E-commerce Security Enhancement

Saikat Hossain
Department of CSE
United International University (UIU)
Dhaka, Bangladesh
shossain201214@bscse.uiu.ac.bd

Lailafin Nahar Tithy
Department of CSE
United International University (UIU)
Dhaka, Bangladesh
ltithy201332@bscse.uiu.ac.bd

Muntasir Jahid Ayan
Department of CSE
United International University (UIU)
Dhaka, Bangladesh
mayan201439@bscse.uiu.ac.bd

Mir Moynuddin Ahmed Shibly
Department of CSE
United International University (UIU)
Dhaka, Bangladesh
moynuddin@cse.uiu.ac.bd

***Abstract*—In the realm of e-commerce website security, protecting sensitive user data and against malicious threats are paramount. This study presents a comprehensive approach to strengthen an e-commerce platform through a multi-layered security framework by accommodating infiltration, propagation, aggregation, and exfiltration measures. Infiltration defenses include robust mechanisms such as email alerts, failed login restrictions, input validation, two-factor authentication, CSRF protection, and rejection of SQL injection attempts. These tactics ensure that user access is authenticated, validated, and protected against common attack vectors like brute-force attacks and cross-site request forgery. Propagation protects including password hashing, implementation of security headers, systematic event logging, and session management. By employing these strategies, the system strengthens its resilience against unauthorized access, data breaches, and session hijacking. Aggregation strategies involve role-based authorization, database activity logging, data loss prevention mechanisms, and access control policies. These measures enable granular control over user permissions, audit trails for system activities, and preemptive measures to mitigate data loss or unauthorized access incidents. Exfiltration defenses focus on network firewall implementation, scheduled data backups, and rejection of access attempts from known malicious IPs and domains. These precautions bolster the system's ability to detect and prevent unauthorized access, maintain data integrity, and safeguard against external threats. Overall, the proposed security framework provides a comprehensive and robust defense mechanism against a wide range of security threats in the e-commerce domain, ensuring the confidentiality, integrity, and availability of sensitive user data and resources.**

I. Introduction

The information security framework includes e-commerce security, which is especially applied to the elements that impact e-commerce, such as computer security, data security and additional broader domains within the context of information security. With its unique intricacies, e-commerce security is one of the most conspicuous security elements that impact the end user through their regular financial interactions with businesses.

Electronic technology security and privacy are big concerns these days. M-commerce offers security. Issues pertaining to other technology within the field. Users have been directly impacted by privacy concerns that have been found to reveal a lack of confidence in a number of situations, including social networking, e-recruitment technologies, electronic health records, and commerce. One of the main and ongoing issues preventing people and businesses from using e-commerce is security. A lot of the time, stakeholders and the development team overlook security. They believed that security is not a crucial factor. They focused more on needs related to user interface, dependability, and usability. Because of this, a number of security incidents, including fraud, phishing, hacking, and cybercrime, have happened in the information system. A WannaCry Worn Ransomware Attack occurred in 2017, On 20.0000 users [1]. 28,430,843 times, Indonesia has been attacked, increasing by 135,672,984 times [2].

Web e-commerce apps that accept payments (online banking, electronic transactions, debit cards, credit cards, PayPal, or other tokens) face additional compliance challenges. Targeted websites pose a higher risk of data loss or manipulation, with more serious repercussions. Online purchasing involves following specific steps to ensure a safe and secure purchase.The e-commerce business is tackling security concerns on internal networks. Guidelines for system and network security are accessible for e-commerce personnel to understand and execute. Educating consumers on security issues is crucial for e-commerce security, even being in its early stages. Trojan horse programs targeting client systems are the most significant hazard to e-commerce as they can bypass or subvert most security measures. Authentication and authorization mechanisms for e-commerce transactions. To install these programs on a remote computer, simply send email attachments. Consumers are increasingly concerned about privacy due to identity theft and impersonation. E-commerce companies must also prioritize this concern.

