# 说明

**该靶场含有当前多种漏洞复现，可供使用者练习web安全技术**

**分别为：DVWA 、SQLI-labs 、XSS-labs 、Upload-labs 、pikachu 、bWAPP**

**以下靶场相关知识及问题都可在 百度 中找到，开始学习更好的web安全技术吧**

# DVWA

DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。

DVWA共有十个模块，分别是:

1.Brute Force（暴力（破解））

2.Command Injection（命令行注入）

3.CSRF（跨站请求伪造）

4.File Inclusion（文件包含）

5.File Upload（文件上传）

6.Insecure CAPTCHA （不安全的验证码）

7.SQL Injection（SQL注入）

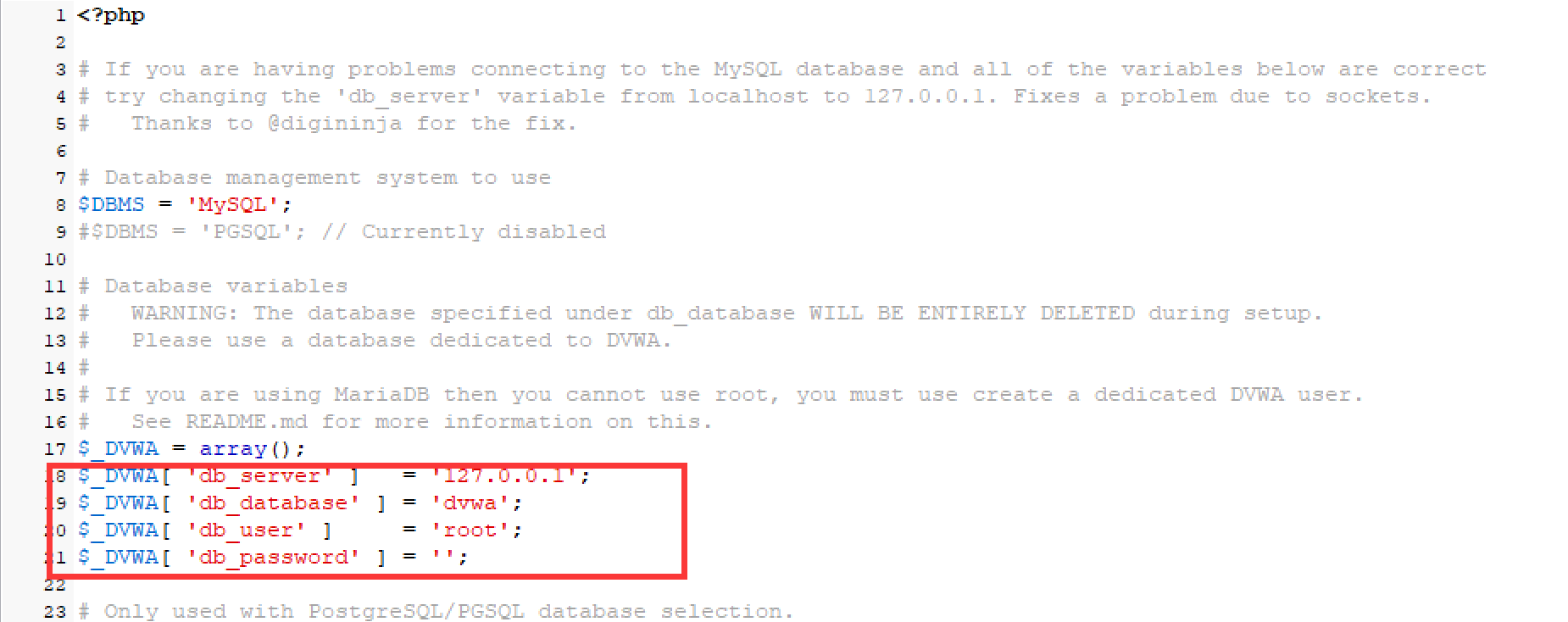
8.SQL Injection（Blind）（SQL盲注）

9.XSS（Reflected）（反射型跨站脚本）

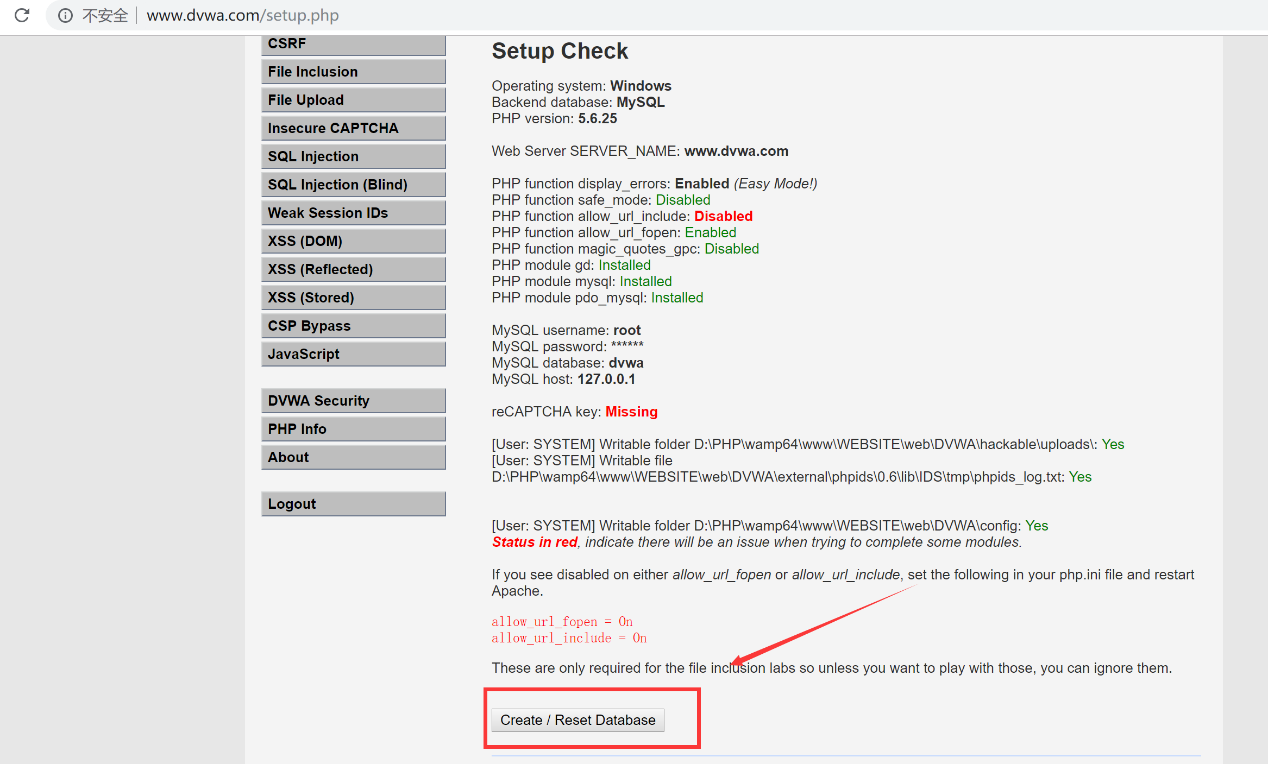
10.XSS（Stored）（存储型跨站脚本）

**Dvwa使用需要检查数据库账号密码即数据库数据的导入**

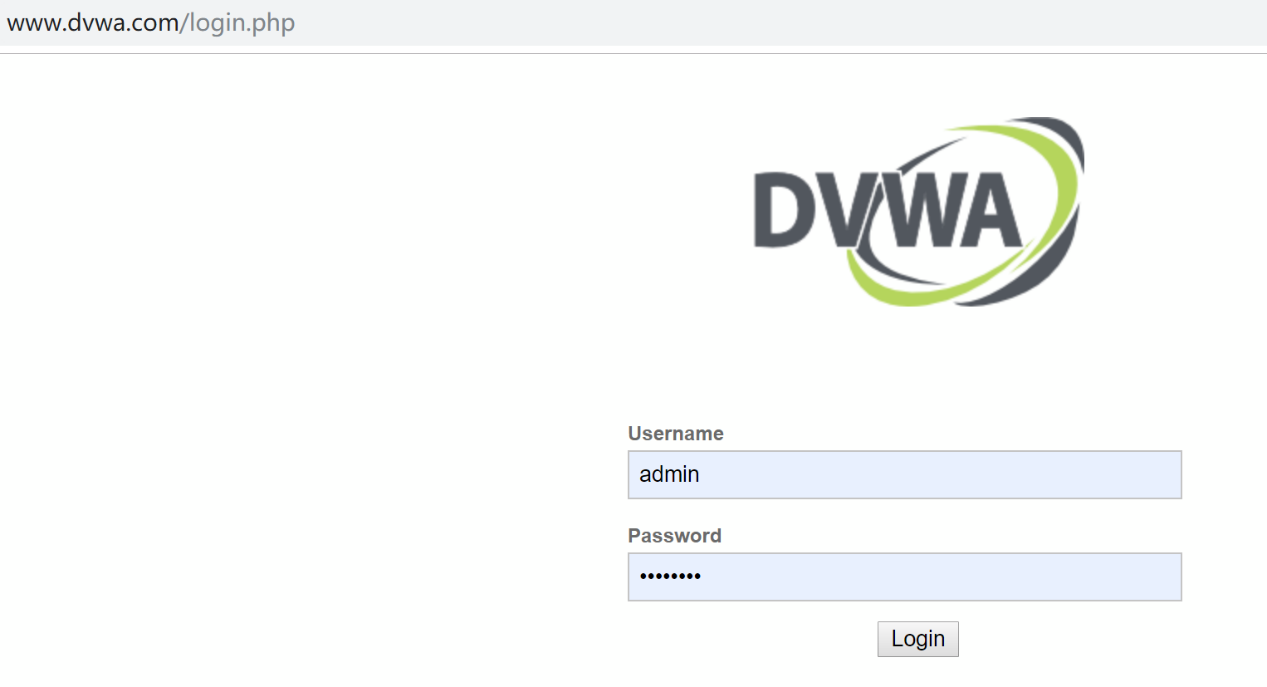
配置DVWA配置文件，在config/config.inc.php里:



在浏览器中访问http://域名/setup.php,然后点击网站下方的Create/Reset Database按钮。



接着会跳转到DVWA的登录页面 默认用户名：admin 默认密码：password



# Sqli-labs

Sqli-labs是一个印度程序员写的，用来学习sql注入的一个游戏教程。

SQLI，sql injection，我们称之为sql注入。何为sql，英文：Structured Query Language，叫做结构化查询语言。常见的结构化数据库有MySQL，MS SQL ,Oracle以及Postgresql。Sql语言就是我们在管理数据库时用到的一种。在我们的应用系统使用sql语句进行管理应用数据库时，往往采用拼接的方式形成一条完整的数据库语言，而危险的是，在拼接sql语句的时候，我们可以改变sql语句。从而让数据执行我们想要执行的语句，这就是我们常说的sql注入。

SQLi-Labs是一个专业的SQL注入练习平台，适用于GET和POST场景，包含了以下注入：

1、基于错误的注入（Union Select）

字符串

整数

2、基于误差的注入（双查询注入）

3、盲注入（01、基于Boolian数据类型注入， 02、基于时间注入）

4、更新查询注入（update ）

5、插入查询注入（insert ）

6、Header头部注入（01、基于Referer注入， 02、基于UserAgent注入，03、基于cookie注入）

7、二阶注入，也可叫二次注入

8、绕过WAF

绕过黑名单\过滤器\剥离\注释剥离 OR＆AND 剥离空格和注释剥离 UNION和SELECT隐瞒不匹配

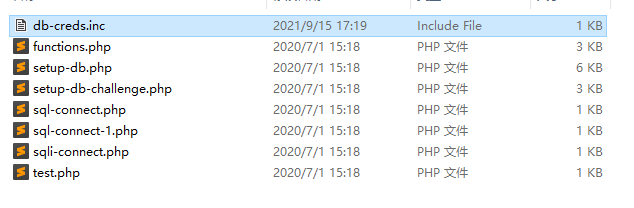
9、绕过addslashes()函数

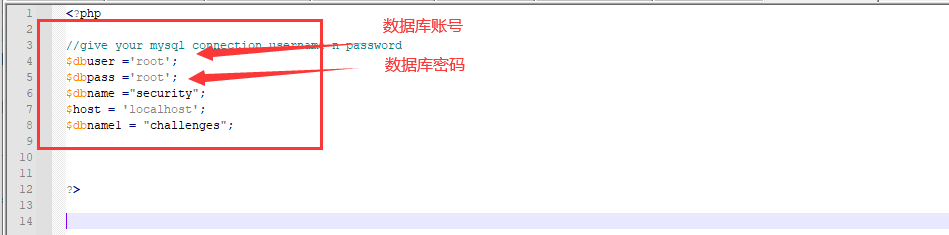
10、绕过mysql\_real\_escape\_string()函数（在特殊条件下）

