Evaluating Performance and Security Vulnerabilities of Bangladeshi E-commerce Websites Using JMeter and OWASP ZAP

Md. Nafis Ulfat
American International University - Bangladesh
Email: 25-93602-1@student.aiub.edu
DR. Firoz Ahmed
American International University - Bangladesh
Email: fahmed@aiub.edu

Abstract—**E-commerce has become a crucial part of Bangladesh's digital economy, but issues with website performance and security can affect user experience and trust. This research focuses on the evaluation of the performance and security of popular Bangladeshi commerce websites. The main goal of this research is to assess how well these websites perform under heavy traffic and to identify common security vulnerabilities. Performance testing was done using JMeter to simulate user traffic, while security testing using OWASP ZAP aimed to identify common security vulnerabilities in websites, particularly focusing on issues such as weak encryption and poor user authentication. Based on the results, this study proposes a framework, BESPT (Bangladeshi E-commerce Security & Performance Testing), which is also introduced to guide future assessments of performance and security for e-commerce platforms in Bangladesh. The findings revealed that many e-commerce sites slow down with high user traffic, causing potential frustration for customers. In terms of security, several vulnerabilities were identified, including insecure data protection and authentication flaws. In conclusion, this paper highlights the importance of improving website performance and security on e-commerce websites in Bangladesh. Addressing these issues can enhance the shopping experience and build greater trust among users.**

Index Terms—**Performance testing, Security testing, E-commerce, Bangladeshi websites, JMeter, OWASP ZAP.**

I. Introduction

In recent years, e-commerce has significantly transformed the shopping habits of people in Bangladesh. With just a few clicks, consumers can now purchase goods from home, making the process faster and more convenient than ever. E-commerce in Bangladesh has seen exponential growth in recent years, but challenges like a lack of logistics, technical knowledge gaps, and inconsistent security protocols remain significant barriers to sustainable development(1). While the growing demand has led many businesses to establish an online presence, these challenges, especially related to logistics, technical capabilities, and security, hinder the industry's full potential. These challenges pose serious threats to the sustainability and reliability of online services in Bangladesh. E-commerce success depends not only on product offerings but also on website performance and security. If a website is slow or frequently crashes, customers may leave without completing their purchases. The collapse of some e-commerce ventures due to trust and regulatory failures has severely impacted consumer confidence, calling for stricter legal and operational frameworks(2). Similarly, security weaknesses can expose personal and financial information, leading to serious risks for both businesses and users. Despite digital growth, many Bangladeshi websites, including financial and government platforms, suffer from vulnerabilities like XSS and SQL injection, highlighting the urgent need for improved cybersecurity(3). While online shopping continues to grow rapidly in Bangladesh, limited research has focused specifically on evaluating the performance and security of local e-commerce platforms. Understanding these technical shortcomings is essential for building trust, ensuring smooth user experiences, and shaping future development strategies. In response to these challenges, this study aims to assess the performance and security aspects of leading Bangladeshi e-commerce websites, identify key technical issues, and propose practical solutions to improve their reliability and safety.

Despite the fast-paced growth of e-commerce in Bangladesh, many websites continue to struggle with performance inefficiencies and security vulnerabilities. Security testing of E-commerce websites identifies major weaknesses like weak authentication and insufficient session handling, exposing users to hazards(4). Web commerce sites' vulnerability scans underscore common threats like SQL injection and cross-site scripting, calling for enhanced protection schemes(5). Common issues include slow page loading times, server crashes during checkout, and insecure data handling. These problems not only disrupt user experience but also affect consumer trust and overall sales.

Although these concerns are well-recognized globally, research focusing specifically on Bangladeshi e-commerce websites is limited. To address this gap, the study seeks to answer the following questions:

1) What are the main performance issues faced by

Bangladeshi e-commerce websites?

2) What security risks are common on these platforms?
3) What strategies can be adopted to enhance website performance and security to ensure a better user experience and safer transactions?

The primary goal of this study is to examine the performance and security vulnerabilities of Bangladeshi e-commerce platforms and recommend effective solutions. The specific objectives include:

1) Assess how well Bangladeshi e-commerce websites perform in terms of speed, stability, and user experience.
2) Identify common security risks and vulnerabilities affecting these platforms.
3) Propose best practices and solutions to enhance website performance and security.

