Investigating vulnerabilities of personal data on financial websites

Olena H. Fedorenko[1], Sofiia V. Velychko[1,2] and Yelyzaveta V. Kaidan[3]

[1]*Donbas State Pedagogical University, 19 Batyuk Str., Sloviansk, 84116, Ukraine*
[2]*National University "Odesa Law Academy", 23 Fontanska Str., Odesa, 65009, Ukraine*
[3]*Ivan Franko National University of Lviv, 1 Universytetska Str., Lviv, 79000, Ukraine*

Abstract

This paper investigates the vulnerabilities of personal data on financial websites. It analyzes potential threats and attack methods and proposes comprehensive protection strategies from both user and organizational perspectives. The security of specific financial sites is evaluated, and recommendations are provided.

Keywords

personal data, financial websites, data breaches, cybersecurity, attack methods

1. Introduction

In today's digital age, personal data security has become a paramount concern, especially in the context of financial websites. As more individuals rely on online platforms for managing their finances, the risks associated with data breaches and unauthorized access have grown exponentially [1]. The consequences of compromised financial data can be severe, ranging from identity theft and fraudulent transactions to long-term damage to credit scores and reputation [2].

The vulnerability of personal data on financial websites is a multifaceted issue involving a complex interplay of technological, human, and organizational factors. Attackers employ an ever-evolving array of techniques to exploit weaknesses in web application security, such as SQL injection, cross-site scripting (XSS), and phishing [3]. These threats are compounded by the increasing sophistication of cybercriminals and the proliferation of hacking tools on the dark web [4].

Recent high-profile data breaches, such as the Kyivstar incident in December 2023, have highlighted the devastating impact of successful attacks on financial platforms. In this case, hackers managed to infiltrate the mobile operator's infrastructure, disrupting services for millions of users and compromising sensitive customer data [5]. The breach not only caused immediate financial losses but also eroded public trust in the security of online transactions [6].

Effective protection of personal data on financial websites requires a multi-pronged approach, involving both proactive measures by organizations and informed vigilance by individual users [7]. Financial institutions must implement robust security controls, such as encryption, access management, and regular auditing, to safeguard customer data from unauthorized access [8]. At the same time, users need to adopt best practices for online security, including strong password hygiene, enabling two-factor authentication, and being cautious when sharing personal information [9].

This paper aims to provide a comprehensive analysis of the vulnerabilities threatening personal data on financial websites and propose strategies for enhancing security in this critical domain. The primary objectives of this research are:

1. To identify and categorize the most common vulnerabilities and attack methods targeting financial websites based on industry reports and academic literature.

CS&SE@SW 2024: 7th Workshop for Young Scientists in Computer Science & Software Engineering, December 27, 2024, Kryvyi Rih, Ukraine

fedorenko.elena1209@gmail.com (O. H. Fedorenko); sofiavelichko33@gmail.com (S. V. Velychko); kaidan.yelv@gmail.com (Y. V. Kaidan)
0000-0002-1897-874X (O. H. Fedorenko); 0000-0002-2728-6796 (S. V. Velychko); 0000-0002-2350-2228 (Y. V. Kaidan)

2. To conduct a security assessment of two prominent financial websites – OLX.ua and Privat24.

The remainder of this paper is structured as follows: section 2 presents an in-depth analysis of common vulnerabilities and attack methods targeting financial websites; section 3 explores user-oriented and organization-oriented strategies for enhancing personal data protection; section 4 offers a detailed security assessment of OLX.ua and Privat24; and finally, section 5 concludes with a summary of key findings and recommendations for future research.

2. Analysis of attack methods and vulnerabilities

Financial websites are prime targets for cybercriminals due to the sensitive nature of the data they handle and the potential for direct financial gain. Attackers employ a wide range of methods to exploit vulnerabilities in web applications, servers, and user behaviours [3].

