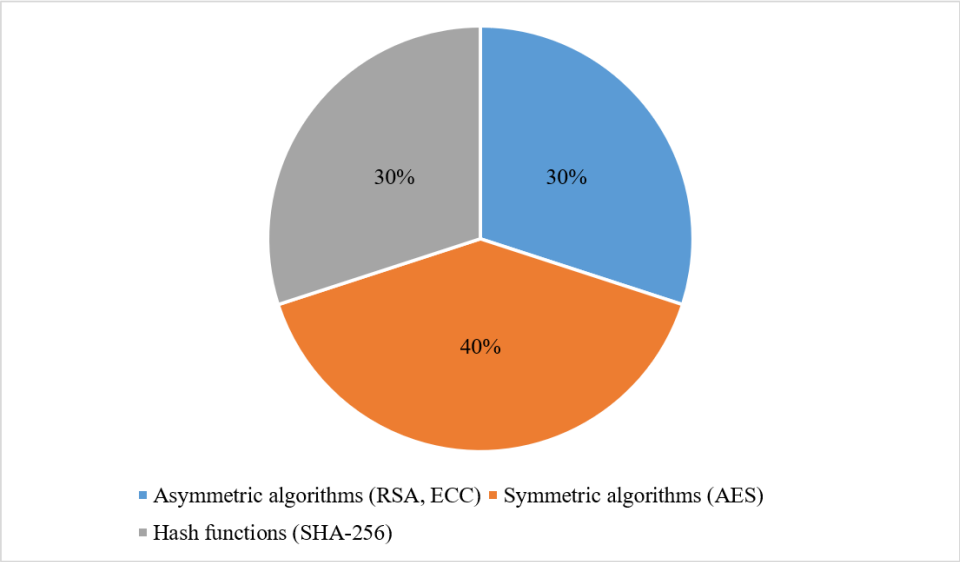

Figure 2. Importance of security data encryption methods Front-end development

Source: compiled by the authors.

The use of data encryption during transmission is a key aspect of ensuring the security of web applications. To do this, developers can use transport layer encryption protocols such as HyperText Transfer Protocol Secure (HTTPS) [12]. HTTPS provides secure data transfer between the client and the server by encrypting information, which significantly reduces the risk of hackers intercepting and reading confidential data. When using HTTPS, all traffic between the user's browser and the server is automatically encrypted, which ensures the confidentiality of the transmitted information. This encryption method not only protects user data, but also ensures the integrity and authenticity of the transmitted data. Thus, HTTPS is an effective means of protecting information during transmission on the network. Encryption key management plays an important role in ensuring data security. This includes secure storage and key exchange between the various components of the system. Encryption keys must be protected from unauthorised access, and updated and restored if necessary. Effective key management ensures the safety of information and prevents possible attacks on data.

Testing and auditing of encryption mechanisms are necessary to ensure their reliability and security [13]. Regular vulnerability checks and audits help identify potential problems and errors in the implementation of data encryption. This allows developers to fix the detected vulnerabilities and increase the security level of the system as a whole. Testing and auditing also contribute to compliance with security standards and ensure user confidence in the system.

The introduction of authentication and authorisation mechanisms is a critical step in ensuring the security of the system [14]. The authentication mechanism is designed to verify the authenticity of users by authenticating their IDs. The study examines various authentication methods such as password authentication, two-factor authentication, biometric authentication, etc. The goal is to ensure reliable authentication of users before granting access to confidential data. The authorisation mechanism determines user access rights to various resources and system functionality. Access rights management methods, role-based access model, role-based access policies, and other aspects were considered. The goal is to ensure that only authorised users have access to certain sensitive data corresponding to their roles and rights. The consideration of these mechanisms in the framework of the study is aimed at ensuring that only authorised users have access to confidential data, and at preventing unauthorised access to them. All these mechanisms work together to protect the confidentiality of data, prevent unauthorised access to it, and ensure compliance with information security principles. Their consideration and analysis within the framework of the study helps to identify and implement optimal data protection strategies in the Front-end architecture. Figure 3 depicts the importance of different authentication mechanisms in Front-end development.

