USER GUIDE V1.0.0

SlashNext Phishing IR SDK Guide

TABLE OF CONTENTS

1 | INTRODUCTION

SlashNext Phishing Incident Response SDK allows users to develop their own automation scripts (playbooks) to perform certain data enrichment using SlashNext On-demand Threat Intelligence cloud APIs.

The **SlashNext Phishing Incident Response** enables users to analyzes the provided IoCs (URL, IPv4 or FQDN) with the SlashNext **SEER™** threat detection cloud to get definitive, binary verdicts (malicious or benign) along with forensics data including screenshots, HTML, and more.

SlashNext threat detection uses browsers in a purpose-built cloud to dynamically inspect page contents and site behavior in real-time. This method enables SlashNext to follow URL re-directs and multi-stage attacks to more thoroughly analyze the final page(s) and makes a much more accurate, binary determination with near-zero false positives. It also detects all six major categories of phishing and social engineering sites. These include credential stealing, rogue software / malware sites, scareware, phishing exploits (sites hosting weaponized documents, etc.), and social engineering scams (fake deals, giveaways, etc.).

Use cases include abuse inbox management where SOC teams can automate URL analysis for phishing emails to save hundreds of hours versus more manual methods. Playbooks that mine and analyze network logs can also leverage SlashNext URL analysis on demand.SlashNext not only provides accurate, binary verdicts (rather than threat scores), it provides IOC metadata and screen shots of detected phishing pages. These enables easier classification and reporting. Screen shots can be used as an aid in on-going employee phishing awareness training and testing.

The SlashNext Phishing Incident Response SDK uses an API key to authenticate with the SlashNext cloud. If you don't have a valid API key, contact the SlashNext team: support@slashnext.com

2 | REQUIREMENT

SlashNext Phishing Incident Response Console requires Python 3.6 with **setuptools** installed on your system and have access to internet.

If you don't have Python3.6 installed please use following commands

```
sudo apt install python3

sudo apt install python3-pip

sudo python3 -m pip install setuptools
```

3 | INSTALLATION

Please follow the steps given below to install the SlashNext Phishing IR Console along with SlashNext Phishing IR SDK on your system.

Note
Please note that SlashNext shall provide you with the zip file which contains following directory structure.

```
├──     doc
|         ├──     SlashNext Phishing IR Console Guide.pdf
|         └──     SlashNext Phishing IR SDK Guide.pdf
├──     src
|         ├──     setup.py
|         └──     SlashNextPhishingIRConsole
|                   ├──     ...
|                   └──     ...
├──     README.md
```

1. Unzip the package provided by SlashNext.

2. Open a Terminal and go to the 'src' directory.

3. Run the following command which installs all the required modules along with SlashNext Phishing IR Console and SDK.

```
sudo python3 -m pip install .
```

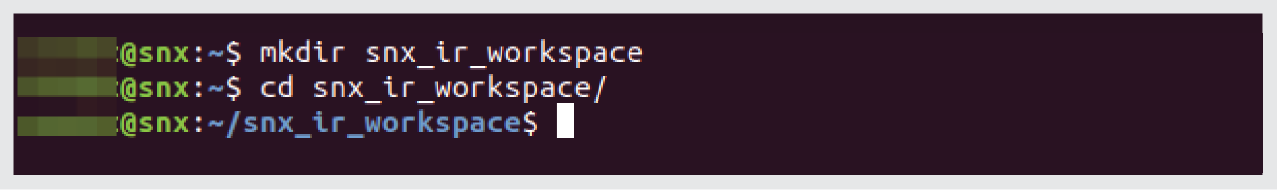
4. In order to uninstall the SlashNext Phishing IR Console package, run the following command.

```
sudo python3 -m pip uninstall slashnext-phishing-ir-console
```

4 | CONFIGURATION

Follow the steps listed below to run/activate the SlashNext Phishing Incident Response SDK on your system.

