BIT695 TMA4 REUBEN COLLINS 3911591

a. Browse to https://www.owasp.org/index.php/Category:OWASP_Testing_Project. You can either download the PDF guide or just browse the wiki page (below the image of the book). This is a valuable resource for ensuring your web application follows best practice in regards to securing it and the data. For this question you are to read *Chapter 2 Introduction* before commencing with the rest of this question.

   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.

One of the first issues I have thought of in terms of security testing for the Board Games Aficiandos example is that there were no tests performed during the Software development life cycle (SDLC).

As there was no testing of the program in place for people, process or the Application itself, one would have to say it would fail a security test within the OWASP guidelines.

By utilising some of the prescriptive and descriptive frameworks provided by the OWASP for integration into the SDLC process, I believe the application could conform to these standards.

OWASP guidelines indicate there are four major testing techniques used:

- Manual Inspections & Reviews
- Threat Modelling
- Code Review
- Penetration Testing

The first technique utilises manual review of code early in the software development life cycle. It uses tested techniques and review to make sure code conforms to guidelines.

I would say that my application would fail this as I did not review the code after getting sections working.

Threat modelling involves emulating various hacking techniques. It is able to be done early on in the SDLC. As I did not do this when developing my code, my application would fail this guideline.

Source code review. I did actually review my code when building the application. This was to mainly ensure information was verified using Javascript. I would give the application a partial pass on this guideline.

I did not do any penetration testing. The application would fail on this point.

As for issues with the security of my application, there are many.

OWASP guidelines really state that security comes down to basic authentication, authorisation, or encryption controls.

My application is lacking in all these areas.

There is no user authentication, there should be some form of check to ensure the user is an actual person, not a bot.

There is no authorisation, an example here would be when a bank uses your phone to authorise a transaction.

There is no form of data encryption. Data held in my database is quite freely available with quite basic SQL commands. This is more than possibly quite a large issue fore security.

Another security issue is password validation. Securities standards with OWASP state that the password used needs to be "a password complexity of six alphanumeric characters must be enforced by the authentication controls used by the application." (owasp.org).

This means some form of back end would need to enforce this guideline.

b. Use your favourite web browser and browse to 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.

- Within the context of this CIA triad, discuss the impact and importance of availability for an e-commerce enabled web application.

In the context of an e-commerce enabled web application, availability is hugely important.

To maximise sales and profit, the system has to basically be available 24/7. It has to available whenever, so the end user sees it as a reliable platform.

Downtime, though sometimes necessary for updates, needs to be kept to a minimum.

Every minute per year a platform is unavailable can have large financial repercussions for a web application. This really is the impact availability has on an e-commerce app.

There is another way availability can be discussed in the context of an e-commerce web app, user information.

User information has to be available, accessible, and quickly accessible at that for the the application to be user friendly..

For instance, say a user wants to buy a new computer but does not have the funds needed to do so.

They click on the web app. And see that an online finance option is available.
When clicking on this option, there is a sign up function linked to your Facebook sign in.

The person then signs up with their Facebook login and is taken to the final pages of the finance document and ultimately the check out.

My point here is: the availability of the user's data in Facebook is facilitating end user experience.

It is all so easy to buy the new computer as the information is been securely passed from app to app
with the CIA guidelines and objectives in mind.

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

The above example showing the importance of availability also illustrates some limitations of the CIA model.

In the context of user authentication and log in techniques, modern web applications use multiple ways to do this. The availability requirements for user information has expanded.

There are a lot of ways user information can be retrieved. This has complicated the idea of availability within the context of the CIA model. And how to keep this data secure.

The CIA model expects the user to be able to easily log in to an e-commerce web at any time.

As I have stated above, with multiple ways to login, information is being accessed in many different ways from many different locations.

This is literal minefield for security.

With different components hosted all over the globe, information is everywhere.

All this information is subject to different countries' laws. This makes the availability guideline in a CIA context blurred – it seems better suited to a traditional client-server models.

Another important aspect is that, availability also relates to the down time of the physical web application. It needs to be available at all times.

With many more apps relying on cloud based componentry, it can be easier to achieve nearly 100% availability.

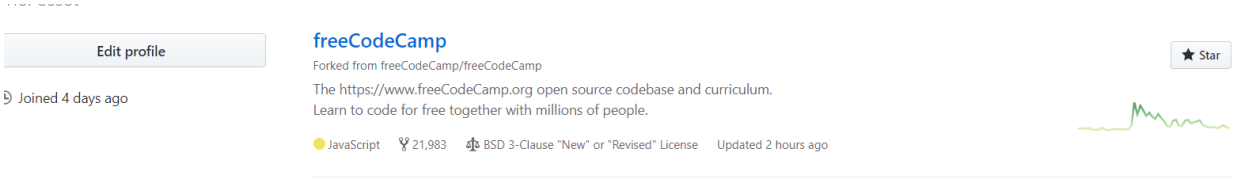
The CIA availability guideline does not necessarily have as much importance now that the cloud is more in use.

Again it seems to be targeted at the more traditional client-server architecture. Web based apps relying on physical hardware such as a servers and hard drives.

