Development Team Project: Design Document

Team 2 - Sathira Padukka, Babatunde Ahmed, Yin Ping Lai

# 1. Introduction

*https://www.allmytype.co.uk* is a blog-type application where it allows users to log in and enter their blog and allow other users to read their thoughts on the subject with primary target being audience from the United Kingdom. The site holds basic information of users via registration giving the option to post an inspiration or comment on existing ones. This document will go over the governing bodies and regulations, vulnerabilities assessment and recommendations and potential mitigations. Based on the operations of the website as stated above, it naturally falls under certain governing bodies and act of the United Kingdom. This includes:

* The Data Protection Act (DPA) 2018 [1] and the United Kingdom General Data Protection Regulation (UK GDPR) [2] governed by the UK Government
* The Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003 [3] governed by the UK Government

As a result of this, the site is required to follow certain guidelines which include:

* Ensure getting the user’s consent for using cookies.
* Ensure that commenters can access, amend, and withdraw their data anytime according to the UK GDPR article 17.
* Ensure that personal data are stored in a secure way and prevent unauthorized or unauthenticated access according to the UK GDPR article 5(1)(f) [3] and section 3 of DPA.

To ensure the safety of user's data and be compliant with the governing and regulatory bodies it is important to do a comprehensive vulnerability assessment and check of this application through a comprehensive penetration test.

# 2. Vulnerabilities Assessment

## 2.1 Methodology:

* For this penetration test, we will be using a **grey-box** approach using both black-box and white-box resulting in using brute force attacks to try and find vulnerabilities or weaknesses to exploit by trial and error coupled with manual testing as we some information about the website architecture and framework.
* The penetration testing process would be carried out in 5 stages with each stage estimated to be completed within a week. This includes Planning and Reconnaissance, Scanning, Exploitation, Maintaining Access, and the Analysis of the Results.
* Since this is a web application, we will be using the **OWASP** Testing Methodology with major focus on security testing.

## 2.2 Stages:

|  |  |  |
| --- | --- | --- |
| Stage | Process | Timeline |
| Planning and Reconnaissance | This includes setting the scope, agreement, limitation, and metrics of the project. | Week 1 |
| Scanning | This is a periodic or continuous interaction with the target component using different Network connections, applications, and word lists to gather information such as Application map, directory listing, network information and other vulnerabilities. | Week 2 |
| Exploitation | Use of the vulnerabilities found in the scanning step above to launch an attack on the component with the possibility of discovering further vulnerabilities. | Week 3 |
| Maintaining Access | Create alternative access to maintain access even in case of disconnection through exploitation route. | Week 4 |
| Analysis of the Results | Review and quantify findings based agreed metrics and provide feedback report. | Week 5 |

## 2.3 Tools:

|  |  |  |
| --- | --- | --- |
| Name | Description | Target Vulnerabilities |
| Burp Suite | An integrated platform/graphical tool for performing security testing of web applications | Unauthorized requests |
| OWASP Zap | An open-source web application security scanner | XSS,  SQL Injection |
| Metasploit | An open-source penetration testing system and a development platform that allows to create security tools and exploits. | Network |
| Nmap | Utility for network discovery and security auditing | Network |
| SQL Map | SQL Map automates the process of detecting and exploiting SQL injection. | SQL Injection |
| W3af | Scanner and exploitation tool for Web applications |  |
| KNOXSS | XSS tool | XSS |

# 4. Recommendations and potential mitigations

|  |  |  |
| --- | --- | --- |
| Risk | Mitigation | Recommendation |
| Authentication and Authorization | Revoke access to the device if the device is lost/stolen to mitigate unauthorized access. | When handling authorization and authentication use industry standard methods such as JSON Web Tokens. |
| Handling Cookies | To prevent such attacks there are mitigation methods such as, using HTTPS methods of authentication. | Have the capability to check the source address and referrer of the authenticated user periodically and if there is a mismatch then end the session and shorten the expiry time of the cookie allocated to that web server (Mazerik, 2013). |
| Softaculous (Auto installation Software) | Review applications auto-installer to check for known vulnerabilities, compliance issues, vendor support and maintenance. | Installation of applications should go through a review process by a security council before being installed. |
| Web application firewall (WAF) | Configure the WAF in a proper manner as it will give you a false sense of security. | Make use of patch management, malware detection intrusion detection and prevention systems that are provided by the WAF. |

# References:

[1] The Legislation of the UK Government. 2018. *The Data Protection Act 2018*. [online] Available at: <https://www.legislation.gov.uk/ukpga/2018/12/introduction> [Accessed on 21 Mar 2022].

[2] The Legislation of the UK Government. 2021. *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 (United Kingdom General Data Protection Regulation)*. [online] Available at: <https://www.legislation.gov.uk/eur/2016/679> [Accessed on 28 Mar 2022].

[3] The Legislation of the UK Government. 2003. *The Privacy and Electronic Communications (EC Directive) Regulations 2003*. [online] Available at: <https://www.legislation.gov.uk/uksi/2003/2426/contents> [Accessed on 21 Mar 2022].

[4] Robert B. 2022. *Privacy and Electronic Communications Regulations (PECR)*. [online] Available at: <https://www.termsfeed.com/blog/pecr/#Consent_And_The_Pecr> [Accessed on 21 Mar 2022].

[5] IMUNIFY 360. (n.d.). *Imunify360: Security solution with malware scanner*. [online] Available at: <https://www.imunify360.com/imunify360/> [Accessed 22 Mar. 2022].

[6] www.ncsc.gov.uk. (2021). *Log4j vulnerability - what everyone needs to know*. [online] Available at: <https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know>.

[7] Mazerik, R. (2013). *Risk associated with cookies*. [online] Infosec Resources. Available at: <https://resources.infosecinstitute.com/topic/risk-associated-cookies/>.

[8] Batbold, B. (2021). *Handling Authentication and Authorization with Node*. [online] Quick Code. Available at: <https://medium.com/quick-code/handling-authentication-and-authorization-with-node-7f9548fedde8> [Accessed 26 Mar. 2022].