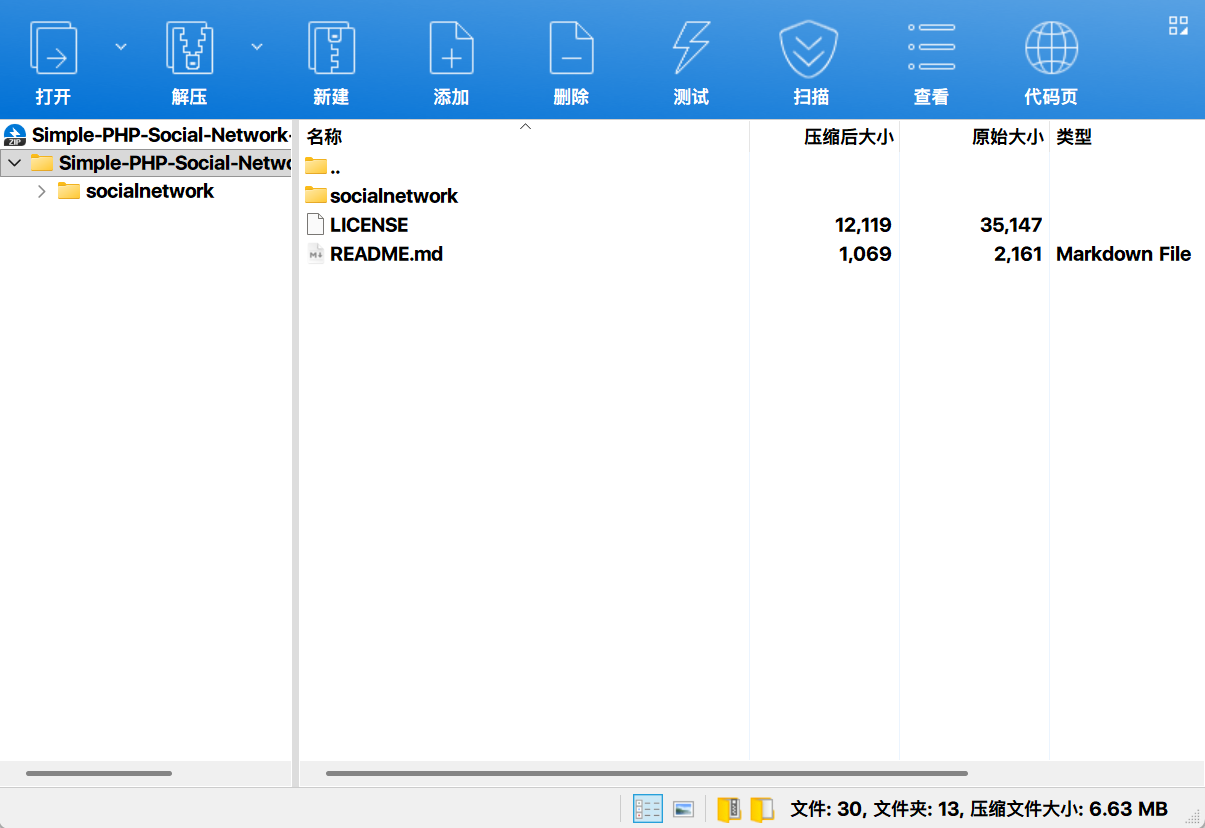
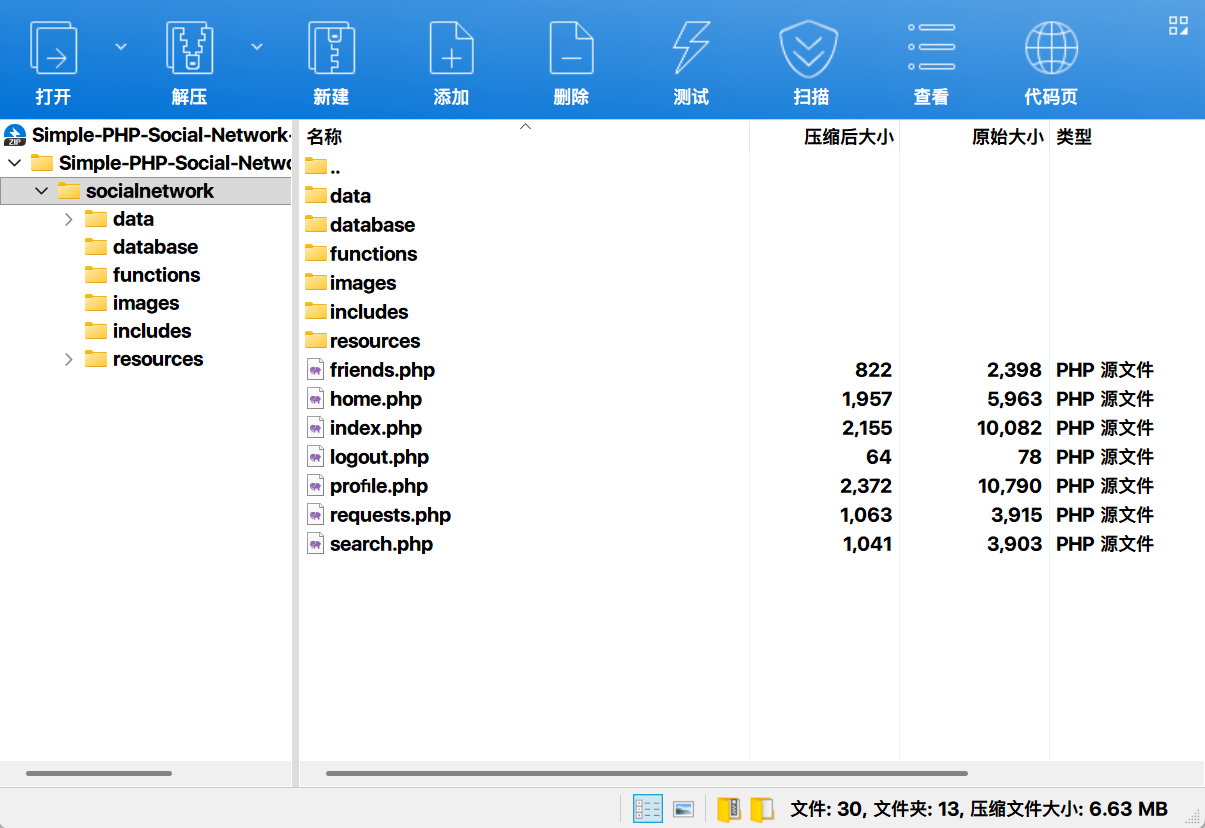
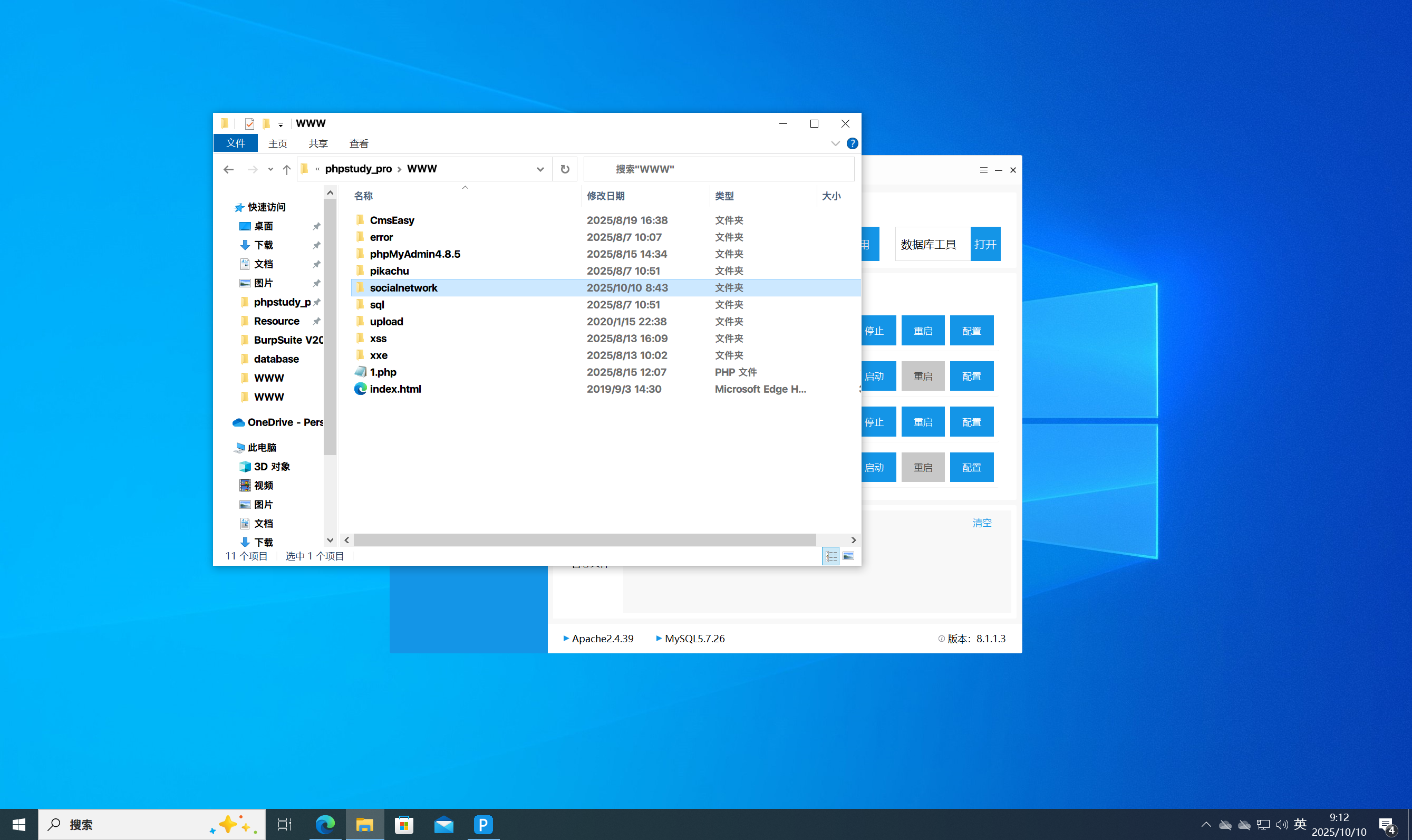
