NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

You are developing a web application that runs on the Linux OS and that provides server administration functionalities (e.g., changing the hostname of server). Since there's no built-in feature in Java to change the hostname of machine, you have to use a Linux command to do so. The `setHostname` method takes a `String` as the new hostname, attempts to change the hostname of the server, and returns `true` if it succeeded and false otherwise. Consider the snippet of code below and answer the following questions, assuming that the code has all required permissions to execute.

```
01   // OMITTED: Import whatever is needed
02   public final class SystemUtils {
03     public static boolean setHostname (String hostname)
04         throws Exception {
05       String cmd = "hostname '" + hostname + "'";
06       ProcessBuilder builder = new ProcessBuilder("sh", "-c", cmd);
07       Process process = builder.start();
08       int exit = process.waitFor();
09
10       if (exit == 0)
11         return true;
12       else
13         return false;
14     }
15   }
```

Questions:

1. What will the `setHostname` method do when executed?

2. If a program calls the `setHostname` method as `setHostname("'$(shutdown)'")`, which one statement is correct?

a. `setHostname` throws an exception due to invalid character in the argument.
b. `setHostname` fails and returns `false` because of the invalid character in the argument.
c. `setHostname` sets the hostname of the server to "shutdown".
d. `setHostname` sets the hostname of the server to "0".
e. None of the above.

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

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

ANSWER:
e
The code is trying to enclose the argument in single quotes to prevent inline-command evaluation (line #5). However, since the single quote (if there is any in the argument) is not escaped, the inline-command injection is still possible. For the given string in the question, the "`shutdown`" command (as inline-command) in the argument will be executed before executing the "`hostname`" command.

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

TAGS:
java, processbuilder-class, command-injection, input-verification, input-sanitization

CATEGORIES:
Blindspot - YES
Type - Command Injection
Number of distinct functions - 4
Number of total functions - 4
Blindspot function - `new ProcessBuilder()`
Function call omitted - NO
Blindspot type - Incorrect usage
Number of Parameters in the blindspot function - 3 parameters
Cyclomatic complexity - 3

NAME:
ProcessBuilder class - This class is used to create operating system processes.

DESCRIPTION:
Each ProcessBuilder instance manages a collection of process attributes. The start() method creates a new Process instance with those attributes. The start() method can be invoked repeatedly from the same instance to create new subprocesses with identical or related attributes.

BLINDSPOT:
This class is highly vulnerable to command injection attack and programmers should avoid using it, if possible. If there is no way to avoid, the data passed to the method should be carefully verified and sanitized.

CORRECT USE EXAMPLE:
#N/A

MORE INFORMATION:
#N/A

REFERENCES:

1. ProcessBuilder
2. OWASP: Command Injection