

Matthew Howells (P1702520) PHP web security report - final submission

by Matthew Howells

FILE	2386_MATTHEW_HOWELLS_MATTHEW_HOWELLS__P1702520__PHP_WEB_SECURITY_REPORT_-_FINAL_SUBMISSION_241229_1051347438.DOCX (179.19K)		
TIME SUBMITTED	02-MAY-2020 08:20PM (UTC+0100)	WORD COUNT	1093
SUBMISSION ID	125954060	CHARACTER COUNT	5878



Website with Dynamic Content

Matthew Howells (1702520)
(WISA)
Web Technologies (ACCA5022)
Gaynor Thomas

Monday, 5th May 2020

Contents

1. Introduction:	3
2. Key Findings:	3
3. Website Security Overview	4
3.1. Website Navigation:	4
3.2. Login Systems:	5
3.3. SSL Certificate	6
3.4. Website Spambots:	6

1. Introduction:

This report intends to work towards exploring the topic of cyber-attacks of online businesses and gathering an overview of how they would address these issues when producing a live website. This can include considering previous attacks that have been made against similar online platforms. For certain establishments, it may not be until their cyber systems are compromised that this topic becomes top priority. Throughout this assignment important measures have been researched and observed in order to work towards identifying many issues that are being addressed by connected operators.

2. Key Findings:

As expected, while researching, creators show that while developing any online content web security must always remain top priority [1]. This can help ensure that businesses are well prepared to avoid potential damage being made to their services. It is always ideal to handle potential cyber-attacks sensibly. This can include certain steps that companies take in order to avoid potential disruptions being made to their online services. Unfortunately, cyber criminals can have the skills to potentially gain unauthorised levelled access to operating web servers and databases in order to attack systems in various ways [2]. For this reason, simple steps and requirements must be followed in order to improve website security. This awareness or knowledge could ensure the safety and welling of the company Aswell as its staff, allowing for progression and development in future online company procedures.

3. Website Security Overview

3.1. Website Navigation:

While choosing to develop the designed School of Applied Computing (SoAC) information-based website, the dynamic user content had to be supported. For this reason, different styles of interactive features had to be rolled out as a way of providing an innocent user-friendly experience for all clients and visitors. This interactive process can include presenting a selection of navigation buttons as a way of allowing visitors to be able to navigate the website quickly. Unfortunately, fragmented navigation links can easily become embedded into a website, which may potentially lead to non-existent web pages containing malware. Organisation websites have been known as easy targets, where hackers produce malicious links to steal visitor's personal information or cause harm to electronic devices; this is categorised as phishing. Each navigation link has been tested as part of the SoAC website ensuring the correct links are made between each page.

3.2. Login Systems:

These days most popular websites including, online shops now offer users the chance to subscribe to their services by creating an online account. As part of this process, an active login form is what most website's offers visitors as a way of granting additional access to a website, in order to access hidden content. This considers the extra phases of important terms of authentication that are projected, when visiting any live website. This feature can select between verifying if an operator claims to be a definite individual wishing to responsibly access any undisclosed information, by using an allocated username and password. Often the vulnerability is found in a text input field for users, including a username, where an SQL statement is running within the background breaching confidentiality. As companies carry out potential developments, they may choose to roll out easier alternative log-in options by offering users multiple ways of accessing stored information. This can include asking different categorised security questions or passcodes in order to be granted additional permission, to perform a particular action. Most websites that are created by using PHP may accept text entry's as a username and password in order to grant access. SQL Injection Attacks can target these programmed pages by accepting unauthorised access, by entering a string that contains one single quote without requiring any usernames or passwords.

3.3. SSL Certificate

Secure Sockets Layer (SSL) certificates are expected on all websites: certificates are used, in order to convert data, in transit amongst the hosting web server and the clients web browser. This helps ensure that an information is sent to the right server and is not intercepted. While installed onto a web server, SSL activates a padlock and the https protocol, in order to allow secure connections, from web servers to browsers, to be made. SSL is used to protect credit card transactions, data handover and logins. Most recently SSL is becoming the normality when aiming to secure the safe browsing of various social media sites and portals. When visiting a website that is encrypted with SSL, the browser will form a connection with the webserver; look at the SSL certificate and then bind together the browser and server. This binding connection is secure so that no one besides the user and website that is submitting the information can see or access what is typed into the browser; this can be recognised by websites using https instead of http.

3.4. Website Spambots:

A spambot is a package which is designed to try to collect, or harvest, personal information such as e-mail addresses from the Internet, in order to construct mailing lists intended for sending unsolicited e-mails; this can also be known as spam. In order to beat spambots, certain website have now developed safeguards techniques during any sign-up processes. This can be demonstrated where users must confirm their identity, by filling out characters or clicking on pictures linked, to a category being asked. This stands as "Completely Automated Public Turing tests or CAPTCHA. Unfortunately, users of most websites are potentially at risk of having information stolen. This does not only affect everyday users using live websites, but it can affect the stability of the website, plus, accuracy of the data that is being filtered into the website. In addition to security issues, selected spambots may attempt to overload or slow down available web servers. This may slow down development as well as lowering rankings on search engines.

3.5. Encryption

Encryption is a process that encodes a message that can be only be read by certain people. This can include passwords that are stored within a hidden database. An example can be administrators who carry out regular maintenance developments or have the rights to change user details on request. A similar topic linked can include making sure any SQL embedded is sanitised in order to avoid further SQL injection being inputted to carry out damage. SQL injection allows attackers the opportunity to crack passwords by using similar pieces of code. It is always important for all users to change their password regularly for their own safety.

Matthew Howells (P1702520) PHP web security report - final submission

GRADEMARK REPORT

FINAL GRADE

51 / 100

GENERAL COMMENTS

Instructor

Database - You do have two tables, but they are stand-alone and not linked. You need to show normalisation between tables. "Department" would be an excellent field to make a foreign key.

5/10

Range of coding (eg joins, searches, admin tools) A reasonable search based on a radio button. The add a staff member needs validation, at the moment I can add a blank member of staff and it will add them - although curiously not to the users table so they wouldn't be able to log in? Add/Edit/Delete are working OK, although one of your links, "Delete a user login" doesn't work. Upload image works, but not in the way you intend - you don't write a database entry, so you don't know which staff member it relates to. Login is OK - you have protected access to the secret.php page, but not to any other page? I can still get in and search for example?

Overall, a reasonable attempt and you have demonstrated some skills.

17/30

Overall Integration - Try not to stretch the images, it makes them look bad. It is a bit strange to have almost all the website content on one page. Splitting it over several pages would help the user. 6/10

Report

Issues identified/How issues relate to your website.

You have identified some of the issues, I would have liked to see further research beyond the classwork - no references included? You should also be relating these points to the website produced which was the second part of the question. For example, is your login system good? If the site went live, would SSL be needed? Is your site susceptible to SQL Injection do you think?

13/30

Total 41/80

Overall - 51%

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7
