M O'Rourke

BIT695 – TMA4 | 3910662

BIT695 – Web Technologies

Tutor Marked Assessment 4

TASK ONE:

1. *With reference to the case study from TMA1, do you think the web application for the case study would be considered secure and pass any of the tests according to the OWASP guide?*

Using the case study from TMA1 to consider if it would be secure or pass any of the tests according the Open Web Application Security Project (OWASP) will be discussed. As noted by OWASP “the aim of the project is to help people understand the what, why, when, where and how of testing web applications.” (OWASP, 2014, p.9)

As advised by OWASP (2014) there are three components to ensure that any testing will be effective: people, process and technology. The use of technology to make sure that a project is implemented properly, the process to make sure that acceptable policies and procedures are in place and people to make sure they understand how to use the procedures through awareness and training. Testing by using all the components of people, process and technology will help an organisation detect any issues before they grow into problems such as bugs in the technology.

Along with the three components when testing web applications the issue of security needs to be considered as part of the project process. OWASP (2014) states “it is essential to build security into the Software Development Life Cycle (SDLC) to prevent reoccurring security problems with an application.” (p. 11)

Using the case study of the Board Games Aficionados and the internet considered in TMA1, we will look at whether the case study will pass or fail any of the testing noted by OWASP. In the first instance, the case study does consider all the three components of people, process and technology. But to a limited extent for all three components. Limited in the case of people due to availability of resources such as rooms and members, limited in the process for the Board Games Aficionados as no clear procedures or policies are noted about how the club should be run and limited in technology as the club’s website is only hosted by a free internet provider.

OWASP (2014) discusses some ten principles of testing, we will consider three of these principles and compare it to the case study of TMA1 to check whether they would pass or fail according to OWASP.

The first principle we will consider is that of understand the scope of security for a project. According to OWASP (2014), this concerns knowing how much security a project will need. In that the level of security for a project will be given a certain classification, that is “a classification that states how they are to be handled (e.g., confidential, secret, top secret).” (OWASP, 2014, p. 12) If we look at the case study for the Board Games Aficionados club, there has been no discussion of security for the club and no level of security has been noted. At this stage, I would say that the Board Games Aficionados club has failed the principle of the scope of the security due to lack of understanding about how much security is needed for the club and the information gathered by the club has no clear classification level. These requirements need to be taken into account when developing the club’s profile further on the internet or on a mobile application.

The second principle to be considered is that of using source code when available for a project. This refers to testing code used for a project, as noted “it is difficult for dynamic testing to test the entire code base…if the source code for the application is available…(give) to the security staff to assist them while performing their review.” (OWASP, 2014, p.12) When comparing this principle with the TMA 1 case study of the Board Games Aficionados club, we would like to provide a pass for club as we can advise the code for the club has been standards-compliant tested with the use of two validation services provided by W3C.

As noted by the following websites:

* W3C mark-up validation service <https://validator.w3.org/>
* W3C CSS validation service <https://jigsaw.w3.org/css-validator/>

The final principle to be discussed will be that of documenting the test results. OWASP (2014) states “it is important to produce a formal record of what testing actions were taken, by whom, when they were performed, and details of the test findings.” (p.12) When we consider the study case of Board Games Aficionados from TMA1 against the principle of documenting test results, this would be noted as a fail for testing under OWASP. As there is no documented record of any testing actions that have been done.

1. *Use your favourite web browser and browse to* [*http://panmore.com/the-ciatriad-confidentiality-integrity-availability.*](http://panmore.com/the-cia-triad-confidentiality-integrity-availability) *Read through the article and answer the following. Feel free to use alternative sources should the above article prove to be insufficient.*

What do we mean by availability as noted by Henderson (2016)? He states that availability is one of three main goals to ensure information is secure, as information technology is used both at home and in organisations. He further advises:

“…availability is the situation where information is available when and where it is rightly needed…is linked to information security because effective security measures protect system components…(to ensure) that information is available.”(Henderson, 2016, para. 6)

For any e-commerce web application making sure that users are able to access information when needed is important.

As noted by Kesh, Ramanujan & Nerur (2002), availability happens when the necessary systems are available when required. “For an e-commerce site this means that the customer order systems are available all the time…..two major threats to availability problems are virus attacks and denial of service (DOS)” ( Kesh, et al, 2002, p. 150)

Kesh et al (2002) advises that a virus attack can happen when viruses are attached to files that need to be executed and can affect different programmes and documents of an e-commerce site by deleting or changing files. While Denial of Service (DOS) happens when a system is overloaded with loads of information that blocks access for legitimate users of an e-commerce site. And is mainly achieved through emails or fake hosting addresses.

If an organisation was to solely rely on the three measures noted by Henderson (2016) of confidentiality, integrity and availability as a guide to measure how secure information is. Then that organisation would not be responding to dynamic technology developments that can happen in a short period of time.

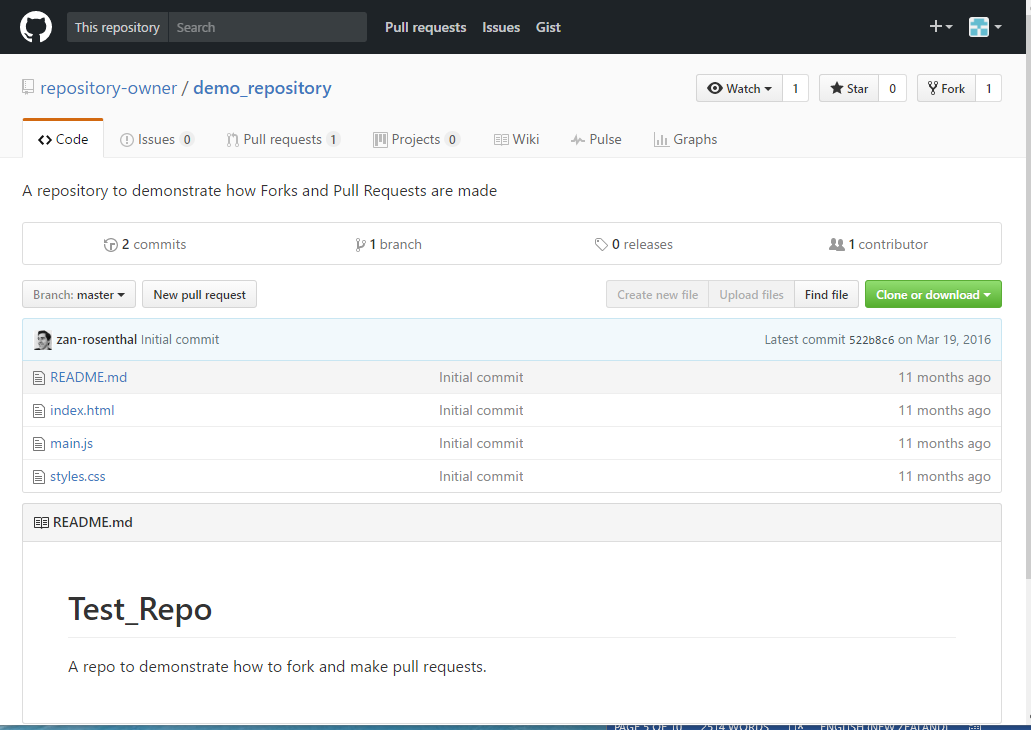
Chan & Kwok (2001) provides a definition of web-based e-commerce applications as:

