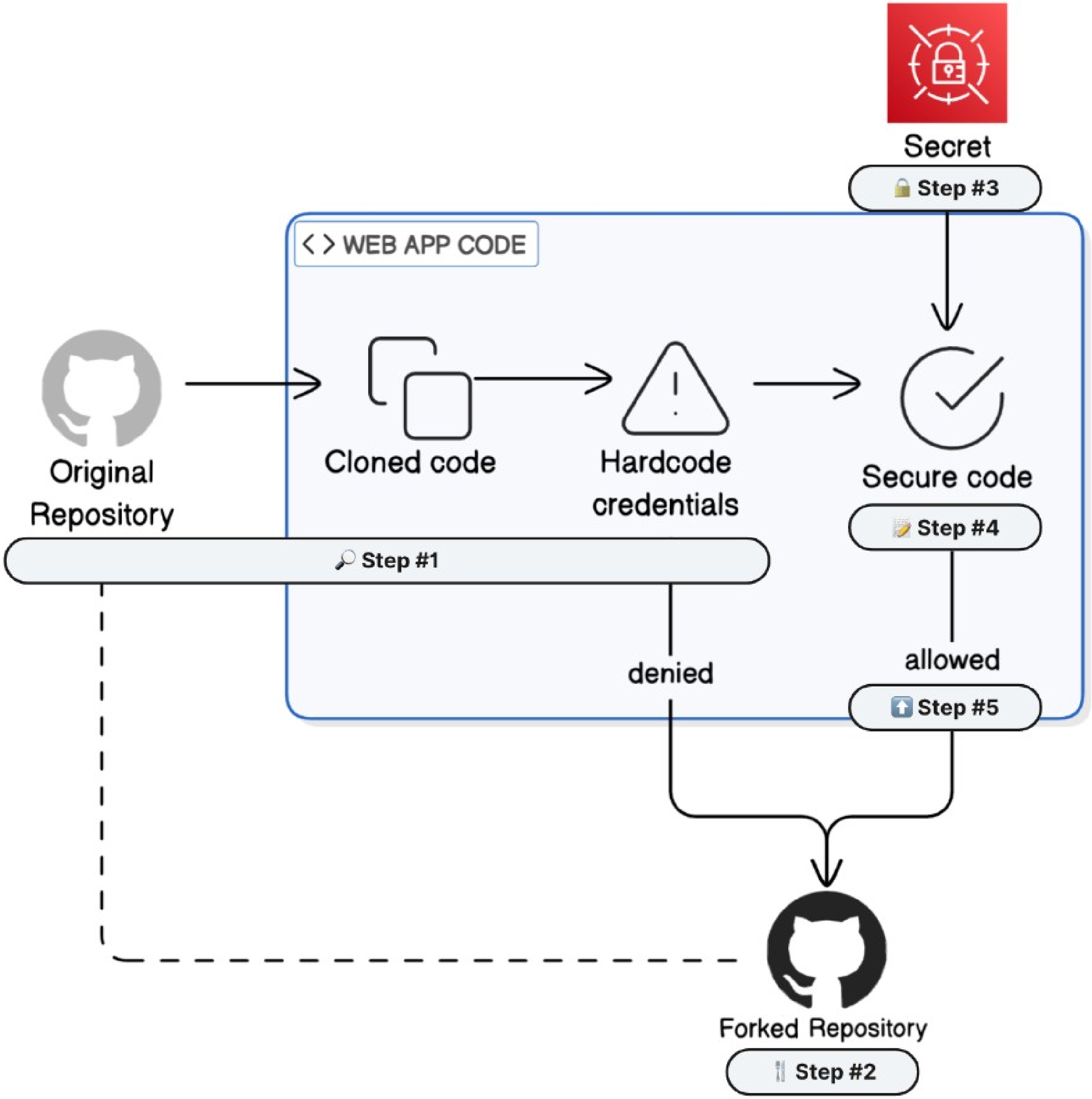
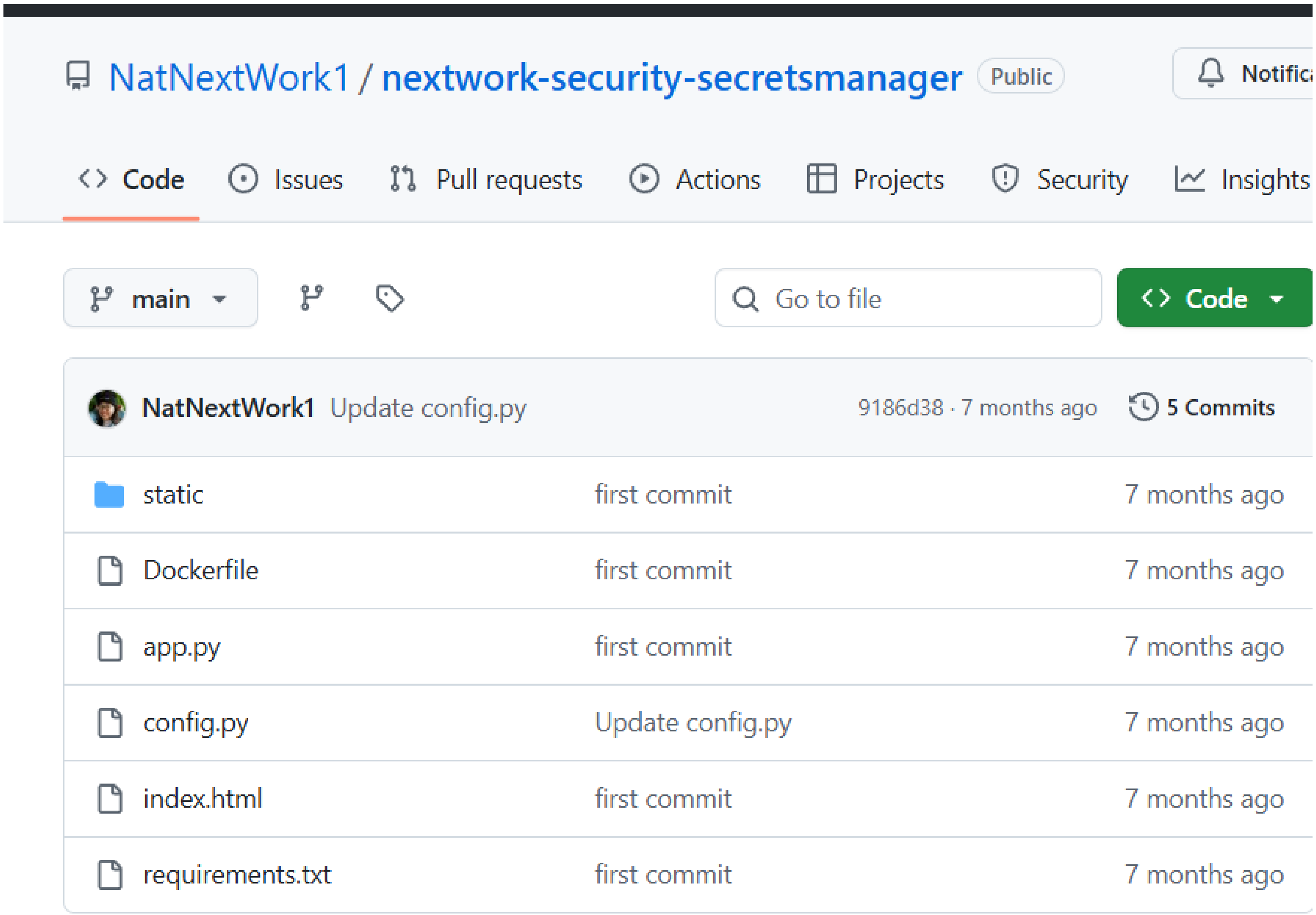
How to update an insecure web app to use AWS Secrets Manager?



