TM4 - Web technologies

Contents

[Task 1A 3](#_Toc453871103)

[Task 1b1 4](#_Toc453871104)

[Task 1b2 5](#_Toc453871105)

[Task 2A 6](#_Toc453871106)

[Task2b 8](#_Toc453871107)

[Task 2c 11](#_Toc453871108)

[Task 3a 12](#_Toc453871109)

[Task 3b 13](#_Toc453871110)

Task 1A  
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?   
Comment on the security and the pass/fail state of the web application.

Discuss at least three examples from the web application relating to security and/or issues identified by the OWASP to support your answer.

*After reading through the OWASP guide the application developed for TM1 and TM2 do not meet the requirements and would not be considered secure, they would not pass any of the tests. Therefore the application itself is in a fail state.*

*The applications do not meet most of the requirements according to the OWASP guide however I have chosen the next 3 items to explain in detail.*

* Encrypt authentication data in storage and transit to mitigate risk of information disclosure and authentication protocol attacks. (Muller, 2015)

*Data that is collected in the forms that we have developed is saved directly to the PHP form and can be viewed by accessing the page, the pages do not ask for login details or a password and are able to be viewed by anyone.*

* Error and Exception Handling

*The forms that were developed did involve error and exception handling however from a security standpoint the information was presented in a non-secure manner any person accessing the forms could see the coding involved by clicking on the source file – there was no encryption of code.*

* User and Session Management

*The web application was not designed in a way that allows users to create a username and password therefore there is no user management that is able to take place this includes information such saved passwords, roles, security options etc. Session management cannot take place due to users not being required to be logged in.*

# Task 1b1

Use your favourite web browser and browse to http://panmore.com/the-ciatriad-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.

* *When looking at the CIA Triad it is important to follow all three of the key areas when developing an e-commerce website, Confidentiality, integrity and availability are the concepts most basic to information security. These concepts in the CIA triad must always be part of the core objectives of information security efforts.*
  + *Confidentiality*
    - *Customers come to your e-commerce website to browse your wares and hopefully purchase whatever it is that you are selling. When you go to buy something online you are asked to enter personal information such as your name, date of birth, address, phone number and other personal information. A customer trusts you with this information and therefore you should keep the information confidential*
  + *Integrity*
    - *Integrity is an important aspect of an e-commerce website because you are trusting that the information that you present to the outside world is correct. Almost all data is still entered manually and is prone to human error or careless access and use. As part of the integrity you need to ensure that the errors in the information system remains unchanged during the storage, transmission and usage of the information when provided. When the customers give you their personal information they are also hoping that you protect this data and don’t use it for other purposes. Integrity relates to information security because accurate and consistent information is a result of proper protection. The CIA triad requires information security measures to monitor and control authorized access, use, and transmission of information.*
  + *Availability*
    - *The main concern in the CIA triad is that the information should be available when authorized users need to access it. Availability is maintained when all components of the information system are working properly. In regards to an e-commerce website it is important that the information be available especially if you are offering limited time services, you need to know how many customers you have, what they purchased, when they purchased it by having this information available to you, you would be able to forecast potential sales and amounts.*