II. Related Works

Security issues remain a major barrier for e-commerce users and enterprises. This article examines the perception of security in e-commerce B2C and C2C websites. From both a customer and an organizational standpoint. [3]

E-commerce website owners focus on attracting clients and

ensuring visitor security, while also considering ways to improve the site's functionality. End consumers should rate e-commerce websites and take precautions to stay safe in the online community. This research analysis publication aims to provide readers with a clear understanding of the technology that enables secure transactions and safety tips. E-commerce site owners can increase visitor trust by implementing trust marks and security strategies. [4]

Xiao et al. [5] investigated e-commerce product recommendation agents and reviewed empirical articles on e-commerce product offering agents published from 2007 to 2012. They chose 34 papers to review, covering themes such as recommendation agent type, preference elicitation, explanation, and the social elements of recommendation agents. They also discussed the operational features of social recommendation agents, user perception variables such as pleasure, understood recommendation quality, understood trade-off issue, and understood social presence, as well as modifying factors such as gender, regulatory focus, reactance level, temporal distance, and decision context. They proposed an updated conceptual model of the recommendation agent for further research. However, the study focused primarily on some aspects, such as social presence, perceived utility, trust, contentment, and perceived ease of use, as user evaluation variables for recommendation bots. Using the conceptual model is an important feature in their research.Many research have been conducted on the security elements of e-commerce technology infrastructure, including communication security, secure payment systems, and fraud protection [6]–[8].

Liu et al. [9] discovered that trust and social factors influence customers while engaging in mobile commerce transactions. Traditional authentication methods rely on identification for security and access control. They also include encryption and authentication. Algorithms require powerful computer technology. P2P e-commerce should prioritize improving authentication mechanisms and optimizing traditional encryption and authentication algorithms [10]. While e-commerce presents opportunities for the banking industry, it also introduces new risks and vulnerabilities, including security concerns. Information security is crucial for efficient and effective online payment transactions. Determining its definition is challenging because to ongoing technological and business changes, necessitating a coordinated approach of algorithmic and technical solutions. [11].

The success of an e-commerce operation depends on various aspects, such as the company model, team, and customers. Investors, product, and data security (transmission and storage). Recent high-profile "cracker" attacks have highlighted the importance of data security, including the impersonation of Microsoft employees for digital certification and the misuse of customer credit card numbers on e-commerce sites [12]. E-commerce transactions between customers and sellers involve information queries, price quotations, order placement, payment, and after-sales support. Services. Maintaining trust in the legitimacy, confidentiality, and prompt delivery of online transactions can be challenging [13]. Privacy and security might be regarded as ethical issues. The commercial sector prioritizes privacy and security concerns. It can impact the success or failure of businesses, particularly e-commerce [14]. The current protocols and methods generally bring extra communication and computation costs to all parties involving in the e-commerce system [15]. E-commerce system security and web sites security is the most overlooked aspect of securing data [16]. Data security technology plays a crucial role in the development of e-commerce systems [17]. A transaction processing system for e-commerce by using a blockchain technology, zero-knowledge proof and modified elliptic curve cryptography encryption is proposed [18]. The safety problem has become the focus of the application domain about e-commerce [19]. The development of efficient and safe electronic commerce management system is very necessary [20].

III. System Architecture

The architecture is the 3 layered security architecture. Where in the first layer, authentication firewall will work and some infiltration security feature will act. Any malicious activity will be prohibited the login for the user. Then the second layer has two application which are acted as propagation and aggregation. Lastly, the last layer act as exfiltration and data backup is the main task of this layer. In Fig.1 We have shown how our security system works.

IV. Methodology

For Security measures, we have maintained Breach Quadrilateral. And, try to touch every quadrilateral with at least one feature.

A. Infiltration

In Fig.3 All steps of Infiltration have shown: Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract.

1) E-mail Alert: Implemented to notify users via email upon successful login attempts, enhancing account security awareness. Utilized Django's send mail function along with SMTP configuration to send email notifications to users' registered email addresses upon login.

2) Failed Login: Set a limit on consecutive failed login attempts to mitigate brute-force attacks and unauthorized access attempts.Integrated Django's ratelimit decorator to restrict the number of login attempts from a single IP address within a specified time frame, temporarily blocking further attempts after reaching the limit.

3) Input Validation: Enforced validation of user input on registration forms to ensure the accuracy and integrity of user-provided data. Leveraged Django's built-in form validation features to validate user input, enforcing proper formatting and constraints on registration forms.

