

# Windows下DVWA靶场和SQL-libs靶场搭建

原创

waxcj 于 2022-04-25 17:26:43 发布 1658 收藏 1

分类专栏: [信息安全](#) 文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/waxcj/article/details/124408113>

版权



[信息安全](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

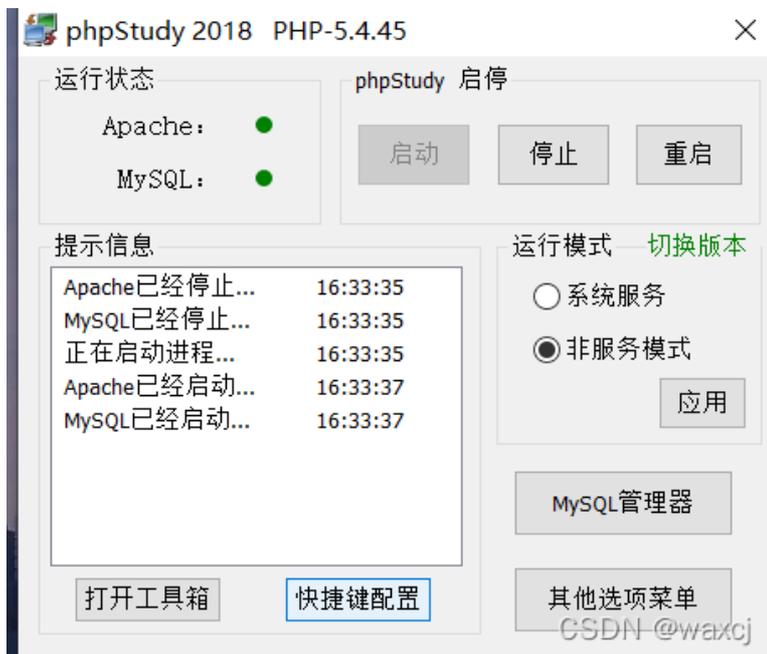
今天咱们来聊聊像网安小白比较适合靶场环境, 比较著名的有DVWA靶场和SQL-libs靶场等等。

