International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Dynamic Threats in E-Commerce

Prof. Mugdha Dharmadhikari
Assistant Professor, PES Modern ,College of Engineering, Pune – 411005 Maharashtra, India

Ameya Shingane
SY MCA
PES Modern College of Engineering
Pune – 411005 Maharashtra, India

Abstract:

As the e-commerce sector continues to expand, the intricate and interconnected nature of online transactions presents numerous security hurdles. E-commerce involves the online transaction of goods and services between businesses and consumers. The frequency of online transactions within e-commerce is on the rise, accompanied by a surge in various forms of security breaches targeting e-commerce systems. This trend exposes consumers to potential risks of compromising their personal data, often due to a lack of awareness regarding the security measures involved in online transactions. Safeguarding the internet environment for conducting online purchases and sales is of paramount importance. Adversaries exploit vulnerabilities within the components of e-commerce systems to perpetrate attacks. Thus, there is a pressing need for proactive and adaptable security approaches that harness advanced technologies, including machine learning, alongside real-time monitoring capabilities, to identify and address emerging threats. In summary, this summary acts as a preliminary exploration paving the way for an in-depth examination into the evolving threats confronting e-commerce. The aim is to furnish valuable insights into effective countermeasures and strategies for mitigating risks. Given the ongoing evolution of the digital landscape, comprehending and mitigating dynamic threats is essential for ensuring the sustainable advancement of e-commerce platforms.

Introduction:

E-commerce serves as a crucial driver of industrial advancement, offering a streamlined, user-friendly, and expeditious avenue for business operations. Nevertheless, the expansion of online transactions brings about a corresponding increase in the risks posed to the security of e-commerce systems. These threats compromise system integrity, potentially leading to breaches that endanger consumer privacy. Consumers, often unaware of the security risks associated with online transactions, face the potential loss of personal information. Hence, ensuring the safety of internet transactions is imperative for the sustainable growth of online commerce.

Security stands as a cornerstone in any information technology system, demanding vigilant attention. Ignoring security requirements not only creates operational risks for users but also undermines customer trust. Hardware, software, and data are chief elements necessitating protection within any organization. Security principles encompass confidentiality, ensuring data access only by authorized personnel; integrity, maintaining data integrity and authorized access; and availability, ensuring data accessibility in the required format when needed.

For organizations engaged in e-commerce, additional security concerns emerge. Non-repudiation ensures that participants cannot deny their online actions, while authenticity verifies the identity of participants. Privacy safeguards control the usage of private information exchanged during online transactions. Security measures aim to shield businesses from catastrophic data loss, preserving both internal operations and external services. Organizations face the challenge of balancing the expenses associated with implementing security measures against the potential repercussions on

customer trust and the reputation of the company should a security breach occur.

1. Literature review:

Suh and Han emphasize the growing public apprehension regarding internet and e-commerce security due to prominent cases of major security breaches. [1]

According to Ray and Ray, a fair exchange protocol is essential in e-commerce to guarantee equitable transactions, ensuring no party can exploit the system through misconduct or premature termination of the protocol.[2]

Faisal Nabi emphasizes the critical role of secure software and maintaining server-side security and privacy also. It suggesting the consideration of proprietary encryption algorithms over public ones to mitigate potential vulnerabilities and flaws. [3]

Eliza Mik addresses mistaken identity as a pertinent issue in e-commerce transactions [4] proposing biometric authentication methods such as fingerprints, iris scans, and facial recognition to prevent identity fraud in remote authentication processes.

Ashraf Sarah Kazi and Bharat Saraf both point out that e-commerce, particularly cases involving third-state defendants, is excluded from the jurisdiction of the Brussels I regulation.[5]

Roger Clarke and Dan Svantesson provide an intricate framework for e-commerce transactions. They advise against inundating consumers with overly complex transaction process descriptions and stress the significance of comprehending the practical functioning of the model.[6]

Malicious individuals could potentially exploit time-of-check to time-of-use attacks by altering prices in URLs, leading to adverse effects on organizations' revenues. [7]

2. Methodology

2.1 Threats to security

E-commerce security systems face both accidental and malicious threats, which can be mitigated through control measures and procedures to safeguard websites and minimize vulnerabilities. Malicious threats include hackers manipulating sensitive information, burglars stealing unprotected data, and imposters posing as legitimate users. Additionally, threats may arise from fake websites, malicious emails containing hidden components, and unauthorized data transmission to third parties. Determining the full scope of threats can be difficult, as attacks from authenticated users are often more prevalent than those originating from unidentified sources or hackers.

