**RESULTS AND EXECUTIVE SUMMARY**

**Introduction**

The website ginandjuice.shop has undergone a comprehensive security assessment, identifying issues affecting its confidentiality, integrity and availability. Section I will detail the black-box methodology used for the security assessment. Section II will detail the identified security risks found during the scanning. The risks will be ranked according to the DREAD threat model in section III. The website will be compared to industry security standards in section IV, and section V will summarise the data, providing recommendations for remedying vulnerabilities.

**I. Methodology and limitations**

The assessment utilised a black-box methodology with the Kali Linux operating system, “renowned for its specialized focus on penetration testing, computer forensics and security auditing” (Akhtar, 2024). ZAP was used to identify vulnerabilities associated with the OWASP Top Ten, a framework highlighting web applications' most critical security risks (OWASP, 2021).

As the NCSC (2024) states, this methodology effectively models an attacker’s perspective of the site. However, with limited awareness of the website’s internals, such as access to server rooms and hardware security, website owners are encouraged to conduct a white-box test to verify all assets (human, web and physical) and internal processes.

Furthermore, whilst the open-source nature of these tools helped minimise costs for the security assessment, the limitations imposed by being free restricted their depth of analysis. This had to be overcome by manual testing and human intuition. For future assessments, using fully licensed versions such as BurpSuite Professional, which offers improved features such as built-in payloads (Wear, 2023), will provide a more comprehensive view of the security issues associated with the website.

**II. Scanning Results**

**Automated Scanning Results**

As Figure One (below) illustrates, the automated ZAP scan found multiple issues with various levels of risk.

A blue rectangular object with text

Description automatically generated

*Figure One (Above): The various degrees of risk found by the ZAP scan.*

High-risk areas include cross-site scripting (XSS), one of the most severe and common web attacks that uses malicious payloads to execute code (Wang, 2024). XSS risks are heightened with the no HttpOnly flag set on cookies, meaning session high-jacking is also possible (Nidecki, 2020).

There was a lack of cross-site request forgery tokens, a protection against an attack that can force users to submit an HTTP request to a destination without their intent, potentially causing accounts to be taken over (Yaworski, 2019). The scan demonstrated that the website uses the outdated framework AngularJS, which increases the risk of exploitation because it is no longer patched (AngularJS, 2022).

**Manual Scanning Results**

BurpSuite showed that credentials were being sent in plaintext. This significantly increases the risk of theft and data breaches. Website areas are also susceptible to SQL injection attacks, which attackers use to extract information from databases (Yaworski, 2019). Fraudsters have used this attack to gain vast amounts of sensitive data, such as credit card information (Haworth, 2018).

A Nikto scan showed ginandjuice.shop was susceptible to a BREACH attack, a vulnerability in which an attacker may gain the credentials of a legitimate user and impersonate them (Trace Security, 2023).

The identified security risks align with many of the categories in the OWASP Top Ten. Figure Two (below) indicates a high-risk profile for ginandjuice.shop. Half of the Top Ten are identified on the website, highlighting the urgency to address these issues to protect user data and comply with security standards.

A diagram of a computer code

Description automatically generated with medium confidence

*Figure Two (Above): The risks mapped to categories in the OWASP Top Ten*

**III. Categorising The Risk**

Whilst not as thorough as other models such as PASTA, which requires a high level of expertise to implement (Hiremath, N.D.), DREAD allows a critical evaluation of the security risks and an easy-to-understand assessment of where the business should dedicate its time and finances. It assesses risks based on their damage potential, reproducibility, exploitability, affected users, and discoverability (Olmsted, 2024). Each risk is given a score of one to ten per category, and an average score is then taken. The DREAD model is shown in the Table Two below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Threat | D | R | E | A | D | Average |
| Cryptographic Failures | 8 | 6 | 7 | 8 | 5 | 6.8 |
| Injection | 9 | 9 | 9 | 8 | 9 | 8.8 |
| Outdated Components | 7 | 5 | 8 | 7 | 6 | 6.6 |
| Security Misconfiguration | 7 | 6 | 7 | 6 | 6 | 6.4 |
| Broken Access Control | 9 | 7 | 8 | 9 | 6 | 7.8 |

*Table Two (Above): Each risk mapped against the DREAD threat model*

Injection has been ranked the most critical. This is due to the risk of unauthorised database access, potentially affecting all users. SQL injection attacks are also relatively easy to perform, with freely available tools like Sqlmap on Kali Linux easing the process (Kali, N.D.).