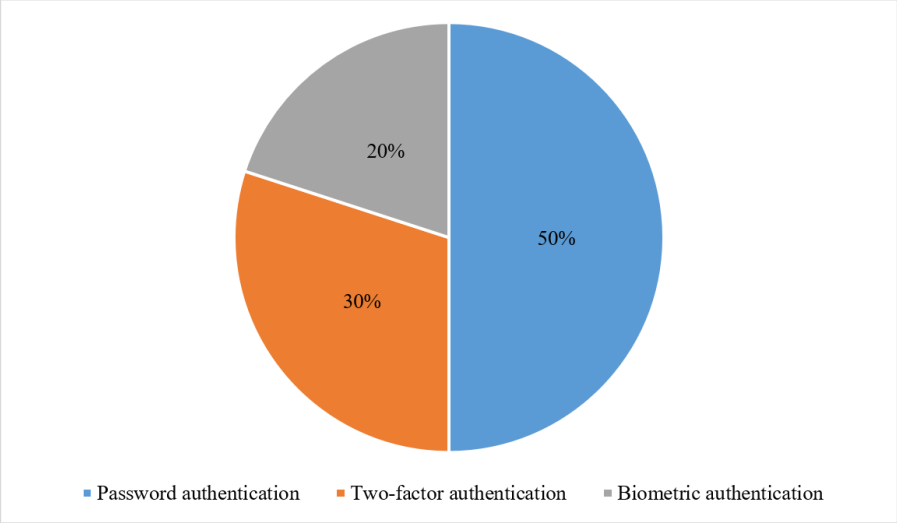

Figure 3. Importance of authentication mechanisms in Front-end development

Source: compiled by the authors.

To ensure the security of the Front-end architecture, compliance with security standards such as OWASP Top Ten is of particular importance, which is a key aspect of achieving this goal. This ensures not only that the technologies and methods used comply with security recommendations, but also provides developers with a reliable foundation to minimise risks and vulnerabilities during the development and operation of Front-end applications. By complying with OWASP Top Ten security standards, developers get access to an extensive set of recommendations and best practices that can be directly applied to applications under development. These recommendations cover various aspects of security, including protection against cross-site scripting, Structured Query Language (SQL) injections, incorrect authentication, incorrect authorisation, and other common threats. Compliance with security standards also helps to raise developers' awareness of current trends and threats in the field of cybersecurity. This allows them to be prepared for new threats and respond effectively to them using advanced protection methods. Moreover, by complying with security standards, developers get the opportunity to demonstrate a high

level of user data protection, which strengthens trust in their applications and helps strengthen the company's image as a whole.

Training and awareness-raising are important components in ensuring the security of Front-end architecture [15]. To achieve this goal, training events are held for both end users and developers. For end users, the training covers various aspects of security in an online environment, including the threats they may face when using web applications, and data protection methods. This may include training on how to store passwords securely, recognise suspicious activity, and notify about security threats. For developers, the training is aimed at an in-depth understanding of data protection methods and the application of best practices in the development of Front-end applications. This includes training on modern security threats, authentication and authorisation methods, and data encryption principles. Training events for developers may also include practical exercises and case studies, allowing them to put their knowledge into practice and develop secure applications from the very beginning of the process.

Considering the development of an effective Front-end architecture, key recommendations are highlighted, based on which developers can actively contribute to ensuring the security of the Front-end. The following aspects are personal recommendations developed based on the analysis. It is recommended to conduct periodic code audits with an emphasis on identifying potential vulnerabilities and evaluating the overall security of the code base. This approach will help identify and fix problems even at the development stage, reducing security risks. It is important to actively monitor updates to third-party libraries and components used in the project. It is recommended to update dependencies regularly, implementing security fixes, and paying special attention to maintaining up-to-date versions. Developers are advised to strictly adhere to established security standards during the design and writing of Front-end code. This includes the use of safe programming practices, proper data entry processing, and careful management of cross-site scripting.

