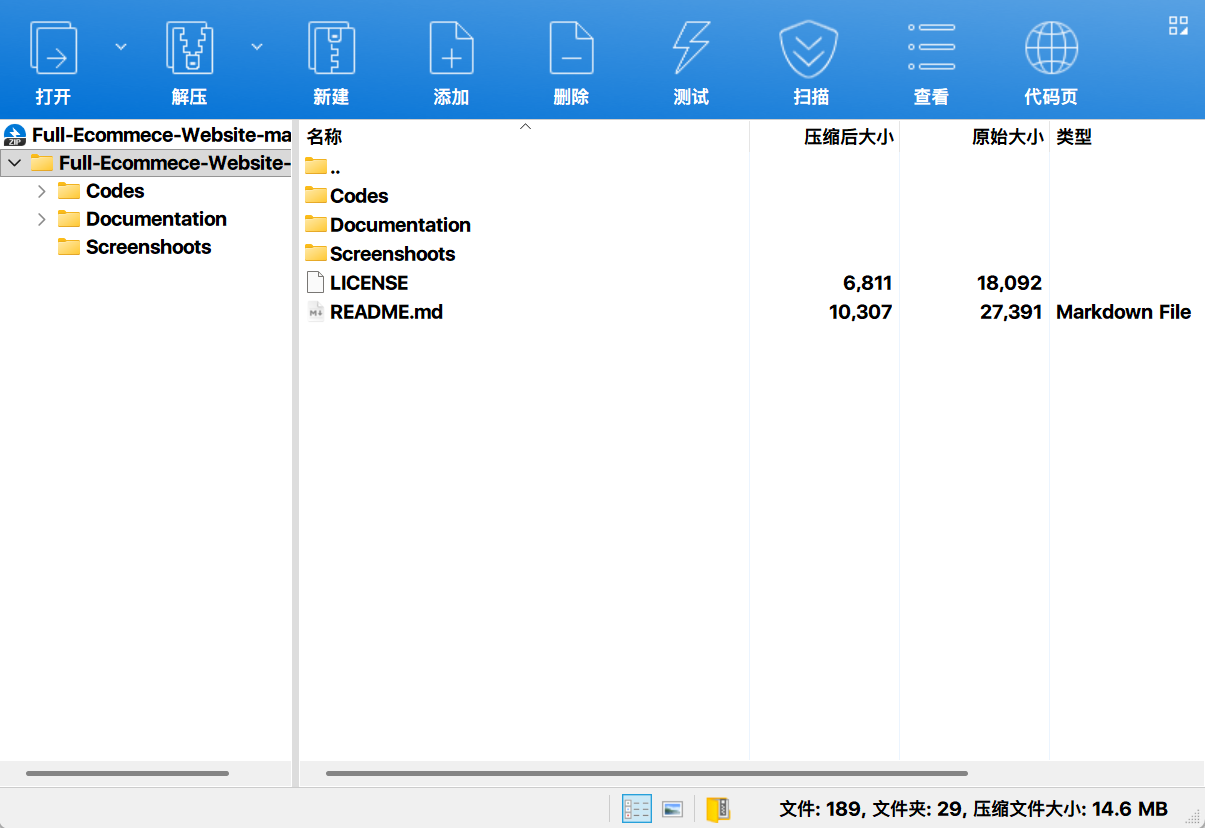
Project address：<https://github.com/ashymuzuro/Full-Ecommece-Website>

