1. 实验原理

**1. Apache+MySql+PHP**

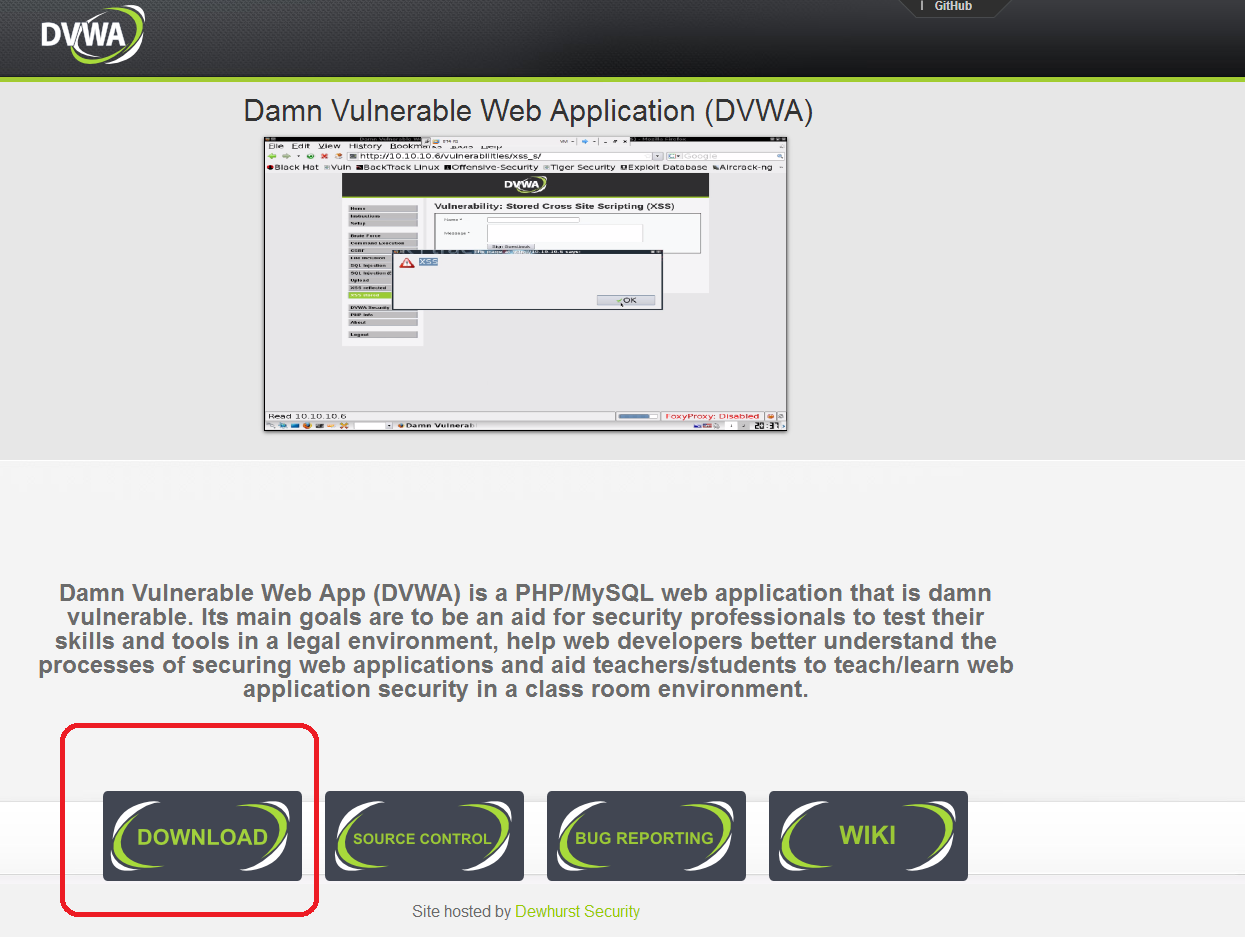
Apache(音译为阿帕奇)是世界使用排名第一的Web服务器软件。它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的Web服务器端软件之一。它快速、可靠并且可通过简单的API扩充，将Perl/Python等解释器编译到服务器中。

MySQL是一个关系型数据库管理系统，由瑞典MySQL AB 公司开发。MySQL 是最流行的关系型数据库管理系统之一，在 WEB 应用方面，MySQL是最好的 RDBMS (Relational Database Management System，关系数据库管理系统) 应用软件之一。

PHP（Hypertext Preprocessor）即“超文本预处理器”，是在服务器端执行的脚本语言，尤其适用于Web开发并可嵌入HTML中。PHP语法利用了C、Java和Perl，该语言的主要目标是允许web开发人员快速编写动态网页。PHP脚本程序主要应用于Web服务端开发，命令行和编写桌面应用程序。PHP支持和所有web开发语言之间的WDDX复杂数据交换。关于相互连接，PHP 已经支持了对Java对象的即时连接，并且可以透明地将其用作PHP对象。