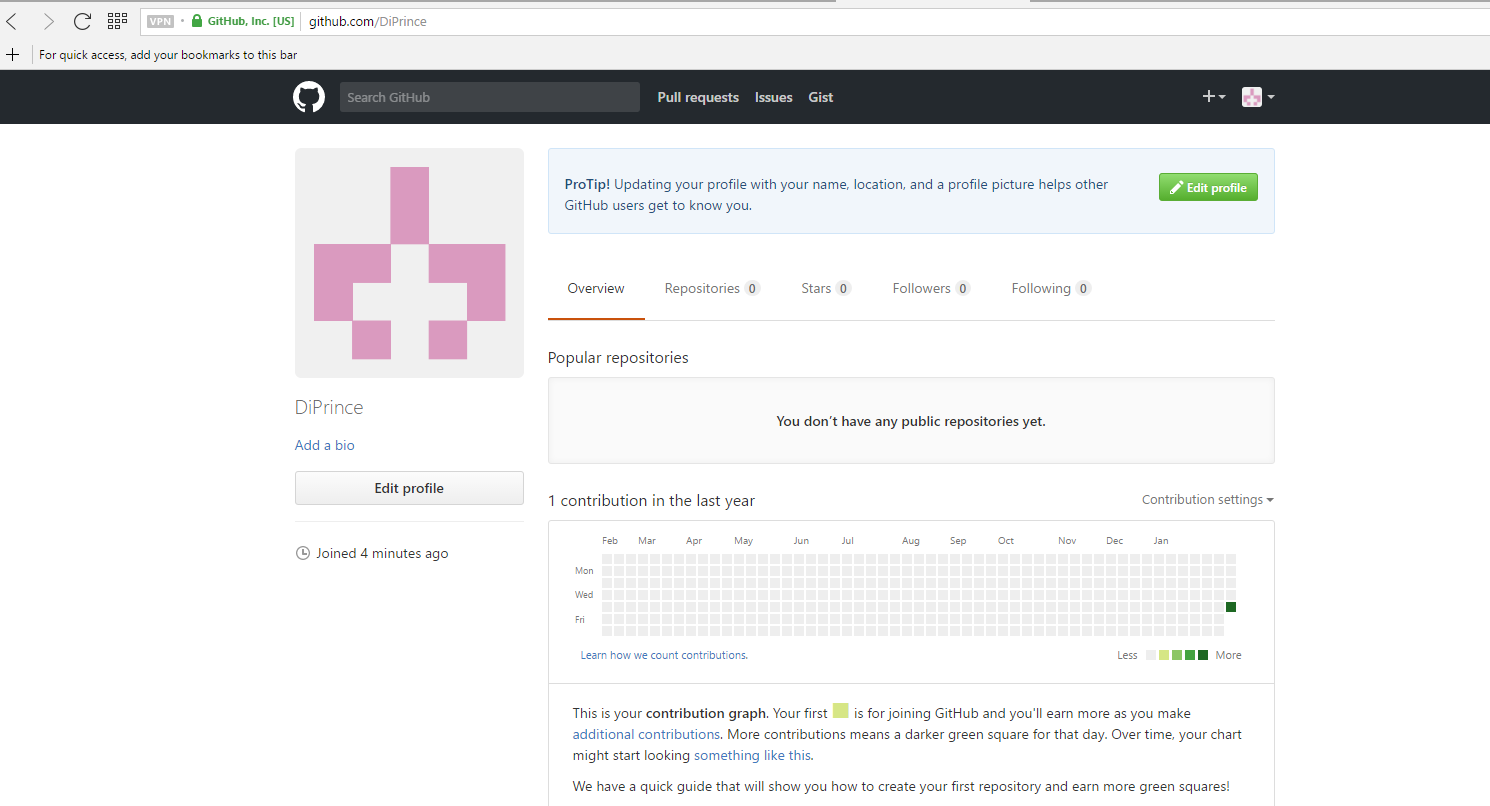
“…different sets of hyper-linked Web pages possibly inter-mixed with legacy applications being deployed in different hardware platforms using different, incompatible technologies to conduct business to business transactions among different companies in different geographical locations.”

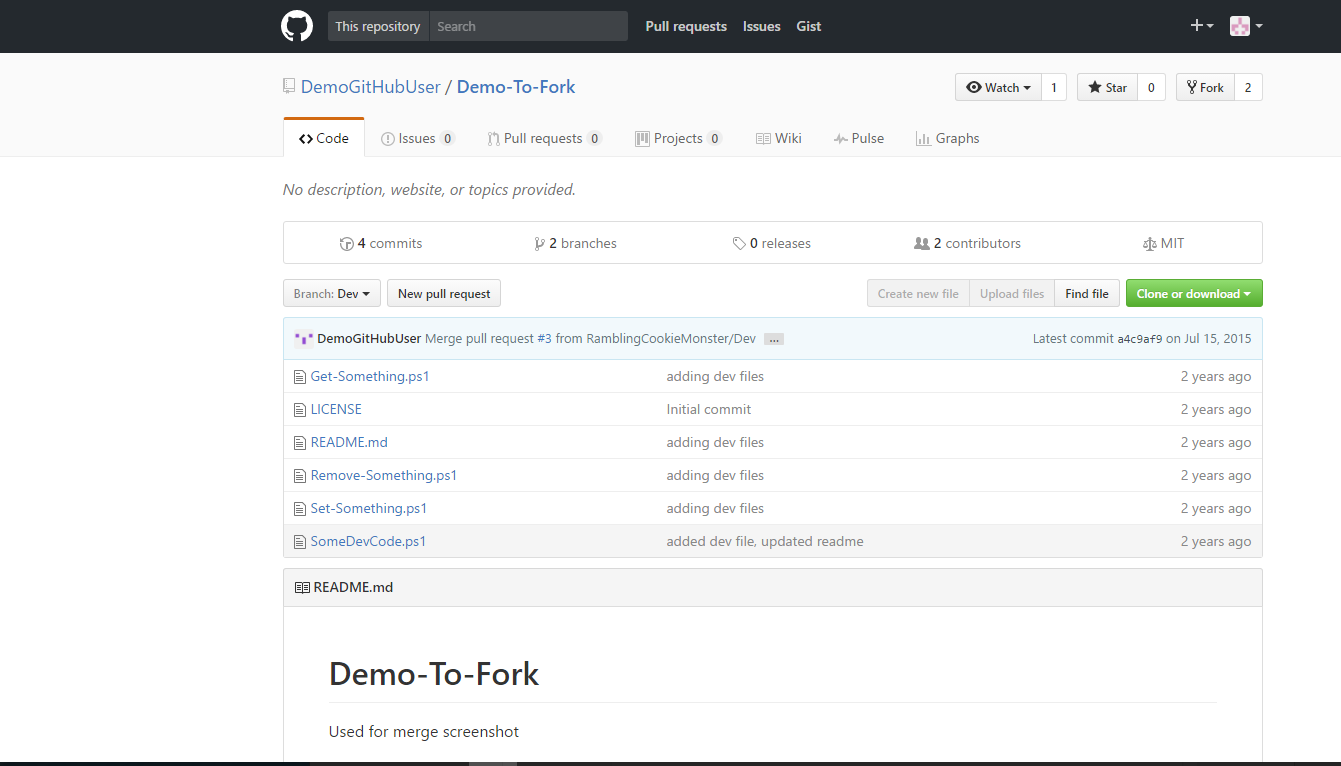
By considering the definition of e-commerce provided by Chan & Kwok (2001) it suggests that many different types of hardware, technologies and locations should be taken into account when looking at e-commerce applications. With today’s web applications this is a necessary part of web development and ensuring information remains secure for both users and developers, which is a limitation for Henderson (2016) as only three goals are considered to ensure information remains secure and standards compliant.