4) Two Factor Authentication: Integrated Google Authenticator for OTP generation to add an additional layer of security to the admin panel. Integrated Google Authenticator for OTP generation, utilizing the django otp package and configuring the admin site to enforce 2FA for admin users.

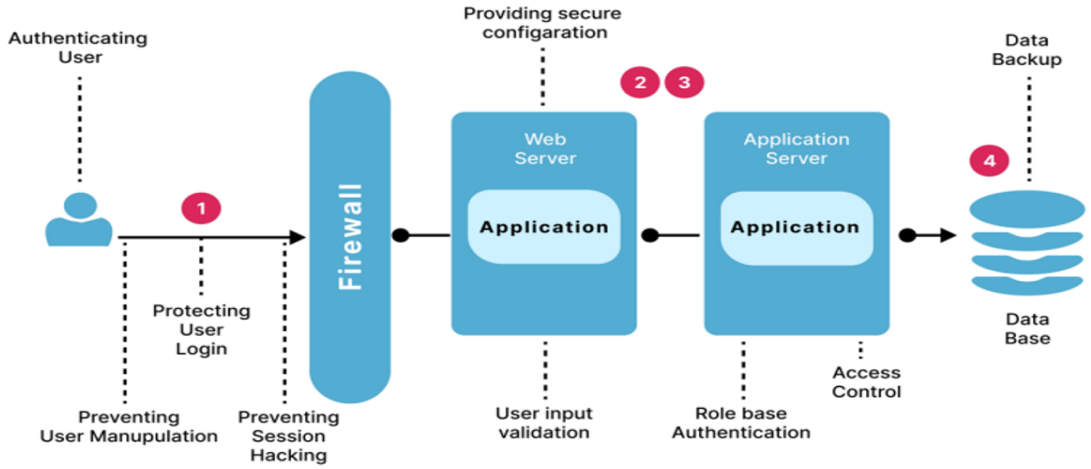

Fig. 1. Four security breach

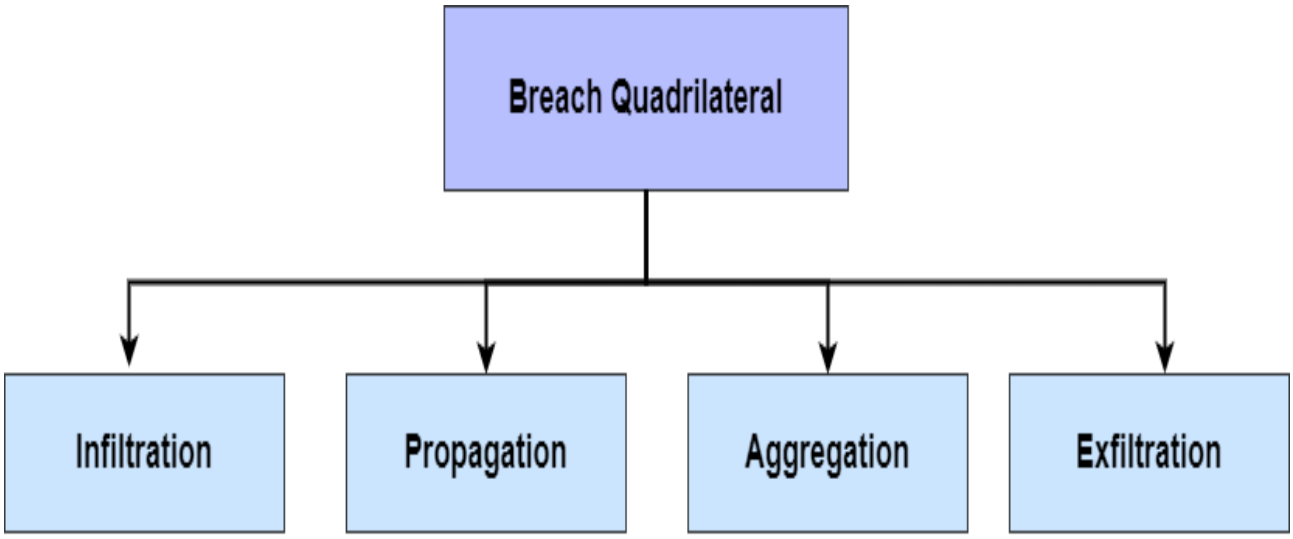

Fig. 2. Four security breach

5) CSRF: Utilized CSRF tokens to prevent Cross-Site Request Forgery (CSRF) attacks, ensuring that each form submission originates from the expected user. Implemented CSRF token generation and validation for every form in the system, adding a secure random token to each form submission and validating it on the server-side.

