



Methods

In the previous chapter, we talked about the first of two major security issues that are included with every Meteor project by default. That issue was the ability for users to navigate through all of the data inside the database until we removed the autopublish package. Based on the changes we made, though, users now only have access to the data that belongs to them.

To demonstrate the second major security issue, enter the following statement into the console:

```
PlayersList.insert({name: 'test'});
```

We've made it so users can't navigate through the project's data, but users can still freely insert data into the database by using the console. This means **any user** could fill the database with any sort of unwanted data. Users also have the ability to modify and remove data from the database so by default, they basically have complete administrative permissions. This functionality is contained in a package named Insecure, and while it's convenient during development, it's something we need to turn off before we share the application with the world.

To remove this package from the project run the following command

```
meteor remove insecure
```

Then, once the package is removed, switch back to the browser and try playing around with the application. You'll notice that the `insert`, `update`, and `remove` functions have stopped working from inside the console and inside the interface. This means the application is a lot more secure. But we'll need to make some changes to get the interface working again while still preventing users from manipulating the database through the console.