The recommendations provide for careful monitoring of data storage methods on the client side, considering the specifics of threat and vulnerability analysis. In this context, it is recommended to actively use encryption mechanisms for data stored on the client side in order to prevent unauthorised access and protect confidential user information from possible threats. It is also strongly recommended to use the HTTPS protocol to ensure secure data transfer between the client and the server.

Threat and vulnerability analysis highlighted the importance of combating cross-site scripting, CSRF attacks, and the risks associated with client-side data storage. The study of cross-site scripting revealed that insufficient filtering of data entry and unverified output of information can open up opportunities for the introduction of malicious scripts. Recommendations include implementing strict filtering methods, secure data output, and using Content Security Policy to prevent XSS attacks. Analysis of CSRF attacks has revealed their serious threat potential, especially in the context of Front-end web applications. Recommendations include the introduction of mechanisms for generating unique CSRF tokens, regular updating of session data, and strict access control to important operations. An assessment of vulnerabilities related to data storage on the client side revealed the risks associated with the use of cookies and local storage.

These personalised recommendations provide practical steps to improve the security of Front-end development and can be implemented into the workflow to ensure the reliability and protection of web applications being created.

4. DISCUSSION

The Front-end security architecture is a fundamental aspect of security in web applications. The research has penetrated deeply into this issue, identifying key points that form the basis for the reliability and confidentiality of user data. Interface design has a significant

impact on the overall security of the system, and this study emphasises that effective protection begins from the very beginning of development – with Front-end design. The threat analysis highlighted the importance of developing and implementing effective mechanisms to protect user data. The methods of storing and transmitting data on the client side pose significant risks that require reliable measures to ensure them. Various types of attacks, such as cross-site scripting and cross-site request forgery, can leak confidential information and cause damage to both users and organisations.

It is important to note that a detailed examination of the Front-end architecture reveals vulnerabilities and security threats that may be overlooked at higher levels of development. The study raised questions not only about the technical side of security, but also about the impact of interface design on data security.

The research represents a very relevant contribution to the modern digital world, where threats to the security of user data are becoming more significant. With the growth of digitalisation and the widespread use of web applications, ensuring reliable protection of user data is becoming an integral part of development. The importance of education and training for both developers and end users should be emphasised. Teaching users the basics of cybersecurity and developing self-defence skills can significantly reduce the risk of successful attacks.

The purpose of the study by P.N. Hiremath et al. [16] was a critical analysis of the MyWebGuard tool in terms of its effectiveness in ensuring security and protecting online privacy. The research was aimed at identifying the strengths, possible limitations, and potential for improvements of this tool. The results not only identified strengths and areas for further improvement of the tool, but also provided valuable recommendations for developers and users in order to improve the security environment on the Internet. Both studies successfully address security and privacy concerns, and contain overlapping recommendations or conclusions. The main purpose of the study by P. N. Hiremath et al. [16] was to identify the strengths and weaknesses of this tool, and to provide recommendations for its improvement. In turn, this study focuses on the analysis of existing data protection methods at the Front-end, which contribute to the creation of an effective and reliable architecture for protecting user data in the face of modern cyber threats. Both studies aim to increase the level of security on the Internet.

S. Hutt et al. [17] evaluated the current infrastructure used in the Massive Open Online Course (MOOC) and its compliance with security and privacy requirements. The assessment of the technical side of the MOOC infrastructure included an analysis of the protection of servers, databases, and their transfer. The researcher identified technological weaknesses and vulnerabilities and offered recommendations for their elimination. The effectiveness of access control systems and their ability to prevent unauthorised access to students' personal information was investigated and the privacy policies offered by MOOC providers were analysed. S. Hutt et al. [17] highlighted technological weaknesses and vulnerabilities, offering recommendations for their elimination. The study also assessed the effectiveness of access control systems and their ability to prevent unauthorised access to students' personal information, and analysed the privacy policies offered by MOOC providers. In turn, this study focuses on creating recommendations based on the analysis carried out in it. Both papers emphasise the importance of data security and privacy, but from different perspectives.

