

1801285 Gemma Dunlop - Web Technologies Assignment 2

by Gemma Dunlop

FILE	11145_GEMMA_DUNLOP_1801285_GEMMA_DUNLOP_-_WEB_TECHNOLOGIES_ASSIGNMENT_2_241229_1078787522.DOCX (6.81M)		
TIME SUBMITTED	04-MAY-2020 07:09PM (UTC+0100)	WORD COUNT	1935
SUBMISSION ID	126177217	CHARACTER COUNT	9999



Website with dynamic content report

Gemma Dunlop (1801285)

Table of Contents

Table of Figures	1
Abstract	2
1. Introduction	2
2. Digital certificates and SSL	2
3. Spam Bots	3
4. SQL Injection	3
5. Password Hashing	7
6. CSRF	7
7. Firewalls	8
8. Conclusion	8
References	9

Table of Figures

Figure 1: HTTP vs HTTPS	3
Figure 2: Login Page on Marvel Website using 'OR 1=1--' as username.	4
Figure 3: Screenshot of Marvel page showing authorised access for the user.	4
Figure 4: Login page using 'OR 1=1--' as username and password.....	5
Figure 5: Screenshot of Marvel page showing authorised access for the user.	5
Figure 6: Main Menu showing user is logged in using SQL injection.	6
Figure 7: Login Page on Marvel Website using 'OR 1=1--' as username.	6
Figure 8: Screenshot showing access has been denied.	7
Figure 9: PHP code for hashing passwords.	7

Abstract

The vulnerability to cybersecurity threats are advancing in today's digital-first era and as companies, particularly law firms, aim to produce and transact more digitally.

The study 'Cyber Security Breaches Survey 2018' by the Department for Digital, Culture, Media and Sport reveals 98 percent of UK companies surveyed depend on a type of digital contact or service to support their clients and four out of ten (43 percent) have encountered some sort of cyber breach or threat during the past 12 months [1].

Website security is an important consideration for a company with an online presence, and it is as crucial as a website host. A hacked website can lose up 98% of its traffic [2]. Not having a secure website can lead to breach of client data and can result in loss of reputation, large fines and lawsuits.

1. Introduction

The project objective was to create an information-based website with dynamic content using php. The security issues that would need to be considered if the website were to be hosted on the web were discussed. A Marvel website was created to display information about Marvel films and TV shows, providing the novelty option for visitors to sign up to the website so they can contribute to the database by adding additional information about new films or TV shows. The website contains an admin page which can be accessed by logging in with the correct login details. Once logged it, an admin can add data, edit data and delete data from the database.

2. Digital certificates and SSL

The prime responsibility of a Web developer is to protect websites against forged attacks.

SSL allows data to be transferred in an encrypted form across networks. A Secure Socket Layer (SSL) certificate encrypts the communication between the user and the site server such that all third parties such as identity thieves and hackers find the information unreadable [3].

Digital certificates are used to show ownership of a public key by the entity that owns it [4]. An SSL certificate is a form of digital certificate that authenticates a website and allows for encrypted communication. Such certificates indicate to the user that at the time of the issuance of the certificate, the web site provider has shown ownership of the domain. An SSL certificate is essential for banking or ecommerce websites or an online service where the user must enter their credentials. The Marvel website would still require an SSL certificate as Google considers security of websites a ranking factor. To obtain an SSL certificate, the domain name and business ownership are verified, and basic SSL certificates are issued free of charge. SSL certificates benefit the website's security, Google ranking and visitor's security [5]. Since October 2017, Chrome (version 62) shows a "NOT SECURE" alert when

users enter text in a form on an HTTP tab, and in Incognito mode on all HTTP sites. Eventually, on all pages served over HTTP Chrome will show a Not Safe alert, irrespective of whether or not the page includes confidential input fields [6]. Therefore, the Marvel website should use HTTPS for all pages.