6) SQL Injection Prevention: Rejected access attempts from known malicious IPs and domains to prevent unauthorized access and potential security breaches. Maintained a list of known malicious IPs and domains and implemented a mechanism to block access attempts originating from these sources.

7) Malicious IP/Domain Reject: Blocked access from predefined malicious IP addresses and domains to prevent potential security breaches and unauthorized access attempts. Maintained a list of known malicious IPs and domains and implemented a mechanism to block access attempts originating from these sources, enhancing overall system security.

B. Propagation

In Fig.4 All steps of Propagation have shown:

1) Password Hashing: Used Django's default password hashing mechanism to securely store user passwords in the database. Utilized Django's default password hashing mechanism (PBKDF2 with SHA256) to hash and store passwords securely.

2) Security Headers: Configured security headers to enhance web application security. Configured security headers, including Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, and X-XSS-Protection.

3) Systems Events Logs: Implemented logging of system events for monitoring and troubleshooting. Configured logging settings to record critical database events and changes,

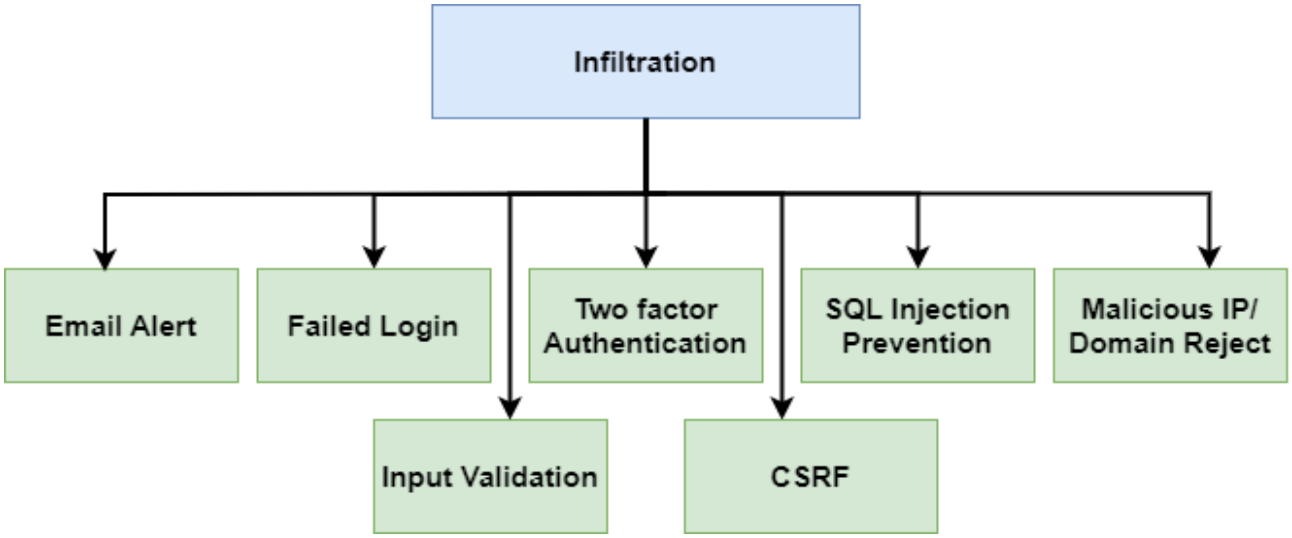

Fig. 3. Infiltration steps

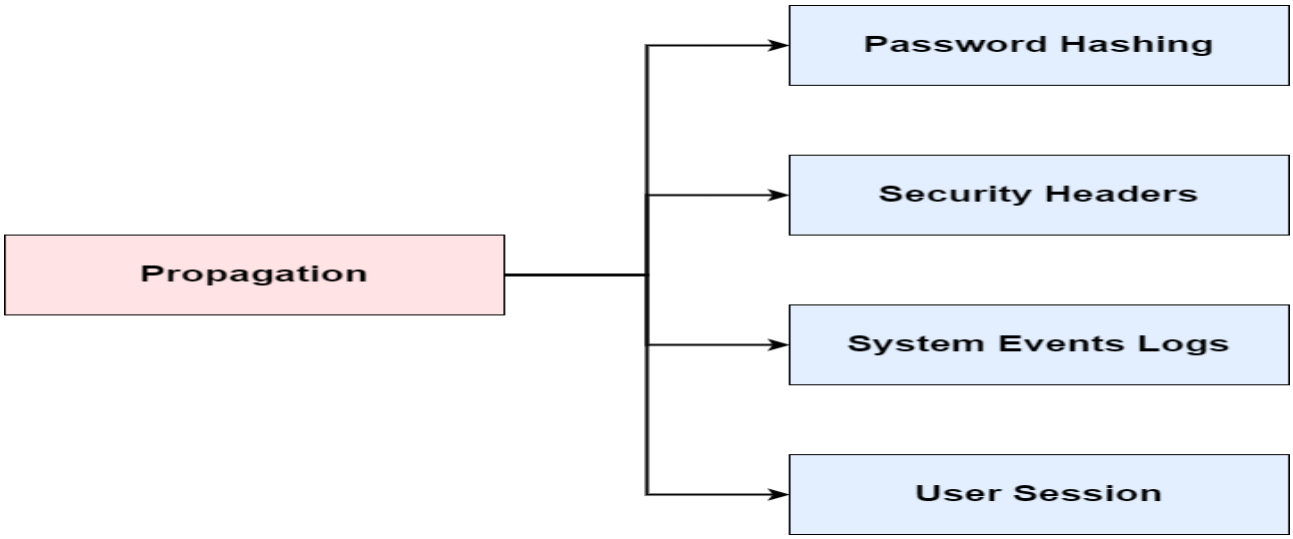

Fig. 4. Propagation steps

including CRUD operations, login attempts, and administrative actions.

4) User Session: Set session timeout to automatically log out inactive users. Configured session management settings to expire user sessions after a specified period of inactivity.

C. Aggregation

In Fig.5 All steps of Aggregation have shown:

1) Role Based Authorization: Established role-based access control for different user roles. Defined separate dashboards and permissions for admin, user, and superuser roles using Django's built-in authentication system.

2) Database Activities: Recorded database activities for auditing and compliance. Configured logging settings to record critical database events and changes, including CRUD operations, login attempts, and administrative actions.

3) Data Loss Prevention: Implemented rollback functionality for restoring the system to previous states in case of compromise or data loss. Developed rollback functionality to revert the system to a previous state using backup data.

4) Access Control: Allowed admin to manage user permissions and activities. Implemented role-based access control (RBAC) to assign specific permissions and privileges to users based on their roles and responsibilities.

D. Exfiltration

In Fig.6 All steps of Exfiltration have shown:

1) Firewall Rejection: Developed custom middleware to block access from unauthorized IP addresses. Implemented custom middleware to filter incoming requests based on IP geolocation, blocking access from specific countries or regions deemed high-risk or unauthorized.

