**SQL注入攻击**

**根据课程第6讲SQL注入攻击中相关内容，进行实践，并记录实践过程并说明攻击每一步具体操作的含义和目的。**

**实验环境：DVWA**

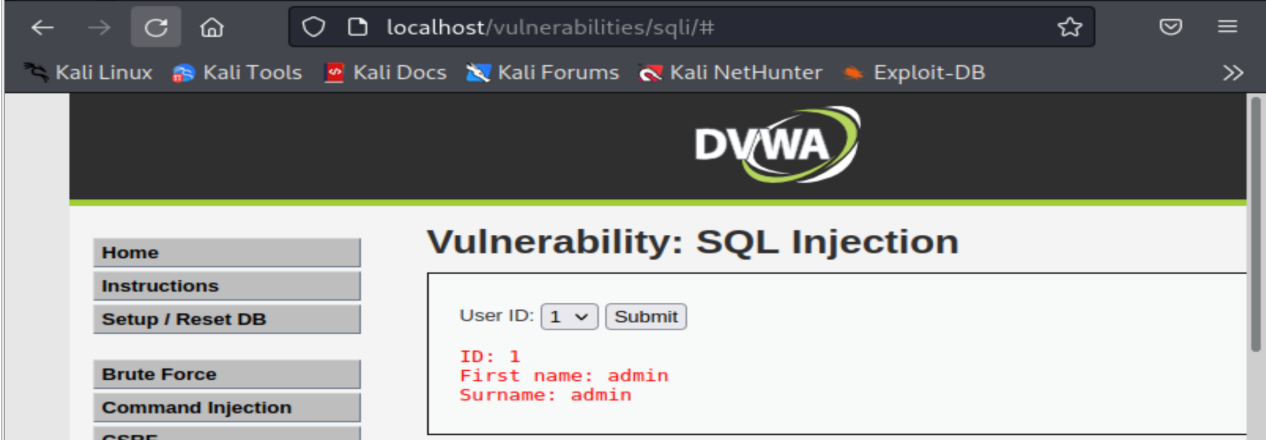
**实验内容：**

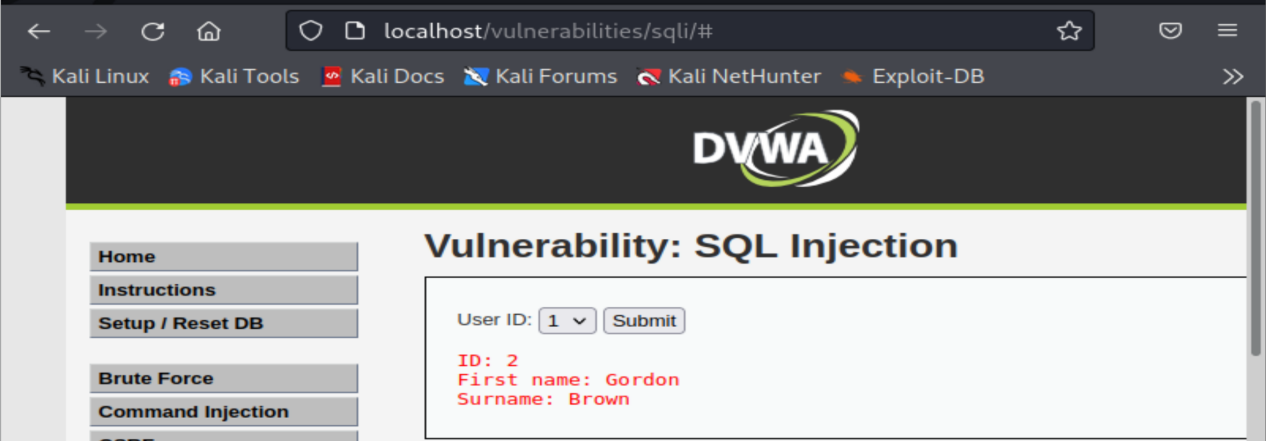
**1. 完成SQL注入，探测数据库名、用户名、所有表名、表中的字段名（Vulnerability：SQL Injection），Security Level: medium、high；**