As more consumers embrace online shopping in Bangladesh, the reliability and safety of e-commerce websites have become increasingly important. A platform that performs well and protects customer data can foster trust, improve customer satisfaction, and encourage repeat purchases. This study is significant as it addresses real-world technical problems faced by many local e-commerce businesses. By identifying performance bottlenecks and security flaws, the findings will help developers optimize website speed and stability. Additionally, the research will provide valuable insights to business owners and policymakers for making informed decisions that promote safer and more efficient digital commerce. Furthermore, this study contributes to the growing body of research on digital transformation in Bangladesh and can serve as a reference for future work focused on enhancing online services in developing countries.

II. Literature Review

Performance testing ensures a web application's reliability and efficiency as user volumes grow. Several studies have analyzed system performance, security vulnerabilities, and optimization strategies across various domains. Also, some research paper highlights risks such as cyber threats and system failures, emphasizing the need for robust security measures and performance optimization frameworks. A study recommends a systematic approach to performance bottleneck detection in the case of extreme ones based on server performance tests with varying CPU frequencies. Apache JMeter was utilized as a load generator, and Elasticsearch and Kibana for analysis in one study to demonstrate severe performance bottlenecks(6). Also, a comparison was done of a web-based teacher information system's performance in terms of login feature, update profile, image upload, and question creation. Improved response times and better throughput with JMeter and BlazeMeter were witnessed, validating the usability of tools for web application testing(7). E-commerce sites are exposed to heavy concurrent user loads and therefore suffer from a great deal of performance problems. A research assessed e-commerce site performance using throughput, availability, and response time measurements based on JMeter. The research emphasized the significance of robust web architecture in addressing heavy traffic loads without any problems(8). The importance of web application performance testing was also depicted by an analysis of load tests on application bottlenecks. One experiment that started from 200 users and ramped up to 500 found there were very considerable differences in throughput, response time, and variation, showing how important performance testing is to decide the points where the improvement can be made(9). A comparative webpage test of Shopee pre-pandemic and during the pandemic period revealed that increased user visits led to higher levels of website stress, and error rates rose to 26% when under load(10). Another study was set to test an electronic payment website, comparing the performance of different web servers, including Nginx and Apache. The study concluded that web application performance testing is necessary to make sure that web applications can handle mass user traffic while still maintaining service quality(11). Last but not least, the performance of university admission portals was tested to determine their ability to handle many student applications. Response time, throughput, and system scalability were measured using JMeter in this study, attesting to the usefulness of performance testing in securing smooth and efficient admission processes(12).

This paper addresses software security practices in the emerging software industry of Bangladesh, emphasizing the ignorance of security beyond the West. It emphasizes the security attitude of developers and security problems in Bangladesh, providing recommendations for sustainable security practices(13). This research has taken into account risks and vulnerabilities in Bangladesh's e-commerce security. It has taken into account the country's lack of awareness regarding digital risks and has recommended policy guidelines for increased security through public awareness campaigns, curriculum revision, and better legal systems(14). This paper discusses SQL injection web application vulnerabilities, particularly in Bangladesh. It analyzes 150 websites to analyze their susceptibility to SQLi-based attacks and compares two third-party tools (Havij and SQLmap) for vulnerability detection(15). This study examines the performance of Bangladesh's ten e-commerce websites using tools like WebpageTest, PageSpeed Insights, and GTmetrix. It calculates factors like load time and overall blocking time to assess site performance and provide optimization suggestions(16). The study focuses on the security of the Bangladeshi e-commerce site using vulnerability-focused techniques like Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS). It uses the scanning tools Acunetix and Nikto(17). The study prioritizes the recognition of vulnerabilities using penetration testing and source code review. It gives importance to high percentages of vulnerability in government websites and presents outcomes in graphical representations(18).

III. Methodology

This study focuses on testing the performance and security of e-commerce websites. A quantitative approach was chosen because it allows us to measure and compare website performance using numbers and data. The goal is to see how well these websites handle heavy traffic and whether they have any security risks.

A. Research Design

An experimental design was used in this study. Websites were tested under various conditions to observe their behavior. Two tools were used:

1) Apache JMeter for performance testing
2) OWASP ZAP for security testing

This approach ensures real results based on actual testing, not assumptions.