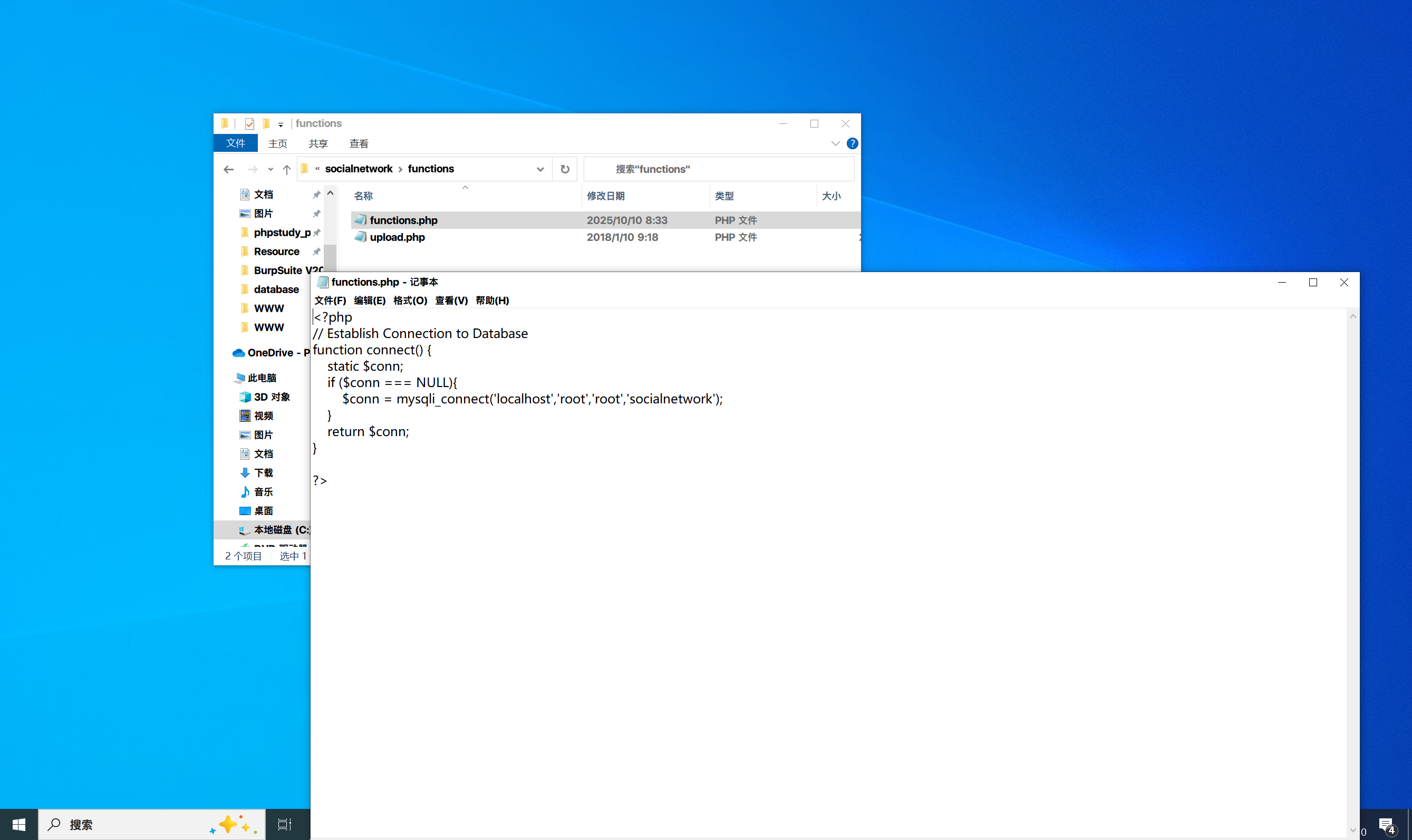
Project Repository: <https://github.com/iPynch/Simple-PHP-Social-Network-Website>