11、堆叠注入（堆查询注入）

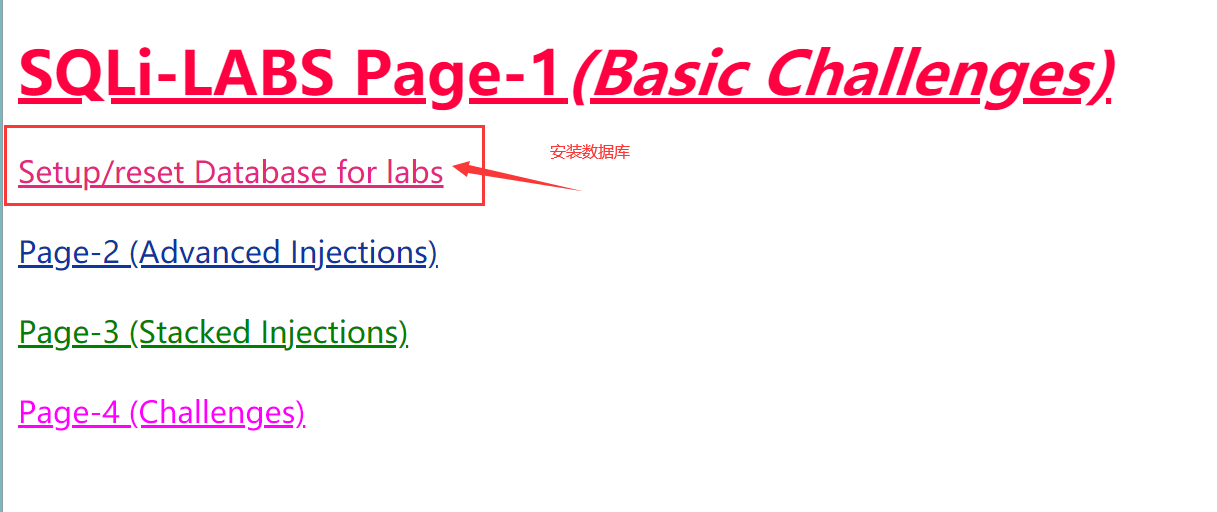
12、二级通道提取

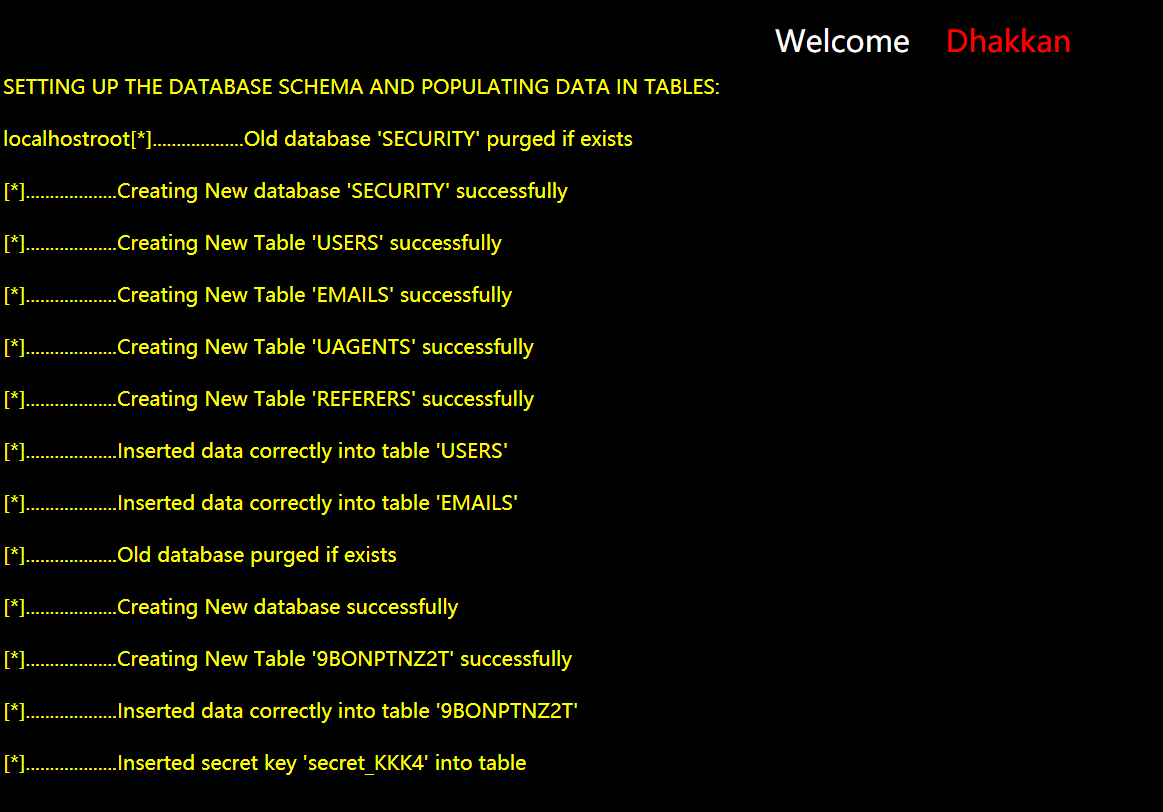
配置数据库账号密码目录： WWW\sqli-labs-php7\sql-connections



