BIT695 TMA4

**Task one**

**a.**

A review of the case study using the OWASP steps of Manual inspection of people and practices, threat modelling, and source code review, Penetration testing was not carried out.

Manual inspection of the people and practices of the organisation, use of architecture.

* Practices of Board Game Aficionados, the core use of the web site is for information serving to the public about the club and locations where club events take place, secondary to this is the Club Secretary maintains a spreadsheet that details game results, records times and an event calendar which is shared via a cloud storage system.

Threat Modelling, vulnerabilities technical, operational, or management

* Threat modelling of the application mainly falls to into two distinct areas, the technical application itself in regards to making sure the web application input form is secure from injection attacks and also has appropriate client side validation to help with server load processing. The second area of potential threat is the cloud shared information that the club uses, without detailed knowledge about how read and write permissions are being handled from an administration sharing point of view. Lack of details in the case study about just the mechanism involved in the sharing process. An area to look into is the manner of access to the data is there a single sign on that all club member know the password too, or is it accessed via individual accounts?

Source code review

* The review of the source code is and most importantly looking at the web application form page.
* Of note the form is submitted to an external add\_player.php for processing this is done by way of a \_POST method which is good as this allows data hiding, by contrast if the method was a \_GET this would not be ideal as the data would not be hidden and easily seen within the URL bar of the browser.
* The use of the client side validation of all form fields was accomplished with the use of regular expressions on allowed characters for each field, first name, last name, e mail and phone. This fits with the testing of the OWASP about injection attacks as the characters required to perform the attack are not permitted in the regular expression.

Overall the structure of the case study web application passes the form client side validation to help prevent injection attacks, while no information is available about the server side processing. More of a concern is the availability and integrity of the cloud based information as not enough is known from the case study about the read/write permissions and backing up of data by the club secretary.

**Task One**

**b.**

Availability is of primary concern for an e commerce site, An e-commerce site primary goal is to sell products and services to their customer base, without information being available to the company’s customers the business will suffer from poor sales, limited business growth to the point where the company has to shut their figurative online “doors”.

Availability in terms of the e-commerce site is about having

* Hardware being up to date and well maintained
* Providing enough network bandwidth to reduce bottlenecks, to help with this consider redundancy, clustered servers.
* Disaster recovery in worst case scenario, how long to get the site up again,
* Firewalls and proxies to help safe guard against intrusions and denial-of-service attacks
* Having the products available for viewing and up to date with stock levels

Availability for an e-commerce site could be defined by bundled together the above to come the statement of making sure that through proper maintenance of the web application and network hardware that the applicatio0n has minimal downtime in order to have the best serve the companies customers. This is a balancing act as there less downtime you require then the more complex and expensive the hardware systems needs to be in order to serve this requirement. This will have to be balanced on the costs of the services vs the sales revenue.

The limitations of the CIA triad with modern web applications is that there is a continual drive for more information, both in the visible data that users actively provide to the applications, but also in latent user metrics about your usage. This activity data includes cookies to help keep track of your activity, heat maps on your “mouse over” areas to build a picture of user interaction with the websites in order to target marketing and products in those areas of the screen. WhatIs.com explains this increased amount of data that needs to be safe guarded places strain on this, due to duplication of data set, disaster recovery plans, and various formats of the data being captured can multiply already high costs. (Matthew Haugh, 2014)

