Task 1

a.

This analysis assumes that the case study web application is a static website, as presented in the TMA1 assessment files. Based on the tests referenced in the OWASP guidelines, the case study web app can be considered secure. The guidelines suggest a review of the source code, and doing so reveals no obvious vulnerabilities. The source code does reveal an unused form submission page in which a user could enter their information in order to "join a game", however the page is not included in the web app index and there is no way to access it by browsing the app. Furthermore, analysis of the source code reveals that the form has no functionality for uploading the entered information to a web server. The OWASP guidelines also suggest penetration testing to ensure the web app is secure. This involves browsing the web app with the intent to find and exploit vulnerabilities. Doing so reveals no obvious vulnerabilities. The web app is a static website. Users cannot perform any actions except to browse between the two available pages. Users do not have an account to log into and there is no user information to protect. Given these facts, it appears there is little that an attacker could do to interact with the web app because it allows no input. It should be noted however that I have little experience in identifying web app vulnerabilities and someone experienced in penetration testing might find exploits which I have missed. A third testing technique identified in the OWASP guidelines is threat modelling. This is a type of risk assessment which helps developers think about the pressing security threats in their app. A threat model will often be a collection of lists and diagrams outlining threats, but this has not been completed for the case study web app. However, it could be argued that the app is very basic and that much of what could be learned from threat modelling the app has already been gleaned from penetration testing.

b.

In the CIA triad, availability refers to information that is available when authorised users need access to it. For an e-commerce enabled web application, availability is especially important. A web app of this kind operates 24 hours a day, every day. For a business that sells goods online, less availability means less orders shipped, less funds transferred, and less customers interacting with the web app and making purchases. As a result, even a short period of downtime can cost a web app a significant amount of money, as well as customers. A user accustomed to the almost-instant gratification of most web apps will likely purchase from a different app if their first choice is experiencing downtime. An e-commerce enabled web app needs to ensure it can handle the amount of customers visiting too, otherwise high traffic could mean users experience a slow and unresponsive app which will then push them to purchase from other faster and more reliable apps. Furthermore, any "time-out" errors that appear to customers as a result of high traffic could instil a level of distrust in the customer.

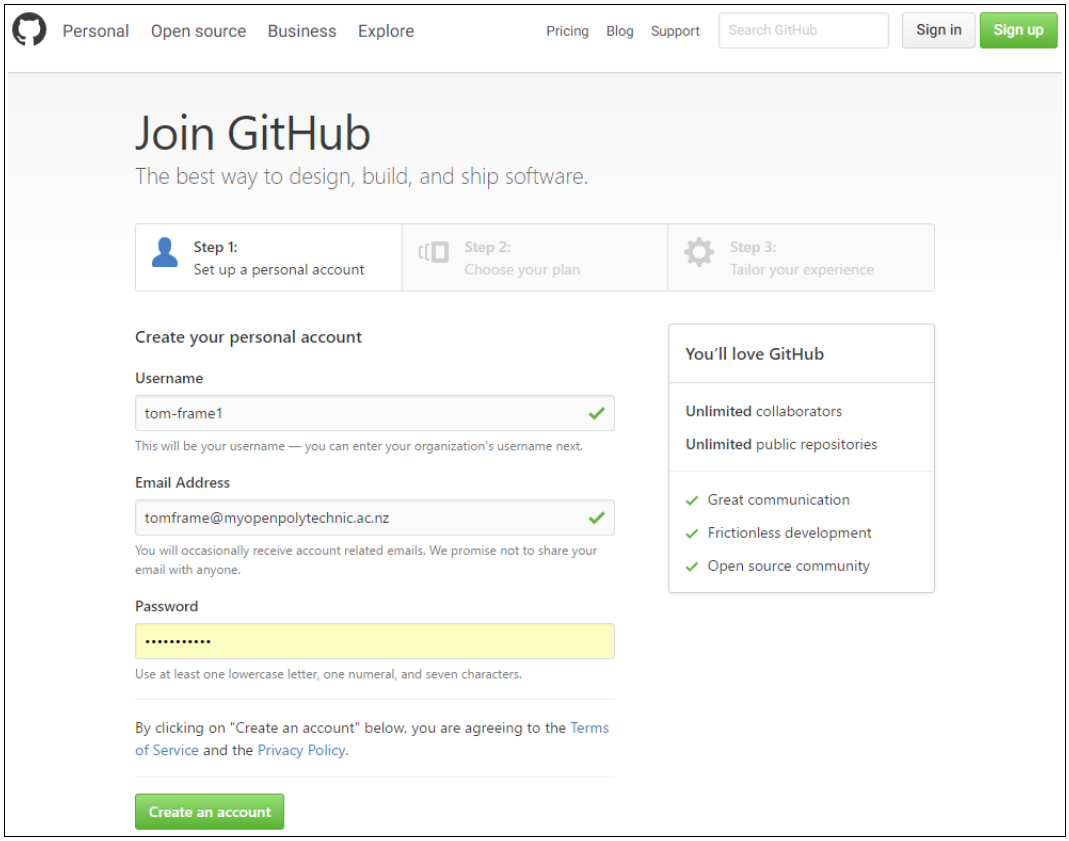
Web applications today can be huge. "Big data" is a term coined for the huge volume of data produced by applications, as well as its variety and the velocity at which it is produced. Given the scale of application data today, the CIA triad model is limited. It does not account for the importance of code validation. A lack of code validation means increased vulnerabilities in the application's code. Given the scale of some "big data" applications, there are more opportunities for attackers to discover a window of bad code in order to compromise the security of an application. Another limitation of the CIA triad model is that it does not consider the "Internet of Things"- the increased embedding of computing devices into everyday objects in order to enable connection to

the Internet. With the increase in the number of Internet connected devices comes the increased chance of vulnerabilities. As a result, user authentication has become more important. The CIA triad is limited in this regard because it does not emphasise the importance of authentication.