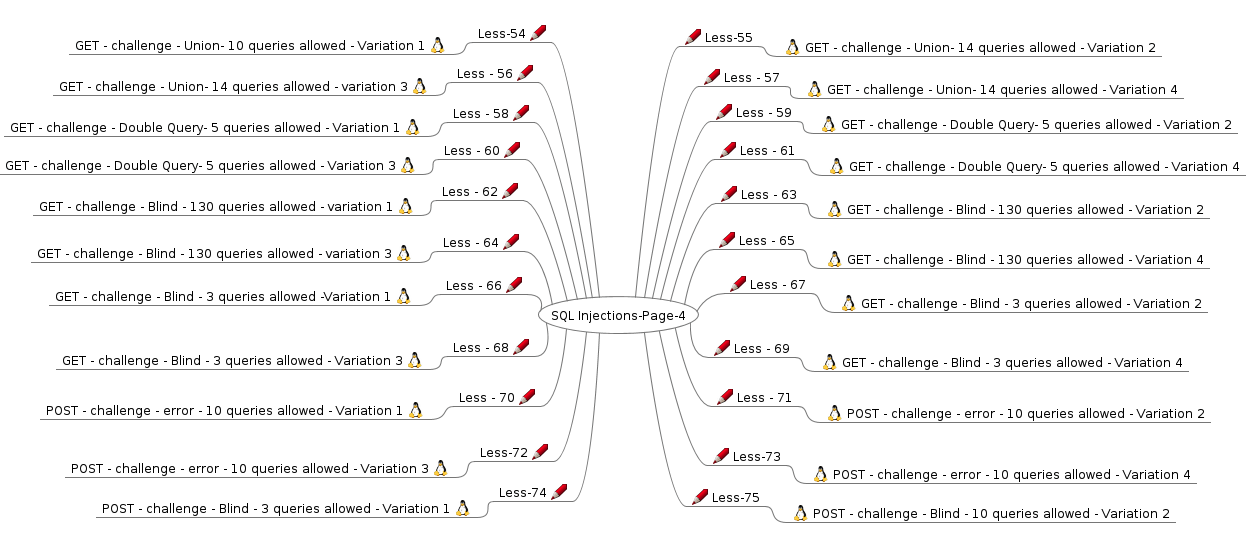


浏览器打开“**http://127.0.0.1/sqli-labs/**”访问首页，并点击“**Setup/reset Database**”以创建数据库，创建表并填充数据。





现在浏览器打开 "http://127.0.0.1/sqli-labs/"向下翻，就可以看到有很多不同的注入点了，分为基本SQL注入、高级SQL注入、SQL堆叠注入、挑战四个部份，总共约75个SQL注入漏洞。



总结：虽然说SQL注入搭建平台很多，程序也很多，但是很多的漏洞测试平台都不专一，大多数平台漏洞包含是比较全面的。

sqli-labs它是只专注SQL注入漏洞的，如果你只想主攻这个SQL注入方向，此平台真的是非常的给力

# XSS

xss-labs是一个使用php语言编写的，专门收集渗透测试和CTF中遇到的各种XSS漏洞的靶场。旨在帮助大家对XSS漏洞有一个全面的了解。目前一共20关，每一关都包含着不同XSS漏洞。



安装即可访问，无数据库配置文件’

# Upload

upload-labs是一个使用php语言编写的，专门收集渗透测试和CTF中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。目前一共20关，每一关都包含着不同上传方式。

集成环境绿色免安装，解压即可使用

## pass-01

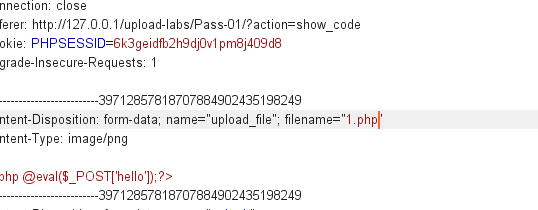
第一步、 查看源码，看看限制的文件类型。



第二步、 文本写入一句话木马，修改文件类型为允许上传类型 （ jpg | png | gif ）。

<?php @eval($\_POST['hello']);?> //一句话木马

第三步、 上传，抓包，修改后缀为php。



上传成功！

# Pikachu

pikachu是一个漏洞练习平台。其中包含了常见的web安全漏洞，如果你是一个渗透测试学习者没有靶场练手，那么pikachu将是一个不错的选择。

Pikachu上的漏洞类型列表如下：

Burt Force(暴力破解漏洞)

XSS(跨站脚本漏洞)

CSRF(跨站请求伪造)

SQL-Inject(SQL注入漏洞)

RCE(远程命令/代码执行)

Files Inclusion(文件包含漏洞)

Unsafe file downloads(不安全的文件下载)

Unsafe file uploads(不安全的文件上传)

Over Permisson(越权漏洞)

../../../(目录遍历)

I can see your ABC(敏感信息泄露)

PHP反序列化漏洞

XXE(XML External Entity attack)

不安全的URL重定向

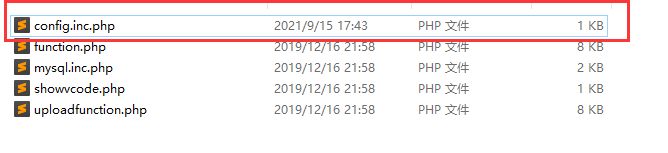
SSRF(Server-Side Request Forgery)