**2.** **DVWA**

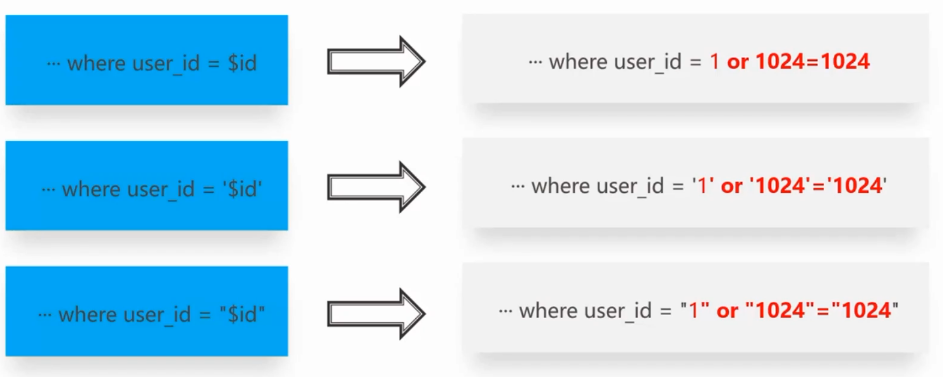
DVWA（Damn Vulnerable Web Application）是一款渗透测试的演练系统，如果需要入门，并且找不到合适的靶机，那推荐从DVWA入手。DVWA其实就是一个php网站，需要事先在自己的电脑上搭好Web服务器（Apache+PHP+MySQL），之后到DVWA的官网（http://www.dvwa.co.uk/）选择下载得到DVWA-master.zip，解压之后放到本地php的网站目录（如htdoc）。



Low级别SQL注入攻击的目标程序源代码



常见注入测试的POC



1. 实验环境

Windows操作系统，Apache+PHP+MySQL网站架构，DVWA脚本。

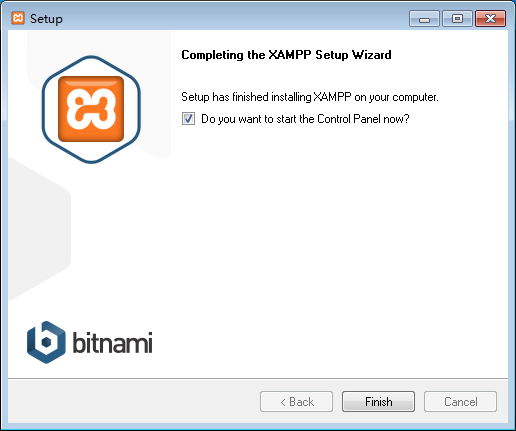
（也可以使用Linux操作系统，选择Linux对应的版本，需要自己去官方网站下载对应的程序）

1. 实验内容与步骤

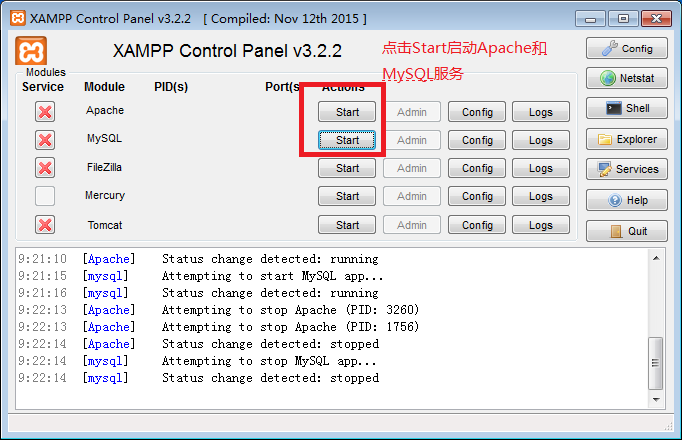
**任务一：在Windows 环境下搭建Web服务器**

1. 为了搭建Apache+PHP+MySQL的Web服务器环境，本实验按照DVWA的推荐，使用XAMPP一站式安装，可以到官方网站下载：https://www.apachefriends.org/index.html，或教师提供的安装软件
2. 之后安装程序，保持默认设置即可，可以看到下面界面。