B. Data Collection Methods

Performance Testing: Six popular Bangladeshi e-commerce websites were selected for evaluation: Daraz, AjkerDeal, Bikroy.com, Othoba, Pickaboo, and Rokomari. These platforms were chosen based on traffic volume, service diversity, and consumer reach. The following tests were conducted to assess website performance:

1) Load Testing: Simulated multiple users accessing the site at the same time.
2) Stress Testing: Gradually increased users to find the point where the website slows down or crashes.
3) Response Time Measurement: Measured how fast pages load and respond to actions like clicking.

Tool Used: Apache JMeter Data Collected: Page load speed, number of handled requests, error rates.

Security Testing: To identify security weaknesses, the following activities were performed:

1) Scanning for Common Threats: Checked for SQL Injection, XSS, CSRF, etc.
2) Authentication Interface Assessment: Checked for common weaknesses in login mechanisms, such as missing input validation or insecure session handling, using automated scanning tools. No real login credentials were used.

Tool Used: OWASP ZAP Issues Checked: Insecure settings, data leaks, and authentication problems.

Website Selection Criteria: Popular e-commerce websites with high traffic and diverse products/payment options were selected. The websites were chosen based on popularity, high user traffic, and variety in products and payment options.

Data Analysis Methods

Performance Analysis: Multiple test scenarios were created simulating different user loads (ranging from 1 to 300 concurrent users) using Apache JMeter. Each test recorded response time, throughput, and error rates under increasing user load conditions to identify system breaking points.

- Page Speed: Measured under different load conditions.
- Error Rate: Percentage of failed or delayed responses.
- User Handling Capacity: Maximum number of users the website could handle without crashing.

Security Analysis:

- Types and Number of Vulnerabilities: Identified during testing.
- Risk Level Assessment: Categorized as critical, moderate, or low.
- Recommendations: Suggested ways to fix or reduce vulnerabilities.

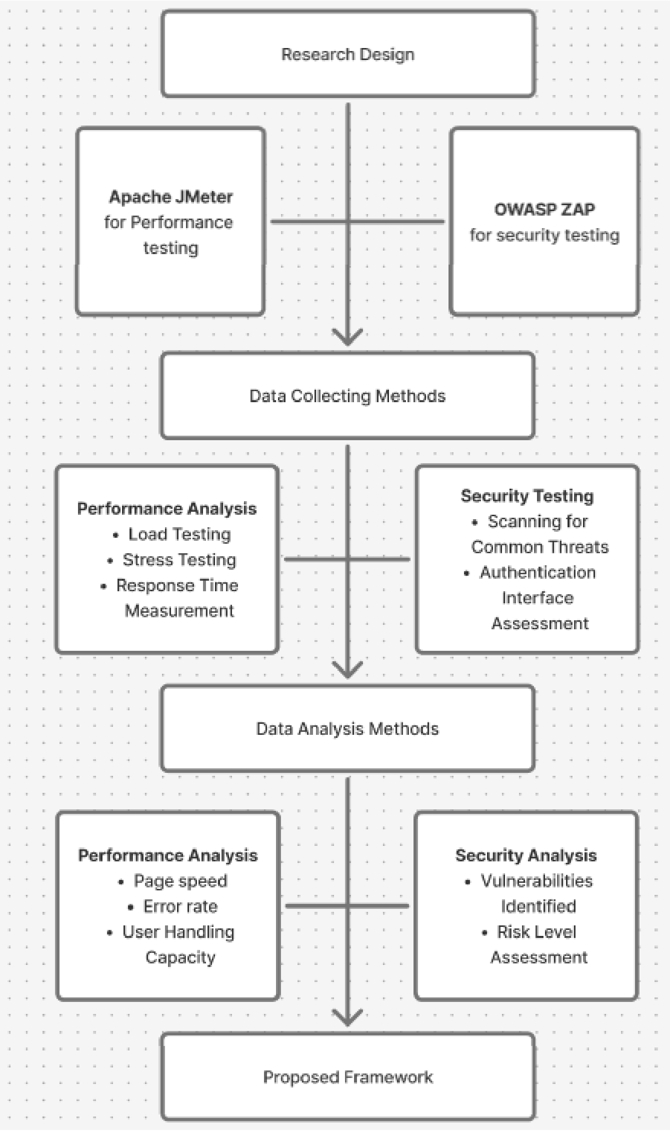

Fig. 1. Research Design

C. Proposed Framework:

To systematize the testing process, this study introduces the Bangladeshi E-commerce Security and Performance Testing (BESPT) framework. The framework consists of six stages:

- Planning

Identify test goals, key performance indicators (KPIs), and security objectives.
Select appropriate testing tools (e.g., Apache JMeter for performance, OWASP ZAP for security).