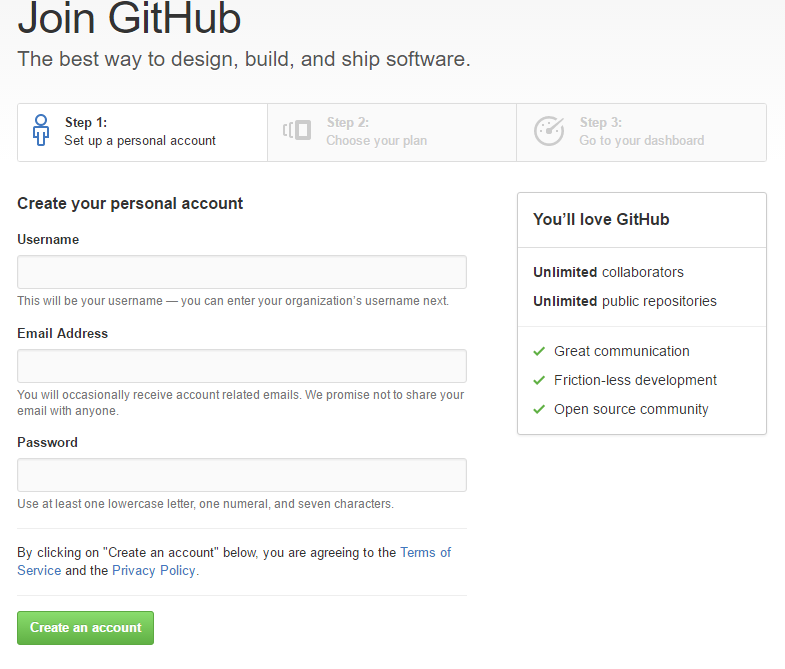
# Task 1b2

What would you consider to be a limitation with this model in terms of today’s web applications?

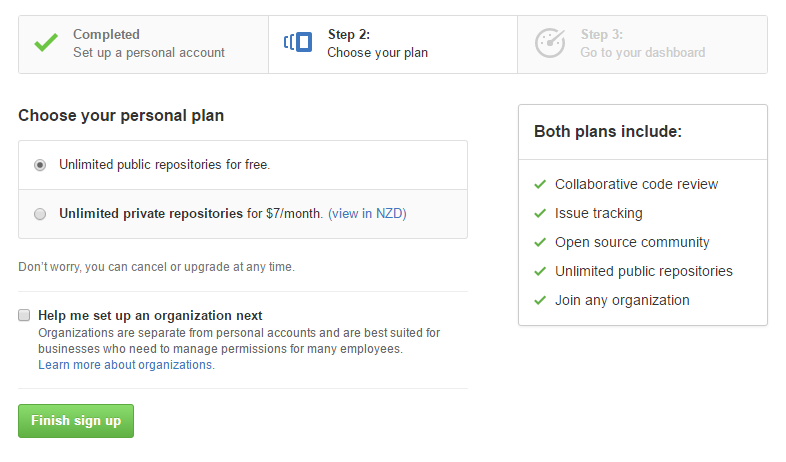
*The CIA triad has the goals of confidentiality, integrity and availability, which are basic factors in information security. Information security protects valuable information from unauthorized access, modification and distribution. While this model and its key fundamental points still apply to today’s web applications they are not necessarily followed and as the web keeps growing and more people come online and develop web applications it is getting harder to enforce these points. Web applications can be developed by anyone with enough experience in coding and they don’t necessarily understand these key concepts. I personally have developed a few web applications including two websites which were linked to Amazon as resellers and I didn’t personally know about the CIA Triad until I came to undertake this course of study.*

# Task 2A

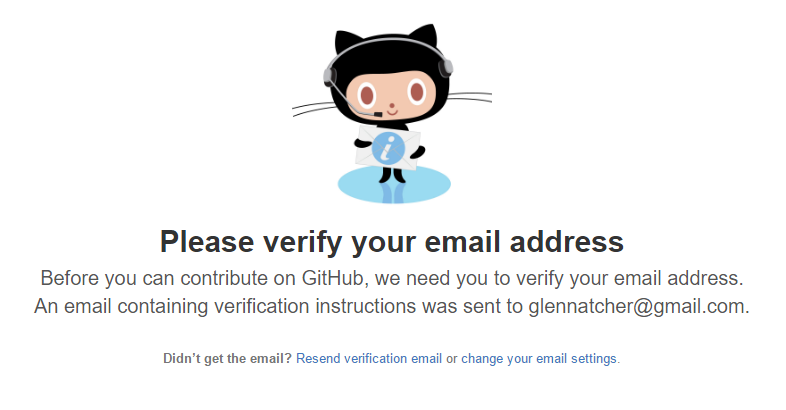
Creating a GitHub account.



