Vulnerability Audit and Assessment

This document presents findings from of a security analysis of the online commerce website *Gin & Juice Shop* (https://ginandjuice.shop), the evaluation of its compliance to standards like General Data Protection Regulation (GDPR) of the European Union (EU) and the United Kingdom (UK), and Payment Card Industry Data Security Standard (PCI DSS), as well as provides the improvement recommendations.

Methodology

The manual security assessment follows the OWASP Web Security

Testing Guide, and automated penetration testing is performed with Zed Attack Proxy (ZAP), as discussed in the original submission (Appendix 1).

The discovered vulnerabilities are evaluated using OWASP Risk Rating Methodology where applicable. Although other risk rating methodologies, like the Common Vulnerability Scoring System (CVSS), are more mature or widely used, OWASP rating still provides a diverse set of criteria and fits well for the purposes of this assessment without being overly complex (Forum of Incident Response and Security Teams, Inc, no date; OWASP Foundation, no date). An online OWASP Risk Rating Calculator implementing the methodology was used (*OWASP Risk Rating Calculator*, no date). The ratings include the overall severity and the Likelihood (LF) and Impact Factor (IF).

Manual Security Assessment

Manual scanning does not reveal any other services under the same domain nor subdomains; the only open ports are 80 and 443, which is consistent with a website (Internet Assigned Numbers Authority, 2025).

The DNS records for the domain reveal that the resource is hosted on the IP addresses associated with Amazon Web Services (AWS). Besides, the received cookies `AWSALB` and `AWSALBCORS` indicate that AWS's *Application Load Balancer* service is used (Amazon Web Services, Inc., no date), which allows to conclude that the resource is hosted on the AWS infrastructure.

Login form implements protection against cross-site request forgery (CSRF). At the same time, multi-factor authentication or login throttling are not implemented, thus allowing for automated attacks and account hijacking.

Automated Security Assessment

ZAP attempts multiple attack scenarios on a large set of webpages at once, and the results later evaluated to determine the vulnerability relevancy and threat level.

Detected Vulnerabilities

Below is the list of the discovered vulnerabilities on the website both during manual and automated assessment in order of their importance.

Customers' Personal Data Disclosure

Category	CWE-425: Direct Request (The MITRE Corporation, no date e)
Description	Links like `https://ginandjuice.shop/order/details?orderId=0254809` are available without authentication and reveal personally identifiable information such as names and addresses. Orders' numbers are predictable, and it is possible to automatically collect the data.

Ranking

Critical (LF: 7.875, IF: 7) (SL:9/M:9/O:9/S:9/ED:9/EE:9/A:9/ID:0/LC:7/LI:0/LAV:0/LAC:9/FD:7/RD:9/NC:7/PV:5)

The risk is immediate: the vulnerability is trivial to discover, exploit, and automate; attacks cannot be traced.

Vulnerable Dependency

Category

CWE-1104: Use of Unmaintained Third Party Components (The MITRE Corporation, no date g)

Description

There are multiple known vulnerabilities in AngularJS 1.7.7 that enable cross-site scripting (XSS) and regular expression Denial of Service (ReDoS) attacks (The MITRE Corporation, 2023, 2025).

AngularJS is no longer supported and does not receive any security updates (Thompson, 2022).

Ranking

There are known vulnerabilities in the library, and it is likely more will be discovered later.

SQL Injection

Category

CWE-89: Improper Neutralization of Special Elements used in an SQL Command (The MITRE Corporation, no date b)

Description

Filtering items in the catalogue by category includes sending a request to server; inserting a quotation mark in the request results in a server error, indicating a possible SQL injection under the URL:

`https://ginandjuice.shop/catalog?category=%27`.

Ranking

Critical (LF: 6.625, IF: 7)

(SL:3/M:9/O:9/S:9/ED:9/EE:5/A:9/ID:0/LC:9/LI:9/LAV:9/LAC:9/FD:7/RD:9/NC:7/PV:5)

The affected URL is available to anonymous users. The vulnerability is easily discoverable and exploitable; it allows unrestricted read and write access to the database.

Reflected XSS

Category

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (The MITRE Corporation, no date a)

Description

Multiple pages of the website incorporate data from GET requests without sanitisation, thus allowing to construct a link that will execute third-party payload once page is loaded:

- `https://ginandjuice.shop/catalog?category=%0A%0D%0A%0D%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E`
- `https://ginandjuice.shop/blog/?search=aaa%22+onload%3D%22alert%281%29&back=%2Fblog%2F`

- `https://ginandjuice.shop/catalog?category=any%0D%0A%0D%0A%3Cscript%3Ealert(1)%3C/script%3E`

Ranking

Critical (LF: 6.375, IF: 7)

(SL:3/M:9/O:7/S:9/ED:9/EE:5/A:9/ID:0/LC:7/LI:7/LAV:0/LAC:7/FD:7/RD:9/NC:7/PV:5)

The vulnerability is easily discoverable and exploitable, although user interaction is required. Pages modified by malicious payload may trick users into revealing their personal data or login details.