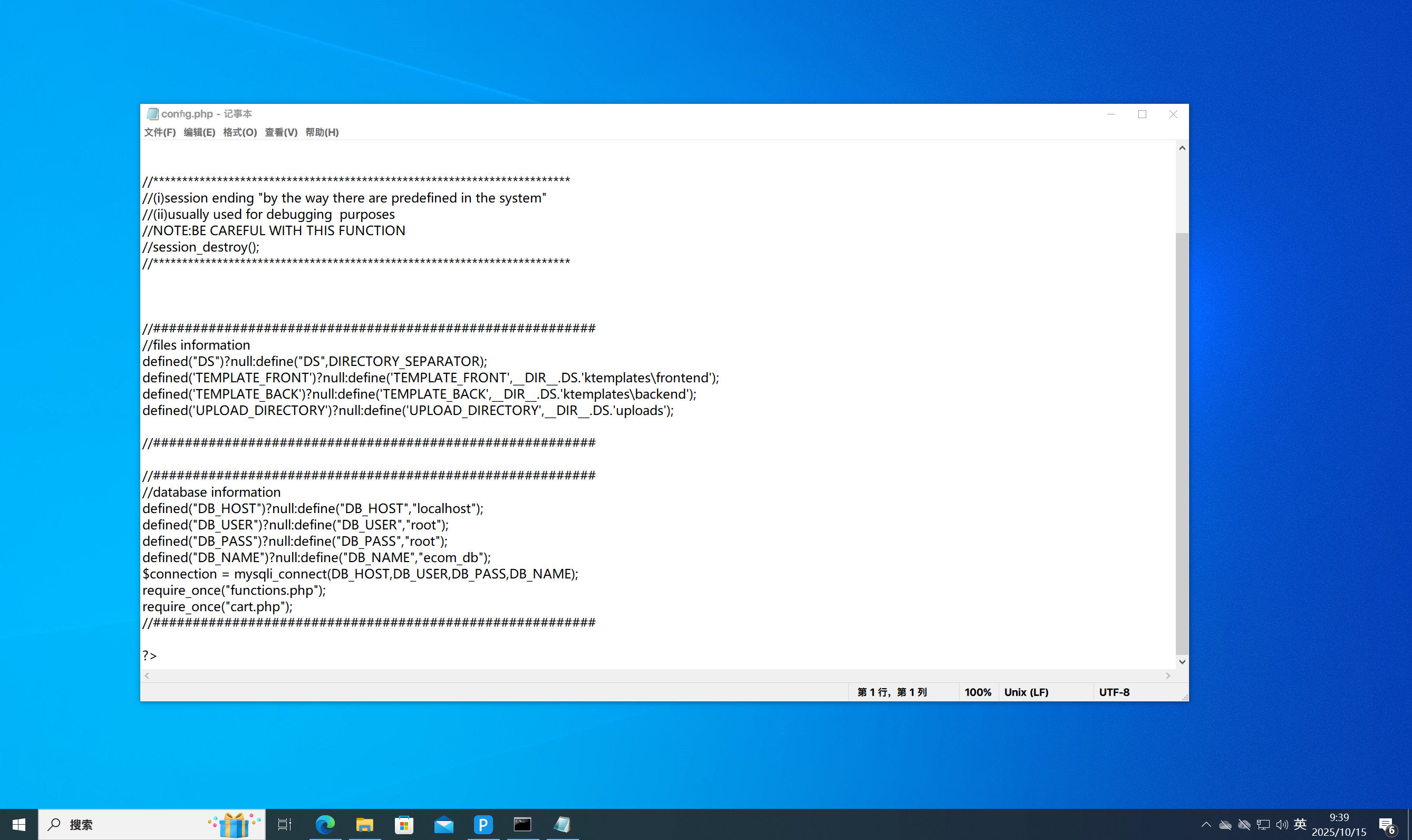
After downloading the project locally, there are the following files:



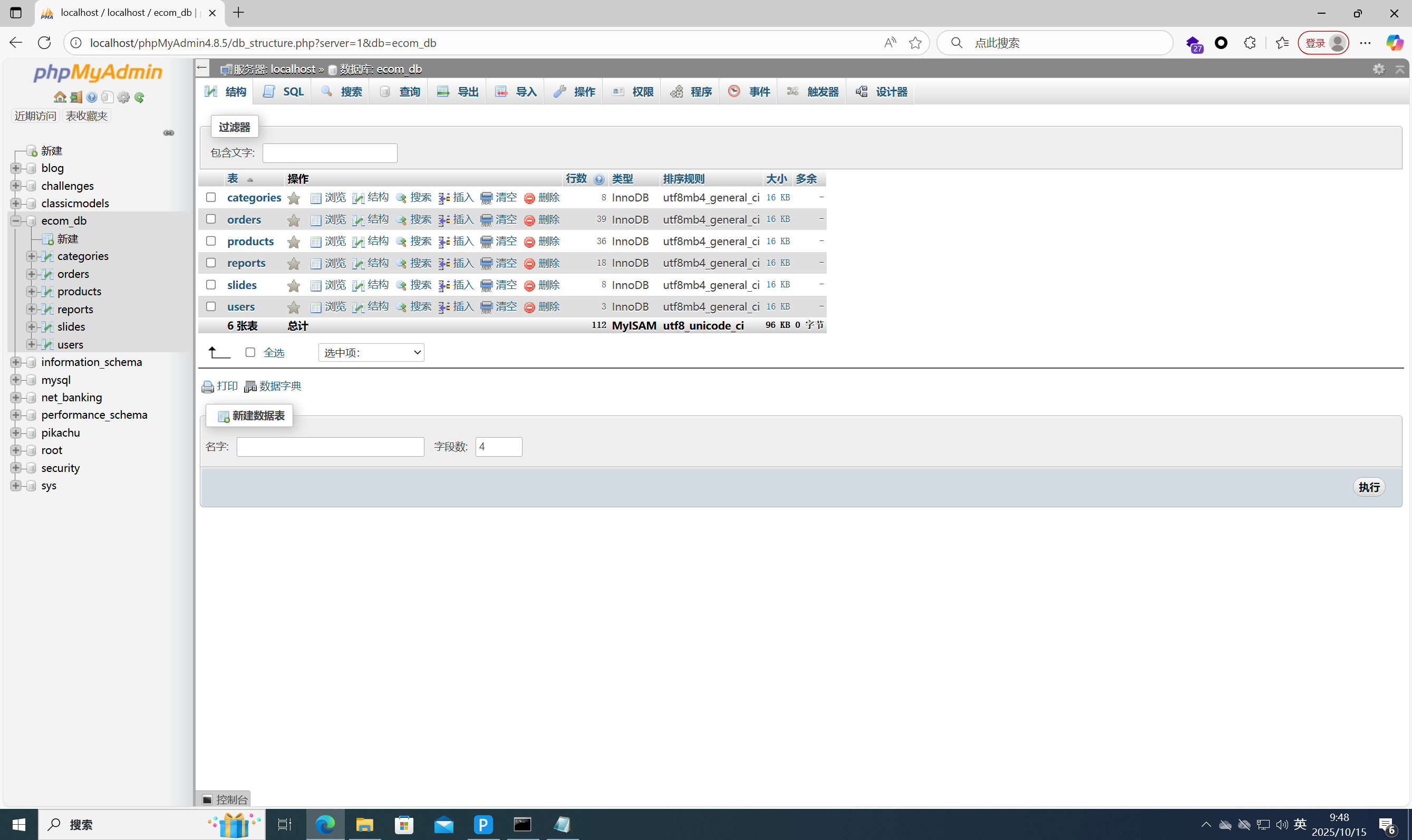
The Codes folder contains the following:



When deploying a project, you only need to modify the contents of the Codes folder:

Modify Codes\kresources\config.php and change the database configuration information 

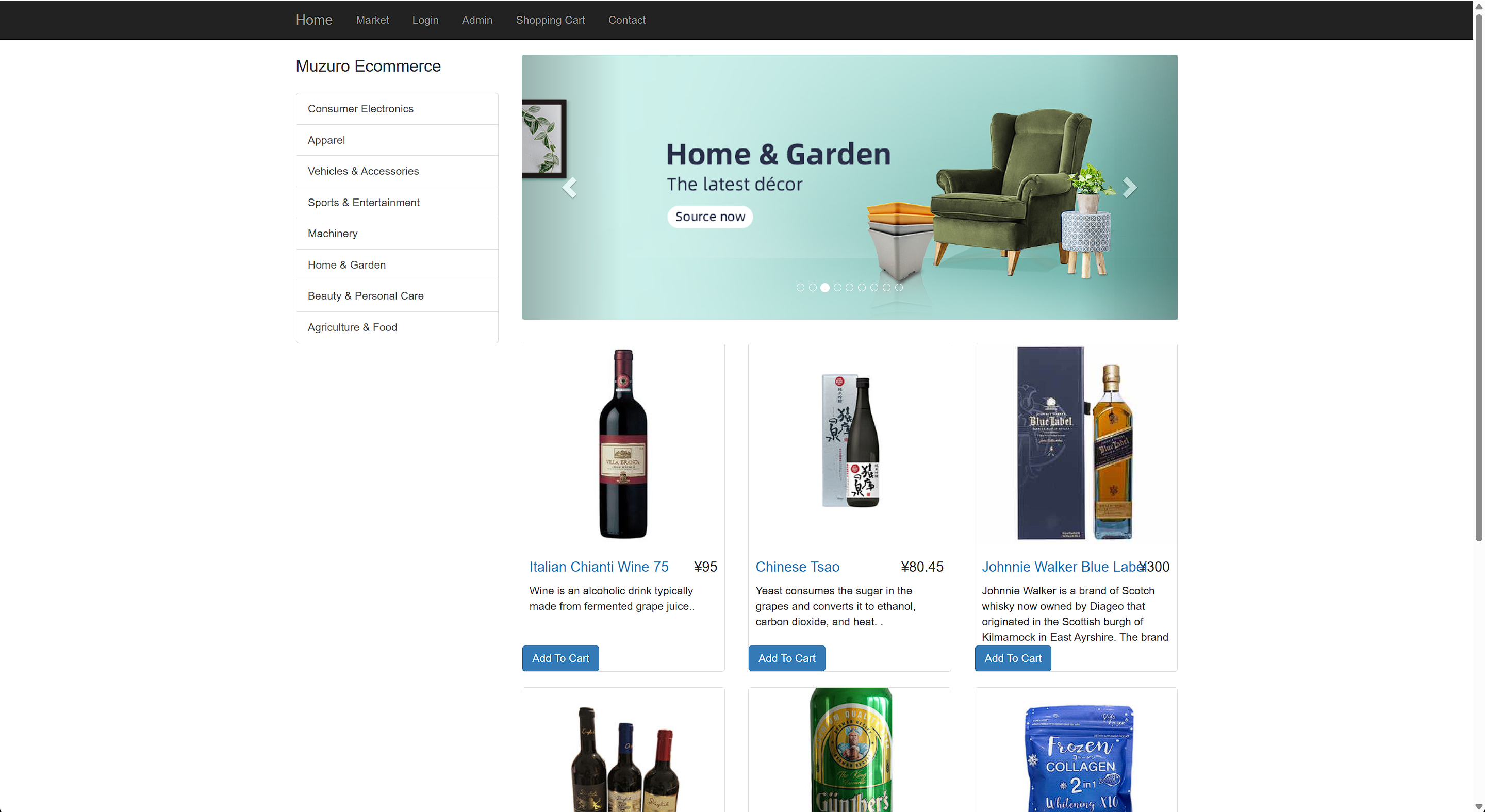
Create a database named ecom\_db and import the Codes/ecom\_db.sql file to the database you just created



