Results and Executive Summary

GIN AND JUICE SHOP

Table of Contents

Introduction 2
Methodologies Used 2
Limitations 2
Summary of work carried out. 2
Reconnaissance and Information Gathering 2
Active Scanning and Vulnerability Testing 3
Security Review 3
Key Endpoints Identified 4
Compliance Assessment 4
Baseline vs Current Security Findings 5
Summary of Findings 5
Key Security Issues Found: 5
Security Standards Evaluation 6
GDPR Compliance (Article 32) 6
ISO 27001 Compliance 6
PCI DSS Compliance 6
Cyber Essentials Compliance 7
Conclusions 8
Key Findings 8
Business and Compliance Risks 8
Summary of Key Findings: 8
Recommendations 9
High Priority (Immediate Action) 9
Medium Priority (Short-Term Fixes) 9
Low Priority (Long-Term Improvements) 9
References 10
Bibliography 11

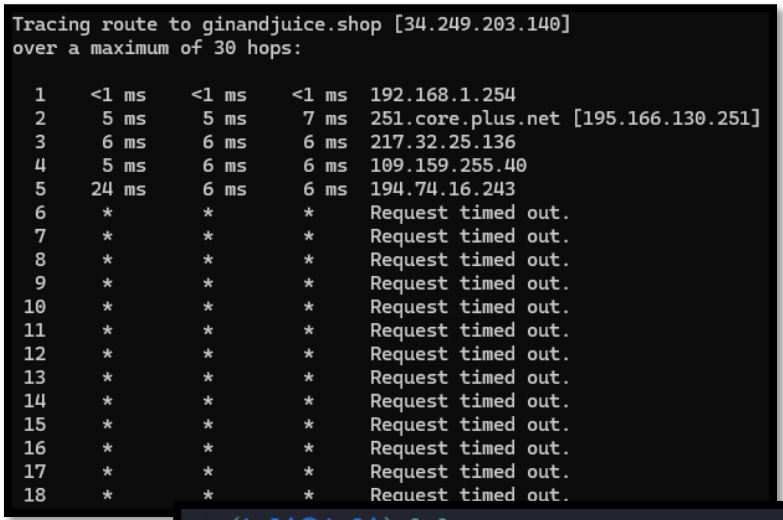
Results and Executive Summary
Gin and Juice Shop

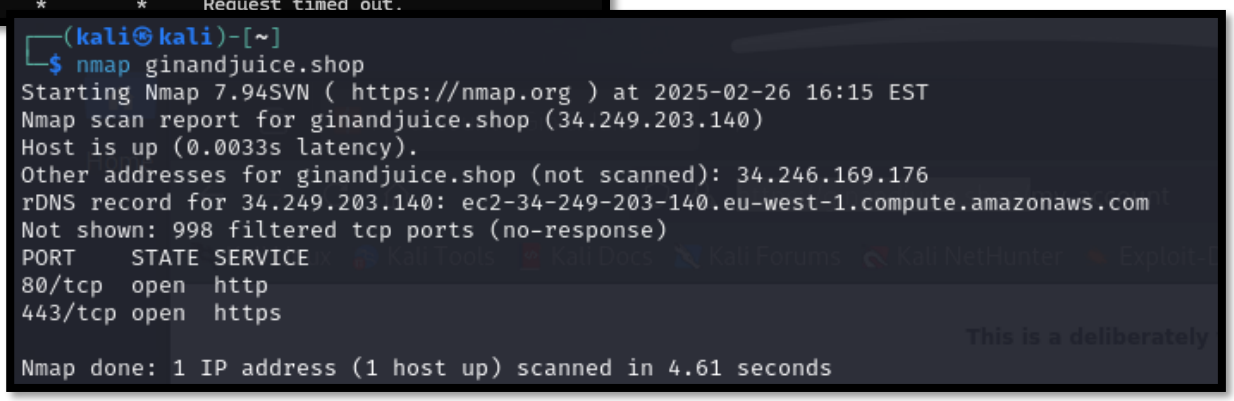
Introduction
The purpose of this security assessment was to evaluate the Gin and Juice Shop's website in terms of security vulnerabilities and compliance with relevant standards, particularly GDPR (European Commission, 2016), ISO 27001 (ISO/IEC, 2022), and PCI DSS (PCI Security Standards Council, 2022). This assessment involved a combination of automated scanning, manual testing, and evaluation against industry standards.

