Gin & Juice Shop (https://ginandjuice.shop) is an online commerce website. As it stores its customers' personal data, it is a likely target for adversaries seeking to steal them and sell on the dark web (Liu *et al.*, 2020). Cyberattacks on enterprises cause service interruptions, and data breaches can be fatal, as they result in significant financial and reputational losses (Hepfer, 2021).

Applicable standards

The below cybersecurity standards of the European Union and the United Kingdom apply to the organisation.

Table 1. Applicable standards

Standard/Regulation	**Applicability**	**Non-compliance**
EU & UK GDPR ('Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)', 2016)	The shop stores customers' personal data	Up to 20,000,000 EUR or 17,500,000 GBP or 4 % of annual revenue (Information Commissioner's Office, 2024)
EU ePrivacy Directive ('Directive 2002/58/EC of the European Parliament and of the Council (Directive on privacy and electronic communications)', 2009) **UK PECR** ('The Privacy and Electronic Communications	The website uses cookie technology	EU: depends on the member state UK: same as GDPR (O'Connors, no date)

Standard/Regulation	Applicability	Non-compliance
(EC Directive) Regulations 2003', 2025)		
Payment Card Industry Data Security Standard (PCI DSS) (Fruhlinger, 2024) **Payment Services Directive (PSD2)** ('Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market', 2015; Stripe, Inc., 2024)	The shop processes cardholder data and accepts online card payments	EU: depends on the member state UK: depends on the violation (Payment Systems Regulator, 2017) Payment processors may impose fines or suspend transactions (Mariano, 2022)

Vulnerabilities

Table 2 presents vulnerability categories relevant for *Gin & Juice Shop* listed in order of potential business impact.

Table 2. Vulnerabilities relevant to Gin & Juice Shop

Category	Description
A06:2021 – Vulnerable and Outdated Components	'Wildcard' weakness with unknown effects

Category	Description
A01:2021 – Broken Access Control A02:2021 – Cryptographic Failures CWE-352: Cross-Site Request Forgery (CSRF)	Leads to data exposure, potentially trivial to abuse
A03:2021 – Injection	Leads to data exposure or modification, account takeover
A07:2021 – Identification and Authentication Failures	Leads to account takeover, data exposure or modification; can partially be mitigated by user, e.g. by using strong password
Denial of Service	Causes service interruption and financial damages; cloud providers offer protection services (Amazon Web Services, Inc., no date; Cloudflare, Inc., no date)
Social Engineering	Account takeover, personal data exposure or modification, but there are little mitigation possibilities for an enterprise

Sources: OWASP Top 10 Team (2021a, 2021b, 2021c, 2021d, 2021e), The MITRE Corporation (no date), European Union Agency for Cybersecurity (2025).

Security Scanning and Testing

This assessment will focus on a *closed box* penetration test to reveal vulnerabilities in the web application and guide future security-related effort (National Cyber Security

Centre, 2022). Due to its nature, the test cannot detect issues with the business logic on the server side.

Manual security assessment of the website will follow the OWASP Web Security Testing Guide, which is selected for its comprehensive approach and level of detail (OWASP Foundation, 2024).

Zed Attack Proxy (ZAP) will be used for automated penetration testing. ZAP supports extensibility and automation, and performs on par with commercial solutions (Albahar, Alansari and Jurcut, 2022). Running ZAP sends many requests; to avoid service interruptions, testing must occur outside peak hours. Another consideration is that the tool may modify data via forms, therefore website functionality must be well understood.

Other tools such as `dig` or `whois` will be used for *fingerprinting* — to gather information about the implementation details for the website.

The approximate timeline for working on the project is on the Figure 1.