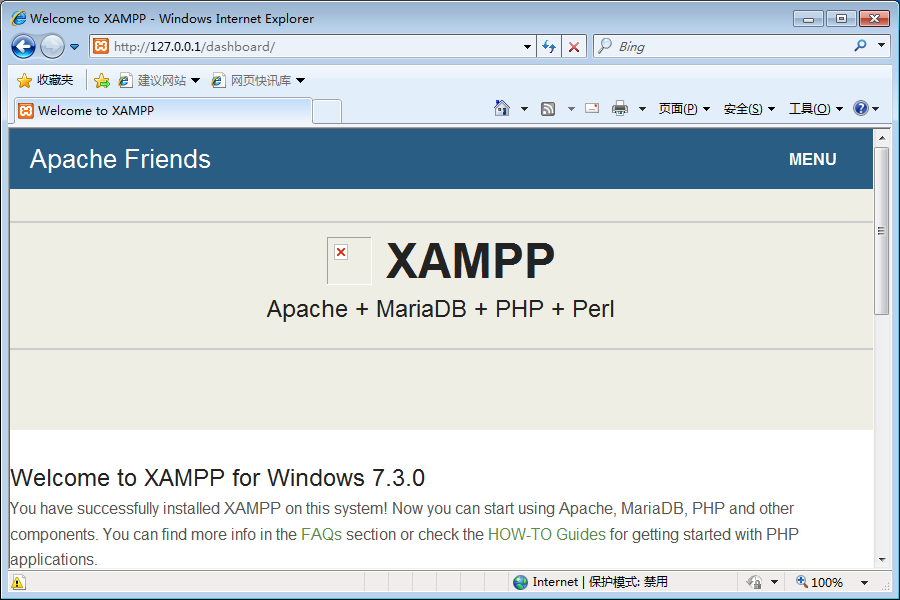
（尽量使用默认路径安装，不然有些服务需要更改配置）



1. 打开程序的主控面板，手动点击开启Apache和MySQL服务，这两个分别是Web服务器和数据库服务器。



1. 服务开启以后，打开一个浏览器，输入127.0.0.1，如果看到以下界面，说明软件和服务安装成功。



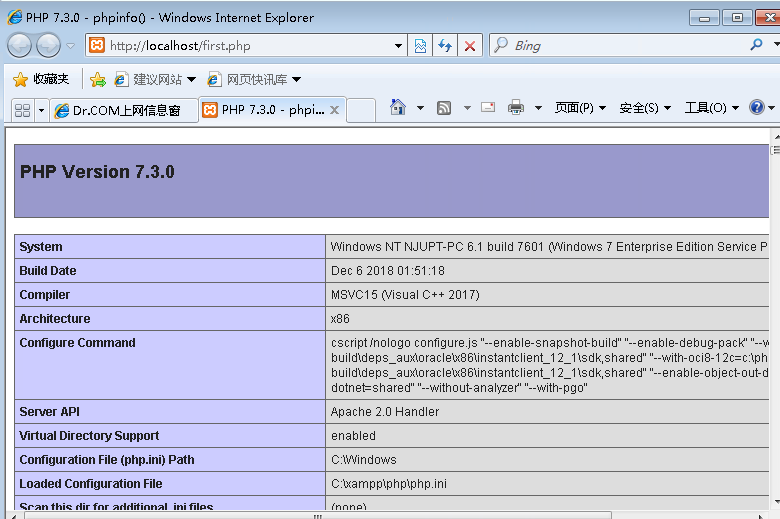
**任务二：测试PHP**

1. 找到Web网站的主目录，如果是默认安装，则是：C:\xampp\htdocs
2. 在该目录下，创建测试文件 first.php，用编辑器打开 first.php

编辑代码如下：

<?php  
phpinfo();  
?>

1. 访问http://localhost/first.php，可以看到下面界面，说明PHP安装成功，第一个PHP程序已经成功运行



1. 如果没有页面出行，可能是Apache服务没有启动，回到任务一的步骤（3），重启服务

**任务三：测试MySQL数据库**

1. 方式一：使用命令行模式，找到MySql所在目录，可以查看MySql的帮助命令进行操作，例如：

1、连接到本机上的MYSQL

首先打开命令行窗口，然后进入目录mysql\bin，再键入命令mysql -u root -p，回车后提示输密码。

如果刚安装好MYSQL，超级用户root是没有密码的，故直接回车即可进入到MYSQL中了，MYSQL的提示符是： mysql>

2、连接到远程主机上的MYSQL。假设远程主机的IP为：110.110.110.110，用户名为root,密码为abcd123。则键入以下命令：

mysql -h110.110.110.110 -u root -p 123;（注:u与root之间可以不用加空格，其它也一样）

* 1. 根据自己的学号，用create命令创建一个数据库，并截图，例如：

create database B19031614;，

* 1. 使用命令行模式创建数据库 first， 命令：create database first;

查看所有数据库, 命令：show databases;

连接数据库information\_schema，命令：connect information\_schema;