Broken access control is ranked next, with high damage potential due to possible unauthorised information disclosure.

Cryptographic failures were ranked third. While the damage potential is high, reproducibility and discoverability are significantly more difficult. They also indicate a failure of specific industry standards, which will be discussed in the next section.

Outdated system components were ranked fourth because of their high damage potential and reproducibility of exploits. Vulnerable software exploits are freely available online and can be found on websites such as ExploitDB (Offsec, N.D.).

Finally, security misconfiguration is ranked last. The cookies issue has a moderate impact, and it is easily rectified. This will be explained in the final section.

**IV. Comparison Against Standards**

These issues indicate a severe failure of industry standards. One example standard is the General Data Protection Regulation (GDPR), which covers strict user data protections (Demirer, 2024). The website is failing in its GDPR commitments, with an elevated risk of a data breach due to plaintext credentials, cryptographic failures, and injection vulnerabilities. This could lead to significant financial and reputational damage, a real-life example being when British Airways was fined a record amount for a data breach in 2018 (BBC, 2020).

Another standard the website needs to improve is the Payment Card Industry Data Security Standard (PCI DSS), a set of requirements imposed on merchants handling cardholder data (Hancock, 2024). This is because of the high rate of cryptographic failures, indicating a lack of protection for sensitive data (Archondakis, N.D.).

**V. Summary of Conclusions and Recommendations**

Figure Three (below) graphically represents the website’s priorities to improve its security standing.

*Figure Three (Above): A hierarchy of priorities for the website to improve*

Injection is the most critical and can be avoided using “prepared statements”, sanitising inputs, or inputting a web application firewall (CloudFlare, N.D.).

Broken Access Control is the next most critical issue. It can be remedied by taking a defence-in-depth approach, using the principle of least privilege, and regularly auditing and testing access controls (Portswigger, N.D.).

The third most critical area to focus on is Cryptographic Failures. Sensitive data must be stored using hashing methods such as SHA-256 instead of plaintext (Clinton, 2023). This will reduce the risk of a data breach and attackers stealing sensitive data.

Vulnerable and Outdated Components ranked fourth. Regular updates and patches are vital to ensure the software is free from exploitation (NCSC, 2019). Website owners must find more recent frameworks and retire AngularJS.

Finally, security misconfiguration can be rectified by ensuring cookies have the HttpOnly flag set. Multifactor authentication is recommended as a further security measure, providing robust measures against repudiation threats (IBM, 2024).

**Conclusion**

There are many areas ginandjuice.shop must improve to strengthen their security standing. Most of the identified OWASP Top Ten highlight a high-risk profile. The website is failing its GDPR and PCI DSS requirements, which could lead to reputational, legal and financial challenges. By taking on board the advice and implementing the mitigating strategies provided, ginandjuice.shop will avoid legal issues and guarantee a strong security posture for the future.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**References**

