

# Second Iteration Final Report:

## mycheapfriend.com

---

## COMS 4156: Advanced Software Engineering

### Team: CheapSkates

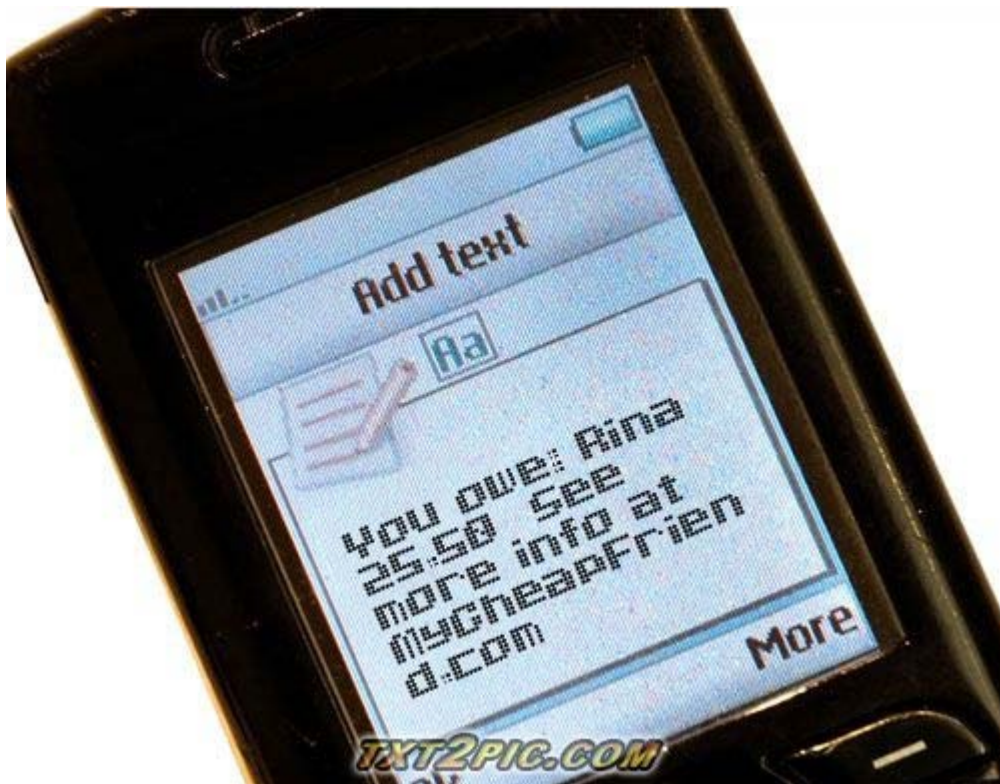
#### Team Members

**Double Trouble:** Waseem Ilahi (wki2001@columbia.edu)

Shaoqing Niu (sn2385@columbia.edu)

**Dynamic Duo:** Michael Glass (mgg2102@columbia.edu)

Huning "David" Dai (hd2210@columbia.edu)



The CheapSkates from MyCheapFriend.com will lend you our Sir, if you give us back feedback soon.

## **Table of Content**

2. Unit Testing and Code Inspection Disposition .....	2
3. Security and Stress Testing .....	3
4. Post Progress Report Defect Log and Disposition .....	4
5. Response to Demo Concerns .....	?
6. Controversies .....	?
7. Revised Schedule (Plan Attached At the End of the Document).....	?

## 2. Unit Testing and Code Inspection disposition

### Non-logic Coding Problems:

#### Controller.java

(MyCheapFriend\MyCheapFriend-ejb\src\java\mycheapfriend\Controller.java)

The following defects were found in the code during the code inspection. The file name is given and the line numbers represent where the defect was in that file. The modified file has different line numbers for similar code, for there have been changes to fix the defects. So the reference is the original file, not the current file that is in the system. The original file has been attached with the submission folder with the name "code\_inspection\_unit\_original.java".