## DVWA靶场搭建简介

DVWA是一款基于PHP和mysql开发的web靶场练习平台, 集成了常见的web漏洞如sql注入,xss, 密码破解等常见漏洞; 适合刚基础网络安全的小白。

### 1: PHPstudy安装

首先我们需要安装phpstudy (推荐是2018版本的, 比较好用一点), 安装好后我们启动phpstudy, 如下图所示。



接下来我们在自己的浏览器中输入127.0.0.1这个IP地址, 如果可以看到显示 Hello World 界面表示PHP study配置好了

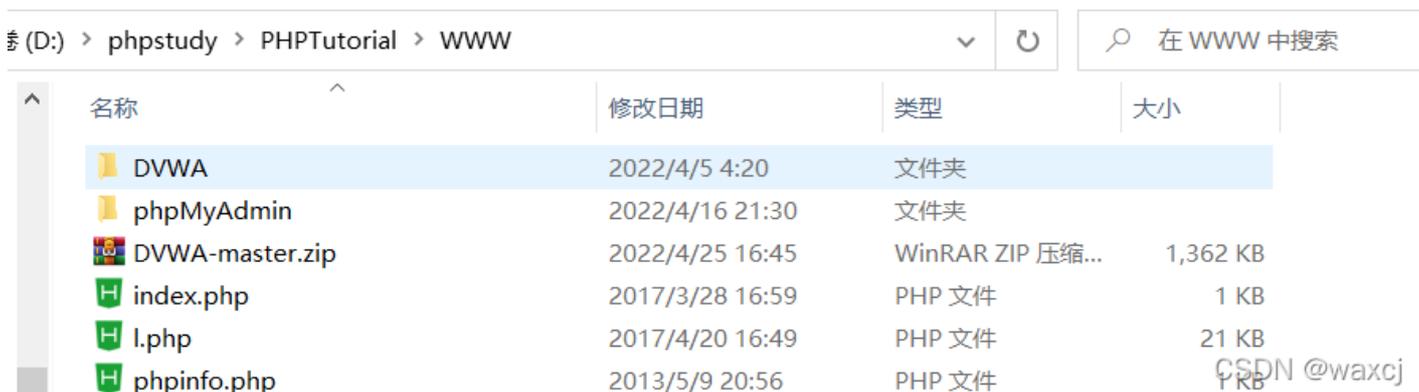
## 2: DWWA下载

我们可以直接进入DWWA官网下载（下载地址[DWWA - 该死的易受攻击的Web应用程序](#)），点击download直接下载



该死的易受攻击的Web应用程序 (DVWA) 是一个PHP / MySQL Web应用程序，非常容易受到攻击。其主要目标是帮助安全专业人员在法律环境中测试他们的技能和工具，帮助Web开发人员更好地了解保护Web应用程序的过程，并帮助教师/学生在课堂上环境中教授/学习Web应用程序安全性。