A. M. Al Hawamleh et al. [18] examined current challenges in the field of cybersecurity, and the role of ethical hacking in improving the protection of personal information. The results of the study revealed that ethical hacking helps to find potential threats and vulnerabilities before they become critical. It increases the level of awareness in the organisation about possible threats and the need to ensure security. Effective cybersecurity strategies, including ethical hacking, are becoming an integral part of the modern digital world, which ensures security and privacy in the Internet environment. The claim that ethical hacking is an integral part of the modern digital world is controversial. In a number of fields or organisations, this

method is not the only correct or appropriate one. Depending on the moral and ethical principles of different individuals or organisations, ethical hacking can be perceived in different ways. It is important to keep in mind that the effectiveness of ethical hacking strongly depends on the context in which it is applied. This method may not be unambiguously recommended in all cases. Both studies highlight the importance of data protection and cybersecurity, but they have different angles and accents, covering a wide range of topics in the field of information security.

The study by C. Arora [19] aimed to analyse the role and contribution of proxies in ensuring privacy in health information exchange in digital health. The researcher has revealed that trusted persons play a critical role in ensuring trust and confidentiality in the exchange of health data. Their functions, such as access control and data encryption, have had a significant impact on the security of digital healthcare. As a result of the analysis of technological aspects of data protection, it was revealed that the use of modern solutions, including blockchain and effective encryption mechanisms, contributed to the reliable protection of medical data from unauthorised access. In comparison with this study, S. Arora's [19] paper focuses on the analysis of a specific area of digital healthcare and the role of trusted persons in ensuring data security. It examines the broader aspects of data security related to the exchange of medical information in digital healthcare, including access control and encryption technologies. While the Front-end security architecture focuses on developing recommendations and strategies to protect user data at the interface level of web applications. Both studies are important in the context of data security and confidentiality, but they address different aspects and offer different approaches to solving the problem.

The purpose of the study by N. Saravanan and A. Umamakeswari [20] was to analyse the effectiveness of grid access control in the context of cloud environments with hybrid security and identify optimal strategies for protecting user data. The work confirmed that the use of grid access control in cloud infrastructures contributed to the effective organisation of access control, providing flexibility, and scalability. Advantages have been identified, such as simplifying user management, reducing the risks of unauthorised access, and increasing the level of traceability of user actions. The researcher identified areas for improving role based access control (RBAC) efficiency in cloud environments, including the integration of modern authentication technologies and more thorough scalability testing. Scalability testing is an important aspect, however, the effectiveness of lattice access control can be confirmed not only through scalability, but also through overall security and compliance with standards. The areas suggested by the researcher to improve RBAC in cloud environments can be effective, however, it must be borne in mind that the security sphere is constantly evolving, and the need for additional security aspects may also arise in the future. The researcher's recommendations on the integration of modern authentication technologies are well-founded, given the dynamism of cyber threats and the need for constant updating of security methods.

The results of the current study demonstrate that the Front-end security architecture and user data protection face a number of urgent challenges. An analysis of the risks associated with the storage and transfer of data on the client side has revealed the need to develop effective mechanisms to ensure confidentiality. The study also highlights the role of access control mechanisms such as authentication and authorisation in ensuring data privacy protection. Vulnerabilities and attacks focused on the Front-end require constant development of methods to prevent and identify new attack methods, especially in the context of problems such as cross-site scripting and cross-site request forgery. In light of the ever-increasing threats, the importance of this research is undeniable. It not only identifies problems but also offers practical solutions aimed at improving the security of web applications.