Methodologies Used
- Reconnaissance and Information Gathering: WHOIS, DNS enumeration and network scanning (Nmap, Traceroute).
- Automated Vulnerability Scanning: Nikto, Burp Suite, and Nmap service detection.
- Manual Penetration Testing: SQL injection tests, CSRF token validation and session security analysis.
- Security Policy Evaluation: Assessment of encryption, access control policies and authentication mechanisms.
- Compliance Review: Cross-checking security controls against GDPR, ISO 27001 and PCI DSS standards.

Limitations
- Restricted backend access prevented in depth analysis of database.
- Time constraints limited extensive penetration testing on APIs.

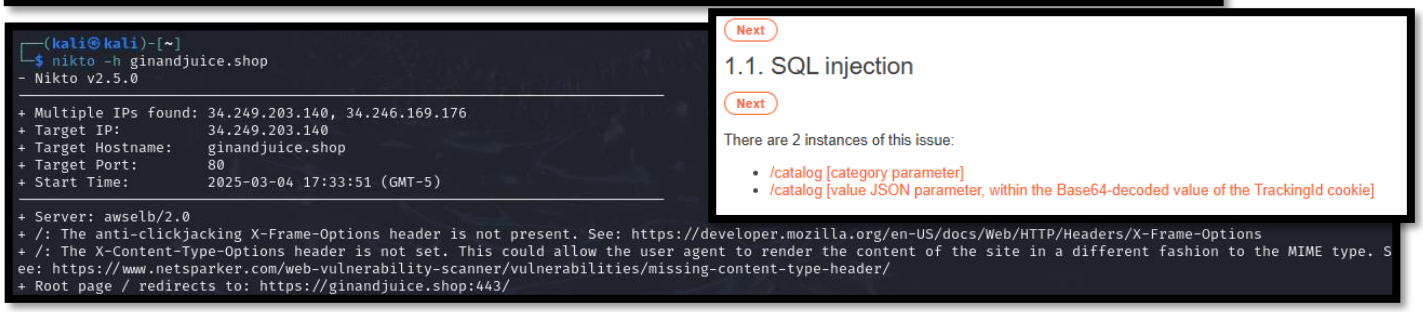
Summary of work carried out.
Reconnaissance and Information Gathering
- WHOIS, DNS and Network Scans (Nmap, Traceroute).

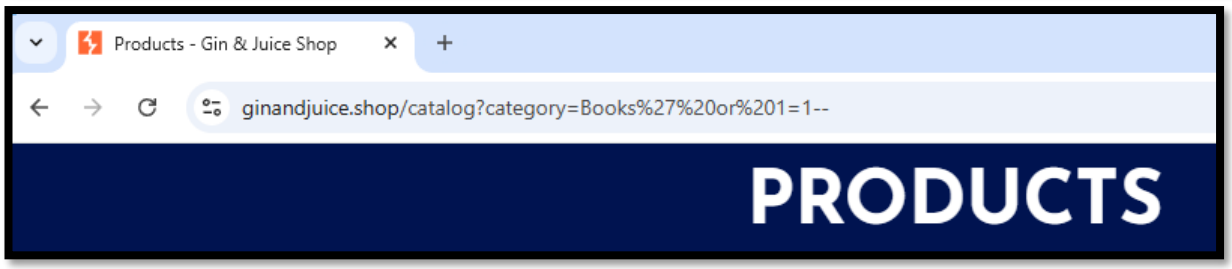




Active Scanning and Vulnerability Testing

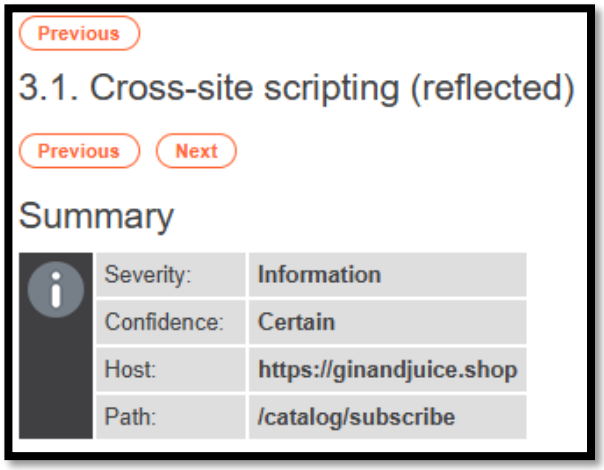
- Nmap, Nikto, Burp Suite, SQL Injection Testing.
- Identified open ports and running services.
- Detected missing security headers.
- Discovered SQL injection vulnerabilities.