- Performance Testing
  Conduct load testing, stress testing, and response time checks using Apache JMeter.
  Measure throughput, server errors, and scalability under user traffic.

- Security Testing
  Scan websites using OWASP ZAP to detect vulnerabilities such as SQL Injection, XSS, CSRF, and weak authentication.
  Perform both automated scanning and manual verification if necessary.

- Analysis
  Evaluate collected data to identify bottlenecks and security flaws.
  Classify issues based on severity (e.g., high, medium, low risk).

- Mitigation
  Apply solutions such as code improvements, better server configurations, and stronger authentication measures.
  Patch vulnerabilities and optimize system performance.

- Re-evaluation
  Re-test the websites after mitigation to ensure improvements were effective.
  Use consistent metrics to compare pre- and post-fix performance and security.

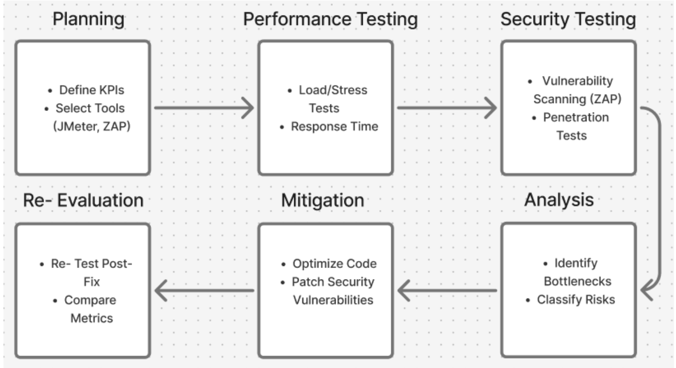

Fig. 2. BESPT Framework

This framework aims to help developers, testers, and policymakers follow a clear process for improving the reliability and safety of Bangladeshi e-commerce platforms.

Only publicly available websites were tested. No modifications were made that could damage or alter the websites. No private or sensitive user data was accessed. All tests were conducted in a safe, controlled environment. The study followed ethical guidelines to ensure no harm was done to any website or user.

We only tested a few selected websites, so results may not be generalizable to all e-commerce websites in Bangladesh. Future studies could expand the sample size and include diverse platforms for broader insights. Performance tests were done in a controlled setup, which may not match real-world conditions exactly. Security testing was non-invasive, so some deep issues might not have been detected.

IV. Results and Discussion

Website Performance Overview

The performance test results for six popular Bangladeshi e-commerce websites AjkerDeal, BikroyDotCom, Daraz, Othoba, Pickaboo, and Rokomari revealed significant differences in terms of speed, stability, and user capacity.

Table 1 - Website Performance Overview

Website	APDEX	Avg (ms)	Max (ms)	Error %
AjkerDeal	0.254	23467.97	195570	0.47
BikroyDotCom	0	61755.12	537379	3.5
Daraz	0.313	7692.71	69525	0.29
Othoba	0.181	22052.82	107883	6.75
Rokomarydotcom	0.187	23044.55	137252	1.01

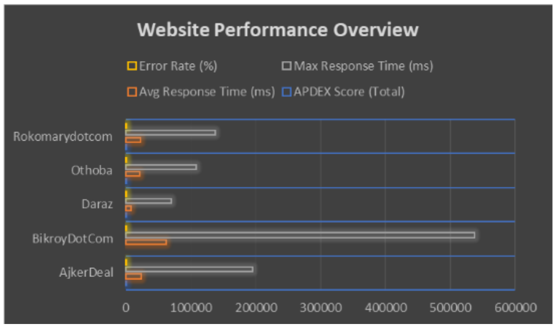

Fig. 3. Website Performance Overview

Best Performer: Daraz showed the highest APDEX score (0.313), fastest average response time (7692.71 ms), and lowest error rate (0.29

Worst Performer: BikroyDotCom had the lowest APDEX (0.000) and highest average and maximum response times, suggesting poor scalability and user experience.

