NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

You are developing a web application requiring authentication and authorization. The persistent store used for credential information (usernames and passwords) is a SQL database. The database has a table called "`users`" organized into three columns: "`id`" (the primary key), "`name,`" and "`username.`" You are asked to write a helper method to update the username . Consider the snippet of code below and answer the following questions, assuming that the code has all required permissions to execute.

```
01   # import whatever is needed
02   def update_user(id, username)
03      # Code omitted for db connection and getting an object of cursor
04       sql = "UPDATE users SET username = %s WHERE id = %s"
05       cur.execute(sql % (username, id))
```

Questions:
1. What will the function do when executed?

2. If the method `update_user` is invoked with an arbitrary value of `username`, which one of the following statements is correct?

a. The method updates the `id` and `username` fields.
b. The method updates only the `username` field.
c. The method may perform some other operation.
d. None of the above.

[Other statistical questions will be imported here while creating the survey.]

NOTE: ANSWER IS TO BE SHOWN TO THE PUZZLE TAKER AT THE END OF THE SESSION.

ANSWERS:
1. The function accepts two values and performs a SQL UPDATE command.
2. c
The user could input a string like `"Robert; DROP TABLE users; --"` as the username, which makes the database drop the `users` table, thus making a SQL injection possible.

NOTE: THE REST OF THIS DOCUMENT CONTAINS EXTRA INFORMATION FOR THE PROJECT RESEARCHERS. IT IS NOT TO BE SHOWN TO THE PUZZLE TAKERS.

TAGS:
Python, sql-injection, input-verification, input-sanitization

CATEGORIES:
Blindspot - YES
Type - SQL
Number of distinct functions - 1
Number of total functions - 1
Blindspot function - `curs.execute()`
Function call omitted - YES
Blindspot type - Omitted function call
Number of parameters in the blindspot function - 1 parameter
Cyclomatic complexity - 2

NAME:
Cursor object - An object that represents a precompiled SQL statement.

BLINDSPOT:
The fact that the `Cursor` class can resolve SQL injection vulnerability only if it is used correctly may cause a blindspot. The simplest way to build SQL queries is string concatenation. This simple way of performing SQL queries is highly vulnerable to SQL injection attacks.

CORRECT USE EXAMPLE:
To see the correct way to use the API, look at the PX57-curs.execute puzzle.

MORE INFORMATION:
N/A

REFERENCES:
1. https://www.owasp.org/index.php/SQL_Injection
2. http://bobby-tables.com/python