**BASELINE ANALYSIS AND PLAN**

**Introduction**

Whilst ginandjuice.shop appears secure on initial assessment with the use of HTTPS, which is critical for protecting data in transit (CIO, N.D.), a more in-depth security assessment is required to ensure a strong security posture. This report will provide an outline for these future assessments.

**Potential Security Challenges**

Future security assessments will be guided by the “OWASP Top Ten,” which lists web applications' most critical security risks (OWASP, 2021). Table One provides examples and their impact on the business.

|  |  |
| --- | --- |
| Risk | Business Impact |
| Broken Access Control | Sensitive customer data may be exposed. |
| Injection Attacks | Injected malicious code may lead to a data breach, affecting customer trust. |
| Server-Side Request Forgery | Exposes internal systems to attacks. |
| HTTPS Misconfiguration | This may give a false sense of security, affecting consumer trust. |

*Table One: Possible security challenges and business impact.*

It is imperative to ensure the website is free from these risks as they can expose sensitive data and damage internal systems, negatively affecting consumer trust and reputation.

**Standards**

Similarly, if ginandjuice.shop fails to comply with legal standards such as the General Data Protection Regulation (GDPR) and its strict data mandates (Demirer, 2024), this will result in reputational damage. One example is the consumer trust Equifax lost after a data breach in 2017 (Egress, 2023). Financial and legal challenges will also be present, such as when British Airways was fined in 2018 (BBC, 2022). Technical standards like the NIST Cyber Security Framework are one way to prevent this (Federal Trade Commission, N.D.) and compliance with the framework will be verified during the assessments.

**Methodology and Tools**

Two approaches can be used during the assessments: black-box and white-box. The former shares no information with the testers and “accurately models the risk faced from attackers”; the latter validates management controls, sharing complete information with the testers (NCSC, 2024). Black-box testing will be the preferred method due to the tests’ remote nature and its proficiency in replicating an attacker’s perspective. Possible tools to be used are in Table Two.

|  |  |
| --- | --- |
| Tool | Description |
| NMAP | Used to identify open and exploitable ports. |
| BurpSuite | Helpful in detecting website application vulnerabilities. |
| Nessus | A vulnerability scanning tool that can check compliance with various standards (Tenable, N.D.). |

*Table Two: Tools used in the security assessment.*

**Limitations and Assumptions**

Whilst black-box testing is suitable for gaining an attacker's perspective of the site, there is the potential to miss vulnerabilities due to its limited scope. Website owners must perform white-box testing to validate internal processes and achieve a more accurate security picture. This combination of testing will guarantee that all assets, including human, physical, and web, have been assured. Furthermore, proper configuration of the tools mentioned above, such as controlling the speed of an NMAP scan, is also encouraged to prevent tests from appearing as an unauthorised attack (Hartman, 2024).

**Implementation Plan and Timeline**

A robust implementation plan is needed to ensure the efficacy of testing. Split into three distinct phases over two weeks, it is as follows:

1. **Scanning (3 Days).** This is the initial scanning of the site, conducted during off-peak hours to negate business impact. The aim is to identify vulnerabilities and open ports that widen the threat landscape.
2. **Interpretation (4 Days).** Results are analysed and ranked according to their impact and severity. This will contribute to a fully-costed mitigation plan.
3. **Implementation (7 Days).** This time allows the owners to approve financial recommendations such as new firewalls and will enable the IT team to implement the plan effectively.

**Summary**

Whilst there are indications that this is a secure website using HTTPS, more assessments are required to guarantee this. A combination of black-box and white-box testing is to be used over two weeks. This will ensure strong security standing for ginandjuice.shop for the future.

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

**References**

* BBC. (2020) British Airways fined £20m over data breach. Available from: <https://www.bbc.co.uk/news/technology-54568784> [Accessed 08 August 2024].
* CIO. (N.D.) Introduction to HTTPS. Available from: <https://https.cio.gov/faq/> [Accessed 03 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].
* Egress. (2023) Managing data breach reputation damage. Available from: <https://www.egress.com/blog/security-and-email-security/managing-data-breach-reputation-damage#:~:text=Besides%20hefty%20fines%20from%20Britain's,satisfaction%20ratings%20and%20share%20price>. [Accessed 16 August 2024].
* Federal Trade Commission. (N.D.) Understanding The NIST Cybersecurity Framework. Available from: [**https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework**](https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework) [Accessed 01 August 2024].
* Hartman, S. (2024) *Hands-On Ethical Hacking Tactics : Strategies, Tools, and Techniques for Effective Cyber Defense*. Birmingham, England: Packt Publishing Ltd. Available from: <https://learning.oreilly.com/library/view/hands-on-ethical-hacking/9781801810081/?sso_link=yes&sso_link_from=university-of-essex> [Accessed 19 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].
* OWASP. (2021) OWASP Top Ten. Available from: <https://owasp.org/www-project-top-ten/> [Accessed 04 August 2024].
* Tenable. (N.D.) Nessus Scan Tuning Guide: Compliance Configuration. Available from: https://docs.tenable.com/quick-reference/nessus-scan-tuning/Content/Nessus-Scan-Tuning/ComplianceConfiguration.htm [Accessed 14 August 2024].