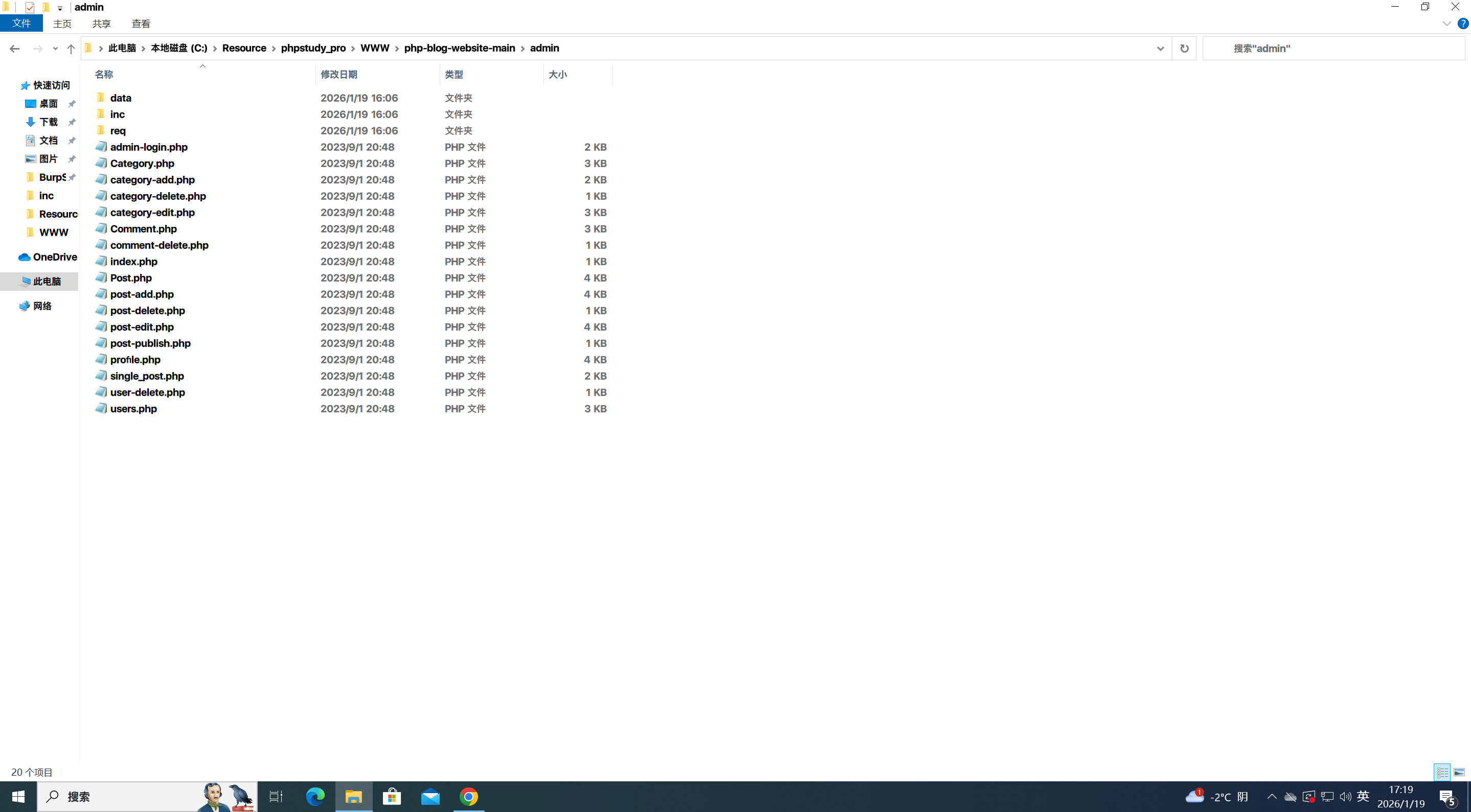
Project URL: <https://github.com/codingWithElias/php-blog-website>

