Vulnerability Assessment Baseline Report for Gin and Juice E-Commerce Platform

Student Name: Lauren Pechey

Student ID: 12696823

Course: Masters of Computer Science

Module: Network Security Management

Professor: Beran Necat

Word Count: 659

Submission Date: 30 June 2025

Overview and Aim

This report provides a preliminary security assessment of the Gin and Juice Shop (GJS) website (https://ginandjuice.shop/), a simulated vulnerable e-commerce platform used for testing and training purposes. It aims to identify potential security vulnerabilities, evaluate their implications for the business, and propose effective tools and strategies to mitigate associated cybersecurity risks.

Introduction

The global e-commerce sector has grown significantly post-COVID-19, reaching USD$6 trillion in 2024 and projected to grow a further 31% by 2028 (Statista, 2025). However, this expansion has also increased the frequency of cyberattacks, particularly targeting small and medium-sized enterprises (SMEs) (NIST, 2023; Shimizu & Hashimoto, 2025). Verizon's (2025) report found that 30% of breaches involved third-parties, 44% involved ransomware, and 34% exploited known vulnerabilities. The GJS website offers a realistic environment to examine the security risks facing retail businesses.

Generic Security Vulnerabilities

To evaluate the general security posture of the GJS website, this analysis focuses on the key vulnerabilities highlighted by OWASP (2024), a framework for identifying and mitigating common web application security risks. The following table highlights the five most critical vulnerabilities in the GJS website, as per OWASP (2024):

OWASP Category	Vulnerability	Explanation
A1: Injection	SQL Injection	User input in "searchTerm" and "category" is not sanitised, allowing database manipulation.

A3: Cross-Site Scripting (XSS)	Reflected & DOM-Based XSS	Input is echoed without filtering, enabling script injection via search and login pages.
A2: Broken Authentication	Insecure Session Cookies	Session cookies lack “Secure”, “HttpOnly”, and “SameSite”, making them easier to hijack.
A5: Security Misconfiguration	Missing Security Headers	Headers like “CSP”, “X-Frame-Options”, and “HSTS” are missing, exposing users to various attacks.
A4: Broken Access Control	Server-Side Request Forgery	The stock API accepts unvalidated Referer headers, allowing internal or external abuse.

Figure 1: OWASP generic vulnerabilities on the GJS website (OWASP, 2024)

Tadhani et al. (2024) support this by showing that injection flaws, broken authentication, and misconfiguration are among the leading causes of real-world data breaches. Given the sensitivity of customer data and the importance of maintaining user trust, it is crucial to identify and mitigate these vulnerabilities (Egho-Promise et al., 2024).

Business-Specific Security Challenges

Business-specific vulnerabilities on the GJS website should be assessed against ISO/IEC 27001, the international standard for information security management (ISO, 2022). It emphasises risk assessment, integrity, access control, secure coding and data protection (ISO, 2022). Several GJS vulnerabilities could jeopardise legal compliance, operational continuity, and customer trust (Egho-Promise et al., 2024). The table below maps five key vulnerabilities to ISO/IEC 27001 controls:

ISO/IEC 27001 Control (Clause)	**Vulnerability**	**Explanation (Business Impact)**
A.9.2.3 – Privileged Access Rights	No Role-Based Access Control (RBAC)	Users may access admin or sensitive functions without restrictions.

A.10.1.1 – Cryptographic Controls	Unencrypted Session Cookies	Cookies lack Secure/HttpOnly, risking session hijacking.
A.12.6.1 – Technical Vulnerabilities	Outdated Libraries Used	Vulnerable JavaScript libraries increase attack surface.
A.14.2.1 – Secure Development Policy	Cross-Site Scripting (XSS)	Input is not sanitised, allowing malicious scripts.
A.18.1.4 – PII Protection	Weak Personal Data Safeguards	No visible measures to protect or encrypt customer data.

Figure 2: ISO/IEC 27001 business-specific vulnerabilities on the GJS website (ISO, 2022)

These findings underscore the need to integrate ISO/IEC 27001 practices in web development and maintenance, especially for personal and transactional data (ISO, 2022). Neglecting these controls risks regulatory penalties, customer distrust, and financial loss (Humayun et al., 2020).

Relevant Standards and Compliance

Since the GJS website handles user data and e-commerce transactions, key cybersecurity standards apply (Moric et al., 2024). The General Data Protection Regulation (GDPR) requires secure handling of personal data with user consent, which GJS lacks—evidenced by missing cookie banners and privacy notices (Haddara et al., 2023). Additionally, the Payment Card Industry Data Security Standard (PCI DSS) requires encrypted payment processing and secure configurations; however, GJS lacks HTTPS consistency and secure payment gateways (Lincke, 2024). Finally, ISO/IEC 27001 calls for risk management, access controls, and logging; GJS shows no login limits, multi-factor authentication, or patching (ISO, 2022). These failures undermine compliance, increase legal risk, and damage user trust (Seaman, 2020).

