Executive Summary: Security Assessment and Compliance Review of the Gin and Juice Shop Website

Student Name: Lauren Pechey

Student ID: 12696823

Course: Masters of Computer Science

Module: Network Security Management

Professor: Beran Necat

Word Count: 1139

Submission Date: 21 July 2025

Executive Summary

This assessment aims to identify potential security vulnerabilities on the Gin and Juice Shop (GJS, https://ginandjuice.shop/), an e-commerce site created specifically for planned vulnerability testing. A combination of tools, including Nmap, Nikto, OWASP ZAP, Burp Suite Community, and Wfuzz, was used to carry out the scans. The goal was to detect weaknesses in secure configuration, data handling, and access control that may pose risks to customers' personal data and the organisation's compliance. This includes adherence to modern guidelines including the General Data Protection Regulation (European Union, 2016) and the International Organisation for Standardisation/ International Electrotechnical Commission 27001 (ISO, 2022). This report summarises the main findings, evaluates the site's security posture against these standards, and outlines prioritised recommendations to address the identified risks.

Methodology:

As mentioned, the security assessment combined automated scanning and manual inspection using a suite of specialised tools. Nmap was employed for enumerating open ports and identifying running services to detect unnecessary or exposed network points (Nmap Project, 2025).

Nikto scanned the web server for outdated software and misconfigurations that could lead to known vulnerabilities (Sullo, 2025). OWASP Zed Attack Proxy (ZAP) and Burp Suite Community Edition focused on uncovering security flaws in web applications, including cross-site scripting (XSS), missing security headers, and session management weaknesses, with Burp Suite enabling manual verification of findings (OWASP, 2025; PortSwigger, 2025). Wfuzz was employed for fuzz testing, which uncovered accessible authentication endpoints and restricted admin paths by probing common and predictable URL patterns (Edge-Security, 2025).

The assessment was non-intrusive, with time constraints and the possibility of false positives acknowledged, necessitating further manual validation where appropriate. Each tool produced evidence in the form of screenshots and logs. The most significant findings from these scans are summarised in the following section, with detailed outputs stored in appendices.

Summary of Findings

To provide clearer and more focused analysis, the vulnerability findings have been organised into two separate tables. Figure 1 presents results from network and server-level scanners, while Figure 2 focuses on application-level tools (Burp Suite, Wfuzz, and OWASP ZAP), highlighting web application vulnerabilities and potential attack vectors. The raw results are included in the appendices at the end of the document.

Tool	Vulnerability Findings	Risk Level	Business Impact
nMap	Detected open services on HTTP (port 80) and HTTPS (port 443), running nginx and AWS Elastic Load Balancer.	Low	Acceptable if properly configured and patched; unencrypted HTTP traffic (port 80) may expose data or invite downgrade attacks if not redirected to HTTPS (Kharat & Chawan, 2022).
nMap	Indications of Cross-Site Request Forgery (CSRF) issues within multiple web forms under /catalog paths detected (Kollepalli et al., 2024).	Medium	CSRF vulnerabilities may enable attackers to carry out unauthorised actions while impersonating authenticated users, risking data integrity and user trust (Kollepalli et al., 2024).
Nikto	Missing Strict-Transport-Security & X-Content-Type-Options headers; Cookies without Secure & HttpOnly flags	High	Weakens protection against MITM attacks and session hijacking. Browsers may incorrectly handle content types, increasing XSS risk (Chaturvedi et al., 2024).
Nikto	Possible BREACH Attack Exposure (Content-Encoding: deflate)	Medium	Attackers may exploit compression to recover secret data over encrypted connections, risking data leakage (Umamageswari & Deepa, 2023).
Nikto	Cookies AWSALB and AWSALBCORS Missing Secure and HttpOnly Flags	Medium	Cookies without Secure and HttpOnly flags can be intercepted or accessed by client-side scripts, risking session hijacking (Kharan & Chawan, 2022).

Figure 1: nMap and Nikto vulnerability findings and business impact

Tool	Vulnerability Findings	Risk Level	Business Impact
OWASP ZAP	Absence of Anti-CSRF Tokens & Weak Session Management: Multiple forms lack CSRF tokens and session controls may be weak.	Medium	Attackers could perform unauthorized actions or hijack sessions, risking user accounts, transactions, and business reputation (Sllame et al., 2024).
OWASP ZAP	Missing Security Headers & Insecure Cookies: No CSP, Strict-Transport-Security, or X-Content-Type-Options headers. Cookies lack HttpOnly, Secure, or SameSite flags.	High	Increases risk of XSS, data leakage, or downgrade attacks. Weak cookie security could expose sessions to interception or manipulation (Al Anhar & Suryanto, 2021).
OWASP ZAP	Vulnerable JavaScript Library Detected: Site uses an outdated JS library with known vulnerabilities.	High	Attackers may exploit old JS to run malicious scripts or bypass controls, putting user data and site integrity at risk (Maniraj et al., 2024).
Burp Suite Community	Intercepted a login POST request: confirmed CSRF token is present but passwords are transmitted in plain POST data (protected by HTTPS).	Info	Standard practice but storing or logging POST bodies insecurely could risk credentials exposure. CSRF token helps prevent forgery attacks (Jose et al., 2023).
Burp Suite Community	Intercepted a POST request to /catalog/cart with parameters productId=2, redir=PRODUCT, and quantity=1. Request uses HTTPS and includes session and tracking cookies.	Info	Standard e-commerce add-to-cart action; if no CSRF token is present, could be vulnerable to CSRF attacks (Gandikota et al., 2023).
Wfuzz	Admin/admin/ADMIN paths returning 403 Forbidden	High	These admin areas are highly sensitive targets. Although access is restricted, any security flaws could allow unauthorized entry, potentially compromising the entire system (Raghu Vamsi & Jain, 2021).
Wfuzz	Accessible sensitive pages like Login, My-account, Logout	High	These endpoints manage user credentials and personal information. If not properly secured, they could be exploited to gain unauthorized access or expose confidential data (Ibrahim & Rosli, 2023).

