Revised MizzouCheckout System

University of Missouri

CS3380: Database Applications and Information Systems

Hunter Ginther, Jakob Daugherty, Zach Dolan, Kevin Free, Michael McLaughlin, and Alyssa Nielsen (Team Lead)

13th May 2016

# Introduction

Mizzou Student Unions (“The Client”) has asked us to help rework there current inventory management system to improve usability, and efficiency. Kevin Free has created an inventory page for displaying all of the items. Using radio buttons to filter the inventory. Back end, this utilizes php to run similar queries in a prepared statement format and display the results. One could sort the inventory by damaged, checked in, checked out, and by the different item categories. From this page, you are also able to edit the condition of any particular item. It will take you to the edit page, only accessible by an admin user through the use of sessions, where you can change the condition to any of the options from the item\_condition table. A drop down menu is populated with the values for every condition. Whatever the user selects is then put into the prepared statement and an update query is performed. We decided not to allow the ability to edit critical information about items and other tables because that shouldn’t be necessary once the items are in the system correctly. Kevin also created all the insert functionality. This page has a drop down menu for what table you want to insert a new entry into. Once selected, the insert page includes different php files to allow for each different table to be added to. This operates very similar to Lab 6. The admin user fills out the fields and they are thrust into a prepared statement and run on the SQL server. Proper sessions and https requirements are met on all pages and it should be fairly unbreakable due to the error checking he included. These pages should meet all the requirements for adding, listing, and editing entries in the tables across the database.

Hunter Ginther has designed and created the custom database and handled inventory operations. Including a system of displaying items based on various item attributes. He also created a system of adding, removing, and updating items and desk locations. Allowing for easy and efficient transitions between desired desk locations. Using the entity relationship design given in class, he turned it into a fully operational MySQL database, with flexibility and durability. Using his knowledge of database operations, he was key in producing a viable inventory table. Complete with color codes based on item attributes like availability and overdue. Finally, he helped with traffic flow and page redirection to ease user access to the system.

Zach Dolan started the design of the website from scratch using bootstrap and implemented an easy to use user interface. Tring to keep it pretty similar to the design and functionality of the current system to avoid a learning curve when the new system is implemented. He also created the style.css file for styling the elements and keeping them the same for an even flow across pages. Favoring centered content wrapped in a single div because it provides an easy transition to mobile devices if the client starts to use tablets vs laptops. A few minor changes were to the UI were made from the initial launching point. Additionally, he worked with the authentication system, including limiting the information being displayed to outside users. Creating the log out system, which takes the user to logout.php, ends their session, destroys variables, and redirects them to the home page. Finally, he also saw the need to clean up the shopping cart of the user. Adding more methods of searching for a student including by pawprint, or lastname. He also added an option to search directly for the item itself to see who has the item checked out. The queries are completed using switch statements around which radio is selected, which are a lot cleaner than several if statements. The queries select the student's most relevant information and populate the table along with the id of the item that matches the id of the student.

Jakob Daugherty hosted the project on his virtual machine, wrote the final documentation, and performed database analytics and administration. Adding a GitHub repository to handle version merging and publishing stability, he also created test data for beta testing on site functionality. Additionally, he produced the final report for the project. While also analyzing database normal form, and functionality. Adding indexes and reworking primary key attributes for more efficient database functionality. Finally, he reviewed or revised all queries for accuracy and security. Adding additional search functionality to the item index page.

Alyssa Nielsen (Team lead) coordinated group meetings, submitted group project assignments and information, and kept track of deadlines. She produced the project presentation, finalized the project proposal, and finalized the project documentation. Conducted database planning and composed group ERD ideas into one submittal format. Next, she constructed the application user interface, implementation, revision, organization, and formatting of all page code. Helped with login functionality, checking login credentials and setting secession variables. Finally, she performed most application testing for functionality, debugging, and resolved outstanding issues. While adding new employee registration functionality.

Michael McLaughlin created check in and check out item functionality. Creating a check.php page to check in or out an item with a single button using item and student id values. This page only requires the item id to check that item back in and, if an item is available, only requires the additional student id to check and item out. These values are sent to the database with time stamps to be inserted into the student\_item\_transaction table. He also used the time stamps to allow the system to keep track of overdue items.

# The MIT License(MIT)

This application is licensed under the MIT license, detailed as follows.

Copyright (c) 2016 Hunter Ginther, Jakob Daugherty, Zach Dolan, Kevin Free, Michael McLaughlin, and Alyssa Nielsen

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# ERD



# Queries

All queries used by our system are detailed below. We have provided the SQL syntax and a detailed description of the expected return of all queries.

