IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

SafetyEcom: A Secure and Specialized E-Commerce Platform for Safety Equipment – A Comprehensive Analysis

Patel Mohammad Hasim Rasid Ahmed[1], Ms. Khushi Vaishnav[2]
Student, P P Savani University, Surat
Lecturer, P P Savani University, Surat
patelhasim744@gmail.com, khushi.vaishnnav@ppsu.ac.in

Abstract: *In this digital era, E-Commerce Systems have emerged to become one of the most preferred methods for making international transactions. Yet, specialty-based e-commerce websites for products such as safety equipment have specific obstacles while trying to integrate efficiency with high security. In this context, this paper will provide an intensive analysis of SafetyEcom which is a specialty-based e-commerce website focusing on providing safety products such as helmets and masks. In doing so, it will describe and review all aspects of the website including its front-end design (PHP, HTML, CSS, jQuery) and back-end programming (MySQL, XAMPP) alongside its development procedure (Incremental Model). Moreover, this work will provide a literature survey about security threats in e-commerce websites from 2014 to 2024. This study finds that E-Commerce websites are the most vulnerable websites and represent 32.4% of all attack targets. Major findings indicate that backdoors (68%), malware (56.4%), and SQL Injection (38%) are major security threats in E-Commerce websites. This work indicates gaps in security-oriented information concerning safety equipment websites and recommends future enhancements in this area.*

Keywords: SafetyEcom, E-commerce security, PHP, MySQL, Incremental Model, Safety equipment, SQL injection, XAMPP

I. INTRODUCTION

The history of e-commerce started on August 11, 1994, with the first ever sale of a compact disc on the web site named American Retail [1]. Thus, an online sale took place for the first time within the framework of the World Wide Web. E-commerce refers to transactions conducted via the internet and associated with transferring both monetary and informational assets. According to global research on digitalisation in 2023, almost 4.9 billion users were using the Internet. This has made digitalisation the main global tendency. Nonetheless, this tendency bears certain risks that cannot be ignored. Online safety is the implementation of particular measures to carry out transactions safely [2]. Otherwise, there will be numerous risks and instances of online fraud. SafetyEcom is an e-commerce platform which is intended to conduct online purchases and sales of various safety items including helmets, masks, and so forth. The SafetyEcom platform comprises such functionalities as:

• Admin functionalities: login, dashboard, categories, products management, orders management, and reporting.
• Customer functionalities: register, login, products browsing, basket, wish list, rating products, and ordering.

This work considers SafetyEcom implementation, identifies security threats, and suggests solutions for the future.

II. BACKGROUND

A. Necessary Conditions for Secure Transactions

Network security serves as the foundation of e-commerce security. There are five important elements that need to be present. Confidentiality offers security to data by not allowing anyone to access the data without permission, for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

example, by encrypting passwords. Integrity maintains the validity of the data and prevents any alterations, like modifying the price while transferring the data. Availability is achieved by providing uninterrupted availability of data to those who have permissions, which means servers should remain up 100 percent of the time. Authentication is done to confirm the identification of a person, typically through administrative or client logins.

B. Security Protocols Used in SafetyEcom

Three primary types of security measures are used by SafetyEcom. HTTPS is the secure protocol of HTTP with SSL/TLS encryption. The SSL certificate encrypts data transfers from the browser to the server. In addition, the security of XAMPP is also adopted by protecting the local database using the MySQL password.

II. LITERATURE REVIEW

The Dimensions database was used to analyse literature between 2014 and 2024. The quantity of publications related to e-commerce crimes has continuously increased, peaking in recent years, as cybercriminals have increasingly begun to direct their activities against online retail establishments.

A. The Industry Most Targeted (2023–2024)

Recent reports say that the e-commerce industry is the most vulnerable, with 32.4% of all cyber attacks happening there. This is much higher than the banking (18.7%), healthcare (15.3%), andgovernment (12.1%) sectors. The Dimensions tool was used to do a literature survey for the years 2014 to 2024. The number of papers published about e-commerce attacks has been steadily rising, reaching its highest point in the last few years as cybercriminals have been targeting online stores more and more.

