SPLK-2001 Q&As

Splunk Certified Developer

Pass Splunk SPLK-2001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-2001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following ensures that quotation marks surround the value referenced by the token?

A. $token_name|s$

B. "$token_name$"

C. ($token_name$)

D. \"$token_name$\"

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/Viz/tokens

QUESTION 2

Which items below are configured in inputs.conf? (Select all that apply.)

A. A modular input written in Python.

B. A file input monitoring a JSON file.

C. A custom search command written in Python.

D. An HTTP Event Collector as receiver of data from an app.

Correct Answer: AD

QUESTION 3

Which of the following formats are valid for a Splunk REST URI?

A. host:port/endpoint

B. scheme://host/servicesNS/*/

C. $SPLUNK HOME/services/endpoint

D. scheme://host:port/services/endpoint

Correct Answer: D

QUESTION 4

Assuming permissions are set appropriately, which REST endpoint path can be used by someone with a power user role to access information about mySearch, a saved search owned by someone with a user role?

A. /servicesNS/-/data/saved/searches/mySearch

B. /servicesNS/object/saved/searches/mySearch

C. /servicesNS/search/saved/searches/mySearch

D. /servicesNS/-/search/saved/searches/mySearch

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.2/RESTUM/RESTusing

QUESTION 5

Consider the following Python code snippet used in a Splunk add-on:

if not os.path.exists(full_path): self.doAction(full_path, header) else: f = open(full_path) oldORnew = f.readline().split(",") f.close()

An attacker could create a denial of service by causing an error in either the open() or readline() commands. What type of vulnerability is this?

A. CWE-693: Protection Mechanism Failure

B. CWE-562: Return of Stack Variable Address

C. CWE-404: Improper Resource Shutdown or Release

D. CWE-636: Not Failing Securely (`Failing Open\\')

Correct Answer: C

Reference: https://dev.splunk.com/enterprise/docs/developapps/testvalidate/securitybestpractices/