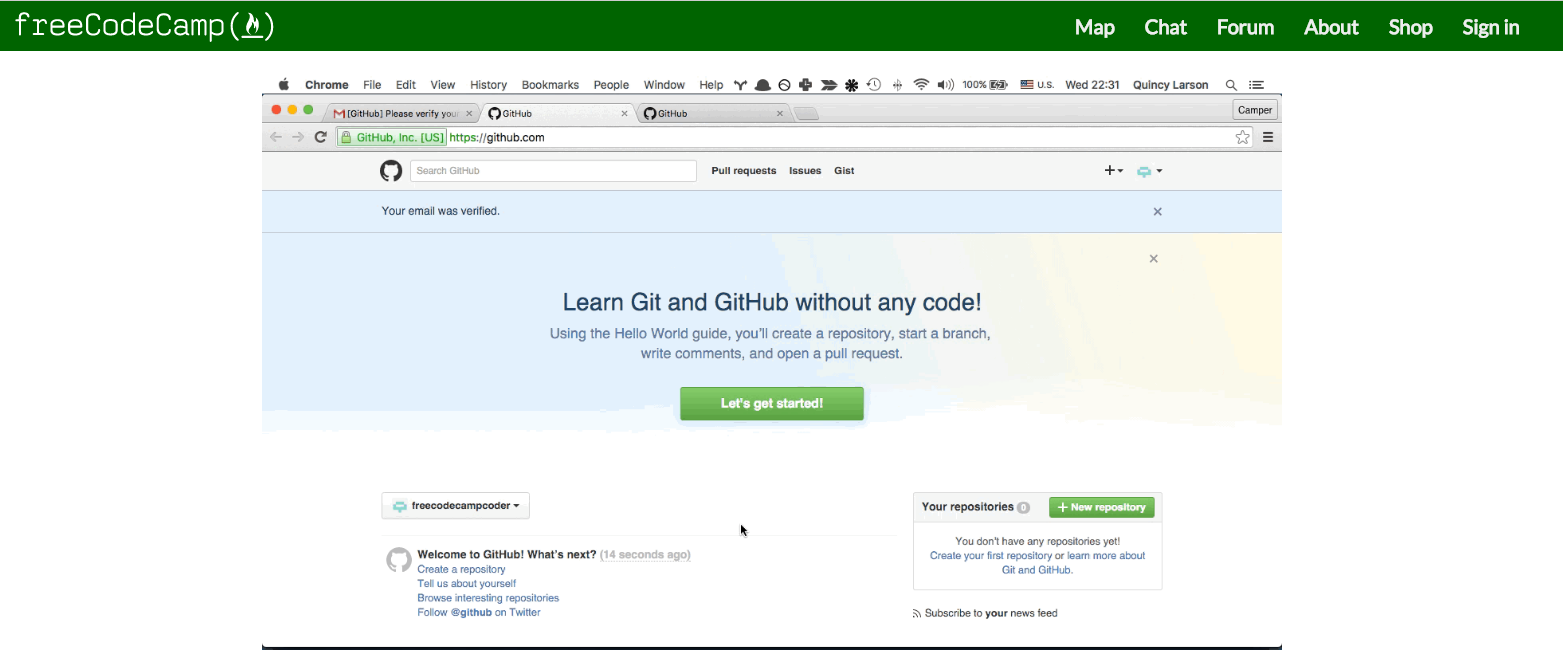
As users and developers are aware and noted by Standards Compliant Coding (2016), if website pages are not standards compliant, some issues may arise that would not help both the user and developer. By using standard compliant codes on website pages, the web pages are easy to load, read, render and upgrade in any browser.

