Bulleted governing bodies/associated regulations:

Governing bodies:
World Trade Organisation (WTO)
United Nations Conference on Trade and Development (UNCTAD)
Organisation for Economic Cooperation and Development (OECD)

Associated regulations:

- OECD Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders 2003
- OECD Consumer Protection in E-Commerce 2016
- Europe Union Directive 2000/21/E.C.
- Data Protection Act 2018
- Payment Services Regulations 2017
- Electronic Identification and Trust Services for Electronic Transactions Regulations 2014
- Consumer Rights Act 2015
- The Consumer Contracts Regulations 2013
- Consumer Protection from Unfair Trading Regulations 2008

Our assigned website is a customer relationship management system for B2C and B2C e-commerce by Sugar CRM, an open-source platform offered as SaaS (Sugar CRM, N.D.). A CRM provides businesses with a platform to manage sales, customer service, business development, recruiting and marketing to efficiently manage external interactions and relationships to increase profitability, productivity and growth. On an international level, there is no distinct governing body; WTO does offer a forum that can facilitate the discussion for governance and regulation frameworks (World Economic Forum, 2019). The OECD and UNCTAD provide recommendations for e-commerce trading and consumer protection. The use of personal data is of particular importance. GDPR and DPA regulations must show information about personally collected data, the purpose of use, retention period, an opportunity to opt-out, and the legal basis of process data information. However, there are slight differences between B2B and B2C e-commerce (Sonovate, N.D.). B2B does not have to specifically ask for consent when processing business data and the allowance of marketing emails to business email addresses if there is a legitimate interest. Conversely, in B2C, you must ask for active consent on all data processing.

Category	Threat	D	R	E	A	D	Risk	Recommendations and potential mitigations
Financial / Payment Fraud	Clean Fraud Fraudsters study organisations' fraud-detection systems meticulously before circumventing them using stolen genuine payment information.	5	1	3	4	5	**3.6**	• Use reliable third-party payment processor such as PayPal and Stripe • Use verification services such as Address Verification System (AVS) and Card Verification Value (CVV) rules • Data encryption • Fraud detection algorithms • Awareness training
	Identity Theft Someone undertakes a fraudulent transaction in someone else's name; this is impersonation fraud.	1	3	2	3	4	**2.6**	
Misconfigurations of Web Applications	Cross-site scripting (XSS) A code injection from the client-side, malicious scripts are injected into otherwise safe and trusted websites.	5	3	4	5	5	**4.4**	• Use Web Application Firewall (WAF) • Use HTTPS and SSL/TLS certificates to secure the website • Data encrypted before storing and transferring • Validate inputs / Special characters filter • Implement Content Security Policy • Use up-to-date software • Apply Principle of Least Privilege (PoLP) • Data backup • Use HttpOnly attribute cookies • Live web vulnerability scanning • Regular patch web and application server
	SQL injection SQL queries inject malicious code via web page input.	5	3	4	5	5	**4.4**	
	Unsecured Website / Unsecured transaction Data from customers or cardholders are stored in plain text files with no encryption. The connection network packet is sent in plain text without encryption.	2	5	5	5	3	**4**	
	Cookie poisoning Modifying a cookie to get unauthorised information about a user.	2	2	4	3	3	**2.8**	
	Buffer overflows It occurs when the volume of data exceeds the memory buffer's storage capacity. As a consequence, while attempting to write data to the buffer, the program overwrites memory locations near the buffer.	4	3	3	1	2	**2.6**	
General Attacks	DoS / DDoS / Botnets An excessive number of connections, sluggish website access and Internet outage.	3	5	3	5	1	**3.4**	• Use WAF • Use Content Delivery Network (CDN) • Use Next Generation Firewall (NGFW) • Use Security Information and Event Management (SIEM) • Use antimalware software • Apply Domain-Based Message Authentication, Reporting & Conformance (DMARC) policy • Spam filtering • External email warning tag • Awareness training • Complexity password requirements • Limit login attempts • Use Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHAs) • Use Multi-factor Authentication (MFA)
	Spam / Phishing Attack Spam is any unwanted, unsolicited digital message transmitted in large volumes. Phishing is a deceptive technique of sending communications that appear to come from trustworthy organisations to get personal information.	1	5	4	4	2	**3.2**	
	Brute Force Attack With trial-and-error, guessing login details, encryption keys, or discovering hidden web pages. Try all conceivable combinations in the hopes of the right guess.	1	5	2	3	1	**2.4**	
System Misconfigurations	Software backdoor / Vulnerability / EoL The security risk of the system that can exploit by hackers.	5	3	5	4	4	**4.2**	• Use up-to-date software • Regular patch web and application server • Use WAF • Live system vulnerability Scanning • Zero Trust networks • Apply PoLP • Delete any inactive or unnecessary access • All sensitive data should be encrypted • Adopting privileged password management • Use MFA
	Unrestricted Access The ability to use or access the Service with an inappropriate role.	5	2	4	3	5	**3.8**	
	Weak Authentication or Authorisation Allow an attacker to execute the functionality in the program or backend server anonymously.	5	2	3	3	2	**3**	