Put the Codes folder directly under the root of the server  
my ip is 192.168.88.149

Acess:<http://192.168.88.149/Codes/public/>

Go to the homepage of the website

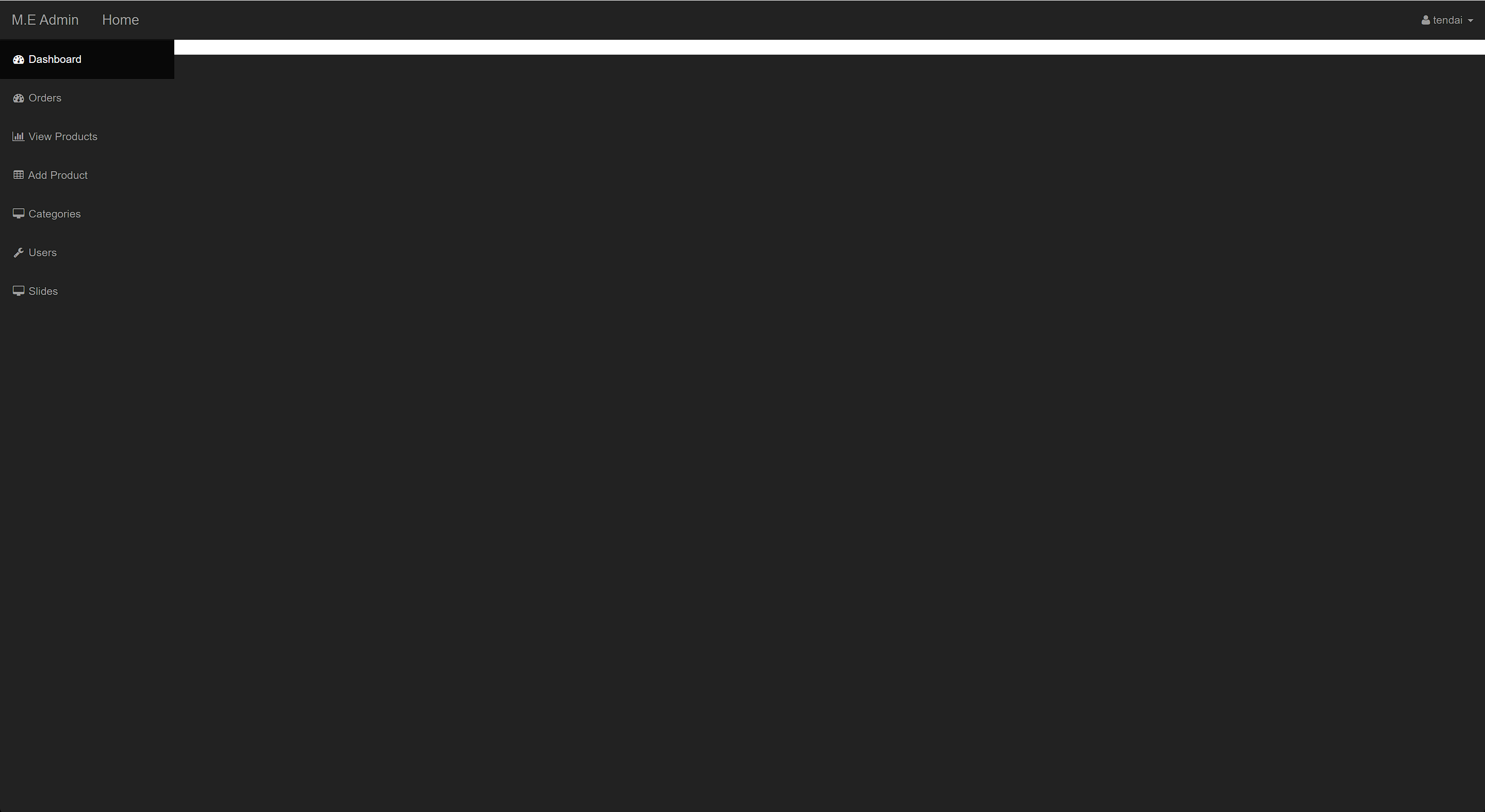


Click **Login** above

Log in with the following account and password:

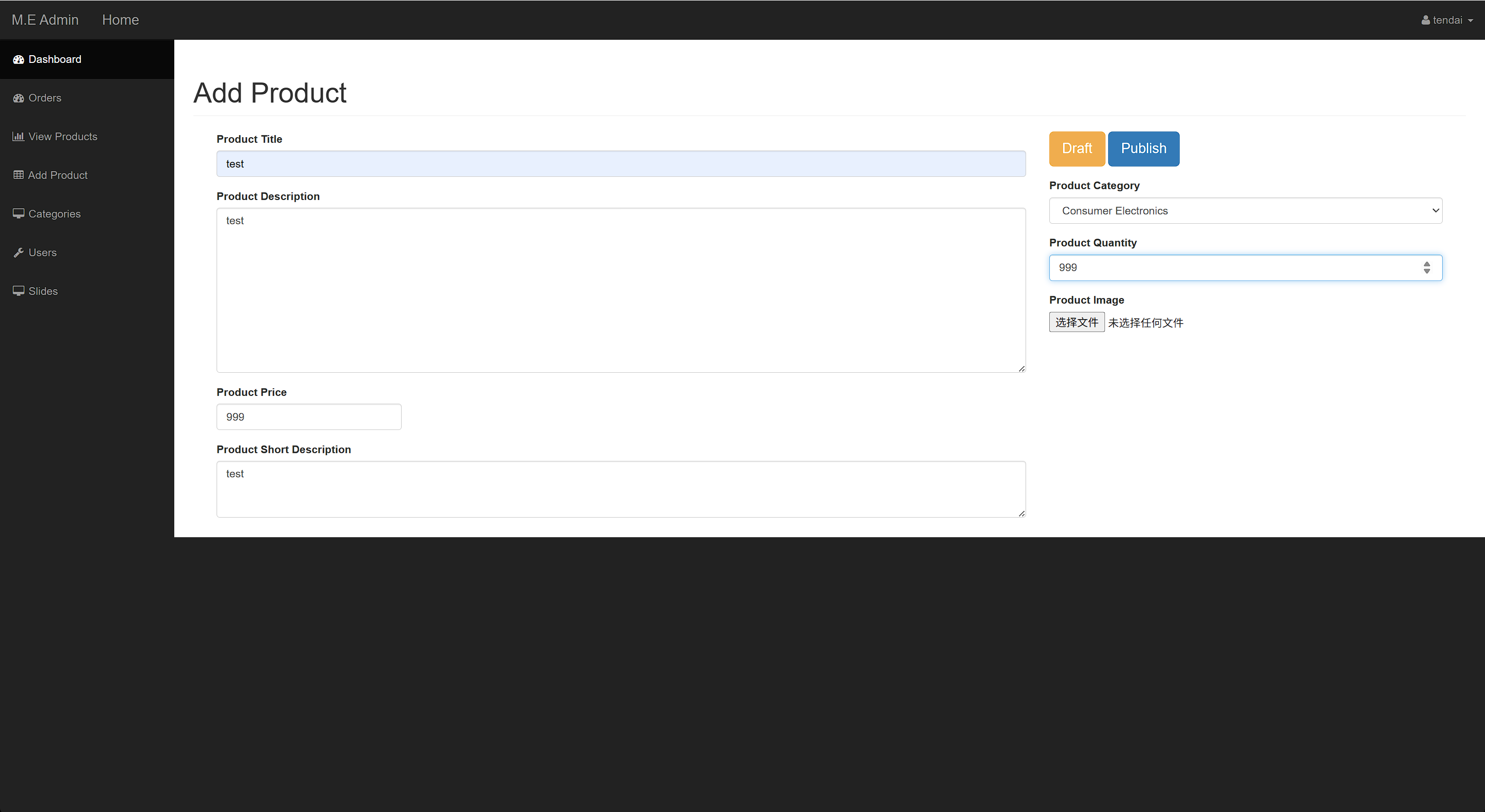
Username：tendai

Passcode: 1234

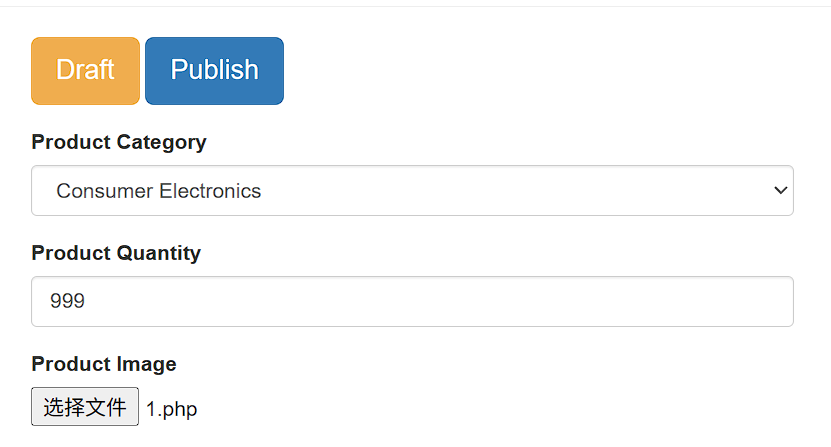


At this point, enter the admin background