Task Two

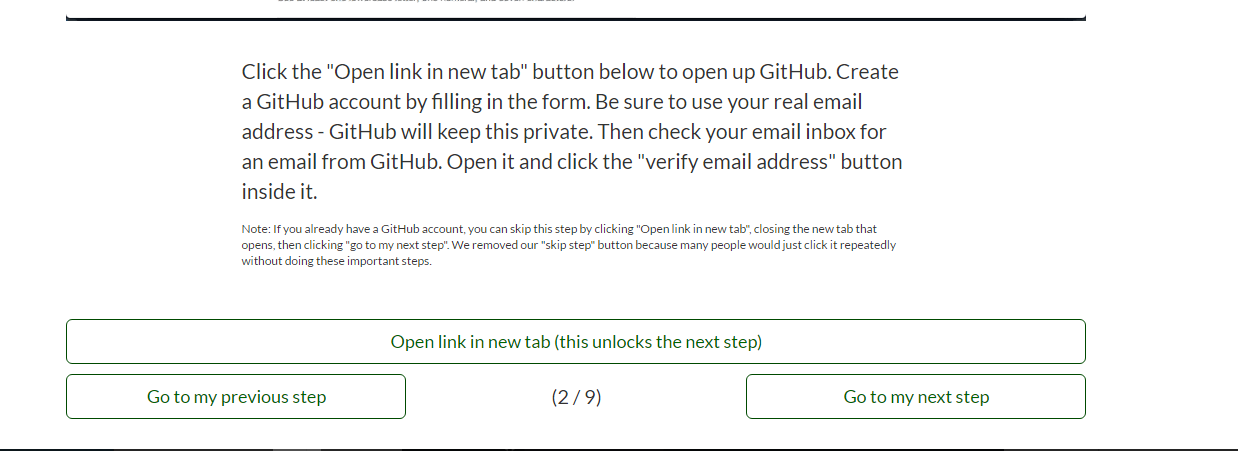




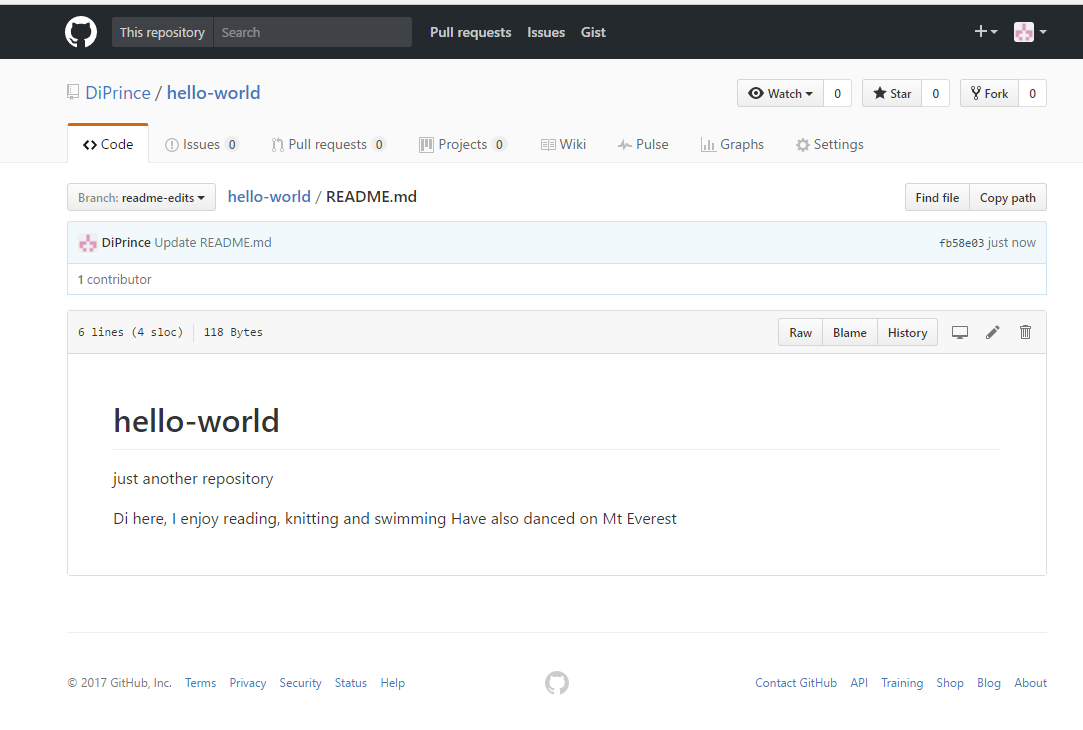




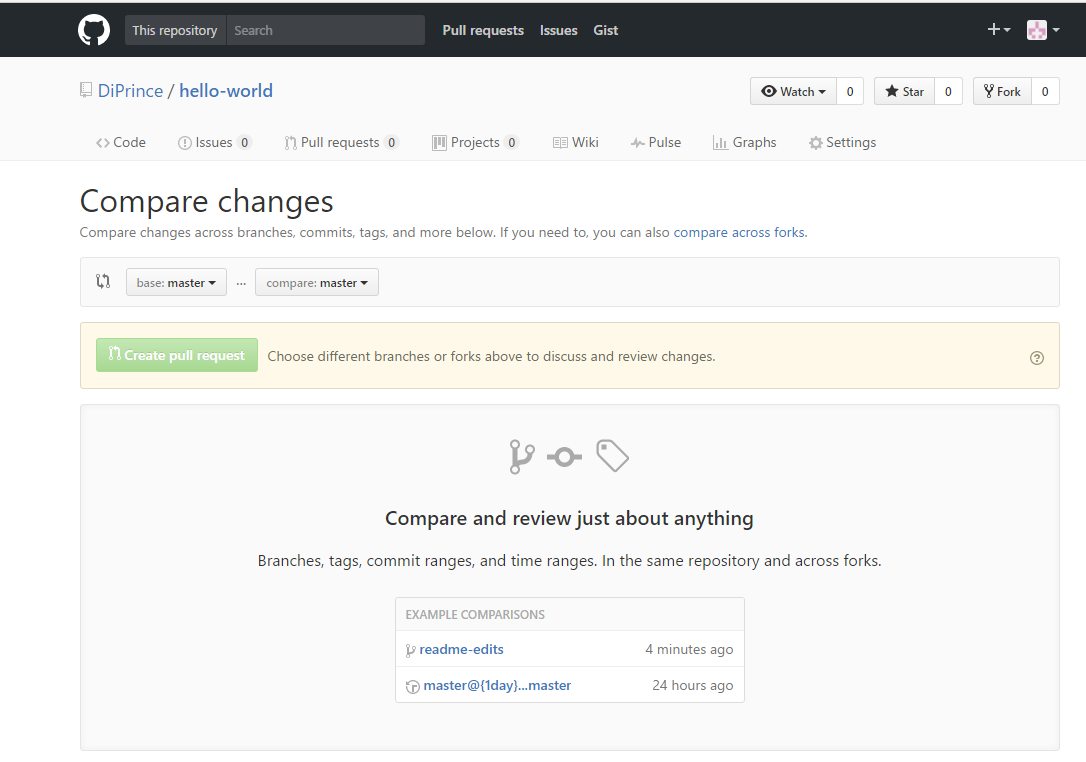
Logging onto to set up Git Hub account.

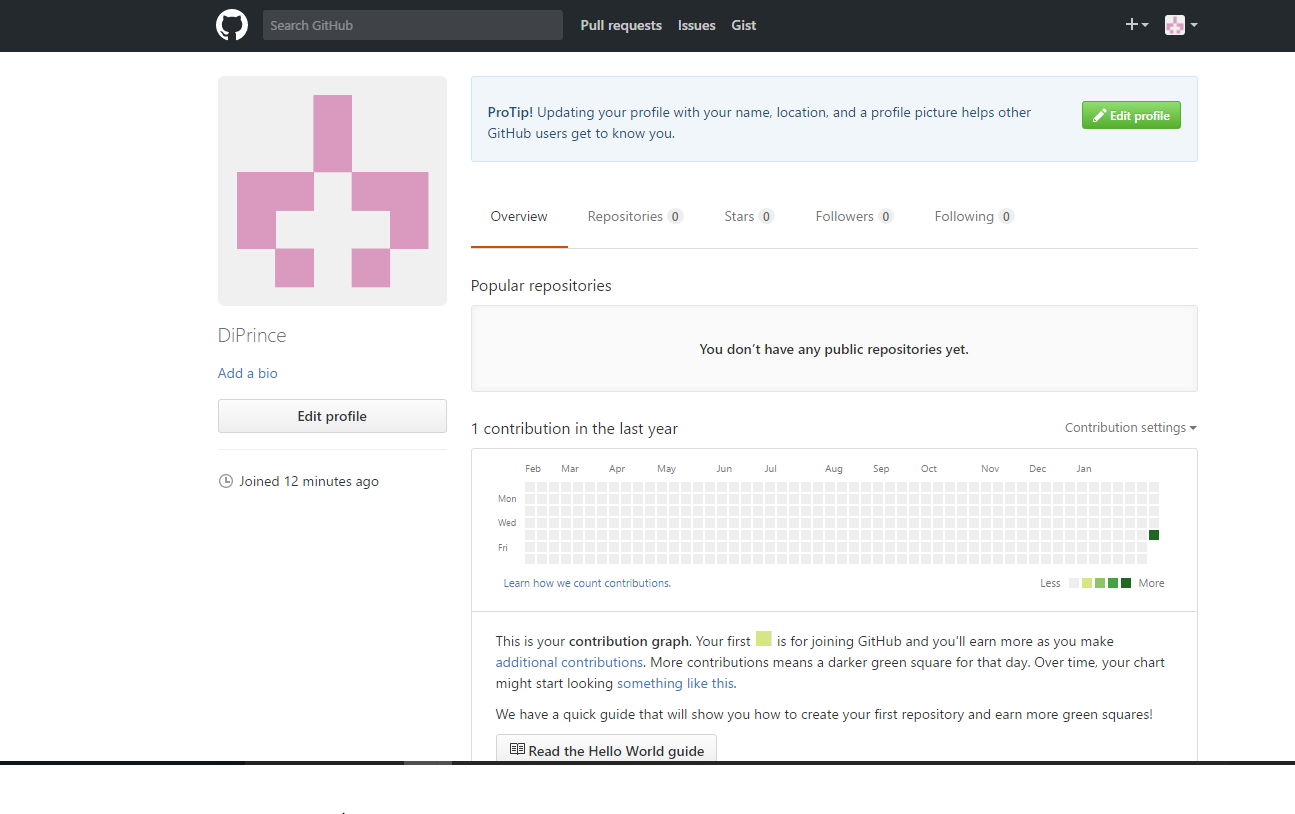


Following the steps to set up the Git Account.

