NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

You are developing a web application that requires 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.

```
# import whatever is needed
def update_user(username, id)
    # CODE OMITTED:
    # Get an object of cursor
    sql = "UPDATE users SET username = %s WHERE id = %s"
    cur.execute(sql, (username, id))
```

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

2. If one calls the `update_user` method 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 performs 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. b
Even if the user inputs a string like `"Robert; DROP TABLE users; --"` as the username, the above code will just update the name to the given string, without performing any other operation.

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 - NO
Type - SQL
Number of distinct functions - 1
Number of total functions - 1
Blindspot function - `curs.execute()`
Function call omitted - N/A
Blindspot type - N/A
Number of parameters in the blindspot function - N/A
Cyclomatic complexity - 2

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

BLINDSPOT:
N/A

CORRECT USE EXAMPLE:
N/A

MORE INFORMATION:
N/A

REFERENCES:

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