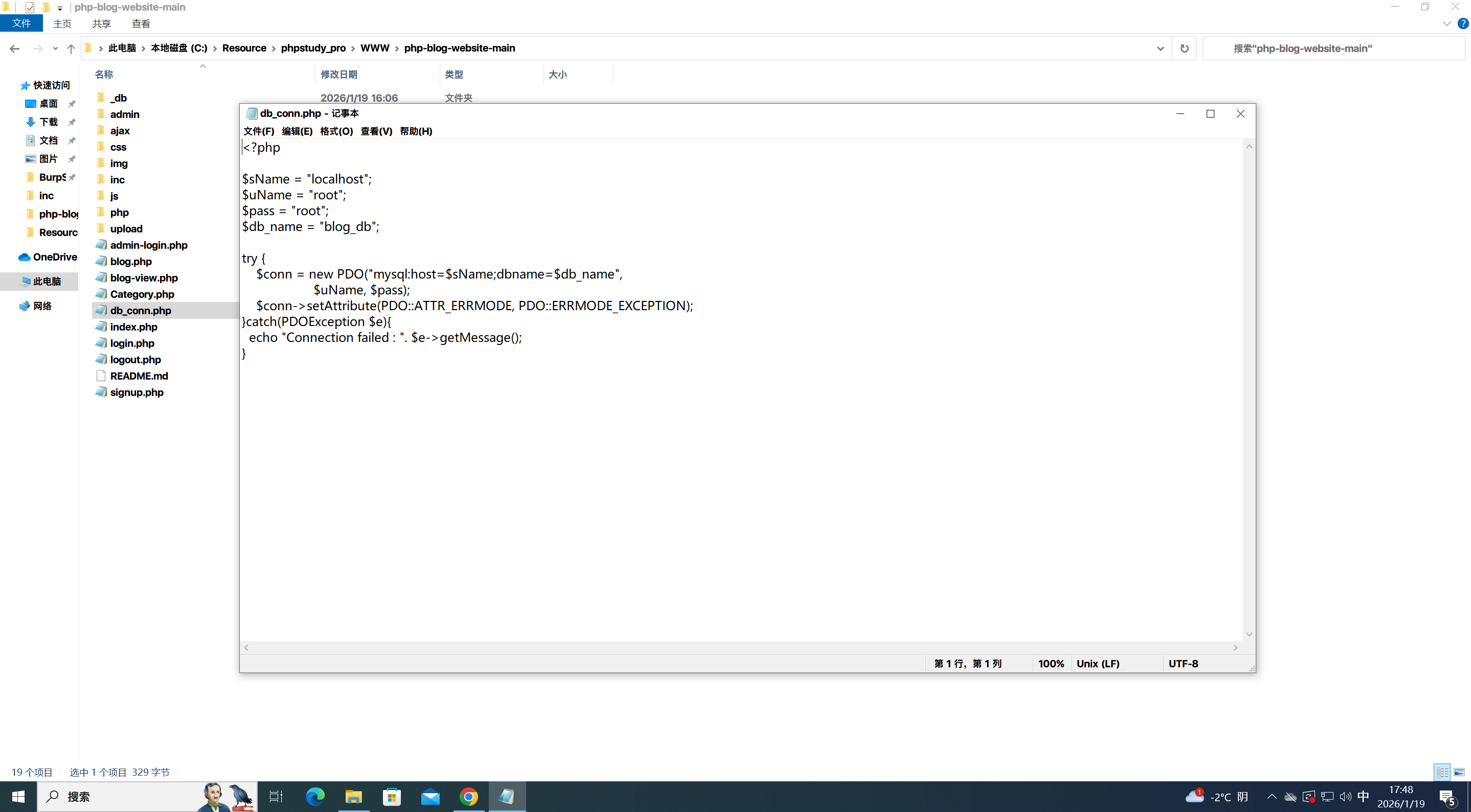
Download the source code and extract it to the server root directory.

You will see the following files (as listed in the project structure).