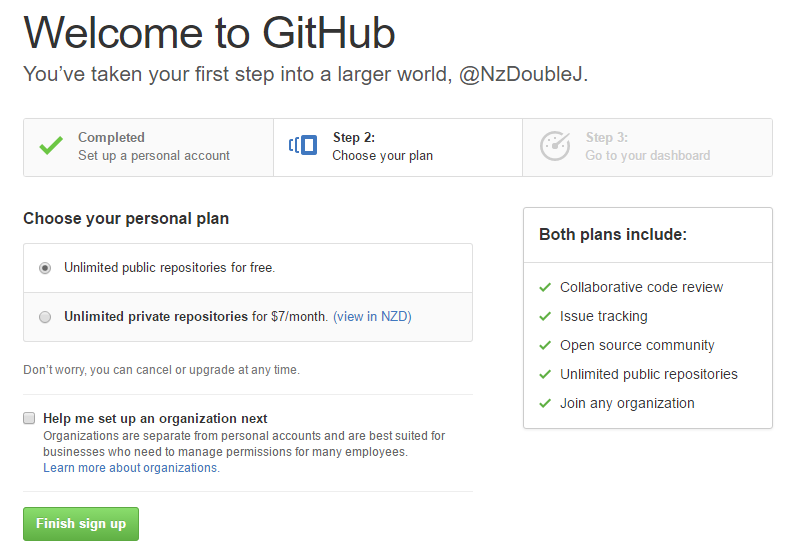
Modern web frameworks are assembled from various individual components to provide a “stack” that come together to perform the application function. All these individual components look after a specific aspect of the overall application, these individual components require information from each other to perform their own task so the complexity of integrating the CIA model into each component but still having the availability to have access to the data within becomes increasing complex to integrate and maintain.

# References

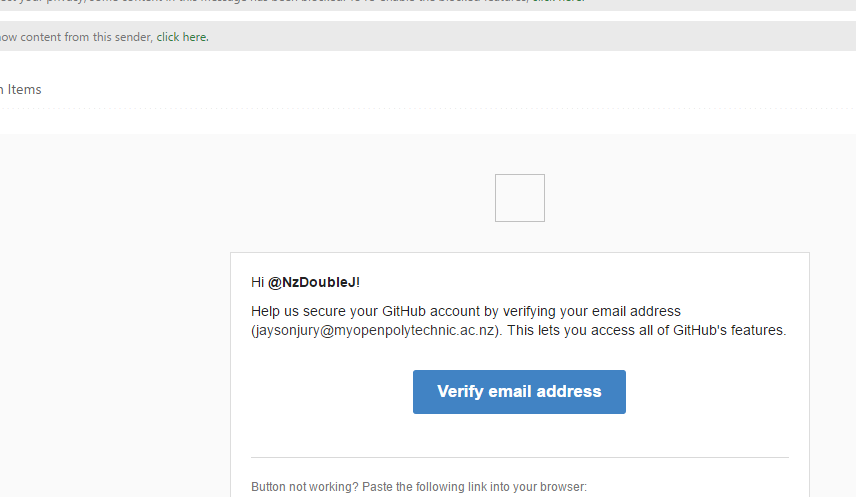
Matthew Haugh, S. G. (2014, November). *What is Confidentiality integrity and avaialbility the CIA triad*. Retrieved from WhatIs.com: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

**Task two**

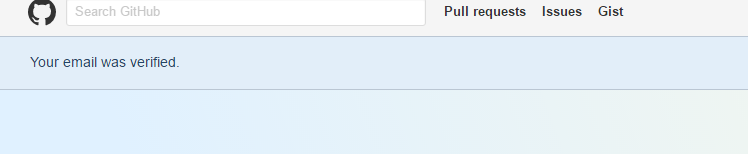
2a.