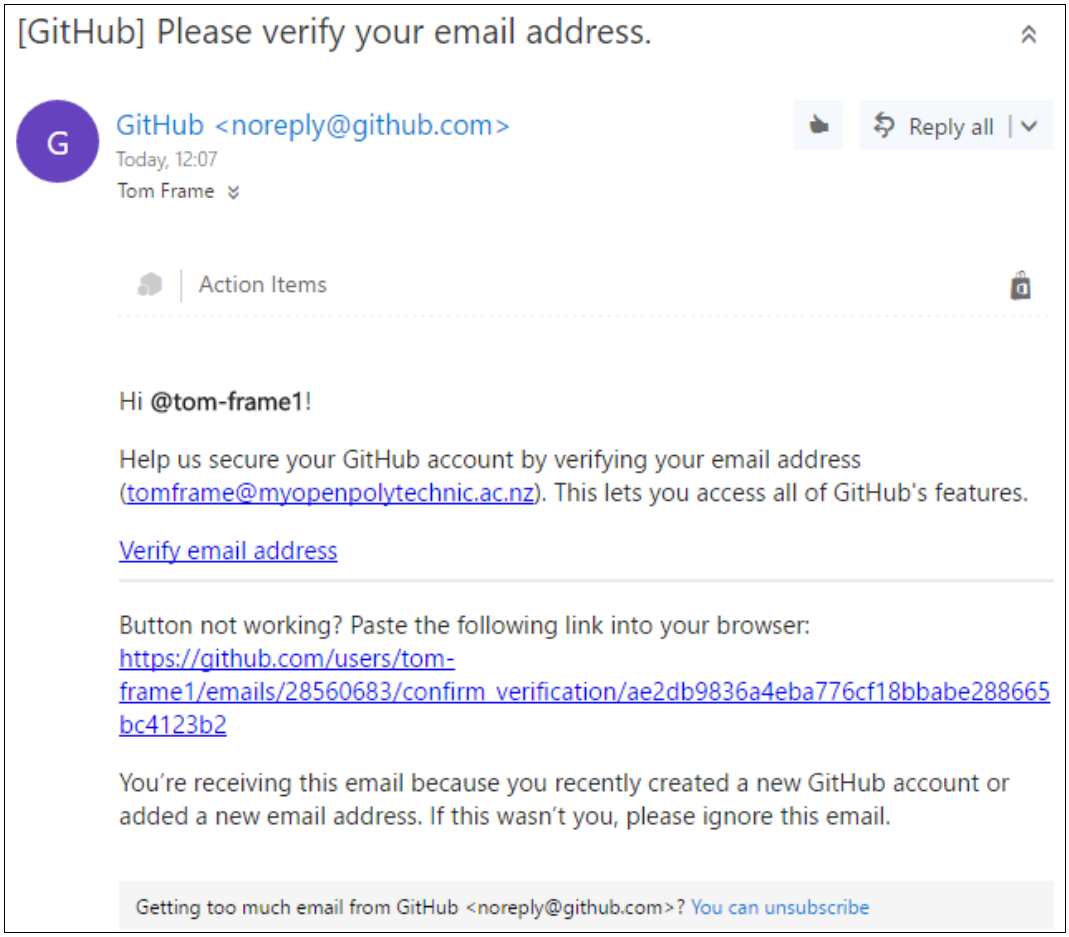
Task 2

a.

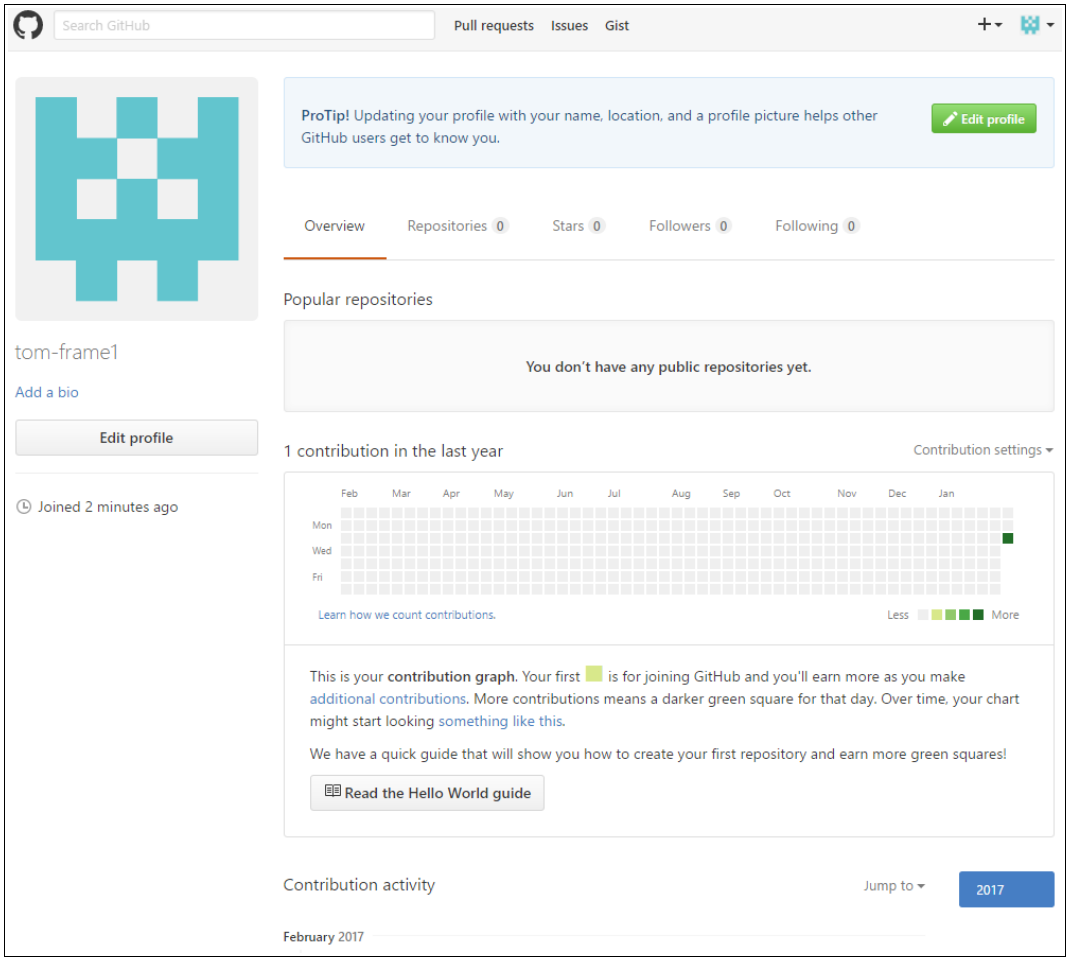
1.