1. Open a terminal and make a new directory which you want to save as a new workspace for SlashNext Phishing IR SDK.



```
[redacted]@snx:~$ mkdir snx_ir_workspace
[redacted]@snx:~$ cd snx_ir_workspace/
[redacted]@snx:~/snx_ir_workspace$
```

2. Open a new python document and write following code to configure and test SlashNextPhishingIR SDK.

```
from SlashNextPhishingIRConsole.SlashNextPhishingIR import SlashNextPhishingIR

 # Creating an instance of the SlashNext Phishing IR class with the workspace location
snx_phishing_ir = SlashNextPhishingIR('/home/developer/snx_ir_workspace/')

# Providing the valid required configuration
snx_phishing_ir.set_conf(
   api_key='xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
   base_url='https://oti.slashnext.cloud/api/'
)

# Testing the configurations (connectivity and authentication)
status, details = snx_phishing_ir.test()

# Checking if the provided configurations are working correctly
if status == 'ok':
   print('Successfully connected the SlashNext cloud.')
else:
   print('Connection to SlashNext cloud failed due to {}'.format(details))
```

3. In case of a successful test (connectivity and authentication), you shall see following output from the code snippet given above.

```
Successfully connected the SlashNext cloud.
```

5 | EXECUTING ACTIONS/COMMANDS

There are two possible ways to execute actions using SlashNextPhishingIR SDK.

5.1 | METHOD 1

With this method the configurations are saved on the disk in a file for future usage and also all the actions are available at within a single instance.

1. The execution of commands is quite easy, you'll need to call the execute function of the SlashNextPhishingIR class with the action string. An action string shall be formatted as following.

```
<Action Name>  <Required Parameter>  <Optional Parameter 1>  <Optional Parameter 2> ...
```

2. An example code snippet of method 1 is given below.

```
from SlashNextPhishingIRConsole.SlashNextPhishingIR import SlashNextPhishingIR
from pprint import pprint


# Creating an instance of the SlashNext Phishing IR class with the workspace location
snx_phishing_ir = SlashNextPhishingIR('/home/developer/snx_ir_vworkspace/')

# Providing the valid required configuration
snx_phishing_ir.set_conf(
   api_key='xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
   base_url='https://oti.slashnext.cloud/api/'
)

# Testing the configurations (connectivity and authentication)
status, details = snx_phishing_ir.test()

# Checking if the provided configurations are working correctly
if status == 'ok':
   # Execute 'slashnext-host-reputation' action with 'host' parameter value 'google.com'
   status, details, responses_list = snx_phishing_ir.execute('slashnext-host-reputation host=google.com')

   if status == 'ok':
      pprint(responses_list)
   else:
      print('Action execution failed due to {}'.format(details))
else:
   print('Connection to SlashNext cloud failed due to {}'.format(details))
```

3. In case of a successful execution, you shall see following output.

```
[
        {
        'errorMsg': 'Success',
        'errorNo': 0,
        'threatData': {
                'firstSeen': '12-10-2018 13:04:17 UTC',
                'lastSeen': '12-23-2019 17:50:41 UTC',
                'threatName': 'N/A',
                'threatStatus': 'N/A',
                'threatType': 'N/A',
                'verdict': 'Benign'
                        }
        }
]
```

5.2 | METHOD 2

With this method the configurations needs to be passed to each action class and also also you'll need to make instances of each action class.

1. An example code snippet of method 2 is given below.

```
from SlashNextPhishingIRConsole.SlashNextPhishingIR.SlashNextHostReputation import SlashNextHostReputation
from pprint import pprint


# Creating an instance of the SlashNextHostReputation class with the API key and Base URL
snx_host_reputation = SlashNextHostReputation(
  api_key='xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx',
  base_url='https://oti.slashnext.cloud/api/'
)

# Execute 'slashnext-host-reputation' action with 'host' parameter value 'google.com'
details, responses_list = snx_host_reputation.execution(host='google.com')

if details == 'Success':
  pprint(responses_list)
else:
  print('Action execution failed due to {}'.format(details))
```

2. In case of a successful execution, you shall see following output.

```
[
        {
        'errorMsg': 'Success',
        'errorNo': 0,
        'threatData': {
                'firstSeen': '12-10-2018 13:04:17 UTC',
                'lastSeen': '12-23-2019 17:50:41 UTC',
                'threatName': 'N/A',
                'threatStatus': 'N/A',
                'threatType': 'N/A',
                'verdict': 'Benign'
                        }
        }
]
```

6 | SUPPORTED ACTIONS/COMMANDS

SlashNext Phishing Incident Response SDK supported actions/commands and outputs are listed below. For example we shall use method 1 of execution.