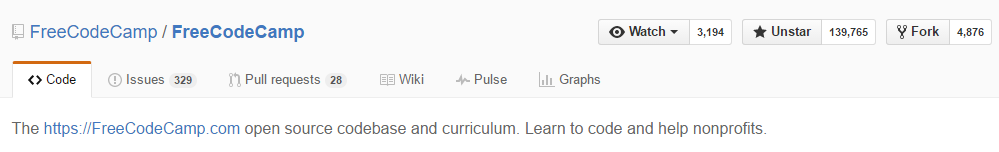


Registering username account

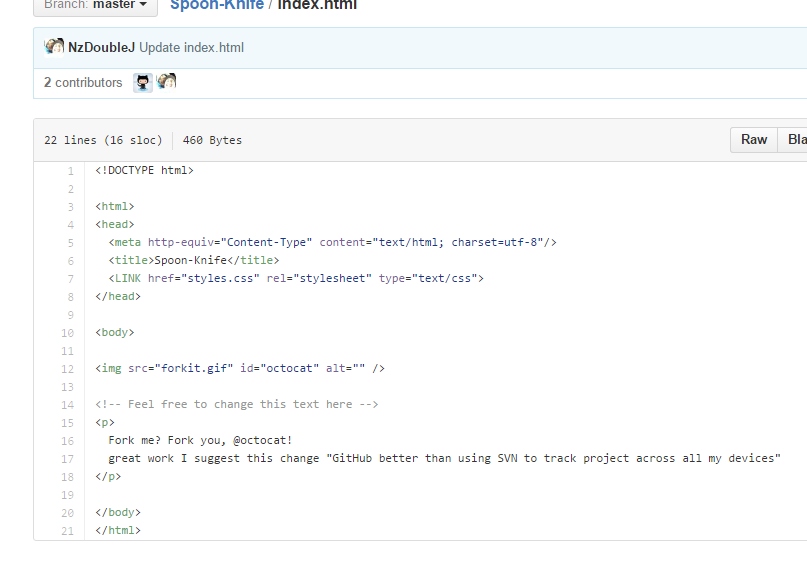


Verifying the e mail address

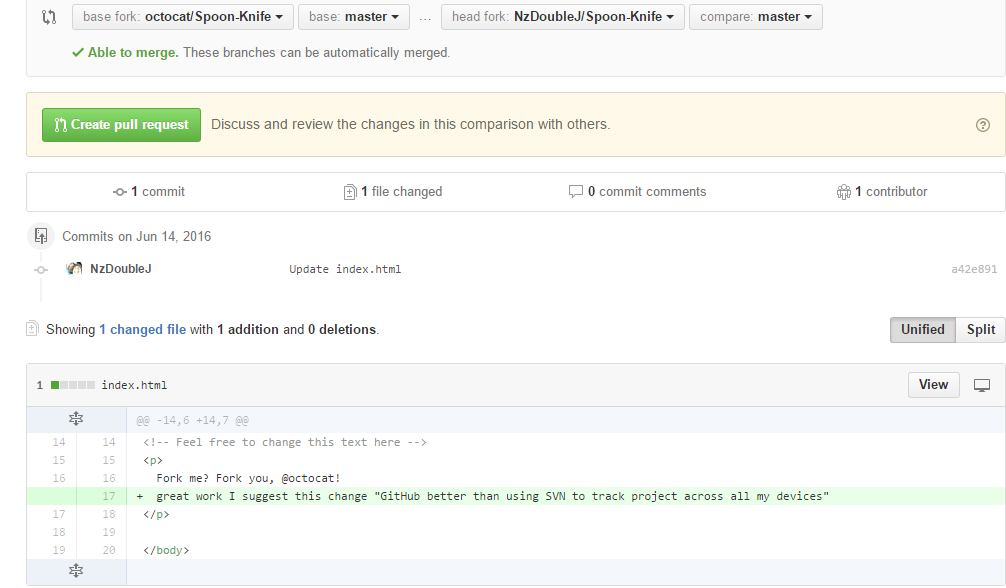




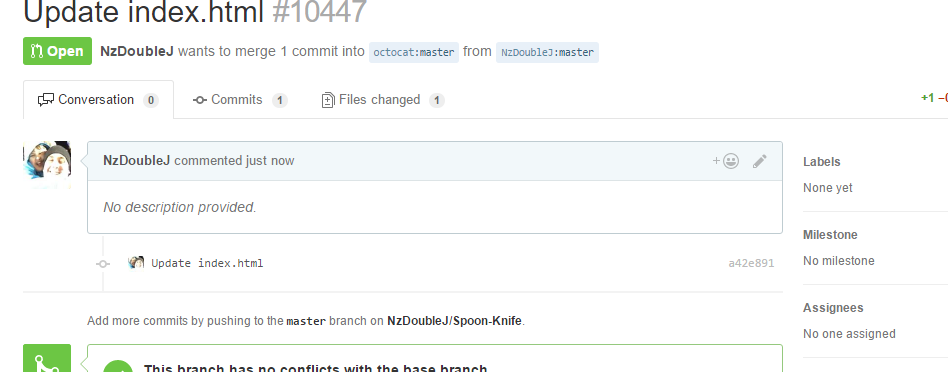
Starring the free camp code repositories