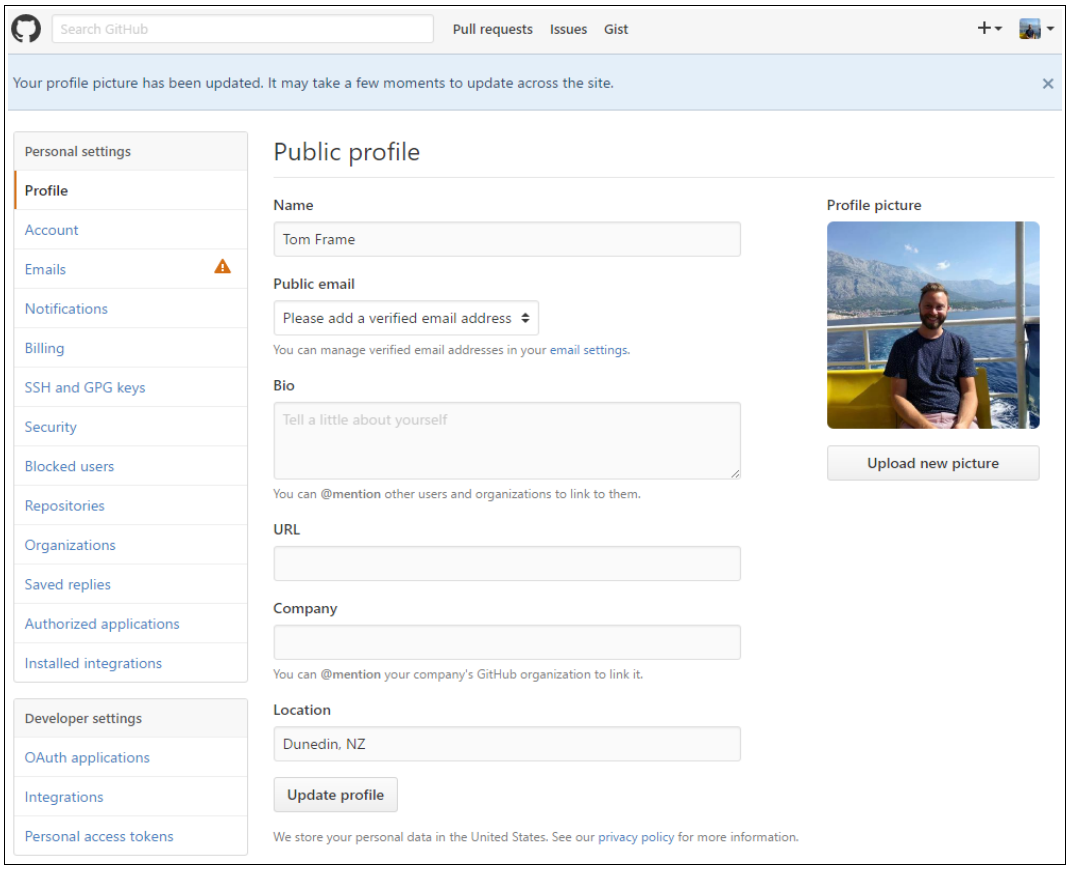
2.


[GitHub] Please verify your email address.
GitHub <noreply@github.com>
Today, 12:07
Tom Frame
Reply all
Action Items
Hi @tom-frame1!
Help us secure your GitHub account by verifying your email address (tomframe@myopenpolytechnic.ac.nz). This lets you access all of GitHub's features.
Verify email address
Button not working? Paste the following link into your browser:
https://github.com/users/tom-frame1/emails/28560683/confirm_verification/ae2db9836a4eba776cf18bbabe288665bc4123b2
You're receiving this email because you recently created a new GitHub account or added a new email address. If this wasn't you, please ignore this email.
Getting too much email from GitHub <noreply@github.com>? You can unsubscribe

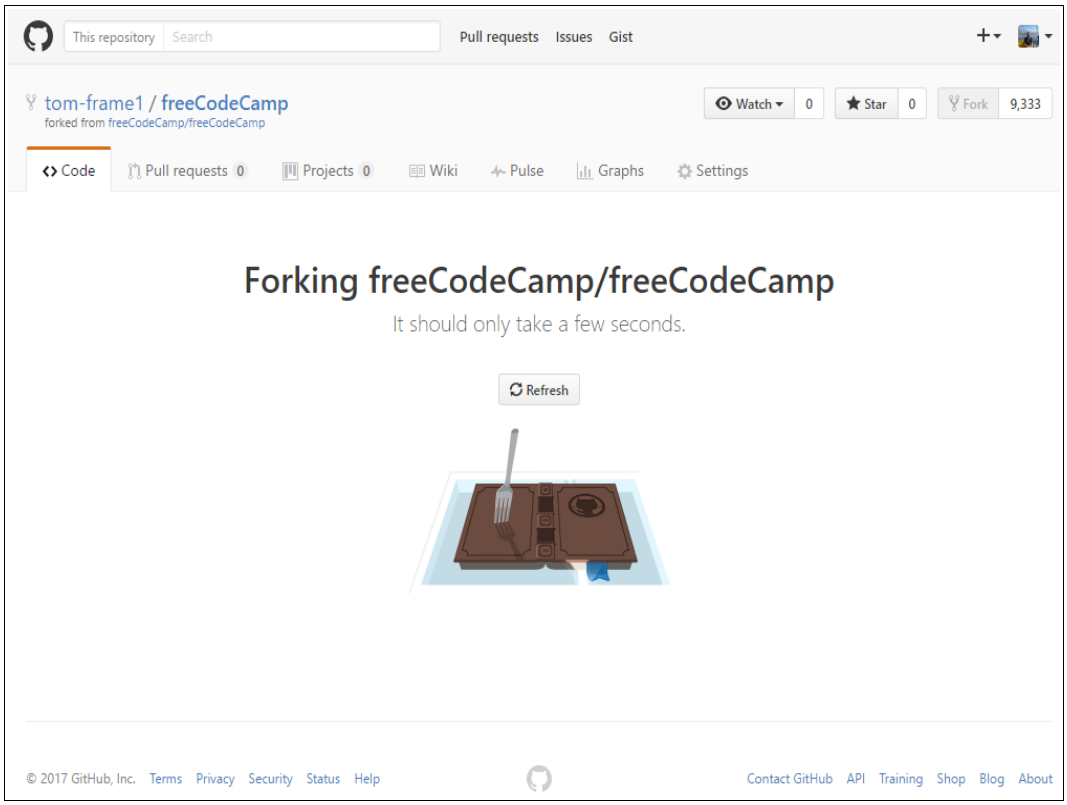
3.