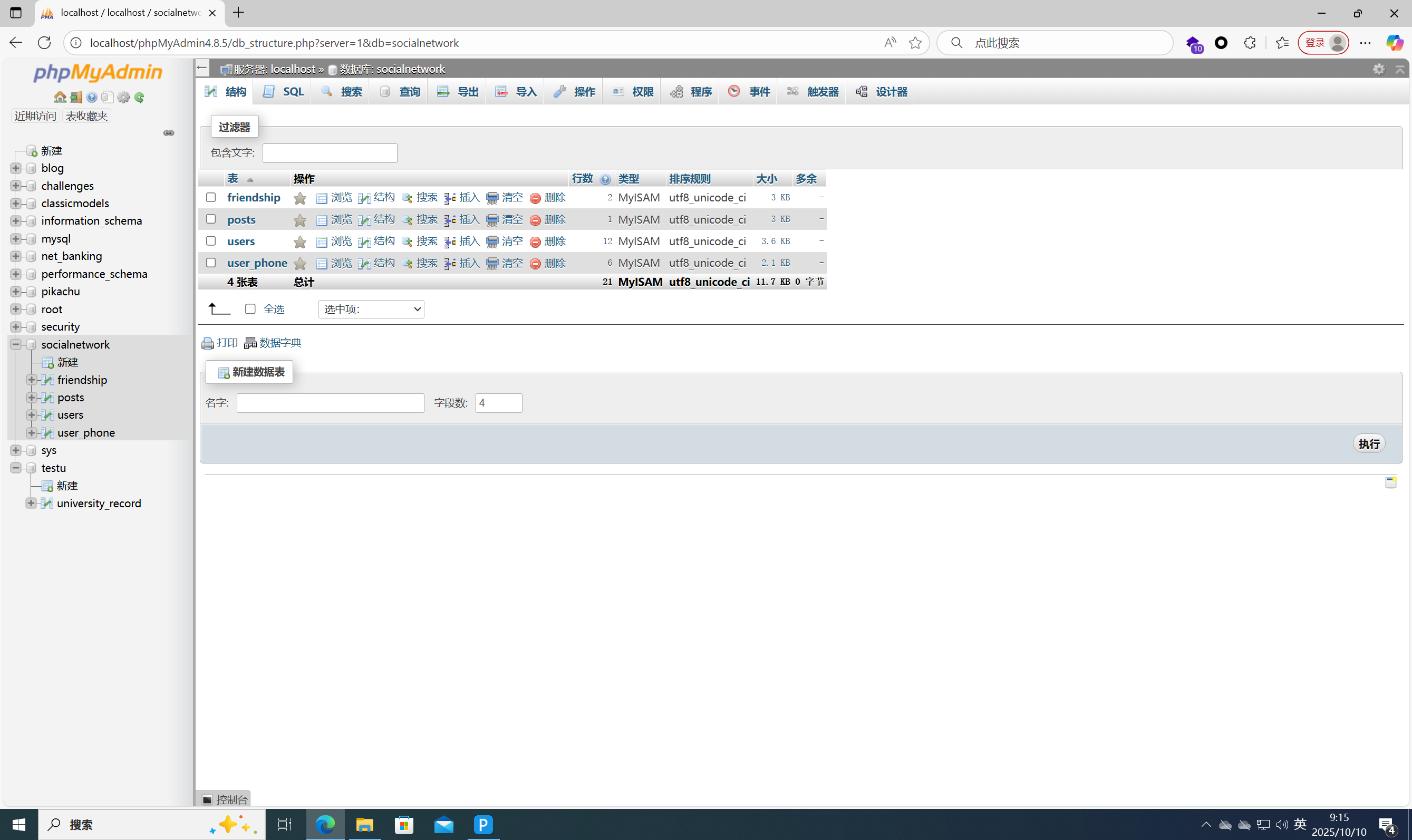
After downloading the project, the following files are included:



Among them, the "socialnetwork" folder contains the following files:

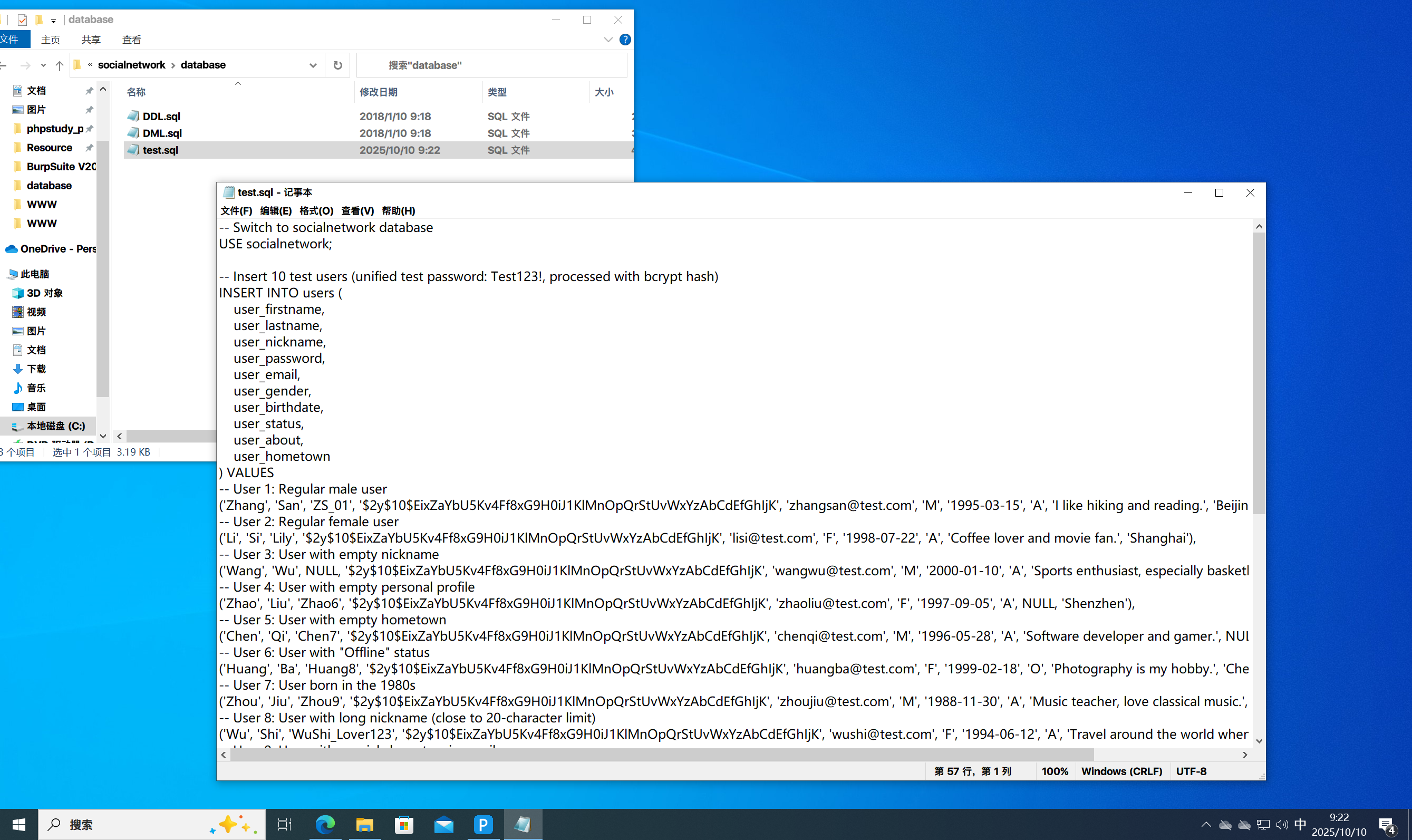
To set up the project, simply place the "socialnetwork" folder in the server root directory. In this case, we will implement this in a virtual machine.