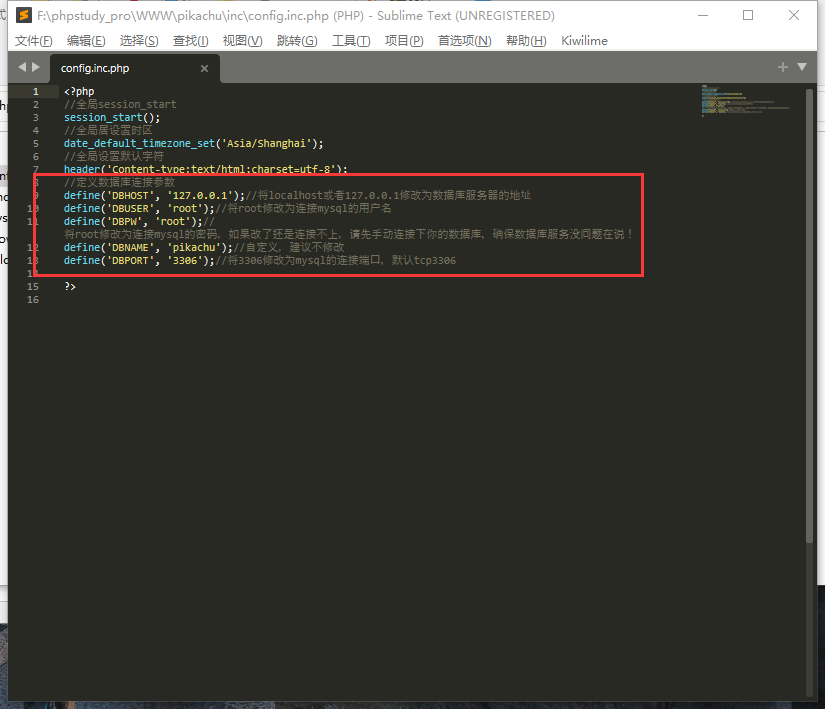
More...(找找看?..有彩蛋!)

管理工具里面提供了一个简易的xss管理后台,供你测试钓鱼和捞cookie~

需要修改数据库账户密码与初始化数据库安装：

数据库配置文件在  **WWW\pikachu\inc**  里







**http://127.0.0.1/pikachu/install.php**

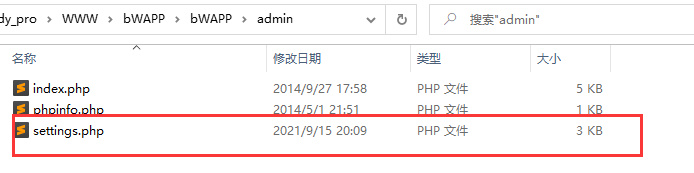
安装完成即可开始学习

# bWAPP

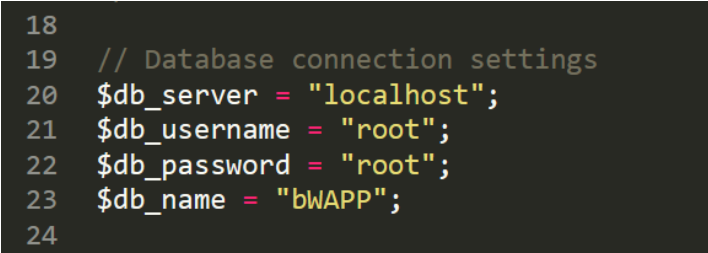
bwapp是一款非常好用的漏洞演示平台，包含有100多个漏洞。开源的php应用后台Mysql数据库

