# Brief Summary of the Work Performed

Bookacheckup.co.uk is a UK-based healthcare website that offers various health checkup services and aims to provide a fast and efficient means for patients to book their checkups online. The website, in its current form, provides limited functionality and lacks many features, summarized in the table below.

Table 1: Functionality and limitations of the current website.



While it is unlikely for a healthcare website to be included in the UK's National Vulnerabilities Database, users should take precautions to protect their personal information when using such websites, such as verifying security and privacy policies and looking for signs of a secure website.

In the baseline analysis and plan submitted at the end of Unit 3, a preliminary inspection revealed a series of potential vulnerabilities that could be further investigated. Given various constraints, including (the lack of) access to various parts of the web application, time constraints, and the sophisticated Intrusion Detection and Prevention System (IDPS) on the web application (namely, Immunify), specific potential threats were investigated further.

The website hostedscan.com provides access to a range of standard penetration tools, including Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP), Open Vulnerability Assessment System (OpenVAS), Sslyze and Nmap. The tool was used to carry out a scan of the target domain to identify vulnerabilities. Following this, SQLMap installed on a Kali Linux distribution running in a Virtual Box on Windows 11 was used to investigate the presence of SQL injection vulnerabilities in the website. This was, of course, in addition to basic scanning tools used, namely, traceroute, dig, and nslookup. Note that these were the final tools used after investigating numerous other options, taking into account a range of factors and challenges faced.

Furthermore, seeing as the app only collects information but does not retrieve or display collected information back on the website at this stage, and taking into account the constraints mentioned, XSS vulnerabilities were not assessed, but this is possible using SQLMap.

The website was manually analysed to determine compliance to the GDPR and the Data Protection Act 2018 as well as the Health Insurance Portability and Accountability Act (HIPAA), both of which apply to this kind of website.

The scan and analysis results were collated and summarized into a set of findings, based on which a set of recommendations were compiled.

# Summary of Findings – Vulnerabilities

Table 2: Summary of type, level and number of threats identified.



Table2 summarizes the security threats identified by the vulnerability scanning exercise, along with the number of threats at each severity level identified. Before continuing to analyze the table, it is worth stating that, despite its simple appearance and seeming lack of security at face value, it was generally found that the site was mostly secure. The biggest factor contributing to the security of the website is the IDPS system–namely Immunify–that has been put in place to detect suspicious network activity and block requests accordingly. IDPS software was discussed in this module as well as our first module. The IDPS was a significant challenge when trying to run a range of automated tools on the website. The IDPS would initially allow basic scans, and then swiftly move in to block all subsequent scans from that IP for a period of time. This could sometimes be mitigated by accessing the website via the web browser, where a prompt from Immunify would be presented to verify that the user is a human, as seen in Figure 1. This was many times not the case, but when it was, it would again temporarily provide access to the website. This demonstrates the crucial importance of an IDPS for any web application.