Typical attack methods:

1. SQL Injection (SQLi) is a technique where malicious SQL statements are inserted into application queries. This allows attackers to manipulate the database, bypass authentication, or extract sensitive information [8]. SQLi vulnerabilities often arise from improper validation or sanitization of user inputs in web forms or URL parameters [10].
2. Cross-Site Scripting (XSS) involves injecting malicious scripts into web pages viewed by other users. When executed, these scripts can steal session cookies, perform unauthorized actions, or redirect users to phishing sites [9]. XSS vulnerabilities typically result from inadequate encoding or filtering of user-generated content [11].
3. Cross-Site Request Forgery (CSRF) tricks authenticated users into performing unintended actions on a web application by exploiting their active session. By crafting malicious links or forms, attackers can make unauthorized transactions or changes to user accounts [8]. CSRF vulnerabilities arise when web applications fail to include proper authentication tokens in sensitive requests [10].
4. Phishing and social engineering use fraudulent emails, websites, or messages to deceive users into revealing their login credentials, personal information, or financial details [5]. Social engineering techniques exploit human psychology to manipulate victims into taking actions that compromise their security [2].
5. Malicious software (malware), such as viruses, trojans, or spyware, can infect user devices to steal sensitive data, monitor keystrokes, or perform unauthorized transactions [3]. Ransomware attacks encrypt user files and demand payment for their release, causing significant financial losses and operational disruptions [12].

Common vulnerabilities:

1. Weak authentication and session management occur when financial websites implement weak password policies, lack multi-factor authentication, or handle sessions improperly. These vulnerabilities expose users to brute-force attacks, credential stuffing, and session hijacking [10]. Attackers can exploit these weaknesses to gain unauthorized access to user accounts and perform fraudulent activities [9].
2. Insecure data storage and transmission arise when sensitive financial data is stored without proper encryption or transmitted over unencrypted channels. This makes the data vulnerable to interception and theft [8]. Failure to secure data at rest and in transit is a significant weakness in many web applications [12].
3. Misconfigured or unpatched systems affect financial platforms running on servers with improper configurations, outdated software, or unpatched vulnerabilities. These systems are susceptible to known exploits and zero-day vulnerabilities [1]. Attackers can leverage these issues to gain unauthorized access, escalate privileges, or compromise the entire system [7].

4. Insufficient input validation and output encoding results when web applications fail to validate user inputs or encode output data adequately. These vulnerabilities make the applications prone to injection attacks, such as SQL injection and cross-site scripting [11]. Lack of input sanitization enables attackers to manipulate application behaviour and extract sensitive information [10].
5. Broken access control and privilege escalation occur when weak access control mechanisms and improper privilege management are in place. Attackers can bypass authentication, access unauthorized resources, or elevate their privileges within the application [3]. Insecure direct object references and broken role-based access control are frequent examples of this vulnerability [9].

Figure 1 presents the OWASP Top 10 Web Application Security Risks, which encompass many of the aforementioned vulnerabilities and provide a standardized framework for assessing and prioritizing security weaknesses.

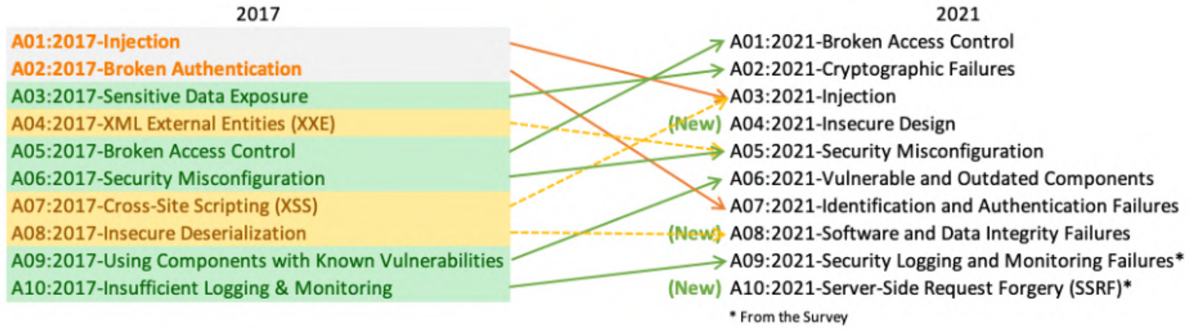

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

Figure 1: OWASP Top 10 Web Application Security Risks (https://owasp.org/www-project-top-ten/).

The complex and interconnected nature of financial systems amplifies the impact of these vulnerabilities. A single compromised account or system can serve as an entry point for attackers to laterally move through the network, escalate privileges, and access a wide range of sensitive data [13]. The consequences can be devastating, including financial losses, reputational damage, legal liabilities, and erosion of customer trust [2].