B. The Most Important Attacks on E-commerce

Backdoor attacks are the most common type of attack on e-commerce systems, happening in 68% of all cases. Malware comes in second at 56.4%, and SEO spam comes in third at 51.3%. There are signs of suspicious behaviour in 44.4% of cases. Cross-site scripting (XSS) is present in 40% of attacks, while SQL injection occurs in 38%. Phishing attacks account for 25% of all attacks, and distributed denial-of-service (DDoS) attacks account for 18%. These numbers show how important it is for e-commerce sites to have multiple layers of security.

C. Target Content Management System (CMS)

WordPress is the CMS with most attacks, present in 90% of hacked CMS sites: Joomla, Magento and Drupal follow. While SafetyEcom is a custom PHP application (notaCMS),it is still the subject of many of the common attack vectors with regards to SQL injection andXSS.

III. METHODOLOGY OF SAFETYECOM

SafetyEcom was built using the Incremental Model, which supports iterative delivery of functionality. The first increment was user registration login and product browsing. The shopping cart feature along with purchasing an order was incorporated into the website at the second stage. Admin panel for Product and Order Management included in the website at the third stage The reporting system, wish list, and ratings were added at the final stage.

A. Tools and Environment

Programming Languages used for front-end PHP, HTML, CSS, jQuery Database Used MySQL 5.1.30 Webserver Used XAMPP (Apache) Operating Systems Supported Windows 7, Windows 8, Windows 10, Windows 11 Web Browsers Supported Chrome, Firefox, Edge, Opera

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

B. Features of PHP Used

The framework uses an object-oriented programming model, externally maintained HTML files, which provide flexibility in UI, externally configurable JSON files, customizable error messages, built-in security and access control features, and portable directory architecture.

C. Features of MySQL Used

MySQL is a relational database system based on a client/server architecture that supports SQL, as well as views and stored procedures (though only within the bounds of limited triggers), and also integrates support for Unicode and replication features suited to backup and scaling.

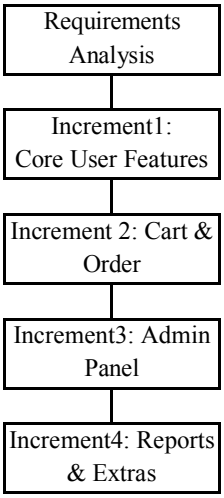


Fig.1.Incremental Model applied to SafetyEcom

IV. WORKING AND SYSTEM DESIGN

A. Actors and Functionalities

Three actors interact with SafetyEcom. Here, the Admin can login to Dashboard, Add/Come up with Categories and Products, Manage Orders, view Reports, Generate Invoices & Log Out. It will allow Customer to register, log in, profile management and display of products and able to add a item into cart as well as wish list, product rating, Order Placing, Invoice View and Log out. A Visitor can browse the website, and see products and look for products without logging in.

B. Data flow Diagram (Level 0)

In the context-level DFD, we see that the system as a whole is displayed in one single process interacting with external two entities that are Admin, Customer, and Visitor. Data flows include login credintials, product details, orders,report.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