Search GitHub
Pull requests
Issues
Gist
ProTip! Updating your profile with your name, location, and a profile picture helps other GitHub users get to know you.
Edit profile
Overview
Repositories 0
Stars 0
Followers 0
Following 0
Popular repositories
You don't have any public repositories yet.
tom-frame1
Add a bio
Edit profile
Joined 2 minutes ago
1 contribution in the last year
Contribution settings
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan
Mon
Wed
Fri
Learn how we count contributions.
Less More
This is your contribution graph. Your first is for joining GitHub and you'll earn more as you make additional contributions. More contributions means a darker green square for that day. Over time, your chart might start looking something like this.
We have a quick guide that will show you how to create your first repository and earn more green squares!
Read the Hello World guide
Contribution activity
Jump to
2017
February 2017

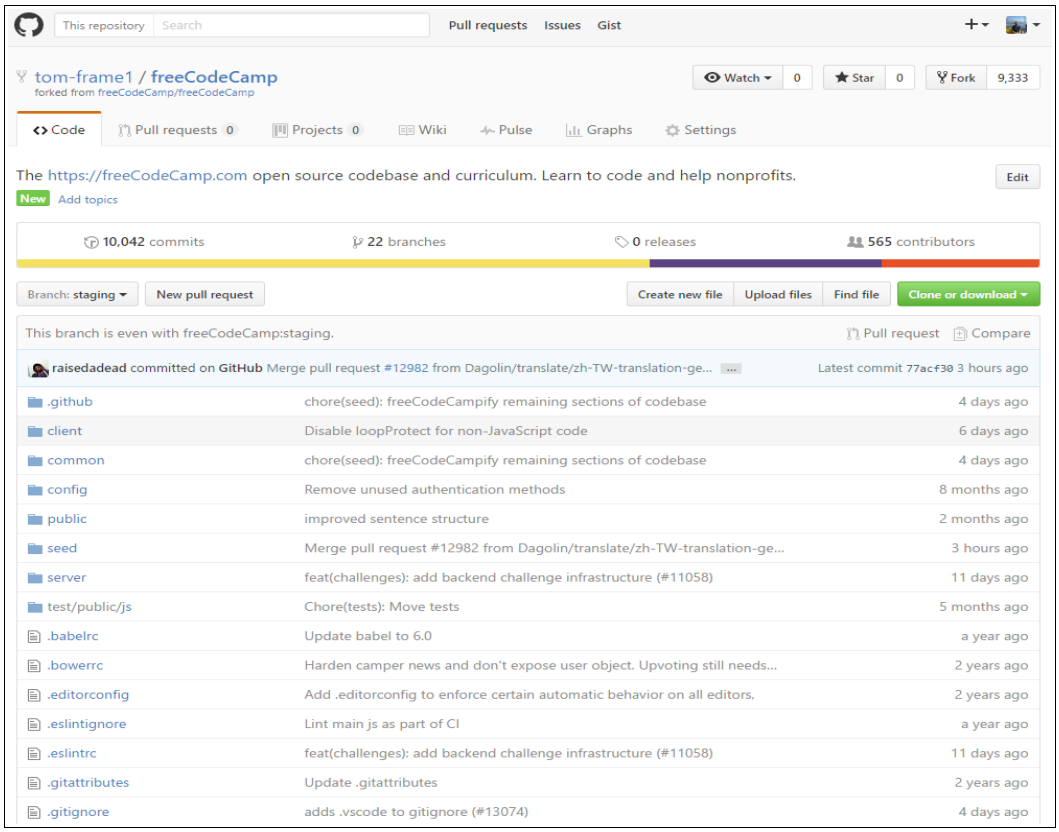
4.


Search GitHub
Pull requests
Issues
Gist
Your profile picture has been updated. It may take a few moments to update across the site.
Personal settings
Profile
Account
Emails
Notifications
Billing
SSH and GPG keys
Security
Blocked users
Repositories
Organizations
Saved replies
Authorized applications
Installed integrations
Developer settings
OAuth applications
Integrations
Personal access tokens
Public profile
Name
Tom Frame
Public email
Please add a verified email address
You can manage verified email addresses in your email settings.
Bio
Tell a little about yourself
You can @mention other users and organizations to link to them.
URL
Company
You can @mention your company's GitHub organization to link it.
Location
Dunedin, NZ
Update profile
We store your personal data in the United States. See our privacy policy for more information.
Profile picture
Upload new picture

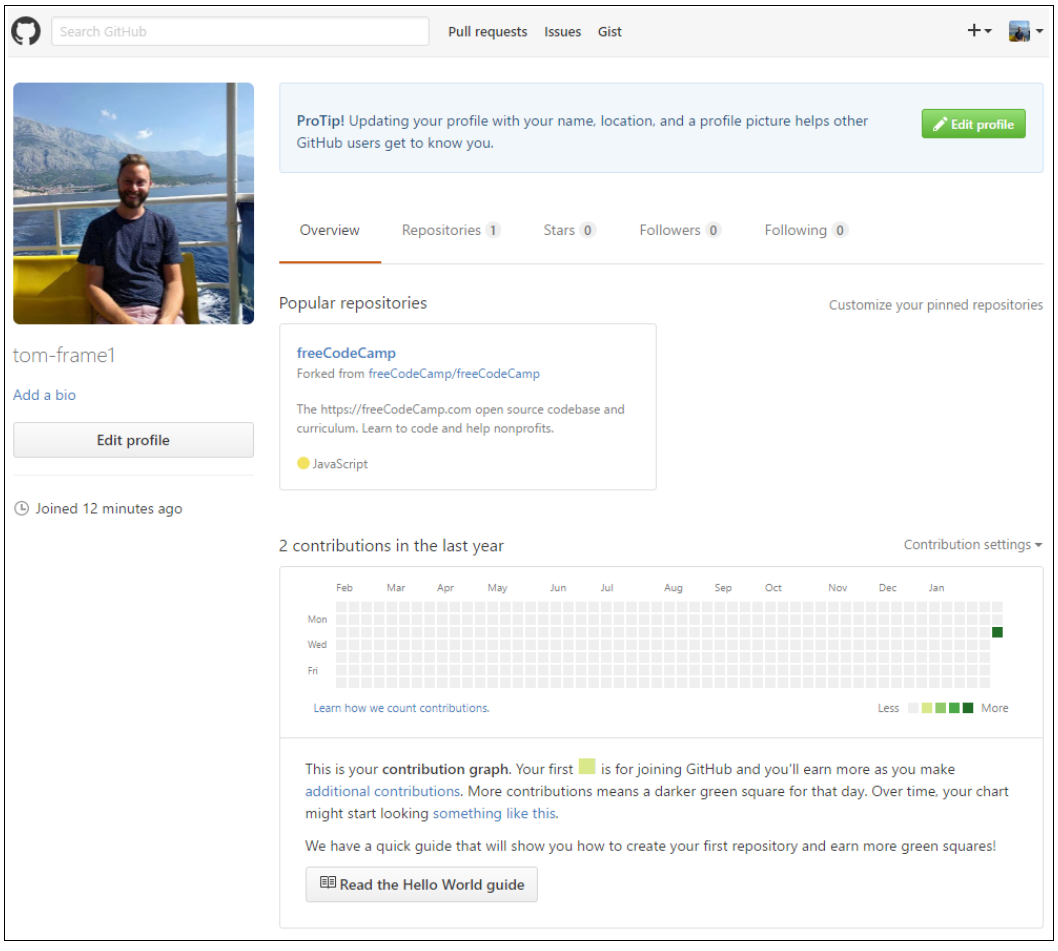
5.