下载好后压缩到phpstudy文件下PHPTutorial下WWW目录中，如图

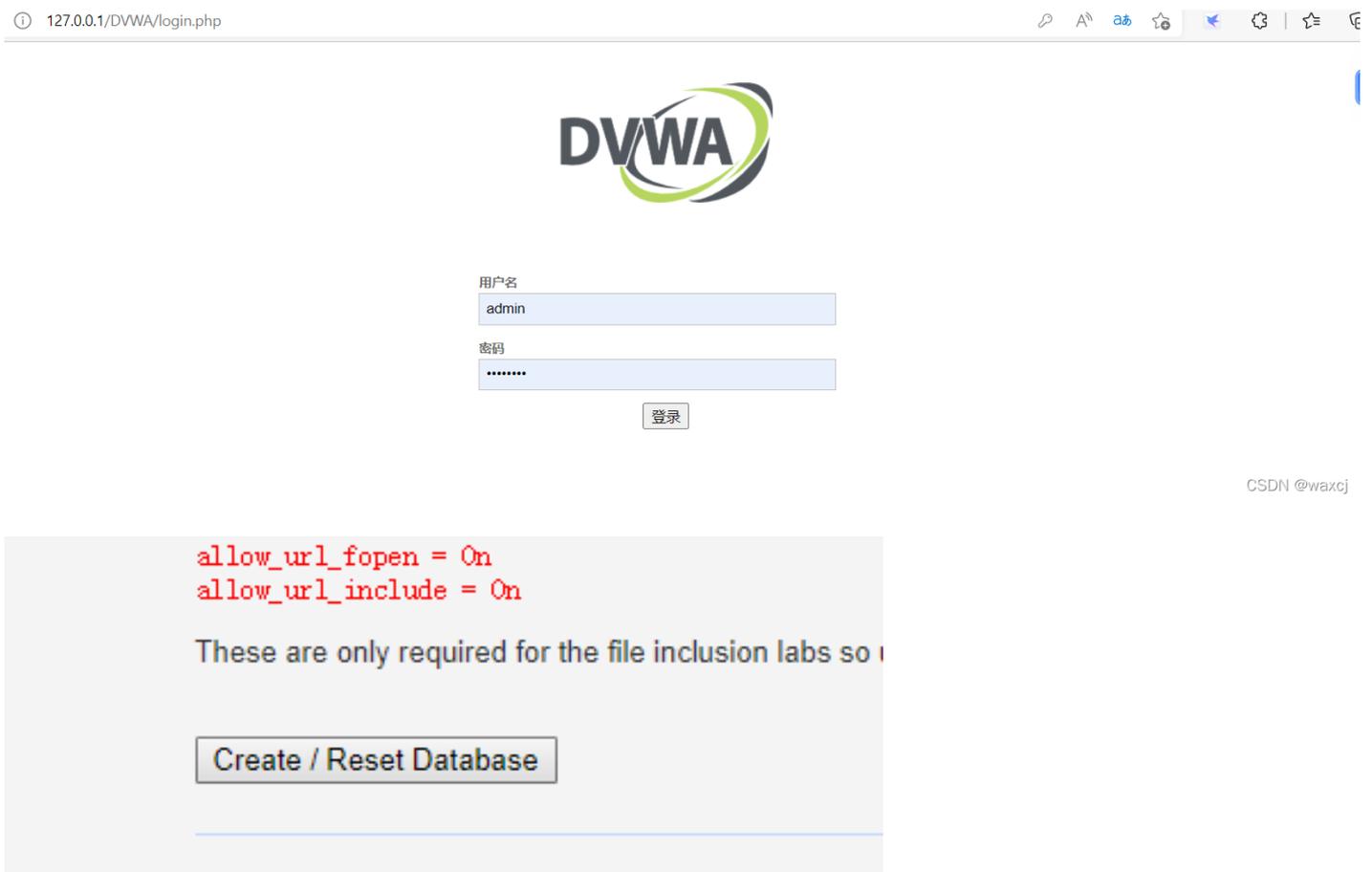


接下来打开DVWA文件夹下的config文件下的config.inc.php.dist，我们把config.inc.php.dist文件的.dist删除后打开。将db\_user和db\_password修改为对应数据库的用户名和密码

```
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'root';
$_DVWA[ 'db_port' ] = '3306';
```

CSDN @waxcj

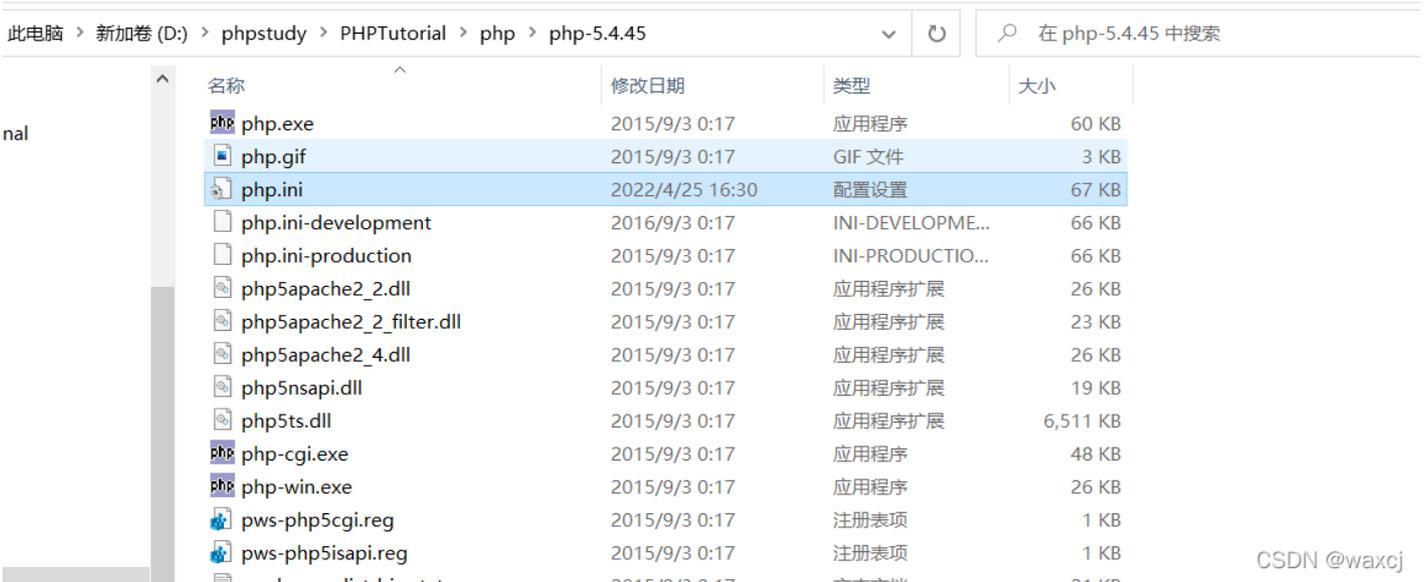
随后即可访问DVWA，在浏览器中输入127.0.0.1/dvwa即可登录，用户名admin 密码password



