Web Application Development

Trevor Kiggundu
001001720
December 2019

A report submitted in fulfilment of the requirements for the module, Web Application Development, Computing and Information Systems Department, University of Greenwich.

COMP1687 Self-Assessment Sheet for the 2019/20 Coursework

Student name: Trevor Kiggundu Student ID: 001001720

URL: https://stuweb.cms.gre.ac.uk/~tk9894h/webcoursework/homePage.php

Student Use													
		Total Mark	Please circle ONE of the grades (0 to 10) for each level below [Level 1 to Level 5]										
Level 1	Account creation & login	15	0	1	2	3	4	5	6	**7**	8	9	10
Level 2	Student Tasks	15	0	1	2	3	4	5	6	**7**	8	9	10
Level 3	Tutor Tasks	30	0	**1**	2	3	4	5	6	7	8	9	10
Level 4	Cookie	5	0	1	2	**3**	4	5	6	7	8	9	10
Level 5	Usability	5	0	1	2	3	4	5	6	7	**8**	9	10
Staff Use													
Self-assessment		5	0	1	2	3	4	5	6	7	8	9	10
Level 6	LSEPi discussion	25											

Comments:

What the student did well in this assignment?

- The usability of the application was good. I made sure to use some form of CSS to make the page look good.

What the student could improve in this assignment?

- Completion of the required tasks of level 1, before attempting level 2 etc.
- More research into coursework features, better database designs.

What the student can take forward to your next assignment?

- Better time management.
- More reliance on the tutors for feedback.
- Prior research before programming to avoid restarting the coursework.

Application Functionality:

Level 1: Account Creation and Login

- Most of level 1 completed.

Level 2: Student Tasks

- Half to most of level 2 completed

Level 3: Tutor Tasks

- Minimal parts of level 3 completed.

Level 4: Cookie

- Minimal parts of level 4 completed.

Level 5: Usability

- Most of level 5 has been implemented.

Description of Bugs in system:

Level 1: Account Creation and Login

- Duplicate ID's can be entered into the database, leading to confusion. Passwords cannot be stored as encrypted; they can still be viewed in the database. Session state does not prevent unauthorized access.

Level 2: Student Tasks

- The student does not have provision to save the peer evaluation without finalising it; cannot later edit/change it during a different login instance. Image only saves as a string in the database, not an image/blob.

Level 3: Tutor Tasks

- Tutor can login with admin login/password: 000000000, however the tutor will be directed to a student style page, emphasizing a lack of functionality. All of the other tutor functionalities are missing.

Level 4: Cookie

- Minimal cookie implementation inside the code. General webpage cookies are evident, but they were not invoked by the students' code.

Level 5: Usability

- Minimal issues regarding usability, the application is responsive rather than adaptive.

Level 6's article:

1 Introduction

There have been numerous rapid advances in the technological field throughout the 20th and 21st century, both regarding the hardware and software aspects of the practice. A product of such software developments is a 'cookie', which in web development terms, refers to a "small piece of data that a server sends to the user's web browser" (Anon, n.d.). Cookies changed the landscape of web development completely, as they allowed for better session management, personalization and tracking features, aiding in the storage of "current state information of a website in the user's computer" (Mazerick, 2015). With all technological advancements however, comes a new trail trail of accidental issues that would have never existed before the given change, and cookies, unfortunately, are not immune to this phenomenon. This essay aims to discuss the Legal, Social, Ethical and Professional (LSEPi) issues that could potentially plague a product attempting to use cookies, as well as the Political, Philosophical and Economic implications (PPEi) involved, in order to efficiently risk assess those possible occurrences and aim to provide suitable solutions regarding the given task of Web Application Development.

2 Types of Cookies

There are various different types of cookies, with each performing different tasks and given different permissions in a web application. The two main types however, are 'session cookies' and 'persistent cookies'; a session cookie "goes away when the user shuts the browser down", while a persistent cookie "resides on the hard drive of the user and is retrieved when the user comes back to the Web page" (MDN Contributors, 2019). Despite their positive impact on the advancement of software and web design, the creation of cookies brought along an onslaught of issues regarding legality, sociability, ethics and professionalism as they involved the handling of user inputted and/or saved data.

3 Legal Issues

A common legality issue that plagues cookie usage is the illegal copying and distribution of user data, a practice that can potentially jeopardize multiple aspects of the client's everyday lifestyle. The lack of a properly functioning cookie in web development could result in encryption issues, exposing sensitive user data and violating the Data Protection Act of 2018, which is designed to "protect personal data stored on computers" (UK Government, 2018). Violations of these rules are highly scrutinized, with fines "up to £500,000 for failure to comply with the Data Protection Act" (Zaheer, n.d.), further stressing the importance of proper cookie implementation. However, even seemingly functioning cookies can be prone to threats. The most common way to achieve this is via 'network eavesdropping', a practice where hackers use non-encrypted cookies to "impersonate a user and perform a malicious task" (Frankenfield, 2019). Luckily, there have been numerous software solutions to combat problems like these, such as 'HTTPS protocol',

which only send a cookie via an “encrypted channel, such as a TLS connection” (Barth, 2011). Nevertheless, failing to properly secure a web application and its corresponding cookies can lead to consumers filing legal complaints if their information is compromised, especially as the web developers are obligated to keep this information secure.