- **Line 155, 157, 173, 184, 382, 404, 414, 490, 510, and 515:** Inconsistency in the use of true and false. Some places we use Boolean.TRUE/FALSE and others we use true/false.
  - Fixed in revision 219, committed 12/02/09 by waseemilahi
  - Everything changed to true/false. No more Boolean.TRUE/FALSE.
- **Line 73:** Very large logic expression. May be confusing to the readers.
  - Fixed in revision 219, committed by waseemilahi
  - A method was created that broke the expression into multiple if's and returned a Boolean value that was assigned to the variable. The method definition is at the line 199.
- **Line 75, 78, 83, 89, 92, 403, and 436:** Comments were placed to the right of the statements rather than above, like in other cases in the source.
  - Fixed in revision 219, committed by waseemilahi
  - The entire inconsistent comment placement was removed and the comments were moved above each statement they document.
- **Line 612:** Left over TODO comment from earlier development.
  - Fixed in revision 219, committed by waseemilahi
  - The comment was removed.
- **Line 62 – 145:** The main method is a bunch of if – else and switch statements. TA suggested encapsulating this further by dividing those functionalities (Switch's) into separate function calls, to avoid confusion.
  - Fixed in revision 219, committed by waseemilahi
  - Multiple methods were created, each handling a subset of features. The handle method calls these methods in succession. And the appropriate method handles the task, if it can't/doesn't the handle moves on to the next call. Thus, the control flows through the code.

## Logic Errors (bugs)

EmailInfo.java

(MyCheapFriend\MyCheapFriend-ejb\src\java\mycheapfriend\EmailInfo.java)

- Error type on success wasn't always set to "no error". Fixed on revision 237.
- Didn't catch invalid boundary case "me 6462294050 bob" Fixed on rev 237.

All the problems found in code inspection and the unit testing, were fixed before the submission of second iteration progress report. After the report, no new errors were found in these two cases.

## 3. Security and Stress testing:

Our user interface is relatively simple, so testing each aspect of it doesn't need to be too complicated. We will split the attack into attacks on each of the interfaces.

### The Web UI:

The web UI is an administrator interface, where administrators should have "root" access once they are authenticated. Here is our attack plan for the relatively simple Web UI.

#### 1. Going through the security

Try the overflowing the fields in the web form.

The attack: We sent requests with really looooooong username and password (1000/10000/100000 characters), and almost broke Internet Explorer. However, since we used try-catch to validate the inputs get posted, our system didn't crash.

#### 2. Going around the security

Try accessing administrator URLs without logging in.

The attack: We tried to get into the administrator interface by accessing its URL and skipping the login authentication. We put "localhost:8080/MyCheapfriend-war/Administrator" in the address field and succeeded to gain "root" privilege without providing proper login information. This defect is named as "**Vulnerability 1**".

#### 3. Accessibility attack.

If we break into the system, the root user's index page is heavy weight, as it lists all database elements. Repeatedly requesting this page (assuming A) the database is thoroughly populated and B) we have access to the page) would be a way

of attacking the system's accessibility. That being said, once a root user has been compromised, they could simply turn off the system, so it's probably not worth exploring this attack.

The attack: Since we could easily go around the authentication, we were able to stop the service in the roles of malicious users.

### **The Text UI:**

The Text UI receives emails from text messages and parses them into logical system objects. Given the:

1. Going through the security  
Try impersonating phone numbers with phone-number like email addresses from other hosts (impersonating SMS). ie 6462294050@gmail.com, or sending an email from our own smtp server impersonating vtext.com or att.com.

The attack:

2. Accessibility attack:  
Sending emails with large attachments, or very large message bodies might slow down our e-mail fetcher's speed of retrieving new messages.

The attack: We sent text messages and emails (Since Vulnerability 2 is not fixed) to our server trying to slow our system. It took the server five minutes on average processing a message/email with a 5 MB attachment. This is recorded as **“Vulnerability 3”**

### **Stress Testing:**

## **4. Post Progress Report Defect log and disposition**

## **5. Response to Demo Concerns**

.....

## **6. Controversies**

There are no controversies among the team at this point.

## **7. Schedule**

Due to the concern about tea assignments, from the TA, we have attached the revised schedule at the end of this document.

