Design Proposal

Introduction

This document is the first part of a two-part analysis of the given website's security. In this part, we identify theoretical threats to the website, and make recommendations to protect against them.

Methodology

To make recommendations, we establish a theoretical foundation by identifying the website's industry, regulations that apply to it, and introduce theoretical frameworks to identify potential vulnerabilities. We present examples of how these vulnerabilities could be exploited, the impact thereof, and make recommendations to protect against each.

In the second part, we will select programs to scan for the vulnerabilities identified herein. We will then scan to verify their existence, provide a detailed analysis of our findings compared to this paper's, and provide detailed recommendations for mitigation.

Website Context

The website under inspection (https://www.readmyblog.co.uk/) is a weblog marketing site, and its intended audience is those interested in discovering or marketing blogs. The website uses NucleusCMS, an open-source program for maintaining blogs.

Regulations

As the website is in the field of blogging, it has no industrial regulations to follow. However, we identify general security and data regulations which it should follow.

UK GDPR/DPA

The website's domain is in the United Kingdom, thus it must follow the UK GDPR and the 2018 Data Protection Act (ico, n.d.a; UK.GOV, n.d.). To comply with both regulations, the website would need to implement the following relevant standards (Bhatia, n.d.; SkillsPlatform, n.d.):

- Process data lawfully, fairly, and transparently,
- Store data for specific purposes only,
- Obtain consent from data owners to use their data,
- Track all data breaches,
- Enforce a lifespan on data,
- Regularly verify the accuracy of data stored,
- Enforce the right to be forgotten,
- Secure all data in storage and in transit,
- Assign a Data Protection Officer to process the data,
- Enforce accountability for those working with data, and
- Train staff on data processing.

OWASP Top Ten

The Open Web Application Security Project (OWASP) aims to improve web application security. To achieve this, it drives the OWASP Top Ten initiative, which lists the ten most severe vulnerabilities faced by web applications. It is curated using feedback from prominent security companies and researchers (OWASP, 2021a).

Framework Selection

To make recommendations for securing the website, we introduce theoretical frameworks which assist in detecting vulnerabilities and quantifying their impact.

The STRIDE and DREAD frameworks are a popular choice, however, they are not ideal for real-world analysis. STRIDE is too limited in scope to yield practical insights in industrial contexts (Bernsmed et al., 2022; Mani & Venkatasen, 2018), and is time-consuming to implement (Shevchenko et al., 2018; Siddique, 2021). DREAD calculations are often inaccurate due to subjective interpretation and Microsoft ceased using it in 2010 (Nweke & Wolthusen, 2020).

Due to its focus on web applications and reliance on up-to-date, real-world information, we use the 2021 edition of the OWASP Top Ten to replace STRIDE. We use it to identify areas where vulnerabilities may exist in the website.

To replace DREAD, we use the Common Vulnerability Scoring System (CVSS) v3.1 framework. Like DREAD, it quantifies vulnerability impact by assigning a score, but CVSS is more objective because it has strict specifications (FIRST, 2019). We use CVSS during the scanning phase to rank the vulnerabilities found in a way that is contextualised to the website.

Theoretical Security Vulnerabilities

Using the OWASP Top Ten, we identify theoretical vulnerabilities below. Each OWASP category has an example of how it could be exploited on the website.

OWASP Category	Example
A01:2021 - Broken Access Control	An attacker gains access to administrator-only features by manipulating URLs.

A02:2021 - Cryptographic Failures	Account credentials are not encrypted in the website's storage.
A03:2021 - Injection	An attacker executes arbitrary JavaScript in a reader's browser by writing scripts in a blog post.
A04:2021 - Insecure Design	The website allows multiple administrators, allowing an attacker to create their own administrator account.
A05:2021 - Security Misconfiguration	An attacker gains additional information about the server the website uses due to improper NucleusCMS settings.
A06:2021 - Vulnerable and Outdated Components	The website uses an old version of NucleusCMS, which an attacker finds a vulnerability for, and exploits.
A07:2021 - Identification and Authentication Failures	NucleusCMS allows the use of easily guessed passwords.
A08:2021 - Software and Data Integrity Failures	The website does not verify the authenticity of external resources.
A09:2021 - Security Logging and Monitoring Failures	Suspicious behaviour (e.g. rapid failed logins) do not alert the website owner.
A10:2021 - Server Side Request Forgery (SSRF)	Attackers can obtain information about the server the website is running on by reading local files on it.