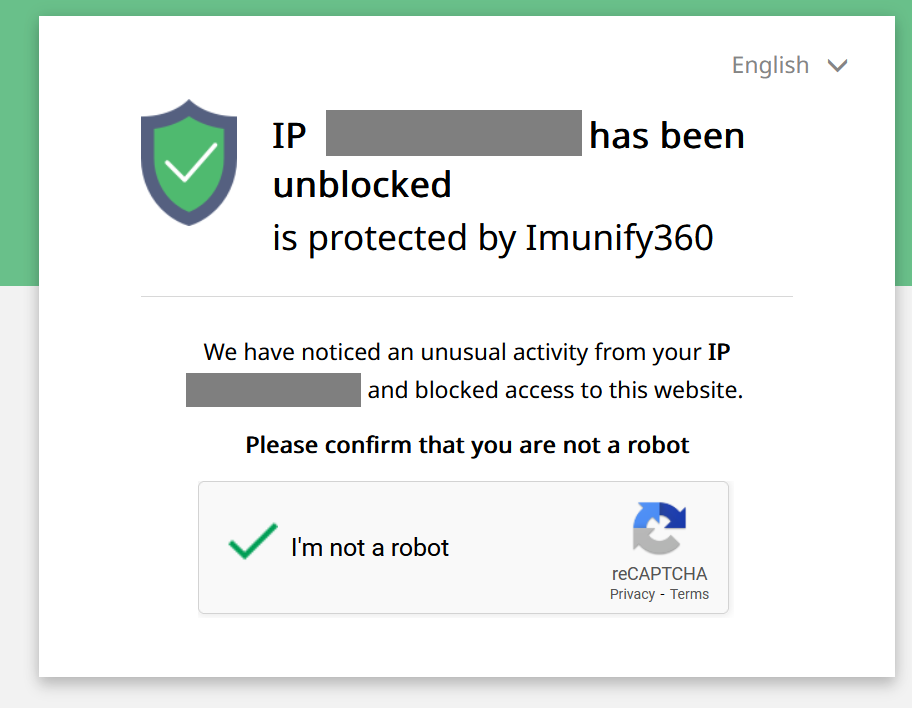


Figure 1: Immunify blocking requests after one or more scans.

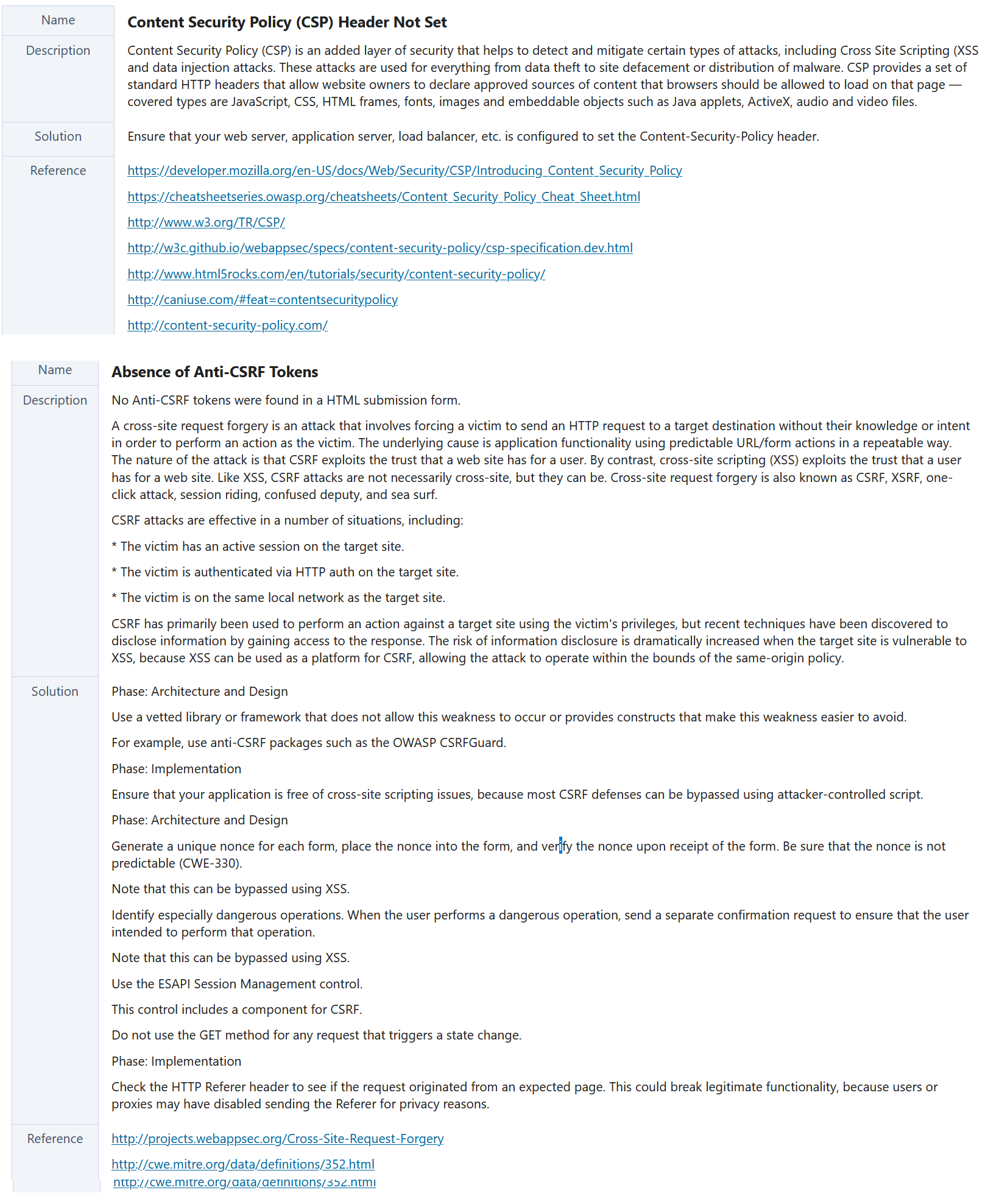
As seen in Table2, two high risk issues identified were: the existence of an unknown port 37661 which was open on the server; and the use of an outdated and vulnerable jsquery JavaScript library.