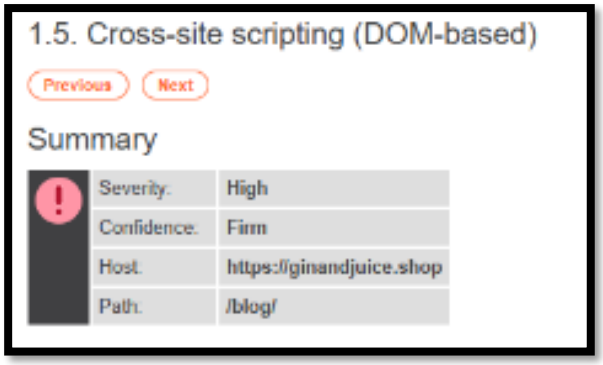


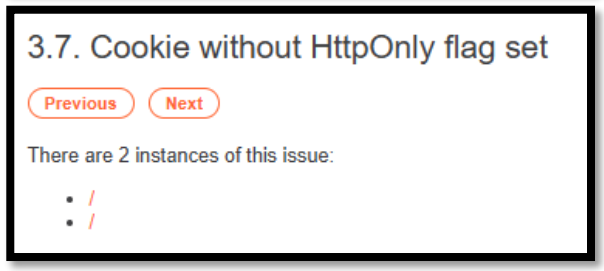


Security Review

- Session management and authentication testing.
- CSRF vulnerabilities detected.
- Cookie security analysis.