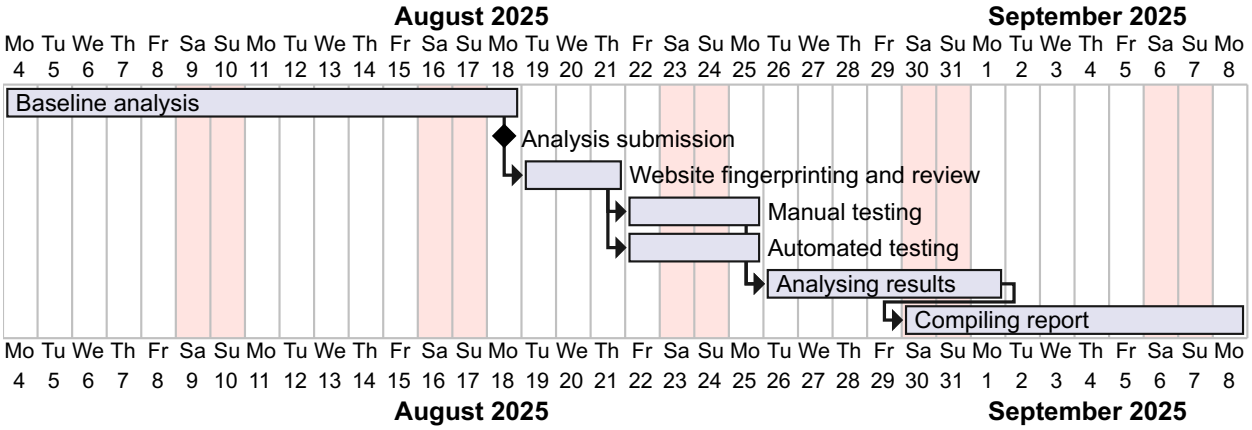

Figure 1. Website testing timeline

Concluding Remarks & Recommendations

This document outlines the cybersecurity testing strategy for *Gin & Juice Shop* that ensures its compliance with the applicable standards and best practices. However,

occasional testing is insufficient; proactive measures (most to least important) are also recommended:

1. Employee education on the topic to enable security-oriented solutions in the future (Kamil, Lund and Islam, 2023).
2. Security testing routine in the company, e.g. based on OWASP Web Security Testing Framework (OWASP Foundation, 2020).
3. Regular audits to track and foster compliance with standards and legislations (Fallatah, 2025). Additionally, security-related certifications like SOC 2 or ISO 27001 both guide organisations in implementing security and improve the organisations' public image (Disterer, 2013; Secureframe, no date).

References

Albahar, M., Alansari, D. and Jurcut, A. (2022) ‘An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities’, *Electronics*, 11(19), p. 2991. Available at: https://doi.org/10.3390/electronics11192991.

Amazon Web Services, Inc. (no date) *Network Posture Analysis and Managed DDoS Protection - AWS Shield - AWS*, *Amazon Web Services, Inc.* Available at: https://aws.amazon.com/shield/ (Accessed: 15 August 2025).

Cloudflare, Inc. (no date) *DDoS Protection & Mitigation Solutions*. Available at: https://www.cloudflare.com/ddos/ (Accessed: 15 August 2025).

‘Directive 2002/58/EC of the European Parliament and of the Council (Directive on privacy and electronic communications)’ (2009). Official Journal of the European Union. Available at: http://data.europa.eu/eli/dir/2002/58/2009-12-19 (Accessed: 15 August 2025).

‘Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market’ (2015). Official Journal of the European Union. Available at: http://data.europa.eu/eli/dir/2015/2366/oj/eng (Accessed: 15 August 2025).

Disterer, G. (2013) ‘ISO/IEC 27000, 27001 and 27002 for Information Security Management’, 2013. Available at: https://doi.org/10.4236/jis.2013.42011.

European Union Agency for Cybersecurity (2025) *Threat Landscape | ENISA*. Available at: https://enisa.europa.eu/topics/cyber-threats/threat-landscape (Accessed: 14 August 2025).

Fallatah, E. (2025) ‘Ensuring Compliance: Data Privacy Audits Under Global Privacy Regulations’, *International Journal of Applied Economics, Finance and Accounting*, 22(2), pp. 133–144. Available at: https://doi.org/10.33094/ijaefa.v22i2.2308.

Fox, G., Lynn, T. and Rosati, P. (2022) ‘Enhancing consumer perceptions of privacy and trust: a GDPR label perspective’, *Information Technology & People*, 35(8), pp. 181–204. Available at: https://doi.org/10.1108/ITP-09-2021-0706.