Figure 2: Burp Suite, Wfuzz, and OWASP ZAP vulnerability findings and business impact

The vulnerability assessment employed a layered scanning approach combining network and application-level tools to identify security weaknesses. Network scans with nMap revealed open HTTP (port 80) and HTTPS (port 443) services, along with missing security headers such as Strict-Transport-Security and X-Content-Type-Options (Kharan & Chawan, 2022). These gaps increase the risk of downgrade attacks, man-in-the-middle (MITM) interception, and cross-site scripting (XSS) (Kollepalli et al., 2024).

Nikto confirmed missing Secure and HttpOnly cookie flags, and the use of deflate content encoding suggested susceptibility to BREACH attacks (Chaturvedi et al., 2024). Application-level scanning with tools like OWASP ZAP, Burp Suite, and Wfuzz revealed exposed login and admin endpoints that could be leveraged for unauthorised access attempts (Al Anhar & Suryanto, 2021). The discovery of accessible authentication and administrative paths indicates potential risks for privilege escalation and credential misuse if security controls are inadequate (Ibrahim & Rosli, 2023). Overall, these findings highlight gaps in access controls and configuration that need to be strengthened to reduce the risk of exploitation.

Evaluation against Security Standards

Evaluation Against GDPR

The identified vulnerabilities present significant challenges to GDPR compliance, particularly concerning the protection of data from the outset and as standard. The open HTTP port without enforced HTTPS redirection risks unencrypted data transmission, violating Article 32’s mandate for appropriate technical security controls to protect data confidentiality and accuracy (European Union, 2016). Similarly, missing security headers and outdated software components demonstrate insufficient risk mitigation and accountability measures (Haddara et al., 2023). Injection vulnerabilities and weak authentication mechanisms threaten the confidentiality and integrity of personal data, increasing the likelihood of breaches that require timely notification to supervisory

authorities (Agabmoro, 2019). The findings underscore a lack of continuous monitoring and incident response capabilities, further undermining GDPR's principles (Haddara et al., 2023). Organisations must therefore enhance cybersecurity controls and incident management to uphold data subject rights and regulatory obligations.

Evaluation Against ISO/IEC 27001

From an ISO/IEC 27001 perspective, the vulnerabilities indicate non-conformance with key controls, including access control (A.9), cryptography (A.10), and system development and maintenance (A.14) (ISO, 2022). The absence of enforced encryption on HTTP traffic violates cryptographic control requirements (A.10.1), while missing security headers and outdated components contravene secure system development practices (A.14.2) (ISO, 2022; Putra et al., 2021). Injection flaws and weak authentication mechanisms reveal insufficient enforcement of access controls (A.9.1) and authentication processes (A.9.4) (Suorsa & Helo, 2023). Additionally, the findings suggest gaps in vulnerability assessment and treatment procedures (A.12.6), essential for timely risk mitigation (Suorsa & Helo, 2023). To comply, organisations must strengthen their ISMS by integrating robust vulnerability management, patching, and monitoring aligned with ISO/IEC 27001 standards.

Conclusions

The vulnerability assessment of the GJS site demonstrates that it currently exhibits multiple weaknesses that could be exploited to gain unauthorised access, compromise sensitive data, or disrupt business operations. The findings reveal recurring issues, such as missing critical security headers, weak session and cookie management, the absence of robust CSRF protections, and the exposure of sensitive resources like backup files and administrative panels.

These security gaps demonstrate weak alignment with industry standards. As has been discussed, GDPR Article 32 Mandates that organisations apply suitable technical and organisational safeguards to secure personal data, while ISO/IEC 27001 sets out best practices for securing information assets. If not addressed, these vulnerabilities could lead to regulatory breaches, reputation damage, and significant financial consequences in the event of data loss or compromise (Gandikota et al., 2023). It is therefore essential that the organisation adopts a proactive approach to secure configuration, access control, secure coding practices, and continuous monitoring to maintain a security posture that matches the evolving threat landscape.

Recommendations

To mitigate the identified risks and achieve compliance with GDPR and ISO/IEC 27001, it is strongly recommended that the organisation prioritises the resolution of high-impact issues first, followed by medium and low-risk improvements. The measures should focus on eliminating easy-to-exploit exposures, strengthening session management, enforcing modern security headers, and ensuring that backup files and sensitive directories are never accessible via brute-force methods (Moric et al., 2024).

The table below outlines the recommended actions in priority order, linking each measure to the main business impact and reason for its urgency.

Priority	Recommendation	Rationale and Benefit
High	Remove or restrict access to the hidden admin panel (/admin/) by enforcing strong authentication, IP allowlisting, and monitoring.	Reduces the risk of unauthorised privileged access and potential full system takeover (Agabmoro, 2019).
High	Delete exposed backup files (/backup.zip) from the web root or store them in a secure, access-controlled location with encryption.	Prevents unauthorised access to sensitive system or customer data, mitigating data breach risk (Verizon, 2025).

High	Implement essential HTTP security headers such as Strict-Transport-Security (HSTS), Content Security Policy (CSP), and X-Content-Type-Options (Egho-Promise et al., 2024).	Strengthens defences against downgrade attacks, MITM interception, and cross-site scripting (XSS) (Egho-Promise et al., 2024).
Medium	Enforce Secure, HttpOnly, and SameSite attributes on all cookies, especially session cookies.	Mitigates session hijacking risks and enhances user privacy during transmission.
Medium	Add and verify anti-CSRF tokens for all forms that modify user or system data.	Blocks attackers from performing unauthorised actions on behalf of authenticated users (Kollepalli et al., 2024).
Medium	Remove or update any outdated JavaScript libraries to the latest supported versions.	Closes known security holes that could be exploited through vulnerable front-end components (Egho-Promise et al., 2024).
Low	Redirect all HTTP traffic on port 80 to HTTPS by default and ensure TLS certificates are up to date.	Ensures encrypted communication and protects credentials and session data in transit (Kharan & Chawan, 2022).

In summary, timely implementation of these recommendations will significantly reduce the site's risk profile, strengthen its compliance with regulatory and best practice standards (OWASP, 2024; ISO, 2022), and improve customer trust in the security of its online services. Continuous testing, patching, and monitoring should also be embedded into the organisation's ongoing operations to sustain this improved posture over time.

