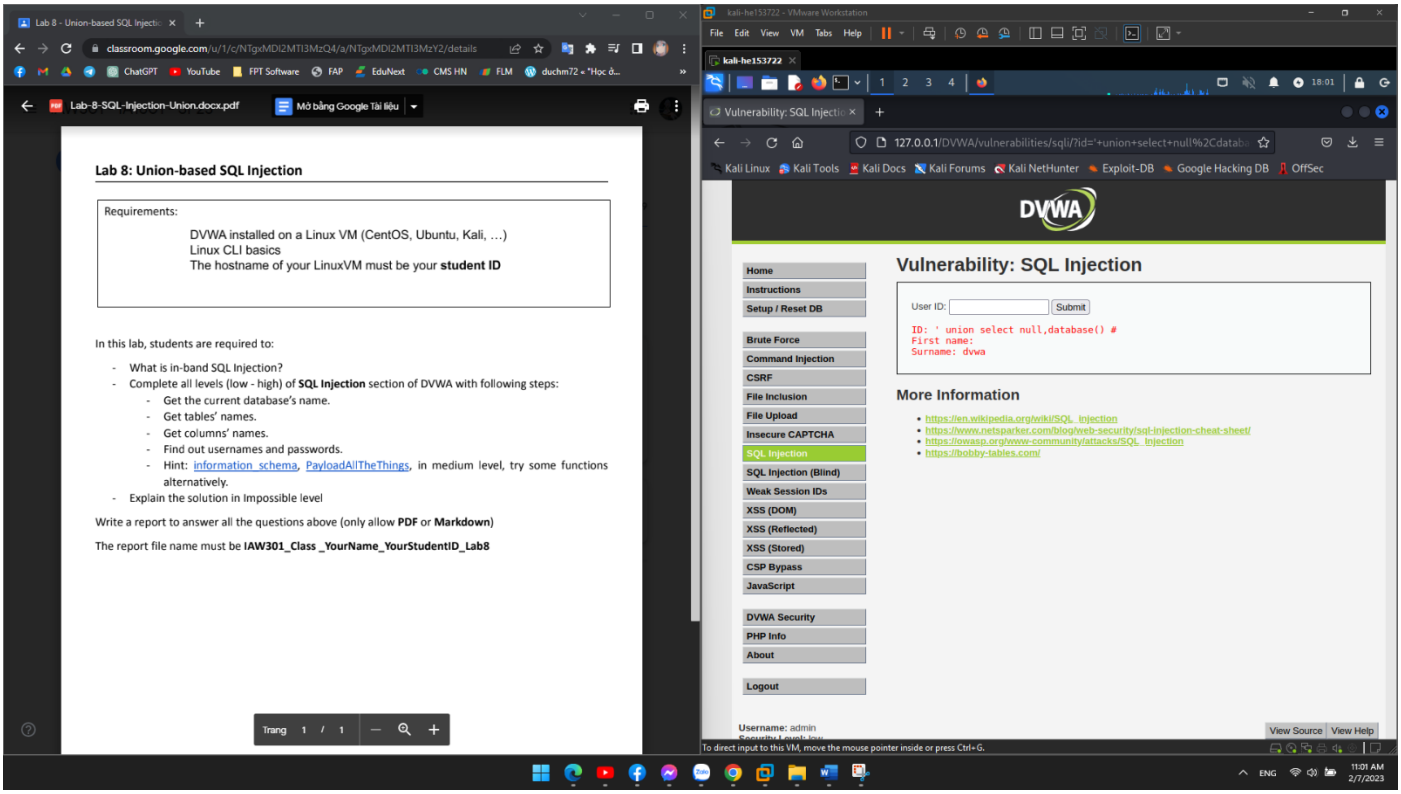
Lab 8: Union-based SQL Injection

What is in-band SQL Injection?