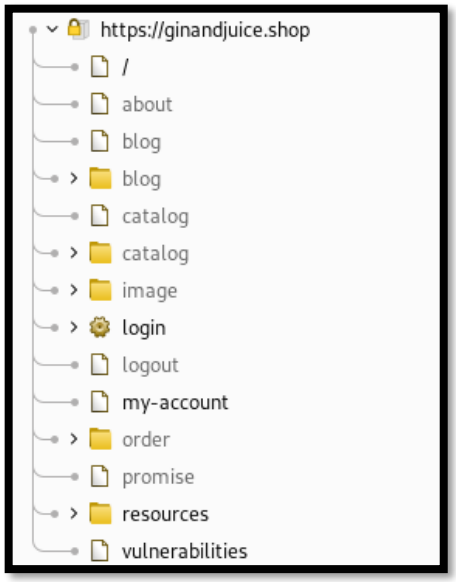






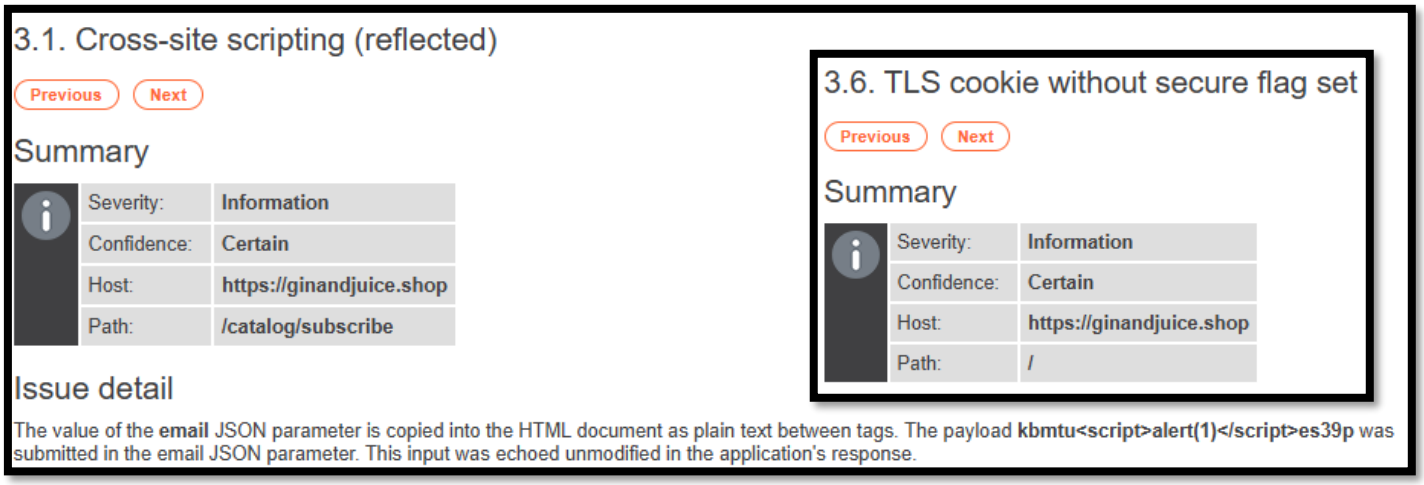
Key Endpoints Identified

Endpoint	Function	Security Concerns
/login	User authentication	No MFA, weak session management, brute-force risk
/my-account	User account dashboard	Session hijacking risk, missing secure cookies
/catalog	Product listings	SQL Injection risk
/catalog/product/stock	Stock availability API	CSRF vulnerability, SQL Injection
/order	Transaction processing	Potential lack of encryption-at-rest
/blog	CMS-driven content	CSRF vulnerability in comment forms
/resources	Public file repository	Possible directory listing exposure
/vulnerabilities	Possible test/debugging environment	Potential exposure of sensitive development data



Compliance Assessment

- GDPR Article 32 and Cyber Essentials evaluation.
- Checked encryption, access controls and security policies.



Baseline vs Current Security Findings

Security Aspect	Baseline Expectation	Actual Findings
HTTPS Encryption	Enforced	No HSTS, weak HTTPS enforcement
Access Controls	MFA enabled	No MFA, weak session management
SQL Injection Protection	Parameterised Queries	Vulnerable endpoints (/catalog/filter)
CSRF Protection	Tokens & Secure Forms	CSRF vulnerabilities in forms
Security Headers	Present	Missing X-Frame-Options, Content-Security-Policy
GDPR Compliance	Compliance	No Compliance
Regular Security Audits	Annually	No evidence of security audits

Summary of Findings

Key Security Issues Found:

- Lack of Data Encryption (TLS not enforced, missing HSTS header).
- Weak Access Controls (No MFA, weak session management).
- SQL Injection Vulnerabilities (/catalog/filter, /catalog/product/stock).
- CSRF Vulnerabilities (/catalog/cart, /blog).
- No Web Application Firewall (WAF) Detected (Higher risk of automated attacks).
- Missing Security Headers (X-Frame-Options, X-Content-Type-Options).
- No Regular Security Audits Conducted.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	4	3	2	9
	Medium	0	0	0	0
	Low	1	0	3	4
	Information	18	4	1	23
	False Positive	0	0	0	0

Security Standards Evaluation

GDPR Compliance (Article 32)

GDPR Requirements:

- Encryption for personal data.
- Secure access control and authentication.
- Protection against unauthorised access.

Findings:

- Unencrypted form submissions. Violates GDPR Encryption Rules.
- SQL Injection vulnerabilities. Risk of data leakage.
- No MFA. Fails access control requirements.

Conclusion: The website does not meet GDPR security requirements. Immediate remediation is required to avoid potential compliance violations and penalties.

ISO 27001 Compliance

ISO 27001 Requirements:

- Risk Management: Ongoing vulnerability assessment and mitigation.
- Access Control: Restricted administrative access, MFA implementation.
- Data Security: Encryption of sensitive data.
- Incident Response and Logging: Mechanisms for detecting, responding to and documenting security incidents.

Findings:

- Lack of formal risk assessment and vulnerability management process.
- No Multi-Factor Authentication (MFA) for account security.
- Encryption not enforced for login and sensitive transactions.
- No evidence of security monitoring/logging.