Tools, Justifications and Methodology

Tools such as Nmap, Nikto, OWASP ZAP, and Burp Suite were chosen for their proven effectiveness in detecting network and application-layer vulnerabilities (Singh et al., 2024; Thaqi et al., 2022):

Tool	Justification	Challenge Addressed	Methodology
nMap	Network scanner to identify open ports and network exposure (Singh et al., 2024)	Network vulnerabilities	Remote, automated black-box scanning
Nikto	Scans for outdated server software, default files, and misconfigurations (Choudri et al., 2024)	Security misconfiguration	Remote, automated web server scanning
OWASP ZAP	Identifies XSS, broken authentication, and insecure sessions via HTTP traffic (Choudri et al., 2024)	XSS, session management issues	Intercepts HTTP traffic for dynamic testing
Burp Suite	In-depth analysis of web vulnerabilities to uncover SQLi and logic flaws (Thaqi, Vishi & Rexha, 2022)	Injection flaws, logic errors	Interactive, deep penetration testing
Wfuzz	Performs fuzzing to discover injection points and hidden endpoints (Hsu, 2019)	Injection flaws, hidden vulnerabilities	Automated fuzz testing on inputs

Figure 3: Tools for assessing GJS vulnerabilities (ISO, 2022)

Timeline:

The following timeline outlines the key activities and their scheduled weeks for the security assessment of the GJS website:

Week	Activity
1	Initial assessment and research
2	Tool selection and preparation

3	Simulated scanning and evaluation

Figure 4: Timeline of proposed vulnerability assessment

Recommendations and Mitigation Strategies

The following recommendations align with industry best practices from the OWASP Top 10 (2024) and ISO/IEC 27001 standards, promoting both technical security and regulatory compliance:

Recommendation	**Purpose / Benefit**
Enforce HTTPS site-wide	Encrypts data in transit to prevent interception
Implement input validation and sanitisation	Prevents injection attacks like SQLi and XSS
Review and update server configurations	Reduces risk from outdated or insecure settings
Apply secure cookie attributes (HttpOnly, Secure)	Protects session data from theft or manipulation
Introduce Multi-Factor Authentication (MFA)	Strengthens admin login security through layered access controls
Schedule vulnerability scans during off-peak hours	Minimises business disruption and ensures timely threat detection

Figure 5: Security Recommendations for the GJS Website (ISO, 2022; OWASP, 2024)

Limitations and Assumptions

This analysis is based on black-box testing only. No access to source code, databases, or live systems was granted. Some logic flaws may not be detectable through automated scans (Hsu, 2019). Tool outputs may include false positives or miss subtle business logic issues (OWASP, 2024). It is assumed that testing is conducted ethically and with consent for educational purposes.

References:

Choudhri, R., Kataria, B., Ratnani, H., Jha, S., & Gupta, P. (2024) 'The hidden network penetrator based on port and vulnerability scan testing technique' *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON).* New Delhi, India. 1-5.

Egho-Promise, E., Lyada, E., Asante, G., & Anna, F. (2024) Towards improved vulnerability management in digital environments: A comprehensive framework for cyber security enhancement. *International Research Journal of Computer Science* 11(5): 441-449. DOI: https://doi.org/10.26562/irjcs

Haddara, M., Salazar, A., & Langseth, M. (2023) Exploring the impact of GDPR on big data analytics operations in the e-commerce industry. *Procedia Computer Science* 219(1): 767-777.

Hsu, T.. (2019) *Practical Security Automation and testing: Tools and techniques for automated security scanning and testing in devsecops*. 1st ed. Birmingham: Packt Publishing Ltd.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020) Cyber security threats and vulnerabilities: A systematic mapping study. *Computer Engineering and Computer Science* 45(1): 3171-3189. DOI: https://doi.org/10.1007/s13369-019-04319-2

ISO. (2022) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Available from: https://www.iso.org/standard/27001 [Accessed 28 Jun 2025].

Lincke, S. (2024) *Information security planning: A practical approach*. Cham, Cham: Springer International Publishing Springer.

Moric, Z., Dakic, V., Djekic, D., & Regvart, D. (2024) Protection of personal data in the context of e-commerce. *Journal of Cybersecurity and Privacy* 4(3): 731-761. DOI: https://doi.org/10.3390/jcp4030034

NIST. (2023) *National Vulnerability Database.* Available at: https://nvd.nist.gov/ [Accessed 28 June 2025].

OWASP. (2024) *OWASP Web Security Testing Guide (WSTG)*. Available from: https://owasp.org/www-project-web-security-testing-guide/ [Accessed 28 Jun 2025].

Seaman, J. (2020) *PCI DSS: An Integrated Data Security Standard Guide*. Berkeley, CA: Apress.

Singh, A., Sharma, S., Reddy, K., Soni, P., Ghuman, S., & Gill, U. (2024) 'Automated network vulnerability assessment with nMap: A comprehensive approach' *2024 Second International Conference on Advanced Computing.* Sonipat, India. 208-214.

Shimizu, N. and Hashimoto, M. (2025) *Vulnerability Management Chaining: An integrated framework for efficient cybersecurity risk prioritization*. Available at: https://arxiv.org/abs/2506.01220 [Accessed: 30 June 2025].

Statista. (2025) *Global Retail E-Commerce Sales 2022-2028*. Available from: https://www.statista.com [Accessed 28 June 2025].

Tadhani, J., Vekariya, V., Sorathiya, V., Alshathri, S., & El-Shafai, W. (2024) Securing web applications against XSS and SQLi attacks using a novel deep learning approach. *Scientific Reports* 14(1803): 1-17. DOI: https://doi.org/10.1038/s41598-023-48845-4

Thaqi, R., Vishi, K., & Rexha, B. (2022) Enhancing BURP suite with machine learning extension for Vulnerability Assessment of Web Applications. *Journal of Applied Security Research* 18(4): 789-807. DOI: https://10.1080/19361610.2022.2096387

Verizon. (2025) *Data Breach Investigations Report*. Available from: https://www.verizon.com [Accessed 27 June 2025].