NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO

Consider this snippet of Python code that implements a music directory by storing information about song titles, artist names, album names, and release dates in a MySQL database. The user is asked to enter the genre of music for which they are searching. This input is then passed to a database, which uses this information to select songs and returns them to the user. 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
03  genre = input("Please enter your desired genre>")
04
05  # Open database connection
06  db = MySQLdb.connect("localhost","allUsers","54373$!@","MUSICDB")
07
08  '''
09  Prepares a cursor object that will hold the
10  information on the rows accessed by our query
11  '''
12  cursor = db.cursor()
13  cursor.execute("SELECT songName, albumName, releaseDate "
14      "FROM Songs WHERE genre = '%s'", genre)
15
16  # Get all the rows
17  results = cursor.fetchall()
18  for row in results:
19     print(row)
20
21  db.close()
```

Questions:

1. What will the program do when executed?

2. What type of information could a user retrieve from this program?

a. The song name
b. The album name
c. The artist name
d. A and B
e. Any attribute from the database

[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. It will return records from the database that match the specified genre.

2. d
The way that the code calls the execute function prevents SQL injection, thus no information other than what is in the SELECT statement can be extracted.

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

TAGS:
Python, sql, sql-injection, mysql, database

CATEGORIES:
Blindspot - NO
Type - Injection
Number of distinct functions - 8
Number of total functions - 8
Blindspot function - N/A
Function call omitted - NO
Blindspot type - N/A
Number of parameters in the blindspot function - N/A
Cyclomatic complexity - 2

NAME:
cursor.execute(query_string, params=None, multi=False)

DESCRIPTION:
This method executes the given database operation (query or command). The parameters found in the tuple or dictionary parameters are bound to the variables in the operation. Variables are specified using %s or %(name)s parameter style (that is, using format or pyformat style). The function execute() returns an iterator if multi is True.

BLINDSPOT:
String interpolation for SQL queries can be very dangerous because it does not escape the input parameters correctly and will leave the application open to SQL injection attacks.

CORRECT USE EXAMPLE:
#N/A

MORE INFORMATION:
#N/A

REFERENCES:
1. http://www.tutorialspoint.com/python/python_database_access.htm
2. http://stackoverflow.com/questions/775296/python-mysql-with-variables