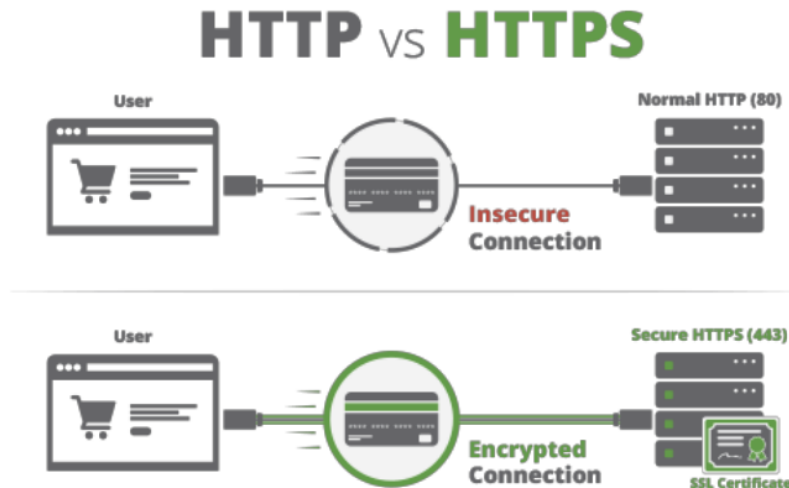


Figure 1: HTTP vs HTTPS [7].

3. Spam Bots

Bots are programs used to execute repetitive tasks, usually operating over the internet. Spam bots are malicious programs which post spam messages in various places. Once spam bots create fake accounts on websites, they can then spam messages in areas where users interact online such as forums and comment sections [8].

CAPTCHA [9] is a useful tool to prevent bots from creating accounts however it is not a completely foolproof strategy as it only prevents less sophisticated bots. Another useful trick is adding an extra question which is easy for humans to answer but not bots such as "What colour is the sky?".

Another method is using hidden input fields which humans will be unable see and to fill in but bots can. The Marvel website allows the user to sign up and they can add new data. Spam bots could sign up and add multiple irrelevant data to the database so adding a few methods to prevent spam bots is necessary. For the purposes of the Marvel website, the author would use CAPTCHA to limit bots from automatically adding content.

4. SQL Injection

SQL injection attacks inject malicious commands into user input parameters which are sent to the server instead of legitimate data. If a user enters their correct username and password,

they will be able to see their details once they're logged in. If a web application has not been properly built to sanitise data inputs, the hacker can inject SQL commands into the login form and retrieve data by gaining unauthorised access [10].

If the code ' OR 1=1--' is typed into the username field and the password "password1", the string

```
SELECT * FROM people WHERE username=" OR 1=1--" AND password='password1'
```

is created.

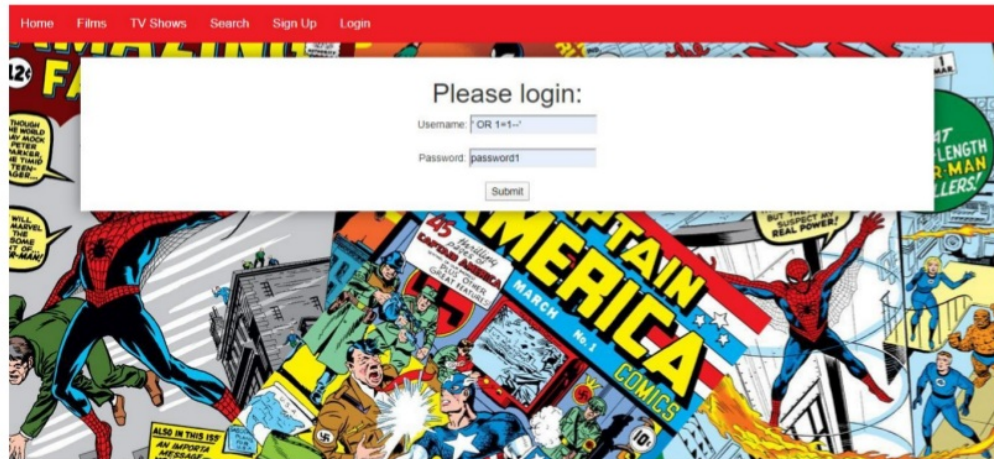


Figure 2: Login Page on Marvel Website using 'OR 1=1--' as username.