CRLF Injection

Category

CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers (The MITRE Corporation, no date c)

Description

Filtering by categories in the catalogue sends a request to the server that includes the user-provided parameters verbatim. They are not sanitised nor validated, allowing to prepare a link that breaks HTTP headers formatting and allows to insert any payload, including malicious headers or an XSS attack.

Ranking

Critical (LF: 6.375, IF: 7)

(SL:3/M:9/O:7/S:9/ED:9/EE:5/A:9/ID:0/LC:7/LI:7/LAV:0/LAC:7/FD:7/RD:9/NC:7/PV:5)

The vulnerability is easy to discover and exploit, can lead to account hijacking, stealing and corruption of data.

Absence Of Anti-CSRF Tokens

Category	CWE-352: Cross-Site Request Forgery (CSRF) (The MITRE Corporation, no date d)
Description	The lack of CSRF tokens in the cart management forms allows to manipulate cart contents from third-party resources.
Ranking	Low (LF: 5.375, IF: 0.5) (SL:3/M:1/O:7/S:9/ED:9/EE:5/A:9/ID:0/LC:0/LI:1/LAV:0/LAC:7/FD:1/RD:1/NC:0/PV:0) The vulnerability is easy to discover and exploit, but there is no data disclosure, and the impact is limited to nuisance. Critical forms like login or place order are protected.

Applicable standards

The applicability of the standards below as well as non-compliance are discussed in the original submission (Appendix 1).

EU And UK GDPR

The General Data Protection Regulation sets strict rules on how personally identifiable information must be stored, transferred, and processed. The website implements authentication and authorisation mechanisms, where user profiles are not available to unauthenticated users. However, access to order details is not restricted, and personally identifiable information such as customers' names, home addresses, and orders' contents are revealed, which is a violation of article 32 of GDPR which prohibits unauthorised disclosure of personal data ("Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)," 2016). Besides, the discovered vulnerabilities such as possible XSS or SQL injection attacks can lead to data breaches, for which the *Gin & Juice Shop* may be found liable under GDPR, and that are likely to result in brand damages and financial losses.

PCI DSS

PCI DSS is a standard mandated by the card brands. It requires that the cardholder data can only be accessed by authorised personnel (PCI Security Standards Council, no date). *Gin & Juice Shop* reveals the cardholder names on the order pages, and other vulnerabilities can lead to data breaches revealing other sensitive information such as account numbers. Non-compliance with PCI DSS are higher transaction fees from the payment processors, ongoing fees, or shop's transactions being suspended (Mariano, 2022).

Concluding Remarks & Recommendations

It is advised to follow the steps below to mitigate the discovered vulnerabilities:

1. Immediately restrict access to order pages for unauthorised users.
2. Evaluate whether the known vulnerabilities in AngularJS pose any immediate risk, upgrade to the latest available version, start investigating future migration to a supported framework.
3. Implement content security policy headers in the server responses to prevent loading data from and sending to third-party resources, e.g. as a part of XSS attacks (OWASP Foundation, 2025b).
4. Implement sanitisation for all user-provided input and use injection-proof methods for executing SQL queries. For example, if the backend for the website

uses PHP, prepared statements can protect the website against SQL injections (The PHP Documentation Group, no date).

5. Implement more robust authentication methods, such as two-factor authentication (OWASP Foundation, 2025a).
6. Avoid disclosing server errors to prevent attackers from gaining information about website implementation, as per CWE-550 *Server-generated Error Message Containing Sensitive Information* (The MITRE Corporation, no date f).
7. Update forms on the website to use CSRF tokens.

Any logs that are collected must be reviewed for evidence of past attacks. If there is evidence of past or ongoing attacks, this must be immediately reported to the regulator such as the UK Information Commissioner’s Office.

To prevent future attacks, employee education, routine security testing, and regular audits are still recommended as discussed in the original submission (Appendix 1).

References

Amazon Web Services, Inc. (no date) *Edit target group attributes for your Application Load Balancer - Elastic Load Balancing*. Available at: https://docs.aws.amazon.com/elasticloadbalancing/latest/application/edit-target-group-attributes.html (Accessed: September 4, 2025).

Forum of Incident Response and Security Teams, Inc (no date) *CVSS v4.0 Specification Document*, *FIRST — Forum of Incident Response and Security Teams*. Available at: https://www.first.org/cvss/v4-0/specification-document (Accessed: September 5, 2025).

Internet Assigned Numbers Authority (2025) *Service Name and Transport Protocol Port Number Registry*. Available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1 (Accessed: September 4, 2025).