Moderate Performance: AjkerDeal and Rokomari had moderate APDEX scores but relatively high response times, indicating room for optimization.

Table 2 - Error Pattern Analysis

Website	Major Error Types
AjkerDeal	Connection Timeout (75%), Non-HTTP Errors (25%)
BikroyDotCom	Chunked Message Failures (40%), Unknown Host/Socket Exceptions (30%)
Daraz	SSL Handshake Failures (40%), No Response (40%)
Othoba	504 Gateway Timeout (89.66%), 502 Bad Gateway (10.34%)
Rokomary	503 Service Unavailable (50%), Read Timed Out (25%), No Response (25%)

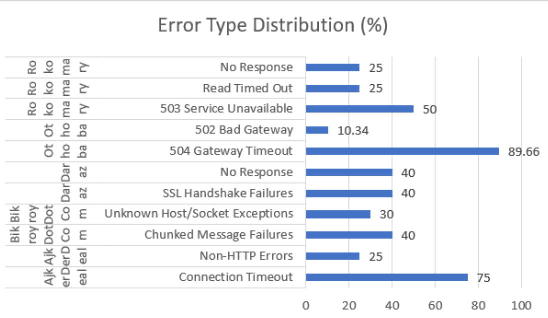

Fig. 4. Error Type Distribution)

AjkerDeal and Rokomari faced issues with timeouts and temporary server unavailability. Daraz had secure connection-related problems but still managed better performance overall. Othoba suffered from a very high rate of gateway timeout errors, indicating server overload. BikroyDotCom showed the most critical failure types, with severe connection-level breakdowns.

The analysis indicates that not all websites are equally optimized for high traffic. While Daraz performed the best, most websites (especially BikroyDotCom and Othoba) struggled under stress. This suggests that:

- Infrastructure upgrades and server-side optimizations are needed for several platforms.
- Common bottlenecks include slow page load times, server unavailability, and connection issues, especially during peak load.
- Performance testing tools like Apache JMeter can reveal critical system weaknesses before real users experience them.

In the security testing phase, we analyzed the number of alerts raised for different websites based on their risk level and the confidence of the results. The following tables summarize the findings for risk levels and sites where vulnerabilities were detected.

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence in the testing report. The percentages in brackets represent the count as a percentage of the total alerts.

From the table, we can observe:

- Medium and Low risk alerts make up the majority of the alerts, with Medium risk at 52.6% and Low at 36.8%.

Table 3 - ALERT COUNTS BY RISK AND CONFIDENCE

Risk/Confidence	User Confirmed	High	Medium	Low	Total
High	0 (0.0%)	2 (10.5%)	0 (0.0%)	0 (0.0%)	2 (10.5%)
Medium	0 (0.0%)	1 (5.3%)	2 (10.5%)	1 (5.3%)	4 (21.1%)
Low	0 (0.0%)	1 (5.3%)	5 (26.3%)	1 (5.3%)	7 (36.8%)
Informational	0 (0.0%)	0 (0.0%)	3 (15.8%)	3 (15.8%)	6 (31.6%)
Total	0 (0.0%)	4 (21.1%)	10 (52.6%)	5 (26.3%)	19 (100%)

- Informational alerts constitute 31.6% of the total alerts, providing useful insights for improving security measures.

Alert Counts by Site and Risk

This table shows the number of alerts raised for each website at different risk levels. It includes the number of alerts raised at or above each risk level for every site.

Table 4 - ALERT COUNTS BY SITE AND RISK

Site	High (>= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
ajkerdeal	0 (0)	9 (9)	12 (21)	5 (26)
bikroy	2 (2)	4 (6)	7 (13)	6 (19)
daraz	2 (2)	4 (6)	9 (15)	8 (23)
pickaboo	1 (1)	3 (4)	5 (9)	7 (16)
priyoshopretail	1 (1)	3 (4)	10 (14)	6 (20)