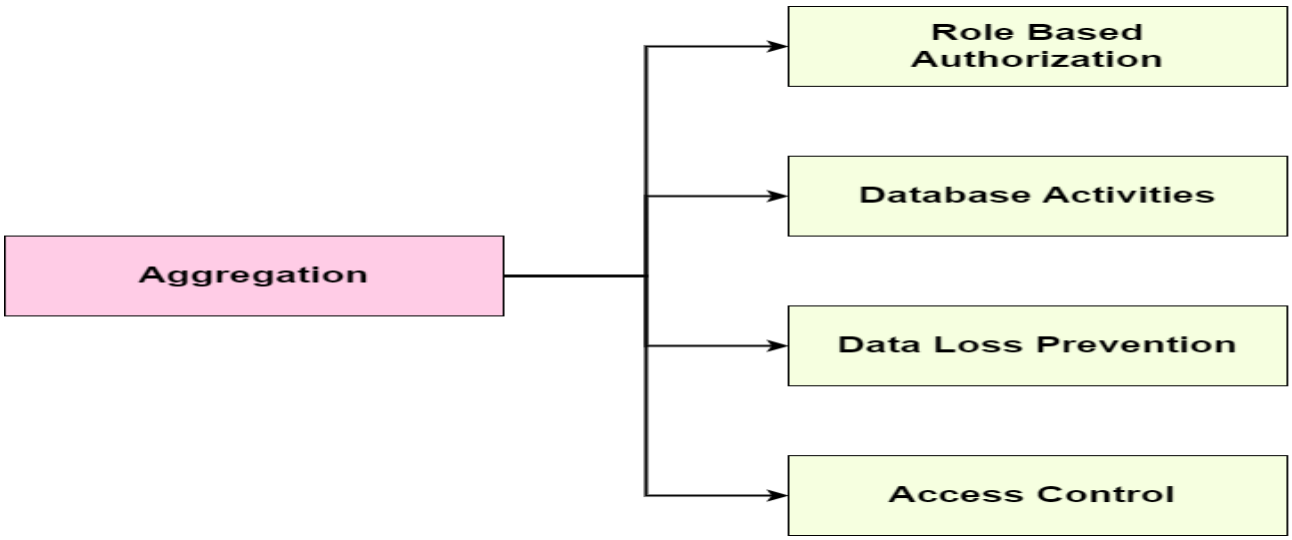

Fig. 5. Aggregation steps

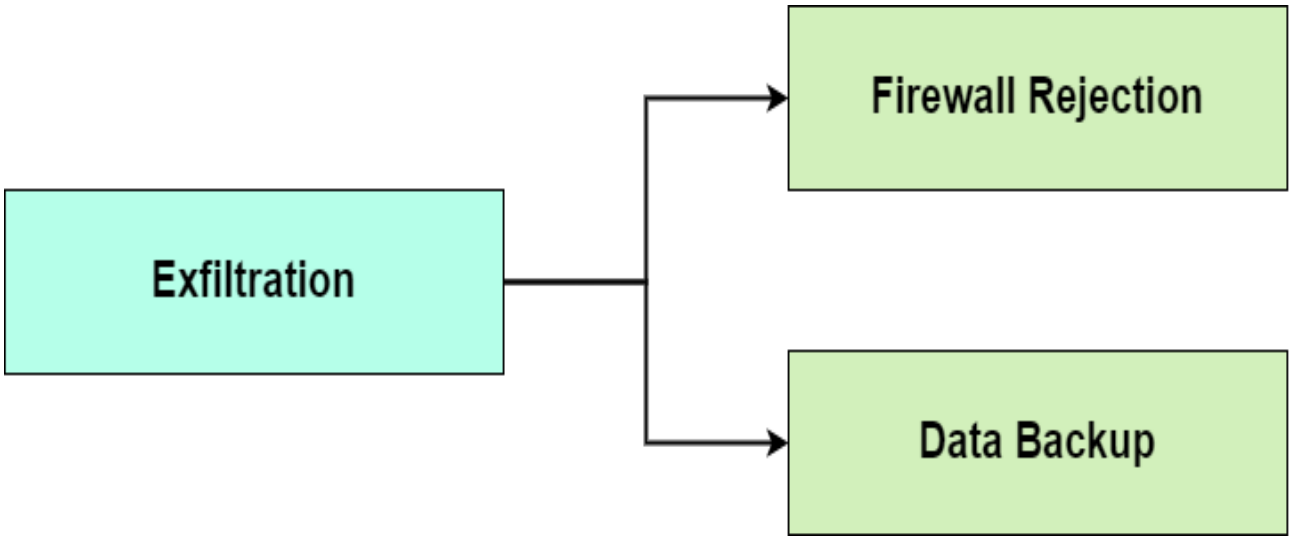

Fig. 6. Exfiltration Steps

2) Data Backup: Scheduled backups of the database for data integrity and recovery. Implemented scheduled backups of the database at specified intervals, generating backup files in PDF format and sending them via email for archival and recovery purposes.