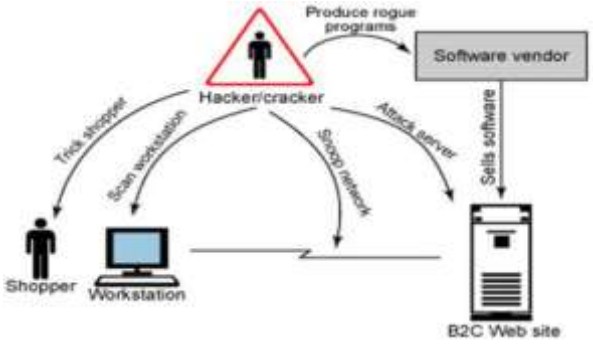
Web browsers, utilized by online consumers for transactions, introduce risks to privacy and security , particularly when visiting unfamiliar or untrusted links. Uploading or downloading files can also create vulnerabilities in secure systems. Cookies, used to maintain state between web connections, pose privacy risks by allowing web servers to track browsing habits without user consent. ActiveX controls on webpages can further compromise security by downloading system information and transmitting it to servers without authorization.

E-commerce security faces a multitude of additional threats, including unauthorized access, malicious code, and financial fraud such as credit card fraud and denial-of-service attacks. To address these threats, it's crucial to identify potential security vulnerabilities, assess hackers' expertise and efforts, and analyze available hacking tools and resources. This analysis can inform security enhancements and standards to bolster e-commerce security measures effectively.

3.2 Security Threats

In the realm of E-Commerce, vulnerabilities primarily reside at the system's entry and exit points, presenting opportunities for attackers to exploit. Encompassing the Shopper, the Shopper's

device, the network link connecting the shopper and the server of the website, and the software provider, among other aspects. The diagram in Figure 1 depicts the potential targets that attackers might target. Attackers or hackers can employ various methods of security breaches.



I. Deceiving the Shopper

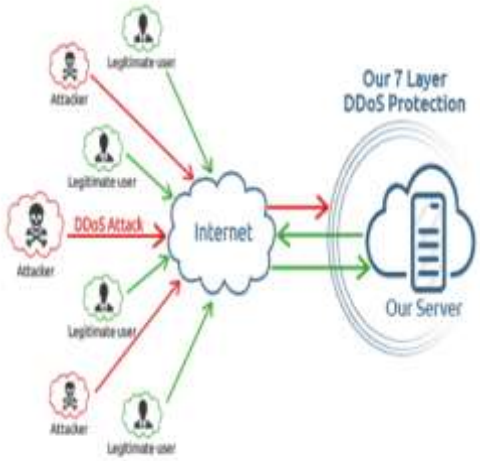
Certain highly lucrative attacks, while seemingly simple, hinge on deceiving the shopper, a tactic referred to as social engineering techniques. These approaches entail observing the shopper's actions to gather exploitable information. For example, one commonly used tactic involves posing challenge questions, such as inquiring about the mother's maiden name on various websites. If a site inadvertently discloses a password upon answering the challenge question, not only is that site compromised, but there's also a likelihood that the shopper employs the same login credentials elsewhere.

In a common scenario, the assailant makes contact with the shopper, pretending to be a representative from a previously visited website, and solicits personal information. Following this, the assailant poses as the shopper and furnishes these details to a customer service representative at the website, asking for a password reset to a pre-determined value.

Another widespread type of social engineering attack involves phishing schemes. Hackers leverage the names of well-known websites to collect login and registration credentials. A shopper might inadvertently land on a fraudulent site because of a typing mistake and inadvertently reveal sensitive information. Alternatively, the attacker dispatches forged emails that appear to originate from trustworthy sources.

Clicking on the links within these emails redirects the shopper to counterfeit sites designed to collect their confidential information.

II. The Distributed Denial of Service (DDoS)



A denial-of-service attack (DoS attack) refers to a security breach wherein the attacker performs actions aimed at preventing legitimate users from accessing electronic devices. This type of attack makes a network resource unavailable to its intended users by temporarily interrupting the services of an Internet-connected host.