As a result, the user is logged in as admin, so has access to all admin features.

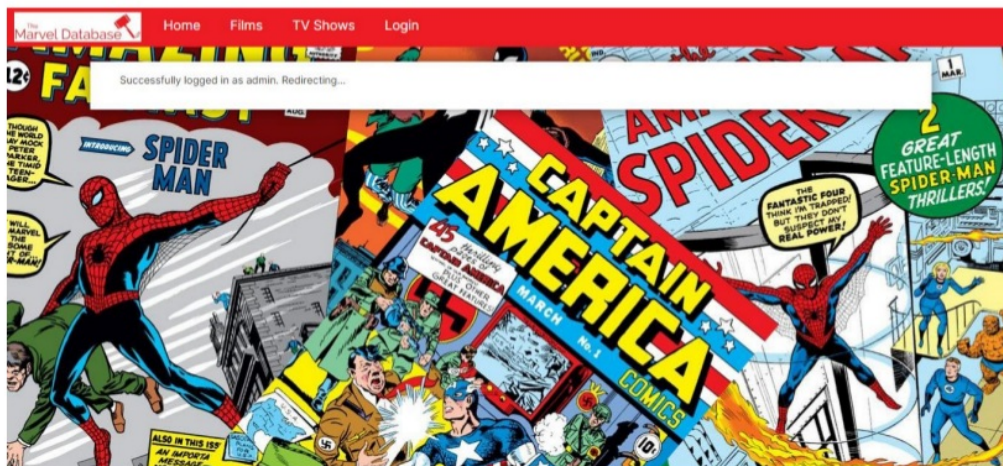


Figure 3: Screenshot of Marvel page showing authorised access for the user.

The password can also be bypassed by using the same code for the password.

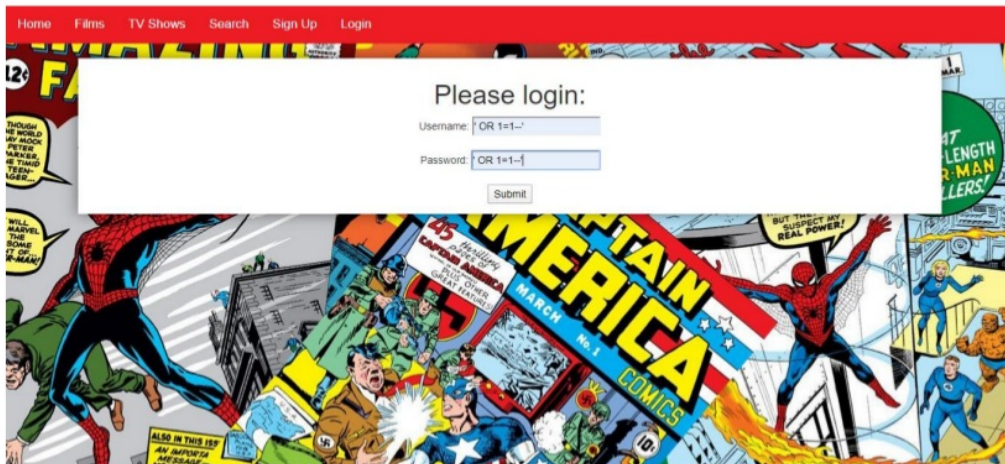


Figure 4: Login page using 'OR 1=1--' as username and password.

The user is logged in as admin, so has access to all admin features.