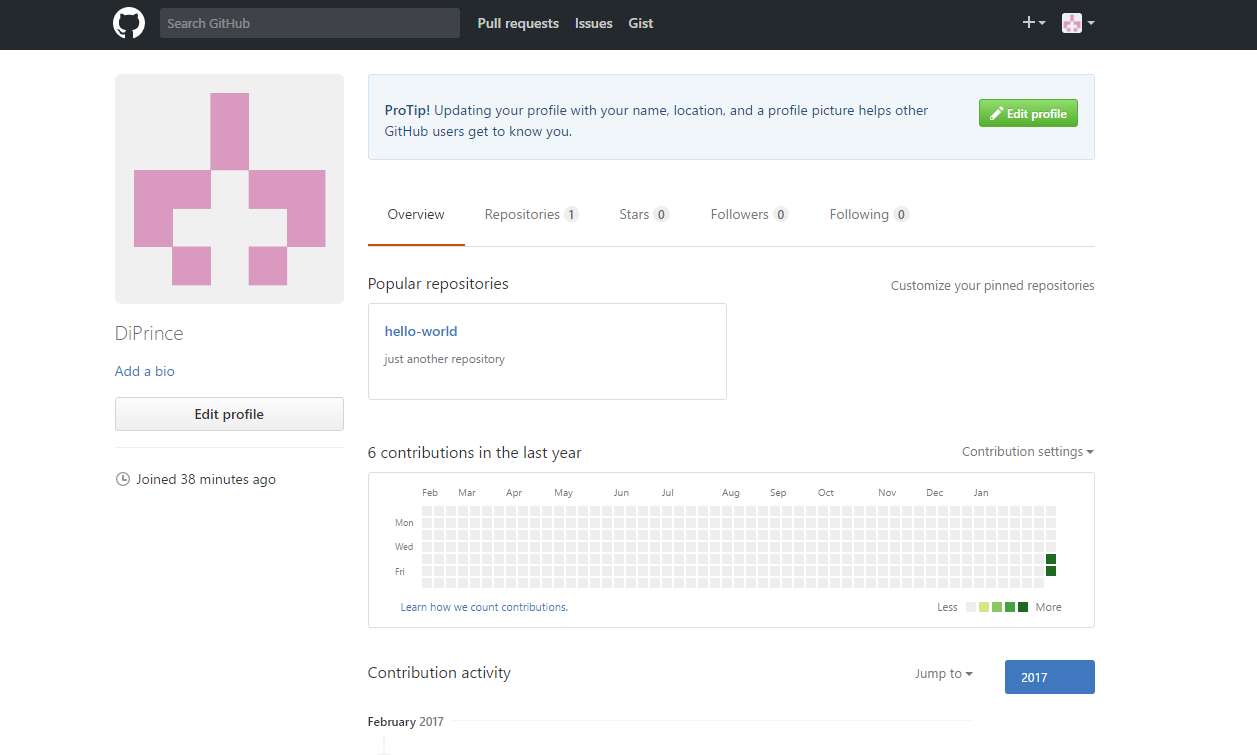


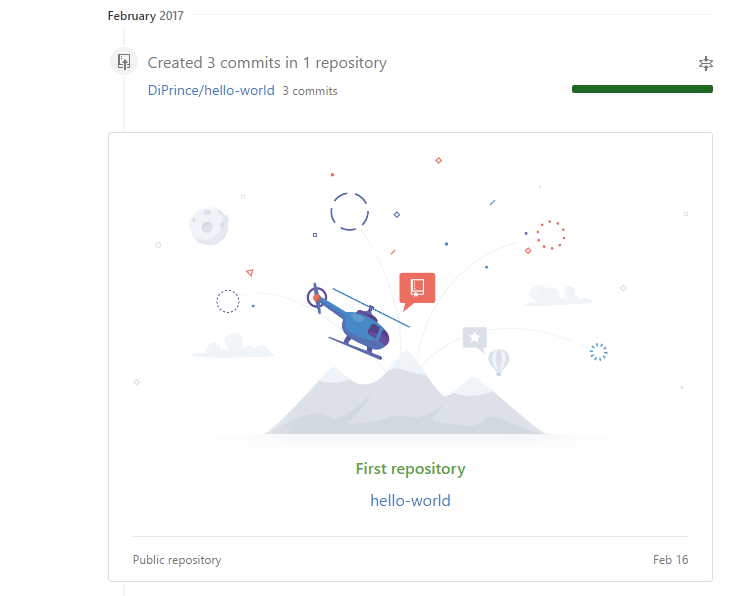
Set-up of Git Hub account under username DiPrince.

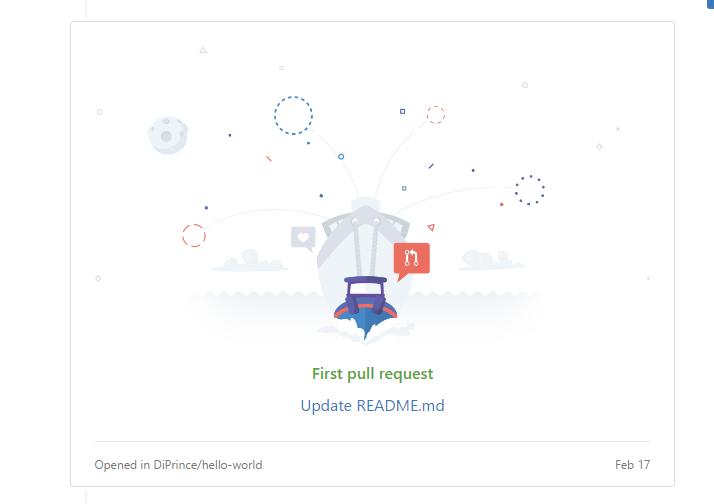


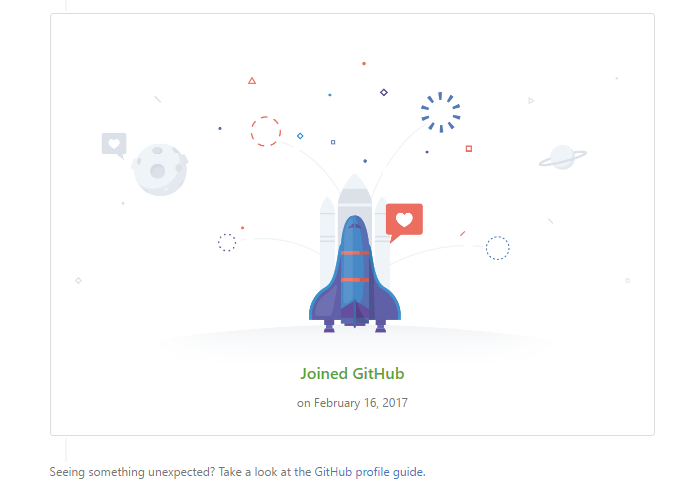


One of the final screenshot of the Git-Hub account before repository created.