Git hub repository to use:

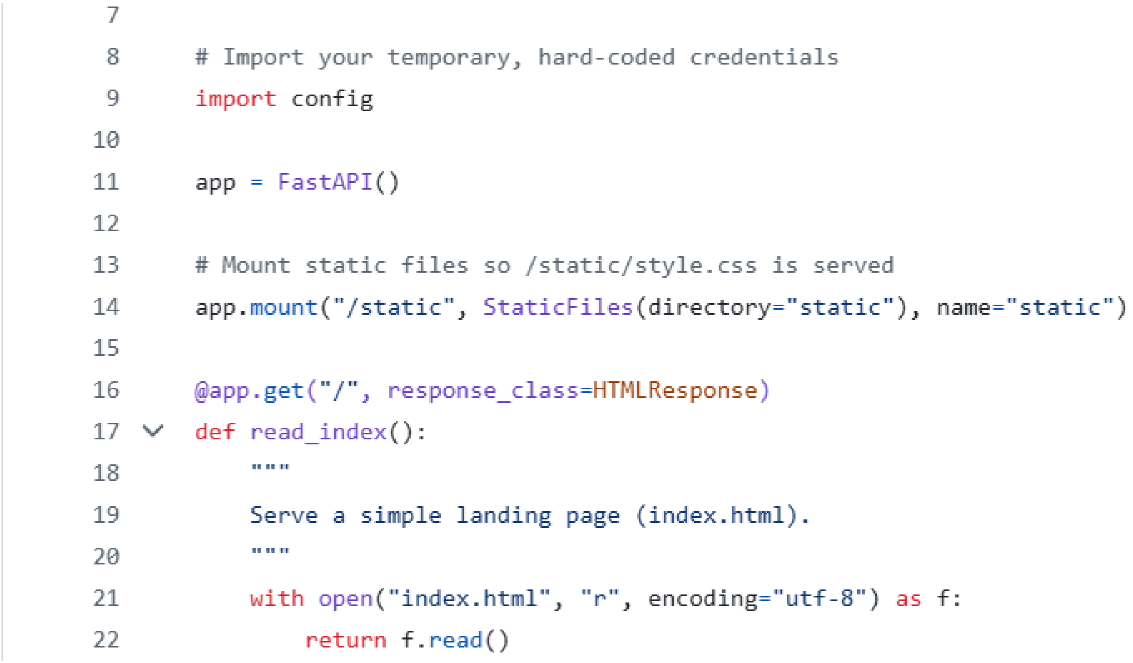
https://github.com/NatNextWork1/nextwork-security-secretsmanager



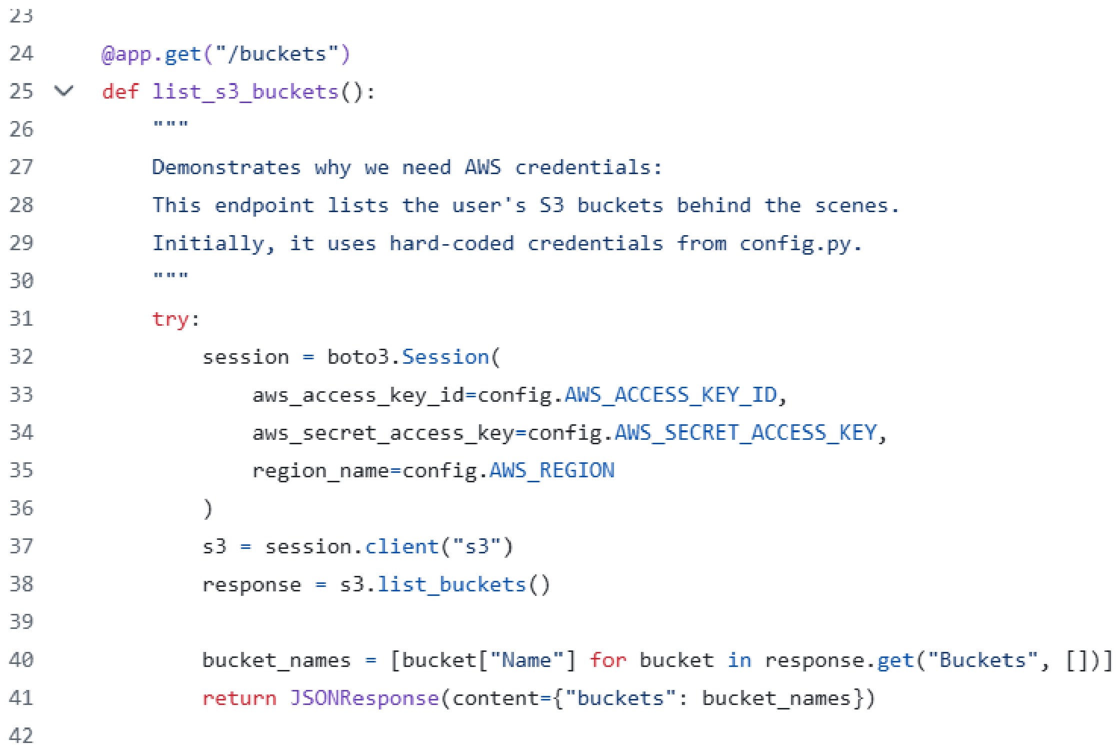
NatNextWork1 Update config.py 9186d38 · 7 months ago 5 Commits