Following this was a large number of ports open on the server, some of which are labelled as low risk because they are necessary e.g. 80 (HTTP), 443 (HTTPS) and 53 (DNS); some labelled as medium risk because their necessity is not clear such as one of 3306 (MySQL) or 5432 (PostgreSQL) since its likely that only one–not both–of these databases are used to store the data, or otherwise not strictly necessary for the specific website in question based on its current described functions, such as 21 (FTP), 25 (SMTP), 110 (POP3) and others. Further information is required to determine whether each of these ports are actually required for the functioning of the web application.

Two additional medium risks were identified, all to do with parameter management on the web app: a Content Security Policy (CSP) header not set; absence of anti-Cross-Site-Request-Forgery tokens. Figure 2 provides additional information about these risks.

Finally, a range of low risk issues were identified, all to do with parameter and cookie management on the web app: cookies with no secure flag, or an HttpOnly flag, or a SameSite attribute; and an “X-Powered-By” HTTP response header leaking information. Figure 3 provides additional information about these risks.

SQLMap revealed that the text fields on the app did not appear to be vulnerable to SQL attacks.

 Figure 2: Two additional medium risks.

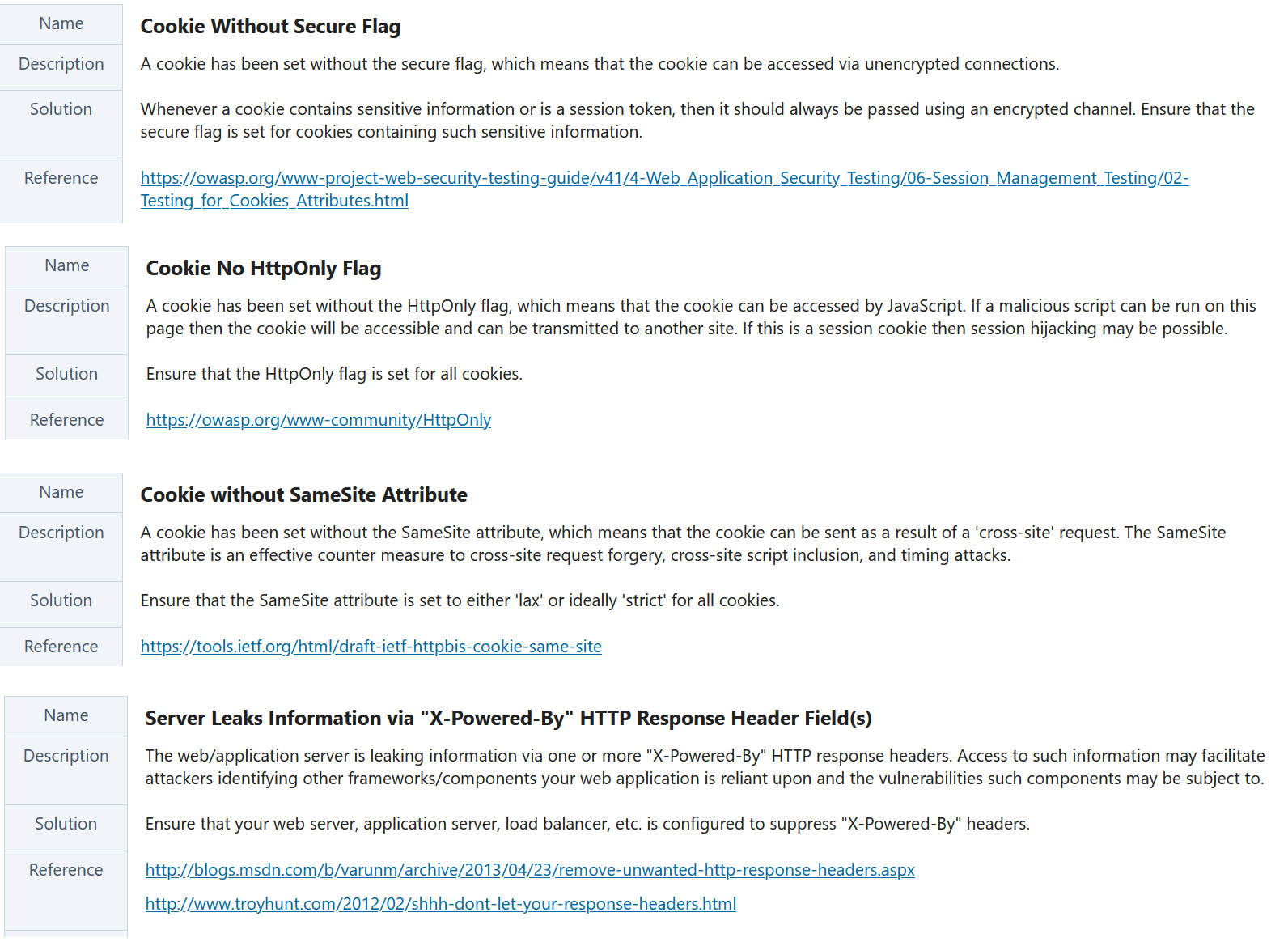


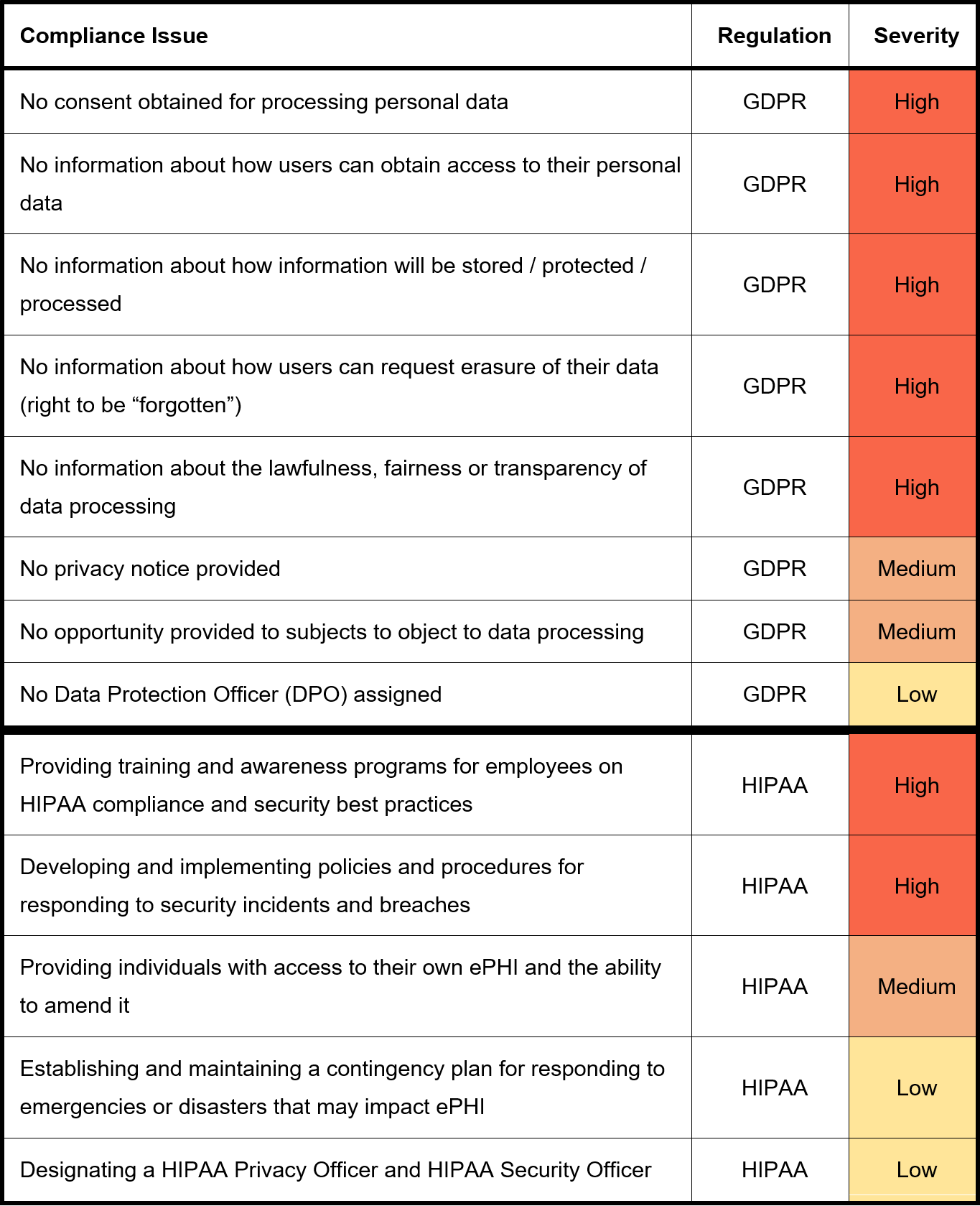
Figure 3: Low Risks

# Summary of Findings – Regulations

When assessing the website against the GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act), several