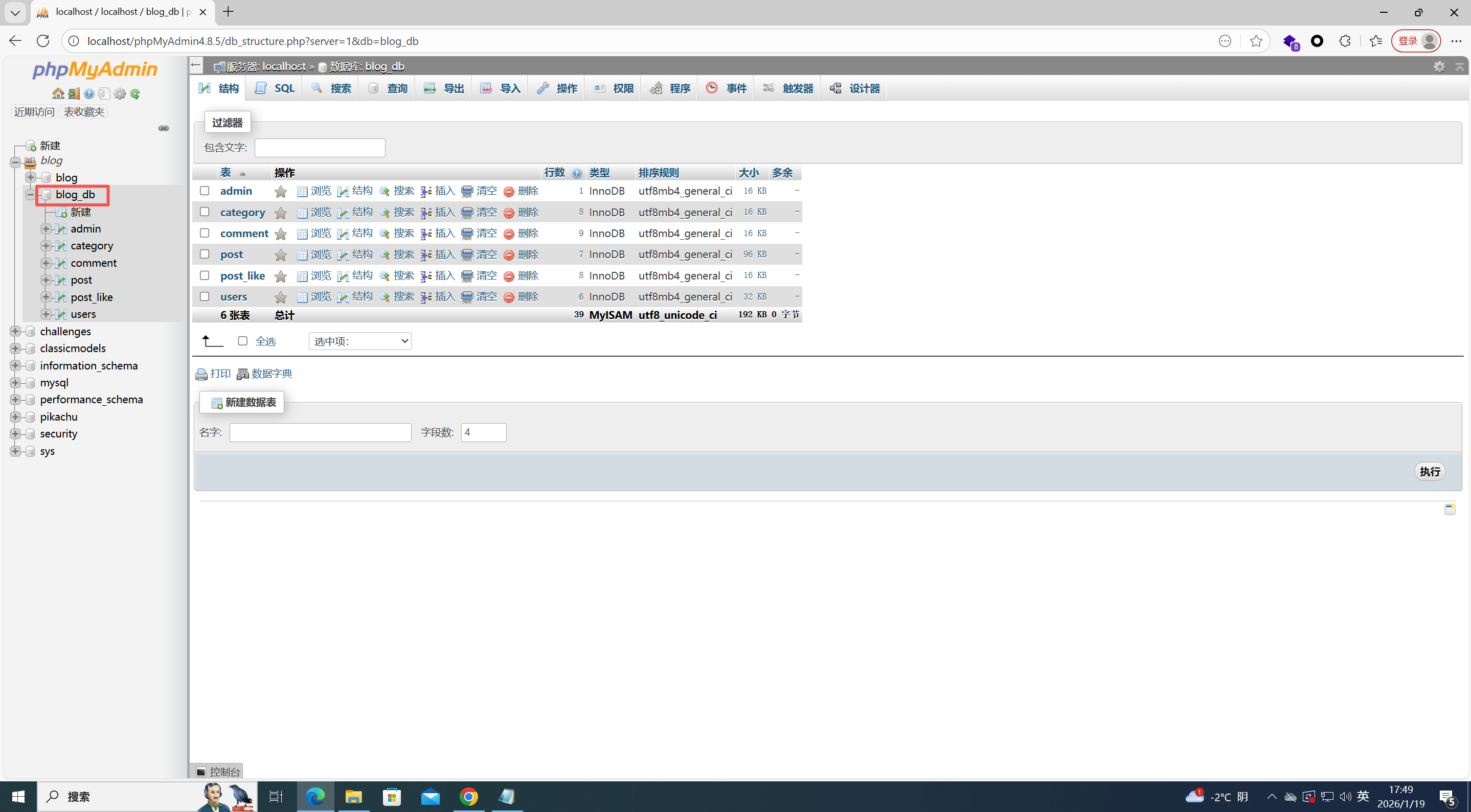


To deploy the project successfully, you need to modify the db\_conn.php file:

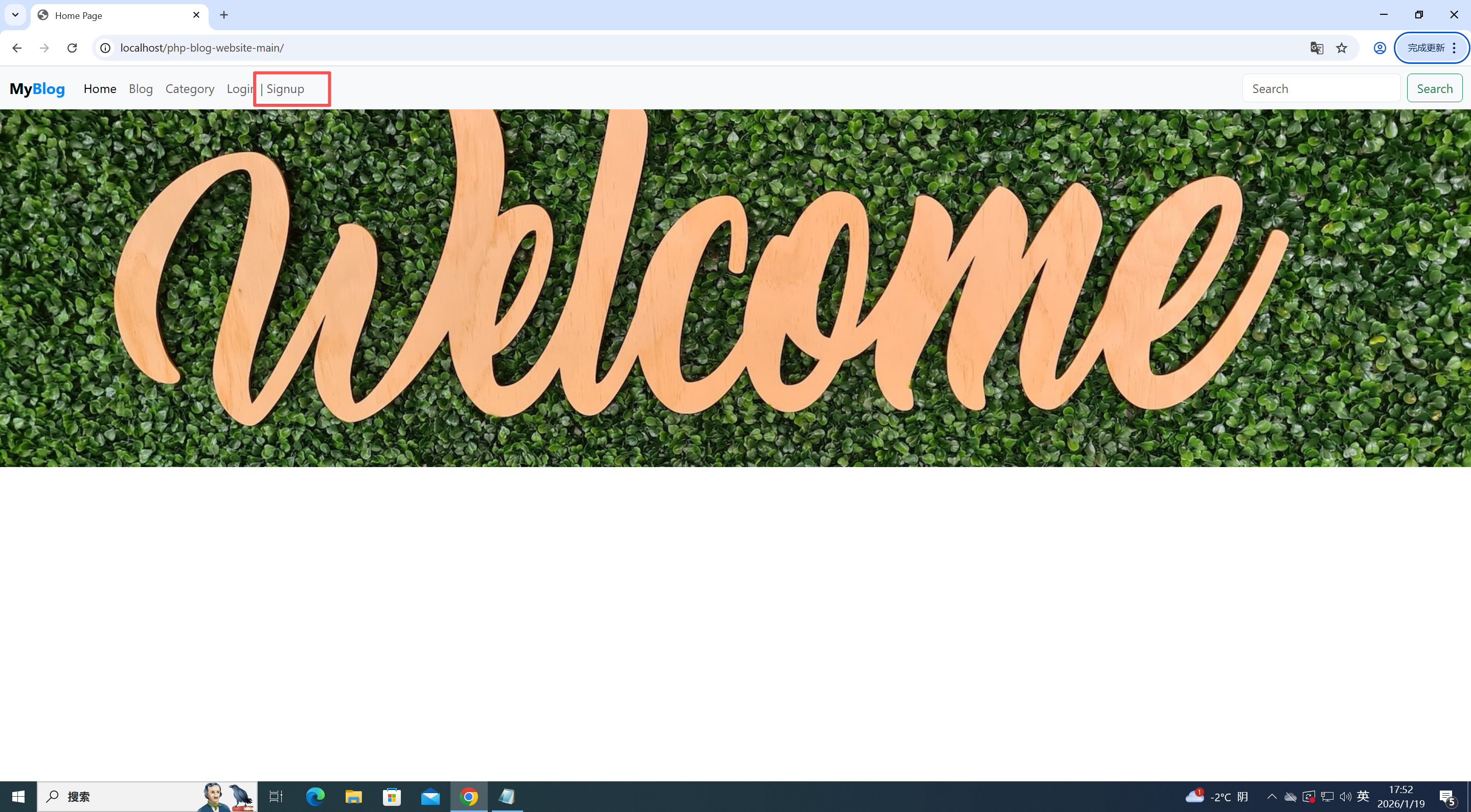
Fill in the database configuration information (such as database host, username, password) into the file.