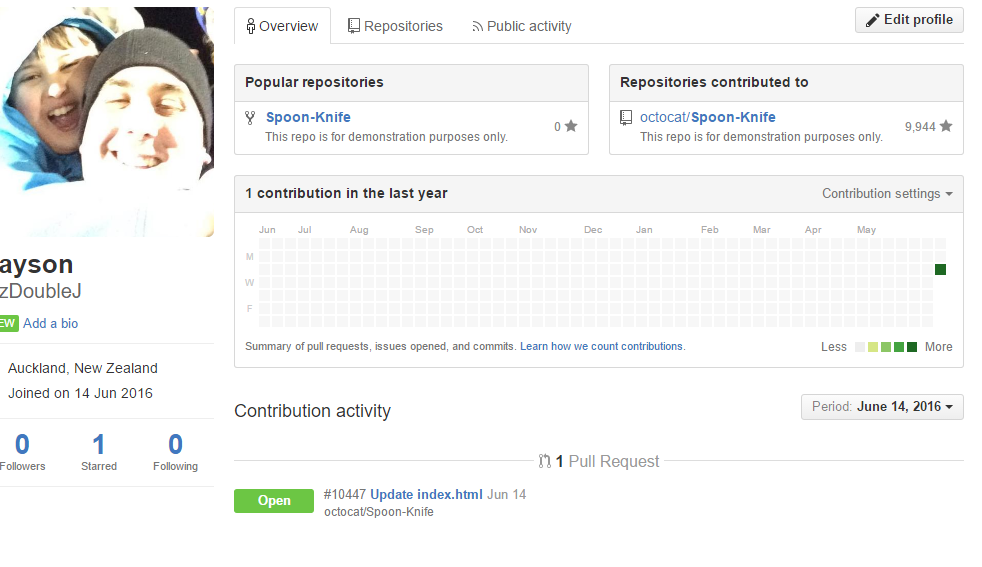


Commit to the index html from the forked repo



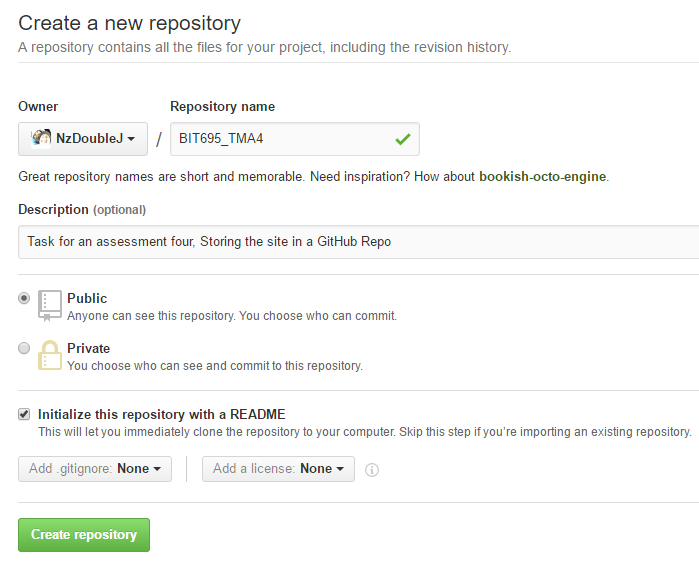
Create pull request for the commit