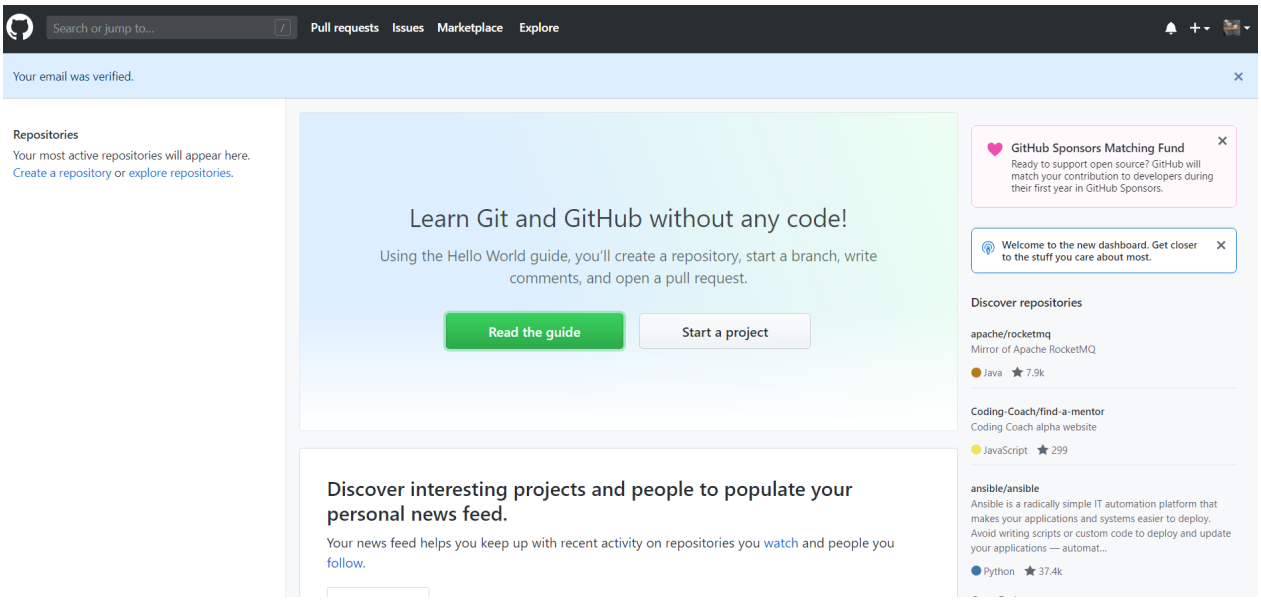
Task 2: Version control

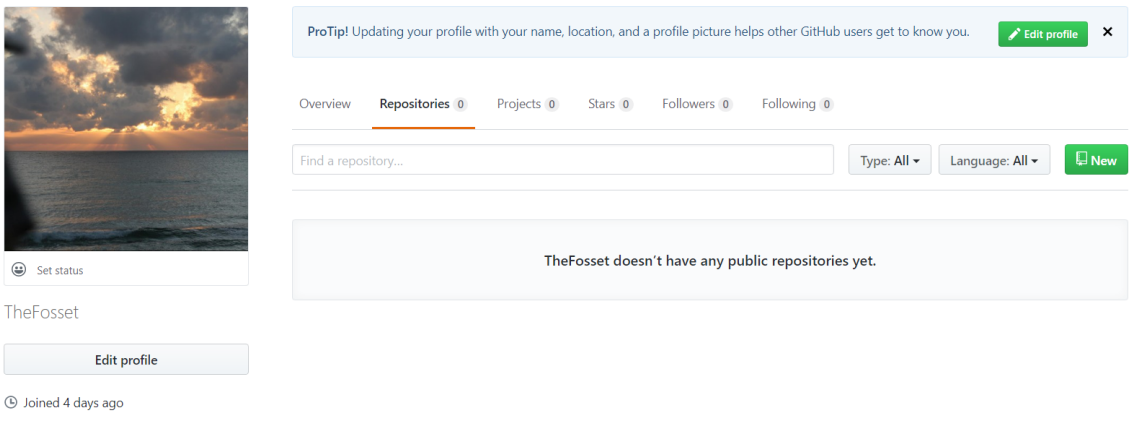
A.)

Forked repository:



Creating a new repository:





TMA4

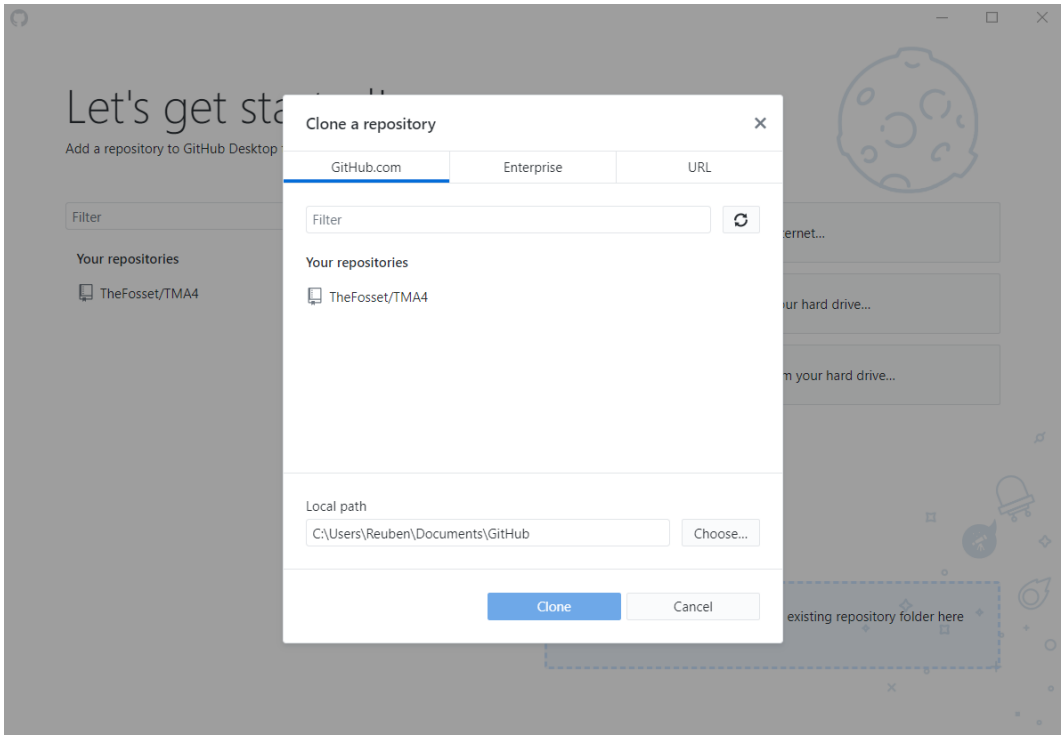
HOME FOR THE TMA4 ASSIGNMET.