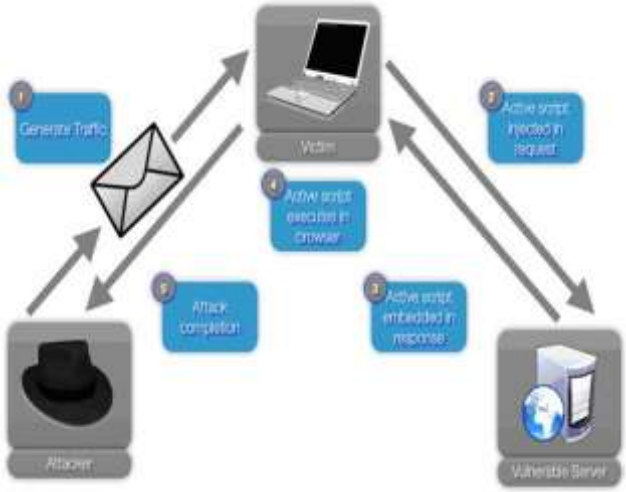
These threats represent the latest iteration of DoS attacks, and their effectiveness hinges on intermediate sites' incapacity to detect, contain, and eliminate the intrusion into their networks. This assault not only poses challenges to the target site but also induces congestion across the entire Internet, as a multitude of packets are routed through diverse paths towards the target.

In this type of attack, the hacker infects computers on the Internet using a virus or similar methods. Subsequently, these compromised computers are manipulated by the hacker. At a predetermined time, the hacker orchestrates them to inundate the target server with frivolous yet resource-intensive requests. Consequently, this attack disrupts not only the target site but also the broader Internet, as

numerous packets traverse varied routes to reach the target.

III. Cross-site script (XSS)

Information flows into a web application from an untrusted origin, typically through a web request. This data is incorporated into dynamic content that is then transmitted to a web user without undergoing validation for potentially harmful content.



There are several types of XSS attacks, including:

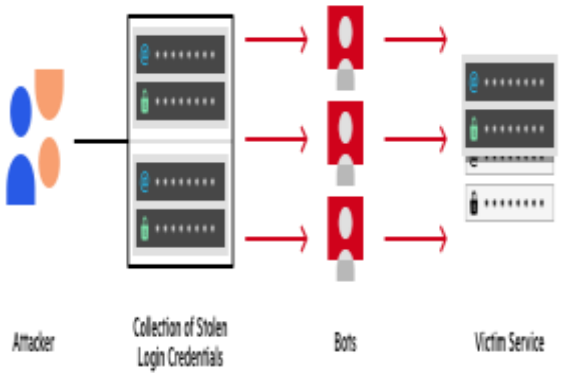
- Reflected XSS: This type of attack happens when a harmful script is inserted into a web page's URL or form input, and then reflected back to the user

- Stored XSS: In this scenario, the injected malicious script is stored on the server and presented to every user who accesses the susceptible page.

- DOM-based XSS: The attack takes place within the Document Object Model (DOM) of the web page, manipulating client-side scripts to execute malicious code.

Cross-site scripting (XSS) attacks present substantial threats to e-commerce platforms since they have the potential to result in the pilfering of sensitive customer data, financial losses, reputational harm, and legal ramifications. Attackers may exploit XSS vulnerabilities to redirect users to phishing pages, steal session cookies, or perform actions on behalf of authenticated users.

IV. Credential Stuffing



It is a cyber-attack technique wherein perpetrators employ automated scripts to attempt numerous combinations of pilfered usernames and passwords, acquired from data breaches or alternative sources, in order to illicitly access user accounts across diverse online platforms, including e-commerce websites.

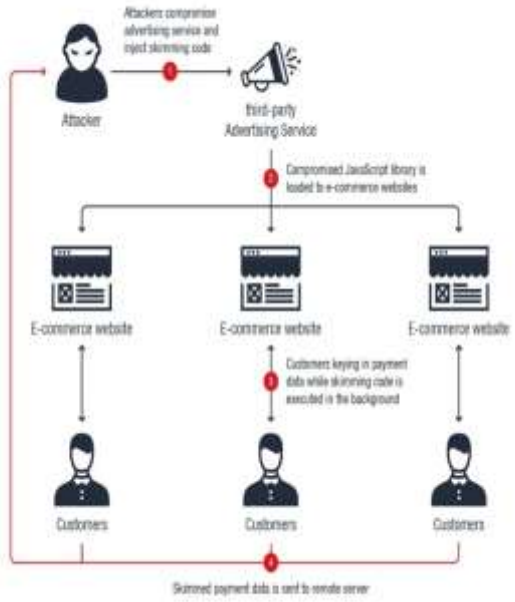
The attackers gather compilations of usernames and passwords that have been leaked from prior data breaches or sourced from the dark web. They use automated tools or scripts to systematically try these credentials across multiple websites, including e-commerce platforms. The goal is to identify accounts where users have reused the same credentials they used on other websites.

Credential stuffing attacks are increasingly common due to the widespread reuse of passwords by users across multiple online accounts- commerce websites are prime targets for credential stuffing attacks because they often store valuable user data, including payment information.