V. Result and Discussion

In our quest to fortify the security of our e-commerce platform, we implemented several key measures aimed at enhancing protection against potential cyber threats. These measures spanned various facets of security, encompassing both preventive and detective mechanisms.

Firstly, we bolstered our security framework by introducing additional layers of defense. This included the implementation of email alerts, which promptly notify administrators of any suspicious activities or unauthorized access attempts. Furthermore, we heightened our vigilance by closely monitoring instances of failed login attempts, thereby preemptively thwarting potential brute force attacks. Additionally, stringent validation protocols were enforced to ensure the integrity and safety of user inputs, thereby mitigating risks associated with injection attacks such as SQL injection and Cross-Site Scripting (XSS).

To fortify authentication mechanisms, administrators were mandated to undergo a multifactor authentication process during login, thereby necessitating the provision of two distinct forms of verification to validate their identity. This stringent authentication protocol acted as a robust deterrent against unauthorized access attempts and significantly mitigated the risk of credential theft.

In tandem with authentication enhancements, proactive measures were undertaken to counteract potential cyber threats.

Specifically, we implemented mechanisms to proactively identify and neutralize malicious activities, effectively thwarting known attack vectors and malicious entities. By leveraging advanced threat intelligence and anomaly detection techniques, we were able to identify and block harmful IP addresses, thereby fortifying our defense perimeter against potential intrusions.

Moreover, a concerted effort was made to reinforce the resilience of our password management system. Through the implementation of stringent password policies and the adoption of cryptographic hashing techniques, we fortified our defenses against password-based attacks, thereby rendering it exceedingly difficult for malicious actors to compromise user credentials.

In addition to fortifying access controls, meticulous attention was devoted to securing sensitive areas of our platform. Access privileges were meticulously curated to ensure that only authorized personnel could access confidential information and critical system functionalities. Furthermore, continuous monitoring of database activities facilitated the early detection of anomalous behavior, enabling prompt intervention and remediation in the event of a security breach.

Furthermore, granular access controls were enforced to regulate user access privileges and restrict unauthorized access to sensitive data. By implementing role-based access control mechanisms, we ensured that only authenticated users with the requisite permissions could access confidential information, thereby minimizing the risk of data breaches.

Collectively, these comprehensive security enhancements culminated in a fortified e-commerce ecosystem, characterized by heightened resilience against potential cyber threats. By adopting a proactive approach to security, we succeeded in safeguarding the integrity, confidentiality, and availability of our platform, thereby fostering trust and confidence among our user base.

VI. Limitations and Conclusion

Despite the comprehensive security enhancements implemented within our e-commerce platform, it is imperative to acknowledge that no system is impervious to determined and resourceful adversaries. Skilled attackers possess the proficiency to exploit vulnerabilities, circumvent security controls, and infiltrate even the most fortified defenses. Thus, while our efforts have significantly bolstered the security posture of our platform, it remains essential to maintain a vigilant stance and acknowledge the inherent limitations of our security measures. Moreover, the dynamic nature of cybersecurity necessitates a proactive and adaptive approach to defense. As the threat landscape continues to evolve, new vulnerabilities emerge, and novel attack vectors surface, underscoring the importance of regular updates and continuous monitoring. By remaining abreast of emerging threats and promptly updating our defenses in response to evolving risks, we can fortify our resilience against potential cyber threats and mitigate the likelihood of successful attacks.

Furthermore, while our security enhancements have been instrumental in fortifying the integrity and security of our platform, certain limitations persist. Notably, certain security features such as input validation, two-step verification, and monitoring of recent activities are currently only implemented for specific sections of our platform, predominantly catering to either administrators or users. Moving forward, there is a concerted effort to extend these security measures to encompass all sections of our platform, thereby ensuring a uniform and comprehensive security posture across all user categories.

In conclusion, while our concerted efforts have yielded significant improvements in the security of our e-commerce platform, the journey towards maintaining a secure online environment is an ongoing endeavor. As custodians of sensitive data and entrusted with safeguarding the interests of our customers, we are committed to the relentless pursuit of security excellence. By adhering to best practices, conducting regular security assessments, and fostering a culture of security awareness, we endeavor to uphold the highest standards of security excellence and ensure the continued safety of our business and clientele in an ever-evolving digital landscape.