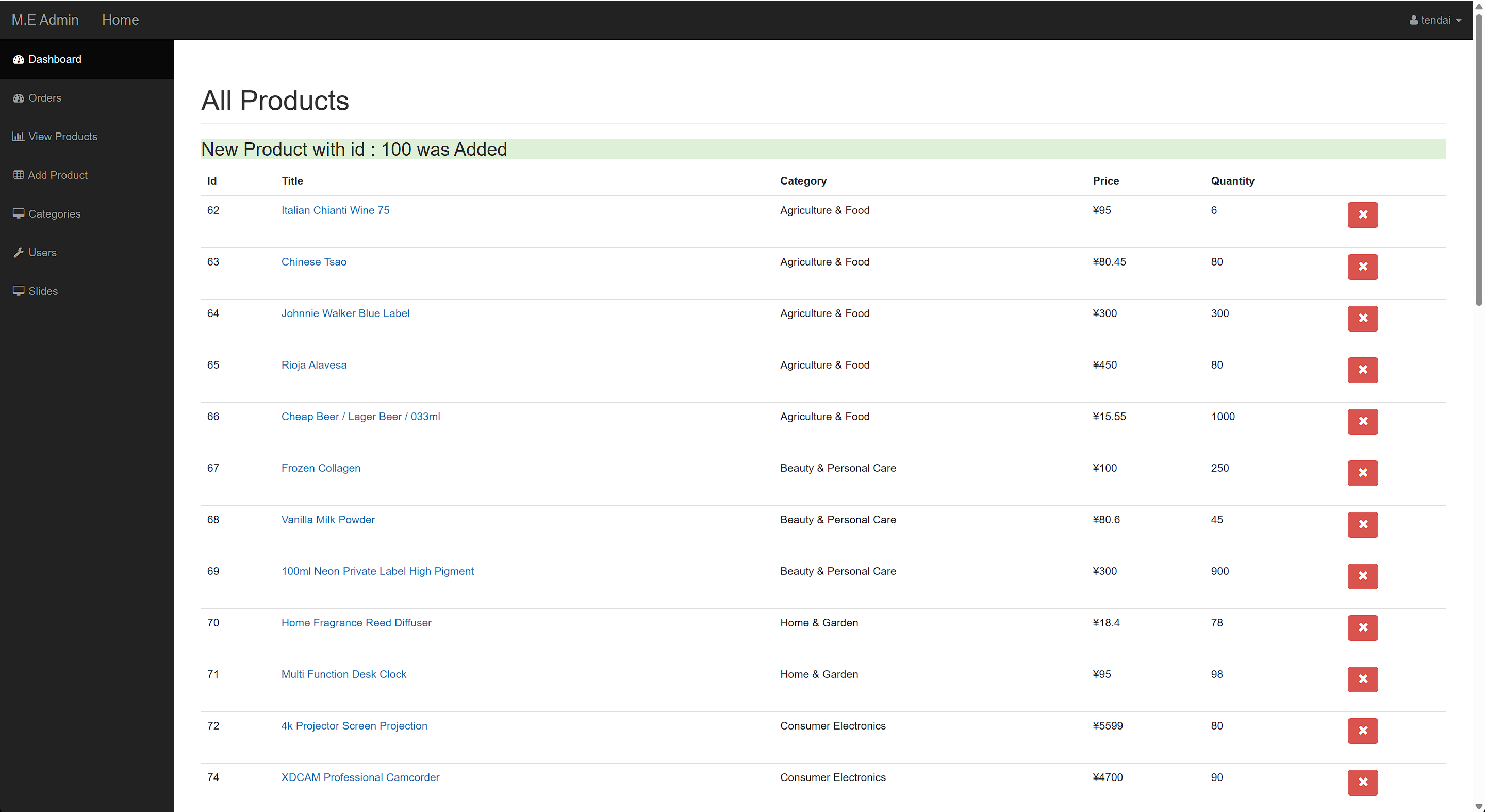
Next visit: <http://192.168.88.149/Codes/public/admin/index.php?add_product>