* SQL (1): SELECT i.id AS `Item ID`, i.name AS `Item Name`,(SELECT sit.student\_id FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Student`,(SELECT sit.employee\_id FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Employee`,available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location`,(SELECT sit.checkout\_window FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Time Due Back`FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND i.location\_id = 1 ORDER BY `Availability`, `Time Due Back` ASC, i.id;
  + Return: All attributes for items located at the Memorial Student Union desk ordered by availability
* SQL (1.1): SELECT i.id AS `Item ID`, i.name AS `Item Name`,(SELECT sit.student\_id FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Student`,(SELECT sit.employee\_id FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Employee`,available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location`,(SELECT sit.checkout\_window FROM student\_item\_transaction AS sit WHERE sit.item\_id = i.id AND sit.transaction\_datetime >= CURDATE() AND sit.transaction\_type = 'Out' AND sit.checkout\_window = (SELECT MAX(sit.checkout\_window) FROM student\_item\_transaction WHERE item\_id = sit.item\_id)) AS `Time Due Back`FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND i.location\_id = 0 ORDER BY `Availability`, `Time Due Back` ASC, i.id;
  + Return: All attributes for items located at the Student Center desk ordered by availability
* SQL (2): SELECT student.name\_first, student.name\_last, student.username, student.email, item.name FROM student inner join item on student.id = item.id where student.id = ?;
  + Return: The first name, last name, username, email, and any items checked out by that student where the student id matches that of the given search term
* SQL (2.1): SELECT student.name\_first, student.name\_last, student.username, student.email, item.name FROM student inner join item on student.id = item.id where student.username = ?;
  + Return: The first name, last name, username, email, and any times checked out by that student where the student username matches that of the given search term
* SQL (2.2): SELECT student.name\_first, student.name\_last, student.username, student.email, item.name FROM student inner join item on student.id = item.id where student.name\_last = ?;
  + Return: The first name, last name, username, email, and any items checked out by that student where the student’s last name matches that of the given search term
* SQL (3.0): INSERT INTO employee (id,username, user\_type, email, salt, hashed\_password, name\_first, name\_last) VALUES (?,?,?,?,?,?,?,?);
  + Return: Inserts a new employee into the employee table
* SQL (4.0): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all items in the inventory
* SQL (4.1): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND i.item\_condition\_id > 2 ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all items in the inventory that are damaged or in unworking condition
* SQL (4.2): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND i.available = 0 ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all items in the inventory that are currently checked out
* SQL (4.3): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND i.available = 1 ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all items in the inventory that are currently available for checkout
* SQL (4.4): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND LOWER(i.name) LIKE LOWER('bike%') ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all bikes in the inventory
* SQL (4.5): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND LOWER(i.name) LIKE LOWER('mac%') ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all Macs in the inventory
* SQL (4.6): SELECT i.id AS `Item ID`, i.name AS `Item Name`, available AS `Availability`, ic.name AS `Item Condition`, l.name AS `Location` FROM item AS i, item\_condition AS ic, location AS l WHERE i.item\_condition\_id = ic.id AND i.location\_id = l.id AND LOWER(i.name) LIKE LOWER('pc%') ORDER BY i.id;
  + Return: The id, name, availability, condition, and location of all PCs in the inventory
* SQL (5.0): INSERT INTO item\_category (id, name, waiver, item\_id) VALUES (?, ?, ?, ?);
  + Return: Creates a new row in the item\_category table
* SQL (6.0): INSERT INTO item\_condition (id, name) VALUES (?, ?);
  + Return: Creates a new row in the item\_condition table
* SQL (7.0): INSERT INTO item (id, name, available, item\_condition\_id, location\_id) VALUES (?, ?, 1, 1, ?);
  + Return: Creates a new row in the item table with a default availability and condition of available and good respectfully
* SQL (8.0): INSERT INTO location (id, name, terminal\_id) VALUES (?, ?, ?);
  + Return: Creates a new desk location in the location table
* SQL (9.0): INSERT INTO waiver (id, name) VALUES (?, ?);
  + Return: Creates a new waiver in the waiver table
* SQL (10.0): SELECT salt, hashed\_password, user\_type FROM employee WHERE username=?;
  + Return: The salt, hashed password, and user type from the employee table where the username matches the given search term
* SQL (11.0): SELECT id, name FROM item\_condition ORDER BY id;
  + Return: The id, and name of all rows in the item\_condition table ordered by id
* SQL (11.1): "UPDATE item SET item\_condition\_id = ' " . $\_POST[ ' Item\_Condition ' ] . " ' WHERE name = ' " . $\_POST[ 'Item\_Name' ] . " ' ";
  + Return: Update the item condition table to the new condition id, given as a post variable, where the item name matches the given post variable.