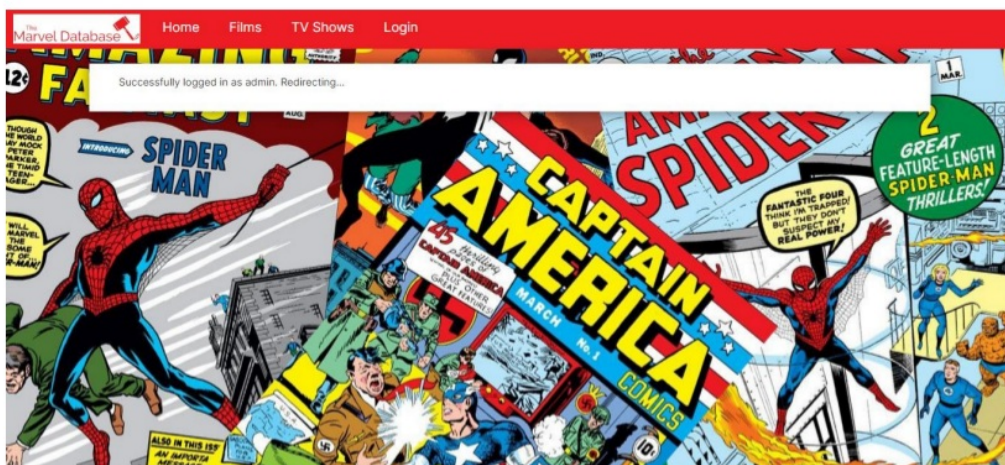


Figure 5: Screenshot of Marvel page showing authorised access for the user.

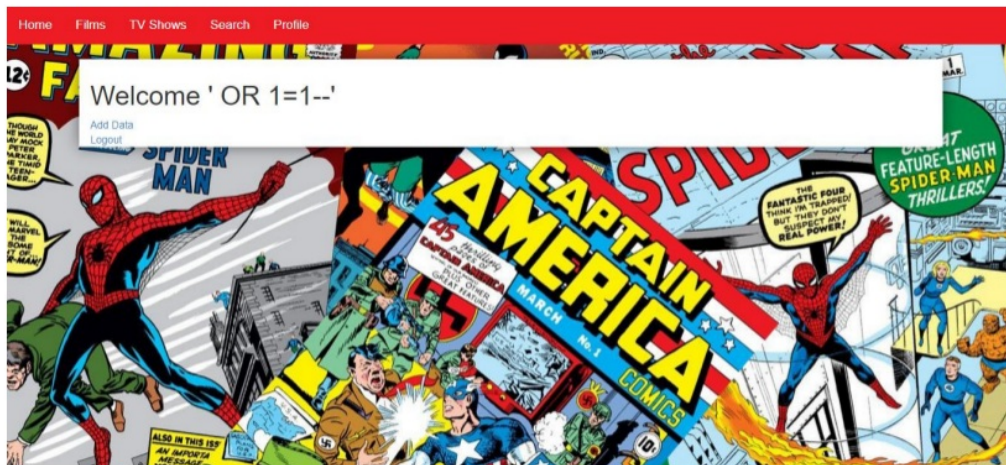


Figure 6: Main Menu showing user is logged in using SQL injection.

Code can be written to remove potentially dangerous characters before data is sent to the server.

```
$un=str_replace('\"', '', $un);  
$pw=str_replace('\"', '', $pw);
```

Now when the user tries logging in using these malicious SQL commands as shown in figure 2:

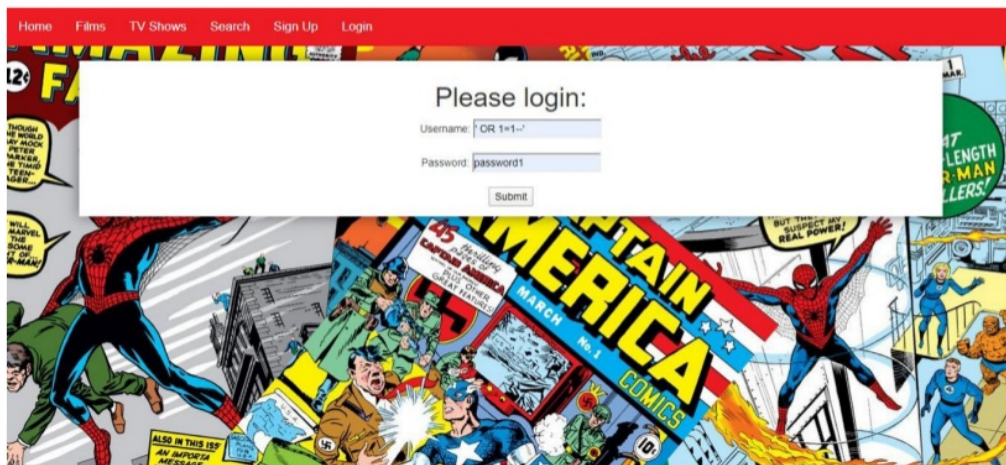


Figure 7: Login Page on Marvel Website using 'OR 1=1--' as username.