Vulnerability Impact

Attackers could exploit the above vulnerabilities on the website, leading to these potential outcomes:

- Sensitive information (e.g., login credentials), could be leaked.
- The website's users could become attacked through some mechanism such as a drive-by-download (Kaspersky, n.d.).
- Attackers could use the website's server for malicious purposes such as distributed denial-of-service attacks.

These outcomes would lead to a violation of GDPR and DPA regulations due to sensitive information being compromised. To comply with UK GDPR and DPA, once the owner knows about a data breach, the data Commissioner must be notified within 72 hours (UK Legislation, 2018). Failing to do so can lead to a fine of up to £8.7 million (ico, n.d.b).

Vulnerability Mitigations

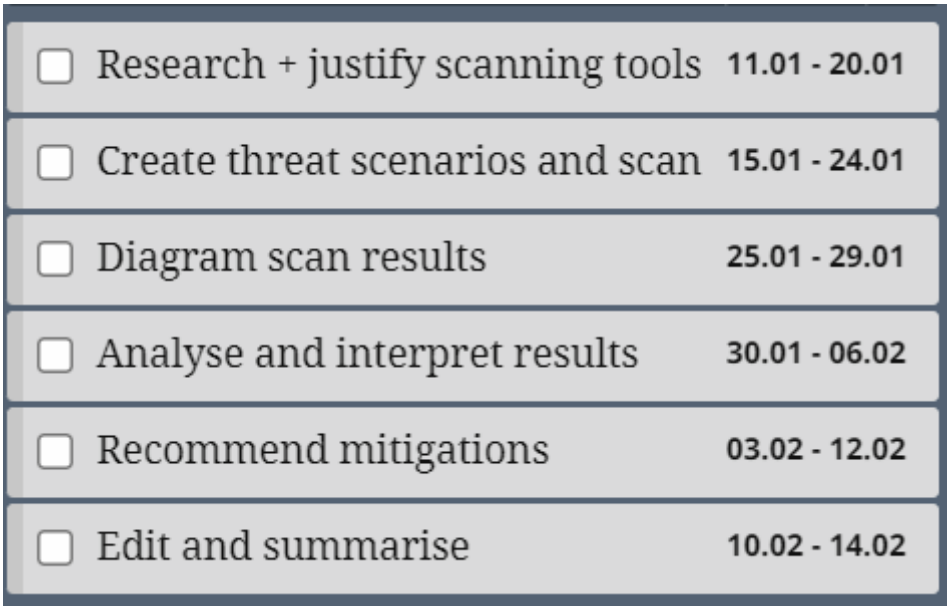
Below, we make recommendations for protecting against the vulnerabilities discussed previously. This list follows OWASP's theoretical prioritisation based on prevalence and impact (OWASP, 2021a), which maps to the blog because it is also a web application.

OWASP Category	Possible Mitigation
A01	Deny privileged resources by default (Lala et al., 2021).
A02	Encrypt data at rest or do not store it (OWASP, 2021b).
A03	Sanitise user inputs and render them as strings (Kellezi et al., 2019).
A04	Implement plausibility checks for requests (OWASP, 2021c).

A05	Regularly review security configurations on NucleusCMS (Loureiro, 2021).
A06	Ensure libraries are kept up-to-date (Nedeljković et al., 2020).
A07	Forbid the use of predictable passwords (OWASP, 2021d).
A08	Obtain external dependencies from official links only (Nedeljković et al., 2020).
A09	Log critical operations with sufficient context to detect attacks (Nedeljković et al., 2020).
A10	Restrict URL schema accepted by the website (OWASP, 2021e)

Timeline

Below, we present the expected timeline for completing the second part of this project. This timeline is available as a real-time Gantt chart.