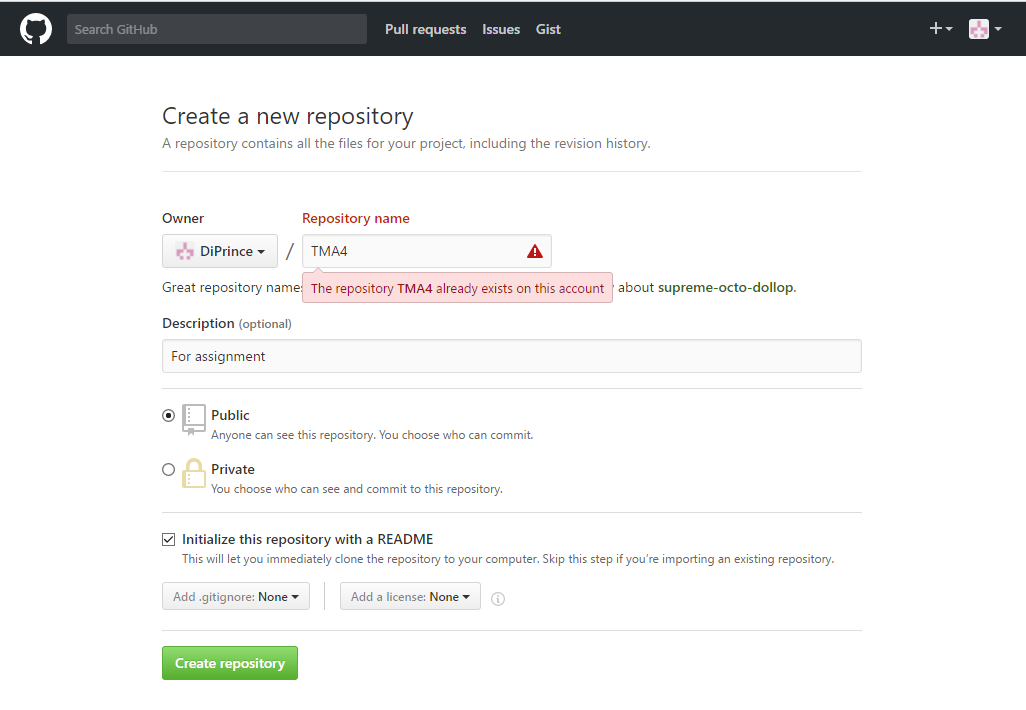


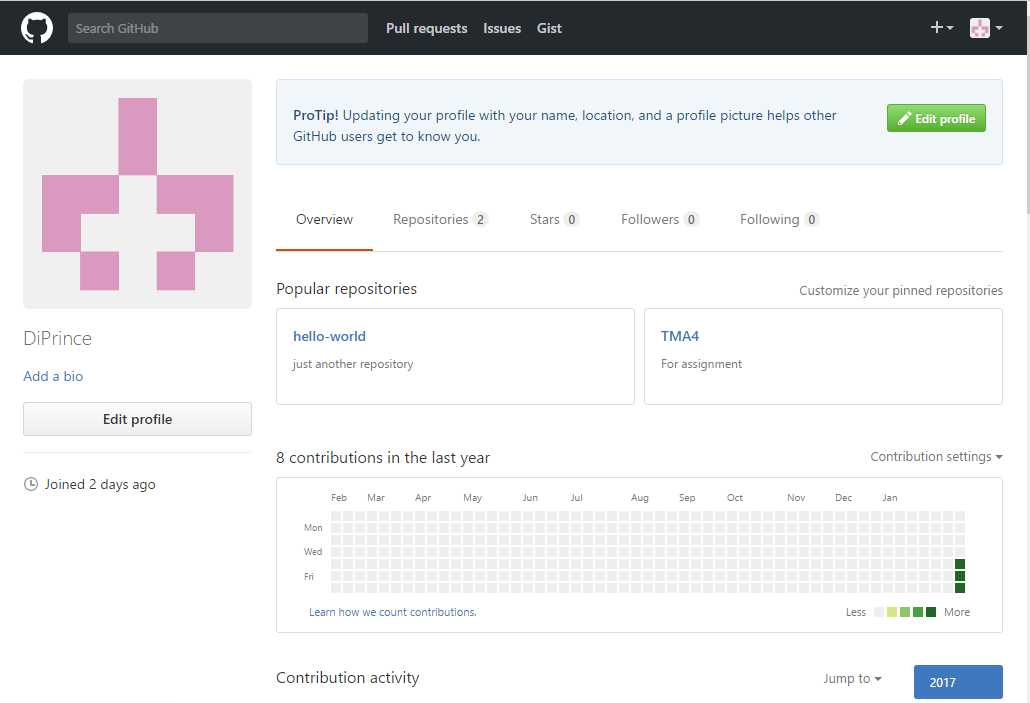


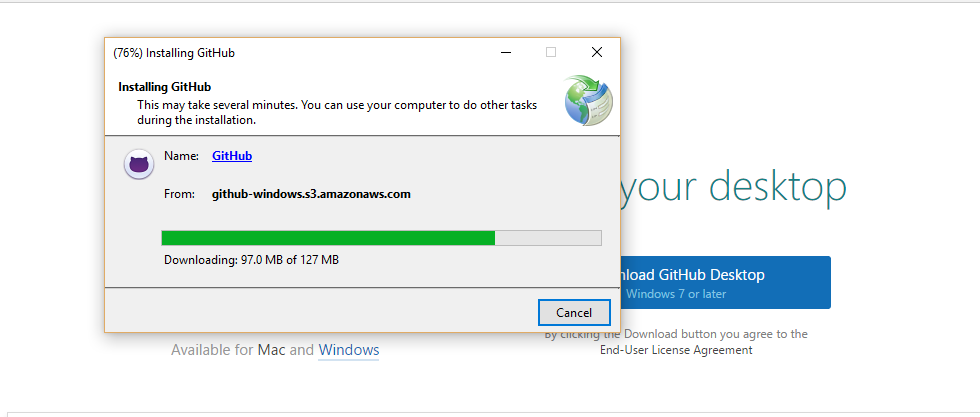


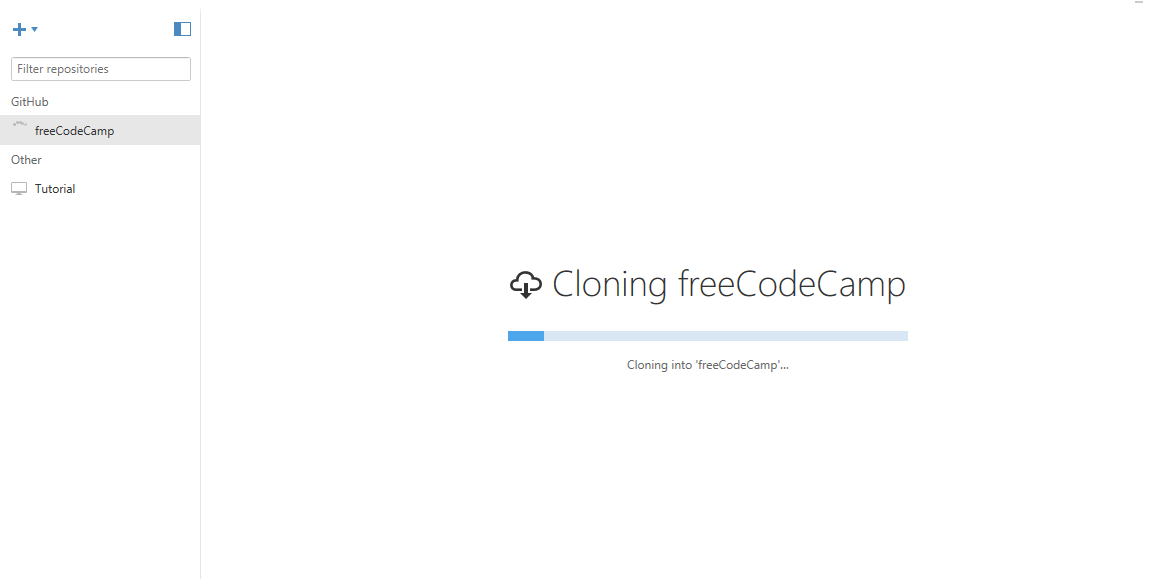


Final screen shots of the GitHub account to confirm joined GitHub, made a pull request and created a repository as noted above.

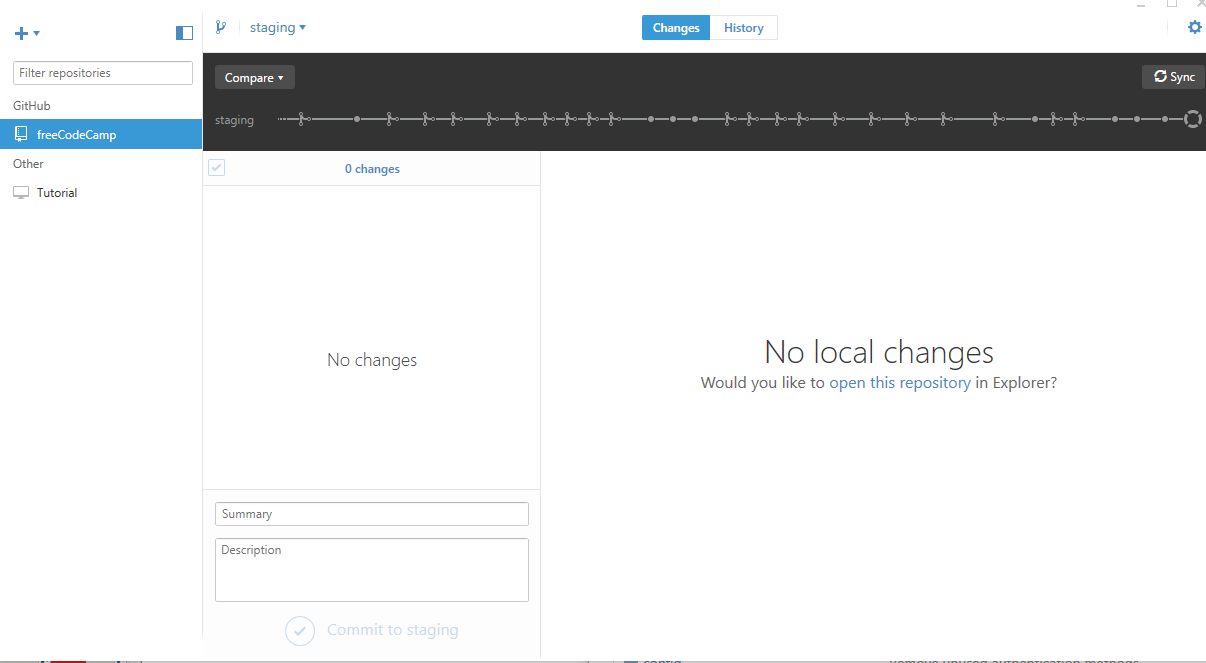








Cloning of freeCodeCamp on Github website.



**Comparison of two platforms – Github and Bitbucket.**

I will consider ten elements presented by Noetic (2016) to make comparisons between the modern web applications of GitHub and BitBucket

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 10 Elements of Web applications (Noetic, 2016) | Github | BitBucket |
| Unique Typography can help display messages | Use of bold lettering, photographs, and different fonts to help with design of the website | Use of bold lettering, different sizes of fonts, and pictures to help the design of the website |
| Ghost Buttons a design element that request user to perform an action | Use of ghost buttons to provide user with more information | Ghost buttons used to provide user with more information |
| Bold Colours can be used to present a colourful side to elements | Use of bright bold colours on website | Use of bright bold colours on website |
| Big Images such as photographs and graphics as a design feature | High resolution photographs and images used on website | High resolution photographs and images used on website |
| Scrolling an element to keep users engaged on remain on a web page | Scrolling used in each section of the website | Scrolling used in each section of the website |
| SVG – Scalale Vector Graphic able to have graphics scale in size without losing quality | Use of SVG image on website example of Globe logo on home page | Use of SVG image on website, example of HipChat logo under Integrations section |
| Card Design as a pattern to display information | Use of card designs on website to help display information for user about products | Use of card designs on website to display information for user about products |
| Full Screen Videos | Use of videos to add to the user experience | Use of videos to add to the user experience |
| Minimalistic Design to make design of webpage look uncluttered and clean | Use of white space, videos, and typography combine to make website appear clean and not cluttered | Use of white space, videos, and typography combine to make website appear clean and not cluttered |
| Flat Icons used as part of web design to give visual impact through use of shapes | Use of icons and shapes to give visual impact on website | Use of icons and shapes to give visual impact on website |

Overall comparison of both platforms has confirmed that modern web applications contain many of the same elements that are necessary to enable dynamic software design.