issues of concern were observed. These are summarized in Table 2 and the legal severity of non-compliance with these issues have also been indicated in the table.

The table shows that there are several guidelines of high, medium and low severity to which the website is non-compliant. Overall, as a UK-based healthcare website that offers health services, the website must comply with GDPR and HIPAA requirements by implementing appropriate privacy and security measures and obtaining explicit consent from individuals before collecting their data. It may be advisable to seek legal and/or regulatory guidance to ensure compliance with GDPR and HIPAA.

Table 3: Compliance issues to GDPRR and HIPAA.



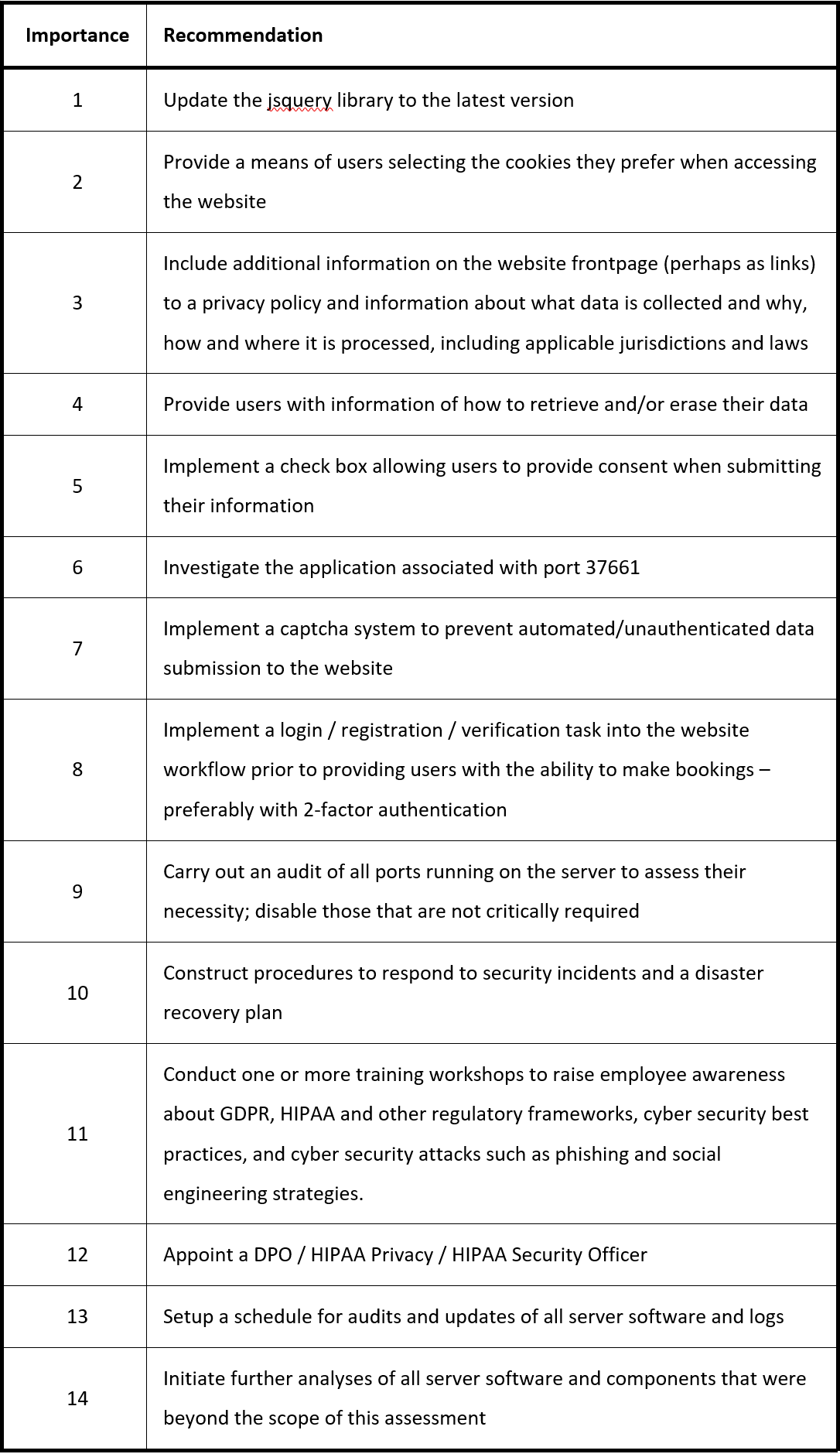
# Summary of Conclusions Based on Findings