References:

Agabmoro, H. (2019) *Software Testing, Data Security and GDPR*. Master's thesis, University of South-Eastern Norway. Available from: https://openarchive.usn.no/usn-xmlui/bitstream/handle/11250/2644673/masterAgabmoro2019.pdf?sequence=1 [Accessed 18 Jul 2025].

Al Anhar, A., & Suryanto, Y. (2021) 'Evaluation of web application vulnerability scanner for modern web application', *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*, Yogyakarta, Indonesia, 15–17 November. pp. 200–204.

Chaturvedi, A., Lakhani, B., Agarwal, T., Mohana, M., Moharir, M. & Kumar, A. (2024) 'A comprehensive vulnerability tools analysis for security and control in IT environment and organizations', *2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, Coimbatore, India, 10–12 January. pp. 612–618.

Edge-Security. (2025) *Wfuzz user guide: advanced usage*. Available from: https://wfuzz.readthedocs.io/en/latest/user/advanced.html [Accessed 16 July 2025].

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

European Union. (2016) *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data*

Protection Regulation). Official Journal of the European Union, L119: 1–88. Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 16 July 2025].

Gandikota, P., Valluri, D., Mundru, S., Yanala, G., & Sushaini, S. (2023) Web application security through comprehensive vulnerability assessment. *Procedia Computer Science* 230(1): 168–182.

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.

Ibrahim, R., & Rosli, M. (2023) 'Evaluation of web application vulnerability scanners using SQL injection attacks', *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*. Kuala Lumpur, Malaysia, 1–6 December. IEEE. 1–6.

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 16 Jul 2025].

Jose, L., Khanna, M. R., Meganathan, D. & Praveen Kumar, B. T. (2023) Web based parameter-tampering on shopping site using BurpSuite testing', in Hiranwal, S. & Mathur, G. (eds.) *Artificial Intelligence and Communication Technologies*. Computing & Intelligent Systems, SCRS, India. 527–535. DOI: https://doi.org/10.52458/978-81-955020-5-9-51

Kharat, P., & Chawan, P. (2022) Vulnerability Management System. *International Research Journal of Engineering and Technology* 9(9): 976–981. DOI: https://doi.org/10.5281/ZENODO.7092162

Kollepalli, R., Reddy, M., Sai, B., Natarajan, A., Mathi, S. & Ramalingam, V. (2024) An Experimental Study on Detecting and Mitigating Vulnerabilities in Web Applications. *International Journal of Safety and Security Engineering* 14(2): 523–532. DOI: https://doi.org/10.18280/ijsse.140219

Maniraj, S., Ranganathan, C., & Sekar, S. (2024) Securing web applications with OWASP ZAP for comprehensive security testing. *International Journal of Advanced Signal and Image Sciences* 10(2): 12–23. Available from: https://xlescience.org/index.php/IJASIS/article/view/175/119

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

Nmap Project. (2025) *Nmap: Network Mapper*. Available from: https://nmap.org/ [Accessed 16 July 2025].

OWASP. (2024) *OWASP Web Security Testing Guide (WSTG)*. Available from: https://owasp.org/www-project-web-security-testing-guide/ [Accessed 16 Jul 2025].

OWASP. (2025) *OWASP Zed Attack Proxy (ZAP)*. Available from: https://www.zaproxy.org/ [Accessed 16 July 2025].

PortSwigger. (2025) *Burp Suite Professional*. Available from: https://portswigger.net/burp [Accessed 16 July 2025].

Putra, D., Tistiyani, S., & Sunaringtyas, S. (2021) 'The use of ISO/IEC 27001 family of standards in regulatory requirements in some countries', 2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev), Jogjakarta, Indonesia, pp. 1-6.

Raghu Vamsi, P. & Jain, A. (2021) Practical security testing of electronic commerce web applications. *International Journal of Advanced Networking and Applications* 13(1): 4861–4873.

Sllame, A., Tomia, T., & Rahuma, R. (2024) 'A holistic approach for cyber security vulnerability assessment based on open source tools', *2024 IEEE 4th International Maghreb Meeting (MI-STA)*, Tripoli, Libya, pp. 68-75.

Sullo, C. (2025) *Nikto Web Server Scanner*. Available from: https://cirt.net/Nikto2 [Accessed 16 July 2025].

Suorsa, M., & Helo, P. (2023) Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A Global Perspective*, 33(3): 285–306. DOI: 10.1080/19393555.2023.2270984.

Umamageswari, & Deepa, S. (2023) 'Vulnerability Assessment in Contemporary Computing', in: Kumar, R. & Pattnaik, P.K. (eds) *Risk Detection and Cyber Security for the Success of Contemporary Computing*. Hershey: IGI Global, 28.

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

Appendices:

Appendix A: Nmap Detailed Output

```
laurhen@Laurens-MacBook-Pro ~ % sudo nmap -sV ginandjuice.shop

Password:
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-18 20:05 +0200
Nmap scan report for ginandjuice.shop (34.246.169.176)
Host is up (0.20s latency).
Other addresses for ginandjuice.shop (not scanned): 34.249.203.140
rDNS record for 34.246.169.176: ec2-34-246-169-176.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.75 seconds
```

Figure A1: N Nmap Service and Version Detection Scan

```
laurhen@Laurens-MacBook-Pro ~ % sudo nmap --script ssl-cert,ssl-enum-ciphers -p 443 ginandjuice.shop

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-18 20:10 +0200
Nmap scan report for ginandjuice.shop (34.249.203.140)
Host is up (0.20s latency).
Other addresses for ginandjuice.shop (not scanned): 34.246.169.176
rDNS record for 34.249.203.140: ec2-34-249-203-140.eu-west-1.compute.amazonaws.com

PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=ginandjuice.shop
| Subject Alternative Name: DNS:ginandjuice.shop, DNS:*.ginandjuice.shop
| Issuer: commonName=Amazon RSA 2048 M03/organizationName=Amazon/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-12-22T00:00:00
| Not valid after:  2026-01-21T23:59:59
| MD5:     4a1a 10fa 9783 432e f7af 0299 681b 595a
| SHA-1:   91e8 a48e 7700 bd77 3015 f5d7 06fe f22f df73 ea56
|_SHA-256: 016f 15f9 5eee 5346 3388 609a 4960 5a3f d3a1 c795 9cbb c36d ac7e 656d 599e a881
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A

Nmap done: 1 IP address (1 host up) scanned in 12.41 seconds
```