To effectively mitigate these risks, financial organizations must adopt a proactive and multi-layered approach to security. This involves implementing robust technical controls, such as encryption, secure coding practices, and regular security testing, as well as fostering a culture of security awareness among employees and users [1]. The following section explores specific strategies and best practices for enhancing personal data protection on financial websites from both user and organizational perspectives.

3. Personal data protection methods

3.1. User-oriented strategies

Awareness and education are critical for empowering users to safeguard their financial data online. By understanding common threats such as phishing scams, social engineering tactics, and malicious websites, individuals can make informed decisions to avoid falling victim to attacks [1]. Financial institutions play a crucial role in this process by providing accessible educational resources, tutorials, and regular updates to inform users about emerging risks and best practices for online security [7].

Strong authentication and password management are fundamental to protecting financial accounts. Users should create strong, unique passwords for each account, avoiding easily guessable information like names or birthdays. Instead, passwords should include a mix of uppercase and lowercase letters, numbers, and special characters [8]. Regularly updating passwords and using password managers can further enhance security [9].

Enabling two-factor authentication (2FA) provides an additional layer of security for financial accounts. This method requires users to provide a second form of verification, such as a one-time code sent to their mobile device or generated by an authenticator app, alongside their password [12]. Activating 2FA significantly reduces the risk of unauthorized access, even if passwords are compromised [11]. Financial institutions should encourage users to enable 2FA and offer guidance on the setup process [1]. Secure device and network configuration is essential for protecting personal information. Users should ensure their devices, including smartphones, tablets, and computers, are protected by up-to-date security software like antivirus programs and firewalls [9]. Regularly applying software updates and patches is necessary to address known vulnerabilities [8]. When accessing financial websites, users should avoid public Wi-Fi networks or unsecured connections, which can be intercepted by attackers [7]. Instead, utilizing a virtual private network (VPN) or mobile data provides a safer alternative [3].

Monitoring and promptly reporting suspicious activities is another key strategy for users. Regularly reviewing financial accounts and statements helps identify unauthorized transactions or changes to personal information [1]. Activating account alerts and notifications can aid in the early detection of potential security breaches [2]. If users suspect fraudulent activities or account compromise, they should immediately report it to their financial institution and follow instructions to secure the account and minimize losses [5].

3.2. Organization-oriented approaches

Compliance with data protection regulations is essential for financial organizations to safeguard personal data and avoid legal consequences. Regulations such as the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL) impose strict requirements for the collection, processing, storage, and transfer of personal data [1]. These regulations mandate obtaining user consent, implementing appropriate security measures, and reporting data breaches within specified timeframes [7]. Failure to comply can result in significant financial penalties and reputational damage [6].

Secure development and testing practices are critical in mitigating vulnerabilities in financial web applications. By implementing secure coding guidelines, conducting regular code reviews, and employing static and dynamic security analysis, organizations can identify and address potential risks during the software development lifecycle [3]. Security testing techniques, such as penetration testing, vulnerability scanning, and fuzz testing, further help uncover weaknesses in security controls, allowing organizations to remediate them before deployment [9].

To protect sensitive data, strong encryption mechanisms should be implemented both in transit and at rest [12]. Using secure protocols like Transport Layer Security (TLS) ensures the safety of data transmitted over networks by preventing interception and unauthorized access [1]. Additionally, sensitive data should be stored in encrypted form using industry-standard algorithms and robust key management practices. This approach minimizes the risk of data breaches and protects information from unauthorized disclosure [8].

Access control and privilege management are fundamental to limiting unauthorized access to sensitive resources. Financial organizations should establish clear roles and permissions for various user groups, such as customers, employees, and administrators while restricting access based on job functions and business needs [3]. Regularly reviewing and updating access privileges, coupled with monitoring user activities through logging and auditing mechanisms, enhances the organization's ability to detect and respond to potential security breaches [1].

Continuous security monitoring and an effective incident response plan are essential for maintaining the security of financial systems and networks [8]. Solutions such as security information and event management (SIEM), intrusion detection and prevention systems (IDPS), and other monitoring tools play a vital role in identifying anomalous activities like unauthorized access attempts or data exfiltration [3]. Establishing a well-defined incident response plan enables organizations to contain, investigate, and recover from security breaches. Regular testing and updating of this plan ensure its effectiveness in mitigating potential damages [7].