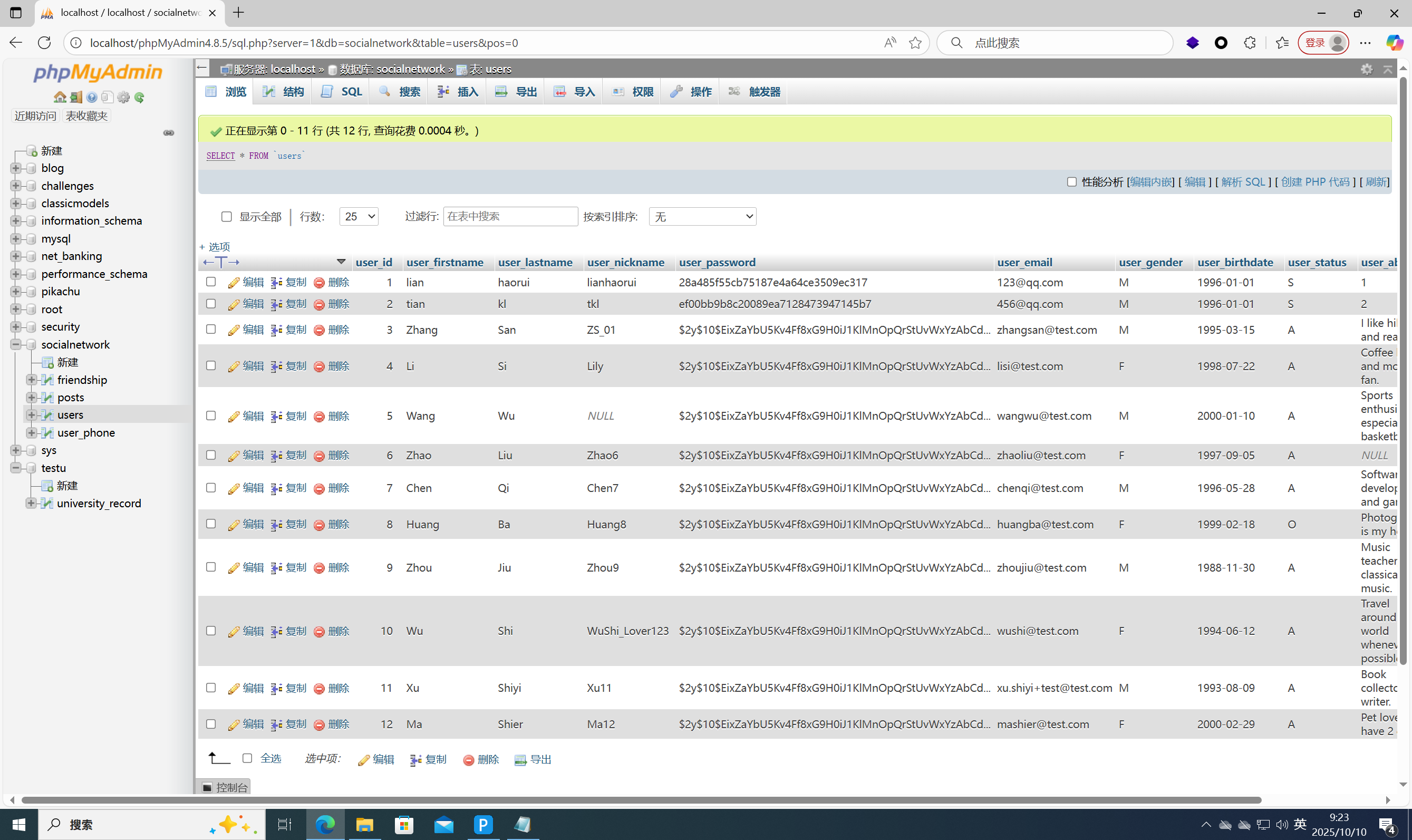
Next, modify the functions/functions.php file to update the database configuration.