Conclusion: The website does not meet ISO 27001 security requirements. Implementing a structured risk management process and enforcing encryption and authentication policies is necessary.

PCI DSS Compliance

PCI DSS Requirements:

- Encryption of payment data at rest and in transit.
- Strict access control measures.
- Regular security audits and penetration testing.
- Use of firewalls and Web Application Firewall (WAF) to protect payment flows.

Findings:

- No evidence of payment encryption (HSTS not enforced, missing secure cookie flags).
- Session security flaws (cookies not secured, weak session timeout policies).
- No Web Application Firewall (WAF) detected to filter malicious traffic.
- No record of regular penetration testing and security audits.

Conclusion: The website does not meet PCI DSS compliance standards, increasing the risk of data breaches and financial fraud. Payment security measures need urgent improvement.

Cyber Essentials Compliance

Cyber Essentials Controls:

- Firewalls and Internet Gateways (AWS Load Balancer detected)
- Secure Configuration (Missing security headers)
- Access Control (No MFA, weak session management)
- Malware Protection (Not tested, no WAF detected)
- Patch Management (Outdated software detected)

Findings:

- Weak password policies and no MFA, Fails compliance.
- Outdated software, Fails patch management.
- Security headers missing, Fails secure configuration.

Conclusion: The website fails Cyber Essentials compliance due to weak access controls, outdated software and missing security configurations. Immediate fixes are needed.

Conclusions

Based on the comprehensive security assessment of Gin and Juice Shop's website, it is evident that critical vulnerabilities exist across various domains, including authentication, data encryption, access control and compliance with security standards. The website fails to meet GDPR, ISO 27001, PCI DSS and Cyber Essentials requirements, exposing it to potential legal penalties, financial losses and reputational damage.

1. High severity issues

1.1. SQL injection
1.2. HTTP response header injection
1.3. Cross-site scripting (reflected)
1.4. Client-side template injection
1.5. Cross-site scripting (DOM-based)
1.6. External service interaction (HTTP)

2. Low severity issues

2.1. Vulnerable JavaScript dependency
2.2. Open redirection (DOM-based)
2.3. Strict transport security not enforced

3. Informational issues

3.1. Cross-site scripting (reflected)
3.2. Client-side prototype pollution
3.3. External service interaction (DNS)
3.4. Input returned in response (reflected)
3.5. Request URL override
3.6. TLS cookie without secure flag set
3.7. Cookie without HttpOnly flag set
3.8. Cacheable HTTPS response
3.9. Base64-encoded data in parameter
3.10. TLS certificate

Key Findings

- Lack of Data Encryption – TLS not enforced, missing HSTS header.
- Weak Access Controls – No Multi-Factor Authentication (MFA), weak session management.
- SQL Injection Vulnerabilities – Found in /catalog/filter and /catalog/product/stock.
- Cross-Site Request Forgery (CSRF) Risks – Present in /catalog/cart and /blog.
- Missing Security Headers – X-Frame-Options, X-Content-Type-Options and other key headers are absent.
- No Web Application Firewall (WAF) – Higher risk of automated attacks.
- No Regular Security Audits – No evidence of penetration testing or vulnerability scans being conducted periodically.

Business and Compliance Risks

Financial Risk – Failure to meet PCI DSS compliance increases the risk of credit card fraud and fines. A data breach could result in severe financial penalties and loss of business revenue.

Legal and Regulatory Risk – Non-compliance with GDPR could lead to fines. ISO 27001 and Cyber Essentials failures indicate a lack of proactive security measures, which can lead to legal repercussions in case of a breach.

Operational Risk – Security weaknesses increase downtime, create vulnerabilities to cyberattacks and weaken user trust. If an attacker exploits these weaknesses, customer data could be compromised, leading to loss of reputation and credibility.

Reputational Risk – Public disclosure of security breaches due to SQL injection, lack of encryption or CSRF exploitation could damage the company's reputation, leading to customer loss and negative media attention.

Summary of Key Findings:

- Critical Risks: SQL Injection, weak encryption, missing security controls.
- Moderate Risks: CSRF vulnerabilities, lack of security audits.
- Compliance Failures: GDPR and Cyber Essentials both fail key security checks.