数据库账号密码配置文件目录

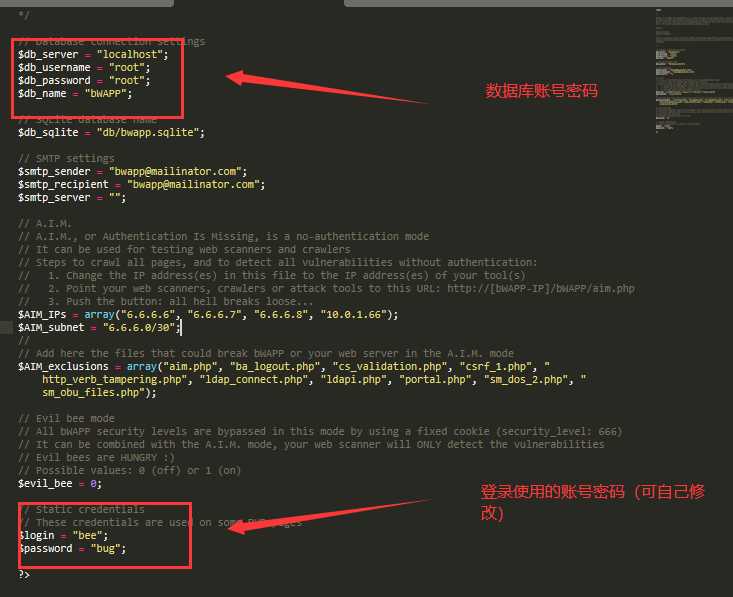
**WWW\bWAPP\bWAPP\admin**



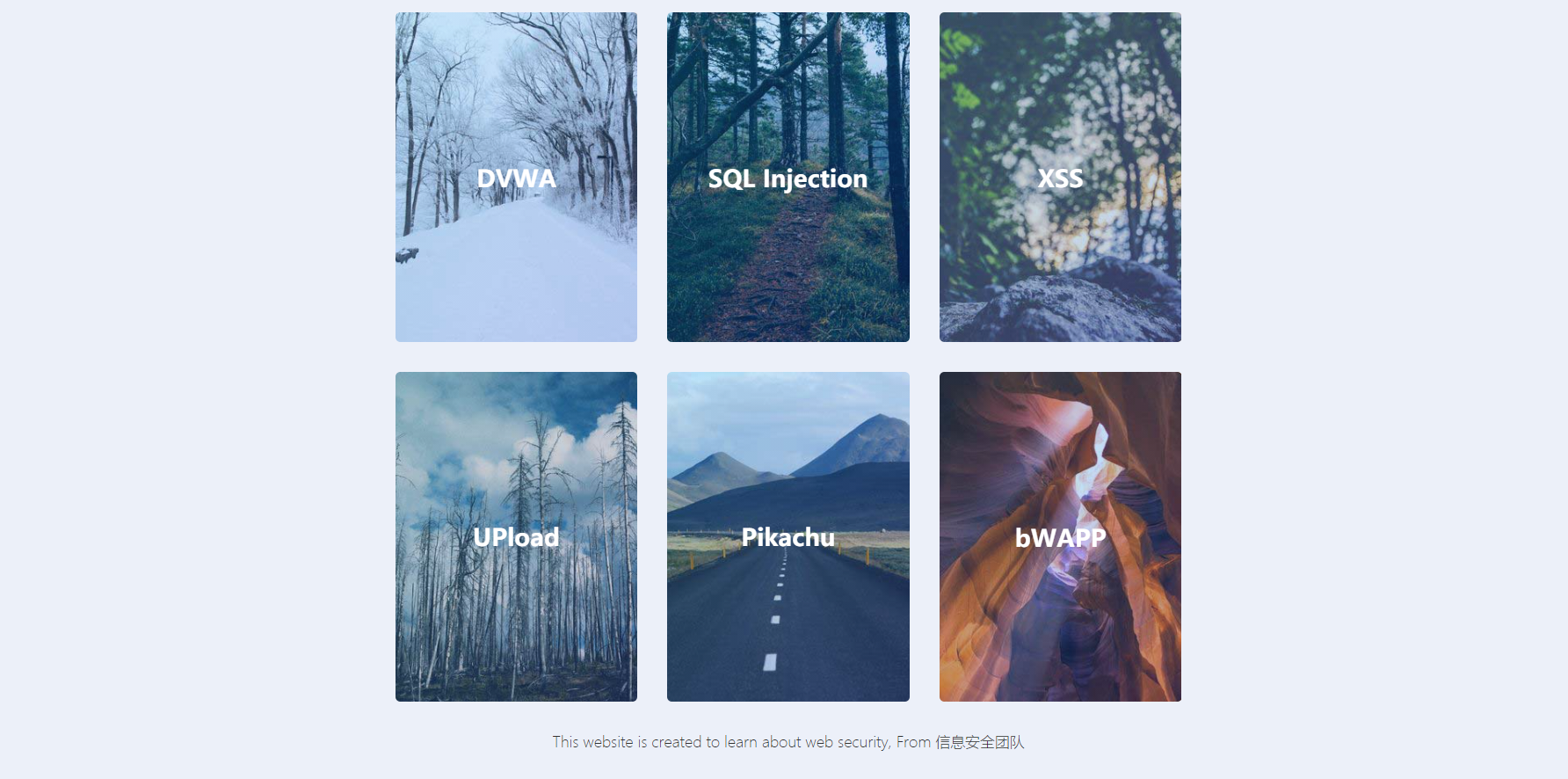
在admin/settings．php下更改数据库连接设置



 同时也能在文件下方看到默认登录账户名及密码，可按需更改



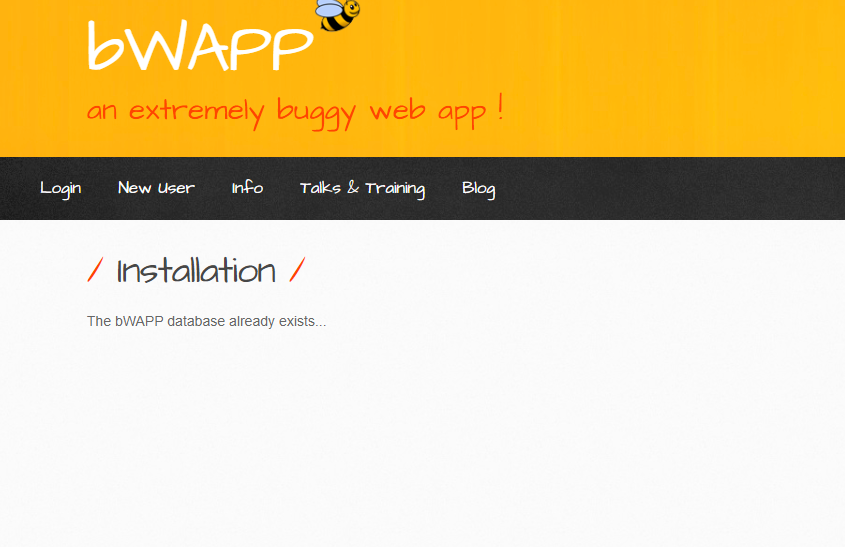