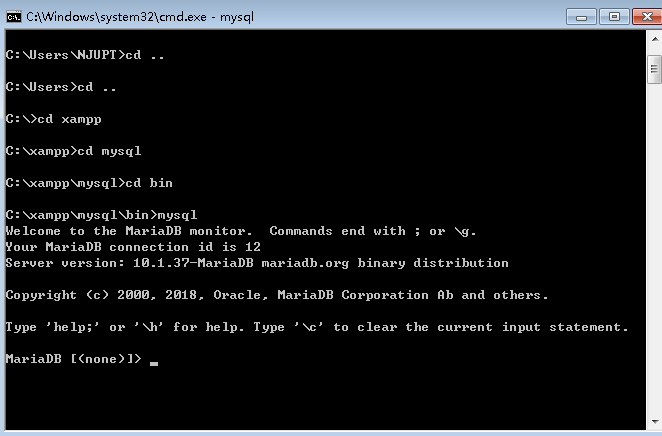
查看数据的所有表，命令：show tables;

查看表user\_privileges的内容：select \* from user\_privileges;

注：所有命令必须以；结尾

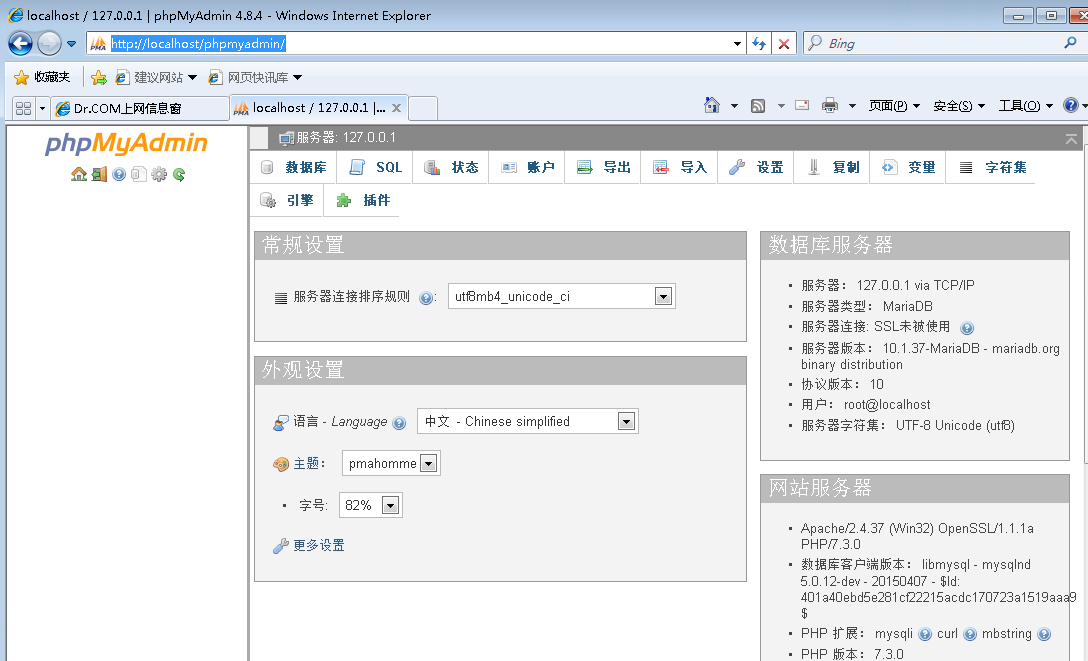
5、退出MYSQL命令： exit （回车）

4、其他命令类似于SQL语句，可以网上查询手册



1. 方式二：使用phpMyadmin管理数据库

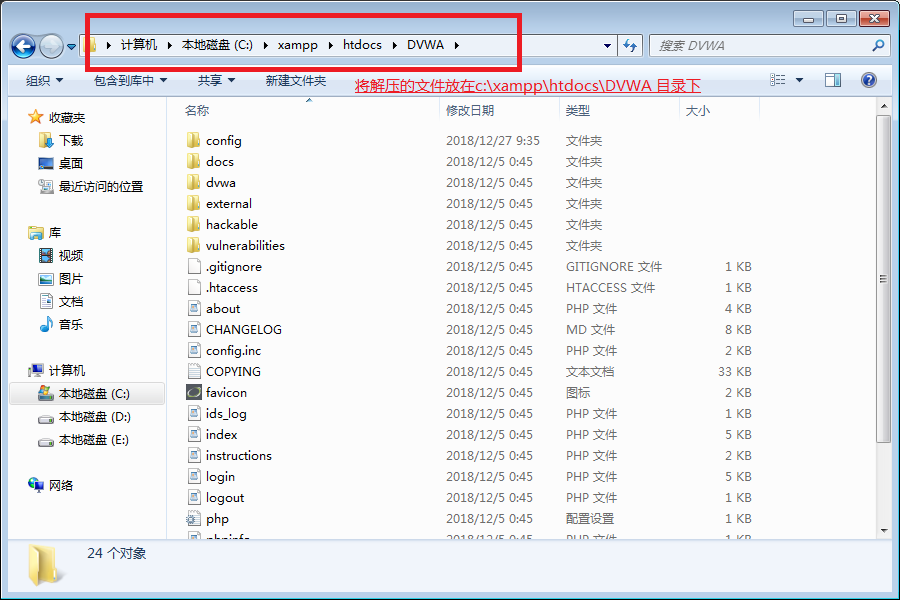
在本机打开浏览器，输入<http://localhost/phpmyadmin/>，可以看到以下界面