Recommendations for an e-commerce website:

1. Use a reliable payment processor such as PayPal and Stripe to separate credit cards and payments transactions from the website database.
2. Using cloud service which provided WAF, CDN or SIEM solutions to prevent malicious code injection and DoS attack.
3. Using HTTPS and TLS/SSL to ensure that personal data and transactions are encrypted before transferring them between the customer device and e-commerce website will help against a Man-In-The-Middle attack (Lokhande & Meshram, 2013).
4. Migrating to up-to-date CRM software (Clint, 2018), setup live vulnerability scanner and patching web and application server regularly.
5. Implement DMARC policy and messaging security to prevent spam and phishing attacks (DMARC, N.D.).
6. Use Antivirus, Anti-Malware, and Firewalls to defend against trojan, malware (Badotra & Sundas, 2020).
7. Securing the server and admin panels by complex passwords and changing them frequently, using multi-factor authentication, and restricting access (inVerita, 2021).
8. Staff and clients should be aware of the security policy and the potential threats; staff should not disclose their login information and password or share their credentials between them (Bader, 2021).
9. Data Backup is crucial to protect e-commerce websites from losing data or costly downtime; regular backup can also help against malware and ransomware (BigCommerce, 2021).

References

Bader, S. (2021) Top Security Threats to Your Ecommerce Site. Available from: https://rewind.com/blog/ecommerce-security-threats/ [Accessed 10 December 2021].

Badotra, S. & Sundas, A. (2021) A systematic review on security of E-commerce systems. *International Journal of Applied Science and Engineering* 18 (2). Available from: https://doi.org/10.6703/IJASE.202106_18(2).010 [Accessed 8 December 2021]

BigCommerce. (2021) Ecommerce Security: Securing Against Cyber Threats 2021. Available from: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/ [Accessed 10 December 2021].

Clint, O. (Apr 6, 2018) Sugar Community Edition open source project ends. *Sugar-News*. Available: https://sugarclub.sugarcrm.com/engage/b/sugar-news/posts/sugar-community-edition-open-source-project-ends [Accessed 18 December 2021].

DMARC. (N.D.) Why is DMARC important?. *Frequently Asked Questions*. Available: https://dmarc.org/wiki/FAQ#Why_is_DMARC_important.3F [Accessed 18 December 2021].

inVerita. (2021) Top 10 E-commerce Security Threats and their Solutions. Available from: https://inveritasoft.com/blog/top-ecommerce-se-curity-threats-and-their-solutions [Accessed 7 December 2021]

Lokhande, P. & Meshram, B. (2013) E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. *International Journal of Advanced Research in Computer Engineering & Technology*. Available from: https://www.researchgate.net/publication/235697382_E-Commerce_Applications_Vulnerabilities_Attacks_and_Countermeasures/link/0046351e3de4208a02000000/download [Accessed 9 December 2021].

Sonovate. (N.D.). Key differences between B2B and B2C when it comes to GDPR. Available: https://www.sonovate.com/blog/key-differences-between-b2b-and-b2c-when-it-comes-to-gdpr/ [Accessed 11 December 2021].

Sugar CRM. (N.D.). Get Busy Being Less Busy. Available: https://www.sugarcrm.com/ [Accessed 11 December 2021].

World Economic Forum. (2019). *The Global Governance of Online Consumer Protection and E-commerce*. Available: https://www3.weforum.org/docs/WEF_consumer_protection.pdf [Accessed 11 December 2021].