This repository
Search
Pull requests
Issues
Gist
tom-frame1 / freeCodeCamp
forked from freeCodeCamp/freeCodeCamp
Watch 0
Star 0
Fork 9,333
Code
Pull requests 0
Projects 0
Wiki
Pulse
Graphs
Settings
Forking freeCodeCamp/freeCodeCamp
It should only take a few seconds.
Refresh
© 2017 GitHub, Inc. Terms Privacy Security Status Help
Contact GitHub API Training Shop Blog About

6.

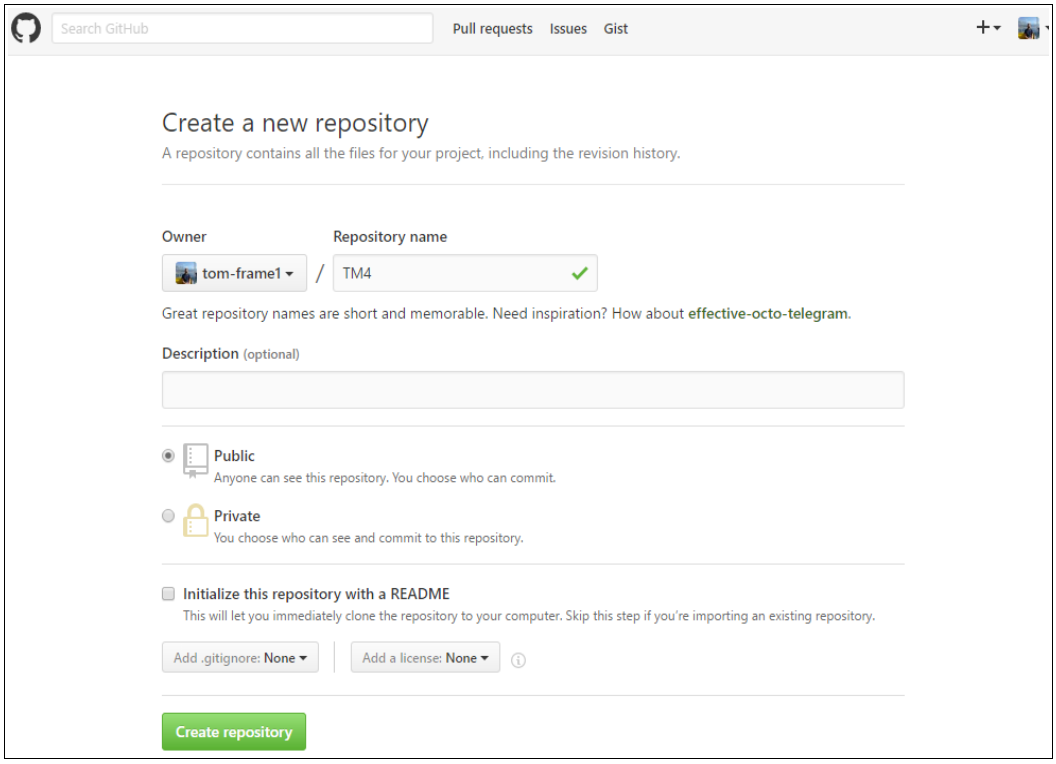

This repository Search
Pull requests Issues Gist
tom-frame1 / freeCodeCamp
forked from freeCodeCamp/freeCodeCamp
Watch 0 Star 0 Fork 9,333
Code Pull requests 0 Projects 0 Wiki Pulse Graphs Settings
The https://freeCodeCamp.com open source codebase and curriculum. Learn to code and help nonprofits.
Edit
New Add topics
10,042 commits 22 branches 0 releases 565 contributors
Branch: staging New pull request
Create new file Upload files Find file Clone or download
This branch is even with freeCodeCamp:staging.
Pull request Compare
raisedadead committed on GitHub Merge pull request #12982 from Dagolin/translate/zh-TW-translation-ge... Latest commit 77acf30 3 hours ago
.github chore(seed): freeCodeCampify remaining sections of codebase 4 days ago
client Disable loopProtect for non-JavaScript code 6 days ago
common chore(seed): freeCodeCampify remaining sections of codebase 4 days ago
config Remove unused authentication methods 8 months ago
public improved sentence structure 2 months ago
seed Merge pull request #12982 from Dagolin/translate/zh-TW-translation-ge... 3 hours ago
server feat(challenges): add backend challenge infrastructure (#11058) 11 days ago
test/public/js Chore(tests): Move tests 5 months ago
.babelrc Update babel to 6.0 a year ago
.bowerrc Harden camper news and don't expose user object. Upvoting still needs... 2 years ago
.editorconfig Add .editorconfig to enforce certain automatic behavior on all editors, 2 years ago
.eslintignore Lint main js as part of CI a year ago
.eslintrc feat(challenges): add backend challenge infrastructure (#11058) 11 days ago
.gitattributes Update .gitattributes 2 years ago
.gitignore adds .vscode to gitignore (#13074) 4 days ago

7.