1. **slashnext-host-reputation** - Queries the SlashNext cloud database and retrieves the reputation of a host.
2. **slashnext-host-report** - Queries the SlashNext cloud database and retrieves a detailed report.
3. **slashnext-host-urls** - Queries the SlashNext cloud database and retrieves a list of all URLs.
4. **slashnext-url-scan** - Perform a real-time URL reputation scan with SlashNext cloud-based SEER threat detection engine.
5. **slashnext-url-scan-sync** - Perform a real-time URL scan with SlashNext cloud-based SEER threat detection engine in a blocking mode.
6. **slashnext-scan-report** - Retrieve URL scan results against a previous scan request.
7. **slashnext-download screenshot** - Downloads a screenshot of a web page against a previous URL scan request.
8. **slashnext-ownload-html** - Downloads a web page HTML against a previous URL scan request.
9. **slashnext-download-text** - Downloads the text of a web page against a previous URL scan request.
10. **slashnext-api-quota** - Find information about your API quota, like current usage, quota left etc.

6.1 | HOST REPUTATION

slashnext-host-reputation
Queries the SlashNext cloud database and retrieves the reputation of a host.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-host-reputation' action with 'host' parameter value 'www.lineageedcx.ru'
status, details, responses_list = snx_phishing_ir.execute('slashnext-host-reputation host=www.lineageedcx.ru')

# Expected Output
[
        {
        'errorMsg': 'Success',
        'errorNo': 0,
        'threatData': {
                                'firstSeen': '08-29-2019 17:09:59 UTC',
                                'lastSeen': '10-30-2019 07:13:06 UTC',
                                'threatName': 'Fake Login Page',
                                'threatStatus': 'No Longer Active',
                                'threatType': 'Phishing & Social Engineering',
                                'verdict': 'Malicious'
                        }
        }
]
```

6.2 | HOST REPORT

slashnext-host-report
Queries the SlashNext cloud database and retrieves a detailed report for a host and associated URL.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database. Can be either a domain name or an IPv4 address.	string	domain / IP

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-host-report' action with 'host' parameter value 'virtualmarketing.pk'
status, details, responses_list = snx_phishing_ir.execute('slashnext-host-report host=virtualmarketing.pk')

# Expected Output
[{'errorMsg': 'Success',
 'errorNo': 0,
 'threatData': {'firstSeen': '10-16-2019 15:41:09 UTC',
        'lastSeen': '10-19-2019 08:54:06 UTC',
        'threatName': 'Fake Login Page',
        'threatStatus': 'No Longer Active',
        'threatType': 'Phishing & Social Engineering',
        'verdict': 'Malicious'}},
 {'errorMsg': 'Success',
 'errorNo': 0,
 'normalizeData': {'normalizeMessage': '', 'normalizeStatus': 0},
 'urlDataList': [{'scanId': '873d9975-c6c4-42ef-9674-ff3ee4a44ed9',
         'threatData': {'firstSeen': '10-16-2019 15:41:09 UTC',
                'lastSeen': '10-16-2019 15:53:44 UTC',
                'threatName': 'Fake Login Page',
                'threatStatus': 'Active',
                'threatType': 'Phishing & Social Engineering',
                'verdict': 'Malicious'},
         'url': 'https://virtualmarketing.pk/xoixnx/Chase2019/myaccount/index.php'}]},
 {'errorMsg': 'Success',
 'errorNo': 0,
 'scData': {'scBase64': 'Replaced with dummy data',
      'scContentType': 'jpeg',
      'scName': 'Webpage-screenshot'}},
 {'errorMsg': 'Success',
 'errorNo': 0,
 'htmlData': {'htmlBase64': 'Replaced with dummy data',
       'htmlContenType': 'html',
       'htmlName': 'Webpage-html'}},
 {'errorMsg': 'Success',
 'errorNo': 0,
 'textData': {'textBase64': 'Replaced with dummy data',
       'textName': 'Webpage-text'}}]
```

6.3 | HOST URLs

slashnext-host-urls
Queries the SlashNext cloud database and retrieves a list of all URLs associated with the specified host.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
host	Required	The host to look up in the SlashNext Threat Intelligence database, for which to return a list of associated URLs. Can be either a domain name or an IPv4 address.	string	domain / IP
limit	optional	The maximum number of URL records to fetch. Default is "10".	numeric	