Fruhlinger, J. (2024) ‘PCI DSS defined: Requirements, fines, and steps to compliance’, *CSO Online*, 3 April. Available at: https://www.csoonline.com/article/569591/pci-dss-explained-requirements-fines-and-steps-to-compliance.html (Accessed: 15 August 2025).

Hepfer, M. (2021) *Gaining Competitive Advantage from Cybersecurity*. Available at: https://istari-global.com/assets/PDFs/ISTARI-Perspectives-Gaining-Competitive-Advantage-From-Cybersecurity.pdf (Accessed: 16 August 2025).

Information Commissioner’s Office (2024) *Penalties*. ICO. Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/ (Accessed: 15 August 2025).

Kamil, Y., Lund, S. and Islam, M.S. (2023) ‘Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders’ perspective on expectations in private organizations in Sweden’, *Information Systems and e-Business Management*, 21(3), pp. 699–722. Available at: https://doi.org/10.1007/s10257-023-00646-y.

Liu, Y. *et al.* (2020) ‘Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web’, in *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*. *2020 IEEE International*

Conference on Intelligence and Security Informatics (ISI), pp. 1–6. Available at: https://doi.org/10.1109/ISI49825.2020.9280540.

Mariano, M. (2022) *PCI Non Compliance Fines & Consequences*. Available at: https://www.ispartnersllc.com/blog/pci-non-compliance-fines-consequences/ (Accessed: 15 August 2025).

National Cyber Security Centre (2022) *Penetration testing*. Available at: https://www.ncsc.gov.uk/guidance/penetration-testing (Accessed: 13 August 2025).

O'Connors (no date) *Penalties for breaching direct marketing regulations set to increase*. Available at: https://www.oconnors.law/news-views/penalties-for-breaching-direct-marketing-regulations-set-to-increase/ (Accessed: 15 August 2025).

OWASP Foundation (2020) *The Web Security Testing Framework*. Available at: https://owasp.org/www-project-web-security-testing-guide/stable/3-The_OWASP_Testing_Framework/0-The_Web_Security_Testing_Framework (Accessed: 16 August 2025).

OWASP Foundation (2024) *OWASP Web Security Testing Guide*. Available at: https://owasp.org/www-project-web-security-testing-guide/ (Accessed: 15 August 2025).

OWASP Top 10 Team (2021a) *A01 Broken Access Control - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A01_2021-Broken_Access_Control/ (Accessed: 14 August 2025).

OWASP Top 10 Team (2021b) *A02 Cryptographic Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ (Accessed: 14 August 2025).

OWASP Top 10 Team (2021c) *A03 Injection - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A03_2021-Injection/ (Accessed: 14 August 2025).

OWASP Top 10 Team (2021d) *A06 Vulnerable and Outdated Components - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/ (Accessed: 14 August 2025).

OWASP Top 10 Team (2021e) *A07 Identification and Authentication Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ (Accessed: 14 August 2025).

Payment Systems Regulator (2017) 'The PSR's approach to monitoring and enforcing the revised Payment Services Directive (PSD2)'. Available at: https://www.psr.org.uk/media/cwxhu2tc/psr-psd2-approach-and-ppg-september-2017.pdf (Accessed: 14 August 2025).

'Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)' (2016). Official Journal of the European Union. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 19 January 2025).

Secureframe (no date) *What is SOC 2? A Beginners Guide to Compliance*, *Secureframe*. Available at: https://secureframe.com/hub/soc-2/what-is-soc-2 (Accessed: 17 August 2025).

Stripe, Inc. (2024) *What is PSD2? A guide to PSD2 compliance*. Available at: https://stripe.com/en-de/resources/more/what-is-psd2-here-is-what-businesses-need-to-know (Accessed: 15 August 2025).

The MITRE Corporation (no date) *CWE - CWE-352: Cross-Site Request Forgery (CSRF) (4.17)*. Available at: https://cwe.mitre.org/data/definitions/352.html (Accessed: 14 August 2025).

‘The Privacy and Electronic Communications (EC Directive) Regulations 2003’ (2025). Statute Law Database. Available at: https://www.legislation.gov.uk/uksi/2003/2426 (Accessed: 15 August 2025).