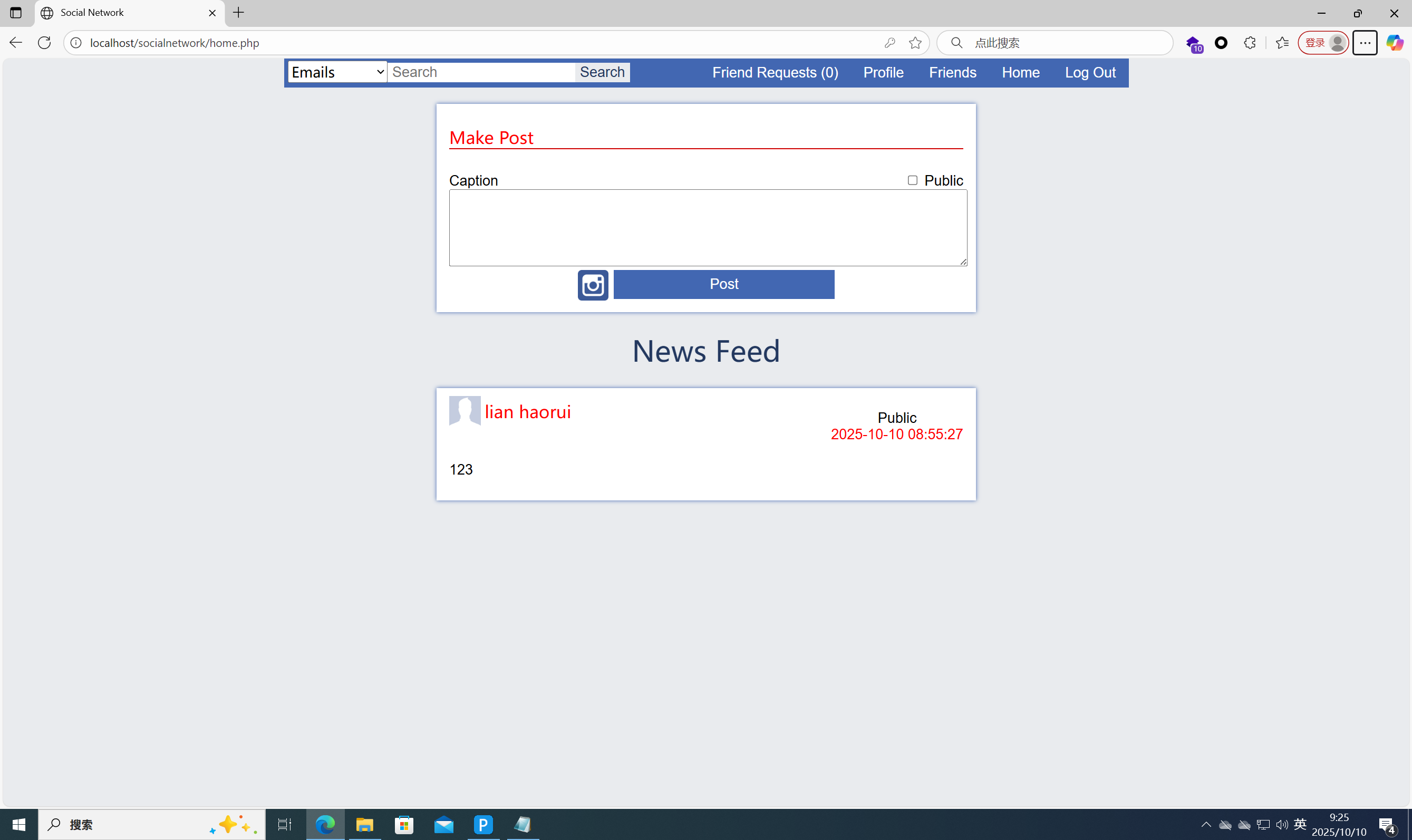
Then, create a database named "socialnetwork" and import the database/DDL.sql file.