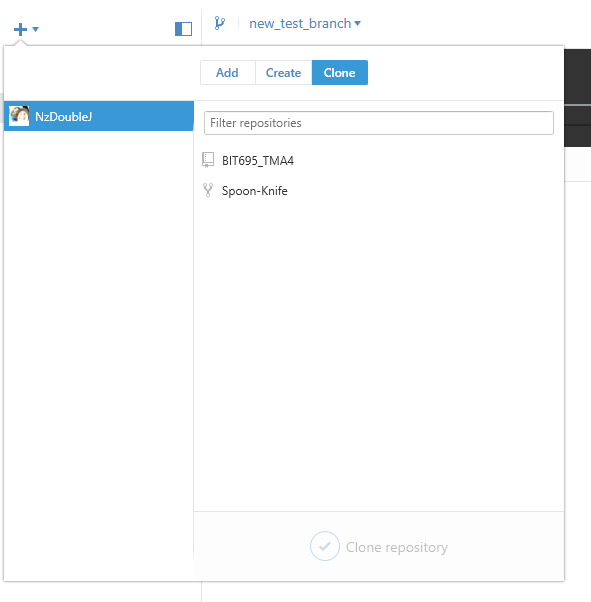


Contribution graph, with the html update pull request.

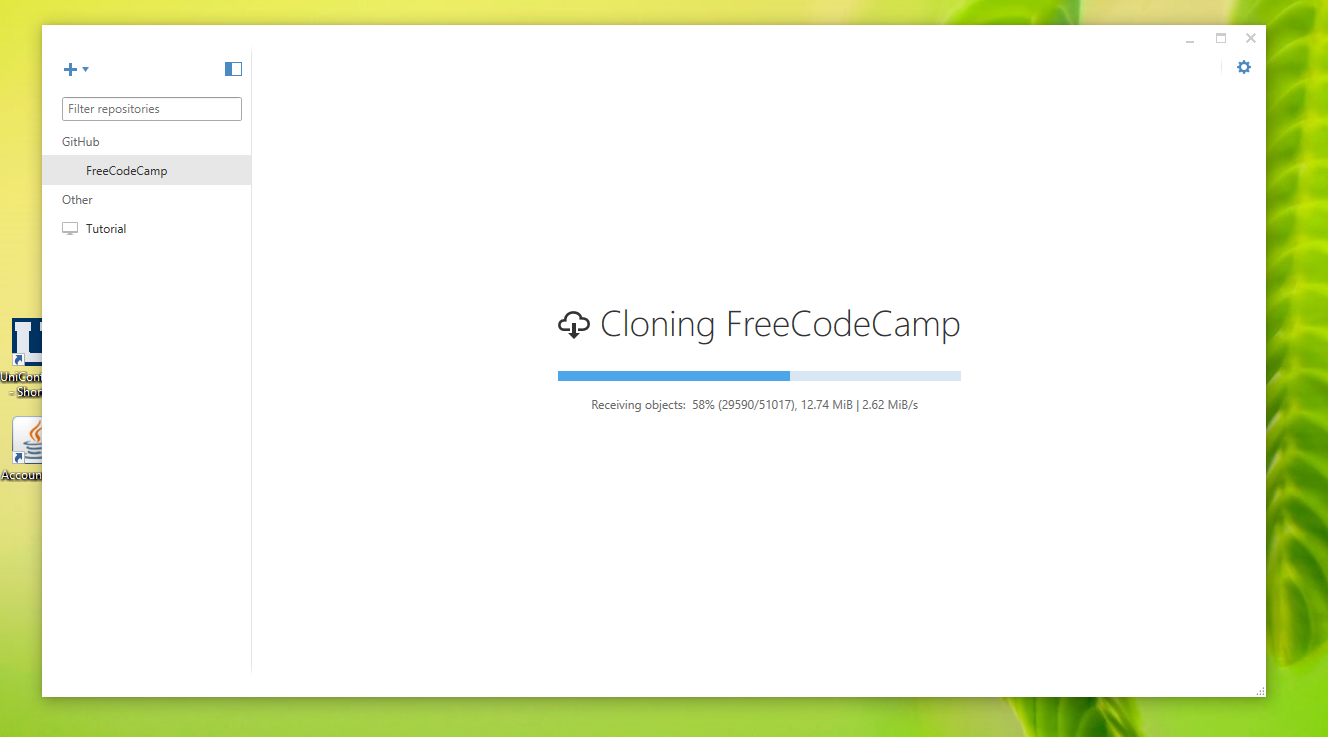
2b.