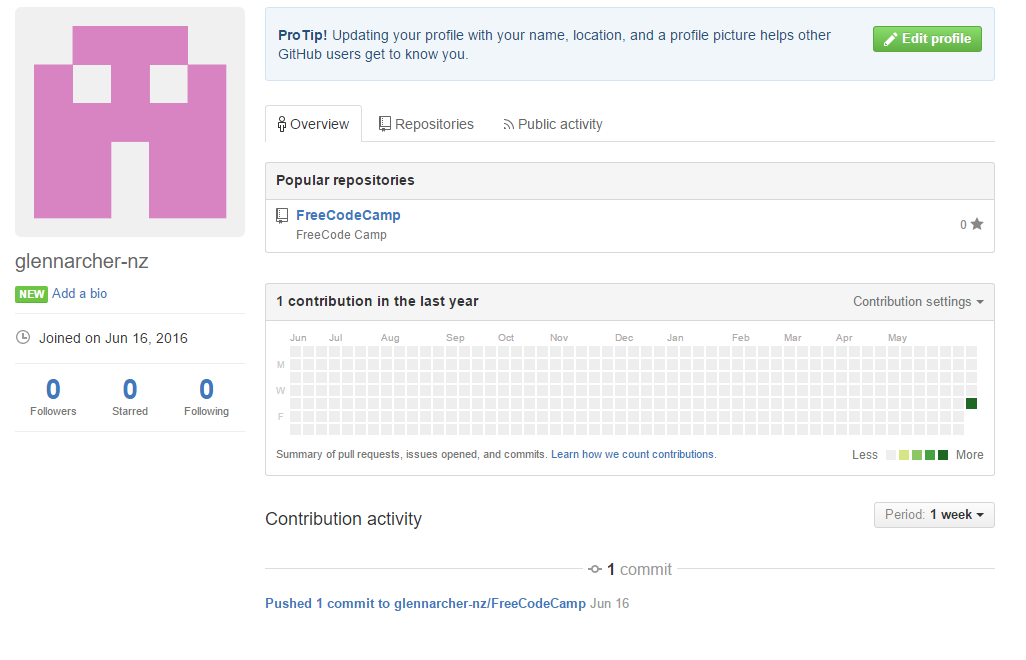
Choosing GitHub Plan



Verifying email address.

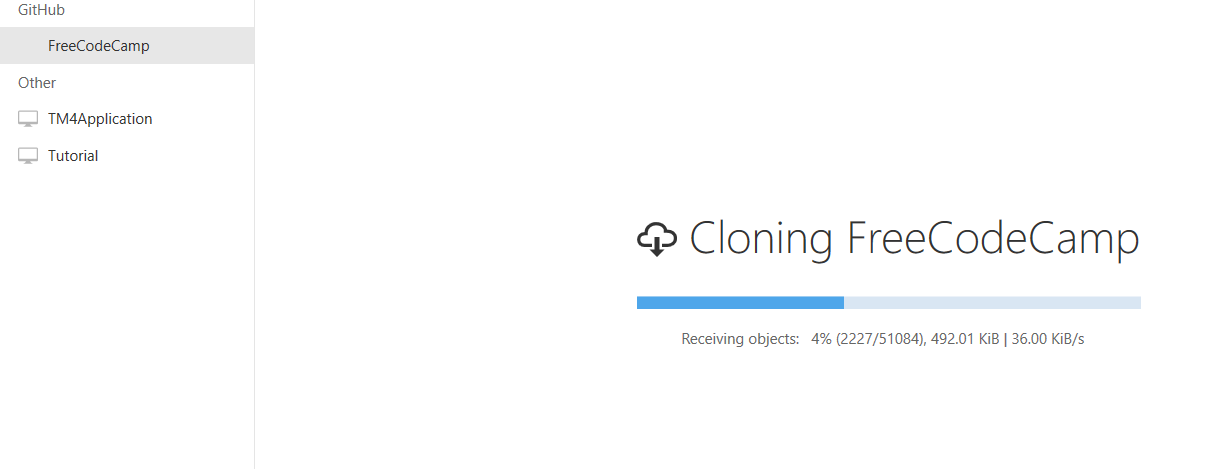


My GitHub account created.