Employee training and awareness are also critical components of an organization's security strategy. Employees are often the weakest link in maintaining security [2], so it is essential to provide regular training and education on their responsibilities in safeguarding sensitive data [13]. Training programs should address secure password practices, recognizing and reporting phishing attempts, handling sensitive data appropriately, and adhering to security policies [1]. Conducting periodic assessments and simulated phishing exercises can help organizations evaluate the effectiveness of their training programs and identify areas for improvement [9].

Implementing a combination of user-oriented and organization-oriented strategies creates a multi-layered defence against threats to personal data on financial websites. By empowering users to make informed security decisions and establishing robust technical and organizational controls, financial institutions can significantly reduce the risk of data breaches and protect the confidentiality, integrity, and availability of sensitive information.

4. Financial website security analysis

4.1. OLX.ua marketplace

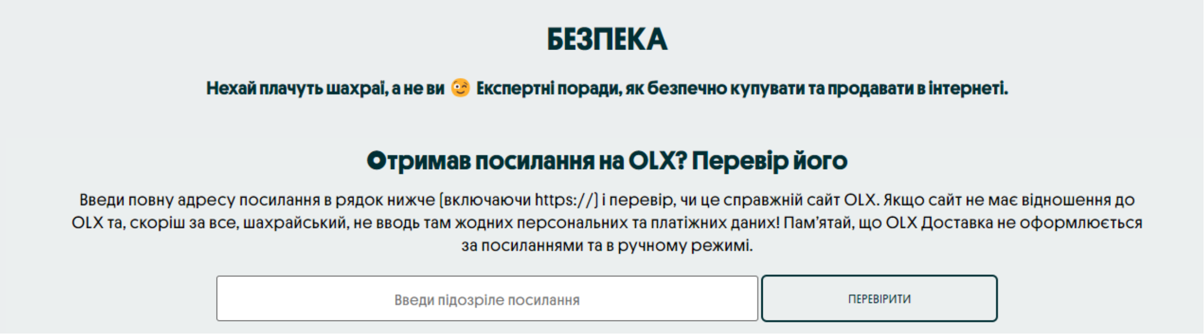
OLX.ua is a leading online marketplace in Ukraine, facilitating the buying and selling of various goods and services. As a platform that handles sensitive user information, including personal details and financial transactions, OLX.ua has implemented several security measures to protect user data.

OLX.ua provides a detailed privacy policy outlining the types of personal data collected, the purposes for which it is used, and the measures taken to protect user privacy [1]. The platform collects user information, such as names, email addresses, and phone numbers, to facilitate transactions and communicate with users. OLX.ua also specifies that it may share user data with affiliated companies and trusted partners for service provision and marketing purposes [7].

OLX.ua uses the HTTPS protocol to encrypt data transmitted between users' browsers and the platform's servers [12]. This ensures that sensitive information, such as login credentials and financial details, is protected from interception by unauthorized parties. The presence of a valid SSL/TLS certificate, indicated by a padlock icon in the browser's address bar, confirms the secure connection [8].

OLX.ua implements user authentication mechanisms to verify the identity of users accessing the platform. Users are required to create an account with a unique username and password, which are used to log in to the system [3]. The platform also provides the option for users to enable two-factor authentication (2FA) for added security, requiring a second form of verification, such as an SMS code, in addition to the password [9].

OLX.ua employs monitoring and fraud detection systems to identify and prevent suspicious activities on the platform [1]. This includes monitoring user behaviour patterns, detecting abnormal transactions, and flagging potential fraud attempts. The platform also provides a reporting mechanism for users to notify OLX.ua of any suspicious or fraudulent activities they encounter [7]. Figure 2 illustrates the process of detecting and preventing fraudulent activities on the OLX.ua online marketplace.



БЕЗПЕКА

Нехай плачуть шахраї, а не ви 😉 Експертні поради, як безпечно купувати та продавати в інтернеті.