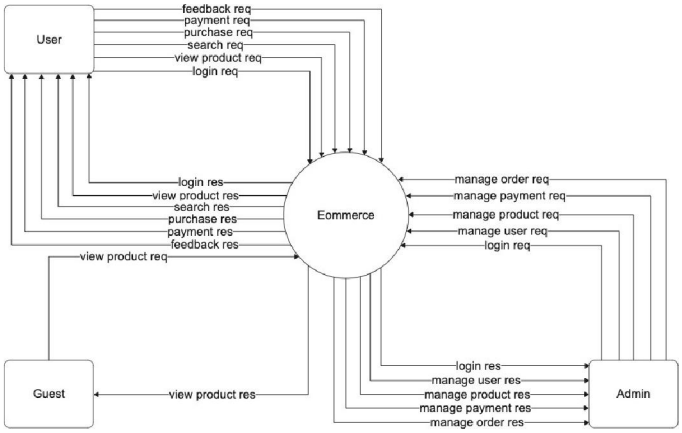


Fig.2.Level0 DFD of SafetyEcom

C. ER Diagram

Entities on ER diagram: Admin, Customer (potentially a member), Cate- gory, Product, Variant (attributes of Products), Option (types of Variants too), Cart, Wishlist for Customers can be represented from an item's detail page itself, Rating given by Customers can also be recorded in the app along with Order and Order Detail. Use Relationships to define that a customer can have multiple orders, tell that a product belongs exactly one category, and associate that products can have different variants and images.

D. The design of the (Selected Tables) Database

Your database contains multiple tables. tbl_admin_login (primary key auto-increment loginid, username VARCHAR 50, password VARCHAR 255 hashed) tbl_category: categoryid (PK), parentcategoryid (FK for subcategories), categoryname- VARCHAR 100 studio_db:Database name and contains the following tables tbl_product-info of products, productid (PK), categoryid (FK), productname(VARCHAR 200) price(DECIMAL 10,2) and description(TEXT). Create Table tbl_order (orderid (PK),custid (FK),orderdate(DATETIME) orderstatus(VARCHAR 50),totalamount)(DECIMAL 10,2)

V. TESTING AND SECURITY MEASURES

A. Testing Types Applied

Several testing strategies were employed. Functional testing checks the log in, registration, cart and order workflows. Load handling and response times were tested for usability. Performance Testing: Performance testing was the testing of system behaviour with concurrent users. Technical aspects: SQL injection, XSS, and authentication bypass were attempted during security testing. Compatibility testing ensured proper functioning on various browsers and operating systems.

B. Test Case Sample — Login

This is one example of a test case for the login module; it consists of four steps, namely: Step 1 - Navigate to the login page, which displays the login form Step 2 - Provide correct user credentials; this redirects you to the dashboard. Step 3 - Provide incorrect user credentials; displays error message.

C. Security Measures Undertaken

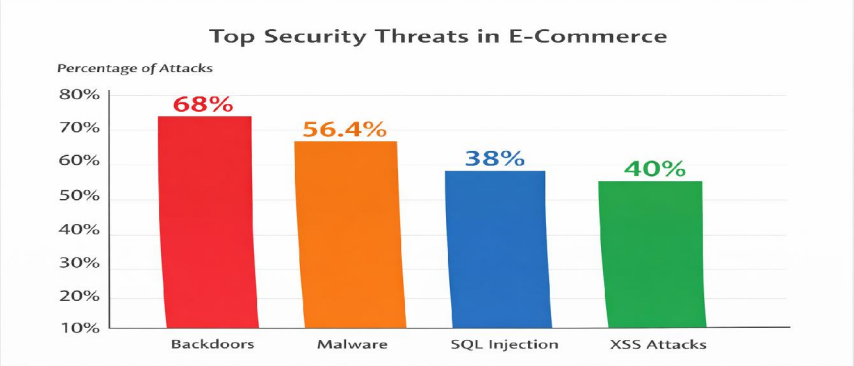
The safetyEcom consists of five main layers of security:
(1) Data between the browser and the server is encrypted using HTTPS with SSL;

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

(2) admin login secure with password hash (MD5/SHA);
(3) SQL Injection and XSS protection through input validation;
(4) session management to prevent unauthorized access;(5) database encryption for sensitive customer data.