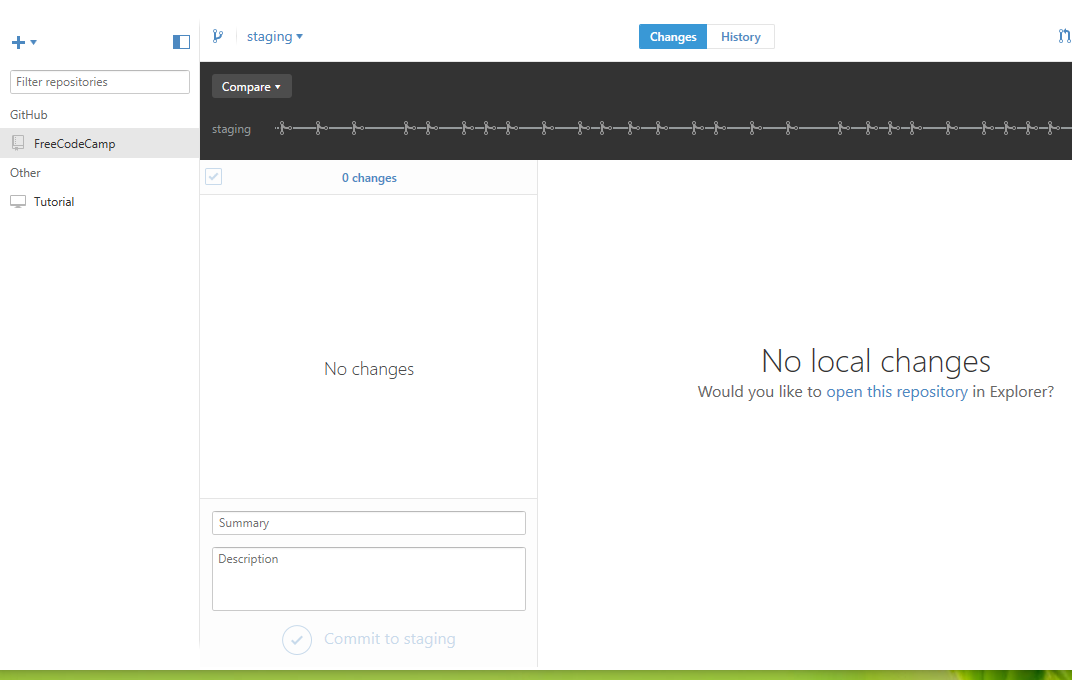
Creating the repo for the assignment



Assignment four GitHub repo



Cloning the repo to the desktop client.



Successfully cloned repo in the local GitHub desktop folder.

2c.

|  |  |  |
| --- | --- | --- |
| **Feature** | Bitbucket.com | GitHub.com |
| Desk top client | Yes the desk top client from bitbucket is called SourceTree. | Yes GitHub has a desktop client called GitHub Desktop |
| Mobile configured web view | Has several community developed native apps for viewing account while on the go. | Site has a mobile friendly area for keeping track of your code while away from the desk. Also native apps available. |
| Private Repositories | Allows free members to create | Only available to paid subscribers. |
| Number of collaborators | * Unlimited with public repos * Is restricted to 5users for free private repos, subscription model to pay for more users accessing private repos | Unlimited number of collaborators for public and private repos, although to get private repos requires subscription model. |
| Team management | Yes allows for branch permission control, allowing who can change your code. | Allows team management with “read” “read-write” or “admin-level” |
| Two factor authentication | Could not find this feature | Two factor authentication by password and an SMS or smartphone app generated code |
| Repo language setting | Allows a setting to set the language of the repo when created | Could not find this feature |
| Syntax highlighting of text | Has some syntax mark-up highlighting | Syntax highlighting support for over 200 languages |
| In code team commenting | Inline threaded conversations and mentions right in the code view | Could not find direct reference in github |
| Social hub | Social side more based on sharing your repositories with people, no social area as such that I found | Social hub so can get involved with the GitHub community |

