Commentary Week 4

Remember that you need to add some weekly comments (400 words). Being able to login to a site is a key component for many web sites. Consider the security aspects that you have put into your site which is just to protect the comments section. What is you were selling items from your site? Talk a bit about whether the security you have on your site is enough; and outline any improvements for a selling site. (300 words)

Logging in to my items web site is necessary, if the user wants to comment on an article linked to an item being displayed. Until now this is the only use of being logged in and having an account, but usually having an account has many more functions, for example buying items, which might be included in the future.

The security aspects that need to be taken into consideration, is making sure that there cannot be any SQL injections into the database. This is secured as inserting into the database is done using prepared sql statements, which enable higher security. Since data laws have increased for storing any type of information on the user’s data, there should be a pop up, asking the user to agree to the Terms and Services, as personal information including their email and their first and surname is stored in the database. Furthermore, the account holders’ passwords are hashed, and they are not stored in the database user table openly, but only the hashed version is used.

If my website would start selling items, the data needed on each user would be more sensitive. Currently only the email of the user logged in is displayed openly, which is also used as to login to their account. This could be unsafe and in future developments should display usernames where users are aware that these will be displayed openly. In addition to this a session variable should be created which automatically logs the current logged in user out after a certain amount of time has passed. Also, a warning should be displayed to users as the comments section also displays the users email, which could be seen as sensitive personal data.

Discus clearly how you would set the session maximum length to 5 mins. (100 words)

I would want to set a maximum session length to 5 minutes, to ensure security for the user that is logged in to that time. This is done by making 5 minutes the default value of the amount of time that the session used should be destroyed since the active user has interacted with the website. I would have to set session.gc\_maxlife to 300s. Checking in my code using (time - $\_SESSION[“last\_used”]) <300s ; which is checking whether the logged in user has been inactive on the site for more than 5 minutes; 300 seconds running an infinite while loop. If this is true, then reset the “last used” variable so the user can still be logged in and use the website. Yet if this statement is false, destroy the current logged in session variable, or set it equal to a time in the past. This needs to be don’t be using session:unset(); and session\_destroy(); which logs out the current user.