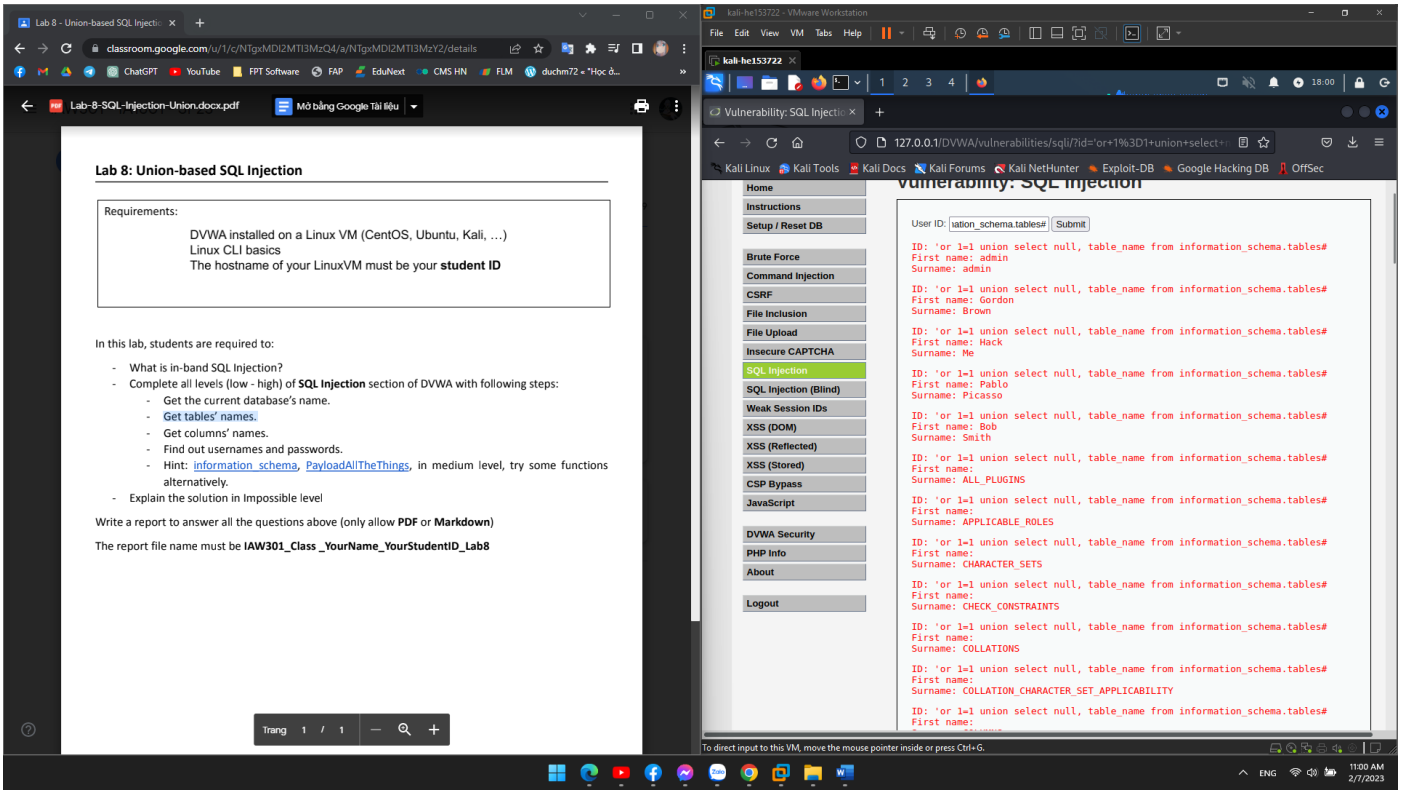
In-band SQL injection is a type of SQL injection attack where the attacker can extract data from a database by sending SQL commands through the same channel used by the application to communicate with the database. This type of attack is characterized by the attacker being able to directly observe the results of their injected commands in the application's responses, typically in the form of error messages or data returned from the database.

