International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 6, Nov-Dec-2026, ISSN (Online): 2395-566X

A Study of Security Challenges and Prevention Techniques in Online Shopping Websites

Harsh Sudhakar Shardul[1] Dr. Deepak Singh[2]
M.Sc. Computer Science
Savitribai phule pune university (sppu)

Abstract- Suryadatta College of Management Information Research & Technology, Pune, India Research Guide: Asst. Prof. Vaishnavi Punalkar Online shopping websites have knowledge about the customer, their account details, delivery information, payment related data. When these systems are not adequately protected, users can be exposed to risks such as attacks on the database, malicious script, account compromise, payment misuse and privacy loss. This paper looks at 5 different security issues (SQL Injection, Cross-Site Scripting (XSS), weak authentication, payment security and customer data privacy) and reviews the common methods for preventing each of them. The questionnaire was administered to 18 respondents, in addition to reading through the published guidance. Eleven of respondents (61.1%) reported knowing about the security risks of online shopping, and 12 (66.7%) reported observing a suspicious or fake shopping website. Theft of payment information was the top answer for the primary concern (5 respondents, 27.8%). Strong authentication and secure database protection were tied for the most selected security measures with 5 (27.8%) each. Findings indicate that respondents are aware of the following risks, but there is no consistency in awareness and security-checking behaviours. The sample is small and convenience, so results only apply to the sample and not the general population.

Keyword: E-commerce security, online shopping, SQL Injection, Cross-Site Scripting, authentication, payment security, data privacy.

I. INTRODUCTION

Online shopping has revolutionized the way people search for and shop products. Customers can compare prices, order and pay online, without having to go to a physical store. Shopping sites collect all of these details to offer these services, including personal information, account details, order history, and payment data. It is because security is an important aspect of the online shopping experience. Security issues can impact customers and businesses alike. There may be a database flaw that allows records to be exposed; unsafe content management can result in scripts being executed in the visitor's browser; insecure username/password controls can allow misuse of the accounts; and weak payment or privacy policies can lead to disclosure of sensitive information.OWASP's web application risk guidance features topics like injection, authentication failures, cryptographic failures and access-control weaknesses that are important topics for developers to consider [1]. This paper explores five security issues and recommended solutions to prevent such issues in web applications. It also details an exploratory research carried out with 18 people to gain insights into their awareness, experiences and attitudes towards the security of online shopping.

1. Research Problem And Question

There is a difference in the technical resources and security measures of online shopping platforms. Users might not know how to recognize an unsafe website; operators of websites have to ensure that databases, accounts, payment flows and information on the hands of customers are protected. The research problem is to grasp these five areas as a whole, and to analyze those safeguards that can apply to an ordinary ecommerce website. The goals are: (1) to identify 5 common security challenges, (2) to describe how they might impact customers and businesses, (3) to discuss measures that can be taken to prevent these challenges, (4) to analyze the opinions of consumers based on a brief survey, and (5) to recommend best practices for preventing security issues in e-commerce development and operation. 2III.

II. LITERATURE REVIEW

1. E-commerce security threats:
Liu et al. examine cyber threats that can impact e-commerce, and highlight that e-commerce has a variety of threats such as system attacks and customer information attacks [2]. This helps to view security as technical controls and organisation.

2. Privacy in online transactions:
Bandara, Fernando and Akter discuss privacy issues in e-commerce and describe it as an area for future research [3]. Their work is relevant because customers have to share

© 2026 IJSRET

information when they shop online and it's important that this is done clearly — otherwise it could impact trust in the customer.

3. Concerns about customer privacy:
Maseeh et al. use a multilevel meta-analysis to study privacy concerns in e-commerce [4]. Their work will serve as a research foundation for analysing the perception of consumers regarding the collection and management of information about them.

4. Web application security guidance:
The Top 10 and Application Security Verification Standard are structured guidelines for recognising and verifying common web application risks from the OWASP community [1, 5]. Secure coding principles like parameterized queries and context-appropriate output encoding are covered in the SQL Injection cheat sheet and XSS prevention cheat sheet [6], [7]. D. Information and data security.

5. Authentication, payments and data protection:
The Digital Identity Guidelines from NIST address requirements and recommendations for authentication and authenticator management [8].

PCI DSS sets a minimum level of technical and operational standards for organizations that store, process or transmit payment account data [9]. The Digital Personal Data Protection Act, 2023 [10] is the act that spells out the legal aspects of processing digital personal data in India. Research gap and contribution. The above resources discuss Web security, privacy, identity and payment protection in various ways. We've compiled five pertinent risks in this paper and included a small exploratory consumer awareness and preference survey. The survey is not meant to establish the effectiveness of the techniques; it documents what the survey takers say about the techniques.