运行PHPStudy，然后在浏览器打开http://127.0.0.1

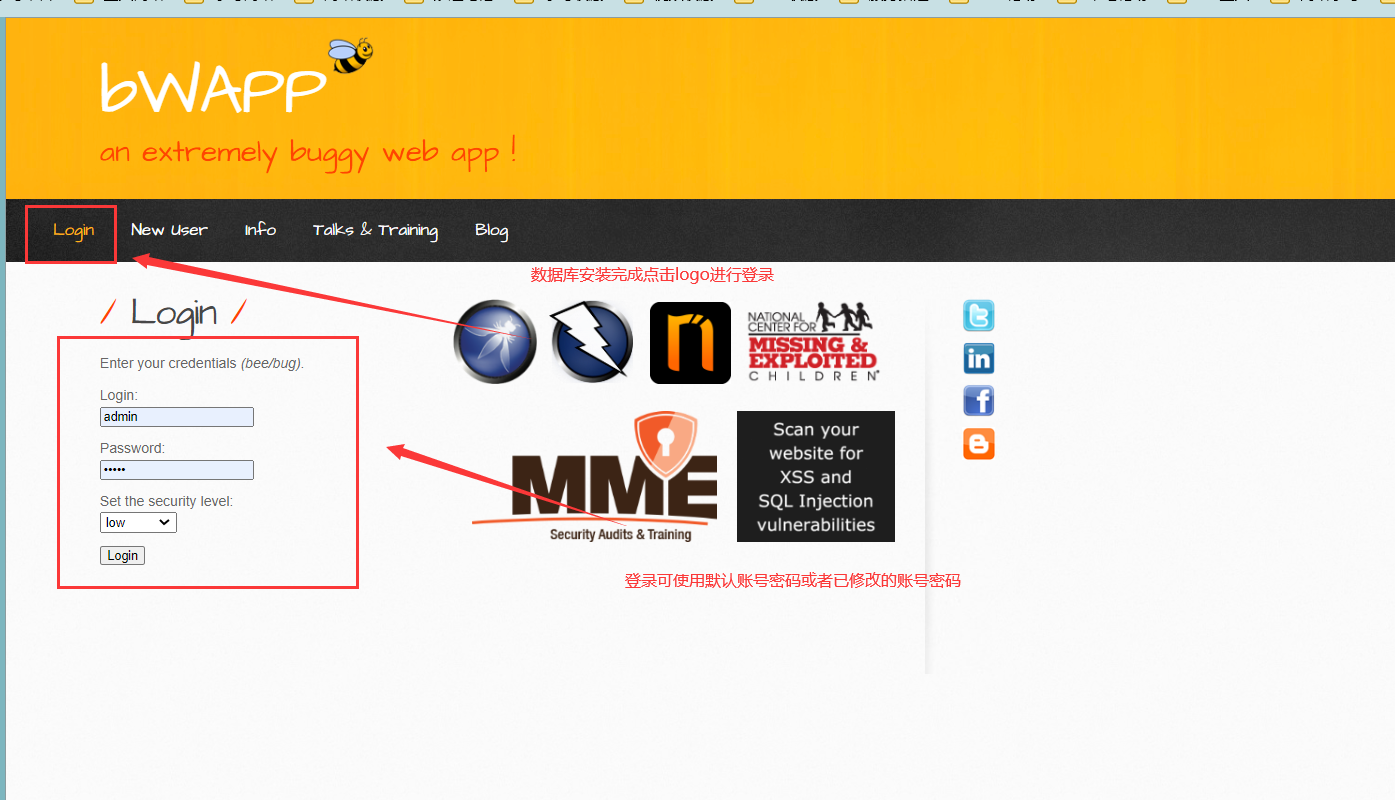


点击BWAPP可快捷跳转至登录界面

**第一次使用需要安装数据库数据**

[**http://127.0.0.1/bWAPP/bWAPP/install.php**](http://127.0.0.1/bWAPP/bWAPP/install.php)



**即可使用**