**TASK THREE**

**a.**

**Planning Table**

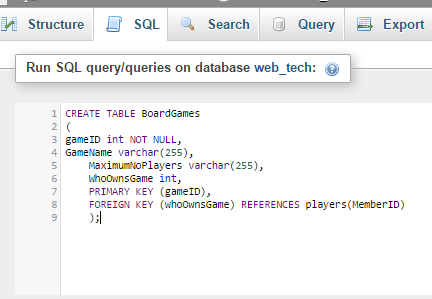
|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Start date and time** | **Expected completion date and time** | **Notes and Comments** |
| Update the database with additional tables | 14th June 7pm | 15th June 6pm | The SQL code for foreign keys may need review on correct syntax |
| Producing the CRUD for the tables | 19 June 1pm | 7-8pm | Could blow out with code snippets |
| Testing the html, CSS and PHP files for each of the crud files | 19 June 7-8pm | 19 June 10pm | Could a lot of time, estimated time usage will be more accurate with more experience, left a lot of time |
| Optimising for the mobile environment | 19th June 12pm | 19th June 1pm | Use of bootstrap CSS to simplified the implementation |
| Standards compliance web side html, CSS | 19th | 19th | Use HTML5 validator https//:html5.validator.nu |
| Upload content to GitHub and download zip | 19th June 10.30 | 19th June 11pm | Noted some people experience server upload delays |

**Risk Assessment**

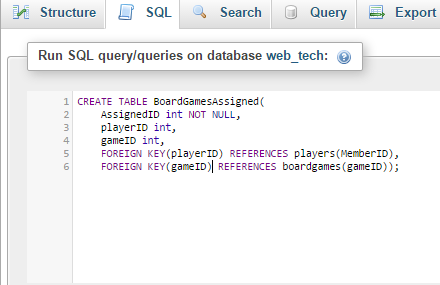
|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Event** | **Impact** | **Mitigation Steps** | **Severity(1-5)** |
| SQL code syntax for foreign and public keys | May not link the tables as intended | Do online review or tutorials and examples, Testing to make sure works as intended | 2 |
| Mobile optimisation | Form not displaying as intended on a mobile device | Allow more testing and refinements of the code for the mobile devices | 3 |
| Project time over run | Not having enough time to fully test all, code thoroughly, getting project out before feel comfortable with it | Make use of more tutorials, to help with.  Make use of previously built know good code as a template for these.  Worse case deliver what is done, call it an Agile development. | 4.5 |
| Compliance validation | May be a lot of non-standards code that needs tiding up. Can blow out the project timeframe if a lot of errors | Allow enough time to work through errors | 4 |
| Upload problems to git | Connectivity issues with servers | Allow time for the upload sync, zip locally | 1 |

b. **Table creation**

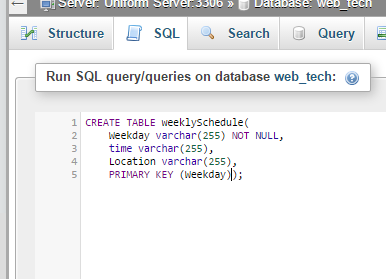
1. Board games table about the board game name maximum number of players and who owns the game.



1. Board game assigned to players, this is a table about who currently has the board game. Refernces game id from the board game table and also references the memberID from the players table



1. The schedule table made of columns weekday (primary Key) time, and location.



1. High score table