V. Magecart Attacks

Magecart is an umbrella term used to describe a collection of cybercriminal groups that specialize in stealing payment card information from e-commerce websites. These attackers typically

compromise the websites' checkout pages or payment forms by injecting malicious JavaScript code, which skims payment card details entered by users and sends them to remote servers controlled by the attackers.



- Initial Compromise: Attackers gain unauthorized access to the ecommerce website's infrastructure, often through vulnerabilities in third-party plugins or software used by the website.
- Malicious Code Injection: Attackers inject malicious JavaScript code into the website's checkout pages or payment forms
- Data skimming: It involves the insertion of code that captures payment card information provided by users during the checkout process, including expiration dates, CVV codes ,credit card numbers..
- Exfiltration: The stolen payment card data is sent to remote servers controlled by the attackers, where it can be sold on the dark web or used to conduct fraudulent transactions.

Magecart attacks primarily target e-commerce websites of all sizes, from small businesses to large enterprises. The impact of these attacks can be severe, leading to financial losses, damage to reputation, legal liabilities, and regulatory fines for failing to protect customer data.

3.3 Impact of cyber attacks

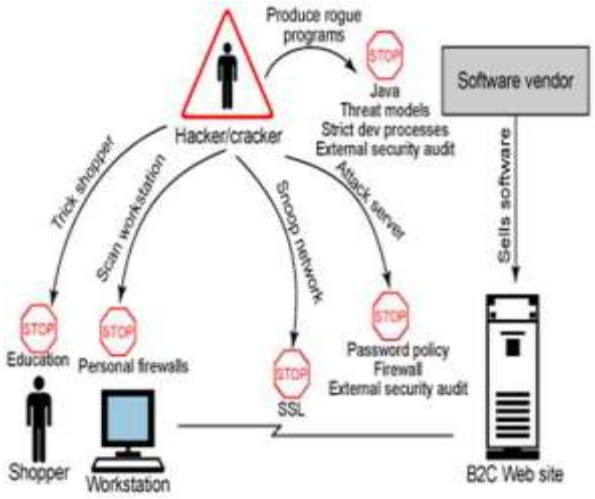
The landscape of security threats facing e-commerce systems is diverse and complex, spanning from social engineering tactics to sophisticated cyber-attacks. Social engineering techniques, such as phishing schemes and impersonation tactics, exploit human vulnerabilities to deceive shoppers and extract sensitive information. These tactics not only compromise individual accounts but also escalate the risk by potentially compromising multiple platforms where users employ the same login credentials. Credential stuffing exacerbates this risk by leveraging stolen usernames and passwords obtained from data breaches or the dark web, enabling unauthorized access to user accounts across various online platforms. The repercussions extend beyond compromised data, threatening user privacy, trust, and the integrity of e-commerce ecosystems.

Moreover, Distributed Denial of Service (DDoS) attacks pose significant challenges by disrupting the availability of e-commerce websites and causing network congestion across the internet. These attacks not only hinder access for legitimate users but also generate widespread disruptions, impacting internet infrastructure and services. Concurrently, Cross-site Script (XSS) vulnerabilities introduce avenues for injecting malicious code into web applications, potentially leading to data breaches, financial losses, and reputational harm. The exploitation of XSS vulnerabilities can result in the theft of sensitive customer information, redirect users to fraudulent websites, and compromise the integrity of e-commerce transactions.

Furthermore, the Magecart threat underscores the risks associated with payment card data breaches, posing severe financial consequences, reputational damage, and legal liabilities for affected businesses. Magecart attacks target e-commerce websites' checkout pages or payment forms, injecting malicious JavaScript code to skim payment card details entered by users. The stolen data is then exfiltrated to remote servers controlled by attackers, where it can be exploited for fraudulent activities or

sold on the dark web. Mitigating these threats necessitates robust security measures, proactive monitoring, and continuous adaptation to evolving cyber threats to safeguard e-commerce ecosystems and preserve user trust and privacy.

4. Cybersecurity Measures for E-Commerce



Even in the face of hackers and cybercriminals, e-commerce continues to be a secure and trustworthy endeavor. Large e-commerce corporations possess substantial resources at their disposal, enabling them to deploy extensive measures to safeguard their customers. They are committed to exploring all legal avenues to ensure the protection of their clientele.

4.1 User Education and Awareness

The security of a system hinges greatly on the actions of its users. Should a customer opt for a feeble password or fail to safeguard its confidentiality, it opens the door for potential impersonation by malicious actors. The stakes escalate if such a compromised password pertains to an administrator, as it could grant access to sensitive areas of the system. In such scenarios, additional layers of physical security are often in place, given that administrator clients are typically shielded behind firewalls. It is imperative for users to exercise discernment when divulging information and to remain vigilant against phishing tactics and other forms of social engineering manipulation through proper education. Implementing educational programs to inform shoppers about common tactics used by attackers, such as phishing schemes and social engineering. This can help users recognize suspicious activity and avoid falling victim to scams.