Отримав посилання на OLX? Перевір його

Введи повну адресу посилання в рядок нижче [включаючи https://] і перевір, чи це справжній сайт OLX. Якщо сайт не має відношення до OLX та, скоріш за все, шахрайський, не вводь там жодних персональних та платіжних даних! Пам'ятай, що OLX Доставка не оформлюється за посиланнями та в ручному режимі.

Figure 2: Fraud detection and prevention process on the OLX.ua online marketplace.

OLX.ua provides educational resources and tips to help users protect their personal information and avoid falling victim to scams or fraudulent activities [1]. The platform's blog and support centre offers guidance on creating strong passwords, identifying phishing attempts, and conducting safe transactions. OLX.ua also encourages users to be cautious when sharing personal information and to report any suspicious activities to the platform's support team [7].

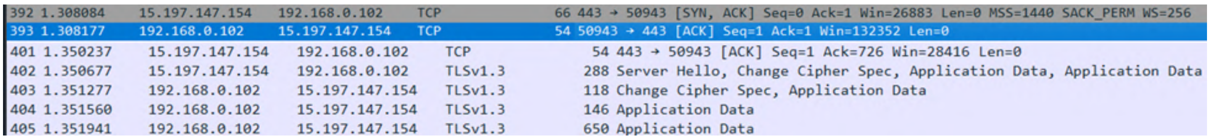
While OLX.ua has implemented various security measures to protect user data, there are still potential areas for improvement. For example, the platform could consider implementing more granular access controls based on user roles and permissions, regularly conducting security audits and penetration testing to identify vulnerabilities, and providing more prominent and accessible security settings for users to manage their account security preferences [3].

4.2. Privat24 online banking

Privat24 is a popular online banking platform in Ukraine, offering a wide range of financial services, including account management, money transfers, and bill payments. As a platform handling highly sensitive financial information, Privat24 has implemented robust security measures to protect user data and prevent unauthorized access.

Privat24 employs a multi-factor authentication process to verify the identity of users accessing their accounts [8]. In addition to a username and password, users are required to provide a second form of authentication, such as an SMS code or a hardware token, to log in to the platform [12]. This helps prevent unauthorized access to user accounts, even if the password is compromised [11].

Privat24 uses strong encryption algorithms to protect sensitive data transmitted between users' devices and the platform's servers [9]. The platform employs the TLS1.3 protocol, which provides robust encryption and secure communication channels [12]. Packet sniffing analysis conducted on Privat24's network traffic confirmed that sensitive data, such as login credentials and financial information, is not transmitted in plaintext and is protected by encryption (figure 3).



```
392 1.308084    15.197.147.154  192.168.0.102   TCP        66 443 → 50943 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM WS=256
393 1.308177    192.168.0.102   15.197.147.154  TCP        54 50943 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
401 1.350237    15.197.147.154  192.168.0.102   TCP        54 443 → 50943 [ACK] Seq=1 Ack=726 Win=28416 Len=0
402 1.350677    15.197.147.154  192.168.0.102   TLSv1.3    288 Server Hello, Change Cipher Spec, Application Data, Application Data
403 1.351277    192.168.0.102   15.197.147.154  TLSv1.3    118 Change Cipher Spec, Application Data
404 1.351560    192.168.0.102   15.197.147.154  TLSv1.3    146 Application Data
405 1.351941    192.168.0.102   15.197.147.154  TLSv1.3    650 Application Data
```

Figure 3: Packet sniffing in wireshark.