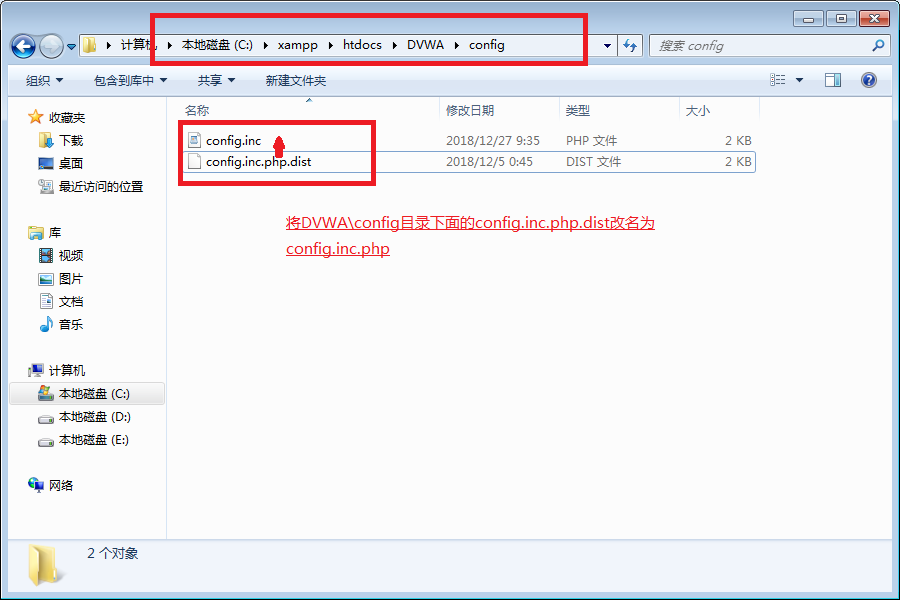
1. 在phpMyadmin图形界面下，尝试完成（2）步骤中类似的操作（除了不需要创建first数据库）

**任务四：安装DVWA软件**

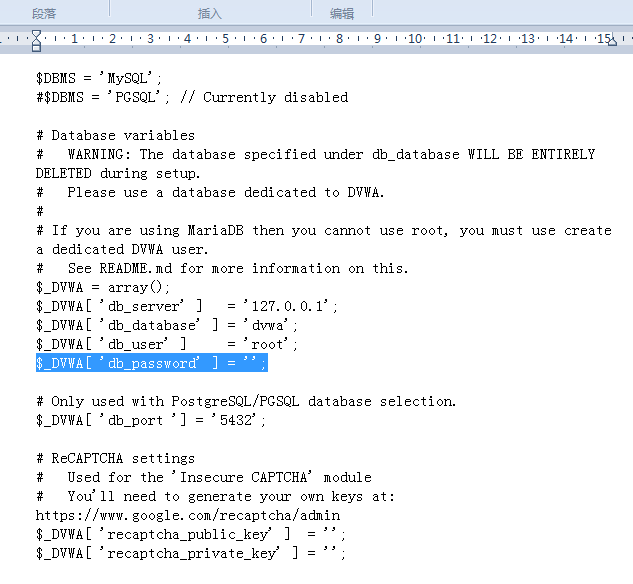
1. 到DVWA的官网（http://www.dvwa.co.uk/）选择下载得到DVWA-master.zip，或者使用教师提供的软件。解压后，大部分文件是PHP和配置文件，在 c:\xampp\htdocs目录下新建一个DVWA文件夹，把刚才解压的所有文件放到该目录下。注意，htdocs目录既是网页http://127.0.0.1访问的根目录，如果要访问DVWA，使用网址 http://127.0.0.1/DVWA即可，如果自己更改目录名和结构，自行更改访问网址。可以先看一下README文件。