Figure A2: SSL/TLS cipher output

```
laurhen@Laurens-MacBook-Pro ~ % sudo nmap -A ginandjuice.shop

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-18 20:15 +0200
Nmap scan report for ginandjuice.shop (34.249.203.140)
Host is up (0.20s latency).
Other addresses for ginandjuice.shop (not scanned): 34.246.169.176
rDNS record for 34.249.203.140: ec2-34-249-203-140.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
|_http-server-header: awselb/2.0
|_http-title: Did not follow redirect to https://ginandjuice.shop:443/
443/tcp open  ssl/http AWS Elastic Load Balancing
|_http-title: Home - Gin &amp;amp; Juice Shop
| ssl-cert: Subject: commonName=ginandjuice.shop
| Subject Alternative Name: DNS:ginandjuice.shop, DNS:*.ginandjuice.shop
| Not valid before: 2024-12-22T00:00:00
|_Not valid after:  2026-01-21T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   14.43 ms  192.168.100.1
2   15.92 ms  gpon-willowvale-transit-asr.zol.co.zw (197.211.213.165)
3   38.28 ms  41.173.56.17
4   35.15 ms  gi-1-1-0.lza-p1-rr-jhb.liquidtelecom.net (46.17.232.64)
5   34.64 ms  gi-5-0-1.lzw-p1-msv.liquidtelecom.net (46.17.232.111)
6   31.84 ms  41.175.223.170
7   ... 11
12  193.73 ms ec2-34-249-203-140.eu-west-1.compute.amazonaws.com (34.249.203.140)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.73 seconds
```

Figure A3: Aggressive Scan Output

```
laurhen@Laurens-MacBook-Pro ~ % sudo nmap -sV --script=default ginandjuice.shop
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-18 20:17 +0200
Nmap scan report for ginandjuice.shop (34.246.169.176)
Host is up (0.21s latency).
Other addresses for ginandjuice.shop (not scanned): 34.249.203.140
rDNS record for 34.246.169.176: ec2-34-246-169-176.eu-west-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://ginandjuice.shop:443/
|_http-server-header: awselb/2.0
443/tcp open  ssl/http AWS Elastic Load Balancing
|_http-title: Home - Gin &amp;amp; Juice Shop
| ssl-cert: Subject: commonName=ginandjuice.shop
| Subject Alternative Name: DNS:ginandjuice.shop, DNS:*.ginandjuice.shop
| Not valid before: 2024-12-22T00:00:00
|_Not valid after:  2026-01-21T23:59:59

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.89 seconds
```

Figure A4: nMap with script default output

Appendix B: Nikto Detailed Output

```
laurhen@Laurens-MacBook-Pro ~ % sudo nikto -h https://ginandjuice.shop/ -output nikto_report.txt

Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 34.249.203.140, 34.246.169.176
+ Target IP:          34.249.203.140
+ Target Hostname:    ginandjuice.shop
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=ginandjuice.shop
                   Altnames: ginandjuice.shop, *.ginandjuice.shop
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time:         2025-07-15 18:35:32 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Uncommon header 'x-backend' found, with contents: 5627c4f1-ddb0-4f5b-8722-0b627141ab68.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://dev
eloper.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the cont
ent of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerab
ility-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie AWSALB created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web
/HTTP/Cookies
+ /: Cookie AWSALB created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/W
eb/HTTP/Cookies
+ /: Cookie AWSALBCORS created without the httponly flag. See: https://developer.mozilla.org/en-US/do
cs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to
the BREACH attack. See: http://breachattack.com/
+ OPTIONS: Allowed HTTP Methods: GET .
+ 7961 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-07-15 20:27:19 (GMT2) (6707 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure B1: Nikto basic report

```
laurhen@Laurens-MacBook-Pro ~ % sudo nikto -h https://ginandjuice.shop/ -Tuning 1234567 -output nikto_full_report.txt
Password:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 34.246.169.176, 34.249.203.140
+ Target IP:          34.246.169.176
+ Target Hostname:    ginandjuice.shop
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=ginandjuice.shop
                   Altnames: ginandjuice.shop, *.ginandjuice.shop
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time:         2025-07-16 12:36:49 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: Uncommon header 'x-backend' found, with contents: fae8b994-7be4-4847-99d5-b5eefdeb5aed.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie AWSALB created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie AWSALB created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie AWSALBCORS created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ OPTIONS: Allowed HTTP Methods: GET .
+ 4357 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-07-16 13:39:18 (GMT2) (3749 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure B2: Nikto deep scan report