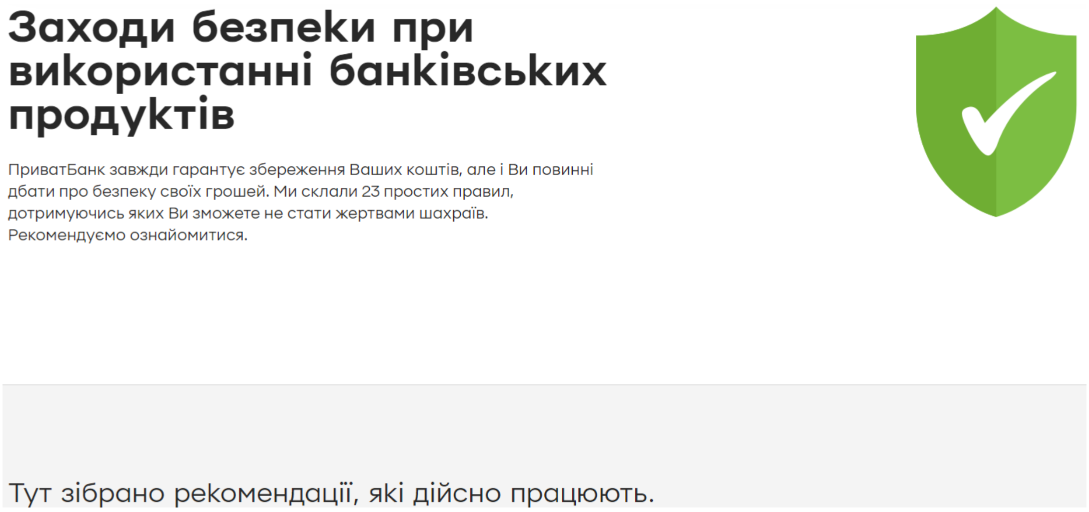
Privat24 has implemented advanced fraud detection and monitoring systems to identify and prevent fraudulent activities on the platform [1]. This includes real-time monitoring of transactions, behavioural analysis of user activities, and machine learning algorithms to detect anomalous patterns [7]. Privat24 also provides users with the ability to set up transaction alerts and notifications, allowing them to quickly detect and report any suspicious activities on their accounts [2].

Privat24 places a strong emphasis on user education and awareness regarding online banking security [1]. The platform provides a dedicated security centre on its website, offering information and guidance on safe banking practices, identifying phishing attempts, and protecting personal information. Privat24 also regularly communicates with users through email and in-app notifications, providing updates on emerging security threats and reminding users to maintain good security habits [5].

Privat24 ensures compliance with relevant data protection regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR) [1]. The platform follows strict data handling and storage practices, implementing access controls, data encryption, and regular security audits to maintain the confidentiality and integrity of user data [7].

Figure 4 presents a screenshot of Privat24's online banking interface, highlighting the platform's security features and user authentication process.

While Privat24 demonstrates a strong commitment to user data protection and implements various security measures, there is always room for improvement. The platform could consider implementing



Заходи безпеки при використанні банківських продуктів

ПриватБанк завжди гарантує збереження Ваших коштів, але і Ви повинні дбати про безпеку своїх грошей. Ми склали 23 простих правил, дотримуючись яких Ви зможете не стати жертвами шахраїв. Рекомендуємо ознайомитися.

Тут зібрано рекомендації, які дійсно працюють.

Figure 4: Privat24 online banking security features.

biometric authentication methods, such as fingerprint or facial recognition, to enhance user authentication [8]. Regular penetration testing and vulnerability assessments can help identify and address any potential weaknesses in the platform's security controls [3]. Additionally, Privat24 could expand its user education efforts to include more interactive and engaging content, such as videos and quizzes, to reinforce security best practices among its users [9].

5. Conclusions

Protecting personal data on financial websites is a critical concern in today's digital landscape. As the reliance on online platforms for financial transactions and services continues to grow, so do the risks associated with data breaches, unauthorized access, and fraudulent activities. This paper has provided an analysis of the vulnerabilities threatening personal data on financial websites, the attack methods exploited by malicious actors, and the strategies that users and organizations can employ to enhance data protection.

The analysis of common vulnerabilities and attack methods highlighted the importance of addressing weaknesses in web application security, such as injection flaws, cross-site scripting, and broken authentication. It also emphasized the need for users to be vigilant against social engineering tactics, such as phishing and malware, which can compromise their personal information.

To mitigate these risks, the paper proposed a multi-layered approach to personal data protection involving both user-oriented and organization-oriented strategies. Users play a critical role in safeguarding their own data by adopting strong authentication practices, maintaining device security, and staying informed about emerging threats. Organizations, on the other hand, must implement robust technical controls, such as encryption, access management, and regular security testing, while fostering a culture of security awareness among employees.

The security assessments of OLX.ua and Privat24 provided practical insights into implementing personal data protection measures on popular financial platforms. While both platforms demonstrated various security controls and user education efforts, there were still potential areas for improvement, such as more granular access controls, biometric authentication, and interactive security training.

Future research in this domain could focus on developing more advanced and automated tools for detecting vulnerabilities in financial web applications, exploring the unique security challenges posed by emerging technologies, such as blockchain and artificial intelligence, and evaluating the effectiveness of specific data protection regulations in mitigating risks.