The user is denied access.

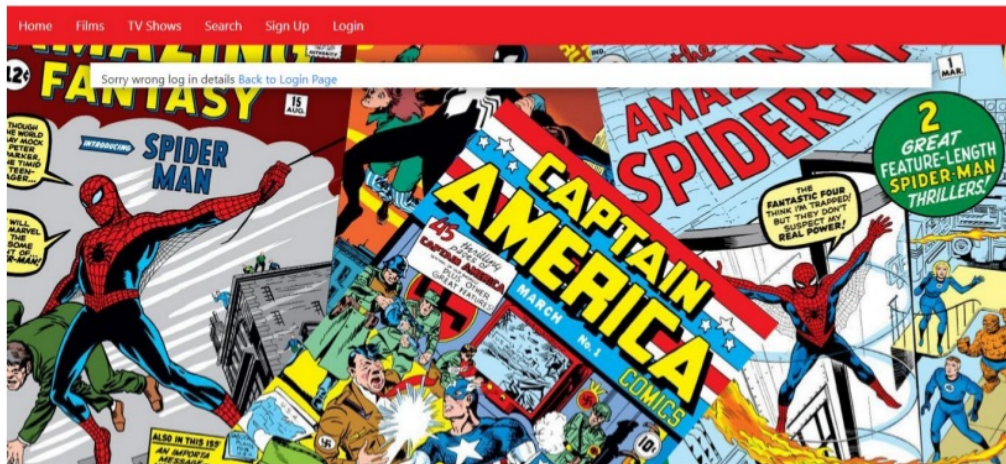


Figure 8: Screenshot showing access has been denied.

5. Password Hashing

A hash is intended to serve as a "one-way function": An operation performed mathematically which is easy to execute, but very difficult to reverse [11]. It transforms readable data, like other types of encryption, into a scrambled cypher. But instead of allowing someone to decrypt the data with a specific key, like standard encryption functions do, hashes are not designed for decryption.

Alternatively, any time the password is typed on a page, it automatically re-executes the same hash and compares the findings against the hash generated by the password when it was created, testing the integrity of the password without needing to store the vulnerable password itself.

Password hashing was used on the Marvel website as it is simple to implement, and it protect users' passwords in the database as shown in figure 8.

```
$hash = password_hash($pword, PASSWORD_DEFAULT);
```

Figure 9: PHP code for hashing passwords.

6. CSRF

Cross-Site Request Forgery is a form of malicious manipulation of a website where unauthorised commands are performed simply by using a successfully authenticated/authorised user's browser transmission [12]. In an effective CSRF attack, the attacker can involuntarily force the target user to perform an action. This may involve, for

example, changing the email address on their account, modifying the password, or making a transfer of funds [13].

If the Marvel website were to become live, it would be essential for suitable measures to be taken to prevent CSRF attacks from modifying user's personal info or adding data to the website which is irrelevant.

CSRF attacks could be shielded from users by using anti-CSRF tokens in an easy and very powerful way [14]. The fundamental concept behind anti-CSRF tokens (also known as synchronizer token patterns) is to provide a piece of information (token) to the internet server and to test if the web explorer sends it back. This bit of information would be unlikely for a third person to guess. Until the piece of information is checked, the application cannot continue.

7. Firewalls

Getting clear passwords and an SSL certificate is fine, but not always enough to keep the website secure. A web server firewall would be necessary for the Marvel website if it were to become live on the internet, so it is secure, and it works at its best.

It prevents unnecessary web traffic from reaching the site and offers security against:

- Breaches
- SQL injection
- DDoS attacks
- Cross-site scripting
- Brute force attacks
- Zero-day exploits [15].

8. Conclusion

The main purpose of this project is to create a database driven website which supports dynamic content.