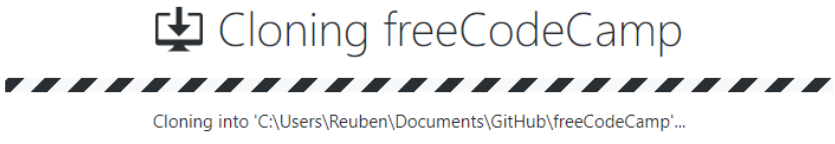
Updated 19 minutes ago

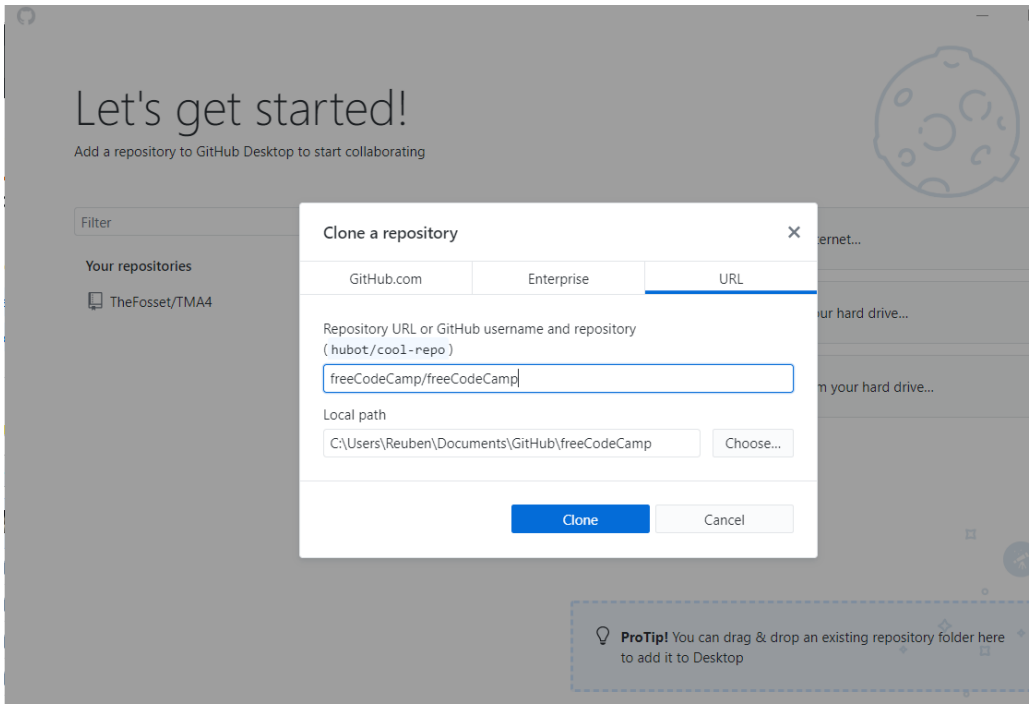
Star

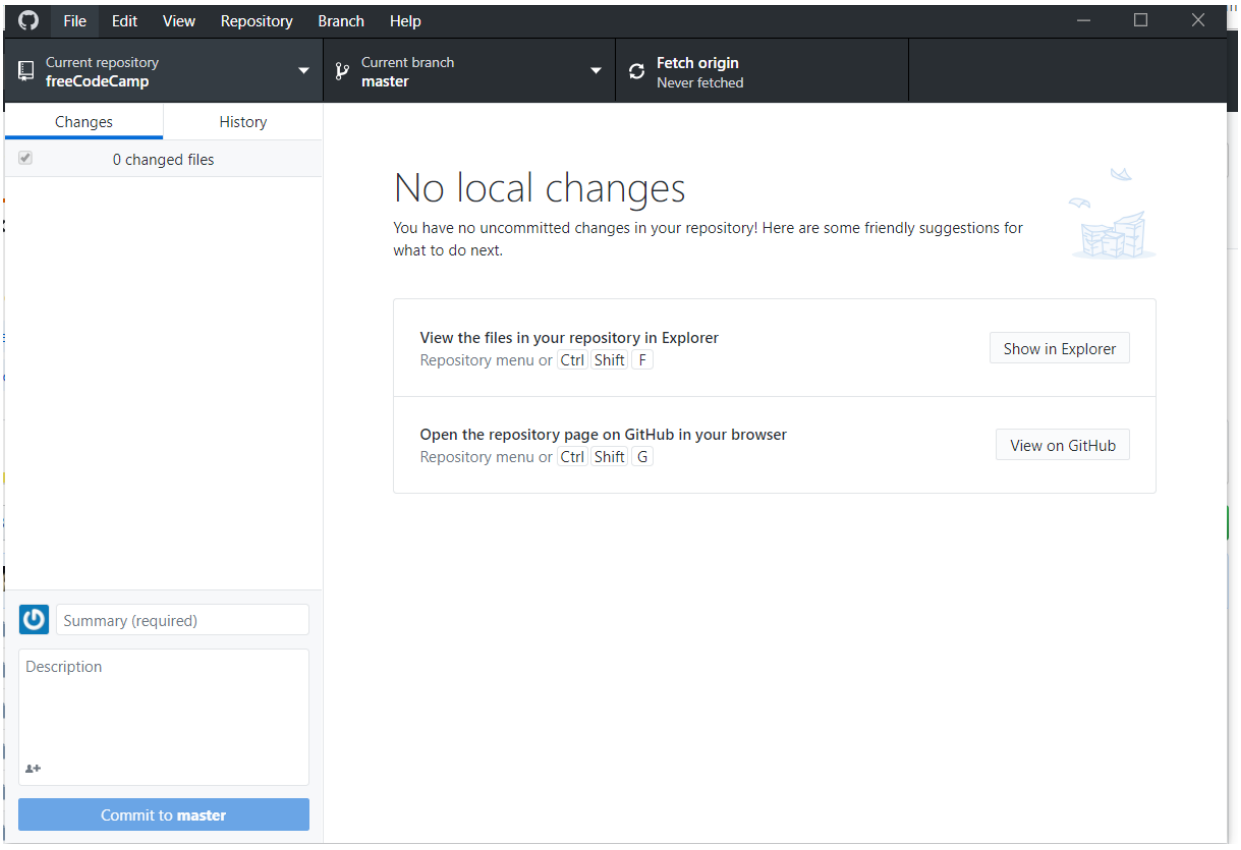
B.)

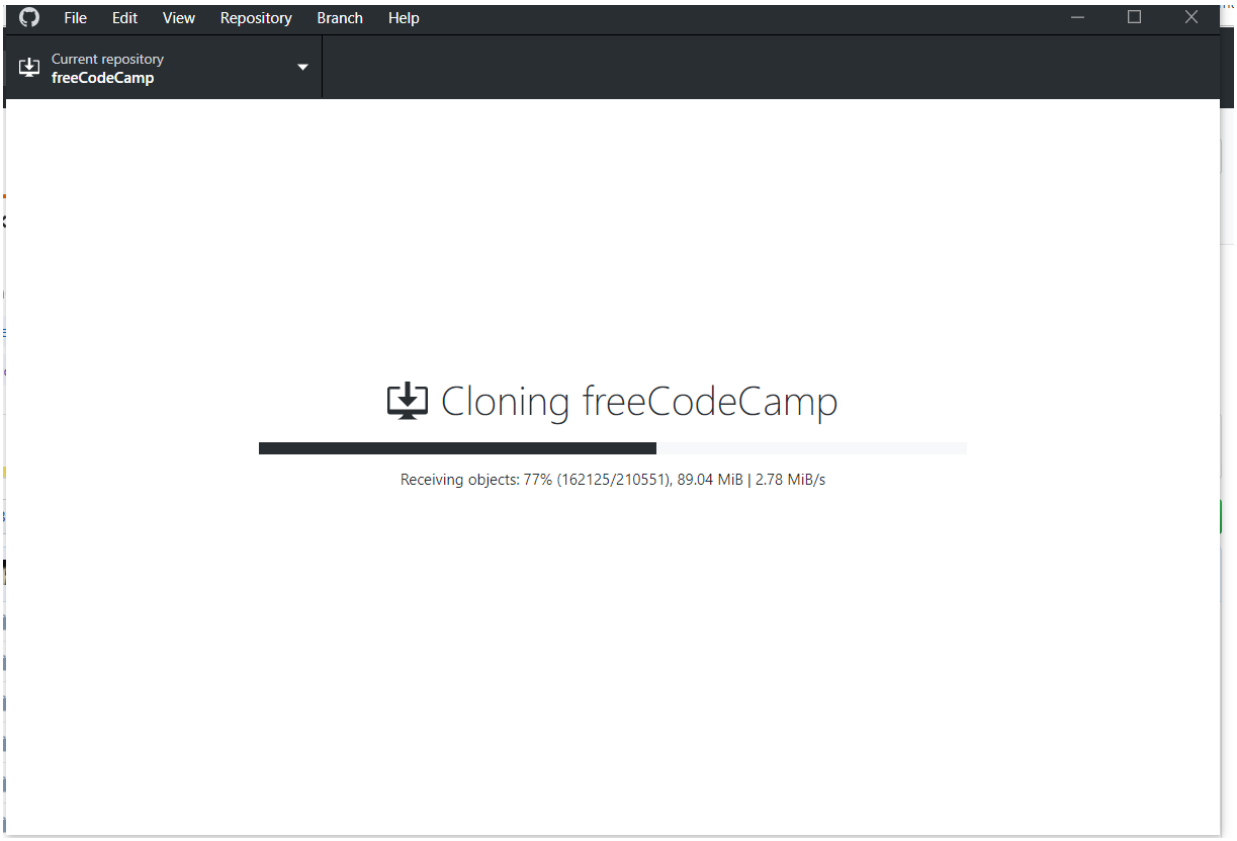
Clone a repository:






Let's get started!
Add a repository to GitHub Desktop to start collaborating
Filter
Your repositories
TheFosset/TMA4
Clone a repository
GitHub.com
Enterprise
URL
Repository URL or GitHub username and repository
(hubot/cool-repo)
freeCodeCamp/freeCodeCamp
Local path
C:\Users\Reuben\Documents\GitHub\freeCodeCamp
Choose...
Clone
Cancel
ProTip! You can drag & drop an existing repository folder here to add it to Desktop


File
Edit
View
Repository
Branch
Help
Current repository
freeCodeCamp
Current branch
master
Fetch origin
Never fetched
Changes
History
0 changed files
No local changes
You have no uncommitted changes in your repository! Here are some friendly suggestions for what to do next.
View the files in your repository in Explorer
Repository menu or Ctrl Shift F
Show in Explorer
Open the repository page on GitHub in your browser
Repository menu or Ctrl Shift G
View on GitHub
Summary (required)
Description
Commit to master


File
Edit
View
Repository
Branch
Help
Current repository
freeCodeCamp
Cloning freeCodeCamp
Receiving objects: 77% (162125/210551), 89.04 MiB | 2.78 MiB/s


Edit profile
Joined 4 days ago
freeCodeCamp
Forked from freeCodeCamp/freeCodeCamp
The https://www.freeCodeCamp.org open source codebase and curriculum.
Learn to code for free together with millions of people.
JavaScript
21,983
BSD 3-Clause "New" or "Revised" License
Updated 2 hours ago
Star

c. Browse to https://bitbucket.org/. This is a platform very similar to Github. Take some time to peruse the site and compare this platform with Github.

Describe the compared features.

Your answer should be in table form and you need to compare at least 10 features. Don't just place a yes/no response into the table. Think of this table as a feasibility study for a project so the detail on the features matters.

Bitbucket vs HitHub(https://bitbucket.org/product/comparison/bitbucket-vs-github).

GitHub	**BitBucket**
Extension tools. Where you host source code can effect how you streamline workflow. App integration tools better manage projects from issue tracking to live chat. This is a comparison toBitBucket. In terms of quantity integrations, The Atlassian Marketplace blows GitHub out of the water. Unifying your extensions under Atlassian means more coherent workflows.	Uniflying your code under Atlassian Marketplace wins over the GitHub competitor.
Open source community. GitHub is the largest host of source code in the world.	More tailored to propriety code.
Server pricing: GitHube would cost users up to $21,600 p/y (https://www.business2community.com/business-innovation/bitbucket-vs-github-best-version-control-software-business-01623901).	BitBucket would only cost $2400 p/y.
Supported VCS: Git.	Mercurial, Git.
Public Repos. Free, Unlimited.	Free Unlimited.
Intergration: Jira, Crucible, Jenkins, Bamboo.	Asana, Zendesk, CloudBees, Travis, CodeClimate, AWS, Windows Azure, Google Cloud, and Heroku.
Popular products hosted: Bootstrap, Node,js, jQuery, Rails, Homebrew	Adium, Mailchimp, Opera, Python, Django.
Notable extra features: Two-factor authentication, Github Pages, Github Gists.	Bootstrap, Node,js, jQuery, Rails, Homebrew

Not available.	**Bitbucket Pipelines** is a feature of Bitbucket that gives you one place to build, test and deploy with integrated CI/CD. Benefit from configuration as code and unlimited scaling without managing build infrastructure. (https://bitbucket.org/product/comparison/bitbucket-vs-github).
Take actions in Slack. They can't do this in GitHub.	With the Bitbucket bot for Slack, teams can take action from their channel. Merge, comment, and even nudge reviewers on pull requests. .

a. **Planning activity**. All projects require planning if they are to succeed. For this question you need to create a schedule (tabular) of activities and a risk assessment.

   The schedule outlines how you are going to proceed with the development and when certain activities need to be completed by. The schedule should correlate with a typical application development lifecycle. Use the following table structure as an example for the schedule.

Activity	Start date and time	Expected completion date and time	Notes or comments

Activity.	Start date and time.	Expected completion date and time.	Notes or comments.
Revision of TMA2.	02/06/19	03/06/19	Get the context of the mini project in relation to the app I built in TMA2.
Design the extended interfaces / wireframes.	03/06/19	04/06/19	Considering this really is done already, I will be extending the the application to achieve more usability.

Code review / bug testing.	04/06/19	06/06/19	Review existing code and look at any bugs that need fixing before designing the new interfaces.
Coding.	07/06/19	14/06/19	Coding the SQL/PHP/CSS/HTML
Testing.	14/06/19	16/06/19	Testing the application.
Deployment.	16/06/19	16/06/19	Upload to repository. Upload to MYOP.

The risk assessment is another core aspect of your typical development life cycle. Identify at least five risks that can influence the success of your project. Use the following headings as a guide.

Risk event	Impact	Mitigation steps	Severity (1-5)

Risk event	Impact	Mitigation steps	Severity
Underestimation of the time/resource commitment.	The project could be late or not ready for a deadline.	Make sure the work is being carried out in a timely and efficient manner. Make sure all hardware is sufficient to handle the project.	5
Scope creep.	The issue of adding on functionality that was not on the original brief. In this case, should not be too much of a problem as I'm just making the app fully functional.	Make sure that no time is spent on functions not required for the assessment.	3
Misunderstanding development issues.	Realise that bugs do crop up. They can slow development as they are fixed in the software development life cycle.	Try to fix any issues as quickly as possible.	5
Inaccurate project estimation.	Deadlines might not be accurate or things may take longer than expected.	Try to stick to the project plan as closely as possible.	3
3rd party integration.	It might take longer than expected to get everything uploaded on the different platforms required by the assessment.	Research steps need to get the project uploaded and functional.	5

b. **Database update**. Before we continue with the web content and coding, we need to add in the missing database tables. Currently you should have the *players* and *board_games* tables.

The following is a suggestion of the potential missing tables.

1. Board games (who has what board game available).
2. Board games assigned to players (An additional database table joining the players with a particular board game) You should already have the basics of this table but there may be some fields.
3. Schedule (should include a venue).
4. Scoring (a typical high-score tracking table).

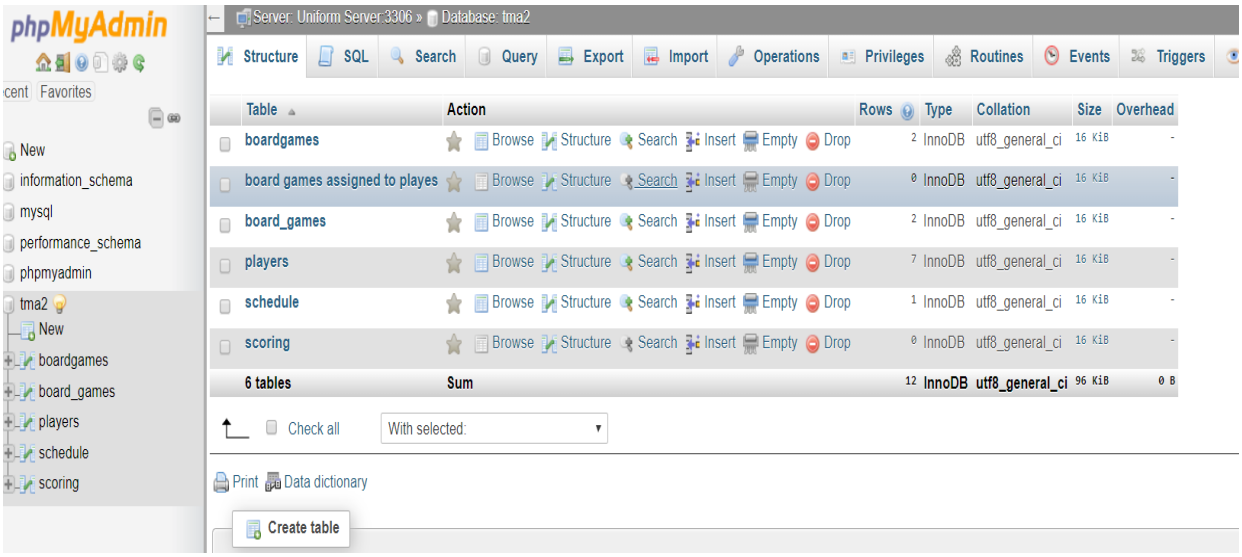
Keep in mind this database model does not include any LUTs (Look-Up Tables) such as town names, postal codes, etc.

