

Framework: Laravel

Database used: mysql

Development environment: Homestead

The application is a simple book store.

Functionality from the users point of view:

Admin

- Can promote other users to admins and remove own role as admin
- Can restrict any user logging in the application (cannot delete users)
- Can add books. Can add and delete book instances.

Admin / Basic user (logged in user)

- Can search books and add book instances to cart and "buy" them
- Can update his own information (name and email)
- Can review his own purchases
- Can restrict his own access to application (some admin can then cancel this)

Unregistered user

- Can only search books

CRUD: Application have all these functionalities

MVC: Laravel application's structure follows MVC

Application is safe:

CSRF : Application has forms that takes care of this automatically (laravelcollective/html)

Application has also forms that are basic HTML forms. {{ csrf-field() }} is added to these.

SQL-injections: Laravel uses PDO so SQL-injections are handled automatically

XSS: eg. htmlspecialchars(\$request->input('name'), ENT_QUOTES, "utf-8");

Validation:

eg.

```
$this->validate($request, [  
'name' => 'required|string|max:255',  
'email' => 'required|string|email|max:255',  
]);
```

HTML-verbs (GET, POST and PUT) are are used correctly

Status codes: Application generates status code 401 unauthorized if no admin tries to open admin panel

Template engine: Blade

Running the application

1. check Laravel .env for database connection information
2. php artisan migrate
3. php artisan db:seed

Admin:

email: a@a.a

password: admin