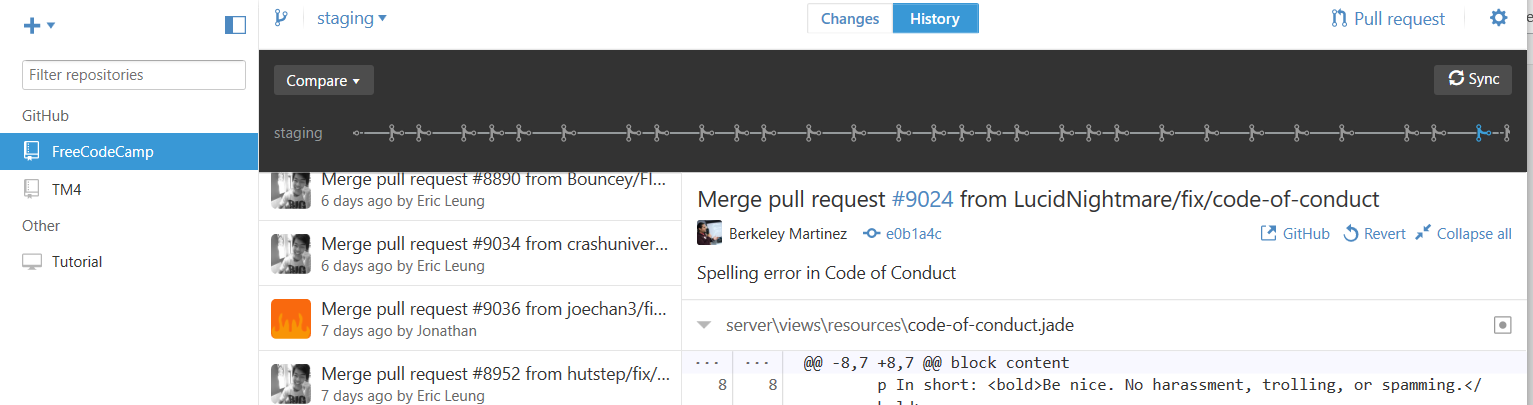


# Task2b

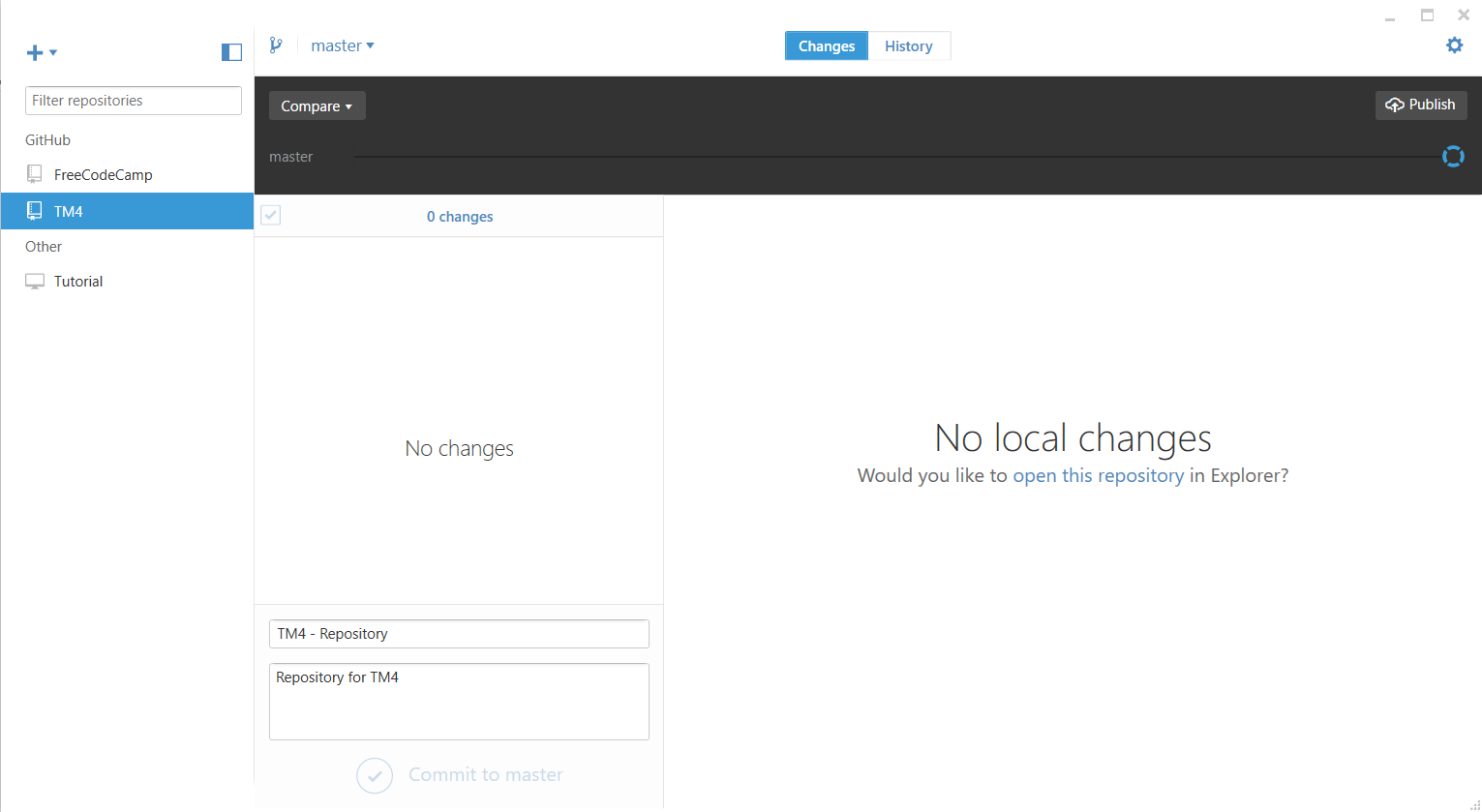
Cloning Free Code Camp



FreeCode camp cloned and opened in GitHub desktop



New Repository created for TM4



# Task 2c

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Feature** | **GitHub** | **BitBucket** | **Comments** |
| 1. Pull Requests |  |  | Both Github and BitBucket allow you to pull information from their online repositories |
| 1. Branch Permissions |  |  | While GitHub allows you to set permissions, BitBucket takes this one step further and you can set permissions or branches of a project |
| 1. Collaboration |  |  | Both Github and BitBucket allow you to collaborate on a project with other employees |
| 1. Diff Views |  |  | BitBucket allows for Diff views, however GitHub has built it into their collaborative code. |
| 1. Jira Integration |  |  | Both Github and BitBucket support Jira integration through the use of an API |
| 1. 3rd Party Integrations |  |  | Both Github and BitBucket support additional 3rd Party API integrations to allow you to code better |
| 1. Programming Languages |  |  | GitHub supports more programming languages then BitBucket |
| 1. Desktop Client |  |  | Both Github and BitBucket have desktop clients that allow you to connect to repositories however Githubs client is more user friendly |
| 1. Pricing |  |  | Both support free Public repositories however if you want to go private there is a cost involved – Bit Bucket is cheaper for more users then GitHub |
| 1. Issue Tracking |  |  | Both Support Issue tracking and problems with Code – BitBucket lays this out better then github however. |
| 1. Wiki |  |  | GitHub has a better Wiki for support and layout and this allows better end user support. |

In conclusion both of the tools have features that are unique to themselves however it would come down to what I was trying to achieve, if this was going to require a private repository then I would most likely choose to use Bit Bucket due to the pricing for a group of users.