Appendix C: OWASP ZAP Application Scan Results

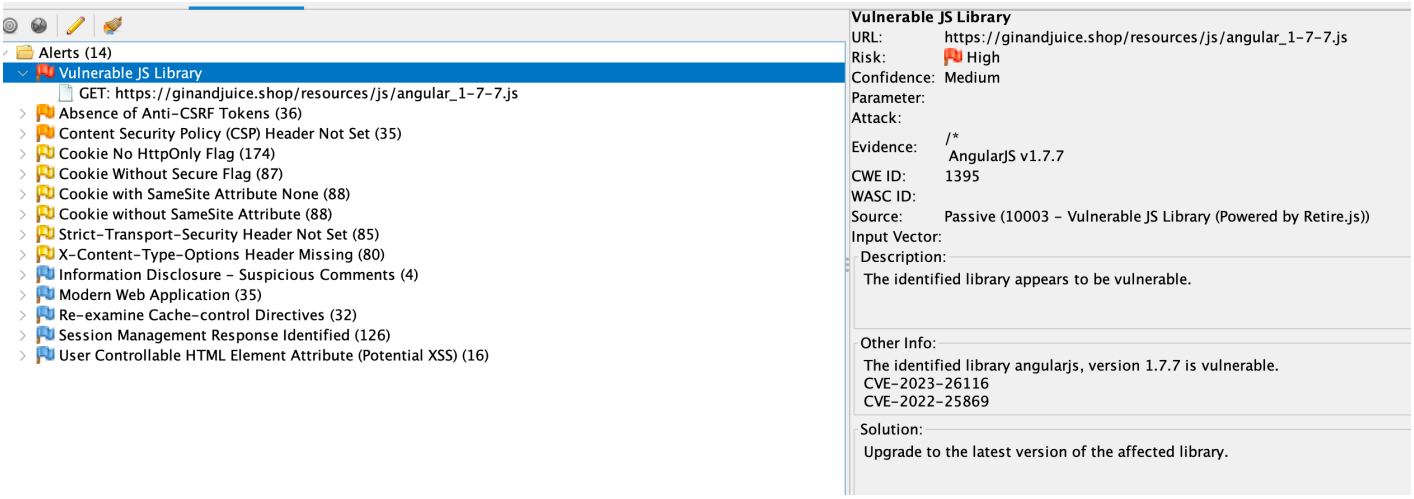

Figure C1: ZAP detection of Vulnerable JS Library

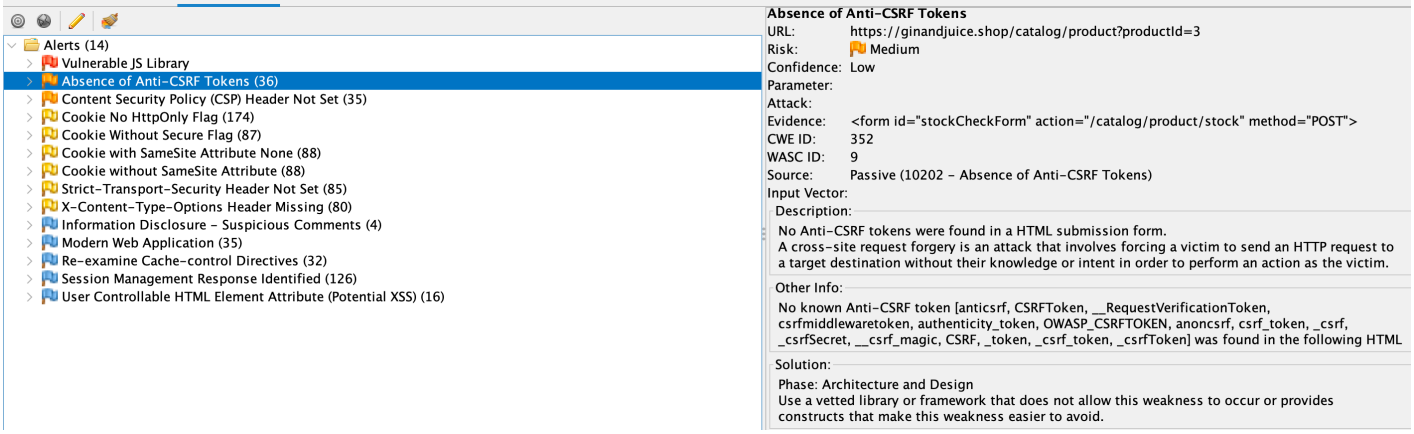

Figure C2: ZAP detection of Absent CSRF Tokens