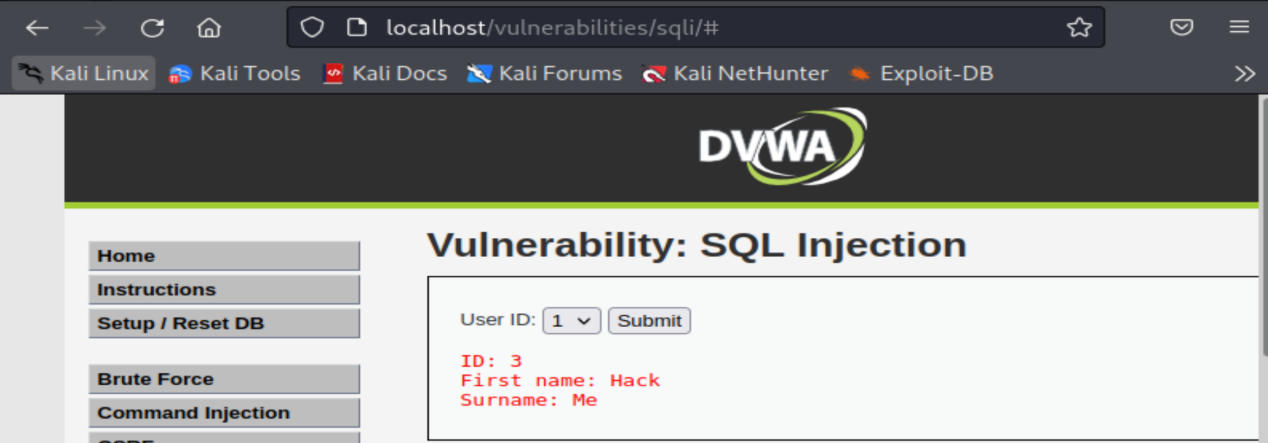
Medium：

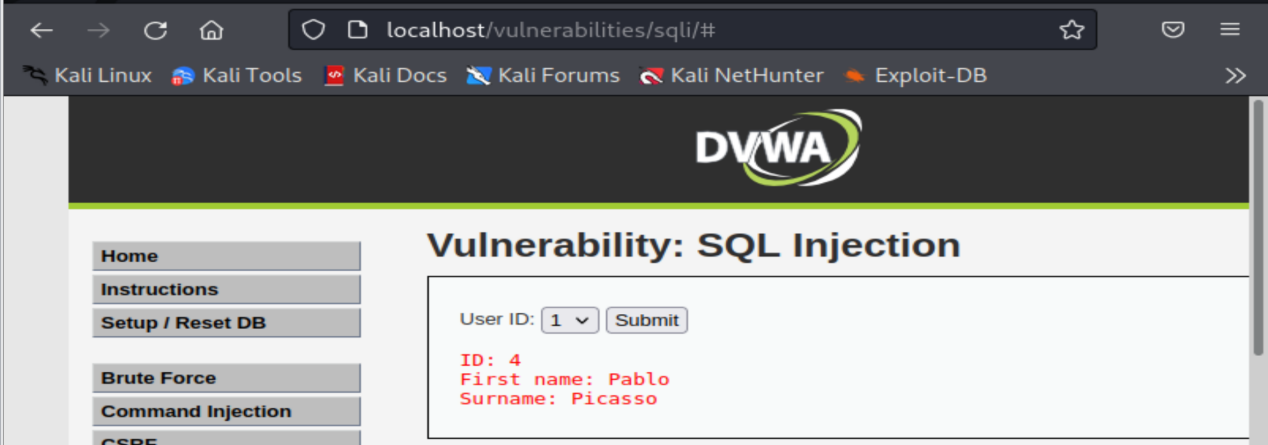
1. 选择不同的User ID，并点击Submit。

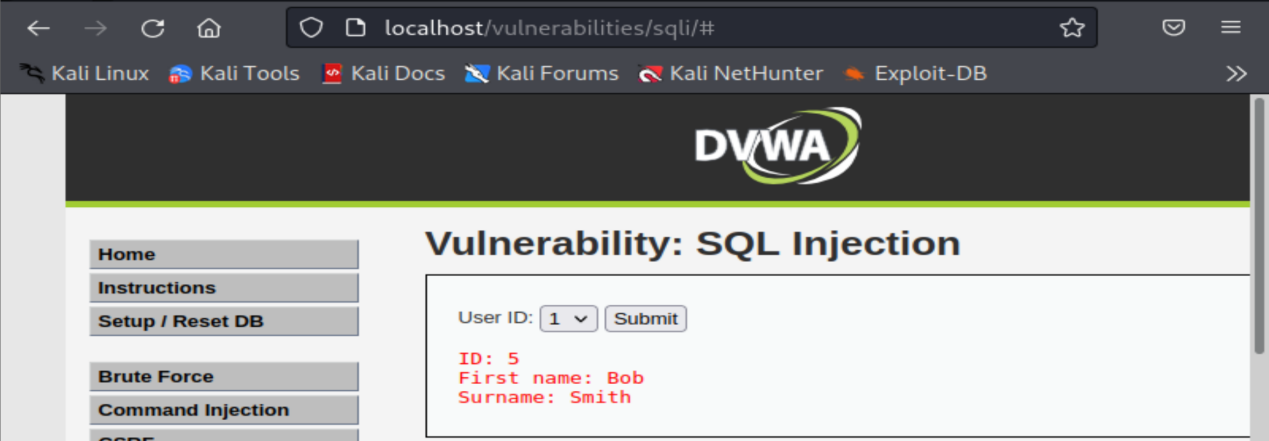
2. 得到不同的用户名。