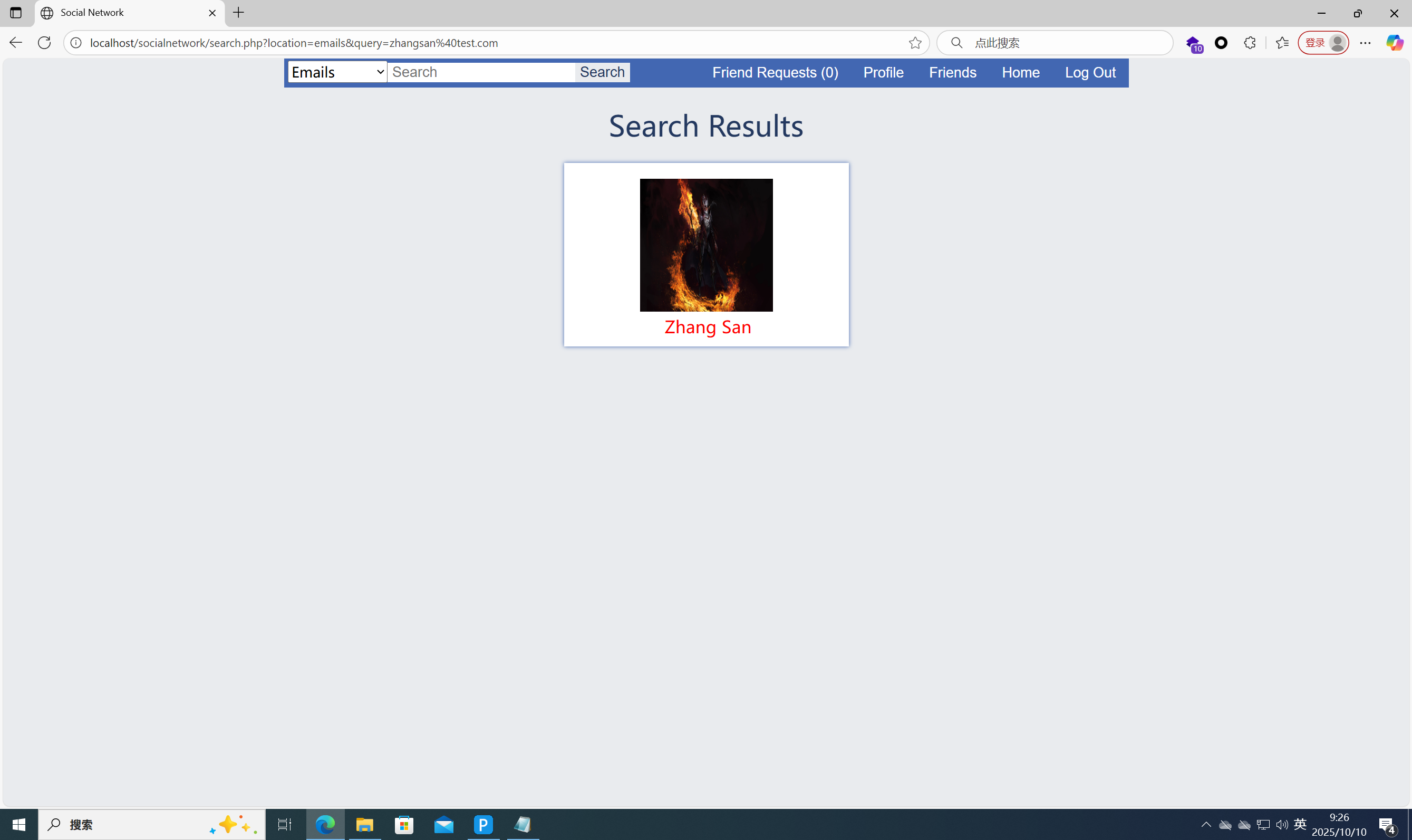
Once the database is created, proceed to import test data. Since there are issues with database/DML.sql, here we provide a SQL script for creating test data (named test.sql).

|  |  |
| --- | --- |
| 01  02  03  04  05  06  07  08  09  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47  48  49  50  51  52  53  54  55  56 | -- Switch to socialnetwork database  USE socialnetwork;    -- Insert 10 test users (unified test password: Test123!, processed with bcrypt hash)  **INSERT** **INTO** users (      user\_firstname,      user\_lastname,      user\_nickname,      user\_password,      user\_email,      user\_gender,      user\_birthdate,      user\_status,      user\_about,      user\_hometown  ) **VALUES**  -- User 1: Regular male user  ('Zhang', 'San', 'ZS\_01', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'zhangsan@test.com', 'M', '1995-03-15', 'A', 'I like hiking and reading.', 'Beijing'),  -- User 2: Regular female user  ('Li', 'Si', 'Lily', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'lisi@test.com', 'F', '1998-07-22', 'A', 'Coffee lover and movie fan.', 'Shanghai'),  -- User 3: User with empty nickname  ('Wang', 'Wu', NULL, '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'wangwu@test.com', 'M', '2000-01-10', 'A', 'Sports enthusiast, especially basketball.', 'Guangzhou'),  -- User 4: User with empty personal profile  ('Zhao', 'Liu', 'Zhao6', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'zhaoliu@test.com', 'F', '1997-09-05', 'A', NULL, 'Shenzhen'),  -- User 5: User with empty hometown  ('Chen', 'Qi', 'Chen7', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'chenqi@test.com', 'M', '1996-05-28', 'A', 'Software developer and gamer.', NULL),  -- User 6: User with "Offline" status  ('Huang', 'Ba', 'Huang8', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'huangba@test.com', 'F', '1999-02-18', 'O', 'Photography is my hobby.', 'Chengdu'),  -- User 7: User born in the 1980s  ('Zhou', 'Jiu', 'Zhou9', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'zhoujiu@test.com', 'M', '1988-11-30', 'A', 'Music teacher, love classical music.', 'Chongqing'),  -- User 8: User with long nickname (close to 20-character limit)  ('Wu', 'Shi', 'WuShi\_Lover123', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'wushi@test.com', 'F', '1994-06-12', 'A', 'Travel around the world whenever possible.', 'Hangzhou'),  -- User 9: User with special characters in email  ('Xu', 'Shiyi', 'Xu11', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'xu.shiyi+test@test.com', 'M', '1993-08-09', 'A', 'Book collector and writer.', 'Nanjing'),  -- User 10: User with birthday on February 29 (leap year)  ('Ma', 'Shier', 'Ma12', '$2y$10$EixZaYbU5Kv4Ff8xG9H0iJ1KlMnOpQrStUvWxYzAbCdEfGhIjK', 'mashier@test.com', 'F', '2000-02-29', 'A', 'Pet lover, have 2 cats.', 'Wuhan');    -- Add phone numbers for some users (关联user\_phone表, complying with foreign key constraints)  **INSERT** **INTO** user\_phone (user\_id, user\_phone) **VALUES**  (1, 13800138000),  -- Phone number for user 1  (2, 13900139000),  -- Phone number for user 2  (3, 13700137000),  -- Phone number for user 3  (5, 13600136000),  -- Phone number for user 5  (7, 13500135000),  -- Phone number for user 7  (10, 13400134000); -- Phone number for user 10    -- Verify insertion results (optional execution to confirm successful data insertion)  **SELECT**      u.user\_id,      u.user\_firstname,      u.user\_lastname,      u.user\_email,      p.user\_phone  **FROM** users u  LEFT JOIN user\_phone p **ON** u.user\_id = p.user\_id  **ORDER** **BY** u.user\_id; |

