作业 2 内容

基础部分：

1. 部署sqli_labs 靶机
2. 尝试操作和复现课程 sql 注入相关内容（dvwa 和sqli_labs 等）

实践部分：

1. 漏洞通报学习

   附件：sql 注入 通报.rar

   内容：

   结合课程学习内容，阅读和分析理解漏洞通报内容

2. SQL 注入攻击日志分析

   根据提供的附件access.log，自行分析和检索理解日志结构，并分析攻击的过程

提交部分：

1. 实践部分 1：

   针对漏洞通报中的内容，结合课程内容，回答如下问题

   0. 文中的 PoC 是什么意思，另外自行扩展学习两个概念：exp、payload 是什么意思，描述三者差别和关系

   1. 根据漏洞通报中的信息，详述漏洞的成因是什么，结合课程内容，判断利用方式属于课程中哪种sql 注入方式（Union,报错,boolean 盲注,时间盲注），并解读说明使用的注入语句含义

   2. 根据漏洞通报中的信息，写出获取当前数据库中第三个表名的利用请求代码

   3. 仔细观察漏洞通报中的信息，尝试分析猜测后台数据库中用户口令可能的保存方式，并通过自主学习叙述这种保存方式的目的和作用

2. 实践部分 2：

   根据对 access.log 的分析，结合课程内容，回答如下问题，并说明分析过程（大概步骤的截图等，如有使用自行编写的代码，可以附上代码）

   1. 结合课程内容，攻击过程采用的注入方式是什么？
   2. 攻击过程获取的 flag 的数据库名、表名和列名分别是什么？
   3. 攻击过程最终获取的 flag 字符串是什么？格式为 flag{XXXXXXX}