Governance as Code (GaC) technology provides a systematic way to ensure that front-end architectures adhere to predefined security standards automatically. This technology can streamline the enforcement of architectural standards, helping to protect

user data and enhance privacy in front-end applications. GaC technology allows for the automatic verification of front-end architectures against security models to prevent vulnerabilities and ensures consistency across systems by maintaining uniform security standards [21]. The implementation of GaC automates the enforcement of security rules before deployment, enabling early detection of potential security issues and ensuring compliance with regulations like General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or California Consumer Privacy Act (CCPA). By defining important security rules as code and applying these automatically using tools like Open Policy Agent, organizations can prevent deployment of applications that do not meet strict security criteria, thus enhancing the overall security posture. Integrating GaC not only facilitates a proactive security approach in front-end development but also helps in maintaining continual compliance and adjusting security measures in response to emerging threats. Given its potential to transform security protocols, Governance as Code technology, as outlined under patent WO2022250564, could significantly mitigate risks associated with user data and privacy violations, setting a new standard in secure software development practices.

5. CONCLUSIONS

Protection of user data and privacy play a key role in modern web applications. The findings emphasise that successful data protection begins with the development stage of Front-end web applications. Technical solutions, such as the use of encryption and measures against attacks, are insufficient without considering the details in the design of the interface. The study revealed various threats and vulnerabilities faced by the Front-end architecture in the field of data privacy protection. Learning encryption mechanisms, access control and adhering to security standards such as the OWASP Top Ten have proven to be key steps in providing strong security.

The study highlights that training and awareness-raising of Front-end developers in the field of security is an essential component of ensuring a reliable architecture. Access control mechanisms such as authentication and authorisation have played a critical role in protecting data privacy. Reliable user authentication and access control to various resources helped prevent unauthorised access and ensure data integrity. The practical tips and recommendations presented in the study form the basis for developers, providing them with a better understanding and readiness to respond to a variety of threats. Front-end developers, aware of the current threats, make more informed decisions in the process of creating interfaces. The training provides not only theoretical knowledge, but also practical skills necessary to build secure and sustainable web applications.

The practical advice obtained in the course of the study plays a key role in the development of reliable security strategies in the field of Front-end development. They are valuable recommendations that help to increase the level of protection of web applications and interfaces. An important element is the awareness of Front-end developers of current threats and effective methods of preventing them. Moreover, the integration of GaC technology, as detailed in the article, offers a systematic framework to ensure that all elements of the front-end architecture adhere to set security guidelines and configurations. This approach enhances the security strategies implemented, further safeguarding user data from emerging threats and vulnerabilities.

The study provides practical guidance for Front-end developers, highlighting the importance of security education and awareness. The practical tips and recommendations presented in the study create the basis for an effective response to threats, contributing to the creation of more reliable architectures. Subsequent research in this area may focus on the further development of educational programmes and tools to support the security of Front-end development.