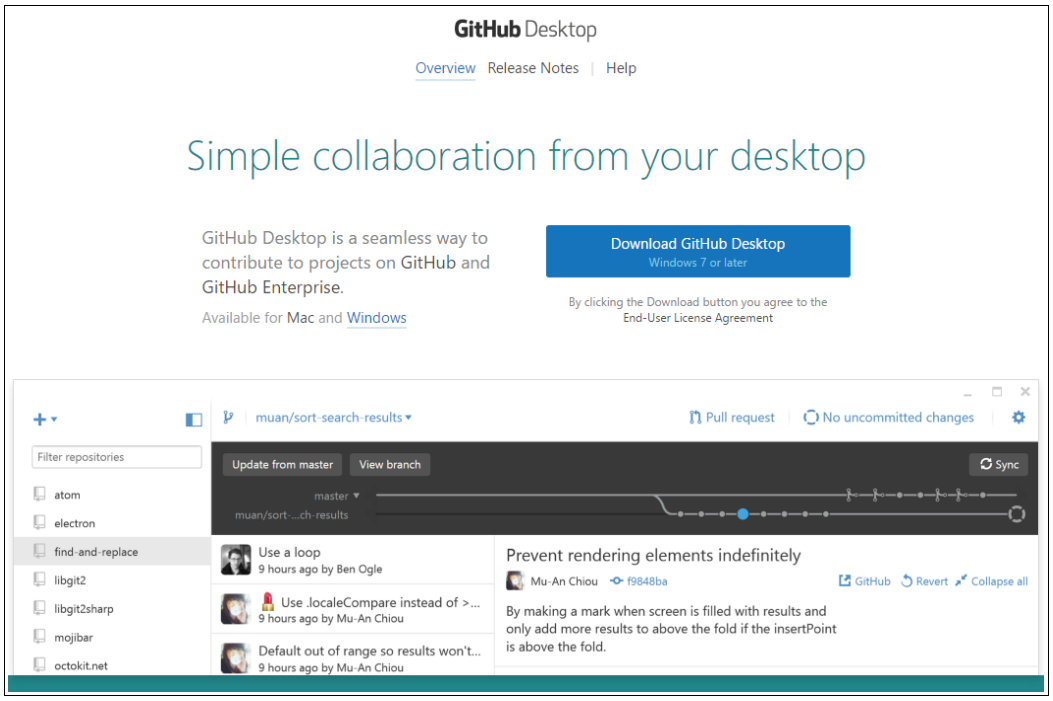

Search GitHub
Pull requests Issues Gist
ProTip! Updating your profile with your name, location, and a profile picture helps other GitHub users get to know you.
Edit profile
Overview Repositories 1 Stars 0 Followers 0 Following 0
tom-frame1
Add a bio
Edit profile
Joined 12 minutes ago
Popular repositories
Customize your pinned repositories
freeCodeCamp
Forked from freeCodeCamp/freeCodeCamp
The https://freeCodeCamp.com open source codebase and curriculum. Learn to code and help nonprofits.
JavaScript
2 contributions in the last year
Contribution settings
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan
Mon
Wed
Fri
Learn how we count contributions.
Less More
This is your contribution graph. Your first is for joining GitHub and you'll earn more as you make additional contributions. More contributions means a darker green square for that day. Over time, your chart might start looking something like this.
We have a quick guide that will show you how to create your first repository and earn more green squares!
Read the Hello World guide

b.

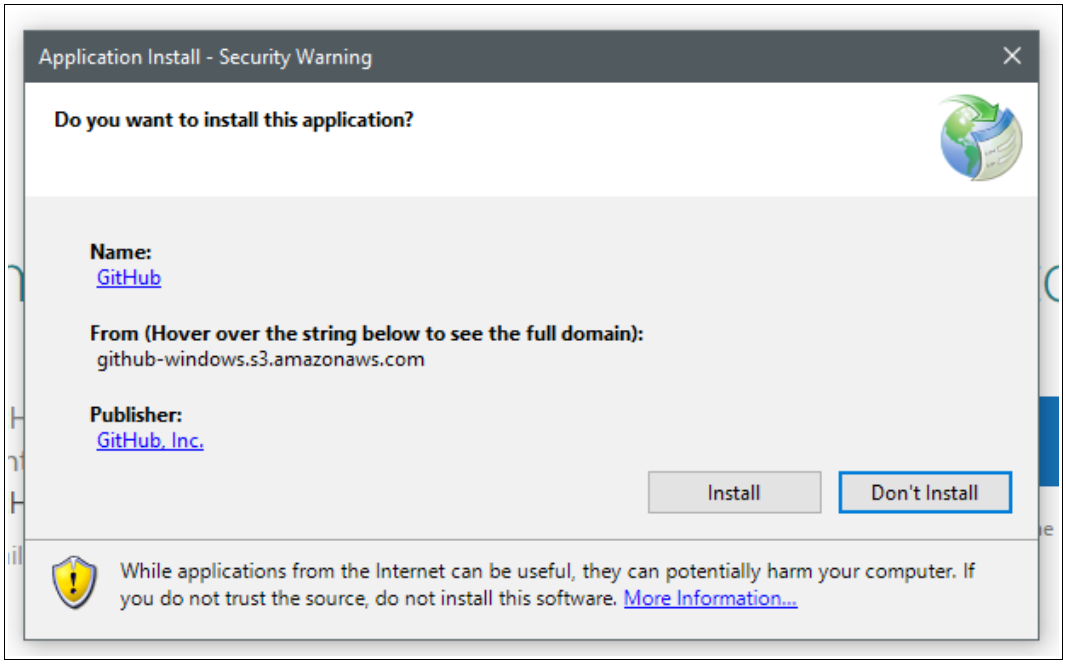
1.


