Design Document for allmytype.co.uk

Group 2

Elizabeth Cook

Jurbe Jubet

Isioma Vina Okafor-Tolofari

Osarodion Samuel Tolofari

Contents

1.0 Introduction

Any organisation using a website must take appropriate steps to ensure its security (Thia & Hieu, 2019). This is vital to prevent an attack that could compromise the website and to ensure compliance with governing bodies and regulations. Following a review of https://allmytype.co.uk, this report identifies the applicable regulations, intended audience, and information held on the site and then assesses the potential vulnerabilities, risks and how these can be mitigated.

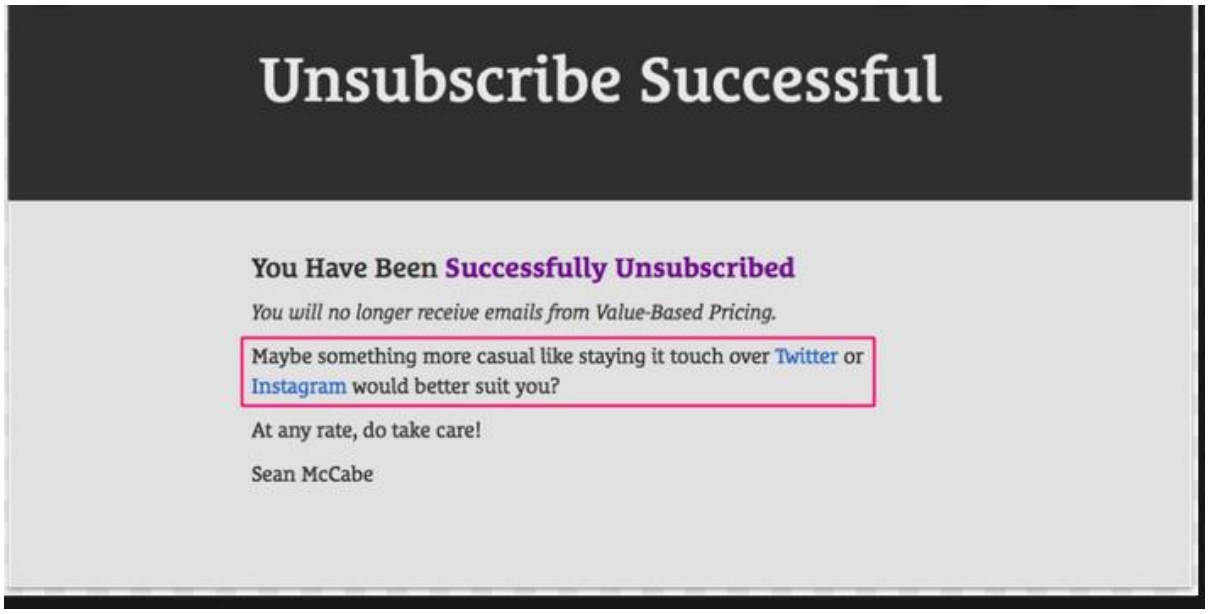
2.0 Governing Bodies and Regulation

- **General Data Protection Regulation (GDPR);** All UK organisations must abide by GDPR when processing personal information (ICO, 2018).
- Personal data must be secured by appropriate technical measures to ensure the confidentiality, integrity and availability of the systems.
- Consent must be given for the use of personal data, and the right to be forgotten must be met.
- The information must be used in a manner that is fair, lawful and transparent, for specified, explicit purposes, be limited to what is necessary and kept for no longer than needed. (Gov.UK, 2018).
- **Uniform Domain-Name Dispute-Resolution Policy;** protects against cybersquatting (ICANN.org, 2016)
- **The Intellectual Property Office guides UK Copyright law**; Owners found by the courts to be infringing copyright can be fined and or imprisoned (Intellectual Property Office, 2011).

3.0 Intended audience and functionality

The website is publicly available to anyone who has the URL. The website administrator can log into the site, and users can enter names and comments. Visitors may submit their email addresses to subscribe to posts; their email may be held, which is classed as personal information (ICO, 2018).

Emails must only be sent to those who opt-in to receive them (including newsletters, sales or not). To maintain compliance with GDPR, users must have the ability to unsubscribe from blog emails after signing up. Most email software will do this automatically, but you must not remove the 'unsubscribe' link by accident. Subscribers should be able to easily unsubscribe themselves from your email list by following simple steps.



4.0 Vulnerabilities in Web Design

GDPR requires data protection by design; in order to meet this requirement, the website must be built with security features and take into consideration vulnerabilities that could impact the personal data stored on the site. Threat modelling should be completed for critical authentication, access control, business logic, and key flows and plausibility checks integrated at each tier of the application (OWASP, 2021). The OWASP (2021) top 10 vulnerabilities can be used to advise on the highest security risks to web applications and should be a focus when designing any site that holds personal information. Applying mitigating actions against each vulnerability can protect an organisation from GDPR breaches (Vagenas & Iakovakis, 2019).