References

1. Tsulukidze M., Nyman-Metcalf K., Tsap V., Pappel I., Draheim D. Aspects of personal data protection from state and citizen perspectives – Case of Georgia. In: I.O. Pappas, P. Mikalef, Y.K. Dwivedi, L. Jaccheri, J. Krogstie, M. Mäntymäki (Eds.), Proceedings of the 18th IFIP WG 6.11 Conference on e-Business "Digital Transformation for a Sustainable Society in the 21st Century".2019. pp. 476-488. Cham: Springer. https://doi.org/10.1007/978-3-030-29374-1_39
2. Napetvaridze V., Chochia A. Cybersecurity in the making – Policy and law: A case study of Georgia. *International and Comparative Law Review*, 2019, 19 (2), pp. 155–180. Available at: https://doi.org/10.2478/iclr-2019-0019. https://doi.org/10.2478/iclr-2019-0019
3. Sivasangari A., Kishor Sonti V. J. K., Poonguzhali S., Deepa D., Anandhi T. Security framework for enhancing security and privacy in healthcare data using blockchain technology. In: A. Khanna, D. Gupta, S. Bhattacharyya, A.E. Hassanien, S. Anand, A. Jaiswal (Eds.), *Proceedings of ICICC 2021 "International Conference on Innovative Computing and Communications"*, 2021, pp. 143–158. Singapore: Springer. https://doi.org/10.1007/978-981-16-2594-7_12
4. Feldman D., Haber E. Measuring and protecting privacy in the always-on era. *Berkeley Technology Law Journal*, 2020, 35 (1), pp. 197–250. Available at: https://btlj.org/data/articles2020/35_1/05_Haber_FinalFormat_WEB.pdf.
5. Amo D., Alier M., García-Peñalvo F. J., Fonseca D., Casañ M. J. Protected users: A moodle plugin to improve confidentiality and privacy support through user aliases. *Sustainability*, 2020, 12 (6), p. 2548. https://doi.org/10.3390/su12062548
6. Kaur J., Garg U., Bathla G. Detection of cross-site scripting (XSS) attacks using machine learning techniques: A review. *Artificial Intelligence Review*, 2023, 56 (11), pp. 12725–12769. https://doi.org/10.1007/s10462-023-10433-3
7. Likaj X., Khodayari S., Pellegrino G. Where we stand (or fall): An analysis of CSRF defenses in web frameworks. In: *RAID '21: Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses*, 2021, pp. 370–385). New York: Association for Computing Machinery. https://doi.org/10.1145/3471621.3471846
8. Dalimunthe S., Reza J., Marzuki A. Model for storing tokens in local storage (cookies) using JSON Web Token (JWT) with HMAC (Hash-based Message Authentication Code) in e-learning systems. *Journal of Applied Engineering and Technological Science*, 2022, 3 (2), pp. 149–155. https://doi.org/10.37385/jaets.v3i2.662
9. Cheah S., Selvarajah V. 2021. A Review of common web application breaching techniques (SQLi, XSS, CSRF). In: *Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*, pp. 540–547. Dordrecht: Atlantis Press. https://doi.org/10.2991/ahis.k.210913.068
10. Walton S., Wheeler P. R., Zhang Y. I., Zhao X. R. An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 2020, 35 (1), pp. 155–186. https://doi.org/10.2308/ISYS-19-033
11. Kaur J., Lamba S., Saini P. Advanced encryption standard: Attacks and current research trends. In: *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2021, pp. 112–116). Greater Noida: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICACITE51222.2021.9404716
12. Raman R. S., Evdokimov L., Wurstrow E., Halderman J. A., Ensafi R. Investigating large scale HTTPS interception in Kazakhstan. In: *IMC '20: Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 125–132). New York: Association for Computing Machinery. https://doi.org/10.1145/3419394.3423665
13. Li S., Xu C., Zhang Y., Du Y., Chen K. Blockchain-based transparent integrity auditing and encrypted deduplication for cloud storage. *IEEE Transactions on Services Computing*, 2022, 16 (1), pp. 134–146. https://doi.org/10.1109/TSC.2022.3144430
14. Omotunde H., Ahmed M. A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond. *Mesopotamian Journal of Cyber Security*, 2023, pp. 115–133. https://doi.org/10.58496/MJCSC/2023/016
15. Song L., García-Valls M. Improving security of web servers in critical IoT systems through self-monitoring of vulnerabilities. *Sensors*, 2022, 22 (13), 5004. https://doi.org/10.3390/s22135004
16. Hutt S., Baker R. S., Ashenafi M. M., Andres-Bray J. M., Brooks C. Controlled outputs, full data: A privacy-protecting infrastructure for MOOC data. *British Journal of Educational Technology*, 2022, 53 (4), pp. 756–775. https://doi.org/10.1111/bjet.13231
17. Al Hawamleh, A. M., Alorfi, Sulaiman M, A., Al-Gasawneh, J.A., Al-Rawashdeh, G. Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, 2020, 63, pp. 7894–7899. Available at: https://solidstatetechnology.us/index.php/JSST/article/view/7202.
18. Arora C. Digital health fiduciaries: Protecting user privacy when sharing health data. *Ethics and Information Technology*, 2019, 21 (3), pp. 181–196. Available at: https://doi.org/10.1007/s10676-019-09499-x. https://doi.org/10.1007/s10676-019-09499-x