# Task 3a

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Activity | | Start date | Start Time | Expected completion date | End time | Notes or comments |
| Design Database tables – | * Board Games | 11th June | 7.30pm | 11th June | 10.30pm | This was completed on time and with no issues. |
| * Board Games > Players Table | 11th June | 7.30pm | 11th June | 10.30pm |
| * Schedule of Games | 11th June | 7.30pm | 11th June | 10.30pm |
| * Scoring (High Score Table) | 11th June | 7.30pm | 11th June | 10.30pm |
| Create SQL Databases for Additional Tables | * Board Games | 12th June | 10.00am | 12th June | 10.30pm | Tasks were completed and tables were created on time |
| * Board Games > Players Table | 12th June | 10.00am | 12th June | 10.30pm |
| * Schedule of Games | 12th June | 10.00am | 12th June | 10.30pm |
| * Scoring (High Score Table) | 12th June | 10.00am | 12th June | 10.30pm |
| Create CRUD forms for additional tables | * Board Games | 13th June | 7.30pm | 13th June | 10.30pm | I ran out of time to complete all the CRUD tables and only managed to complete the first one. This task should have been priortised. |
| * Board Games > Players Table | 13th June | 7.30pm | 13th June | 10.30pm |
| * Schedule of Games | 14th June | 7.30pm | 14th June | 10.30pm |
| * Scoring (High Score Table) | 14th June | 7.30pm | 14th June | 10.30pm |
| Create Web Form | * Board Games | 15th June | 7.30pm | 15th June | 10.30pm | I got stuck creating this – Did not understand properly how to link a foreign key to a table |
| * Board Games > Players Table | 15th June | 7.30pm | 15th June | 10.30pm |
| * Schedule of Games | 15th June | 7.30pm | 15th June | 10.30pm |
| * Scoring (High Score Table) | 15th June | 7.30pm | 15th June | 10.30pm |

|  |  |  |  |
| --- | --- | --- | --- |
| Risk event | Impact | Mitigation steps | Severity (1-5) |
| 1. Has the project sufficient priority within the organisation? | High | Set Priority of tasks and ensure that they are meet. | 1 |
| 1. Are all the technical requirements understood? | Medium | Revise material, make sure the steps of the problem are clear or clarify with the customer | 2 |
| 1. Does the team have experience of the development tools to be employed for the project? | High | The team has slight exposure to what is being asked but this should be less of a problem. | 4 |
| 1. Have requirements been prioritised? | Medium | Organize tasks so that they are priortised, get confirmation that it is working | 3 |
| 1. How likely are the requirements to change once the project has started? | Low | This is unlikely to happen as we are attempting to meet the requirements of the assessment | 5 |

# Task 3b

|  |  |  |
| --- | --- | --- |
| CREATE TABLE players  (  MembershipID INT(11) NOT NULL,  Firstname varchar(255) NOT NULL,  Familyname varchar(255) NOT NULL,  EmailAddress varchar(255),  Phone varchar(255)  ); | CREATE TABLE BoardGames  (  BoardGameID INT(11) NOT NULL AUTO\_INCREMENT=1  BoardGamename varchar(255) NOT NULL,  BoardGamePlayers INT(1) NOT NULL,  ); | CREATE TABLE BoardGamesAssigned  (  BoardGamesAssignedID INT(11) NOT NULL AUTO\_INCREMENT=1  BoardGamename varchar(255) NOT NULL,  FOREIGN KEY (M\_Id) REFERENCES Players(MembershipId)  FOREIGN KEY (BG\_Id) REFERENCES BoardGames(BoardGameID)  ); |
| CREATE TABLE BoardGamesSchedule  (  BoardGamesScheduleID INT(11) NOT NULL AUTO\_INCREMENT=1  Tournamentname varchar(255) NOT NULL,  Tournamenttime varchar(255) NOT NULL,  Tournamentvenue varchar(255) NOT NULL,  ); | CREATE TABLE BoardGamesScoring  (  HighScoreID INT(11) NOT NULL AUTO\_INCREMENT=1  FOREIGN KEY (Game\_Id) REFERENCES BOARDGAMES(BoardGamename)  FOREIGN KEY (Player\_Name) REFERENCES Players(FirstName)  ); |  |