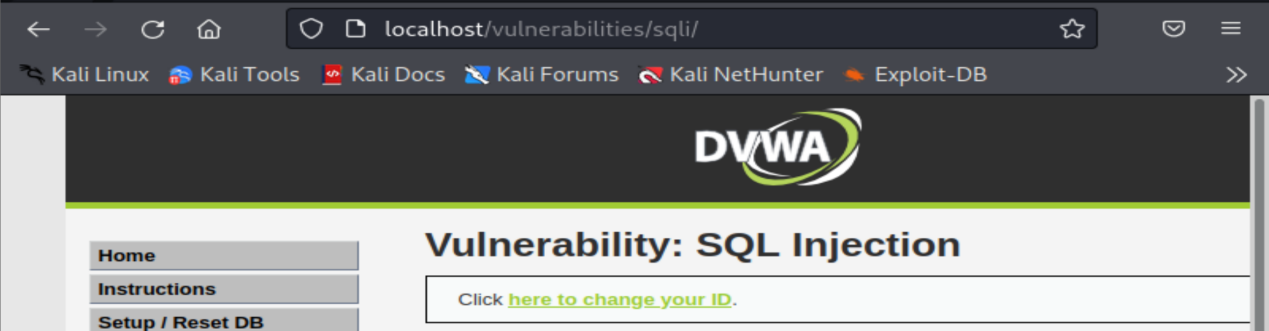




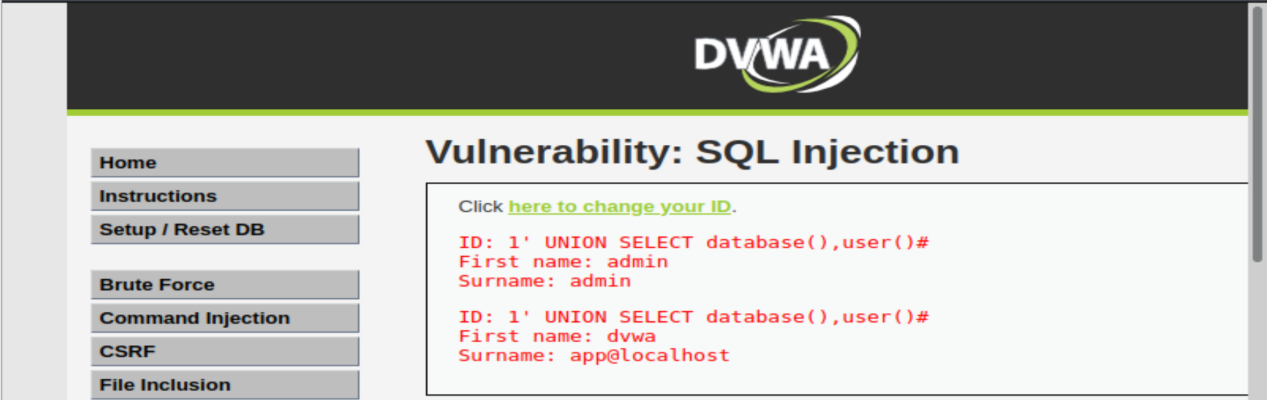


High：

1. 点击进入



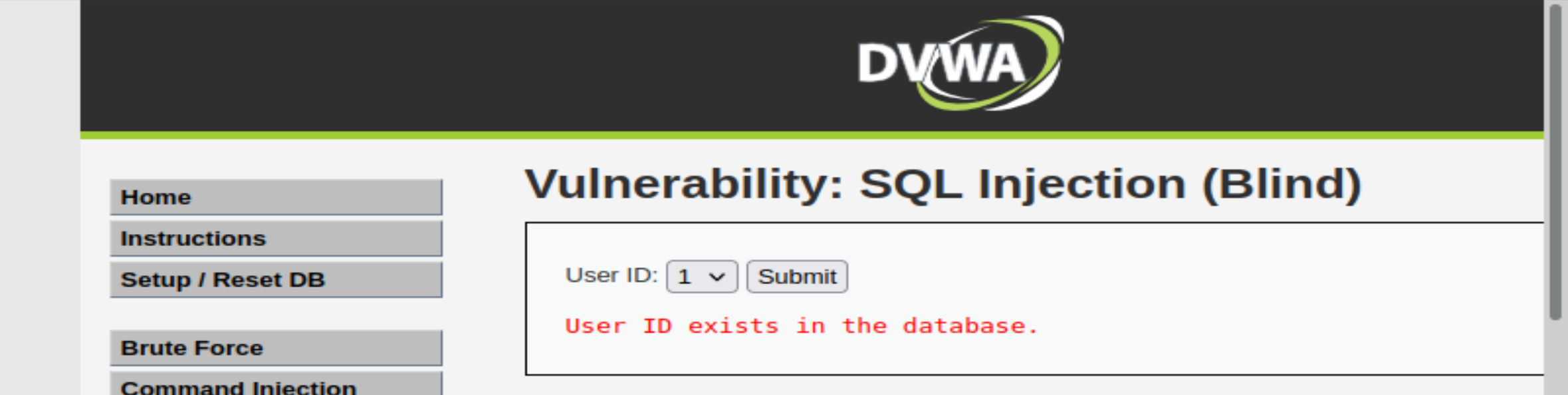
1. 输入1' UNION SELECT database(),user()#