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-host-urls' action with 'host' parameter value 'blueheaventravel.com'
status, details, responses_list = snx_phishing_ir.execute('slashnext-host-urls host=blueheaventravel.com limit=5')

# Expected Output
[{'errorMsg': 'Success',
 'errorNo': 0,
 'normalizeData': {'normalizeMessage': '', 'normalizeStatus': 0},
 'urlDataList': [{'finalUrl': 'https://blueheaventravel.com/vendor/fil-
p/whoops/up/pulp.php?rand=46InboxLightaspxn.4827685990&fid.28.9164762324&fid=1&fav.1&rand.46InboxLight.aspxn.482
7685990&fid.28.9164762324&fid.1&fav.1&email=SmFja2RhdmlzQGV1cmVsaW9zb2xsdXRpb25zLmNvbQ==&.rand=46InboxLi
ght.aspx?n=4827685990&fid=6#x=9164762324&fid=1&fav=1',
            'scanId': 'N/A',
            'threatData': {'firstSeen': '10-16-2019 15:21:56 UTC',
                      'lastSeen': '10-18-2019 01:28:09 UTC',
                      'threatName': 'Fake Login Page',
                      'threatStatus': 'No Longer Active',
                      'threatType': 'Phishing & Social Engineering',
                      'verdict': 'Malicious'},
            'url': 'https://blueheaventravel.com/vendor/filp/whoops/up/index.php?email=Jackdavis@eureliosollutions.com'},
           {'finalUrl': 'https://blueheaventravel.com/vendor/fil-
p/whoops/up/pulp.php?rand=46InboxLightaspxn.4827685990&fid.28.9164762324&fid=1&fav.1&rand.46InboxLight.aspxn.482
7685990&fid.28.9164762324&fid.1&fav.1&email=&.rand=46InboxLight.aspx?n=4827685990&fid=6#x=9164762324&fid=1&fa
v=1',
            'scanId': 'N/A',
            'threatData': {'firstSeen': '10-16-2019 17:39:54 UTC',
                      'lastSeen': '10-18-2019 03:48:20 UTC',
                      'threatName': 'Fake Login Page',
                      'threatStatus': 'No Longer Active',
                      'threatType': 'Phishing & Social Engineering',
                      'verdict': 'Malicious'},
            'url': 'https://blueheaventravel.com/vendor/filp/whoops/up/index.php?email='}]}]
```

6.4 | URL SCAN

slashnext-url-scan
Performs a real-time URL reputation scan with SlashNext cloud-based SEER Engine. If the specified URL already exists in the cloud database, scan results will be returned immediately. If not, this command will submit a URL scan request and return with the message "check back later" and include a unique Scan ID. You can check the results of this scan using the "slashnext-scan-report" command anytime after 60 seconds using the returned Scan ID.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	Required	The URL that needs to be scanned.	string	URL
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	

Execution

The input and output of the command/action are highlighted below.

```
# Execute 'slashnext-url-scan' action with 'url' parameter value 'http://ajeetenterprises.in/js/kbrad/drive/index.php'
status, details, responses_list = snx_phishing_ir.execute('slashnext-url-scan url=http://ajeetenterprises.in/js/kbrad/drive/index.php extended_info=true')