4 Social Issues

Social issues regarding web development mainly involve providing the same equal access to all users and maintaining diversity. This can be a difficult topic to assess when talking about cookies, although there are a lot of talking points that emphasize the compatibility and functionality of the web application across different demographics. A large amount of these topics are discussed in the Disability Discrimination Acts of 1995 and 2010, the latter being a much more revised version of the former due to the change in societal norms. The implementation of a cookie must not make the application “impossible or unreasonably difficult” (UK Government, 2010) for any persons to make use of the service. The implemented cookie must allow for a complex “range of accessibility and usability functions for all users” (UK Government, 2010) regardless of previous user activity. This seems straightforward enough but can become complicated when concepts such as ‘cookie profiling’ are introduced; cookie profiling is the act of using “permanent cookies to track a user’s overall activity online” (Anon, n.d). Cookie profiling can introduce bias that would possibly contradict the Disability Discrimination Acts, as personalized profiles would lead to certain users being given different information compared to others, based on their “browsing habits, age, marital status, and political and religious affiliation” (UK Government, n.d.). The introduction of cookies brings along all these concerns, and it is the duty of the provider of that service to take such steps to resolve/remove the problematic feature(s).

5 Ethical Issues

A variety of ethical issues that involve cookie usage in web development are heavily intertwined with problems of legality as well. Theft in itself is not only unethically correct; it is also a crime, and the fact that some cookies store data on local machines can make this data vulnerable to “cookie hijacking” (Anon, n.d.), with a relatively low level of authentication required. Other techniques such as ‘Cross-site request forgery’ (CSRF), can completely allow hackers to perform feats such as requesting private server details to withdraw money from bank accounts. This is of course, an extreme scenario, but there are other ways that ethical rules can be violated when discussing the topic of cookies. An all too familiar example involves the use of third party cookies, which are typically used by smaller webpages to generate advertising revenue for their growing websites. This can become problematic if/when certain websites fail to disclose the use of third-party cookies, leading to a “lack of consumer trust if cookie use is discovered” (Miyazaki et al, 2008). This lack of trust can lead to the developers losing consumers in general, damaging the overall web application itself. The lack of respect regarding ethics can in turn, also

lead to further legal issues depending on the severity of the offense, so it is very important to be precautious when implementing cookies into a web application.

6 Professional Issues

When developing a system that requires human interaction, there are always going to be professional obligations to the user; these have been broken down into four main objectives. The cookies that are implemented on a webpage must be able to "maintain confidentiality, maintain anonymity and respect copyright (Anon, n.d.) to the user when applicable. The professional issues highlighted are very heavily linked with the previously mentioned legal, social, and ethical issues, though the topic of respecting copyright has not been discussed yet. This can become a problem when a web application is optimized to use third party cookies and does so without the consent of the product that is to be advertised. Failure of a web application to identify the source of a third-party cookie can make the application subject to a copyright claim, leading once again to a lack of trust, confidence and termination of partnership between the two associates. This situation can also be represented on the client side if the use of these cookies is not disclosed to the user, voiding the promise to "maintain consent" (Anon, n.d.) to the user. It is the responsibility of the developers to make sure that the correct professional procedures are followed when implementing cookies into the webpage, as the lack of proper execution can lead to serious consequences.

7 Political

The political and social issues regarding HTTP cookies are almost synonymous, with political issues being a bit trickier to scrutinize as they differ from region to region. A majority of the information detailed in this paper has been based on European Union (EU) Cookie E-Privacy Directives. However, we must not forget that not every country in the world follows EU policies, and there are countries with both weaker and stronger jurisdiction. A developer implementing cookies onto their website should consider the fact that various cookies might not be permitted in other countries. Some countries do not allow for advertising of certain products or ideas, such as Saudi Arabia, a country in which "influence of censorship is still highly prevalent" (Philippe, 2009). This is a region that is known to alter advertisements that do not "comply with the established Islamic laws". This can be a problem for websites using third party cookies, as these external advertisements might not entirely reflect the views of the website. Developers must be mindful of these issues to avoid any possible conflict in an age where a lot of companies are "feeling the pressure to assimilate into other cultures". They must also be wary of how their cookies can be manipulated to spread political propaganda. An example of this involves the 2016 United States Presidential Election, one in which Russia was found guilty of meddling with Facebook advertisements to "promote amplifying divisive social and political messages" (Facebook, 2019) during an extremely important election.