6. Research Methodology
In the study, a descriptive study was employed, which is based on secondary sources and voluntary online questionnaires. This survey was distributed via Google Forms. This analysis is based on 18 completed response sheets, which were exported to come up with the results. No names or contact information are reported in this paper. The questionnaire included the following questions: respondent's profile, frequency of shopping, and awareness of security issues, experience with suspicious websites, views on five security statements, most important security issue, and preferred security protection measures and recommendations. Calculations of counts and percentages were based on denominator 18. If more than one answer may be given in a question, the percentages may exceed 100% and the question is not treated as mutually exclusive. The sample seems to have been a convenience sample, and over-representative of students and those aged 18-25. Therefore, the findings should not be assumed to be representative estimates of all online shoppers and are exploratory in nature. The study did not perform penetration tests or measure the technical performance of the security controls at the websites and did not inspect the websites.

7. Five Security Challenges And Prevention

- **SQL Injection**. is one of the five security challenges and prevention. One of the common ways SQL Injection can happen is if untrusted input is treated as an unsanitized input in a database query. May reveal or change information in a database. Parameterized queries or prepared statements, least-privilege database accounts and appropriate input validation are recommended safeguards [6].
- **Cross Site Scripting (XSS).** XSS is what happens when untrusted content is mishandled so that the browser willtreat it as executable script. This risk can be mitigated by context appropriate output encoding, safe handling of user generated content and using a suitable Content Security Policy [7].
- **Weak authentication**. If the password is reused or is not sufficiently strong, access to the account may bepossible. Websites should use an appropriate password-hashing scheme to store passwords, protect sessions, not have too many attempts to login automatically and provide multi-factor authentication when applicable. There is detailed guidance on authentication and authentication provider management from NIST [8].
- **Payment security**. Payment card data should not be unnecessarily handled or stored on shopping websites.Reduce exposure by trusted payment service providers, secure transport via existing TLS, careful integration and compliance for applicable PCI DSS requirements [9, 11]. A payment gateway isn't a replacement for securing the site and integration.
- **Privacy of customer information.** Websites must gather only data required for an explicit purpose, limit access,secure stored and transmitted data and inform users about the data practices of a website. Any organisation conducting business in India must keep the requirement under the Digital Personal Data Protection Act, 2023 and its rules, in mind [10].

III. ANALYSIS AND RESULTS

There were 18 responses provided in the provided Google Forms export. The largest age group was 21–25 years (10 respondents, 55.6%), followed by 18–20 years (7, 38.9%). One respondent (5.6%) was aged 26–35. Private employees,

© 2026 IJSRET

self-employed/business and government employee respondents accounted for two (11.1%) and one (5.6%) of respondents, respectively, while 13 (72.2%) identified as students.VI. There were 18 entries in the provided Google Forms export. The largest age group was 21–25 years (10 respondents, 55.6%), followed by 18–

years (7, 38.9%). One respondent (5.6%) was aged 26–35. Of the thirteen students, two (11.1%) were self-employed/business and two (11.1%) were private employees, and one (5.6%) was government employee.

Shopping frequency varied. Five respondents (27.8%) shopped once or twice a week, four (22.2%) daily, four (22.2%) occasionally, three

(16.7%) once or twice a month and two (11.1%) rarely. Therefore, half of the sample indicated that they had shopped at least once weekly (9/18, 50.0%)

Table 1. Respondent profile.

Characteristic	Category	Count	Percent
Age	18–20	6	33.3%
Age	21–25	11	61.1%
Age	26–35	1	5.6%
Occupation	Student	13	72.2%

Occupation Private Employee 2 11.1%

Occupation	Business / Self-employed	2	11.1%
Occupation	Government employee	1	5.6%

Source: supplied survey response export (n = 18).

1. Awareness And Reported Security Concerns:

Eleven (61.1%) respondents indicated they were aware of security risks with websites to shop online. Five (27.8%) said no and two (11.1%) responded somewhat. This is a sign that some of this small group was aware, but over one third did not choose an unqualified yes.

Sixty-six.7% of the respondents reported detecting a fraudulent or deceptive e-commerce site. Three (16.7%) said no and three (16.7%) were not sure. This question does not imply that respondents experienced an actual cyberattack but rather whether they observed a suspicious site. Five (27.8%) respondents chose payment information theft as the most concerning security issue. Four respondents (22.2%) chose Cross-Site Scripting and customer data privacy, respectively. Three (16.7%) chose to use weak passwords/account access and two (11.1%) chose to use SQL Injection.