Recommendations

High Priority (Immediate Action)

- Fix SQL Injection vulnerabilities (Implement parameterised queries). SQL injection is one of the most critical vulnerabilities and has been a leading attack vector in web applications for decades (OWASP, 2021)
- Enforce HTTPS (HSTS header, TLS enforcement).
- Implement Multi-Factor Authentication (MFA) for logins. MFA is one of the most effective ways to mitigate unauthorised access risks (NIST, no date).
- Add Security Headers (X-Frame-Options, Content-Security-Policy).
- Fix CSRF vulnerabilities (Implement CSRF tokens).

Medium Priority (Short-Term Fixes)

- Enable Secure Cookies (Secure and HttpOnly flags).
- Regular Penetration Testing and Security Audits.
- Harden session management policies.

Low Priority (Long-Term Improvements)

- Develop a GDPR-compliant Privacy Policy.
- Implement a Web Application Firewall (WAF).
- Train employees on security best practices.

Vulnerability	Risk Level	Recommendation
SQL Injection	High	Implement parameterised queries to mitigate SQL Injection risks.
Lack of HTTPS Enforcement	High	Enforce HTTPS using HSTS headers and strict TLS enforcement.
Lack of Multi-Factor Authentication (MFA)	High	Implement Multi-Factor Authentication (MFA) to enhance login security.
Missing Security Headers	High	Add security headers like X-Frame-Options and Content-Security-Policy.
Cross-Site Request Forgery (CSRF)	High	Implement CSRF tokens to prevent Cross-Site Request Forgery attacks.
Insecure Cookies	Medium	Enable Secure and HttpOnly flags for cookies to prevent exploitation.
Lack of Regular Security Audits	Medium	Conduct regular penetration testing and security audits.
Weak Session Management	Medium	Harden session management policies to prevent session hijacking.
Non-GDPR Compliant Privacy Policy	Low	Develop a GDPR-compliant Privacy Policy for regulatory adherence.
Lack of Web Application Firewall (WAF)	Low	Implement a Web Application Firewall (WAF) to filter malicious traffic.
Insufficient Employee Security Training	Low	Train employees on security best practices to reduce human error risks.

References

European Commission (no date) *General Data Protection Regulation (GDPR) 2016/679*. Available at: https://gdpr-info.eu/ (Accessed: 6 March 2025).

International Organization for Standardization (no date) *ISO/IEC 27001: Information Security Management Systems Requirements*. Available at: https://www.iso.org/standard/27001 (Accessed: 6 March 2025).

National Institute of Standards and Technology (no date) *Multi-Factor Authentication (MFA) Guidance for Small Businesses*. Available at: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication (Accessed: 6 March 2025).

Open Web Application Security Project (no date) *OWASP Top Ten Security Risks*. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 6 March 2025).

PCI Security Standards Council (no date) *Payment Card Industry Data Security Standard (PCI DSS)*. Available at: https://www.pcisecuritystandards.org/document_library/?document=pci_dss (Accessed: 6 March 2025).

Bibliography

Kali Linux (no date) *Kali Linux – Penetration Testing and Ethical Hacking Linux Distribution*. Available at: https://www.kali.org/ (Accessed: 6 March 2025).

Microsoft (no date) *nslookup*. Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup (Accessed: 6 March 2025).

Microsoft (no date) *tracert*. Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/tracert (Accessed: 6 March 2025).

Microsoft (no date) *Whois v1.20*. Microsoft Learn. Available at: https://learn.microsoft.com/en-us/sysinternals/downloads/whois#introduction (Accessed: 6 March 2025).

PortSwigger (no date) *SQL Injection*. Available at: https://portswigger.net/web-security/sql-injection (Accessed: 6 March 2025).

VirtualBox (no date) *VirtualBox – Open Source Virtualization Software*. Available at: https://www.virtualbox.org/ (Accessed: 6 March 2025).

Whois.com (no date) *WHOIS Lookup*. Available at: https://www.whois.com/whois/ (Accessed: 6 March 2025).

Amazon Web Services (no date) *Amazon EC2 Auto Scaling and Load Balancer Guide*. Available at: https://docs.aws.amazon.com/autoscaling/ec2/userguide/autoscaling-load-balancer.html (Accessed: 6 March 2025).