LOW LEVEL

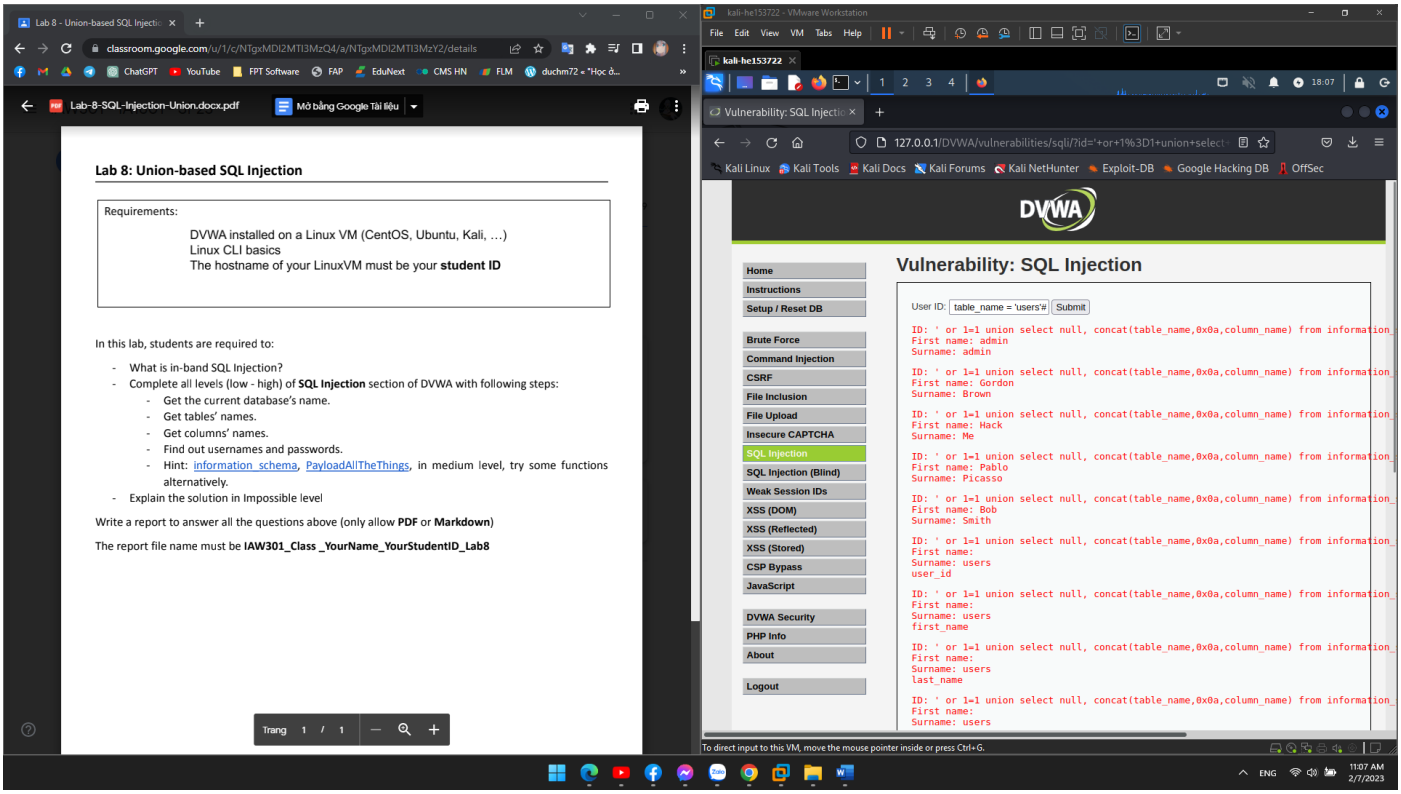
database’s name



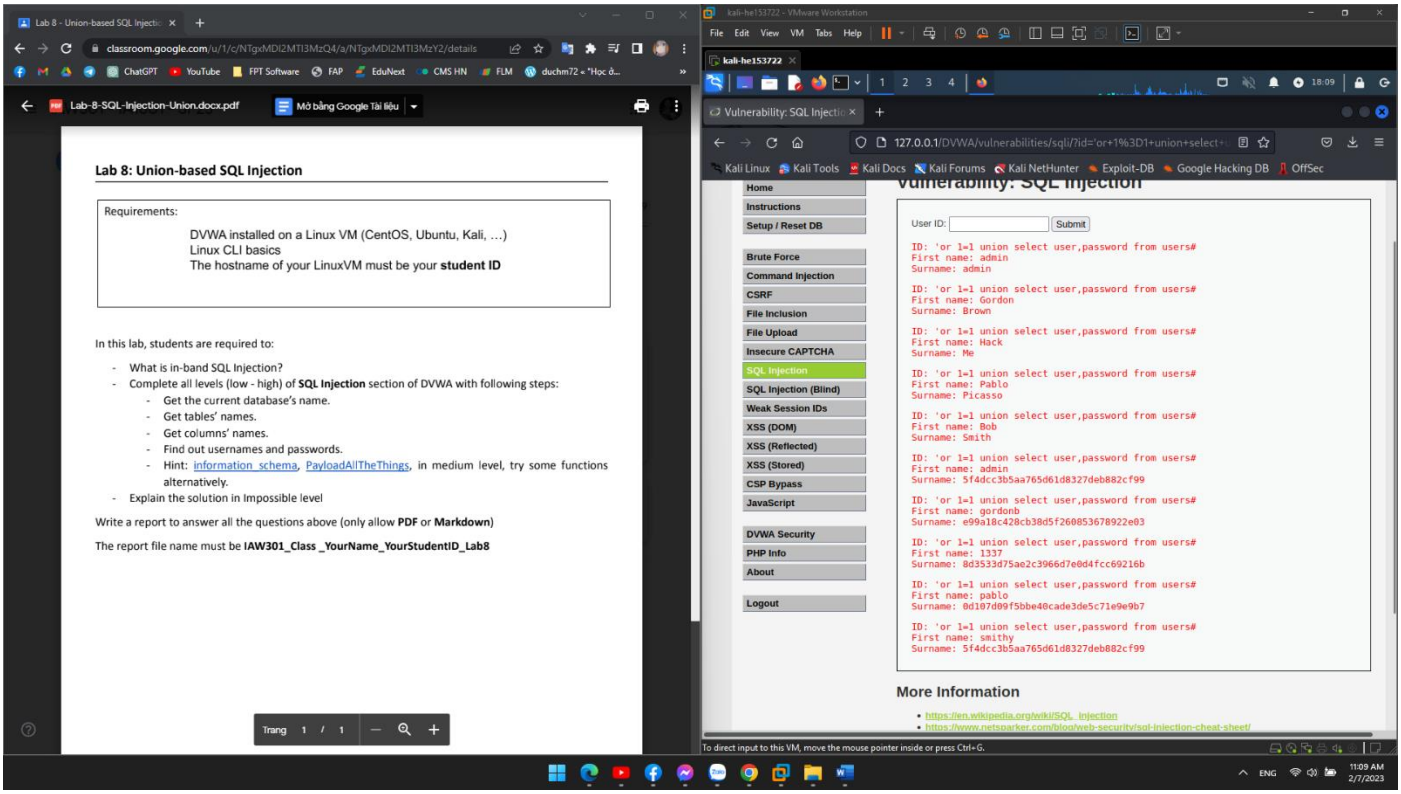
tables’ names



columns’ names

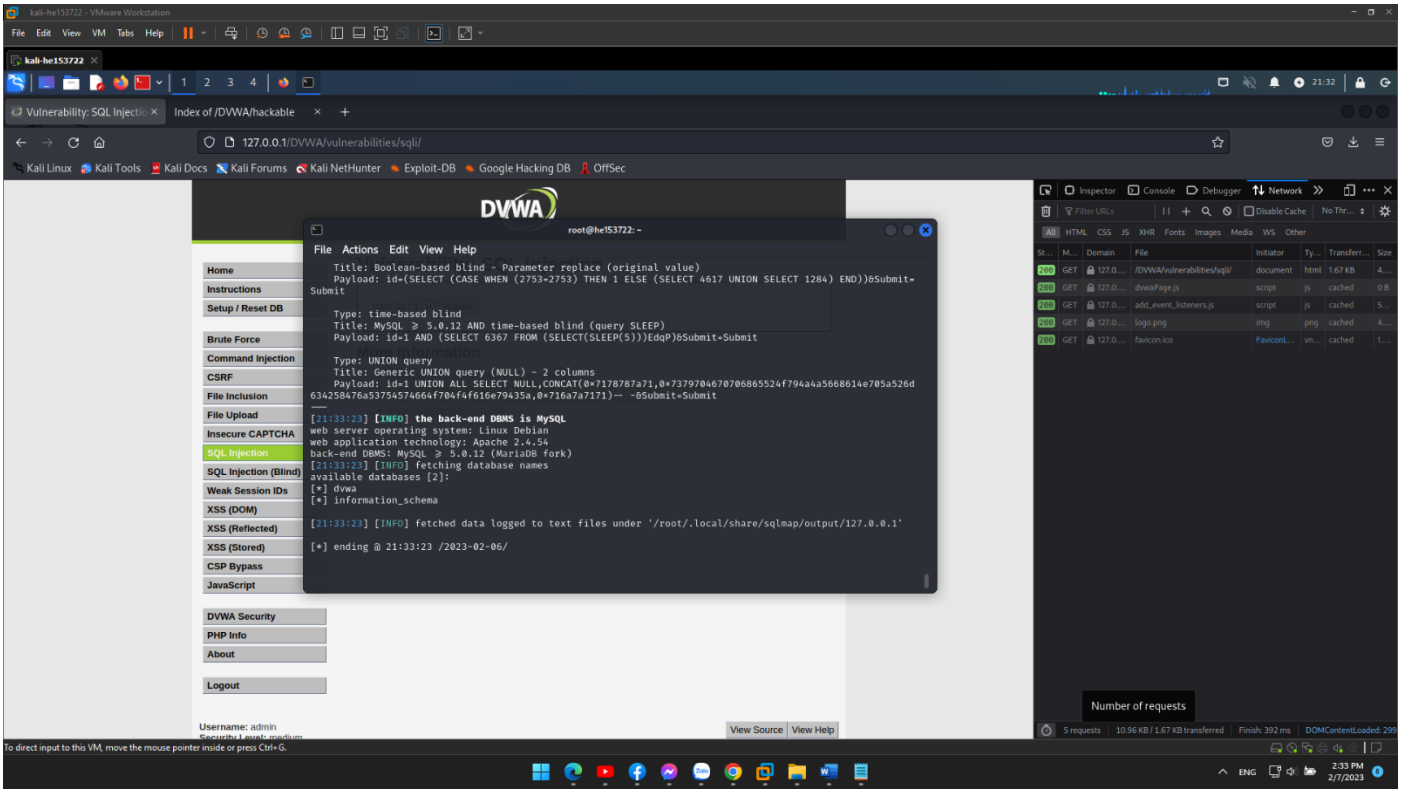


usernames and password