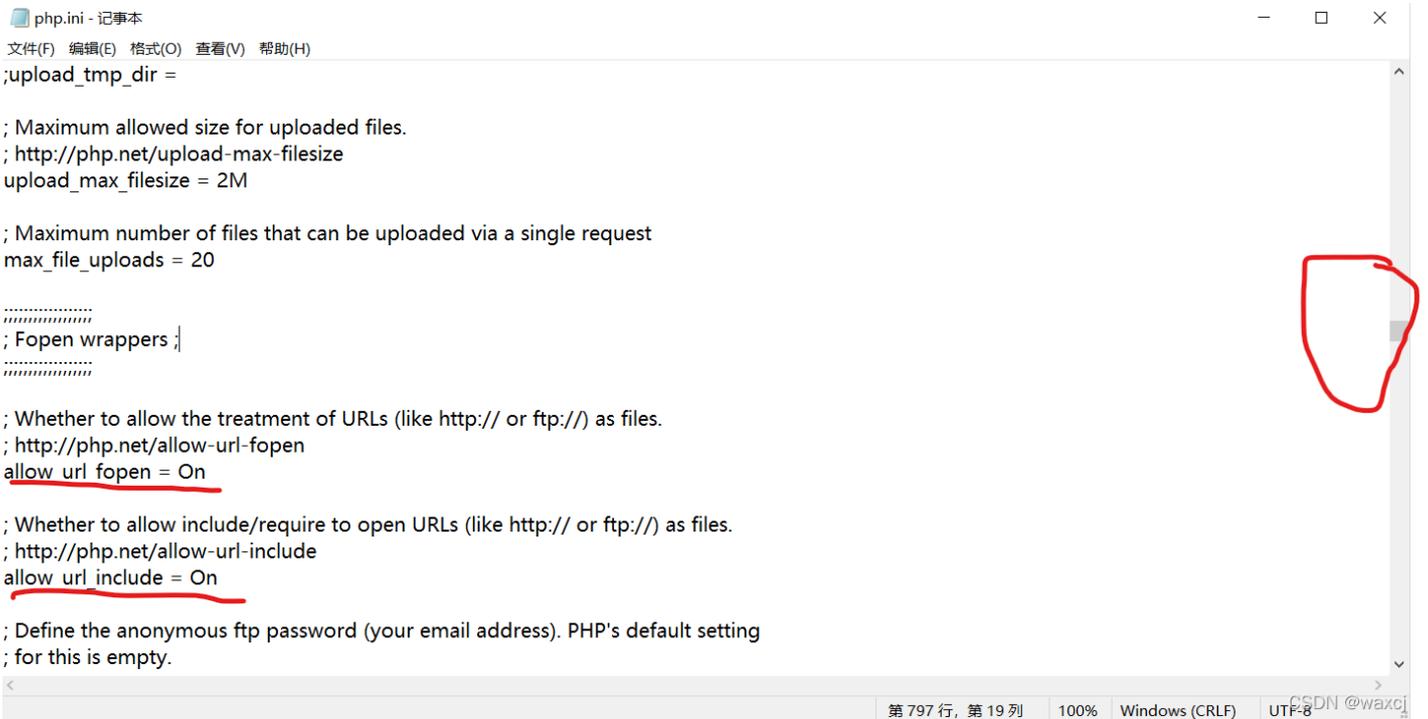
The image shows a browser window at 127.0.0.1/DVWA/login.php. The page features the DVWA logo and a login form with fields for '用户名' (Username) containing 'admin' and '密码' (Password) containing 'password'. A '登录' (Login) button is below the fields. Below the login form, there is a warning message in red text: 'allow\_url\_fopen = On' and 'allow\_url\_include = On'. Below this, it says 'These are only required for the file inclusion labs so'. At the bottom of this section is a button labeled 'Create / Reset Database'.