The distribution shows that the payment and privacy concerns are dominant in the participants' opinions. Respondents were asked to agree, disagree or be neutral about five statements, however, the low number of SQL Injection should not be viewed as less technically dangerous, since the respondents might be less familiar with the term.

Table 2. Awareness and observation of suspicious websites.

Survey item	Response	Count	Percent
Aware of security risks	Yes	11	61.1%
Aware of security risks	No	5	27.8%
Aware of security risks	Somewhat	2	11.1%
Noticed suspicious website	Yes	12	66.7%
Noticed suspicious website	No	3	16.7%
Noticed suspicious website	Not sure	3	16.7%

Source: supplied survey response export (n = 18).

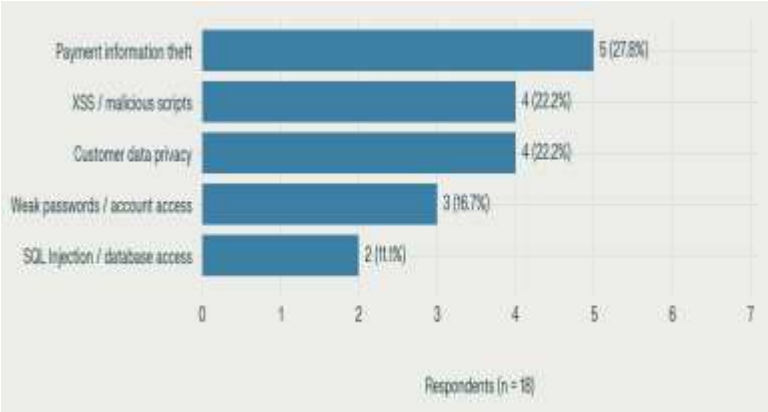

Figure 1. Greatest security concern.

2.Opinions And Preferred Protection Measures:

Eleven respondents agreed with the SQL Injection statement (61.1%) and seven were neutral (38.9%) with none disagreeing. For the XSS statement, seven agreed (38.9%) and 11 were neutral (61.1%). As for strong password and extra verification, eight agreed, six were neutral and four disagreed (44.4%, 33.3%, 22.2%, respectively). Eight (44.4%) agreed that it was important to protect payment information, eight (44.4%) were neutral and two (11.1%) disagreed. For concerns regarding the collection and use of

© 2026 IJSRET

personal information, nine agreed (50.0%), six were neutral (33.3%) and three disagreed (16.7%). There were some neutral answers especially for XSS, indicating that some of the technical terms may not be familiar for respondents.Strong authentication and secure database protection were tied, both receiving five responses (27.8%) when requested which of the following types of protection was most important. Three responses (16.7%) were from trusted payment gateways, and HTTPS received three (16.7%). HTTPS and trusted payment gateways were the second most popular answers, with two each (11.1%).

In addition to HTTPS (16.7%) and trusted payment gateways (16.7%), 11.1% of the respondents answered encryption and privacy protection.

Table 3. Opinions on five security statements, count (%).

Statement topic	Agree	Neutral	Disagree
SQL Injection	11 (61.1%)	7 (38.9%)	0 (0.0%)
XSS	7 (38.9%)	11 (61.1%)	0 (0.0%)
Strong passwords / verification	8 (44.4%)	6 (33.3%)	4 (22.2%)
Payment information protection	8 (44.4%)	8 (44.4%)	2 (11.1%)
Personal information privacy	9 (50.0%)	6 (33.3%)	3 (16.7%)

Source: supplied survey response export (n = 18).

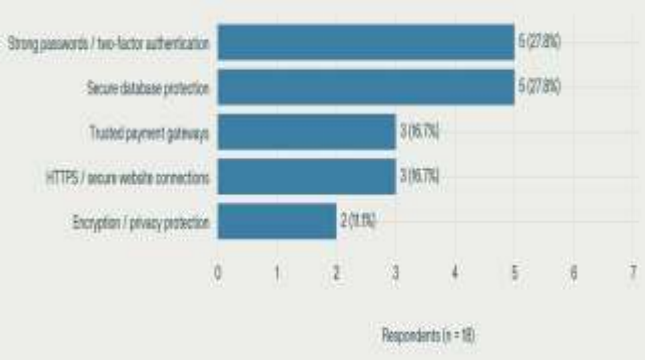

Figure 2. Most important security measure.

3. **Additional Findings And Discussion:**

Seven respondents (38.9%) always checked if a site was secure before putting payment information in the box, eight (44.4%) sometimes, and three (16.7%) rarely. None of the respondents chose never. While this is promising, the large number of sometimes suggests that security processes might not be routine. Five of the respondents (50.0%) responded that online shopping companies ought to offer more information on their security practices, 6 respondents (33.3%) said maybe, and 3 (16.7%) said no. This illustrates the importance of transparent communication about privacy and security and demonstrates some uncertainty on the part of participants.