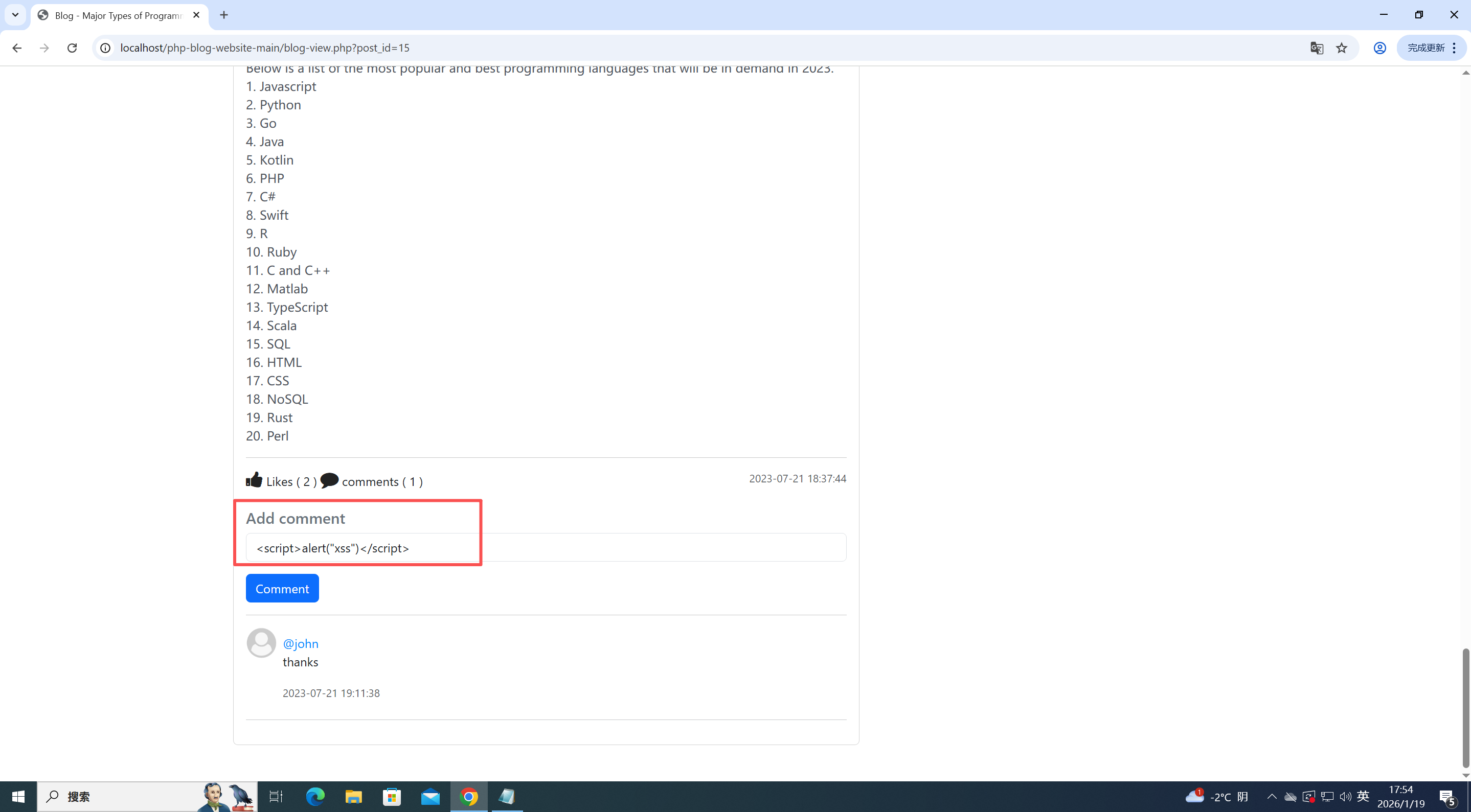


Next, create a database named blog\_db and import the php-blog-website-main\\_db\blog\_db.sql file into this database.