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

OWASP Foundation (2025a) *Authentication - OWASP Cheat Sheet Series*. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html#login-throttling (Accessed: September 4, 2025).

OWASP Foundation (2025b) *Content Security Policy - OWASP Cheat Sheet Series*. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html (Accessed: September 5, 2025).

OWASP Foundation (no date) *OWASP Risk Rating Methodology*. Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (Accessed: September 4, 2025).

OWASP Risk Rating Calculator (no date). Available at: https://owasp-risk-rating.com/ (Accessed: September 5, 2025).

PCI Security Standards Council (no date) “PCI DSS Quick Reference Guide.” Available at: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (Accessed: September 5, 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: January 19, 2025).

The MITRE Corporation (2023) *CVE Record: CVE-2023-26116*. Available at: https://www.cve.org/CVERecord?id=CVE-2023-26116 (Accessed: September 4, 2025).

The MITRE Corporation (2025) *CVE Record: CVE-2022-25869*. Available at: https://www.cve.org/CVERecord?id=CVE-2022-25869 (Accessed: September 4, 2025).

The MITRE Corporation (no date a) *CWE - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting’) (4.17)*. Available at: https://cwe.mitre.org/data/definitions/79.html (Accessed: August 14, 2025).

The MITRE Corporation (no date b) *CWE - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection’) (4.17)*. Available at: https://cwe.mitre.org/data/definitions/89.html (Accessed: August 14, 2025).

The MITRE Corporation (no date c) *CWE - CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') (4.17)*. Available at: https://cwe.mitre.org/data/definitions/113.html (Accessed: September 5, 2025).

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

The MITRE Corporation (no date e) *CWE - CWE-425: Direct Request ('Forced Browsing') (4.17)*. Available at: https://cwe.mitre.org/data/definitions/425.html (Accessed: September 5, 2025).

The MITRE Corporation (no date f) *CWE - CWE-550: Server-generated Error Message Containing Sensitive Information (4.17)*. Available at: https://cwe.mitre.org/data/definitions/550.html (Accessed: September 5, 2025).

The MITRE Corporation (no date g) *CWE - CWE-1104: Use of Unmaintained Third Party Components (4.17)*. Available at: https://cwe.mitre.org/data/definitions/1104.html (Accessed: September 5, 2025).

The PHP Documentation Group (no date) *PHP: Prepared statements and stored procedures - Manual*. Available at: https://www.php.net/manual/en/pdo.prepared-statements.php (Accessed: September 5, 2025).

Thompson, M. (2022) *Discontinued Long Term Support for AngularJS*, *Medium*. Available at: https://blog.angular.dev/discontinued-long-term-support-for-angularjs-cc066b82e65a (Accessed: September 5, 2025).

Appendix 1

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	The website uses cookie technology	EU: depends on the member state UK: same as GDPR (O'Connors, no date)

Standard/Regulation	**Applicability**	**Non-compliance**
Electronic Communications (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 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.

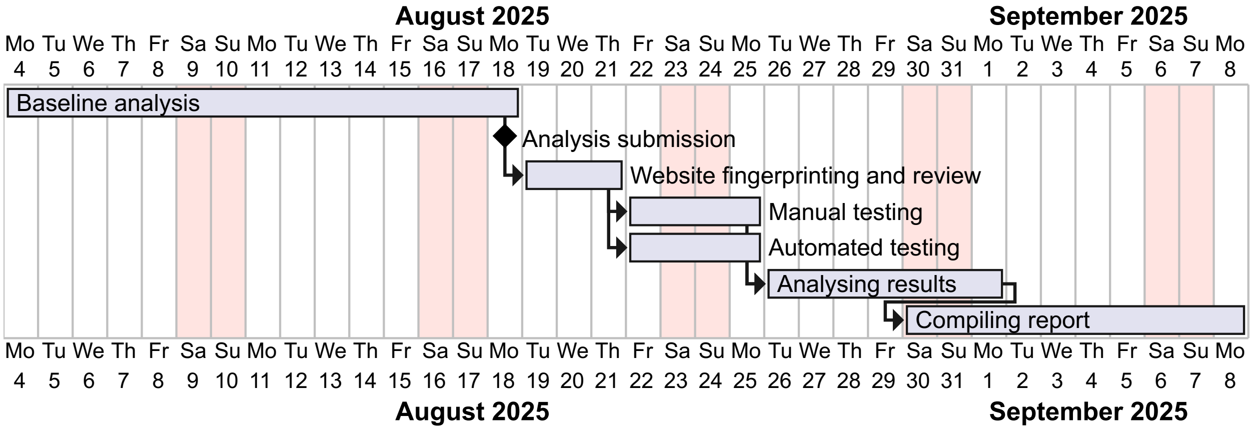

Figure 1. Website testing timeline

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).