

NOTE: SCENARIO IS WHAT THE PUZZLE TAKER SEES.

SCENARIO:

A university professor changes her syllabus quite often. You want to make sure that you have the most up-to-date syllabus so that you do not miss readings or due dates for assignments. You use the following Python script to download the syllabus file from the course homepage and check it against your copy. In the following script, the `urllib.request.urlopen(url)` function opens the given URL, the `file.read` function reads the data from the given URL, and the hash function calculates the hash value of the downloaded data as an integer. The script then compares the calculated hash value to the expected hash value (the expected hash value was calculated and saved in the `LAST_SYLLABUS_HASH` file during the previous call of the `check_syllabus` function). Consider the code below and answer the following questions, assuming that the code has all required permissions to execute.

```
01  # import whatever is needed
02  url = 'http://cise.ufl.edu/class/cise3234/syllabus.pdf'
03  last_syllabus_hash = ... # Read from LAST_SYLLABUS_HASH file
04
05  def check_syllabus(url):
06      print("Downloading syllabus...")
07      file = urllib.urlopen(url)
08      syllabus = file.read()
09      if hash(syllabus) == last_syllabus_hash:
10          print("Syllabus has not changed.")
11      else:
12          print("Syllabus has changed.")
13          last_syllabus_hash = hash(syllabus)
14          # Save last_syllabus_hash in LAST_SYLLABUS_HASH file
```

Questions:

1. What will the function `check_syllabus` do when called?
2. Which of the following is correct if someone calls the `check_syllabus` function?
 - a. The function prints "Syllabus has not changed" if the syllabus has not changed.
 - b. The function prints "Syllabus has changed" if the syllabus has changed.
 - c. The function always prints "Syllabus has not changed."
 - d. The function always prints "Syllabus has changed."
 - e. The function behavior is not predictable.
 - f. a and b

[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:

The file will be downloaded from the given URL and its hash value will be compared to the hash that was previously stored in the LAST_SYLLABUS_HASH file.

2. e

Because of the randomization of the hash seed, we cannot be sure that the hash will be the same for two identical documents, thus the behaviour of the check_syllabus function cannot be predicted.

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-3, hash

CATEGORIES:

Blindspot - YES

Type - Crypto

Number of distinct functions - 3

Number of total functions - 3

Blindspot function - hash()

Function call omitted - NO

Blindspot type - Inappropriate usage

Number of parameters in the blindspot function - 1 parameters

Cyclomatic complexity - 3

NAME:

hash(object)

DESCRIPTION:

Returns the hash value of the object (if it has one). Hash values are integers. They are used to quickly compare dictionary keys during a dictionary lookup. Numeric values that compare as equal have the same hash value (even if they are of different types, as is the case for 1 and 1.0).

BLINDSPOT:

By default, the hash values of str, bytes and datetime objects are “salted” with an unpredictable random value (Each time Python is run, PYTHONHASHSEED is set randomly, so the hash function returns a different value for any uniform input). Although they remain constant within an individual Python process, they are not predictable between repeated invocations of Python. Thus it is possible that one file produces two different hash values (in

different processes) or two different files produce same hash values (in different processes). It is best to use `hashlib.md5` to produce similar results each time.

CORRECT USE EXAMPLE:

#N/A

MORE INFORMATION:

#N/A

REFERENCES:

1. <https://docs.python.org/3.5/library/functions.html#hash>
2. <http://stackoverflow.com/questions/793761/>