

Christine Woods 1704446

by Christine Woods

FILE	5594_CHRISTINE_WOODS_CHRISTINE_WOODS_1704446_241229_20893 32026.DOCX (60.34K)		
TIME SUBMITTED	15-MAY-2020 10:27AM (UTC+0100)	WORD COUNT	972
SUBMISSION ID	127728693	CHARACTER COUNT	5143

PHP

Christine Woods 1704446

Web Technologies

Christine Woods 1704446

School of Applied Computing

University of Wales Trinity Saint David

Declaration by Christine Woods

The work of this report completed under the supervision of Gaynor Thomas. I declare that this report is the product of my own work and is not being submitted for any other degree etc.

Christine Woods .

Acknowledgments

- Gaynor Thomas – UWTSD Lecturer

Introduction

This website has been developed to show an information-based website using PHP. The topic used has been the Medicines Management Department in Swansea Bay Health Board (information is fictional for the purpose of this assignment).

The website connects to the data which has been stored in a normalised database which is accessed, information retrieved, and results displayed.

There is a search function that displays results taken from the database.

The website gives the ability to add, edit and delete records.

It shows basic security measures taken to protect information and has used CRUD functionality.

Contents

INTRODUCTION	5
1. OVERVIEW OF SECURITY MEASURES	7
2. ADDITIONAL SECURITY MEASURES.....	8
2.1 Digital Certificates.....	8
2.2 SSL	8
2.3 Prepared statements.....	8
2.4 File Management	8
2.5 General Measures	8
3. REFERENCES.....	9

1. Overview of security measures

The idea of this website is to hold sensitive information that may only be accessed by those given the correct security login information. It will hold information regarding the Medicines Management department e.g. meeting details along with personal staff details e.g. personal telephone numbers.

There are several security issues that need to be addressed.

The website includes a log in screen which ensures that only those that have been given a login and password may gain access. If incorrect details are entered the website returns a response to the user asking them to try again. This is a good form of security measure although it would not be enough should this website go live. Without good security measures your information is vulnerable and easy for on-line hackers to take advantage of. Attackers are often experienced and can easily gain access to your website and then use it to their advantage to download malicious content. Input and output code should be protected.

Within the Health Board passwords generally expire after 3 months to ensure that they remain secret, this would also need to be added to this website as passwords can be shared or seen by others.

Spambot is a common problem, this is a computer program that gains access to your program sending spam emails. In order to stop this kind of attack CAPTCHA [1] can be used (a challenge/response test determining if the user is a human or a robot).



Figure 1. Example of CAPCHA to eliminate spam attack.

It is not only important to stop access to the website it is also important to stop access to the database. If hackers manage to infiltrate the database, they may enter a specific SQL command within the form to secure the response that is inputted. This will assist the hacker when trying to work on the construction of the data base. This is called SQL Injection [2] and may be used to delete data, steal it used for ransom, or to deface the website. It may be used against one webpage or if there is a network it may be used against the whole system.

Hackers could easily use password' or 1=1 within the password field which then allows access to the database.

To prevent this the user input should be validated, using prepared statements (these are statements that have the parameter values transmitted using a different protocol later on,

therefore the original form is not completed using external input and SQL injection is eliminated). Using the bind_param () function tells the SQL query what parameters and type of data to expect thus minimising the chances of SQL injection.

2. Additional Security Measures

Should the website be implemented, and further functions added, the security measures would need to be enhanced. The following points would need to be implemented to ensure the site could not be tampered with.

2.1 Digital Certificates.

Digital Certificates provide a good level of security as it uses a commercial organisation who can vouch for the identity of the people or organisation with which you are identifying. The organisation provides a certificate that can be verified ensuring who they are. This is a necessary requirement for any website that is protecting their website.

2.2 SSL

The Medicines Management website is for information only, should the website be designed to take payments the security of this website must ensure that it is protected against attacks. Using SSL (Secure Socket Layer) provides protection against threats by using the certificate process and a collection of keys to exchange information to allow protected communication for messages to ensure they have not been infiltrated by a third party. By using the HTTPS protocol, the SSL function is incorporated on initial connection.

2.3 Prepared statements

Cross-site scripting (XSS) and SQL Injection attacks [3] are the most common security problems when using PHP. Additional security measures would need to be implemented to ensure that the Medicines Management website remained safe. This can be achieved by using prepared statements as mention in section 1.

2.4 File Management

Hiding the files in a root directory ensures that an attacker cannot gain access to them through the browser.

2.5 General Measures

To ensure database security good practice should always be adhered to, using firewalls, data encryptions, SQL protection along with checking the code will all help to provide a level of security.

3. References

- [1] C. M. University, "Capcha.net," 2000-2010. [Online]. Available: captcha.net. [Accessed 28 April 2020].
- [2] W. -. S. Injection, "w3SQL - Injection," 1999-2020. [Online]. Available: https://www.w3schools.com/sql/sql_injection.asp. [Accessed 28 April 2020].
- [3] Cloudways, "Ultimate PHP Security Best Practices," Cloudways, 1 January 2019. [Online]. Available: <https://www.cloudways.com/blog/php-security/>. [Accessed 15 May 2021].

FINAL GRADE

56/100

GENERAL COMMENTS

Instructor

Database - Generally OK structure. I can see that you've normalised out a jobs table which is good, but you don't need the full job title in the main table anymore, because this is available in the jobs table (make a join in the code to retrieve it)

7/10

Range of coding (eg joins, searches, admin tools)

Search is good and incorporates a wildcard.

Login is OK but be careful to protect all your pages - I was able to stumble into the protected area without logging in by going to firstpage.php in the URL. Any pages that are sensitive should be protected (as in the secret page shown)

Add doesn't seem to be entirely working, and needs validation. Possibly it's not working because all the database fields state they cannot be null, but you are not entering data for some of them.

I'm a bit mystified by the delete a staff member - you try to get id from the form, but it isn't in there? Not sure why you require the user to enter firstname, last name and job title as this isn't part of your query anyway?

Good use of the timestamp to show previous and future meetings

16/30

Overall Integration - A bit basic, but nevertheless a reasonable layout. Sometimes I get slightly confused with the navigation, but OK on the whole 6/10

Report

Issues identified/How issues relate to your website.

Some good issue identified, but a bit on the brief side. Also some good linking back to your site in the first part, and you've thought about it in context to the health board. SSL I think would need enabling, even without taking payments - there is some personal data being exchanged here.

16/30

Total 45/80

Overall - 56%

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9