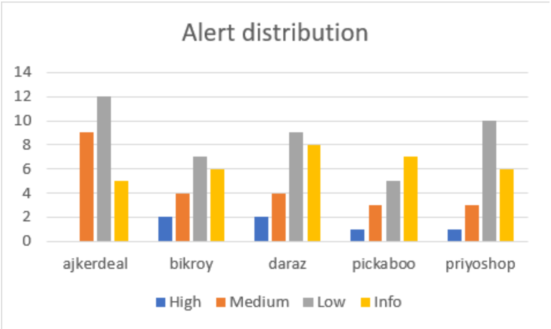

Fig. 5. Alert distribution (High, Medium, Low, Informational

Total Alerts per Site:
ajkerdeal.com = 26, bikroy.com = 30, daraz.com.bd = 46, pickaboo.com = 30, priyoshopretail.com = 39

Grand Total Alerts (All Sites Combined): 171

Risk Distribution:

- The medium and low risk alerts are the most prevalent across all tested websites. This suggests that while most of the vulnerabilities identified are not critically dangerous, they still pose significant risks that need to be addressed.
- Informational alerts are also noteworthy, as they highlight potential improvements that could be made to prevent future vulnerabilities.

Site-Specific Vulnerabilities:

- Sites like https://ajkerdeal.com and https://bikroy.com have a relatively higher number of low-risk and informational alerts, which indicates minor but not critical security weaknesses.
- Websites like https://www.daraz.com.bd and https://priyoshopretail.com show more severe issues, with a mix of high, medium, and low-risk alerts, indicating a need for immediate attention and improvement in security practices.

In the case of Bikroy.com, which exhibited the highest average response time (61,755 ms) and an error rate of 3.5%, we proposed several performance improvement strategies including server upgrade, implementation of caching mechanisms, and optimization of session handling. These recommendations are based on similar studies (19),(20) that reported 60–80% performance improvement after adopting such techniques in the context of Bangladeshi e-commerce platforms. Following these precedents, we estimated that the average response time could be reduced to approximately 10,000 ms and the error rate could drop to around 0.5%. While these improvements are hypothetical and based on secondary findings, they provide a realistic projection of the potential gains achievable through targeted performance tuning.

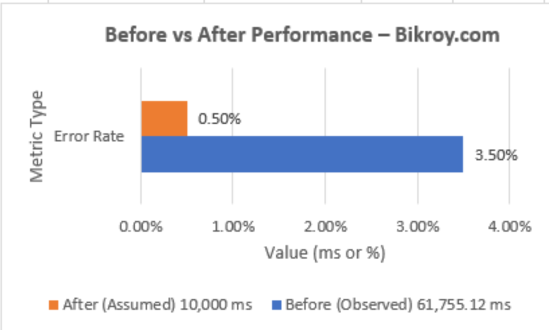

Fig. 6. Before vs After Performance - Bikroy.com

The combined performance and security evaluation reveals that while some Bangladeshi e-commerce platforms demonstrate acceptable technical resilience, many remain ill-equipped for large-scale traffic or robust defense against cyber threats. Key discussion points include:

- Performance Deficiencies: High response times and frequent server errors under simulated load suggest a need for capacity planning, load balancing, and database optimization.
- Security Weaknesses: Even medium-risk vulnerabilities can be exploited to compromise data integrity. Regular penetration testing, code audits, and secure development practices should be institutionalized.
- Need for Structured Testing: The BEPST framework proved effective in providing a clear structure for simultaneous evaluation. Platforms adopting it can benchmark their performance, reduce risks, and improve user satisfaction.

V. Conclusion

This study evaluated the performance and security of several popular Bangladeshi e-commerce websites using Apache JMeter and OWASP ZAP. The results revealed that while a few platforms performed well under pressure, many showed critical weaknesses such as high response times, server errors, and common security vulnerabilities, including weak authentication and insecure data handling. To address these issues, we introduced the BESPT Framework (Bangladeshi E-commerce Security & Performance Testing), a structured approach that combines planning, testing, analysis, and re-evaluation. This framework provides a clear guideline for developers and testers to systematically assess and improve their websites. By adopting regular testing practices and implementing the recommended improvements, Bangladeshi e-commerce platforms can enhance user trust, provide smoother shopping experiences, and reduce the risk of cyber threats. Future research can build on this work by incorporating large-scale, real-time traffic simulations, machine learning based anomaly detection, and comparative benchmarking against international platforms to derive deeper insights into systemic performance and security gaps.