Use the webserver stack from TMA2 to facilitate the next step.

Develop the necessary SQL queries that will create the remaining tables. You have freedom with the column names and data types, keeping in mind the relationships between them. This includes the *players* and *board_games* tables previously covered in TMA2.

Be sure to include the necessary SQL code that enforces referential integrity (Foreign keys), indexing (used for search purposes) and primary keys.

Please see the below Database edit:



My .sql file is included in the project files.

c. **Coding**. There should be at least five complete tables now in your database. Each of these tables, except *players*, would require a set of CRUD forms and supporting server side code. For each of these new tables create the HTML, CSS and PHP for the CRUD forms.

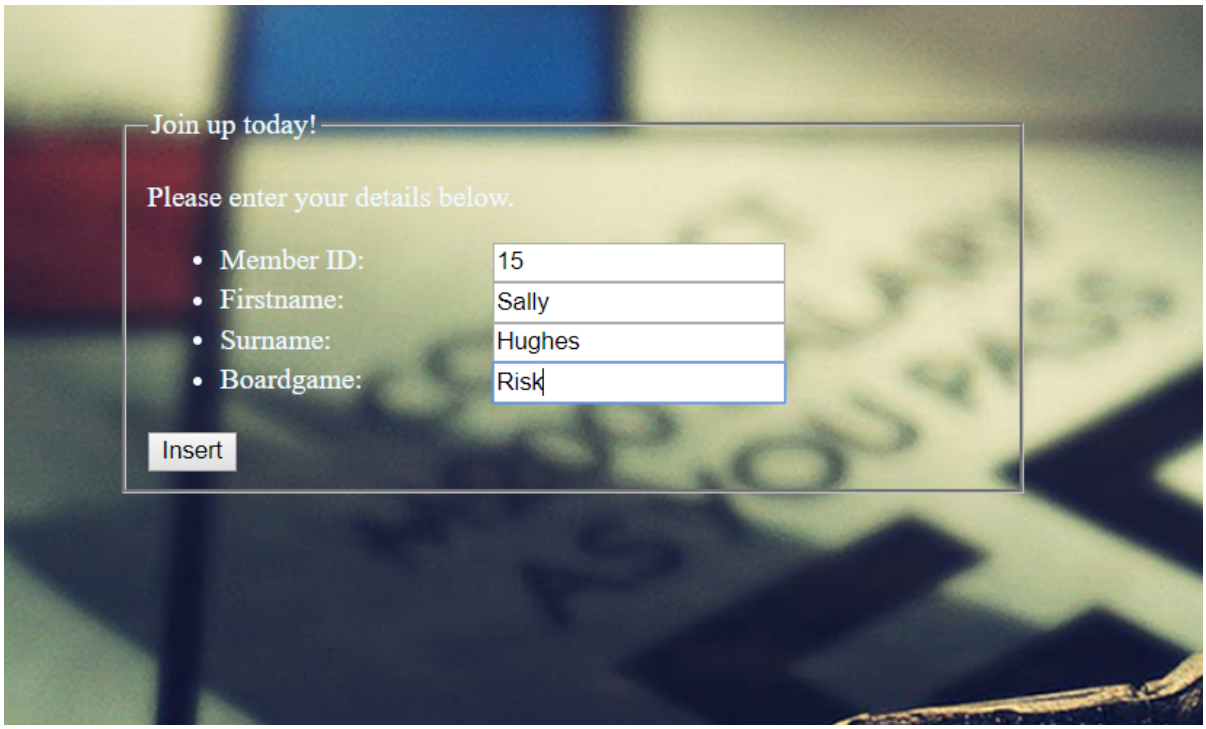
In regards to the player and the board games you will need to edit the *board_games* table. You will have noticed a number of relationships between the tables. For Task 3 we will focus on the relationship between the board games table and the board games assigned to a player. This is the joining table for the player and the board games.

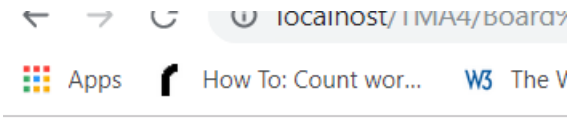
Use the webserver stack from TMA2 to facilitate the next steps.

Please note: full CRUD form are located in the .zip file. I will illustrate them working for one of the new tables and also for the new web form developed for the joining table.

The scoring table.

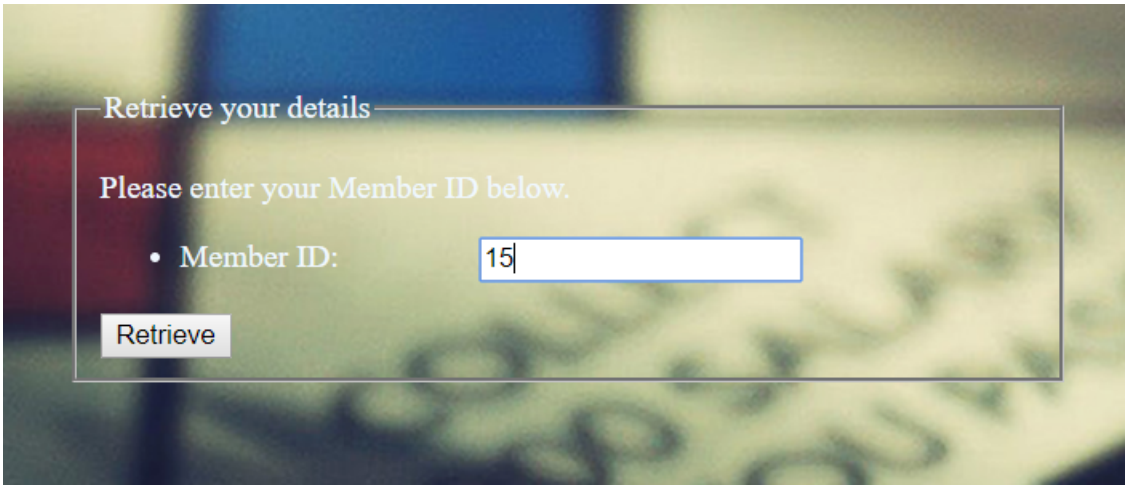
Create a record:





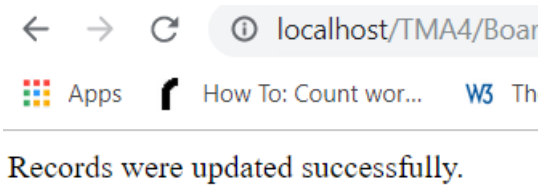
Records inserted successfully.