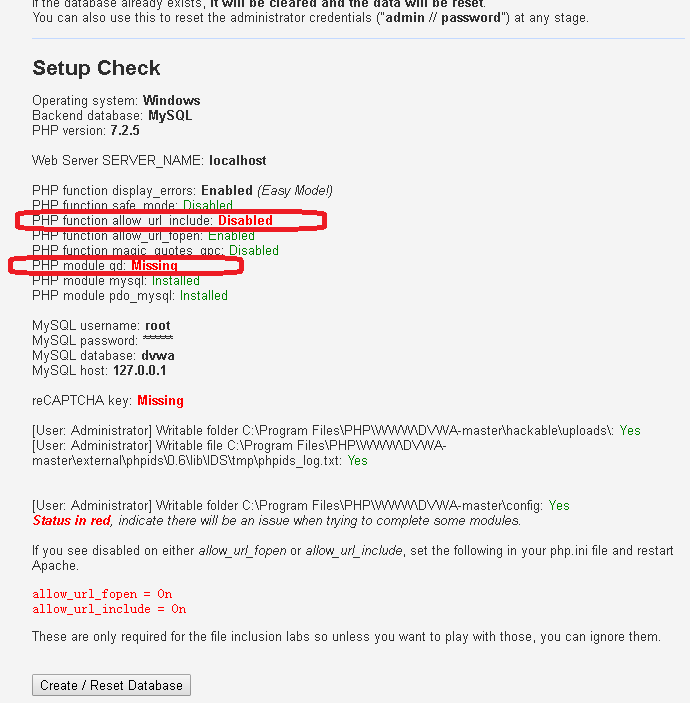
1. 在DVWA的config目录下找到配置文件，按图中提示修改。

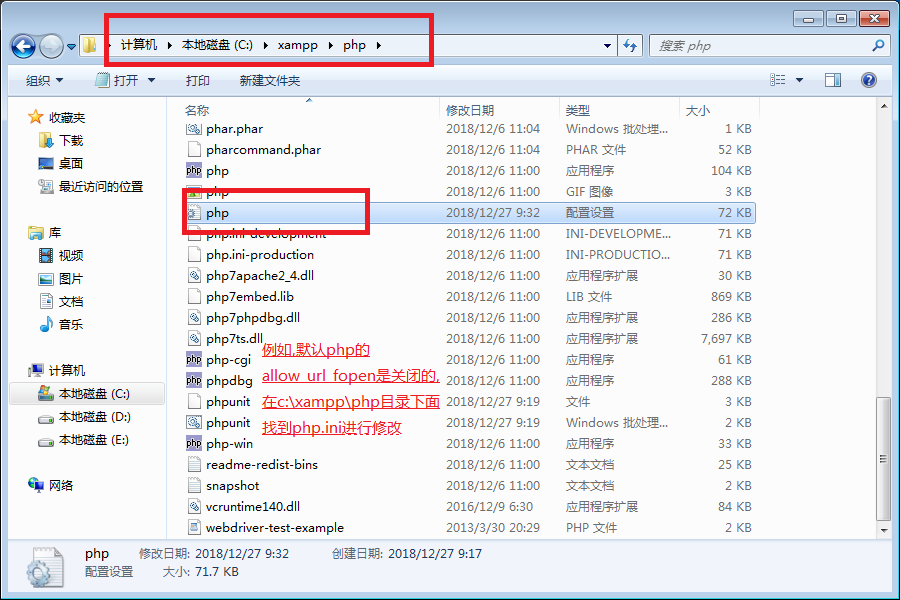


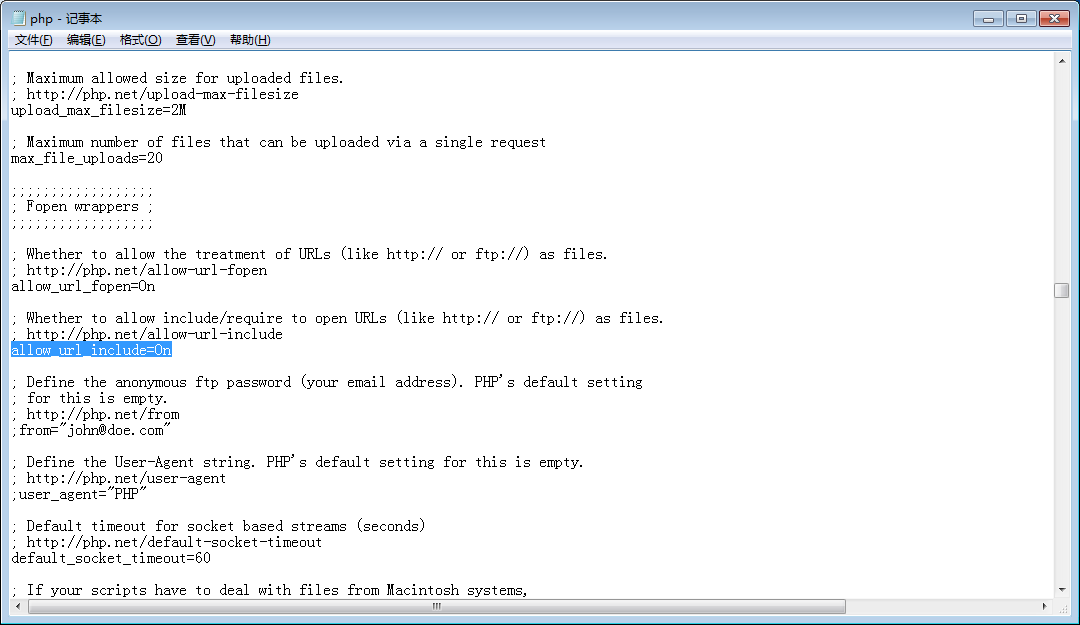
1. 用文本编辑器（如记事本）打开刚才改名的config.inc.php文件，把数据库的密码改为空（因为XAMPP默认安装的数据库密码为空）