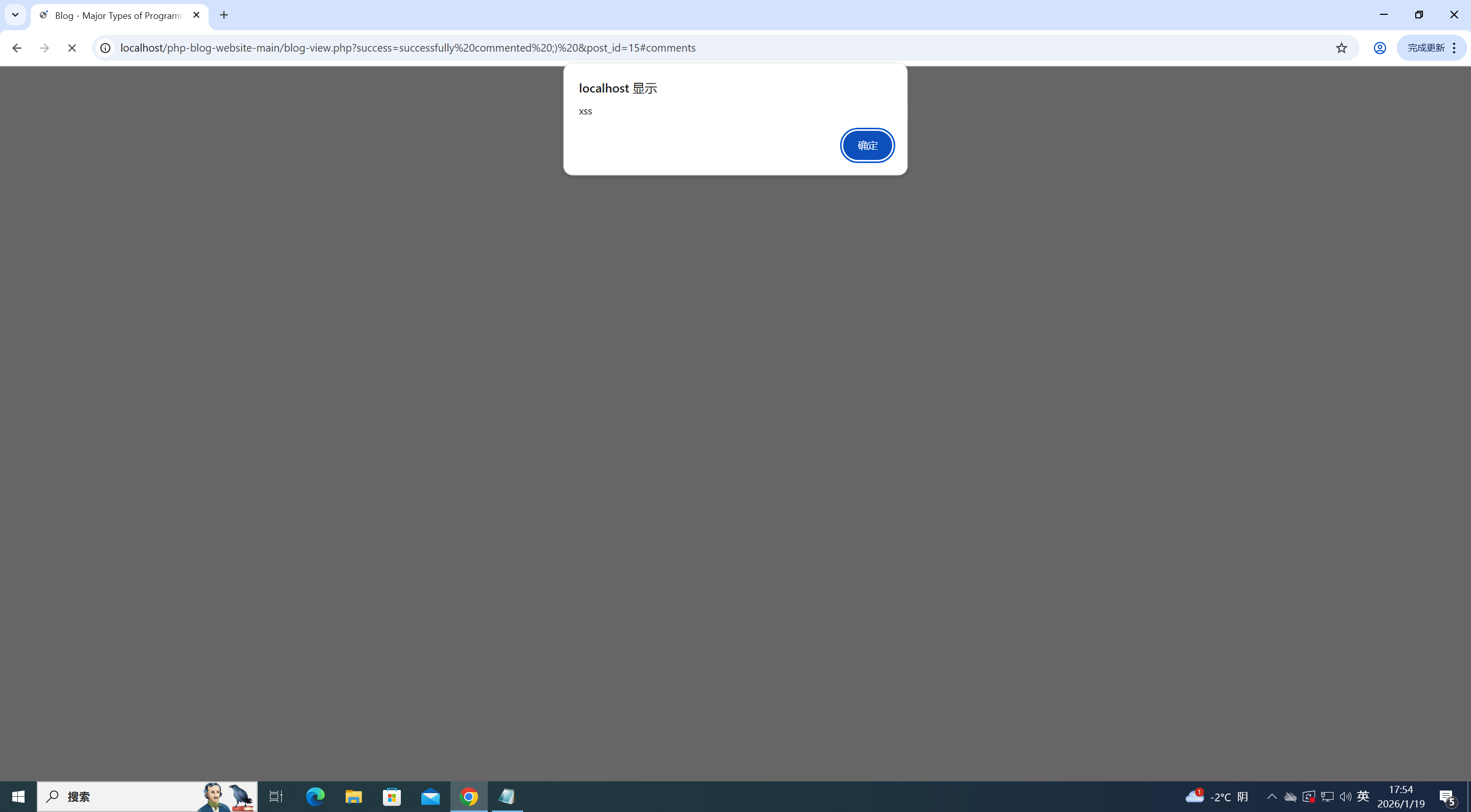
The project deployment is now complete.

Open the website: Register a user (in this case, I registered a user named "test").



Open any article, then enter the following payload in the "Add Comment" section:

**Payload**: <script>alert("xss")</script>



After submitting the comment, a pop-up window appears successfully.

Conclusion: This project has an XSS (Cross-Site Scripting) vulnerability.