Retrieve a record:

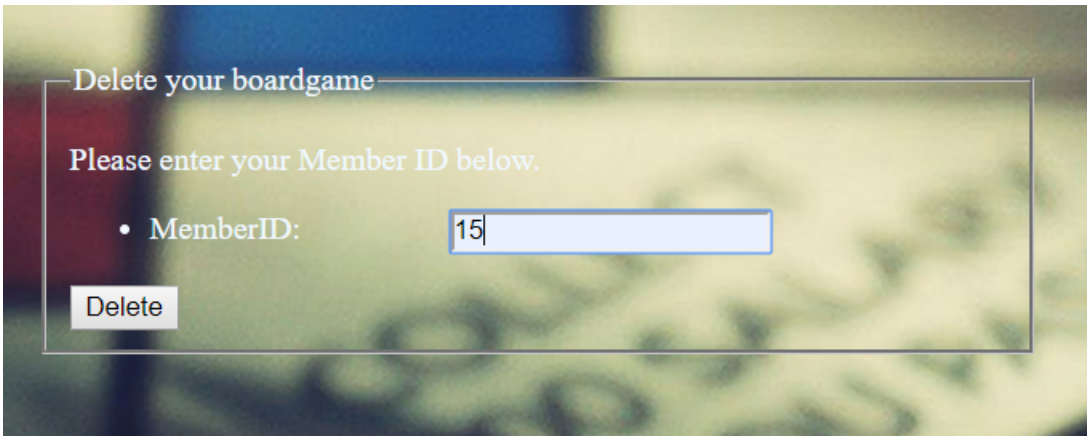


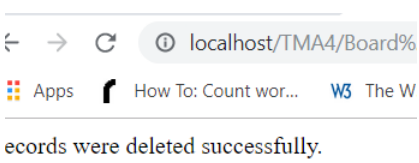
firstname	surname	boardgame
Sally	Hughes	Risk

Update your records:

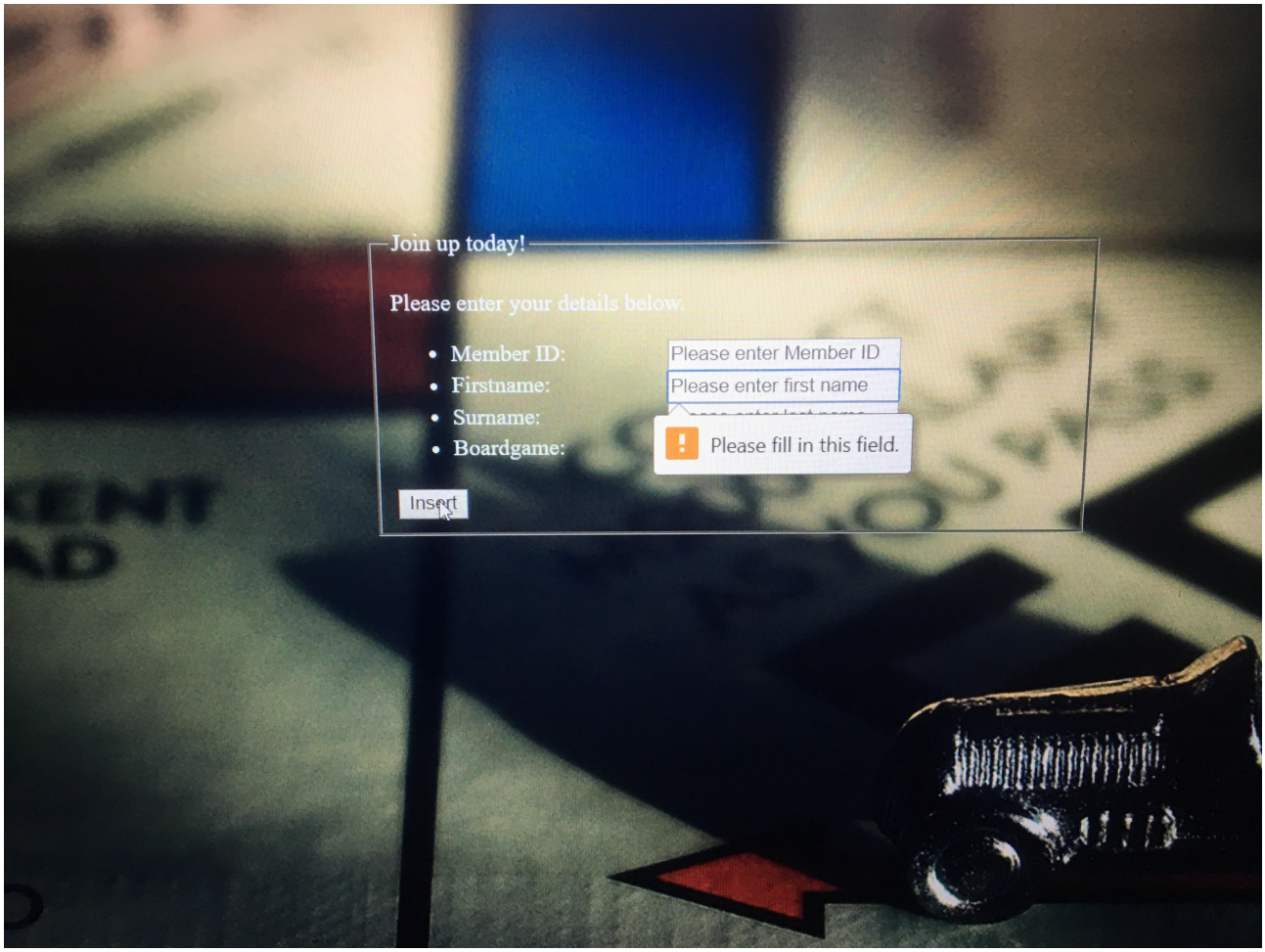


Delete records:





Example of Client side validation in HTML5.