1. 输入

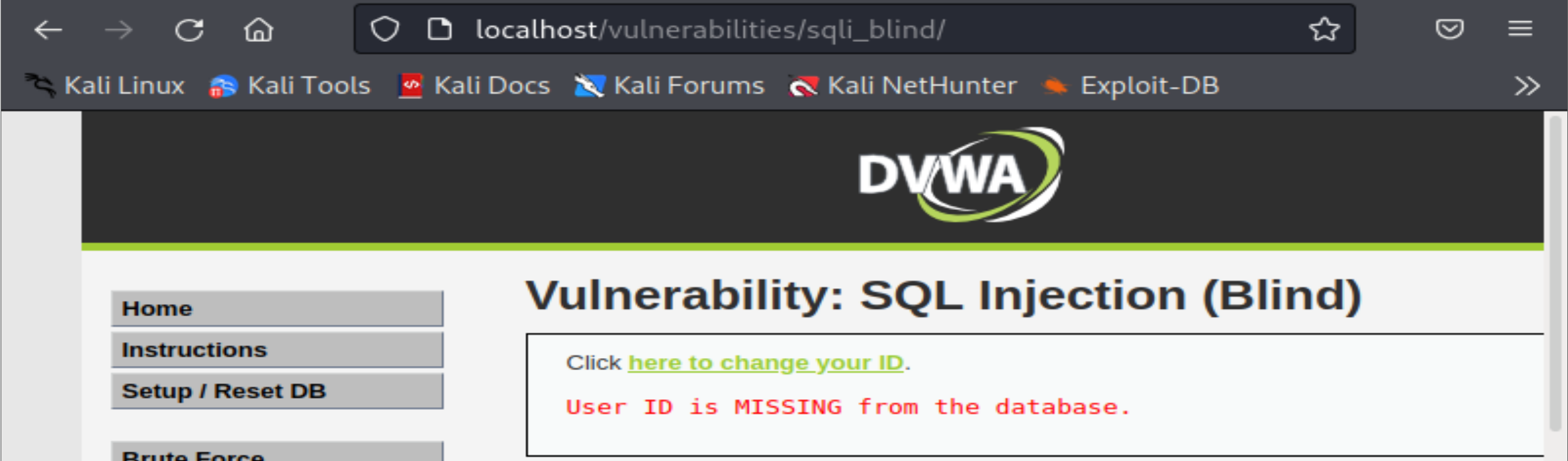
**2．完成SQL盲注攻击，猜测当前数据库名长度（Vulnerability: SQL Injection（Blind）），Security Level: medium、high；**

Medium：选择不同User ID