As clearly demonstrated and enumerated in the previous section, the biggest area of concern with the website is that of non-compliance to key regulatory frameworks. The website hardly complies with any of the guidelines set out in the GDPR and HIPAA, if any. In terms of the security of the website itself, taking into account the limitations on time and access, only two threats of high risk severity were identified, followed by a series of threats of medium and low risk severity. The IDPR system in place plays a key role in ensuring that the application remains secure.

# Recommendations

Based on the above, Table 4 summarizes the recommendations. The ordering is primarily in favour of issues of greater importance, but also taking into account fixes that may be easily and quickly carried out to realize effective change quickly.

Table 4: Summary of Recommendations.



# References

* National Cyber Security Centre (NCSC) (2021). NCSC Homepage. [online] Available at: <https://www.ncsc.gov.uk/> [Accessed 1 Feb 2023].
* UK Cyber Threat Centre (CTC) (2021). UK Cyber Threat Centre. [online] Available at: <https://www.ncsc.gov.uk/services/uk-cyber-threat-centre-ukctc> [Accessed 1 Feb 2023].
* UK Government Digital Service (GDS) (2021). Government Digital Service. [online] Available at: <https://www.gov.uk/government/organisations/government-digital-service> [Accessed 1 Feb 2023].
* UK Government National Security Information (NSI) (2021). UK National Security Information. [online] Available at: <https://www.ncsc.gov.uk/information/national-security-information> [Accessed 1 Feb 2023].
* UK Information Commissioner’s Office (ICO) (2021). Information Commissioner’s Office. [online] Available at: <https://ico.org.uk/> [Accessed 1 Feb 2023].
* UK Cyber Essentials Scheme (CES) (2021). Cyber Essentials Scheme. [online] Available at: <https://www.cyberaware.gov.uk/cyberessentials/> [Accessed 1 Feb 2023].
* Software Alliance (SA) (2021). Software Alliance. [online] Available at: <https://www.software.org.uk/> [Accessed 1 Feb 2023].
* National Technical Authority for Information Assurance (CESG) (2021). CESG Homepage. [online] Available at: <https://www.cesg.gov.uk/> [Accessed 1 Feb 2023].
* CyberUK (2021). CyberUK. [online] Available at: <https://www.ncsc.gov.uk/events/cyberuk> [Accessed 1 Feb 2023].
* UK Government Technology Strategy Board (TSB) (2021). Technology Strategy Board. [online] Available at: <https://www.gov.uk/government/collections/technology-strategy-board> [Accessed 1 Feb 2023].
* Tian, Y., Li, J., & Wang, H. (2016). A comprehensive survey of website security. ACM Computing Surveys (CSUR), 48(3), 33.
* Wang, Q., Li, J., & Ren, K. (2015). Website security assessment: A survey. Journal of Network and Computer Applications, 42, 1-15.
* Uddin, M., & Lee, J. (2017). A systematic review of website security assessment methods. Journal of Information Security and Applications, 36, 68-82.
* Liu, L., & Xu, Y. (2015). Website vulnerability assessment: A review. Journal of Computer Science and Technology, 30(5), 901-910.
* Jia, J., & Rong, Y. (2016). A review of website vulnerability assessment techniques. Journal of Computer Science and Technology, 31(6), 1031-1040.
* Muin, M. A., Kapti, K., & Yusnanto, T. (2022). Campus website security vulnerability analysis using nessus. International Journal of Computer and Information System (IJCIS), 3(2), 79-82.
* Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014, August). A case study on web application vulnerability scanning tools. In 2014 Science and Information Conference (pp. 595-600). IEEE.