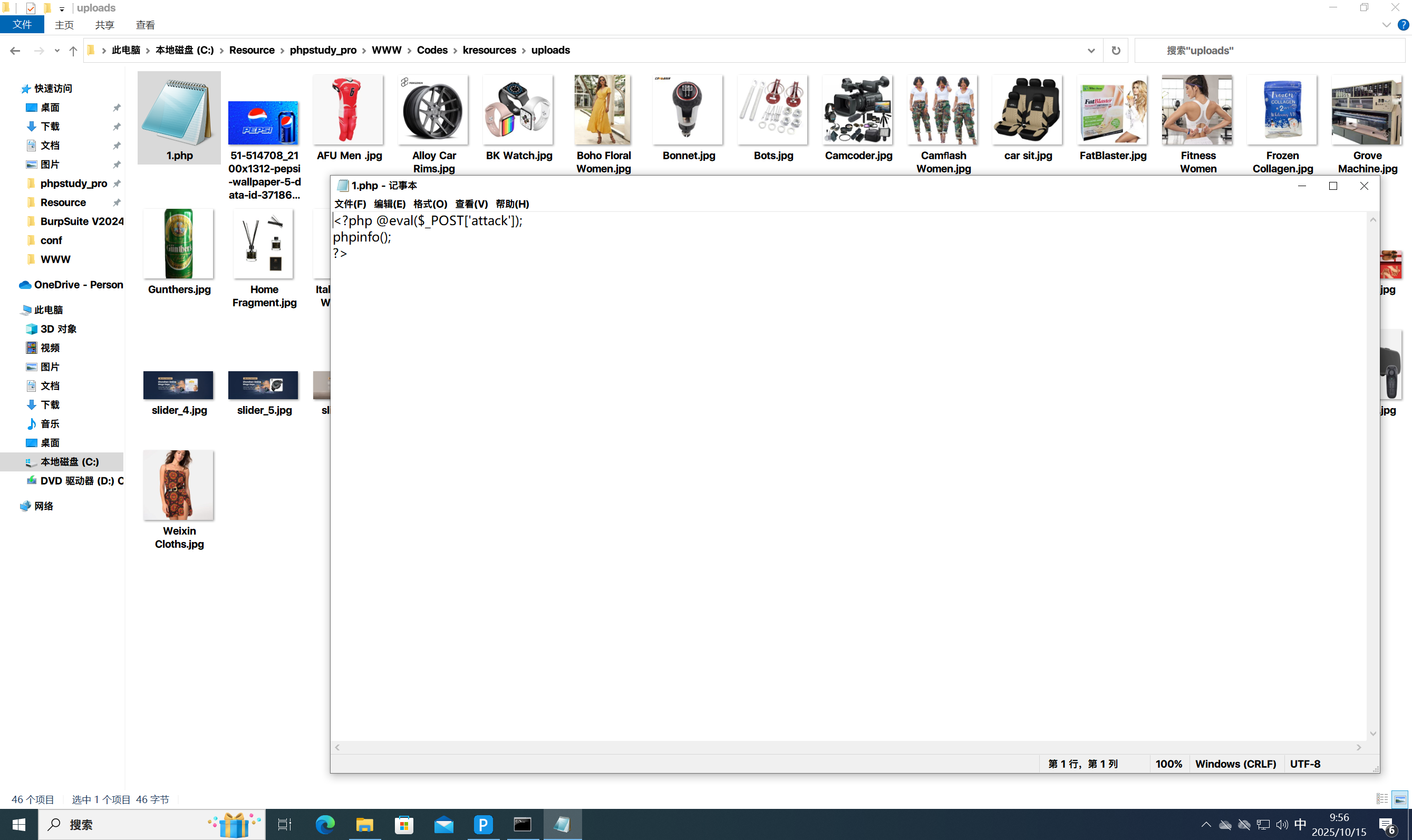
After filling in some necessary information, upload a php one-sentence Trojan