8 Philosophical

Philosophical questions can still be raised about the implementation of cookies despite the advances they have brought along to the technological field. There is still a lot to be desired when examining the reality of modern cookie usage. The overall security of cookies can and should be improved, as there are still too many instances in which “security vulnerabilities” (Vamosi, 2008) are plaguing large companies such as Google and Facebook. The article written by Vamosi (2008) details an occurrence in which a Gmail cookie was disappointingly “stolen via Google spreadsheets”. Publications like these deeply emphasize the fact that even the biggest and most technically sound companies are subject to these threats, and that is the harsh reality of cookie usage. These downfalls have also led to the creation of alternative mechanisms that aim to replicate the function of the cookie with varying positive and negative outcomes; JSON web tokens, hidden form fields and ETags are all products of this research. These new mechanisms show that the fundamental nature of a cookie can and probably will not be changed too much without completely creating a whole new tool. However, there are still many improvements that can be made to the modern cookie, as it remains a very reliable mechanism.

9 Economic

The economic issues regarding cookie implementation revolve deeply around all of the LSEP issues. As mentioned earlier, on the consumer side, the use of various techniques by hackers can allow them to steal customer bank details and commit fraudulent acts such as “withdrawing money from bank accounts” (Anon, n.d.). These can cause economic issues for the consumer, especially if a substantially large amount of money is stolen. Luckily enough, a lot of this damage can be reversed, with Laughton-Coles (2017) stating that “if your money has been taken as a result of fraudulent activities you'll be reimbursed by your bank, as long as it can't prove that you've been grossly negligent”. The consequences on the developer side are a bit less sinister and straightforward, but they are still as important and even less forgiving. Failure to hire the proper professionals to properly encrypt and implement functional cookies can lead to lawsuits later if customer information is compromised, and as mentioned before, these fines can rise as high as £500,000. This leads to financial losses in addition to the humiliation already endured as a result of a breach of data protection policies. Issues like this are easily avoidable if the organization is willing to pay for the proper services/personnel. A small investment like this can save a company hundreds of thousands of pounds, as well as cement them as a trustworthy organization, but they must make the first step towards that securing those privileges.

Conclusion

The creation of cookies has, by no shadow of a doubt, changed the landscape of the software-based technological field. At their best, they are one of the most useful tools on a website, simplifying the essential functions of a modern webpage; at their worst? A controversial and potentially harmful tool that can be exploited for various unethical, political and economic

reasons. At the end of the day, only the developer can be blamed when a cookie falters, and until further advancements are made, they must continue to cater for the Legal, Social, Ethical and Professional, Political, Philosophical and Economic issues that are bound to arise.

References:

- Anon (1995) Disability Discrimination Act 1995, *Legislation.gov.uk*, Statute Law Database, [online] Available at: http://www.legislation.gov.uk/ukpga/1995/50/contents (Accessed December 9, 2019).

- Anon (n.d.) Maintaining Session State with Cookies, *Microsoft Docs*, [online] Available at: https://docs.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms526029(v=vs.90)?redirectedfrom=MSDN (Accessed December 9, 2019).

- Anon (n.d.) What is a cookie profiling? Cookie Tracking , facebook privacy issues, *All About Cookies*, [online] Available at: https://www.allaboutcookies.org/cookies/cookie-profiling.html (Accessed December 9, 2019).

- Barth, A. (2011) HTTP State Management Mechanism.

- Facebook (2019) An Update On Information Operations On Facebook, *About Facebook*, [online] Available at: https://about.fb.com/news/2017/09/information-operations-update/ (Accessed December 9, 2019).

- Frankenfield, J. (2019) What Is an Eavesdropping Attack?, *Investopedia*, Investopedia, [online] Available at: https://www.investopedia.com/terms/e/eavesdropping-attack.asp (Accessed December 9, 2019).

- Laughton-Coles, A. (2017) Is ID theft protection worth it?, *Is ID theft protection worth it?*, GoCompare, [online] Available at: https://www.gocompare.com/money/id-theft-protection/ (Accessed December 9, 2019).

- Mazerick, R. (2015) Risk Associated with Cookies, *Infosec Resources*, [online] Available at: https://resources.infosecinstitute.com/risk-associated-cookies/#gref (Accessed December 9, 2019).

- MDN Contributors (2019) HTTP cookies, *MDN Web Docs*, Mozilla , [online] Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies (Accessed December 9, 2019).

- Miyazaki, Anthony D. (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," Journal of Public Policy & Marketing, 23 (Spring), 19–33

- Philippe, T (2009). "Advertising in Saudi Arabia". ISCOM

- UK Government (2018) Data Protection Act 2018, *Legislation.gov.uk*, Statute Law Database, [online] Available at: http://www.legislation.gov.uk/ukpga/2018/12/section/1 (Accessed December 9, 2019).

- UK Government(n.d.) Equality Act 2010, *Legislation.gov.uk*, Statute Law Database, [online] Available at: http://www.legislation.gov.uk/ukpga/2010/15/contents (Accessed December 9, 2019).

- Vamosi, Robert (2008). "Gmail cookie stolen via Google Spreadsheets". *News.cnet.com*.

- Zaheer, A. (n.d.) consequences of not following the data protection act Archives, *Seersco Articles*, [online] Available at: https://seersco.com/articles/tag/consequences-of-not-following-the-data-protection-act/ (Accessed December 9, 2019).