Search GitHub
Pull requests
Issues
Gist
Create a new repository
A repository contains all the files for your project, including the revision history.
Owner
Repository name
tom-frame1
/
TM4
Great repository names are short and memorable. Need inspiration? How about effective-octo-telegram.
Description (optional)
Public
Anyone can see this repository. You choose who can commit.
Private
You choose who can see and commit to this repository.
Initialize this repository with a README
This will let you immediately clone the repository to your computer. Skip this step if you're importing an existing repository.
Add .gitignore: None
Add a license: None
Create repository

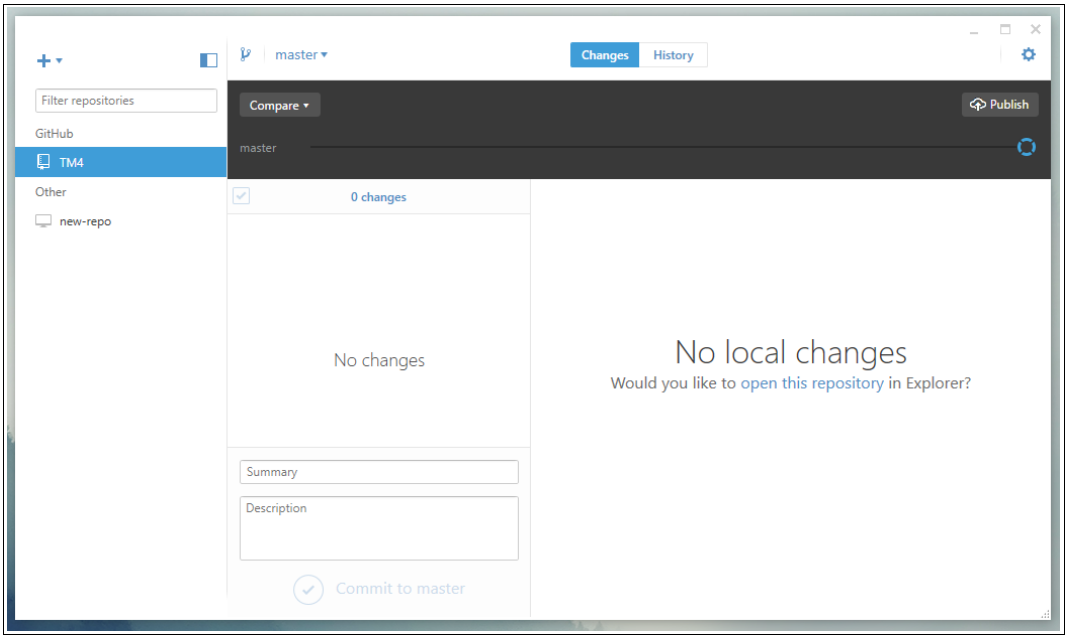
2.


GitHub Desktop
Overview
Release Notes
Help
Simple collaboration from your desktop
GitHub Desktop is a seamless way to contribute to projects on GitHub and GitHub Enterprise.
Available for Mac and Windows
Download GitHub Desktop
Windows 7 or later
By clicking the Download button you agree to the End-User License Agreement
muan/sort-search-results
Pull request
No uncommitted changes
Filter repositories
Update from master
View branch
Sync
atom
electron
find-and-replace
libgit2
libgit2sharp
mojibar
octokit.net
master
muan/sort-...ch-results
Use a loop
9 hours ago by Ben Ogle
Use .localeCompare instead of >...
9 hours ago by Mu-An Chiou
Default out of range so results won't...
9 hours ago by Mu-An Chiou
Prevent rendering elements indefinitely
Mu-An Chiou
f9848ba
GitHub
Revert
Collapse all
By making a mark when screen is filled with results and only add more results to above the fold if the insertPoint is above the fold.

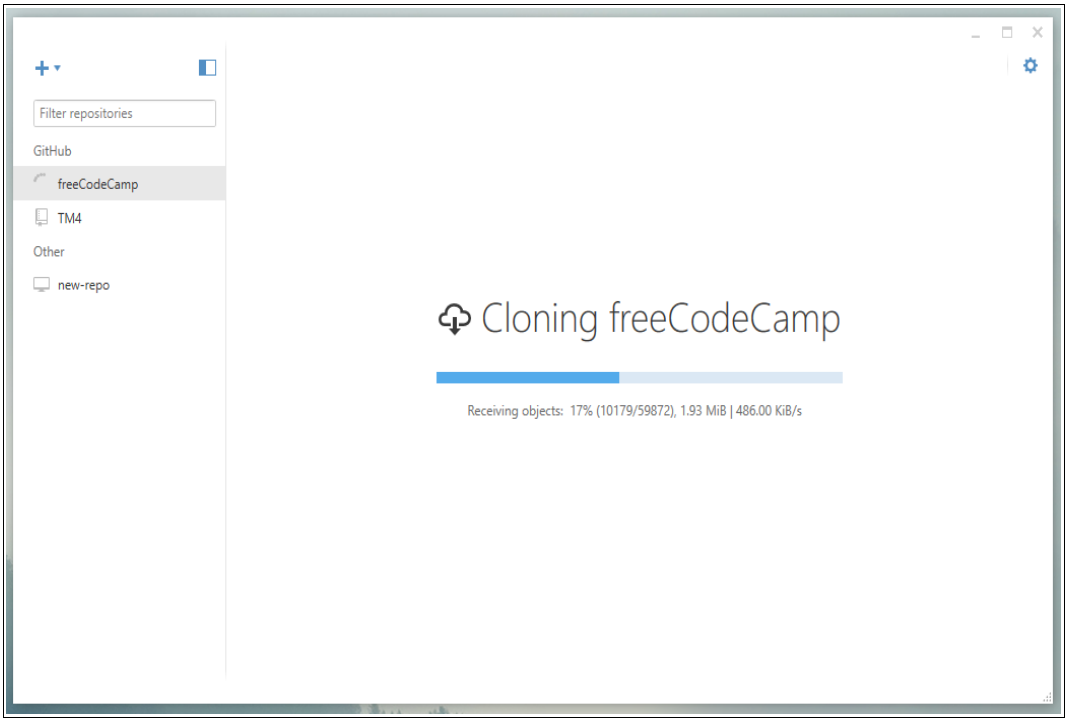
3.


Application Install - Security Warning
Do you want to install this application?
Name:
GitHub
From (Hover over the string below to see the full domain):
github-windows.s3.amazonaws.com
Publisher:
GitHub, Inc.
Install
Don't Install
While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...

4.


master
Changes
History
Filter repositories
Compare
Publish
GitHub
TM4
master
Other
new-repo
0 changes
No changes
No local changes
Would you like to open this repository in Explorer?
Summary
Description
Commit to master

5.


Filter repositories
GitHub
freeCodeCamp
TM4
Other
new-repo
Cloning freeCodeCamp
Receiving objects: 17% (10179/59872), 1.93 MiB | 486.00 KiB/s

c.

