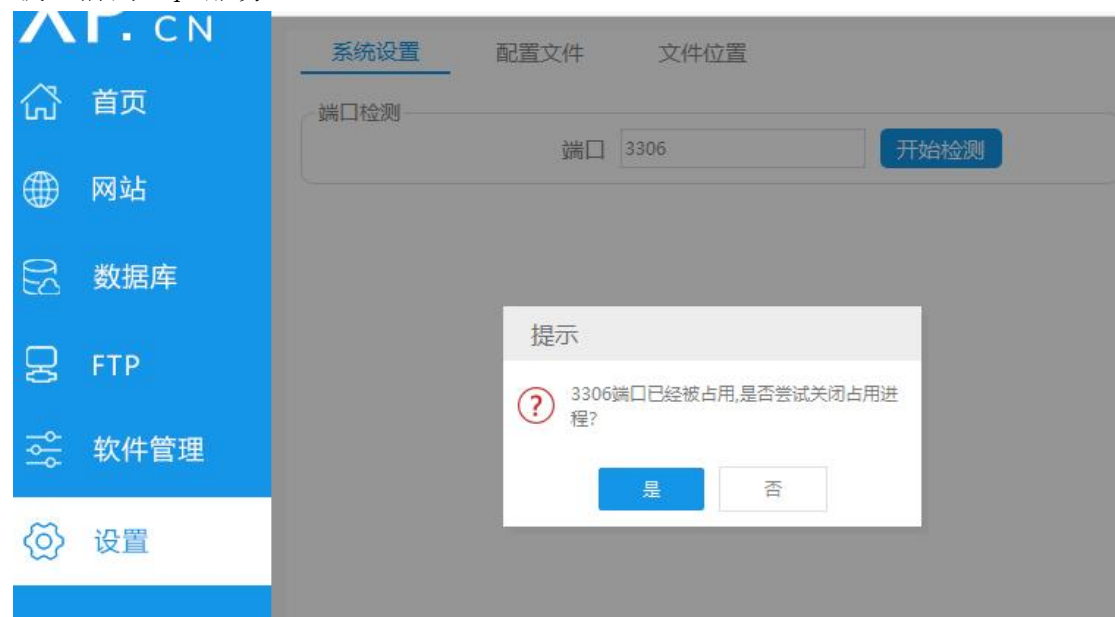
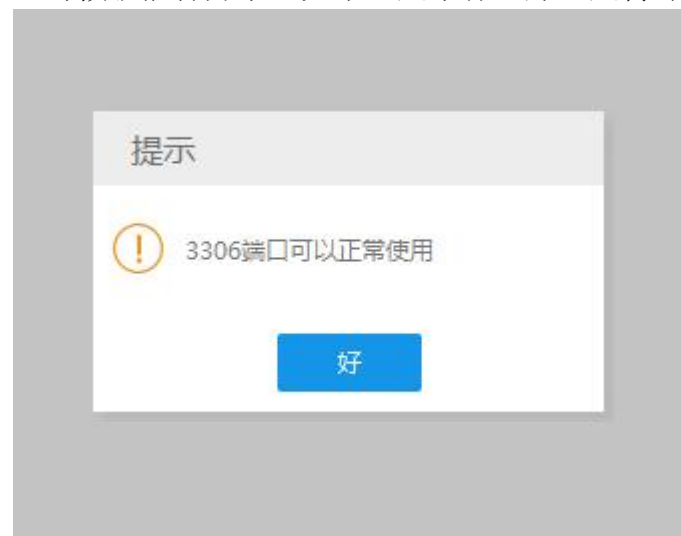


1、Mysql 服务相关

首先是本机的 mysql 和 php 的 mysql 冲突问题，这里额外提供一种方法，不用卸载之前的 sql 服务：



进入主界面-设置，输入默认的端口号并检测，如果被占用把这个端口关闭即可，这时候就能打开了。如果还是不行，那还是得卸载之前的 sql 服务。



Sql 服务开启后，**最好重新创建一个新的用户和 database** (因为 root 权限下存在一些比较重要的配置信息)：



这时候我们进入 phpstudy 的 mysql 的 bin 目录，查看一些配置信息：

D:\phpstudy_pro\Extensions\MySQL5.7.26\bin

```
D:\phpstudy_pro\Extensions\MySQL5.7.26\bin>mysql -u fty -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.26 MySQL Community Server (GPL)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show global variables like 'port';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| port          | 3306  |
+-----+-----+
1 row in set, 1 warning (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| database0 |
+-----+
```

然后修改 dvwa 的配置，和这里保持一致：

```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'database0';
$_DVWA[ 'db_user' ]     = 'fty';
$_DVWA[ 'db_password' ] = '123456';
$_DVWA[ 'db_port' ]    = '3306';
```

这时候，再去 reset 就能成功：

Backend database: **MySQL/MariaDB**
Database username: **ftv**
Database password: *********
Database database: **database0**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**


[User: Administrator] Writable folder D:\phpstudy_pro\WWW\DVWA\hackable\uploads\: **Yes**

[User: Administrator] Writable folder D:\phpstudy_pro\WWW\DVWA\config: **Yes**
Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On  
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

 **Create / Reset Database**

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

Setup successful!

这个地方报错显示连接被拒绝或者服务未开启，可能原因是端口号或者数据库用户密码没输对。

2、CSRF 修改密码失败

有同学做第二个实验时，修改了密码但是去验证仍然显示 **wrong password**。首先按照这个方式检测下你 **dvwa** 使用的 **mysql** 是不是 **phpstudy** 里自带的。

```
D:\phpstudy_pro\Extensions\MySQL5.7.26\bin>mysql -u fty -p
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.26 MySQL Community Server (GPL)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show global variables like 'port';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| port          | 3306  |
+-----+-----+
1 row in set, 1 warning (0.00 sec)

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| database0 |
+-----+
```

然后重启下 mysql 服务:



如果仍未解决则可能是删除了 root 权限下的某些配置信息, 导致 update 的操作不被执行, 这时候卸载重装一遍, 再按照 1 的步骤配置一边即可。



3、SQL 注入显示 union illegal

这是由于不同字符类型的属性排序方式不同

TABLE_NAME	varchar(64)	utf8_general_ci
COLUMN_NAME	varchar(64)	utf8_general_ci
first_name	varchar(15)	utf8_unicode_ci
last_name	varchar(15)	utf8_unicode_ci
user	varchar(15)	utf8_unicode_ci
password	varchar(32)	utf8_unicode_ci

最直接的解决方式是直接修改列的排序规则（这里对应数据库的名称改成你自己的）：

```
ALTER TABLE database0.users MODIFY COLUMN first_name varchar(15)  
CHARACTER SET utf8 COLLATE utf8_general_ci;
```