Security Report

This report will look at the security measures integrated into the Be Free Holiday's (BFH) website to defend against malicious attacks. The report will also look at what measures the website could incorporate at a later stage to increase security.

As a data controller, one of the most important considerations of the website's security measures is to protect the data of its users. As the website asks the user to input their full name, address, and date of birth, this could be considered "identifiable" data or "personal data" under the Data Protection Act 2018. Where personal data is collected, there is a lawful obligation by the controller of this data to ensure the "appropriate security measures" are in place to protect the data (GOV.UK, 2018). Furthermore, there is an expectation between the customer and the company that security measures are put in place to protect the privacy of the customer in the unfortunate event that a malicious attacker did penetrate the website.

The first security measure this report will address is authentication. Authentication "lies at the heart of an application's protection against malicious attack" (Stuttard and Pinto, 2011). At the forefront of authentication is the password. To ensure the password that the user chooses is sufficient, the website checks whether the password is at least 8 characters; a combination of numbers and upper/lowercase characters; that the password is not the same as the username. As Studdard and Pinto (2011, p. 161) state, concerning passwords, "end users typically display little awareness of security issues". Therefore, the website must enforce password rules that guide the user to creating a more secure password. Additionally, the website also takes the following steps to safeguard against authentication attacks: usernames must be unique; a generic message is displayed when a login attempt fails, this ensures that the hacker is unaware whether the username or password is incorrect; finally, passwords are stored in the database as hashed passwords using the built-in PHP function, password_hash(PASSWORD_DEFAULT) which uses the bcrypt algorithm. A final point to note is that at the points of authentication the session ID is regenerated; this is to help prevent session fixation attacks.

The second measure this report will consider is access control. In the 2021 OWASP Top Ten web application security risks, broken access control moved from the top fifth to the top web application security risk (OWASP, 2021). The BFH website protects against broken access control in the following ways: it verifies that the POST method is used where user input containing sensitive data is required by checking the SERVER super global, otherwise an error code is printed, and the user is redirected; limits access to certain pages to logged in users only.

Finally, this report will look at two specific types of attacks that the website would be vulnerable to if security measures are not put in place. The first type of attack is SQL injection. Injection ranks third in OWASP's Top 10 security risks (OWASP, 2021), and could cause significant damage to both the website's functionality and the integrity of the data held in the database. To protect against these types of attacks, the website uses prepared statements and the built-in escape string function to protect itself against malicious code inputted by an attacker attempting to penetrate the database through HTML forms. While escaping special characters to prevent SQL injection is a partially effective measure, using prepared statements is the most effective and "prevents SQL injection vulnerabilities from arising" (Stuttard and Pinto, 2011). Furthermore, prepared statements are used for every database query, not just queries that passes user input, this helps to protect the application against "second-order attacks" (Stuttard and Pinto, 2011). The second type of attack the website's security protects it against is cross-site scripting attacks. The points where an XSS attack are most critical is the text box that allows customers to leave reviews and the text box that allows customers to leave booking notes. To secure the website against XSS attacks at these points, the input is sanitised to escape HTML characters. A measure that the website could implement to is a content security policy which would prevent inline JavaScript being run on the website. While the site currently uses a very small amount of JavaScript to function, any future JavaScript would need to be written in a separate file. However, this would not be a significant issue as "inline script tags are considered bad practice in modern web development" (McDonald, 2020).

Other recommendations for future development

In the future, BFH would benefit from encryption in the form of HTTPS. This would ensure that the website could “guarantee secure communication” (McDonald, 2020) for users. As Najera-Gutierrez et al. (2019, p. 174) states, “always use secure protocols [on the topic of authentication], such as TLS, to submit login information.” In the website’s current state, the information that’s being communicated across the network is vulnerable to viewing and tampering. Additionally, the website could implement two-factor authentication to add an extra layer of security. This would most likely be in the form of a one-time password (OTP) that is sent to the user through SMS, email, or a mobile app. While there are some potential flaws that can arise, multi-factor authentication ultimately “comes from the need to provide an extra layer of security to certain applications and prevent unauthorised access in case, for example, a password is guessed or stolen by an attacker” (Najera-Gutierrez et al, 2019).

References

GOV.UK (2018) *Data Protection Act*. Available at: https://www.gov.uk/data-protection (Accessed: 21 September 2022).

Stuttard, D. and Pinto, M. (2011) *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Second Edition. Indianapolis: John Wiley & Sons, Inc.

OWASP (2021) *OWASP Top Ten Web Application Security Risks*. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 21 September 2022).

McDonald, M. (2020) *Web Security for Developers: real threats, practical defence*. First edition. San Francisco: No Starch Press.

Najera-Gutierrez, G., Ansari, J., Teixeria, D., Singh, A. (2019) *Improving your penetration testing skills: strengthen your defence against web attacks with Kali Linux and Metasploit*. Birmingham: Packt Publishing Ltd.