Feature	GitHub	Bitbucket
Integration tools for extended functionality	Over 92 third-party integrations	Nearly 2,300 integrations on the Atlassian Marketplace
Open source code hosting	The world's largest source for open source code	Used for open source projects, but geared more toward private code
Private repositories	Unlimited, but cost is $9 USD per user, per month on an “Organisation” plan	Unlimited and free for up to 5 users. $10 USD for 10 users, with cost increasing as more users are added
Version control software (VSCs) and importing repositories	Supports Git, SVN, HG and TFS. Does not support Mercurial repositories	Supports Mercurial repositories as well as Git, CodePlex, Google Code, HG, SourceForge and SVN
Discovering repositories	An “Explore” function which allows users to browse repositories with sections for “trending” and showcased repos	Offers only a “Search” function and no ability to browse unknown repositories
On-premise hosting	“Enterprise” plan allows hosting on your own servers starting at $21 USD per user, per year	Hosting on your own server starts at a $10 USD one-time payment for up to 10 users, and this increases as more users are added
Repository size limits	1GB. GitHub sends an email requesting that repository is downsized limit is exceeded. Supports larger repo sizes through separate Git LFS option	1GB, with a hard limit of 2GB at which point pushing to the repository is disabled. Supports larger repo sizes through separate Git LFS option
Desktop client	Official “GitHub Desktop” application	“SourceTree”, an application that can be used with Bitbucket, created by the same developers, Atlassian
Mobile app	Official client now unsupported but third-party alternatives are available such as “OctoDroid”	No official client, only third-party alternatives such as “Bitbeaker”
Social features	Ability to “follow” other users and “watch” projects to be notified of updates. “Issues” section lets users log problems that need to be fixed. “Pull request” button to let others know about changes made to a project and a wiki to collaborate on documentation	Features “Pull request”, “Issues” and wiki but lacks other social features of GitHub

Task 3

a.

Planning

Activity	Start date/time	Expected completion date/time	Notes
User requirements	26/01/17, 06:00	26/01/17, 12:00	Consider the user requirements for a board game club web app. What kind of information will the user enter into the web app? What information will the user browse on the web app?
Software requirements: Plan database tables	26/01/17, 12:00	26/01/17, 18:00	Based on the user requirements, plan a number of database tables. Tables will reflect the type of information a user will input and access. How the tables relate to each other will also need to be planned.
Create database tables	27/01/17, 06:00	27/01/17, 10:00	Develop SQL queries to create each database table and implement referential integrity between tables
Software requirements: Web server	27/01/17, 10:00	27/01/17, 12:00	Ensure Uniform Server is installed and that the web server is functioning
Architectural design: Plan page layouts	27/01/17, 12:00	27/01/17, 20:00	Based on user requirements, decide how users will interact with web app pages (including navigation, form inputs) and plan layouts with wireframes
Detailed design and production			
Code HTML for “C” of C.R.U.D for each database table	28/01/17, 08:00	29/01/17, 20:00	Based on planned page layouts, build the “Create” HTML form for each database table, including PHP code to add data to database
Test each “Create” page	30/01/17, 06:00	30/01/17, 08:00	Test each “Create” page to ensure data is being uploaded to database in Uniform Server
Add JavaScript and PHP validation for “Create” pages, test	30/01/17, 08:00	31/01/17, 20:00	Add required JavaScript and PHP validation, test pages to ensure working as expected

Activity	State date/time	Expected completion date/time	Notes
Create common CSS as well as CSS for “Create” pages	01/02/17, 06:00	01/02/17, 10:00	Plan which CSS classes to use in common CSS file and add CSS code to all “Create” pages to ensure similar look and feel
Code HTML for “R” of C.R.U.D for each database table	01/02/17, 10:00	02/02/17, 20:00	Based on planned page layouts, build the “Retrieve” HTML form for each database table, including PHP code to add data to database
Test each “Retrieve” page	03/02/17, 06:00	03/02/17, 08:00	
Add JavaScript and PHP validation for “Retrieve” pages and test	03/02/17, 08:00	04/02/17, 20:00	
Create CSS for “Retrieve” pages	05/02/17, 06:00	05/02/17, 10:00	
Code HTML for “U” of C.R.U.D for each database table	05/02/17, 10:00	06/12/17, 20:00	Based on planned page layouts, build the “Update” HTML form for each database table, including PHP code to add data to database
Test each “Update” page	07/02/17, 06:00	07/02/17, 08:00	
Add JavaScript and PHP validation for “Update” pages and test	07/02/17, 08:00	08/02/17, 20:00	
Create CSS for “Update” pages	09/02/17, 06:00	09/02/17, 10:00	
Code HTML for “D” of C.R.U.D for each database table	09/02/17, 10:00	10/02/17, 20:00	Based on planned page layouts, build the “Delete” HTML form for each database table, including PHP code to add data to database
Test each “Delete” page	11/02/17, 06:00	11/02/17, 08:00	

Activity	State date/time	Expected completion date/time	Notes
Add JavaScript and PHP validation for “Delete” pages and test	11/02/17, 08:00	12/02/17, 20:00	
Create CSS for “Delete” pages	13/02/17, 06:00	13/02/17, 10:00	
Transfer: Ensure all pages are present in web server	13/02/17, 10:00	13/02/17, 12:00	
Maintenance: Final test for C.R.U.D pages and final CSS touches	13/02/17, 12:00	16/02/17, 20:00	Ensure all forms are validating and working as expected. For example, test that data created with “Create” page can then be deleted with “Delete” page, etc. Add any final touches to formatting/CSS

Risk assessment

Risk event	Impact	Mitigation steps	Severity (1-5, 1 = low)
No computer access (due to breakage, etc)	Medium	Ensure all work is backed up and able to be transferred to new computer with minimal loss of time	3
No internet access	Medium	Ensure that work is backed up to be transferred to a location with internet access, or a back up internet connection is available (e.g. mobile data)	2
Lack of time available	Low	Adhere as close as possible to project plan timings, ensuring unmissable events which could impact available time are allowed for in project plan	2
Unfamiliarity with coding methods	High	Ensure to plan how parts of the project will be coded, and if unsure of how to do something, allow enough time for research into coding methods	4
Unfamiliarity with software	Medium	Ensure that we know how to use the parts of the software (Uniform Server, Notepad++) that are needed for the project before work begins and that time is set aside to learn them	3