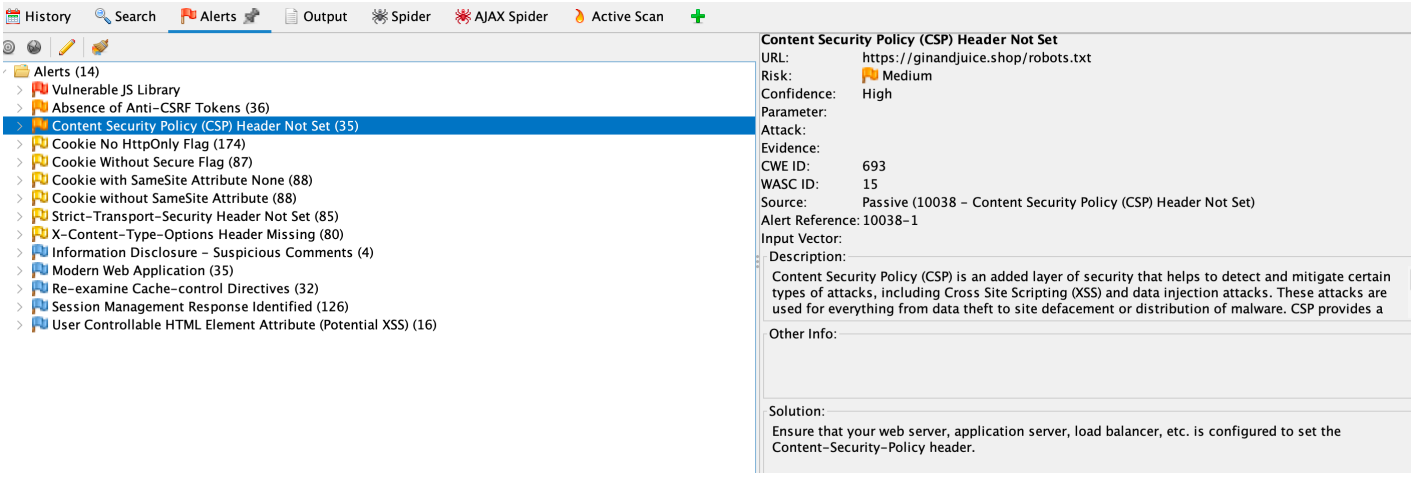

Figure C3: ZAP detection of Content Security Header not set

Appendix D: Burpsuite Community Edition Scans

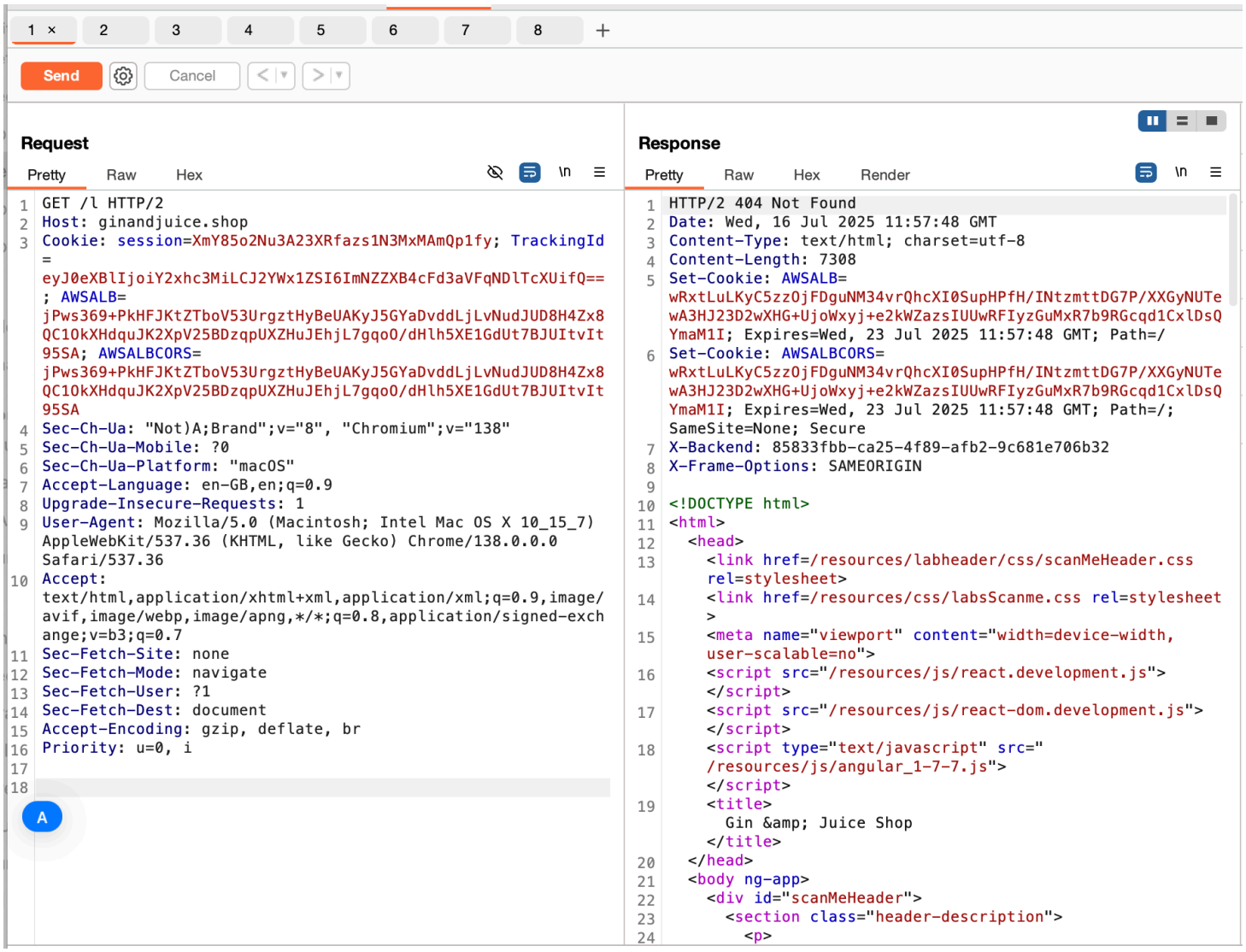