Click **Publish** above



Shows that the upload was successful



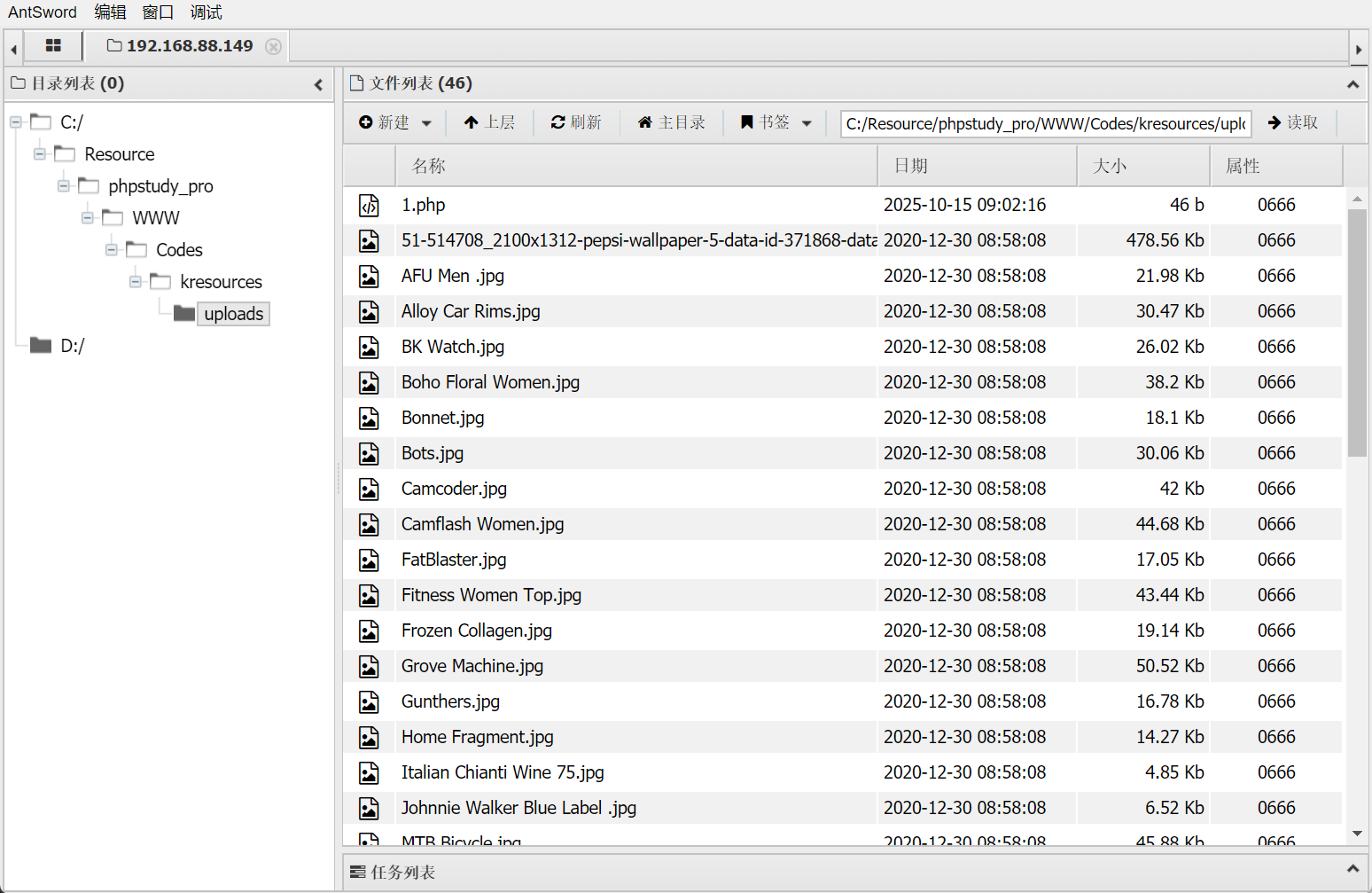
You can see that the Trojan file has been successfully uploaded

Next visit: <http://192.168.88.149/Codes/kresources/uploads/1.php>



php files run successfully.

Open **AntSword** and connect to the server host



The project has a file upload vulnerability