User Documentation

Home Page:

Users will first see the title of the page, “FastTrack” with a little description below. The “Find Out More” button below will take users to the “About Us” section of the page, which provides a brief description about FastTrack delivery services. Users will then see two columns, Customers and Couriers. In the Customers column, there are two buttons, “Search for Jobs” and “Post a Job”. In the Couriers column, there are two buttons, “Search for Trips” and “Post a Trips”. Each of the buttons will link to their pages respectively. Below that, there are two buttons, “Sign Up!” and “Log in” in the blue bar. Users will be taken to the sign up and login pages respectively by clicking on them.

When a user is logged into his/her account, there will be a greeting “Welcome, [username].” in the blue bar, and 3 buttons below: Profile, Log Out or Sign Up! The “Profile” button will redirect you to the user profile page; “Log Out” to the log out page; “Sign Up” to the create account page.

Create Account Page:

When users click on the “Sign Up!” button on the home page, they will be redirected to this page. “Create an Account” button will take users to the “Create an Account” section of the page, which allows users to fill up their details, such as username, password, first name, last name, and e-mail address, which are needed for registration purposes. Users will click on the “Register” button to proceed on, or the “Back” button to return to the home page.

Registration Success Page:

Users will be redirected to this page, once registration is complete. A message saying “Registration Successful!” will be shown on the page, and users will be asked to log in again with their newly created accounts.

Login Page:

Users will fill in their usernames and passwords here, and click on the “Log In” button to sign into their accounts. Also, they have the option of signing in with their Facebook or Google accounts by clicking on the “Log in with Google” or “Log in with Facebook” links. Above those links is the “Forgot your password?” link in which users will be redirected to a new page to reset their password.

Forgot Password Page:

The “Forgot your password?” link in the login page redirects users to this page, where users will be asked to key in their e-mail address registered with their account. Clicking on the “Reset Password” button will send an e-mail containing the password reset link to the e-mail address provided by the user.

Change Password Page:

The password-reset link will redirect users to this page where users are asked to enter their new password twice, the second time for verification purposes. The “Change my password” button will update the user’s password and redirect the user to another page, which lets the user know that password change has been completed.

Logged In Page:

Once a user has successfully logged in from the log in page, they will be linked to this page, that contains a greeting, “Hello, (username).”, and 3 links below, one to return to the homepage, the other to log out, and the last one where users are able to edit their profile.

User Profile Page:

Users are redirected to this page, when they click on the “Profile” button on the homepage. Users will first see the same background as the homepage, but with a different button “User Profile”, which takes them to the User Profile section. Here, all the user information including, username, first name, last name and e-mail address are displayed. Users are able to edit their information by clicking the “Update Profile” button below, and they will be redirected to an edit profile page. The “Back” button returns them to the homepage.

Edit Profile Page:

Here, users are able to edit their profile such as their first name, last name, and e-mail address. The “Update” button updates the user profile, and the “Back” button returns them to the user profile page.

Search for Jobs Page:

The “Search for Jobs” button in the home page will redirect users to this page. Users (customers) are able to filter their search by keying in the start and end destinations, and their before and after dates. The “Search” button will bring them to the search results page, and the “Back” button returns them to the homepage.

Search Results Page:

Here, there will be a list of job/trip listings posted by customers or couriers depending whether the user is searching for a job or trip. Users can click on any of them for more information, which will bring them to the customer or courier listing details page.

Customer Listing Details Page:

The details about the customer listing are provided in this page, including his/her contact info. Users should click on the e-mail address provided to send them an e-mail. If there is a recommendation, it will be listed below the customer details, otherwise it will say “No recommendations”. The “Back” button returns them to the search results page.

Search for Trips Page:

The “Search for Trips” button in the home page will redirect users to this page. Users (couriers) are able to filter their search by keying in the start and end destinations, and their before and after dates. The “Search” button will bring them to the search results page, and the “Back” button returns them to the homepage.

Courier Listing Details Page:

The details about the customer listing are provided in this page, including his/her contact info. Users should click on the e-mail address provided to send them an e-mail. If there is a recommendation, it will be listed below the customer details, otherwise it will say “No recommendations”. The “Back” button returns them to the search results page.

Security Vulnerabilities

SQL injection is a common exploit in which an attacker alters web page parameters to inject SQL code directly in a database. By typing in certain SQL commands into input boxes, an attacker can gain access to protected information from the database. The most vulnerable applications use raw SQL to modify data from the model to database. Our project uses Django’s built in Object relational mapping to map data from the model to the database. Django’s ORM automatically uses automatically escapes all special SQL parameters according to quoting conventions of the database we are using. Thus malicious code will be parsed into harmless statements. We tested it by trying to inject SQL to delete database entries. “SELECT \* FROM user WHERE username = ''; DELETE FROM user WHERE 'a' = 'a';” was injected into several text input boxes across the website and the database remained secure after every input.

Cross Site Scripting is a technique that allows an attacker to insert HTML code into a web page, usually in the form of <script> tag. It can used to steal cookie and session information. Our project uses Django template rendering system to automatically escape all variable values. Our web site was tested by injecting the script “<script>alert('hello')</script>” into various text boxes across the website. On a vulnerable page, the script will cause a pop up with the message ‘hello’ on it. None of the tested pages were vunerable