Figure D1: Burpsuite showing repeater request and response of home page

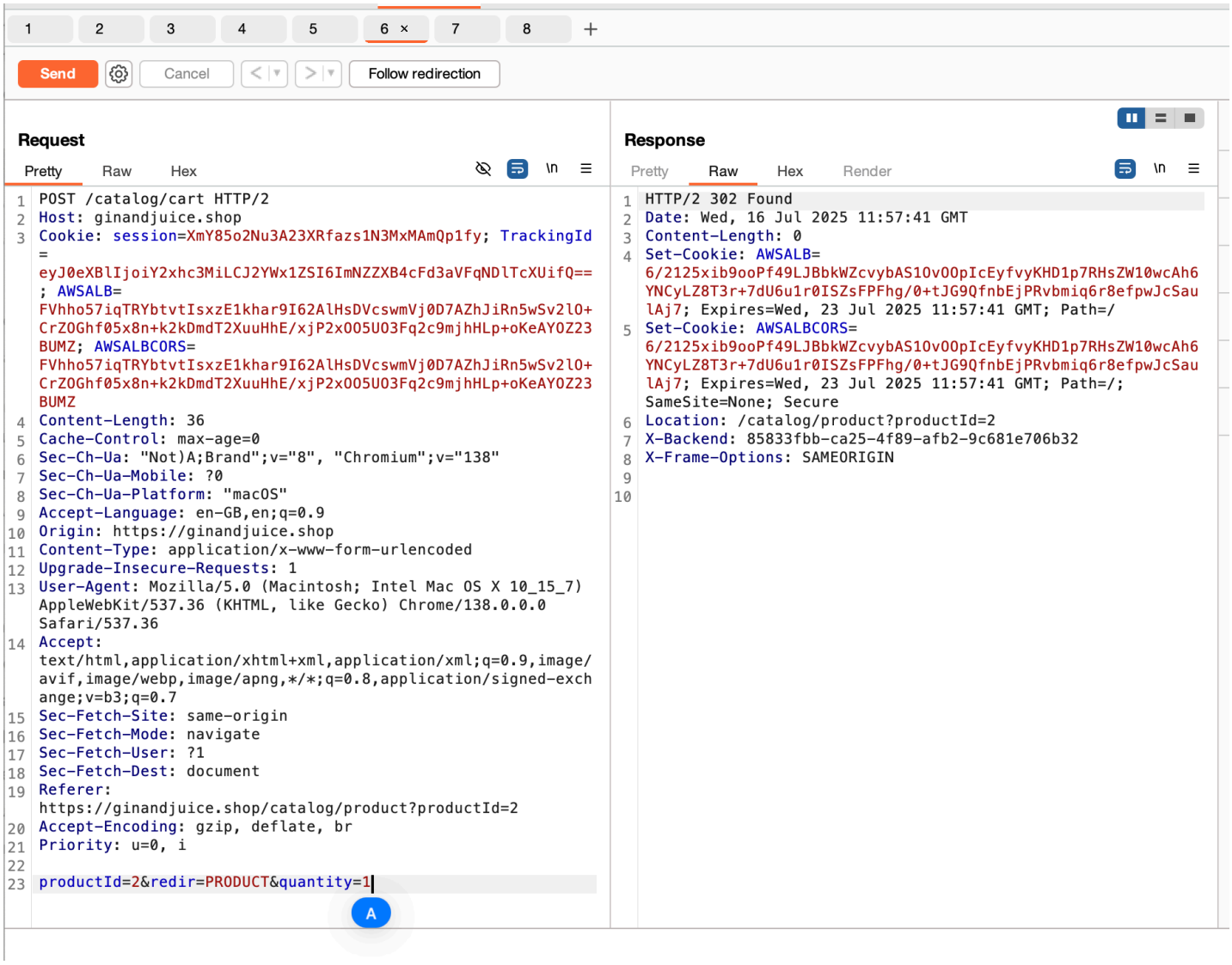

Figure D2: Burpsuite showing repeater request and response of cart page

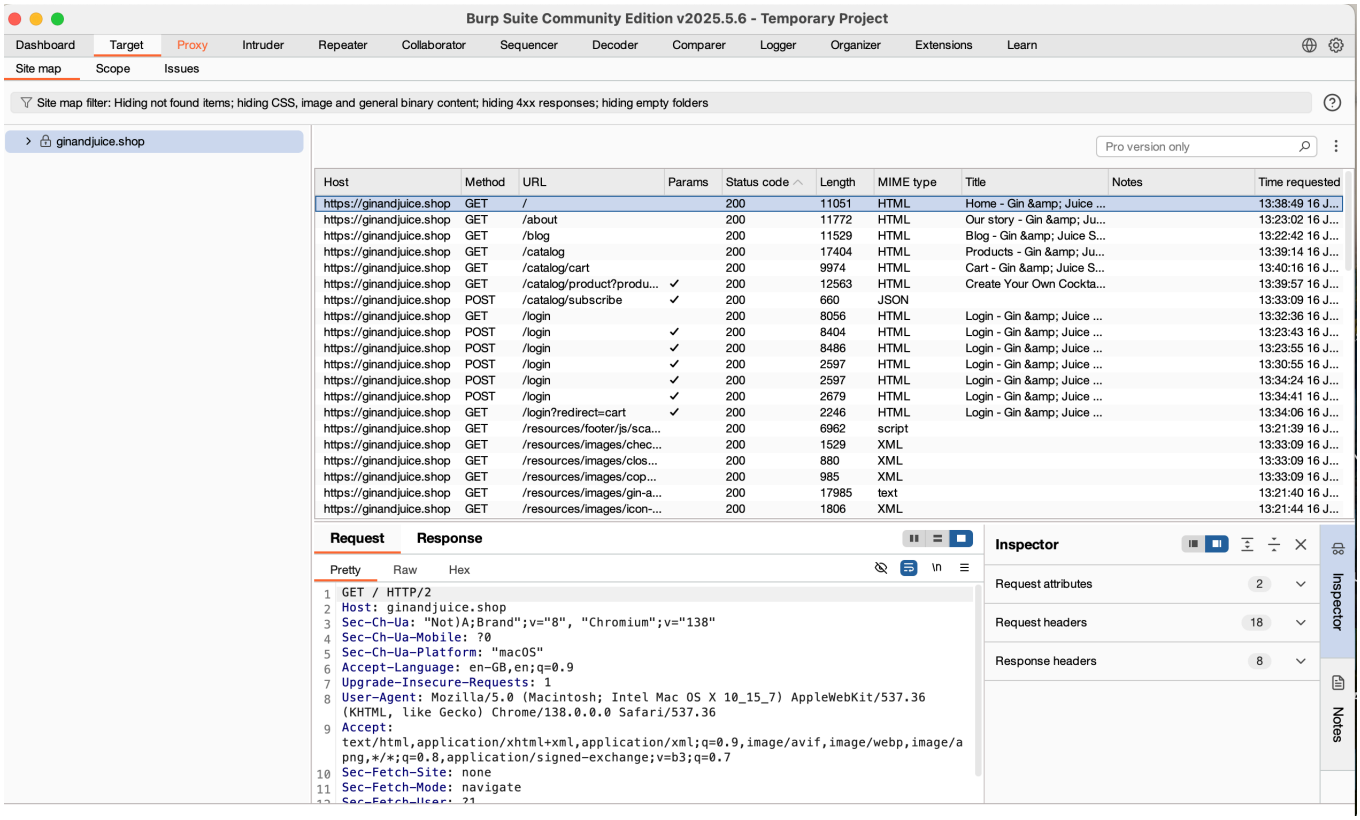

Figure D3: BurpSuite Sitemap of GJS