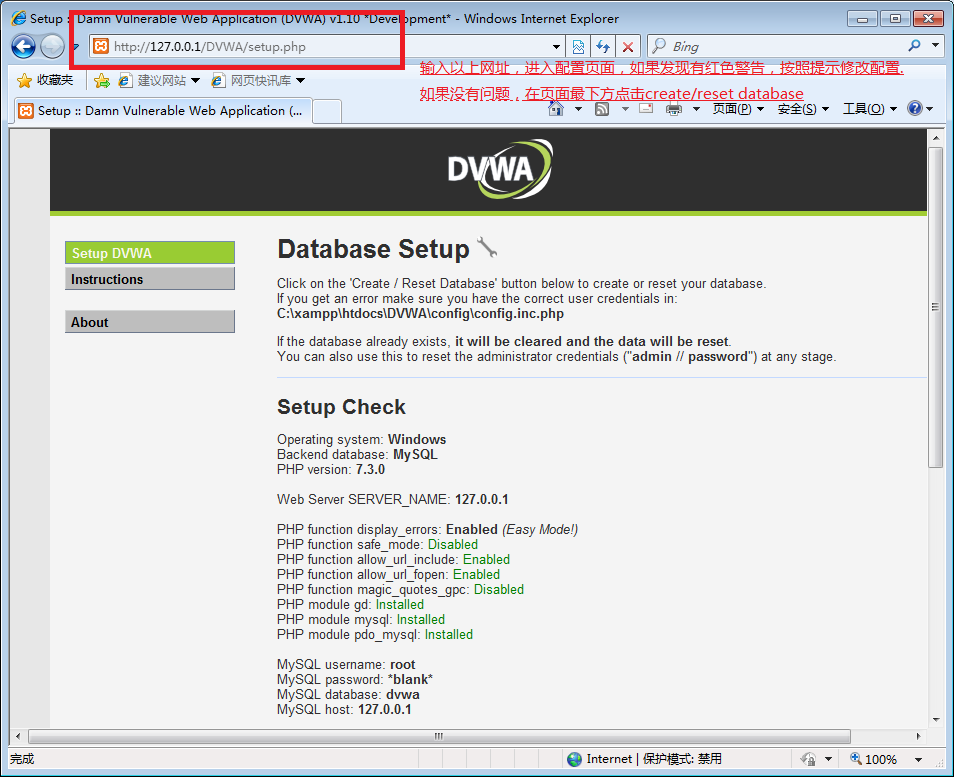
1. 打开http://127.0.0.1/DVWA/setup.php页面，进行配置，如果出现红色错误，则对php.ini文件进行修改。