4.1 Potential Vulnerabilities

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insufficient Logging & Monitoring
- Cryptographic Failures
- Broken Access Control
- Vulnerable and Outdated Components
- Software and Data Integrity Failures
- Improper error handling
- Open ports
- Weak log in credentials

5.0 Vulnerability Risk Assessment & Recommendations

Following the identification of potential vulnerabilities to the site, they have been assessed using a DREAD analysis (Mackman et al, 2003). A rating of 1-10 was used for each category and then scored according to low, medium and high risk to the website. Business priority should be addressing the high risks first.

5.1 DREAD Analysis

Vulnerability	D	R	E	A	D	Score	Rating	Mitigation & Recommendation
Security Misconfiguration	9	6	8	9	6	38	High	• Do not install unused features and frameworks. • Patches must be reviewed and updated as part of a patch management process.
Software and Data Integrity Failures	9	8	8	6	5	36	High	• Review code and configuration changes via a review process.
Improper error handling	8	8	6	4	4	30	Medium	• Ensure sensitive data or credentials are not stored insecurely in plaintext, repositories, or public cloud storage. • Change of default password

								• Secure and regularly update SSH keys.
SQL Injections	6	6	6	3	3	24	medium	• Input validation • Enforce prepared statements and parameterisation • Actively manage patches and updates • Harden your OS and applications
Cryptographic Failures	8	2	5	6	2	23	Medium	• Implement an information classification policy to identify the sensitivity of data stored, processed or transmitted. • Use proper management or encryption keys and ensure strong standard algorithms are in place. • All data must be encrypted in transit using secure protocols such as TLS. • Ensure encryption is enforced by using HTTP Strict Transport Security.
Cross Site Scripting (XSS)	6	5	4	3	2	20	Medium	• Prevent HTML code from being entered into inputs whenever

								possible by preventing them posting that code. • Validating the data to ensure that it meets specific criteria. • Data sanitisation before execution to detect XSS
Cross-Site Request Forgery (CSRF)	6	6	4	2	2	20	Medium	• Enforce “deny by default” firewall policies • Sanitise and validate all client-supplied input data
Insufficient Logging & Monitoring	5	3	3	1	2	14	Low	• Ensure all login attempts, including failed, and other inputs are logged and auditable to identify malicious accounts. These must be kept for a sufficient time to allow forensic analysis if required. • Any log data should be encrypted to prevent attacks on the logging and monitoring systems which could affect repudiation.

Vulnerable and Outdated Components	2	2	2	2	2	10	Low	• Remove any unused or unnecessary features, components or files. • Implement a process to monitor sources such as Common Vulnerability and Exposures (CVE) and National Vulnerability Database (NVD) for known vulnerabilities that can be prevented. This process can be automated for efficiency.
Open ports	2	2	2	2	1	9	Low	• Only use ports that encrypt traffic • Open ports to the internet should sit behind a firewall.
Broken Access Control	2	1	2	2	2	9	Low	• Implement an access control process and ensure this is used consistently across the platform including minimising Cross-Origin Resource Sharing (CORS) usage
Weak login credentials	2	2	2	1	1	5	Low	• passwords should contain special characters, letters, integers

6.0 References

attack.mitre.org. (n.d.). Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®. [online] Available at: https://attack.mitre.org/techniques/T1078/ [Accessed 2 Apr. 2022].

byRosanna. (n.d.). Legal Rules & Guidelines For Bloggers | byRosanna | Squarespace Website Design & Branding UK. [online] Available at: https://www.byrosanna.co.uk/blog/legal-guidelines-for-bloggers [Accessed 1 Apr. 2022].

Gov.uk (2018). Data Protection Act. [online] gov.uk. Available at: https://www.gov.uk/data-protection [Accessed 2 Apr. 2022].

iainfoulds (n.d.). Attractive Accounts for Credential Theft. [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-gb/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft.

Icann.org. (2016). Uniform Domain-Name Dispute-Resolution Policy - ICANN. [online] Available at: https://www.icann.org/resources/pages/help/dndr/udrp-en [Accessed 30 Mar. 2022].

Information Commissioner's Office (2019). Guide to the General Data Protection Regulation (GDPR). [online] ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed 2 Apr. 2022].

Intellectual Property Office (2011). Copyright Acts and Related Laws. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/copyright-acts-and-related-laws [Accessed 30 Mar. 2022].

J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla, and A. Murukan, Improving web application security: threats and countermeasures. Microsoft Redmond, WA, 2003.

OWASP (2021). OWASP Top Ten. [online] Owasp.org. Available at: https://owasp.org/www-project-top-ten/ [Accessed 2 Apr. 2022].

Srinivas (2020). Why Improper Error Handling Happens. [online] Infosec Resources. Available at: https://resources.infosecinstitute.com/topic/why-improper-error-handling-happens/ [Accessed 2 Apr. 2022].

Thai, N.D. and Hieu, N.H. (2019). A Framework for Website Security Assessment. Proceedings of the 2019 7th International Conference on Computer and Communications Management.

Vagenas, P. and Iakovakis, G. (2019). The Combination of OWASP Top 10 and GDPR regulation as a Restraining Tool Against Cyber-crime.