NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

You are asked to write a Python script to open text files. This functionality allows a user to specify the path of a text file and open the file in the default text viewer of the system, and it is implemented by the function `view_text(path)`. This function uses the `mailcap` module to find the proper command to open the file with the text viewer application. The `mailcap.getcaps` function returns a dictionary mapping MIME types to a list of mailcap file entries. The `mailcap.findmatch` function returns a 2-tuple; the first element is the command to be executed and the second element is the mailcap entry for a given MIME type. Consider the snippet of code below (saved in a file named `view.py`) and answer the following questions, assuming that the code has all required permissions to execute.

```
01  #!/usr/bin/python3
02  import os, sys, mailcap
03  caps = mailcap.getcaps()
04
05  def view_text(path):
06    command, mime = mailcap.findmatch(caps, 'text/*', filename=path)
07    os.system(command)
08
09  if __name__ == '__main__':
10    view_text(sys.argv[1])
```

Questions:

1. What will `view.py` do when executed with the path of a text file as argument?

2. What will happen if "`view text-file;ls;#.mp4`" executes in a terminal?

a. If there is a file with the name "`text-file;ls;#.mp4`", the script will open the file in the default text viewer program.
b. The script will open the default text viewer program with the list of files and directories in the current folder as content.
c. The script will open the default text viewer program with empty content.
d. An error will be thrown indicating that the MP4 file type is not supported.
e. 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.

ANSWER:
1. The script will take input as a valid text file name and open the file with the default program corresponding to that file extension.

2. e
The implementation is vulnerable to command injection attacks. The given file contains the `ls` command, which will be executed when `.view.py` is invoked with the input "`view text-file;ls;#.mp4`"

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, command-injection

CATEGORIES:
Blindspot - YES
Type - Injection
Number of distinct functions - 3
Number of total functions - 3
Blindspot function - `mailcap.findmatch()`
Function call omitted - NO
Blindspot type - Validation missing
Number of parameters in the blindspot function - 3 parameters
Cyclomatic complexity - 2

NAME:
mailcap.findmatch(caps, MIMEtype[, key[, filename[, plist]]])

DESCRIPTION:
Mailcap files are used to configure how MIME-aware applications, such as mail readers and web browsers, react to files with different MIME types. (The name "mailcap" is derived from the phrase "mail capability.") For example, a mailcap file might contain a line like video/mpeg; xmpeg%s. Then, if the user encounters an email message or web document with the MIME type video/mpeg, %s will be replaced by a filename (usually one belonging to a temporary file) and the xmpeg program can be automatically started to view the file.

Return a 2-tuple; the first element is a string containing the command line to be executed and the second element is the mailcap entry for a given MIME type. If no matching MIME type can be found, (None, None) is returned.

BLINDSPOT:
If the filename contains shell commands, they will be executed if they are passed to os.system as described in the docs.

CORRECT USE EXAMPLE:
#N/A

MORE INFORMATION:
#NA

§REFERENCES:
https://bugs.python.org/issue24778
https://docs.python.org/2/library/mailcap.html