4.2 Multi Factor Authentication (MFA)

It improves security by requiring users to provide multiple forms of verification before accessing their accounts. Usually, this involves a combination of something they know (such as a password) and something they have (such as a code sent to their mobile device). Even if malicious actors obtain login credentials, they will be unable to access the account without the additional authentication factor.

Types of MFA:

- Two-factor authentication (2FA): It is the most common type of MFA, requiring users to provide two different forms of verification. This usually involves entering a password and then inputting a code sent to their mobile phone.

- Three-factor authentication (3FA): It elevates security measures by necessitating the provision of three disparate types of verification, thereby adding an extra layer of protection compared to 2FA.

- Adaptive authentication: Introduces a dynamic approach to authentication, adjusting the verification requisites based on risk factors such as the user's location, device, behaviour, or recent activity. For instance, When a user attempts to log in from an unfamiliar device or location, they may receive a prompt to provide additional verification.

4.3 Regular Security Audits & Updates

Regular security audits play a crucial role in pinpointing vulnerabilities within the e-commerce platform, such as outdated software or misconfigurations. By promptly applying patches and updates, businesses can fix these vulnerabilities before attackers exploit them to gain unauthorized access or launch attacks.

Types of Audits:

Internal audits, whether executed by internal security teams or third-party auditors, scrutinize the organization's security policies, procedures, and technical controls.

External Audits: External audits involve independent assessments by third-party auditors to validate the effectiveness of the organization's security measures and compliance with industry standards.

4.4 Bot Detection and Mitigation

Bots can be used by attackers for various malicious activities, including DDoS attacks and credential stuffing. Implementing bot detection and mitigation techniques helps differentiate between legitimate users and malicious bots. Techniques like CAPTCHA challenges, rate limiting, and behavioural analysis can help identify and block malicious bot traffic.

Bot Detection Techniques

- Rate Limiting involves constraining the volume of requests originating from a single IP address or user agent within a designated time interval.
- CAPTCHA Challenges: Requiring users to solve CAPTCHA challenges before accessing certain actions to distinguish humans from bots.
- Behavioural Analysis: Analysing user behaviour patterns to identify anomalies indicative of bot activity, such as rapid, repetitive actions.

Types of Mitigation Techniques:

- Blocking: Automatically blocking or restricting access for IP addresses, user agents, or behaviour patterns associated with malicious bot activity.
- Challenge-Response Mechanisms: Deploying challenge-response mechanisms, such as CAPTCHA challenges or email verification, to verify the identity of users.

5. Conclusion

The rise of online transactions has led to an increase in various attacks targeting the security of e-commerce systems. These attacks pose a significant threat to the integrity of systems, potentially leading to decreased levels of protection. Consequently, consumers are at risk of compromising their personal information. Therefore, ensuring the safety of e-commerce transactions is crucial. Security serves as a fundamental aspect of any information technology system and requires continuous monitoring. Implementing control measures and protocols can strengthen website defences and mitigate vulnerabilities. Enhancing security standards requires a thorough understanding of the sources of security threats, assessing attackers' proficiency, and examining the tools and resources they use to breach e-commerce security systems.

6. References

[1] Suh, B and Han I., 2003, “The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce”, International Journal of Electronic Commerce, Vol 7, No. 3, pp. 135-161

[2] Ray, I. & Ray, I. 2002 “Fair Exchange in E-commerce” in ACM SIGecom Exchanges Vol 3, Issue 2 Spring, pp9-17, ACM Press New York

[3] F. Nabi, "Secure business application logic for e-commerce systems," Computers & Security, vol. 24, pp. 208-217, 2005.

[4] E. Mik, "Mistaken identity, identity theft and problems of remote authentication in e-commerce," Computer Law & Security Review, vol. 28, pp. 396-402, 2012.

[5] B. Saraf and A. U. S. Kazi, "Analysing the application of Brussels I in regulating e-commerce jurisdiction in the European Union – Success, deficiencies and proposed changes," Computer Law & Security Review, vol. 29, pp. 127-143, 2013

[6] D. Svantesson and R. Clarke, "A best practice model for econsumer protection," Computer Law & Security Review, vol. 26, pp. 31-37, 2010.

[7] Gehling, B. &Stankard, D. 2005 “eCommerce Security” in Information Security Curriculum Development Conference, September 23-24 2005 pp32-38, Kenneshaw GA