Conclusion

Despite the lack of regulation in blogging, we identify regulations which the website should follow. By mapping them to theoretical frameworks, we identify vulnerabilities, provide recommendations, and ultimately build a foundation for deeper analysis of the website.

References

Bernsmed, K., Cruzes, D., Jaatun, M. & Iovan, M. (2022) Adopting threat modelling in agile software development projects. *Journal of Systems and Software* 183. DOI: https://doi.org/10.1016/j.jss.2021.111090

Bhatia, P. (n.d). A summary of 10 key GDPR requirements. Available from : https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/ [Accessed 17 December 2021].

FIRST. (2019) Common Vulnerability Scoring System version 3.1: Specification Document. Available from: https://www.first.org/cvss/specification-document [Accessed 13 December 2021].

ico. (n.d.a) Who does the UK GDPR apply to? Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/ [Accessed 8 December 2021].

ico. (n.d.b) Personal data breaches. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ [Accessed 20 December 2021].

Kaspersky. (n.d.) What Is a Drive by Download. Available from: https://www.kaspersky.com/resource-center/definitions/drive-by-download [Accessed 19 December 2021].

Kellezi, D., Boegelund, C. & Meng, W. (2019) 'Towards Secure Open Banking Architecture: An Evaluation with OWASP', *Network and System Security, 13th International Conference, NSS 2019*. Sapporo, Japan, 15-18 December. Cham: Springer. 185-198.

Lala, S., Kumar, A. & Subbulakshmi, T. (2021) 'Secure Web development using OWASP Guidelines', *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*. Madurai, India, 6-8 May. New Jersey: IEEE. 323-332.

Loureiro, S. (2021) Security misconfigurations and how to prevent them. *Network Security* 5: 13-16. DOI: https://doi.org/10.1016/S1353-4858(21)00053-2

Mani, P. & Venkatasen, M. (2018) A risk-centric defensive architecture for threat modeling in e-government application. *Electronic Government, an International Journal (EG)* 14(1): 16-31. DOI: http://doi.org/10.1504/EG.2017.10008841

Nedeljković, N., Vugdelija, N. & Kojić, N. (2020) Use of "OWASP Top 10" In Web Application Security', *4th International Scientific Conference on Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture – ITEMA 2020*. Online, 8 October. Belgrade: Association of Economists and Managers of the Balkans. 25-30.

Nweke, L. & Wolthusen, S. (2020) A Review of Asset-Centric Threat Modelling Approaches. *International Journal of Advanced Computer Science and Applications* 11(2): 1-6. DOI: http://doi.org/10.14569/IJACSA.2020.0110201

OWASP. (2021a) OWASP Top Ten. Available from: https://owasp.org/www-project-top-ten/ [Accessed 6 December 2021].

OWASP. (2021b) A02:2021 – Cryptographic Failures. Available from: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ [Accessed 19 December 2021].

OWASP. (2021c) A04:2021 – Insecure Design. Available from: https://owasp.org/Top10/A04_2021-Insecure_Design/ [Accessed 20 December 2021].

OWASP. (2021d) A07:2021 – Identification and Authentication Failures. Available from: https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ [Accessed 19 December 2021].

OWASP. (2021e) A10:2021 – Server-Side Request Forgery (SSRF). Available from: https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/ [Accessed 19 December 2021].

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T. & Woody, C. (2018) Threat Modeling: A Summary of Available Methods. Web: Carnegie Mellon University.

Siddique, A. (2021) Threat Modeling Methodologies for Network Security. Available from: http://doi.org/10.13140/RG.2.2.19672.42249 [Accessed 13 December 2021].

SkillsPlatform. (n.d). What Are the Eight Principles of the Data Protection Act?. Available from: https://www.skillsplatform.org/blog/what-are-the-eight-principles-of-the-data-protection-act/ [Accessed 17 December 2021].

UK.GOV. (n.d.) Data protection. Available from: https://www.gov.uk/data-protection [Accessed 17 December 2021].

UK Legislation. (2018) Data Protection Act 2018 - Section 67. Available from: https://www.legislation.gov.uk/ukpga/2018/12/section/67/enacted [Accessed 19 December 2021].