CSDN @waxcj

点击Create Database后，有可能在安装的时候会报错，如上图红色字体，这样我们就要去phpstudy目录下的PHP文件夹中的php.ini修改allow url fopen 为on



CSDN @waxcj



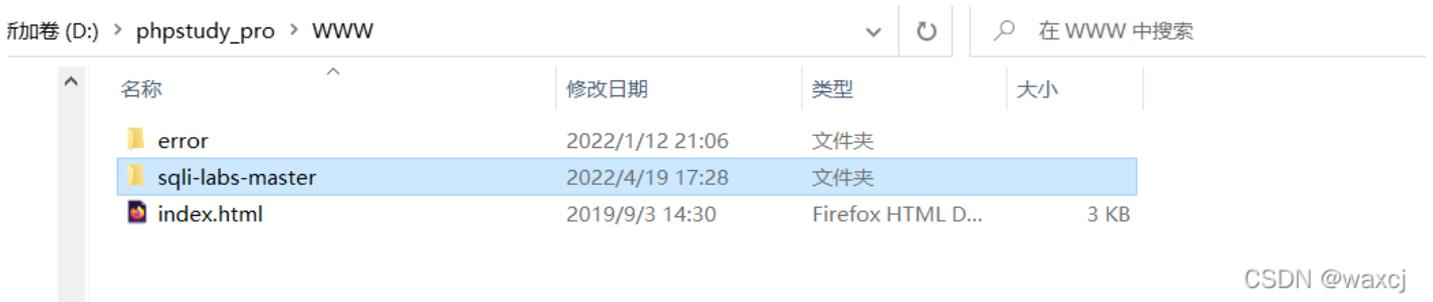
如果安装步骤没有出错的话就是如图所示，不会出现报错



## SQL-libs靶场搭建

首先，SQL-libs靶场也需要下载phpstudy，下载教程可以看上面，下载好后我们需要下载SQL-libs的源码[GitHub - Audi-1/sqli-labs: SQLI labs to test error based, Blind boolean based, Time based](#).推荐在github上下载

我们将下载好的源码解压到phpstudy下的www目录下



打开sql-connections/db-creds.inc文件（是下载的源码里面的文件）

修改inc里面的数据库用户名和密码，因为sqli-libs默认用户名为root，默认密码为空，如图

> phpstudy\_pro > WWW > sqli-labs-master > sql-connections

在 sql-connections 中搜索

名称	修改日期	类型	大小
db-creds.inc	2022/4/19 17:24	INC 文件	1 KB
functions.php	2014/11/1 3:10	PHP 文件	3 KB
setup-db.php	2014/11/1 3:10	PHP 文件	5 KB
setup-db-challenge.php	2014/11/1 3:10	PHP 文件	3 KB
sql-connect.php	2014/11/1 3:10	PHP 文件	1 KB
sql-connect-1.php	2014/11/1 3:10	PHP 文件	1 KB
sqli-connect.php	2014/11/1 3:10	PHP 文件	1 KB
test.php	2014/11/1 3:10	PHP 文件	1 KB

CSDN @waxcj

db-creds.inc - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php

//give your mysql connection username n password
$dbuser = 'root';
$dbpass = 'root';
$dbname = "security";
$host = 'localhost';
$dbname1 = "challenges";

?>
```

CSDN @waxcj

浏览器输入<http://127.0.0.1/sqli-labs-master/>,即可访问，如下图所示即为安装成功



## SQLi-LABS Page-1 (Basic Challenges)

[Setup/reset Database for labs](#)

[Page-2 \(Advanced Injections\)](#)

[Page-3 \(Stacked Injections\)](#)

[Page-4 \(Challenges\)](#)

CSDN @waxcj

希望大家好好研究这几个靶场！得到自己意想不到的收获，还有一些在线靶场是不需要自己搭建的，比如：[墨者学院\\_专注于网络安全人才培养](#)，[【i春秋】-专注网络安全\\_信息安全\\_白帽子的在线学习\\_教育\\_培训平台](#)

[封神台 - 掌控安全在线演练靶场](#)，是一个在线黑客攻防演练平台。等等靶场也是很不错的练习平台

今天的内容就到这了，下次见^0^

创造不易，点个赞在走吧^0^,谢谢大家