VI. RESEARCH GAP

From the comprehensive literature review and data analysis of SafetyEcom, the research gaps are as follows:
• G1: Little research on security by institutional e-commerce platforms for safety devices. Most of these existing studies relate to generalised e-commerce or large marketplaces.
• G2: There are no studies in the academic literature supporting security threat modeling for specialized product categories (helmets, masks, protective gear).
G3: SQL injection and XSS attacks on custom PHP e-commerce sites are still under-researched (especially for small to medium scale projects).
• G4: There is a lack of standardized security framework for small-scale safety equipment e-commerce systems.
These gaps could be filled to make even the most specific e-commerce platforms more powerful.



Top Security Threats in E-Commerce Systems (2014–2024)

VII. CONCLUSION

E-commerce helps in linking the sellers to the buyers; however, it still faces the issue of security. The main focus of this paper will be on SafetyEcom, an e-commerce website. SafetyEcom has been developed in PHP and MySQL in accordance with the Incremental Model, and it performs all the functionalities of an online store perfectly.
Furthermore, according to this research, e-commerce faces the highest number of attacks (32.4%). Backdoors account for 68%, while malware is the second most common threat (56.4%). Input validation, secure session handling, and HTTPS play a significant role in preventing SQL injection and XSS attacks on custom PHP websites such as SafetyEcom.
The tests performed show that all the requirements of functionality, usability, and security have been fulfilled by the system. In addition, it can be concluded from the research that there is still a need for security-oriented research in the area of smaller or unique e-commerce applications.

VIII. FUTURE SCOPE

We also intend to make certain changes in the existing system SafetyEcom. In terms of payments, the user will get a number of additional options, such as PayPal, Razorpay, UPI and even credit cards. To ensure safety of sensitive data, AES-256 encryption will be applied. The admin panel will be optimized by including graphs and charts to track down sales statistics. 2FA login option will be implemented for both customers and admins, ensuring a higher level of security. Mobile versions of the app will be developed for both Android and iOS devices. To identify possible

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

fraudulent transactions earlier, artificial intelligence system will monitor the order status in real-time mode. Finally, the database backup will be carried out on a daily basis in the cloud environment.

REFERENCES

[1]. J. R. Gordon and S. R. Gordon, Information Systems: A Management Approach. The Dryden Press, 1999.
[2]. Y. Jing, "Online payment and security of E-commerce," in Proc. WISA, 2009, p. 46.
[3]. S. Badotra et al., "Security analysis of E-commerce systems," Int. J. Appl. Sci. Eng., vol. 18, no. 2, pp. 1–19, 2021.
[4]. Sucuri Inc., "Website Threat Research Report," 2024.
[5]. ZDNET, "WordPress accounted for 90% of all hacked CMS sites," 2024.
[6]. Dimensions.ai, "Publication data on e-commerce attacks," 2024.
[7]. Imperva, "Cross-site scripting (XSS) attacks," 2024.
[8]. Kaspersky Lab, "DDoS attacks and e-commerce security," 2024.
[9]. Gupta, R. (2024). Cybersecurity threats in e-commerce: Trends and mitigation strategies. Journal of Advanced Management Studies.
[10]. Badotra, S., & Sundas, A. (2021). A systematic review on the security of e-commerce systems. International Journal of Applied Science and Engineering.
[11]. Desamsetti, H. (2021). Crime and cybersecurity as an advanced persistent threat: A constant e-commerce challenge. American Journal of Trade and Policy.
[12]. D'Adamo, I., González Sánchez, R., Medina Salgado, M. S., &Settembre-Blundo, D. (2021). E-commerce calls for cyber-security and sustainability: How European citizens look for a trusted online environment. Sustainability.
[13]. Zhang, Y., & Liu, H. (2024). Cross-site scripting defence for PHP-based online stores: An empirical evaluation of output encoding techniques. Journal of Information Security and Applications.
[14]. Yadav, A., & Singh, V. (2023). A comparative analysis of malware attacks on content management systems vs. custom e-commerce applications. International Journal of Cyber Security and Digital Forensics.
[15]. Smith, T. A., & Jones, L. M. (2024). HTTPS implementation and SSL/TLS security in custom PHP e-commerce applications. Journal of Web Engineering.