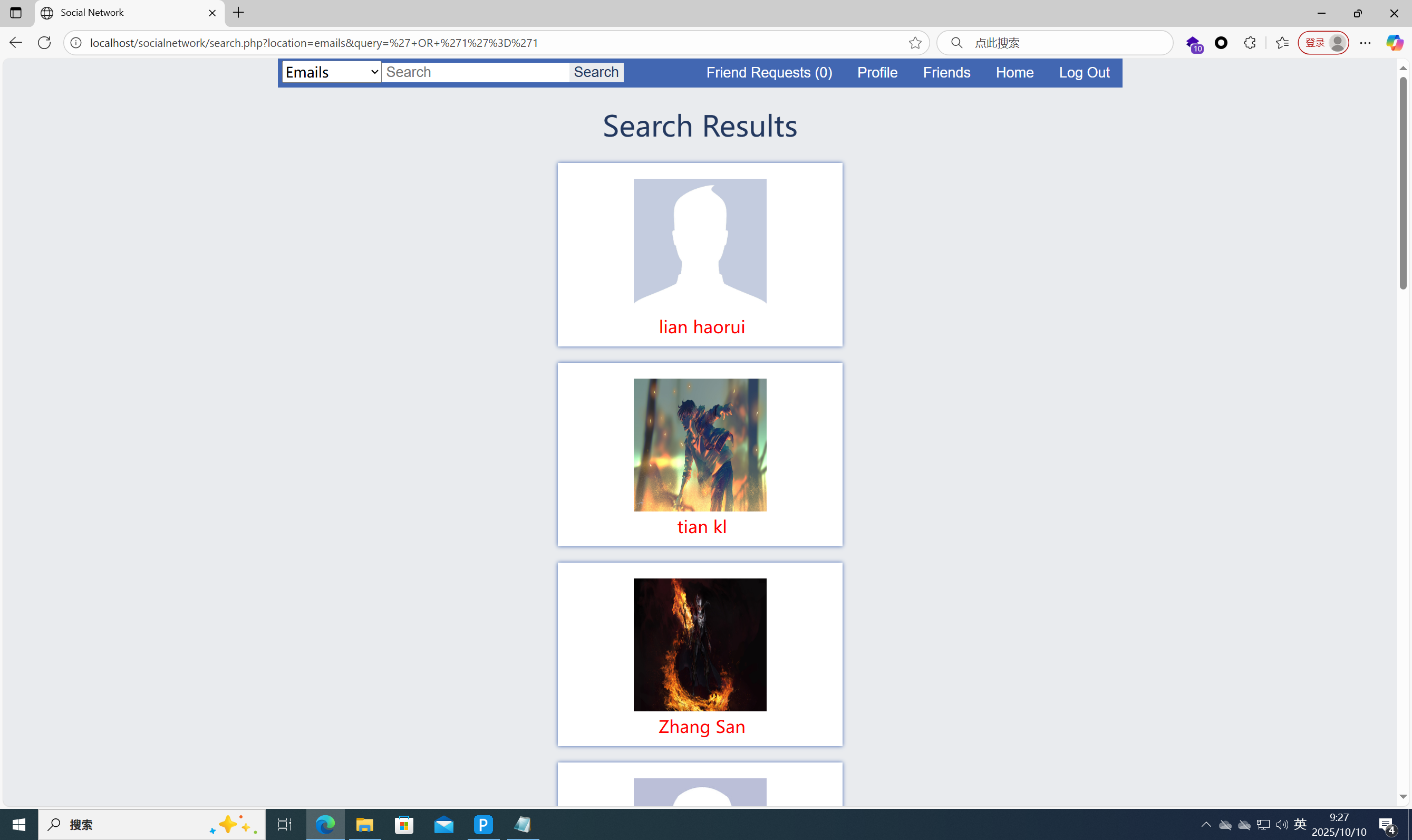




After importing this file, access the website and log in to an account. (Here, we use a self-created account named "lianhaorui".)

In the Search bar, enter: zhangsan@test.com

It can be seen that the test user information is retrieved correctly.

In the Search bar, enter: ' OR '1'='1

All user information can be retrieved.

Therefore, this project has an SQL injection vulnerability.  
Additionally, the payload: ' OR '1'='1 is applicable to all search functions in this project.

。