* Akhtar, Z. B., & Rawol, A. T. (2024). Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective. *International Journal of Advanced Network, Monitoring, and Controls* 9(2):11–22. DOI: https://doi.org/10.2478/ijanmc-2024-0012
* AngularJS. (2022) Version Support Status. Available from: <https://docs.angularjs.org/misc/version-support-status> [Accessed 29 August 2024].
* Archondakis, A. (N.D.) OWASP Top Ten: Cryptographic Failures. Available from: <https://www.pentestpeople.com/blog-posts/owasp-top-ten-cryptographic-failures#:~:text=What%20is%20Cryptographic%20Failure%3F,cause%20of%20sensitive%20data%20exposure>. [Accessed 09 September 2024].
* BBC. (2020) British Airways fined £20m over data breach. Available from: <https://www.bbc.co.uk/news/technology-54568784> [Accessed 08 August 2024].
* Clinton, D. (2023) *LPI security essentials study guide : exam 020-100*. Hoboken, New Jersey: John Wiley & Sons, Inc. Available from: <https://learning.oreilly.com/library/view/lpi-security-essentials/9781394196531/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 09 September 2024].
* CloudFlare. (N.D.) How to prevent SQL injection. Available from: <https://www.cloudflare.com/en-gb/learning/security/threats/how-to-prevent-sql-injection/> [Accessed 29 August 2024].
* Demirer, M., Hernandez, J., Li, D. & Peng, S. (2024) *Data, Privacy Laws and Firm Production: Evidence from the GDPR*. Cambridge, Mass: National Bureau of Economic Research. Available from: <https://www-nber-org.uniessexlib.idm.oclc.org/system/files/working_papers/w32146/w32146.pdf> [Accessed 19 August 2024].
* Hancock, S. (2024) *PCI DSS Version 4. 0 : A Guide to the Payment Card Industry Data Security Standard.* 1st ed. Ely: IT Governance Ltd. Available from: <https://learning.oreilly.com/library/view/pci-dss-version/9781787785090/xhtml/chapter01.html> [Accessed 09 September 2024].
* Haworth, J. (2018) Hackers behind major US credit card breach sentenced. Available from: <https://portswigger.net/daily-swig/hackers-behind-major-us-credit-card-breach-sentenced> [Accessed 29 August 2024].
* Hiremath, O. (N.D.) Comparison of STRIDE, DREAD and PASTA. Available from: <https://www.softwaresecured.com/post/comparison-of-stride-dread-pasta> [Accessed 06 September 2024].
* IBM. (2024) Multi-Factor Authentication. Available from: <https://www.ibm.com/docs/en/cics-ts/6.x?topic=cics-multi-factor-authentication-mfa> [Accessed 19 August 2024].
* Kali. (N.D.) Sqlmap Tool Documentation. Available from: <https://www.kali.org/tools/sqlmap/> [Accessed 29 August 2024].
* NCSC. (2019) The problems with patching. Available from: <https://www.ncsc.gov.uk/blog-post/the-problems-with-patching> [Accessed 29 August 2024].
* NCSC. (2024) How to get the most from penetration testing. Available from: <https://www.ncsc.gov.uk/pdfs/guidance/penetration-testing.pdf> [Accessed 12 August 2024].
* Nidecki, T. (2020) The HTTPOnly Flag – Protecting Cookies against XSS. Available from: <https://www.acunetix.com/blog/web-security-zone/httponly-flag-protecting-cookies/> [Accessed 09 September 2024].
* Offsec. (N.D.) About The Exploit Database. Available from: <https://www.exploit-db.com/about-exploit-db> [Accessed 29 August 2024].
* Olmsted, A. (2024) *Security-Driven Software Development : Learn to Analyze and Mitigate Risks in Your Software Projects*. First edition. Birmingham, England: Packt Publishing Ltd. Available from: <https://learning.oreilly.com/library/view/security-driven-software-development/9781835462836/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 07 September 2024].
* OWASP. (2021) OWASP Top Ten. Available from: <https://owasp.org/www-project-top-ten/> [Accessed 04 August 2024].
* Portswigger. (N.D.) Access control vulnerabilities and privilege escalation. Available from: <https://portswigger.net/web-security/access-control#what-is-access-control> [Accessed 29 August 2024].
* Trace Security. (2023) BREACH Attack: Are you vulnerable? Available from: <https://www.tracesecurity.com/blog/news/breach-attack-are-you-vulnerable> [Accessed 29 August 2024].
* Wang, W., Yi, P., & Xu, H. (2024). DoubleR: Effective XSS attacking reality detection. *Computer Networks (Amsterdam, Netherlands : 1999)* 251: 110567-. DOI: https://doi.org/10.1016/j.comnet.2024.110567
* Wear, S. (2023) *Burp Suite cookbook : web application security made easy with Burp Suite*. Second edition. Birmingham, UK: Packt Publishing Ltd. Available from: <https://learning.oreilly.com/library/view/burp-suite-cookbook/9781835081075/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 29 August 2024].
* Yaworski, P. (2019) *Real-World Bug Hunting: A Field Guide to Web Hacking*. 1st edition. San Francisco, CA: No Starch Press, Incorporated. Available from: <https://learning.oreilly.com/library/view/real-world-bug-hunting/9781098122508/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 30 August 2024].