Northumbria University NEWCASTLE

Secure Website Development Assessment.

Written by Carlos Beleret

KF7013BNN01

Tutor: Emma

Northumbria ID number:

20038178

Index

Introduction

A side effect of the exponential growth that the Internet has had is the privacy of both personal and professional information or also known as the data privacy. On the Internet we find online stores operating, businesses that move large amounts of money, networks of services that enable international commerce, as well as social networking sites that contain very sensitive information on the private lives of their members. In a recent educational research (P O'Brien, Scott W.H. Young, K Arlitsch, K Benedict, 2018) has shown that "third-party tracking can occur when web analytics services, such as Google Analytics, are utilized to measure visitation to websites. These services provide information about website use and user behaviour, which can help libraries improve their online services. However, the analytics services operate sophisticated mechanisms through extensive networks to track users and their behaviour across sites, acquiring user demographics and behavioural patterns."

As the world becomes more connected, the need for security in the procedures used to share information becomes more important. From many points of view, it can be believed without a doubt that the most critical point of Internet security is the parts that intervene directly with the masses of users, the web servers. That is why In the following assessment we will critically review and analyse the security implemented in our website and we will also suggest future improvements concerning data and security of the web server.

Website Security

PHP

The first measures that were taken are related with the language programing of PHP. In this case we tried to avoid exposing sensitive information to such as database credentials, in your PHP code. Instead, it has been stored this information in a separate configuration file known as "*db_config.php"* that is not accessible from the web. Concerning this programming language, we also keep PHP up to date: with an updated installation and their latest security patches. Outdated versions of PHP can have known vulnerabilities that can be exploited by potentials attackers.

When communicating with a database, it can be employed prepared statements to enhance security against SQL injection attacks. By separating the SQL code from the data being provided to the database using prepared statements, you may avoid having malicious data executed as SQL code.(Php.net,2019) Use functions to validate user input: To validate user input and make sure it is the right kind and format, use methods like filter *var().* Hacker attacks and other harmful behaviour may be avoided in this way.

This protection can be seen in our bookings.php file where those methods are used to ensure the protection of the code. These methods are well known as sanitazing. According to the PHP manual, "Sanitizing user input refers to the process of removing any potentially harmful characters or tags from user-supplied data" (PHP, 2020).

Sanitizing data ensures that any malicious code is eliminated before the data is utilised or stored in a database, safeguarding your application from any security issues. It helps to prevent security vulnerabilities such as SQL injection or cross-site scripting (XSS) attacks. According to Michael Cobb, in his book "SQL Server Security" (2005), "Sanitizing user input is a crucial step in securing web applications and should be a fundamental part of any development process."

Improvements:

Also it will be useful to implement in our code functions to mask user input: To mask special characters and shield your website from cross-site scripting (XSS) assaults, use functions like *htmlspecialchars()* when displaying user-provided data.(HTML, 2020)

Log in/out

Another security measure is to advise and provide strong password with special characters. If the user in our website stays is not navigating, a secure session management is implemented. In other words, it will ask again for the credentials. This successful login, can help protect against session hijacking and other types of attacks.

This can be also seen in the FTP client used for this assignment that is not other than FileZilla. It can be used Use SFTP or (FTPS) to encrypt data transmitted between computer and the web server. Furthermore, we use strong password connected to our FileZilla account.

Improvements:

One of the main improvements concerning web server security is not other than Use HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP, the internet protocol used to send data. HTTPS encrypts data sent between a website and a user's browser, aiding in the prevention of man-in-the-middle attacks and other forms of unwanted behaviour. (Bressoud, T & White, D. 2020). In order to get this improvement, it is necessary to acquire an SSL/TLS certificate from a certificate authority to add HTTPS to your website (CA). This certificate acts as an electronic "ID" that visitors may use to verify the validity of the proposed website.

Another upgrade that it has been seen in the past few year is not other than Enabling two-factor authentication. This improvement adds an additional degree of protection by requiring a second form of authentication (could be a text message or email code) in addition to a password.

According to Amin, Ul Haq and Nazir,(2017,)"two-factor verification does enhance security also it builds client resistance. Integrated two factor authentication gives the best convenience to better security, so a two-factor confirmation innovation that can be moved up to coordinate the two elements all the more nearly has the best capacity to become as requirements change and also to amplify client uptake of discretionary two factor authentication"In other words, it Reduces the danger of account takeover: Even if an hacker learns a user's password, they will still require the second form of authentication (e.g., a code delivered to the user's phone) to gain access. This drastically minimises the possibility of an attacker gaining access to the account.

Conclusion

In conclsuion, security is an important part of any website and should be considered throughout the building process. To prevent security vulnerabilities like as SQL injection or cross-site scripting (XSS) attacks, data must be properly sanitised and verified. Other security methods, such as access limits, encryption, and regular security audits, can also assist to safeguard your website.

As we've seen, the implications of a security breach may be serious, including the loss of sensitive data, financial loss, and reputational harm to an organisation that is trying to

create a name in the market. To secure both the website and its consumers, it is critical to consider security in website creation.

In the contemporary digital era, the quantity of online transactions, personal information storage, and other sensitive data storage has increased the necessity for security Security is not an option anymore; it is a need that Website owners and developers should work in the creation process to guarantee its continuity.

Bibliography

1. Amin, A., Ul Haq, I. and Nazir, M. (2017). TWO FACTOR AUTHENTICATION. *International Journal of Computer Science and Mobile Computing*, [online] 6(7), pp.5–8. Available at: https://www.ijcsmc.com/docs/papers/July2017/V6I7201707.pdf.

2. Bressoud, T & White, D. (2020). The HyperText Transfer Protocol. 10.1007/978-3-030-54371-6_20.
3. C. Braz and J.-M. Robert.(2006) Security and usability: thecase of the user authentication methods. In InternationalConference of the Association Francophone d'InteractionHomme-Machine,
4. Cobb, M. (2005). SQL Server Security. Elsevier Inc.
5. Corbett, S. (2013) "The retention of personal information online: A call for international regulation of privacy law", in Computer Law & Security
6. Review, Vol. 29, Issue 3, June 2013, pp. 246–254, doi: 10.1016/j.clsr.2013.03.005

7. HTML ENTITIES HTML ENTITIES. (2020). [online] Available at: https://www.tutorialspoint.com/html/pdf/html_entities.pdf.

8. IBM Security Services. (2015) "2014 Cyber Security Intelligence Index." pp. 3, https://www.ibm.com/developerworks/library/se–cyberindex2014/se–cyberindex2014–pdf.pdf

9. Php.net. (2019). *PHP: Prepared Statements - Manual*. [online] Available at: https://www.php.net/manual/en/mysqli.quickstart.prepared-statements.php.

10. PHP. (2020). Sanitizing User Input. Retrieved from https://www.php.net/manual/en/security.filtering.sanitization.php

11. P O'Brien, Scott W.H. Young, K Arlitsch, K Benedict, (2018) "Protecting privacy on the web: A study of HTTPS and Google Analytics implementation in academic library websites", Online Information Review, Vol. 42 Issue: 6, pp.734-751 https://doi.org/10.1108/OIR-02-2018-0056 2018-09

12. W3schools.com. (2019). *CSS Fonts*. [online] Available at: https://www.w3schools.com/css/css_font.asp.