# Analytics

What sorts of analytics are conducted by your system? Reference the specific queries used to conduct those analytics. How are these analytics useful?

# Normalization

Every table in our database has the characteristics of a 3rd normal form database. Meeting the following requirements: no repeating groups, no non-prime attribute is functionally dependent on a proper subset of any candidate key, and no candidate key contains a transitive dependency. The expired\_waiver and item\_condition\_update tables are in 3rd normal form. This lower normal form allows does not require the use of a Super Key. For the expired\_waiver table, a super key could not be used because the same student may have to sign the same waiver again, if it is expired. So to ensure that we do not have large amounts of duplicate data, the candidate key {student\_id, waiver\_id} has been used. Additionally, the item\_condition\_update table contains time stamped data that may be a duplicate of previous data. For example, throughout its lifetime, a computer my go from good condition to un-working and back again. This made using a super key for the table difficult. With the time stamp element present we have decided to make the candidate key {item\_id, datetime} in order to allow for accurate logging of condition updates. All other tables in our database have been found to be in BCNF.

# Indexing

On our database we have defined quite a few indexes to help with data retrieval, and integrity. We use table id indexes for most personal data and all BCNF tables. Now the indexing for these tables has been defined as the MySQL default because no special indexing was required. Additionally, we have created a unique index on the employee table using the username attribute. This allows for faster login and prevents duplicate username and password combinations. Finally, we have created a auto incrementing index on the student\_item\_transaction table. This auto increment allows for searching of recent transactions fast and easy.

# Security

The Revised MizzouCheckout System application uses several protective security methods, specifically many PHP functions, to prevent SQL injection, Cross-Site Scripting Attacks (XSS) attacks, the use of unsecured HTTP, and other types of attacks. To prevent SQL injection attacks on our site, we used MySQLi prepared statements for any SQL queries we ran, using mysqli\_prepare to link to the database and prepare the SQL query, mysqli\_stmt\_bind\_param to bind the values to the SQL query and create the statement, and mysqli\_stmt\_execute to execute the statements. We also used mysqli\_stmt\_bind\_result and mysqli\_stmt\_fetch when binding the statement to our encrypted data, such as passwords. To prevent XSS attacks, we have used htmlspecialchars on any sensitive user input submitted via forms on our application. We also only store a hashed and salted password in the database, using a random number given via mt\_rand for the salt, and password\_hash for the hashing of the password with PASSWORD\_BCRYPT, which creates a new 60-character password hash using a strong one-way hashing algorithm. We used password\_verify to verify credentials, comparing the user input to the hashed password in the user’s row in the database for login and registration. To be sure that a secure HTTP connection is always being used, we used a redirect at the top of each page to redirect to HTTPS. We also set sessions that are checked on each page the user goes to, so that we will know which user has logged in and used their username and user type as our session variables so that only an admin user has access to the navigation bar buttons for registering a new user and adding items.

# Other Topics

Do you use triggers? Share anything else that needs to be shared with potential users.

# User Manual

## Installation

Step by step, how do you deploy your system. What are the software dependencies (PHP, MySQL, etc..). Do you use any additional libraries (mysqlnd)? How do you install those dependencies? How do you setup the database (Create database, then import using SQL?)? How do you host the website? By reading through this section, I should be able to deploy your system on another server without any issues/questions.

1. Setting up MySQL
   1. Sudo apt-get install mysql-client mysql-server
      1. check that it is working by running ‘man mysql’ from the command line
2. Setting up apache
   1. Sudo apt-get install apache2
      1. Agree or respond with ‘y’ to all question prompts
3. Setting up PHP
   1. Sudo apt-get update
   2. Sudo apt-get install php5
   3. Sudo apt-get install libapache2-mod-php5
   4. Sudo apt0get install php5-mysql
4. Download
   1. Sudo mkdir /var/www/html/<foo>
      1. Where <foo> is the desired directory name
   2. Cd /var/www/html/<foo>
   3. Sudo wget <http://cs3380-jadppf.centralus.cloudapp.azure.com/mucs3380spring2016>
5. Database importation
   1. Next run the MySQL command to run the FinalProject-defs.sql file and import the tables into your database
   2. Then update db.conf to reflect your current database username, password, and database name.
6. Verify
   1. Direct your web browser to the destination folder and your system should display the index.php page, meaning everything is working correctly.

## Website Usage

Create a section for each page in the site. How do you use each page. Include screenshots in each section so there is no confusion. Organize the sections (pages) so that it follows a logical order for using the site. (i.e. Login will likely be the first section). This will be especially important if some pages in your site have dependencies. For example, if one page requires you to select a category from a dropdown menu, the user would likely have been required to create that category using a different webpage first.