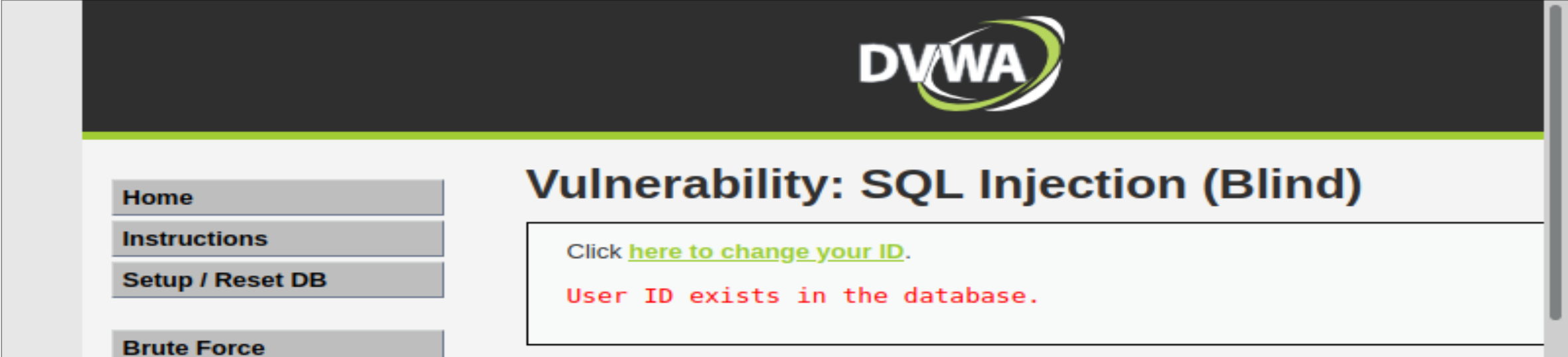


High：

输入1. 1‘ and length(database())>5#



1. 输入1‘ and length(database())>3#



说明长度为4

**3. 完成brute force，Security Level: medium、high；**