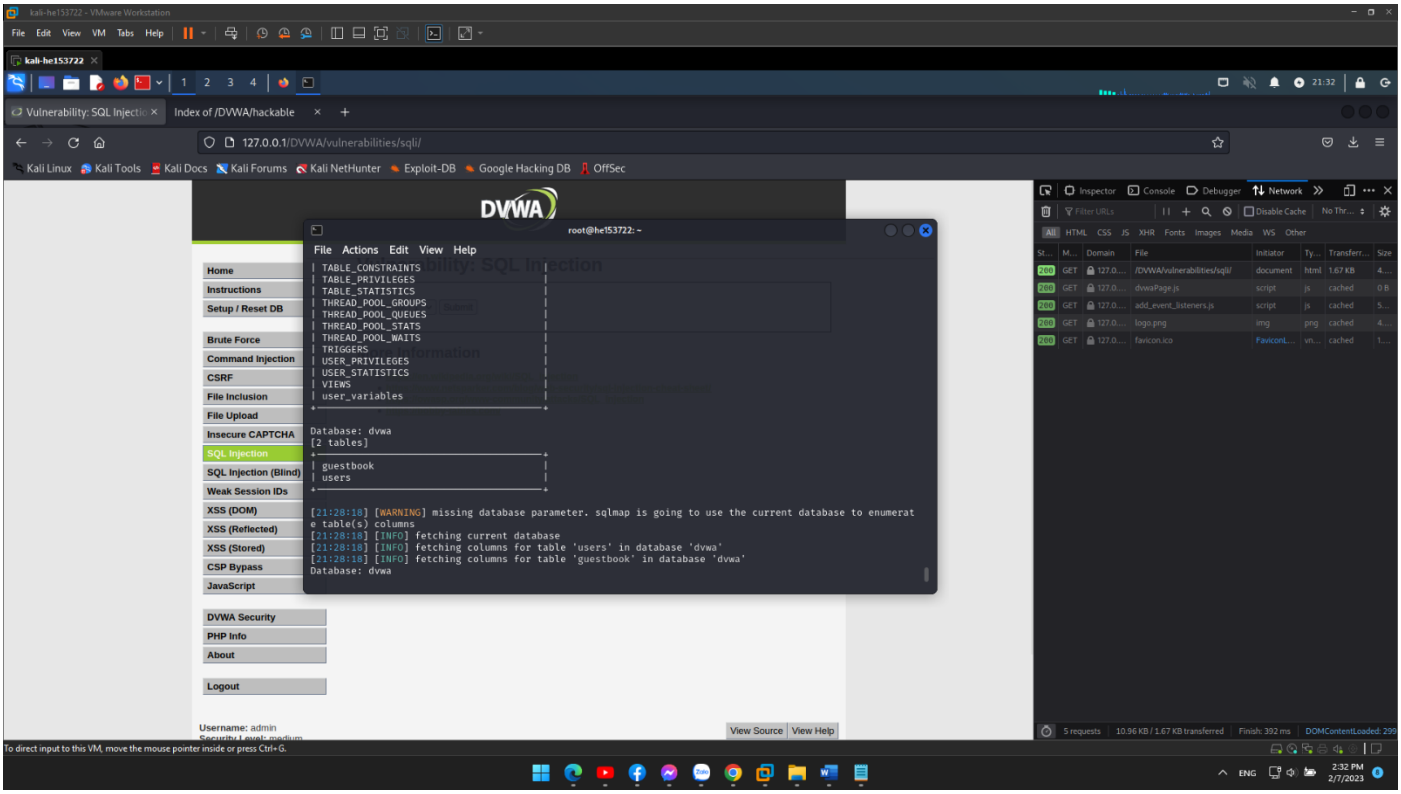


MEDIUM LEVEL

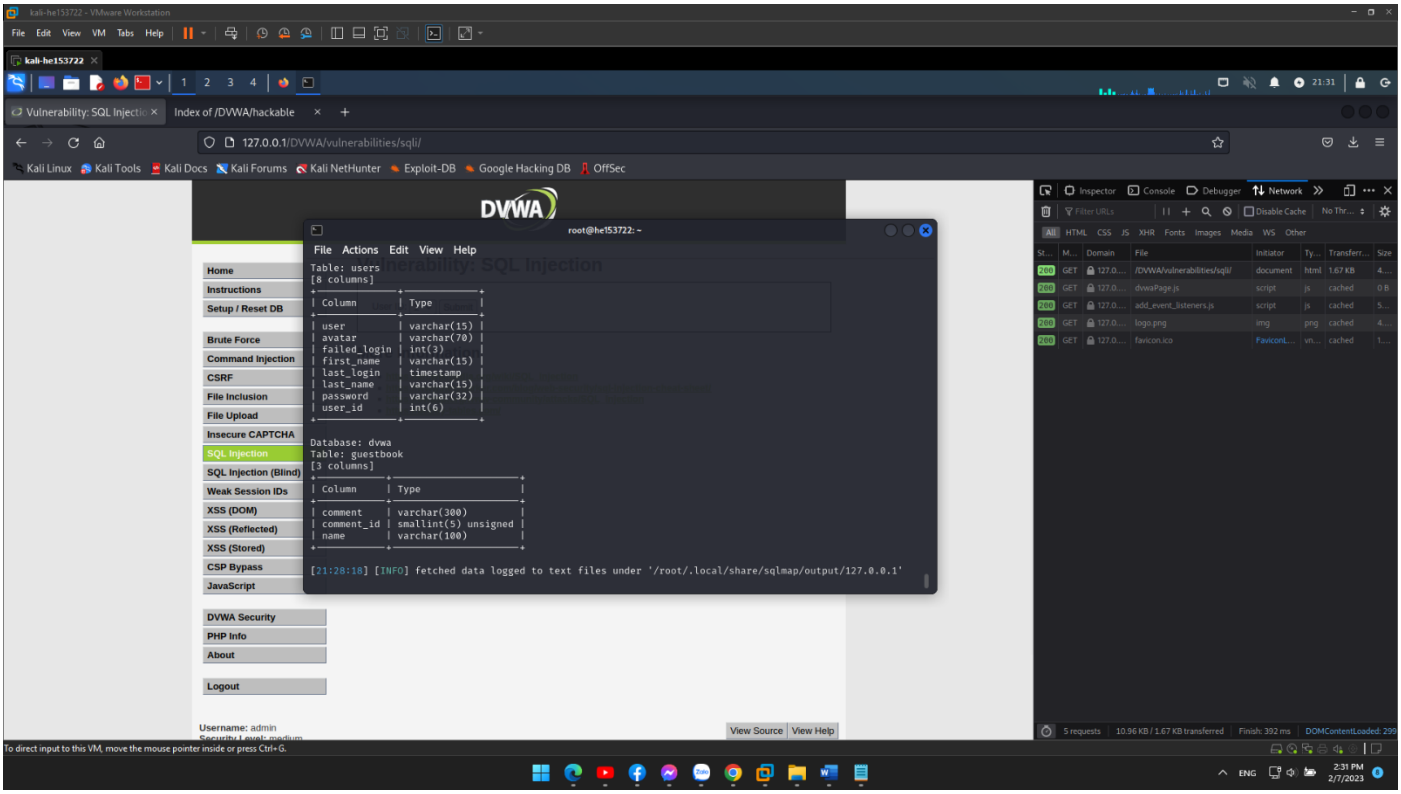
database’s name



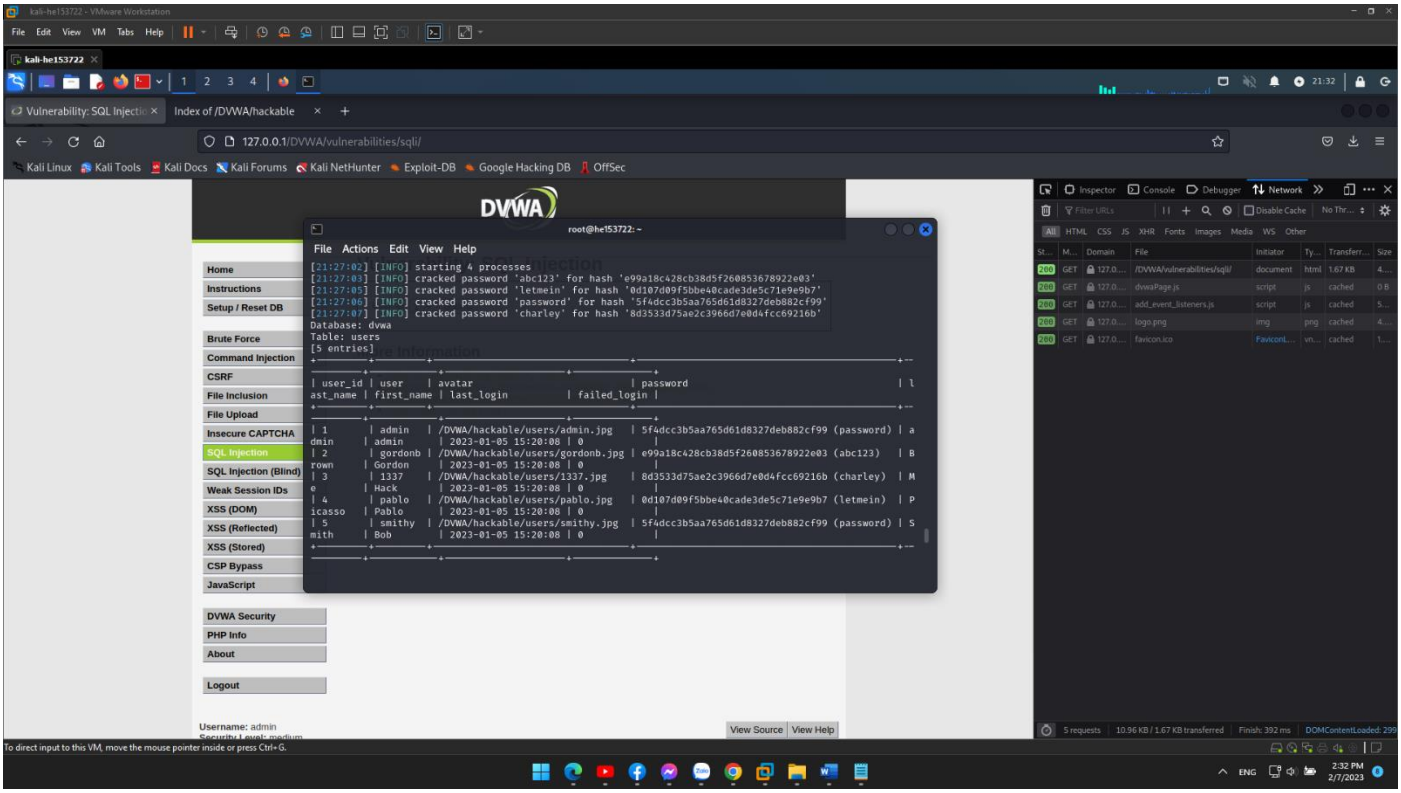
tables’ names



columns’names

