## Assignment 1: Specification & Test Plan

| | |
|---|---|
| WEBSITE NAME: | Burger Port |
| PAGE NAME: | /gift_cards.html |
| PAGE AUTHOR (*Dev 1*): | Daniel Guinto |

## *1. PAGE REQUIREMENTS/SPECIFICATIONS*

This page displays 2 forms: one that allows users to purchase a gift card and one that allows users to check gift card balances.

For gift card purchasing, a user must fill out a form requiring an amount ($) being sent, recipient's name, recipient's email, sender's name, delivery date, and an optional custom message. If a user attempts to send the form with an empty field, the field that was missed will turn red and a focus will be put on it, with the exception of the custom message. Regular expression code is used validate input. This ensures the amount being sent is a positive decimal (up to 2 decimal points), the name inputs contain only letters and 1 whitespace (if first and last name are being entered), the email is of expected email format (e.g. johndoe@email.com) and the delivery date is the present date or a future date. If any of the inputs fail validation, the invalid field will turn red and a focus will be put on it. Once all inputs are successfully entered and pass validation, the following message will appear:

> "Thank you *sender's name* for your purchase! A gift card for $*amount sent* will be sent to *recipient's email* on *delivery date* with the following message: *custom message*".

The information entered will also be stored in a database. Additionally, a button will appear that allows the user to reload the page to purchase another gift card. The electronic gift card will be sent automatically to the recipient's email on the delivery date selected for the $ amount entered.

For checking a gift card balance, the user must fill out a form requiring a gift card number and a pin. Similar to the purchasing form, if a user attempts to send the form with an empty field, the field that was missed will turn red and a focus will be put on it. Regular expression code is also used to validate the input. This ensures that the gift card number is exactly 16 digits long with only numbers and the pin is exactly 4 digits long with only numbers. If an input fails validation, the invalid field will turn red, a focus will be put on it, and a message will appear, notifying the user of the required formats for the input. If the gift card number and pin combination do not match a valid active gift card, an error message will notify the user. Once all inputs are successfully entered and pass validation, the following message will appear:

> "Gift Card Number: *gift card number*. Remaining Balance: $**Balance**"

This balance information is retrieved from a database. A button will also appear, allowing the user to reload the page so that they may check the balance of another gift card.

## *2. SECURITY & QUALITY ASSURANCE CONCERNS*

| | |
|---|---|
| Specification Analyst (*Dev 2*): | Jalaluddin Qureshi |

### Overview

My main security and quality assurance concern for this webpage is that the page uses a form, and these are some of the potential security problems which can be encountered.

1. Buffer Overflow – the maximum size of the data that the user can input into each of the fields has not been set. In this case, the user can put large chunk of malicious data, which cause the server to crash.
2. SQL Injection – It is mentioned in the specification that the user's data would be stored in the database. In this case the user can write SQL statement which can be used to gain unauthorized permission status, or gain access to database table information.
3. It should be clarified in the specification that POST method in the form should be used, so that the input field values entered in the forms should not be visible to an intercepting proxy. This is specially important when gift card number and PIN is used in the form.
4. The user can potentially bypass the client side validation by disabling Javascript on the browser. In this case server side validation should also be used.
5. It appears that the gift card and PIN number is communicated using plain-text. In this case this information is vulnerable to be easily read by someone who gets access to this information e.g. through intercepting proxy. This can be resolved by using hashing the PIN number and then storing it in the database.

**References:**

- https://www.w3schools.com/sql/sql_injection.asp
- Stuttard, Dafydd, and Marcus Pinto. *The web application hacker's handbook: Finding and exploiting security flaws*. John Wiley & Sons, 2011.

## Testing Recommendations

The tests that I would run on this webpage would be…

| TYPE OF TEST | OBJECTIVE |
|---|---|
| Static black-box testing | To fully understand the objectives of the specification, and to ensure that none of the requirements in the specification is misunderstood by the developers. |
| Dynamic black-box testing | To evaluate the form submission without any inner knowledge of the code used to built the form. This way we can gain understanding of any potential problem which an actual user can face. |
| Data Testing (Boundary Conditions) | To evaluate whether the form validation fulfills its objective. So for example for the 4 digit PIN number, we would evaluate the PIN input field with 3, 4, and 5 digit numbers using values 999, 1000, 1001, 9998, 9999, 10000. |
| Data Testing (Default, Empty, Blank, Null, Zero) | Evaluate whether the form validation can detect empty form inputs. |
| Test-to-fail (invalid/ garbage values) | To evaluate whether the form admits invalid input e.g. for the 4 digit PIN number, would it be able to detect 4-character long string value. |
| Logic Flow test | Does the form submission process follows the sequence of steps mentioned in the specification (show error messages/ show thank you message) |
| | |

## *3. DEBUGGING THE REQUIREMENTS/SPECIFICATION*

### My concerns regarding the text of the provided requirements/specifications are…

It is mentioned in the specification that the system validates email in the format given as johndoe@email.com. However it is unclear whether valid emails in the following formats (double dots in the email domain name e.g. johndoe@email.co.ca) would pass/ fail the validation.

**Consistency issues:** In the first paragraph it is written, "*an optional custom message*," and then later toward the end of the paragraph it is mentioned, "*Once **all inputs are successfully entered** and pass validation, the following message will appear*". It is unclear from the specification whether there is strict requirement for the user to input the custom message before the user sees the thank you message.

It is unclear from the specification whether a NoSQL or SQL database will be used to store the data in the database. More clarification about which database environment will be used should be provided.

The specification should elaborate who the user is (in terms of access privilege)? Is the user the person sending the gift card, or receiving the gift card.

In the specification it is mentioned, "an error message will notify the user", more elaboration on this should be provided as to what error message would be displayed to the user.

In the displayed messages given in the specification, the difference between name (presumably variable name) which are only underlined, those which are underlined and have a $ sign, and those with only a $ sign at the beginning of the name should be clarified.

It is specified in the specification that the user can not enter his middle name. In this case it is unclear how would it be communicated to the user that middle name is not allowed in the form name input field.