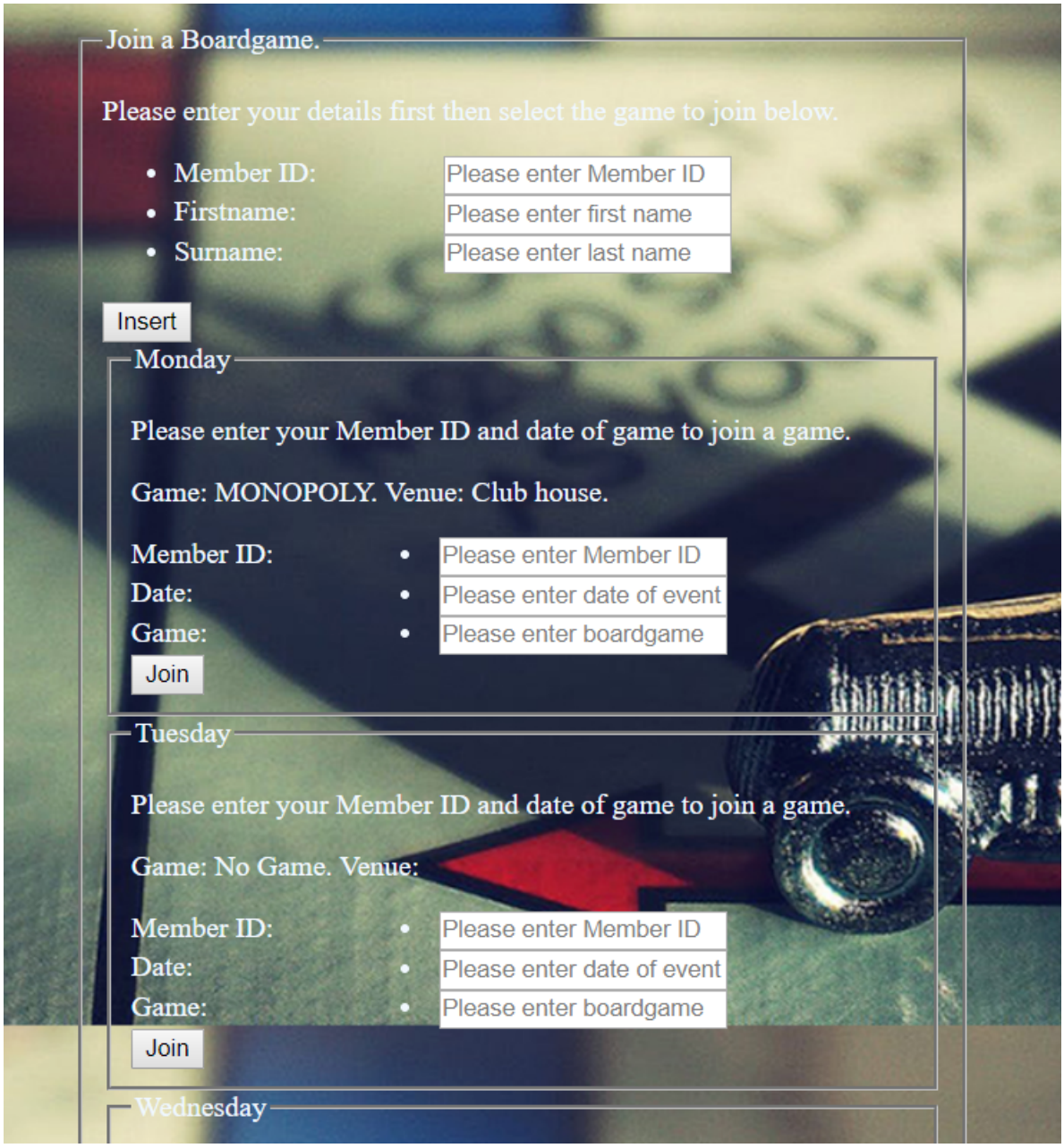
Server side validation example:

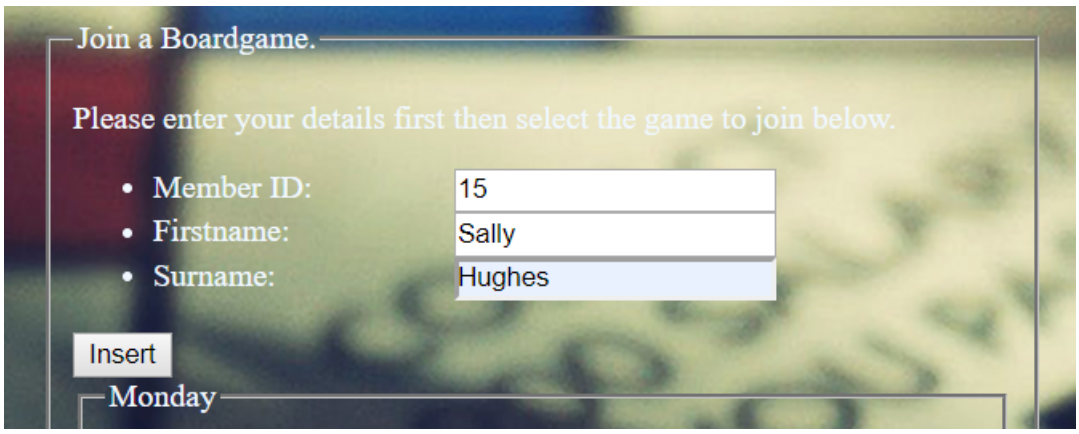
```
/*Form validation. */
if(isset($_POST['MemberID'])){
$MemberID = $_POST['MemberID'];
}else{
    echo "Member ID field is missing";
}
if(isset($_POST['firstname'])){
$firstname = $_POST['firstname'];
}else{
    echo "Fistname field is missing";
}
if(isset($_POST['surname'])){
$surname = $_POST['surname'];
}else{
    echo "Surname field is missing";
}
if(isset($_POST['boardgame'])){
$boardgame = $_POST['boardgame'];
}else{
   echo "Boardgame field is missing";
}
```

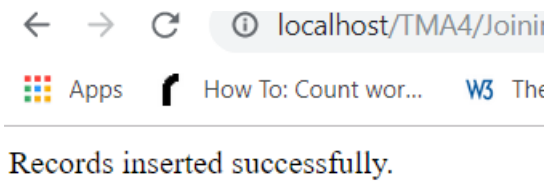
I'll repeat the above presentation for the form I developed for the joining table.

It is worth mentioning that I didn't quite get the form functioning as I would have liked – I struggled with the time constraints. Hopefully the form shows the direction I was going in.

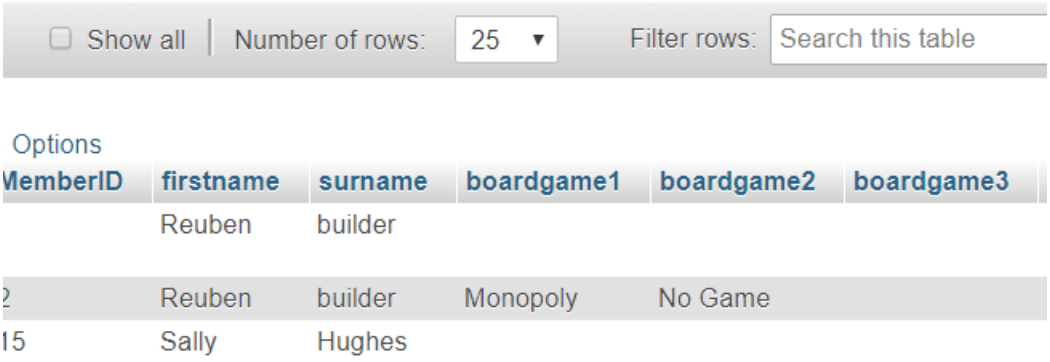
Section of form for joining table:



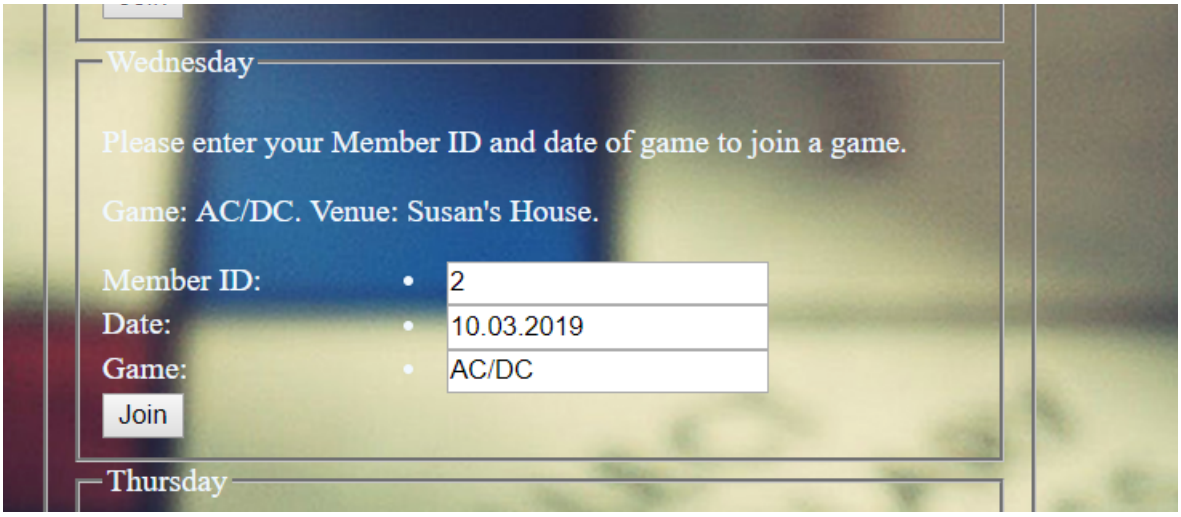


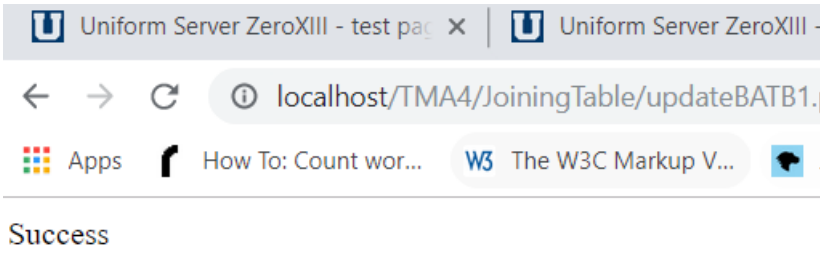


Server table:

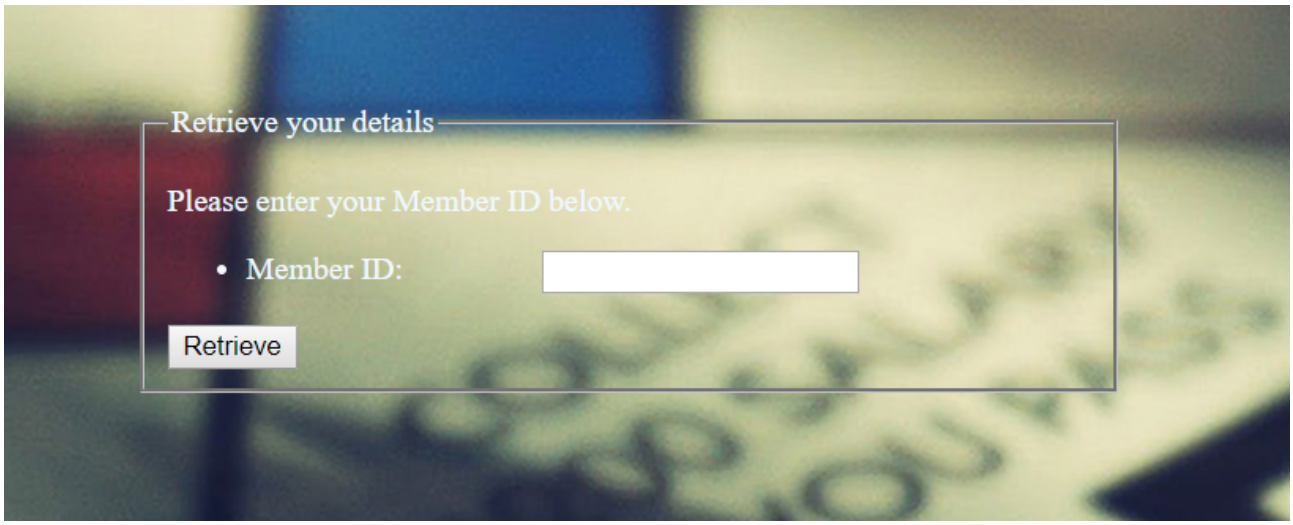


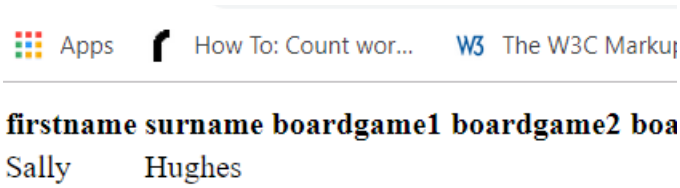
Join a game, using Update php forms.



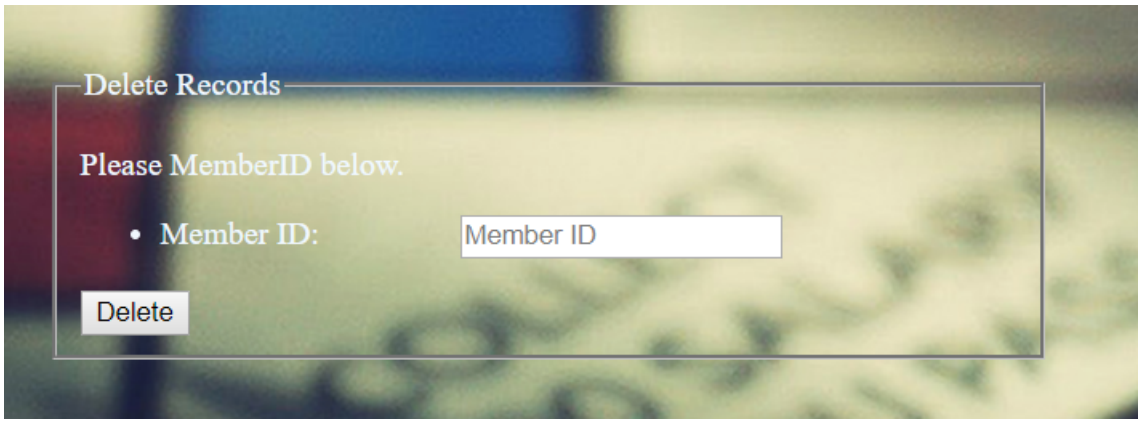


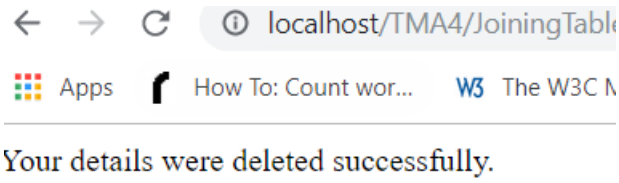
Retrieve data:





Deleting a record:





References

owasp.org (n.d.) *The free and open software security community.* Retrieved from: https://www.owasp.org/index.php/Main_Page (June, 2019.)

Bitbucket.org(2017)*Bitbucket vs GitHub.* Retrieved from: https://bitbucket.org/product/comparison/bitbucket-vs-github (June, 2019).