TASK THREE:

1. To consider the project plan for the case study in TMA1 of the Board Games Aficionados club of Puketapu, a definition provided by Tutorialspoint (2017) states:

“ A project can be characterized as:

* Every project…has a unique and distinct goal
* Project is not routine activity or day-to-day operations
* Project comes with a start time and end time
* Project ends when its goal is achieved…
* Project needs adequate resources in terms of time, manpower, finance, material and knowledge-bank.” (para. 2)

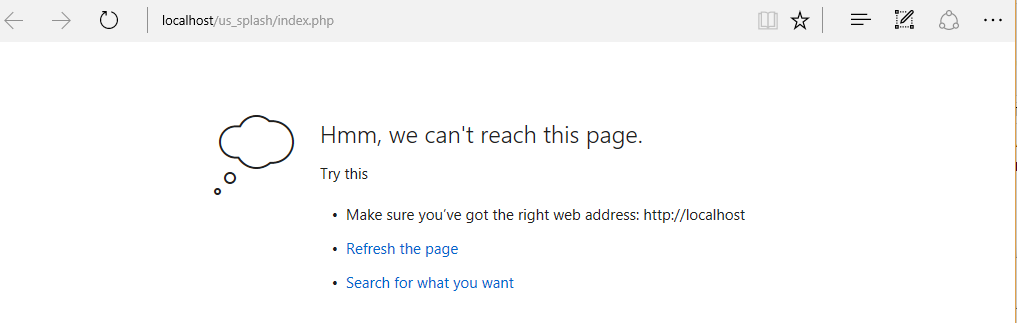
Planning Activity Schedule

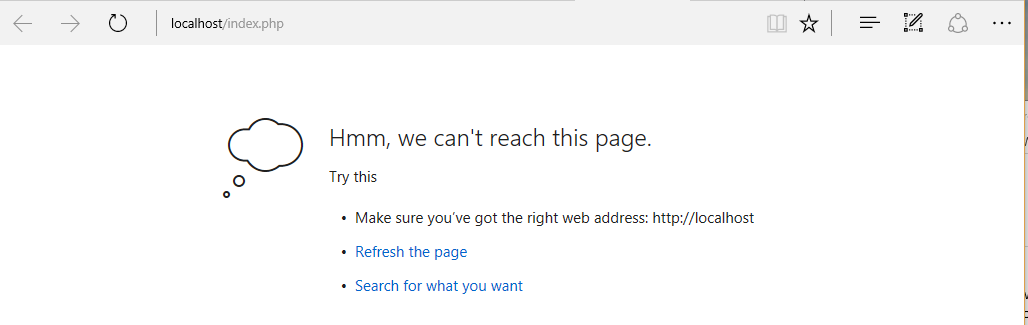
|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Activity | Start date and time | Expected completion date and time | Notes or comments |
| Project Objectives | 31/10/16 @ 9 am | 04/11/16 @ 9 am | Create a web application for the Board Games Aficionados club of Puketapu that is user friendly, cost-effective to run, maintain and upgrade |
| The scope | 07/11/16 @ 9 am | 07/01/17 @ 9 am | The scope of the Board Games Aficionados project includes the planning, design, development, testing of web application. The scope will also include completion of all documents, manuals, and training aids to be used with the web application. The scope of the project will need to be verified |
| Milestone List | 09/01/17 @9 am | 09/03/17 @ 9 am | A list of the major milestones for the project will be required. This will include providing accurate estimates such as software size, effort estimates in terms of personnel and man-hours, time estimation to look at the time needed to produce the software, cost estimation to consider all the factors noted above. |
| Project Schedule + Outputs | 31/10/16 | 31/07/17 | Need to break down project tasks into smaller manageable ones with estimate time frames attached to each task. Have required number of work units for each task and estimate the total time required for the project from start to finish |
| The resources | 31/10/16 @ 9 am | 31/07/17 @ 9am | Ensure that correct amount of resources are allocated to the project. The resources may include human personnel, tools and software packages. |
| The team | 07/11/16 | 31/07/17 | Deciding what members should be on a project and giving team members certain responsibilities when they are needed and when they are not needed |
| Risk Management | 07/11/16 | 31/07/17 | This is discussed in the risk assessment below |
| Project Monitoring | 31/10/16 | 31/07/17 | Monitoring checks to be put in place to ensure tasks are completed. Reports provided to check on the status of activities and task are done on time. Milestone checks to make sure that the major milestones are completed as per each stage of the project plan |
| Project Communication | 31/10/16 | 31/07/17 | Communication can be provided on an oral or written basis. This is important as it ensures that both user, project team members and organization are aware of each stage of the project |
| Change Management | 07/11/16 | 31/07/17 | Changes to any part of the project plan must be considered and any changes may require approval of a person with authority to do so. |

Risk Assessment Schedule

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| Risk Event | Impact | Mitigation Steps | Severity (1 – 5) |
| Scope | If scope of the project is not defined correctly then the project may not fulfil the goal of the project | Ensure that all stakeholders, users, team members and organisation are able to provide views on the scope of the project | 1 – Low impact  5 – High impact  This can have a high impact on the rest of the project if the scope is not clearly defined |
| Time | With all projects there is a start and finish time frame. | Ensure that the timeframes are realistic and take into account the varied steps of the project plan | 1 – Low impact  5 – High impact  This can have a high impact should a project run out of time before it is completed then other costs may arise such as financial, and human resources costs |
| Cost | Estimating costs from the outset of a project will ensure that resources are allocated correctly to the tasks that required to be completed. | Estimating as much as possible the costs for a project to ensure that the project runs efficiently, effectively and on budget | 1 – Low impact  5 – High impact  Cost will have a high impact on the project due to time, resources and budget constraints. No project likes to run over time or over budget. |
| Quality | Ensuring that the project provides a quality product that meets the needs of the client, organisations and team members of a project | Make sure that each project step is monitored and reviewed. | 1 – Low impact  5 – High impact  This can have a high impact. As with all projects, the end product should be of a high standard. If an inferior product is completed, then this poor quality will reflect badly on everyone involved in the project. |

Error message on Apache server and MySQL server still showing after several attempts to ensure UniServerZ is working. I have followed all the instructions noted. But have still not been able to get the uniform server to work as noted by the error messages below.





Final upload to Github repository not completed as files not able to completed on uniform server.

REFERENCES

Chan, M.T., & Kwok, L.F., (2001). Integrating security design into the software development process for e-commerce systems. *Information Management & Computer Security*, 9(3). 112 – 122. Retrieved from

<http://www.emeraldinsight.com.libraryproxy.openpolytechnic.ac.nz/doi/pdfplus/10.1108/09685220110394758>

Henderson, A. (2016). *The CIA Triad: Confidentiality, Integrity, Availability* Retrieved from

<http://panmore.com/the-cia-triad-confidentiality-integrity-availability>

Kesh, S., Ramanujan, S., & Nerur, S. (2002). A framework for analyzing e-commerce security. *Information Management & Computer Security*, 10(4), 149 – 158. Retrieved from

<http://www.emeraldinsight.com.libraryproxy.openpolytechnic.ac.nz/doi/pdfplus/10.1108/09685220210436930>

Meucci, M. & Muller, A. (2014). OWASP – Open Web Application Security Project. *Testing Guide 4.0 release*. Retrieved from <https://www.owasp.org/images/1/19/OTGv4.pdf>

Noetic, S. (2016, May 29). 16 Essential Modern Web Design Elements for Apps and Websites. [Web log post]. Retrieved from <http://noeticforce.com/modern-web-design-elements-apps-and-websites>

Standards Compliant Coding Web Page Mistakes. Retrieved from <http://www.webpagemistakes.ca/standards-compliant/>

Tutorialspoint. (2017). Software Project Management. Retrieved from

<https://www.tutorialspoint.com/software_engineering/software_project_management.htm>

W3C. (2009). CSS Validation Service.

Retrieved from <https://jigsaw.w3.org/css-validator/#validate_by_upload>

W3C. (2013). Markup Validation Service. Retrieved from <https://validator.w3.org>