1. Open-ended feedback. Answering the optional suggestion question revealed some fairly brief responses and a range of different ideas. These ranged from “verification” to “check the database related issue” to a comment on fake or defective products. A few entries were left empty or unfinished to be interpreted. These comments are valuable as suggestions one by one, but are not sufficient to form a thread that can be identified by all online shoppers.

2. Interpretation. According to the survey, the participants are aware of the issues of payment theft, XSS, privacy and account security. However, the neutral responses for technical statements and poor checking habits suggest a degree of awareness deficit. The outcome also indicates that website operators should provide information to the ordinary customer in a language that they can comprehend about measures taken to safeguard data. Technical controls should be put in place from a development point of view, even if customers are not aware of the names of the underlying attacks.

Table 4. Payment-stage checks and security communication.

Survey item	Response	Count	Percent
Checks before entering payment details	Always	7	38.9%
Checks before entering payment details	Sometimes	8	44.4%
Checks before entering payment details	Rarely	3	16.7%
Checks before entering payment details	Never	0	0.0%
Companies should provide more information	Yes	9	50.0%
Companies should provide more information	Maybe	6	33.3%
Companies should provide more information	No	3	16.7%

Source: supplied survey response export (n = 18).

IV. CONCLUSION:

Five security issues were reviewed in online shopping websites and opinions of 18 survey takers were taken into account. Top concerns of the respondents include payment

© 2026 IJSRET

information theft, XSS, customer data privacy. The most common protective measures selected were strong authentication and secure database protection. The survey also indicated some of the respondents were not certain about the technical security issues and the safety of the websites was not always consistent. The results validate a multi-layered approach to ecommerce security. Parameterized database queries, safe output encoding, secure password storage, trusted payment integrations, and securing sessions and using suitable data-protection practices should be used by developers. Clear communication about the use of customer information should take place within businesses. Be careful to interpret the findings as a snapshot of consumers, not a general statement about consumers, as the sample is small and convenience-based.

1. Limitations And Future Scope:

The sample size of 18, students in the sample and the use of self-reported opinions are limitations; the future scope is the extension of data collection to a larger sample size to enhance the result of the study. It did not check websites or confirm reported suspicious experiences. Future studies can include a more extensive and varied sample and improve technical explanations in the questionnaire and make comparisons between age and occupation subgroups. An independent controlled technical investigation may be conducted in an intentionally vulnerable test application of security controls, with authority, to assess their implementation.

REFRENCES

1. OWASP Foundation, “OWASP Top 10: The Ten Most Critical Web Application Security Risks,” 2025. Available: https://owasp.org/Top10/2025/
2. X. Liu et al., “Cyber security threats: A never-ending challenge for e-commerce,” Frontiers in Psychology, vol.13, 2022, article 927398. DOI: 10.3389/fpsyg.2022.927398.
3. R. Bandara, M. Fernando, and S. Akter, “Privacy concerns in E-commerce: A taxonomy and a future researchagenda,” Electronic Markets, vol. 30, pp. 629–647, 2020. DOI: 10.1007/s12525-019-00375-6.
4. H. I. Maseeh et al., “Privacy concerns in e-commerce: A multilevel meta-analysis,” Psychology & Marketing, vol.38, no. 10, pp. 1779– 1798, 2021. DOI: 10.1002/mar.21493.
5. OWASP Foundation, “Application Security Verification Standard (ASVS),” project documentation. Available: https://owasp.org/wwwproject-application-security-verification-standard/
6. OWASP Foundation, “SQL Injection Prevention Cheat Sheet.” Available: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
7. OWASP Foundation, “Cross Site Scripting Prevention Cheat Sheet.” Available: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
8. D. Temoshok et al., “Digital Identity Guidelines: Authentication and Authenticator Management,” NIST SpecialPublication 800-63B-4, 2025. DOI: 10.6028/NIST.SP.800-63b-4.
9. PCI Security Standards Council, “Payment Card Industry Data Security Standard: Requirements and Testing Procedures,” version 4.0.1, 2024. Available: https://www.pcisecuritystandards.org/document_library/
10. Government of India, “The Digital Personal Data Protection Act, 2023,” Act No. 22 of 2023. Available: https://www.indiacode.nic.in/
11. E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, Internet Engineering TaskForce, 2018. DOI:10.17487/RFC8446.
12. National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP29, 2024. DOI:10.6028/NIST.CSWP.29.

© 2026 IJSRET