# Expected Output
[{'errorMsg': 'Success',
  'errorNo': 0,
  'normalizeData': {'normalizeMessage': '', 'normalizeStatus': 0},
  'urlData': {'scanId': 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9',
       'threatData': {'firstSeen': '12-27-2019 07:45:55 UTC',
              'lastSeen': '12-27-2019 07:47:51 UTC',
              'threatName': 'Fake Login Page',
              'threatStatus': 'Active',
              'threatType': 'Phishing & Social Engineering',
              'verdict': 'Malicious'},
       'url': 'http://ajeetenterprises.in/js/kbrad/drive/index.php'}},
 {'errorMsg': 'Success',
  'errorNo': 0,
  'scData': {'scBase64': 'Replaced with dummy data',
       'scContentType': 'jpeg',
       'scName': 'Webpage-screenshot'}},
 {'errorMsg': 'Success',
  'errorNo': 0,
  'htmlData': {'htmlBase64': 'Replaced with dummy data',
        'htmlContenType': 'html',
        'htmlName': 'Webpage-html'}},
 {'errorMsg': 'Success',
  'errorNo': 0,
  'textData': {'textBase64': 'Replaced with dummy data',
        'textName': 'Webpage-text'}}]
```

6.5 | URL Scan Sync

slashnext-ur- scan-sync
Performs a real-time URL scan with SlashNext cloud-based SEER Engine in a blocking mode. If the specified URL already exists in the cloud database, scan result will be returned immediately. If not, this command will submit a URL scan request and wait for the scan to finish. The scan may take up to 60 seconds to finish.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
url	Required	The URL that needs to be scanned.	string	URL
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	
timeout	optional	A timeout value in seconds. If the system is unable to complete a scan within the specified timeout, a timeout error will be returned. You can run the command again with a different timeout. If no timeout value is specified, a default timeout value is 60 seconds.	numeric	

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-url-scan-sync' action with 'url' parameter value 'http://ajeetenterprises.in/js/kbrad/drive/index.php'
status, details, responses_list = snx_phishing_ir.execute('slashnext-url-scan-sync url=http://ajeetenterprises.in/js/kbrad/drive/index.php extended_info=true timeout=30')


# Expected Output
[{'errorMsg': 'Success',
 'errorNo': 0,
 'normalizeData': {'normalizeMessage': '', 'normalizeStatus': 0},
 'urlData': {'scanId': 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9',
          'threatData': {'firstSeen': '12-27-2019 07:45:55 UTC't,
                  'lastSeen': '12-27-2019 07:47:51 UTC',
                  'threatName': 'Fake Login Page',
                  'threatStatus': 'Active',
                  'threatType': 'Phishing & Social Engineering',
                  'verdict': 'Malicious'},
          'url': 'http://ajeetenterprises.in/js/kbrad/drive/index.php'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'scData': {'scBase64': 'Replaced with dummy data',
         'scContentType': 'jpeg',
         'scName': 'Webpage-screenshot'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'htmlData': {'htmlBase64': 'Replaced with dummy data',
          'htmlContenType': 'html',
          'htmlName': 'Webpage-html'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'textData': {'textBase64': 'Replaced with dummy data',
          'textName': 'Webpage-text'}}]
```

6.6 | URL SCAN REPORT

slashnext-scan-report
Retrieves the results of a URL scan against a previous scan request. If the scan is finished, results will be returned immediately; otherwise the message "check back later" will be returned.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID of the scan for which to get the report. Can be retrieved from the "slashnext-url-scan" action or "slashnext-url-scan-sync" action.	string	snx scan id
extended_info	optional	Whether to download forensics data, such as screenshot, HTML, and rendered text. If "true", forensics data will be returned. If "false" (or empty) forensics data will not be returned.	string	

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-scan-report' action with 'scanid' parameter value 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9'
status, details, responses_list = snx_phishing_ir.execute('slashnext-scan-report scanid=c0cb9503-5833-48e4-ae9e-a0f9d4065cf9
extended_info=true')

# Expected Output
[{'errorMsg': 'Success',
 'errorNo': 0,
 'normalizeData': {'normalizeMessage': '', 'normalizeStatus': 0},
 'urlData': {'scanId': 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9',
        'threatData': {'firstSeen': '12-27-2019 07:45:55 UTC't,
                'lastSeen': '12-27-2019 07:47:51 UTC',
                'threatName': 'Fake Login Page',
                'threatStatus': 'Active',
                'threatType': 'Phishing & Social Engineering',
                'verdict': 'Malicious'},
        'url': 'http://ajeetenterprises.in/js/kbrad/drive/index.php'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'scData': {'scBase64': 'Replaced with dummy data',
        'scContentType': 'jpeg',
        'scName': 'Webpage-screenshot'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'htmlData': {'htmlBase64': 'Replaced with dummy data',
        'htmlContenType': 'html',
        'htmlName': 'Webpage-html'}},
{'errorMsg': 'Success',
 'errorNo': 0,
 'textData': {'textBase64': 'Replaced with dummy data',
        'textName': 'Webpage-text'}}]
```

6.7 | DOWNLOAD SCREENSHOT

slashnext-download-screenshot
Downloads a screenshot of a web page against a previous URL scan request.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	snx scan id
resolution	optional	Resolution of the web page screenshot. Can be "high" or "medium". Default is "high".	string	

Execution

The input and output of the command/action are given below.