An analysis of security concerns that were considered on the Marvel website were provided. The security concerns that would need to be addressed if the platform were to go live on the internet were also considered.

References

- [1] C. M. a. S. The Department for Digital, “Cyber Security Breaches Survey 2018,” 2018. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/70207/_Main_Report.pdf.
- [2] Sucuri, “How to Secure & Protect Your Website,” *What is Website Security?*, 12 November 2019.
- [3] A. Russell, “What is SSL?,” *SSL and Digital Certificates, SSL/TLS*, 7 October 2019.
- [4] T. U. o. T. Knoxville, “What is a Digital Certificate?,” Office of Information Technology, 2020. [Online]. Available: <https://help.utk.edu/kb/index.php?func=show&e=1960>.
- [5] S. Si, “Google Is Forcing You to Switch to HTTPS by October or Lose Rankings,” 28 February 2020.
- [6] E. Lawrence, “Avoiding the Not Secure Warning in Chrome,” *Web Updates 2016*, October 2016.
- [7] Securi, “How to Install an SSL Certificate,” [Online]. Available: <https://sucuri.net/guides/how-to-install>.
- [8] Andrzej, “How to Prevent Bots From Spamming Your Sign up Forms,” Elastic Email, 2019. [Online]. Available: https://elasticemail.com/blog/marketing_tips/how-to-prevent-bots-from-spamming-your-sign-up-forms.
- [9] Carnegie Mellon University, “The Official CAPTCHA Website,” CAPTCHA, 2020. [Online]. Available: <https://captcha.com>.
- [10] D. Kar, S. Panigrahi and S. Sundararajan, “SQLiDDS: SQL injection detection using document similarity,” vol. 24, no. 4, pp. 507-540, 2016.
- [11] T. S. D. a. S. Johnson, *Cryptography for Developers*, Elsevier Inc., 2007.
- [12] E. Larkin, “Don't Let Bad Guys Pose as You,” *PCWorld*, vol. 25, no. 4, p. 36–36, 2007.
- [13] P. Desai, “Preventing CSRF Attacks by Verifying Redirection Request and User Session,” *National Journal of Computer Science*, vol. 12, no. 1, pp. 15-26, 2019.
- [14] R. K. a. B. Meshram, “Client Side CSRF Defensive Tool,” *International Journal of Information and Network Security*, 2012.
- [15] N. Tower, “Why Every Website Needs a Web Application Firewall,” 20 October 2017.
- [16] A. S. a. L. A. R.L. Rivest, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Commun. ACM*, 21, no. 2, pp. 120-126, 1978.
- [17] I. Ristic, *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers*, Duck, 2013.
- [18] G. B. a. J.-m. R. Charles H. Bennett, “Privacy Amplification by Public Discussion,” *SIAM Journal on Computing*, 13, no. 3, pp. 661-674, 1984.

1801285 Gemma Dunlop - Web Technologies Assignment 2

GRADEMARK REPORT

FINAL GRADE

66/100

GENERAL COMMENTS

Instructor

Database - Good structure with suitable normalisation on genre. I might have been tempted to make films and tv shows the same table with a field to distinguish, as the majority of the fields are the same and it would allow more efficient searching.

8/10

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

The search is OK but a bit basic - you could use a wildcard here so that when someone searches for "Iron Man" they see both movies. Good use of passing a parameter to the "TV expand.php" page. Sign up is working -but if the fields are left blank, but the user is simply told it has worked. Some validation/feedback is needed.

Login/out is working, but you need to protect the Add film page, it is possible to reach it via the URL when not logged in (as we did with the "secret" page in class)

Add film isn't entirely working - I suspect this is due to a lack of validation more than anything else - the code is OK. Edit username also working OK. No delete?

The link to "sign up to our database" takes me to the search page?

18/30

Overall Integration - Generally the layout is good, but when using the site I'm sometimes left wondering what's happened. More validation/feedback to the user would fix that - just a bit clearer in the signposting. 7/10

Report

Issues identified/How issues relate to your website.

Some good issues identified here. You have also linked the issues to the website produced, albeit a bit briefly in some cases! A good effort.

20/30

Total 53/80

Overall - 66%

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10