VII. Other Links

Video links: https://drive.google.com/drive/folders/1s5jFZYTlX33uqNzv
a

Github Links: https://github.com/saikathossain201214/cs$_e commerce_s ecur$

References

[1] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Computer Communications*, vol. 153, pp. 311–335, 2020.

[2] I. Anwary, "The role of public administration in combating cybercrime: An analysis of the legal framework in indonesia," *International Journal of Cyber Criminology*, vol. 16, no. 2, pp. 216–227, 2022.

[3] M. Halaweh and C. Fidler, "Security perception in e-commerce: Conflict between customer and organizational perspectives," in *2008 International Multiconference on Computer Science and Information Technology*. IEEE, 2008, pp. 443–449.

[4] V. Srikanth and D. R. Dhanapal, "E-commerce online security and trust marks," *International Journal of Computer Engineering and Technology*, vol. 3, no. 2, pp. 238–255, 2012.

[5] B. Xiao and I. Benbasat, "Research on the use, characteristics, and impact of e-commerce product recommendation agents: A review and update for 2007–2012," *Handbook of strategic e-business management*, pp. 403–431, 2014.

[6] S.-K. Kim *et al.*, "Enhanced stochastic methodology for combined architecture of e-commerce and security networks," *Mathematical Problems in Engineering*, vol. 2009, 2009.

[7] L. Qiu, J. Li *et al.*, "Covering the monitoring network: A unified framework to protect e-commerce security," *Complexity*, vol. 2017, 2017.

[8] F. T. Abdul Hussien, A. M. S. Rahma, and H. B. Abdul Wahab, "A secure environment using a new lightweight aes encryption algorithm for e-commerce websites," *Security and Communication Networks*, vol. 2021, pp. 1–15, 2021.

[9] D. Liu and M. Li, "Exploring new factors affecting purchase intention of mobile commerce: trust and social benefit as mediators," *International Journal of Mobile Communications*, vol. 17, no. 1, pp. 108–125, 2019.

[10] S. M. R. Farshchi, "Study of security issues on traditional and new generation of e-commerce model ipcsit vol. 9," 2011.

[11] R. Barskar, A. J. Deen, J. Bharti, and G. F. Ahmed, "The algorithm analysis of e-commerce security issues for online payment transaction system in banking technology," *arXiv preprint arXiv:1005.4266*, 2010.

[12] M. Niranjanamurthy and D. Chahar, "The study of e-commerce security issues and solutions," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 7, pp. 2885–2895, 2013.

[13] I. D'Adamo, R. González-Sánchez, M. S. Medina-Salgado, and D. Settembre-Blundo, "E-commerce calls for cyber-security and sustainability: How european citizens look for a trusted online environment," *Sustainability*, vol. 13, no. 12, p. 6752, 2021.
[14] N. Chawla and B. Kumar, "E-commerce and consumer protection in india: the emerging trend," *Journal of Business Ethics*, vol. 180, no. 2, pp. 581–604, 2022.
[15] S. E. Cebeci, K. Nari, and E. Ozdemir, "Secure e-commerce scheme," *IEEE Access*, vol. 10, pp. 10 359–10 370, 2022.
[16] P. Suchánek, "E-commerce systems and e-shop web sites security," 2009.
[17] L. Li, "Data security technology in electronic commerce system development," in *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*. IEEE, 2023, pp. 1–6.
[18] J. R. Shaikh and G. Iliev, "Blockchain based confidentiality and integrity preserving scheme for enhancing e-commerce security," in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE, 2018, pp. 155–158.
[19] C. Liu, D. Liu, Y. Li, M. Yang, and J. Zhang, "Construction of the electronic commerce security system based on internet," in *2009 Asia-Pacific Conference on Computational Intelligence and Industrial Applications (PACIIA)*, vol. 2. IEEE, 2009, pp. 77–79.
[20] S. W. Guo, "E-commerce information management system data security research," *Advanced Materials Research*, vol. 971, pp. 1924–1927, 2014.