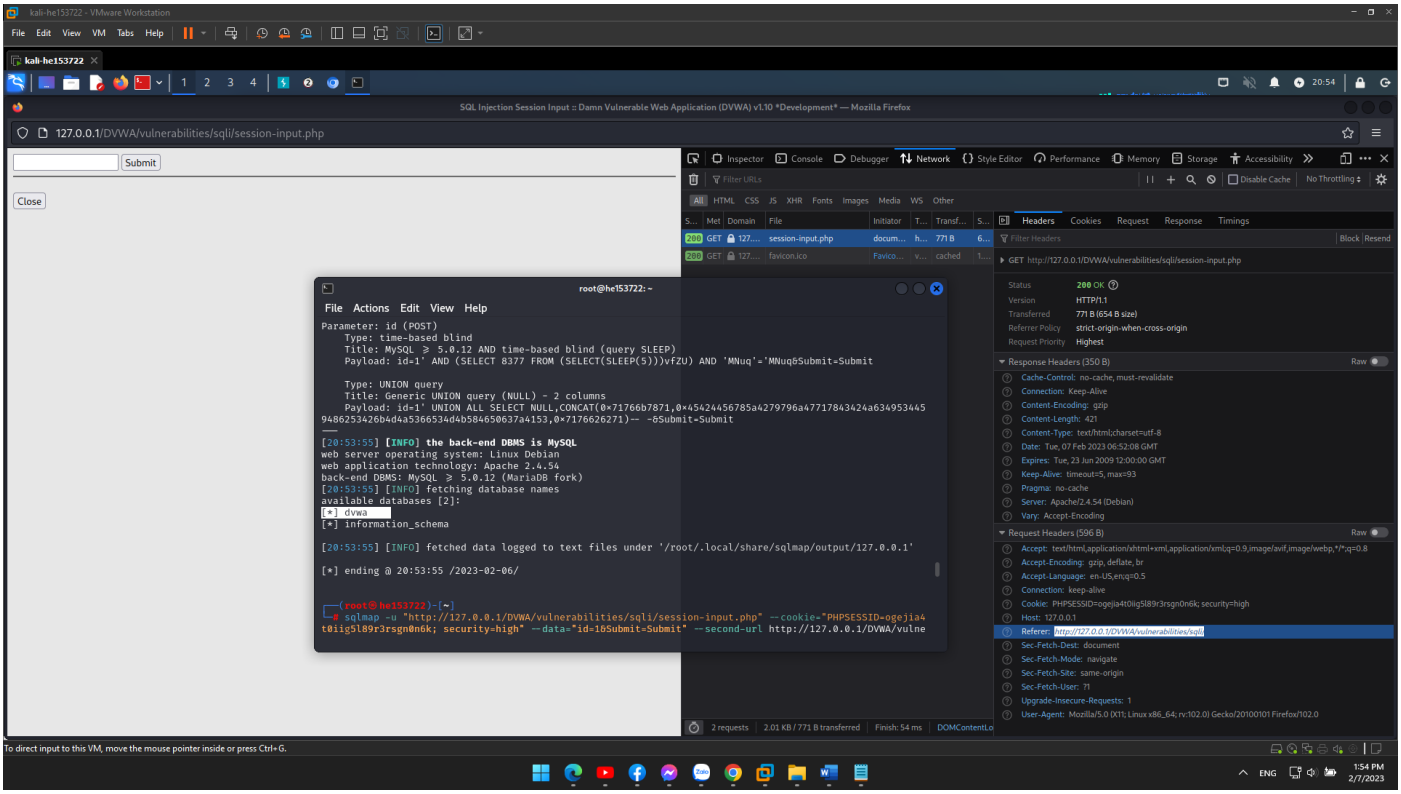


usernames and password

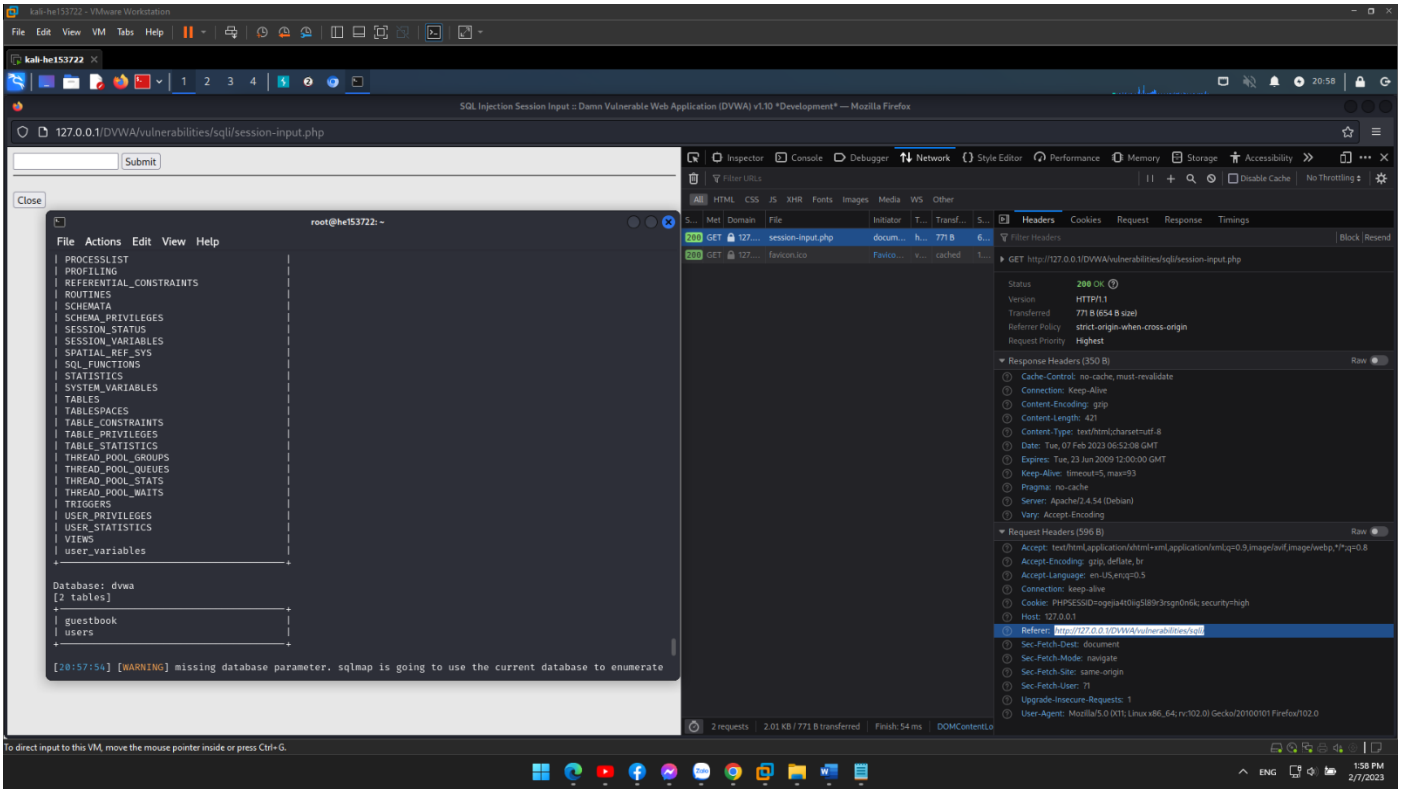


HIGH LEVEL

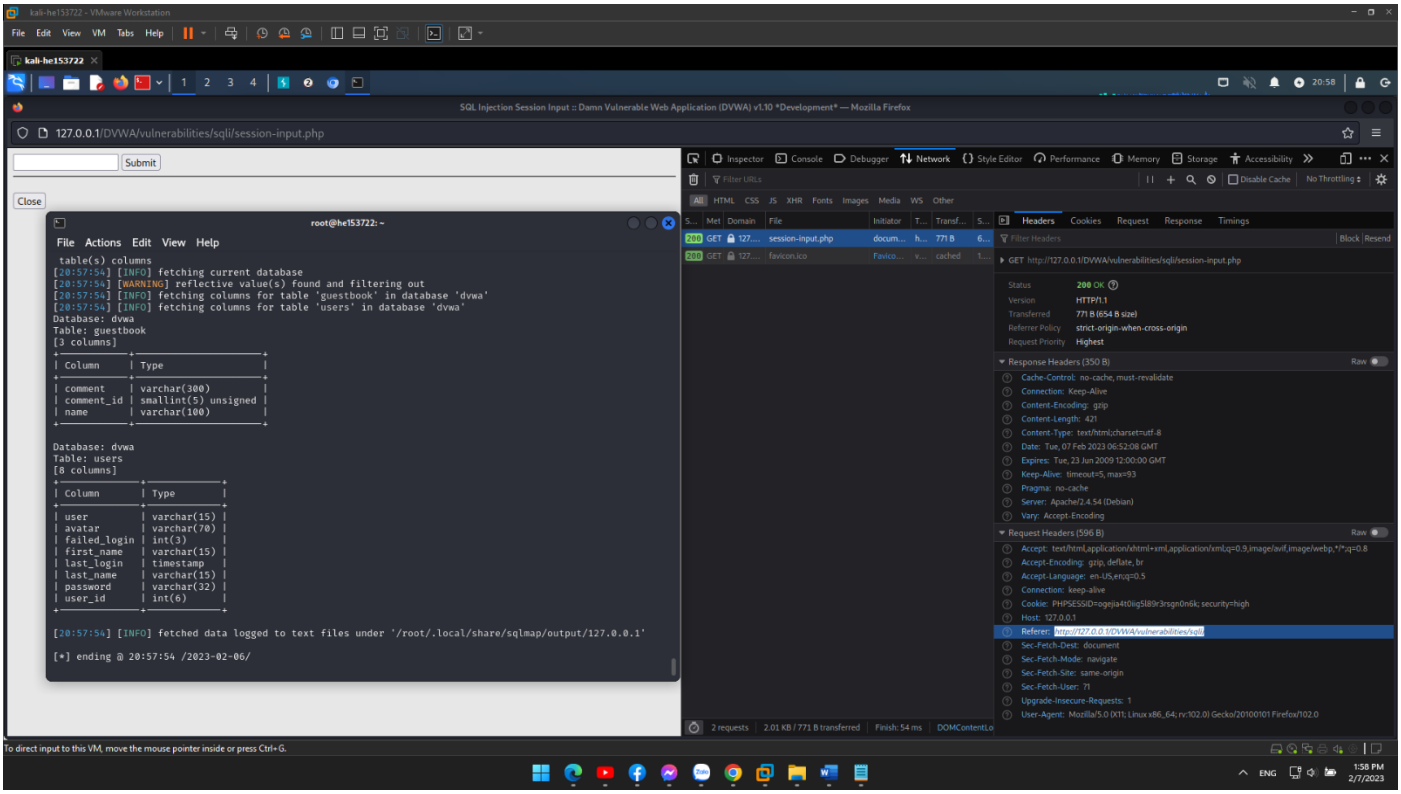
database’s name



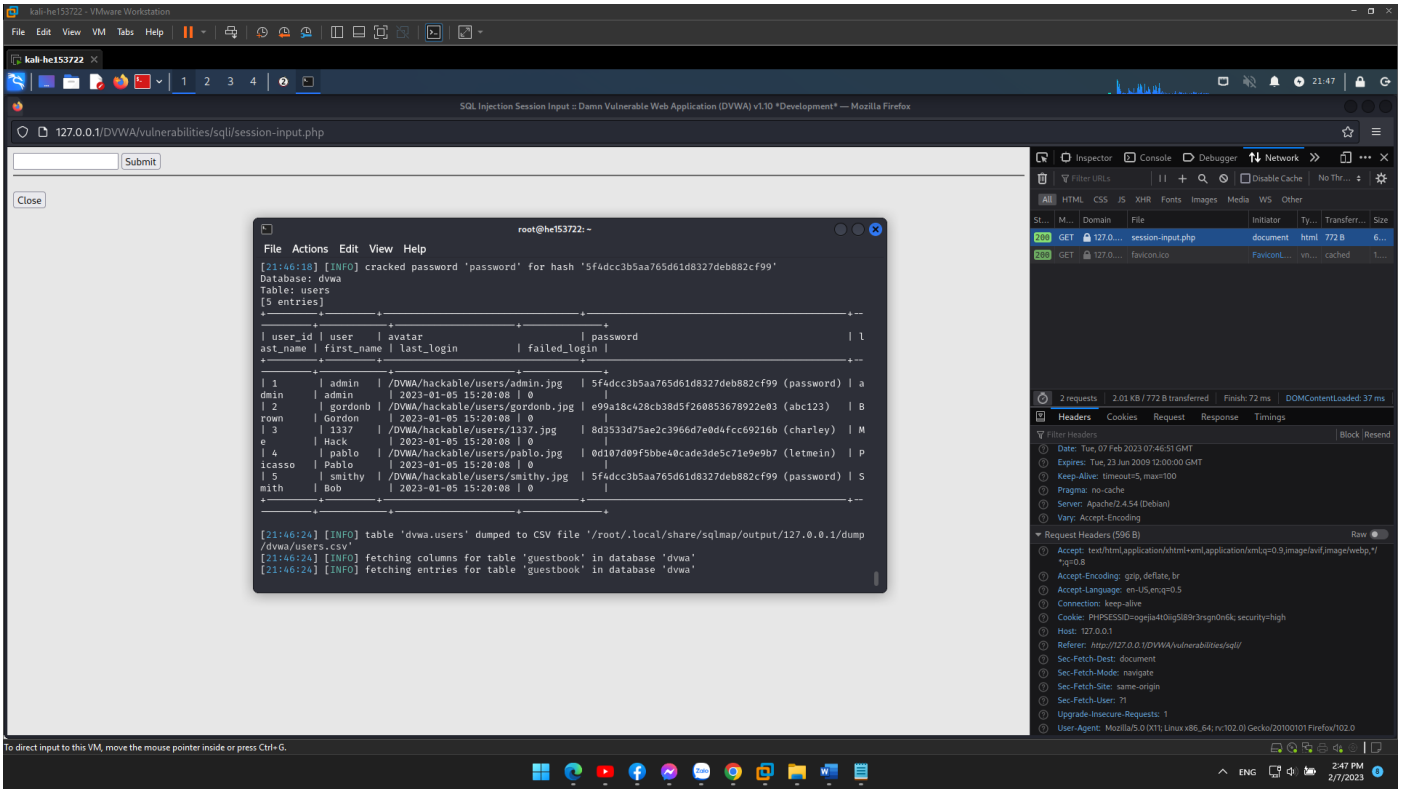
tables’ names



columns’ names



usernames and passwords



Explain the solution in Impossible level

The code first checks if the form has been submitted. If the form has been submitted, it checks an Anti-CSRF token to ensure that the form

request is valid. The code then retrieves the input from the form (the user ID) and checks if it's numeric. If the input is numeric, the code selects data from the database using either MySQL or SQLite, depending on the configuration. The selected data is the first name and last name of the user with the specified ID. Finally, the code generates a new Anti-CSRF token for the next form request.