19. Saravanan N., Umamakeswari A. Lattice based access control for protecting user data in cloud environments with hybrid security. *Computers & Security*, 2021, 100, 102074. https://doi.org/10.1016/j.cose.2020.102074
20. Method and system for verifying the architecture of a software/hardware solution. 2022. Available at: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2022250564.
21. Hiremath P. N., Armentrout J., Vu S., Nguyen T. N., Minh Q. T., Phung P. H. MyWebGuard: Toward a User-Oriented Tool for Security and Privacy Protection on the Web. In: T.K. Dang, J. Küng, M. Takizawa, S. Ha Bui (Eds.), *Proceedings of the 6th International Conference "Future Data and Security Engineering"*, 2019, pp. 506–525). Cham: Springer. https://doi.org/10.1007/978-3-030-35653-8_33

UDC 004.056.5:004.056.8:004.056.75

ЗОВНІШНЯ АРХІТЕКТУРА БЕЗПЕКИ: ЗАХИСТ ДАНИХ КОРИСТУВАЧА ТА КОНФІДЕНЦІЙНОСТІ

Олексій Чечет[1]; Максим Черних[2]; Ярослав Панасюк[3]; Ільнур Абдуллін[4]

[1]New Edge DWC-LLC, Дубай, Об'єднані Арабські Емірати
[2]Boom Pay, Inc, Остін, Сполучені Штати Америки
[3]Agoda Services Co., Ltd., Бангкок, Таїланд
[4]Національний центр інформаційних технологій, Бішкек, Киргизька Республіка

Резюме. *Дослідження цієї теми є актуальним у світлі значного збільшення частоти та масштабів кібератак, які зачіпають різні галузі та організації. Метою дослідження є аналіз існуючих методів захисту даних у Front-end, які здатні ефективно захистити конфіденційність даних користувачів перед обличчям сучасних кіберзагроз. Серед методів, які використовуються, слід відзначити аналітичний, метод синтезу, класифікації, статистичні та інші методи. Виявлено серйозні ризики, пов'язані зі зберіганням конфіденційних даних на стороні клієнта. Зокрема, вразливими місцями, які становлять потенційну загрозу безпеці даних, виявилося використання файлів cookie та локального сховища. Аналіз існуючих веб-додатків довів наявність уразливостей міжсайтового сценарію, які стали шляхом для впровадження шкідливих скриптів. Виявлено, що створення та використання унікальних маркерів підробки міжсайтових запитів для кожного запиту відіграє ключову роль у запобіганні підробці міжсайтових запитів. Упровадження технології «Управління як код» продемонструвало потенціал для автоматизації дотримання встановлених архітектурних стандартів і стандартів безпеки, тим самим посилюючи зовнішній захист від кіберзагроз. Висновки підкреслюють важливість навчання кінцевих користувачів основним принципам безпеки мережі. Наголошено на важливості активної участі розробників у захисті Front-end. Таким чином, надано вичерпний огляд архітектури безпеки Front-end з акцентом на захист даних користувачів і забезпечення конфіденційності. Практичне значення дослідження полягає в наданні конкретних рекомендацій і практичних рішень для покращення Front-end безпеки у веб-додатках і являє собою цінний набір інструментів і підходів, які можуть застосовувати розробники та інженери для посилення безпеки веб-додатків. Додавання технології «Управління як код» являє собою інноваційний рівень автоматизованого забезпечення безпеки, який особливо підходить для вирішення нових проблем кібербезпеки в режимі реального часу.*

Ключові слова: *шифрування даних, вразливості, міжсайтовий скриптинг, розроблення технології, впровадження, архітектура, управління як код.*

https://doi.org/10.33108/visnyk_tntu2024.03.005 *Отримано 18.04.2024*