```
# Execute 'slashnext-download-screenshot' action with 'scanid' parameter value 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9'
status, details, responses_list = snx_phishing_ir.execute('slashnext-download-screenshot
scanid=c0cb9503-5833-48e4-ae9e-a0f9d4065cf9 resolution=medium')

# Expected Output
[ {'errorMsg': 'Success',
  'errorNo': 0,
  'scData': {'scBase64': 'Replaced with dummy data',
        'scContentType': 'jpeg',
        'scName': 'Webpage-screenshot'}}]
```

6.8 | DOWNLOAD HTML

slashnext-download-html
Downloads a web page HTML against a previous URL scan request.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	snx scan id

Execution

The input and output of the command/action are highlighted below.

```
# Execute 'slashnext-download-html' action with 'scanid' parameter value 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9'
status, details, responses_list = snx_phishing_ir.execute('slashnext-download-html
scanid=c0cb9503-5833-48e4-ae9e-a0f9d4065cf9')


# Expected Output
[ {'errorMsg': 'Success',
 'errorNo': 0,
 'htmlData': {'htmlBase64': 'Replaced with dummy data',
          'htmlContenType': 'html',
          'htmlName': 'Webpage-html'}}]
```

6.9 | DOWNLOAD TEXT

slashnext-download-text
Downloads the text of a web page against a previous URL scan request.

Parameters

PARAMETER	REQUIRED	DESCRIPTION	TYPE	CONTAINS
scanid	Required	Scan ID. Can be retrieved from the "slashnext-url-scan" action or the "slashnext-url-scan-sync" action.	string	snx scan id

Execution

The input and output of the command/action are highlighted below.

```
# Execute 'slashnext-download-html' action with 'scanid' parameter value 'c0cb9503-5833-48e4-ae9e-a0f9d4065cf9'
status, details, responses_list = snx_phishing_ir.execute('slashnext-download-html
scanid=c0cb9503-5833-48e4-ae9e-a0f9d4065cf9')


# Expected Output
[ {'errorMsg': 'Success',
 'errorNo': 0,
 'textData': {'textBase64': 'Replaced with dummy data',
          'textName': 'Webpage-text'}}]
```

6.10 | API QUOTA

slashnext-api-quota
Find information about your API quota, like current usage, quota left etc.

Parameters

The input and output of the command/action are highlighted below.

Execution

The input and output of the command/action are highlighted below.

```
# Execute 'slashnext-api-quota' action
status, details, responses_list = snx_phishing_ir.execute('slashnext-api-quota')

# Expected Output
[ {'errorMsg': 'Success',
 'errorNo': 0,
 'quotaDetails': {'consumedAPIDetail': {'customerApiQuota': 21,
                    'downloadHTML': 0,
                    'downloadScreenshot': 0,
                    'downloadText': 0,
                    'hostReputation': 23,
                    'hostUrls': 0,
                    'scanReportWithScanId': 0,
                    'scanSyncReportWithScanId': 0,
                    'urlReputation': 0,
                    'urlScan': 2,
                    'urlScanSync': 0},
         'consumedPointsDetail': {'customerApiQuota': 0,
                     'downloadHTML': 0,
                     'downloadScreenshot': 0,
                     'downloadText': 0,
                     'hostReputation': 23,
                     'hostUrls': 0,
                     'scanReportWithScanId': 0,
                     'scanSyncReportWithScanId': 0,
                     'urlReputation': 0,
                     'urlScan': 6,
                     'urlScanSync': 0},
         'expiryDate': '2020-12-19',
         'isExpired': False,
         'licensedQuota': 1500,
         'note': 'Your annual API quota will be reset to zero, once '
             'either the limit is reached or upon quota '
             'expiration date indicated above.',
         'pointsConsumptionRate': {'customerApiQuota': 0,
                      'downloadHTML': 0,
                      'downloadScreenshot': 0,
                      'downloadText': 0,
                      'hostReputation': 1,
                      'hostUrls': 1,
                      'urlReputation': 1,
                      'urlScan': 3,
                      'urlScanSync': 3,
                      'urlScanSyncWithScanId': 0,
                      'urlScanWithScanId': 0},
         'remainingQuota': 1471}}]
```