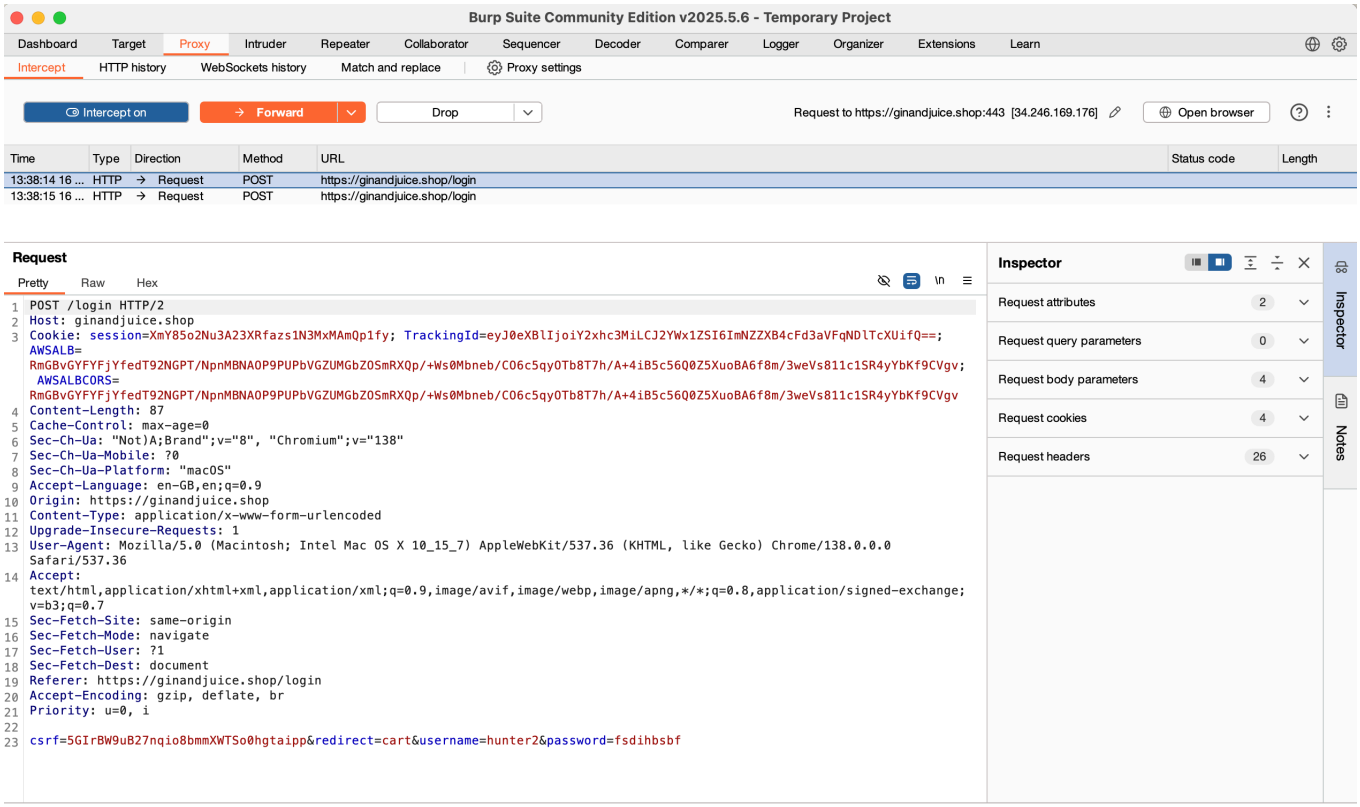

Figure D4: BurpSuite Proxy Interception of GJS

Appendix E: Wfuzz scan results of GJS site

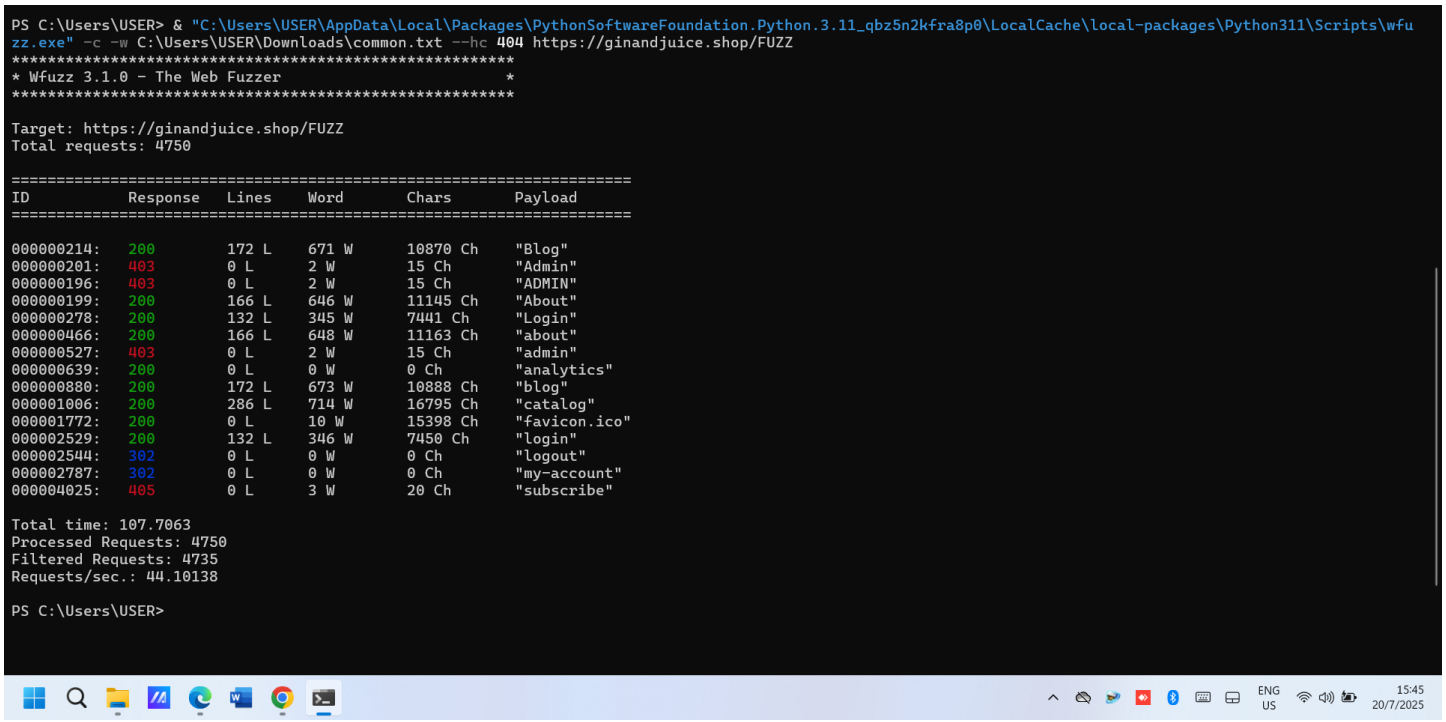

Figure E1: WFuzz Commonlist scan of GJS site