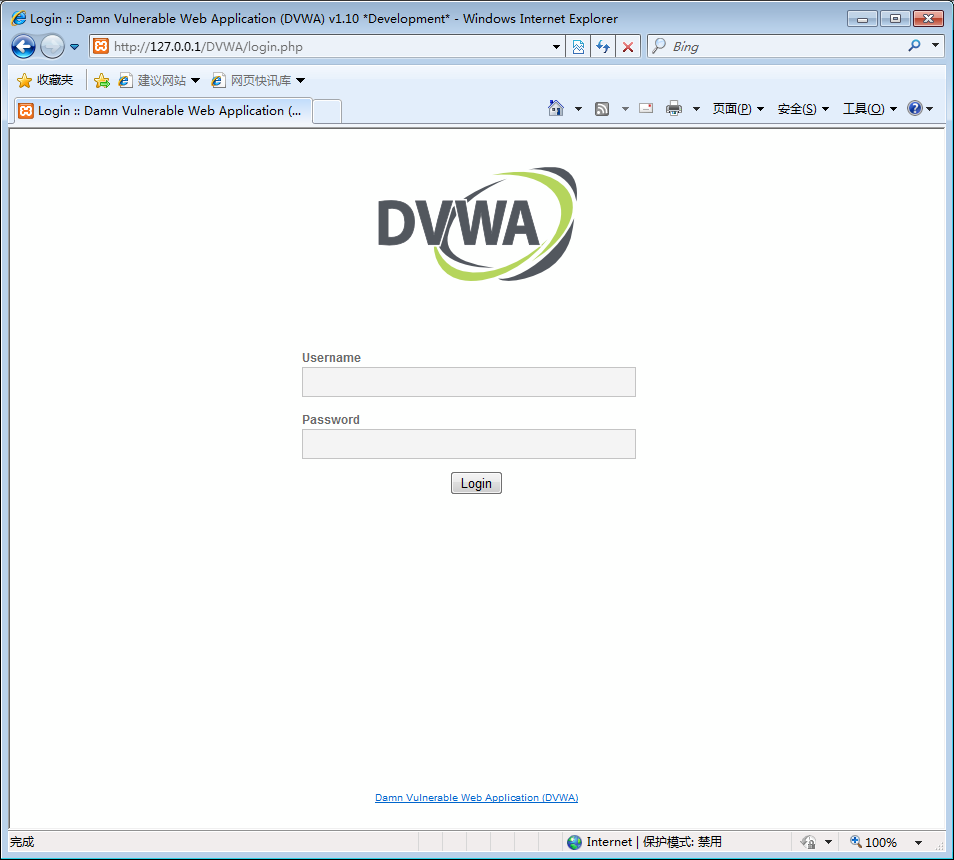




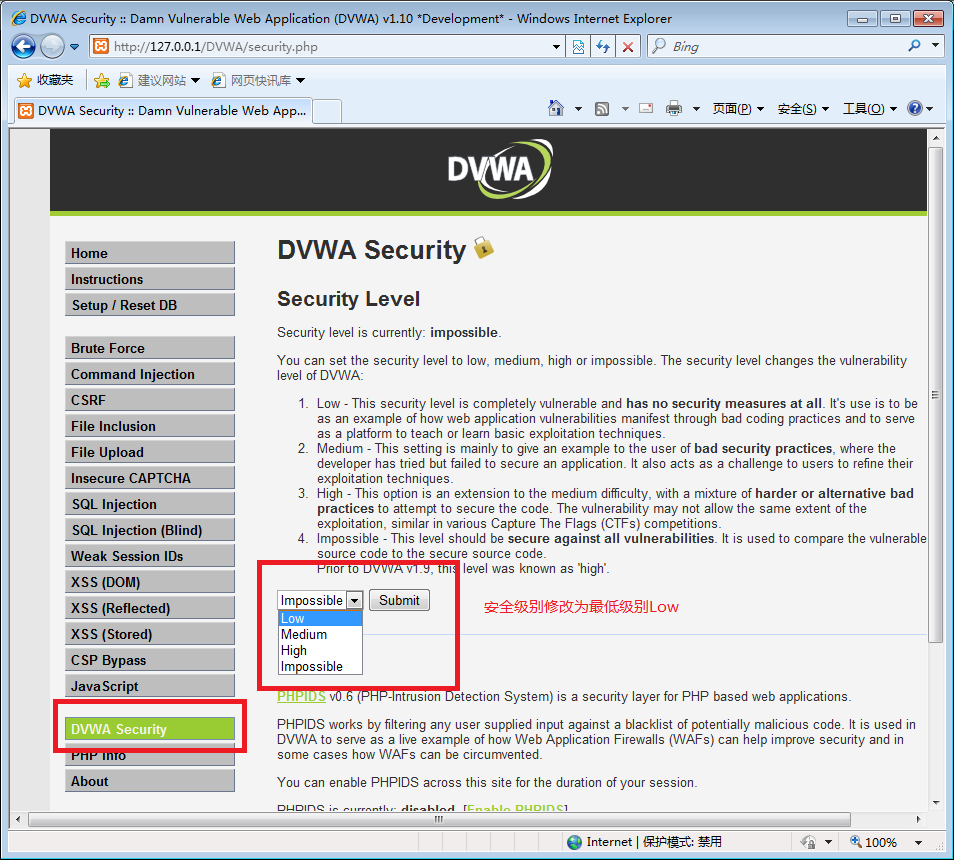
1. 如果http://127.0.0.1/DVWA/setup.php页面中没有红色提示，说明没有问题，可以点击页面最下方的create/reset database的按钮，生成DVMA必须的数据库。

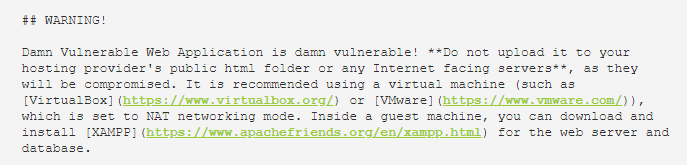


1. 配置完成后，打开http://127.0.0.1/DVWA/login.php，出现下面页面，用户名是admin，密码是password。如果能成功进入，说明这套渗透测试的演练系统已经搭建成功，可以尝试攻防演练，我们后期也会使用到。



1. 初学者一般把安全级别设为最低级low，再进行各类渗透实验。





但不要把DVWA放在外网上，服务器会被攻击。

1. 再次进入phpMyadmin，打开浏览器，输入<http://localhost/phpmyadmin/>，查看数据库的变化。
2. 提交的实验报告
   1. 完成任务三步骤（2），查看表user\_privileges的内容并截图记录。
   2. 完成任务四步骤（8），截图记录并回答实验报告里面的问题。

统一由各班学习委员收齐后，课程结束一周内，压缩打包发送到我的邮箱： 18951896489@163.com