References

[1] Rahman, M. (2023). The Rise of E-Commerce in Bangladesh and Its Expansion. Journal of Management and Administration Provision, 3(3), 93-104.

[2] Chowdhury, M. S. A., Bappi, M. A. U., Imtiaz, M. N., Hoque, S., Islam, S., & Haque, M. S. (2022). The Transition of E-Commerce Industry in Bangladesh: Added Concerns & Ways of Recovery. International Journal of Economics and Finance, 14(7), 1-18.

[3] Rifat, M. A. K., Sultana, Y., & Hossain, B. M. (2023). Vulnerabilities Assessment of Financial and Government Websites: A Developing Country Perspective. International Journal of Information Engineering and Electronic Business, 15(5), 42-53.

[4] Vamsi, P. R., & Jain, A. (2021). Practical security testing of electronic commerce web applications. International Journal of Advanced Networking and Applications, 13(1), 4861-4873.

[5] Baako, I., & Umar, S. (2020). An integrated vulnerability assessment of electronic commerce websites. International Journal of Information Engineering and Electronic Business, 14(5), 24.

[6] Suryaningrat, A., Ramayanti, D., & Sakti, A. D. (2024). Bottleneck Identification in Web Applications using Apache JMeter and Elastic Stack. Jurnal Inovatif: Inovasi Teknologi Informasi dan Informatika, 7(1), 1-11.

[7] Indrianto, I. (2023). Performance testing on web information system using apache jmeter and blazemeter. Jurnal Ilmiah Ilmu Terapan Universitas Jambi, 7(2), 138-149.

[8] Shafana, A. R. F., Musfira, A. F., & Naja, M. M. F. (2021). Assessing the E-commerce websites for performance using automated testing tools.

[9] Suryadevara, S., & Ali, S. (2020, June). Preperformance testing of a website. In CS & IT Conference Proceedings (Vol. 10, No. 7). CS & IT Conference Proceedings.

[10] Musthafawi, A. Z., Mas' adah, A., Sukmadiningtyas, & Ramdani, F. (2020, November). Performance testing on the shopee website in the pandemic period of COVID-19. In Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology (pp. 195-199).

[11] Hidayanto, R., & Sawitri, P. (2019). Performance testing of e-payment website using JMeter. International Research Journal of Advanced Engineering and Science, 4(3), 350-352.

[12] Putri, M. A., Hadi, H. N., & Ramdani, F. (2017, November). Performance testing analysis on web application: Study case student admission web system. In 2017 international conference on sustainable information engineering and technology (SIET) (pp. 1-5). IEEE.

[13] Shrestha, A., Sharma, T., Saha, P., Ahmed, S. I., & Al-Ameen, M. N. (2023). A first look into software security practices in bangladesh. ACM Journal on Computing and Sustainable Societies, 1(1), 1-24.

[14] Islam, M. T., Islam, M. F., & Sawda, J. (2022). E-commerce and cyber vulnerabilities in bangladesh: A policy paper. International Journal of Law and Society, 1(3), 186-203.

[15] Chakma, S., Pushpa, I. A., Tahmiduzzaman, K. B. M., & Rahman, M. S. (2022, October). Performance Analysis of Identifying SQL Injection Vulnerability in the Context of Bangladeshi Websites. In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[16] Hossain, M. T., Hassan, R., Amjad, M., & Rahman, M. A. (2021). Web performance analysis: an empirical analysis of e-commerce sites in Bangladesh. International Journal of Information Engineering and Electronic Business, 11(4), 47.

[17] Rahman, M. A., Amjad, M., Ahmed, B., & Siddik, M. S. (2020, January). Analyzing web application vulnerabilities: an empirical study on e-commerce sector in Bangladesh. In Proceedings of the international conference on computing advancements (pp. 1-6)

[18] Moniruzzaman, M., Chowdhury, F., & Ferdous, M. S. (2019, February). Measuring vulnerabilities of bangladeshi websites. In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-7). IEEE.

[19] Sathiyamoorthi, V., & Bhaskaran, V. M. (2012). Optimizing the Web Cache performance by Clustering Based Pre-Fetching Technique Using Modified ART1. International Journal of Computer Applications, 44(1), 7-9.

[20] Khan, H. (2024). Supercharge Your Next.js App: 10x Optimization Tips for 2024. DEV Community.