Declaration on Generative AI: During the preparation of this work, the authors used Claude 3 Opus to draft content, translate text, draft abstracts, and provide formatting assistance. After using this service, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. Rohendi, D. B. Kharisma, Personal data protection in fintech: A case study from Indonesia, Journal of Infrastructure, Policy and Development 8 (2024). doi:10.24294/jipd.v8i7.4158.

[2] L. Bean, Are you protecting your employee's data?, Journal of Corporate Accounting and Finance 23 (2012) 13–19. doi:10.1002/jcaf.21778.

[3] C. C. Echefunna, J. Osamor, C. Iwendi, P. Owoh, M. Ashawa, A. Philip, Evaluation of Information Security in Web Application Through Penetration Testing Techniques Using OWASP Risk Methodology, in: 2024 International Conference on Advances in Computing Research on Science Engineering and Technology, ACROSET 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi:10.1109/ACROSET62108.2024.10743903.

[4] Y. Mundada, A. Ramachandran, N. Feamster, SilverLine: preventing data leaks from compromised web applications, in: Proceedings of the 29th Annual Computer Security Applications Conference, ACSAC '13, Association for Computing Machinery, New York, NY, USA, 2013, p. 329–338. doi:10.1145/2523649.2523663.

[5] D. Elmaleh, Phishing fordidden, Card Technology Today 19 (2007) 12–13. doi:10.1016/S0965-2590(07)70137-8.

[6] A. S. Choudhury, J. Kwon, A study of the effect of regulations on different types of information security breaches across different business sectors, in: Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings, Pacific Asia Conference on Information Systems, 2016.

[7] E. Velinov, I. Leroy, H. Cetlova, Marketing Process in Information Security Context: Comparison Between Czech Republic and Belgium, in: S. I. Ashmarina, V. V. Mantulenko (Eds.), Proceedings of the International Conference Engineering Innovations and Sustainable Development, volume 210 of *Lecture Notes in Civil Engineering*, Springer International Publishing, Cham, 2022, pp. 567–577. doi:10.1007/978-3-030-90843-0_64.

[8] A. E. Hafez, M. M. Almustafa, Detecting Security Vulnerabilities in Web Applications: A Proposed System, International Journal of Safety and Security Engineering 14 (2024) 1933–1940. doi:10.18280/ijsse.140627.

[9] G. Yasmeen, S. A. Afaq, The Critical Analysis of E-Commerce Web Application Vulnerabilities, in: M. S. Husain, M. Faisal, H. Sadia, T. Ahmad, S. Shukla (Eds.), Advances in Cyberology and the Advent of the Next-Gen Information Revolution, IGI Global, 2023, pp. 22–37. doi:10.4018/978-1-6684-8133-2.ch002.

[10] E. Karafili, D. Sgandurra, E. Lupu, A Logic-Based Reasoner for Discovering Authentication Vulnerabilities Between Interconnected Accounts, in: A. Saracino, P. Mori (Eds.), Emerging Technologies for Authorization and Authentication, volume 11263 of *Lecture Notes in Computer Science*, Springer International Publishing, Cham, 2018, pp. 73–87. doi:10.1007/978-3-030-04372-8_7.

[11] B. Kiruba, V. Saravanan, T. Vasanth, B. Yogeshwar, OWASP Attack Prevention, in: 3rd International Conference on Electronics and Sustainable Communication Systems, ICESC 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1671–1675. doi:10.1109/ICESC54411.2022.9885691.

[12] L. Amasala, M. Ponnuru, P. Srideviponmalar, Secure Goods Storage and Anti-Theft Approach using Ethereum Blockchain, Procedia Computer Science 233 (2024) 1–11. doi:10.1016/j.procs.2024.03.190.

[13] A. Mahalle, J. Yong, X. Tao, Ethics of IT security team for cloud architecture infrastructure in banking and financial services industry, in: W. Shen, H. Paredes, J. Luo, J. P. Barthes (Eds.), Proceedings of the 2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design, CSCWD 2019, Institute of Electrical and Electronics Engineers Inc., 2019, pp. 506–511. doi:10.1109/CSCWD.2019.8791928.