static	first commit	7 months ago
Dockerfile	first commit	7 months ago
app.py	first commit	7 months ago
config.py	Update config.py	7 months ago
index.html	first commit	7 months ago
requirements.txt	first commit	7 months ago

app.py
#Import your temporary, hard-coded credentials.
Def list_s3_buckets():

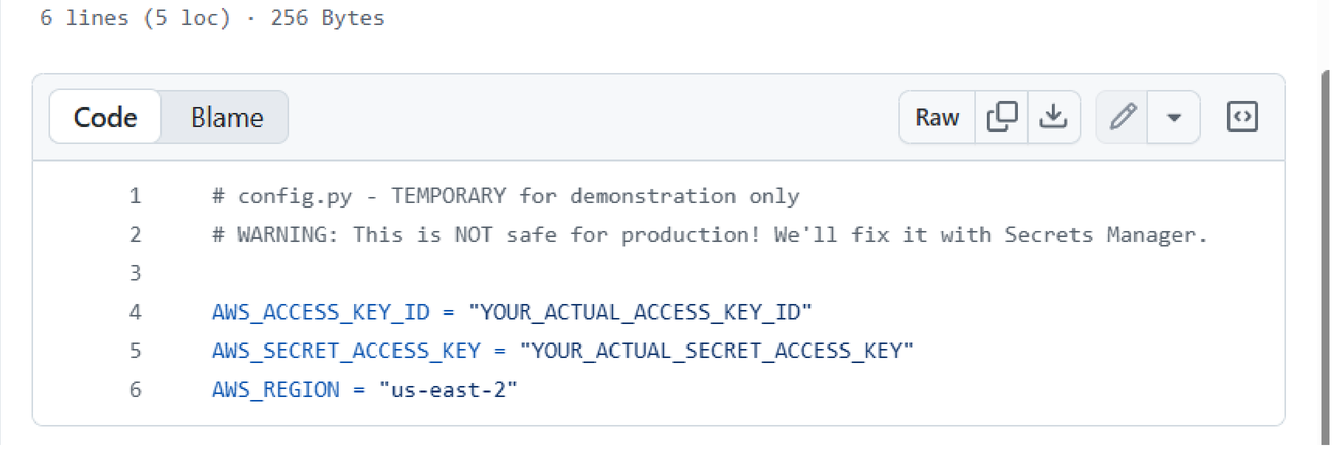


```python

# Import your temporary, hard-coded credentials
import config

app = FastAPI()

# Mount static files so /static/style.css is served
app.mount("/static", StaticFiles(directory="static"), name="static")

@app.get("/", response_class=HTMLResponse)
def read_index():
    """
    Serve a simple landing page (index.html).
    """
    with open("index.html", "r", encoding="utf-8") as f:
        return f.read()
```



```python

@app.get("/buckets")
def list_s3_buckets():
    """
    Demonstrates why we need AWS credentials:
    This endpoint lists the user's S3 buckets behind the scenes.
    Initially, it uses hard-coded credentials from config.py.
    """
    try:
        session = boto3.Session(
            aws_access_key_id=config.AWS_ACCESS_KEY_ID,
            aws_secret_access_key=config.AWS_SECRET_ACCESS_KEY,
            region_name=config.AWS_REGION
        )
        s3 = session.client("s3")
        response = s3.list_buckets()

        bucket_names = [bucket["Name"] for bucket in response.get("Buckets", [])]
        return JSONResponse(content={"buckets": bucket_names})

```

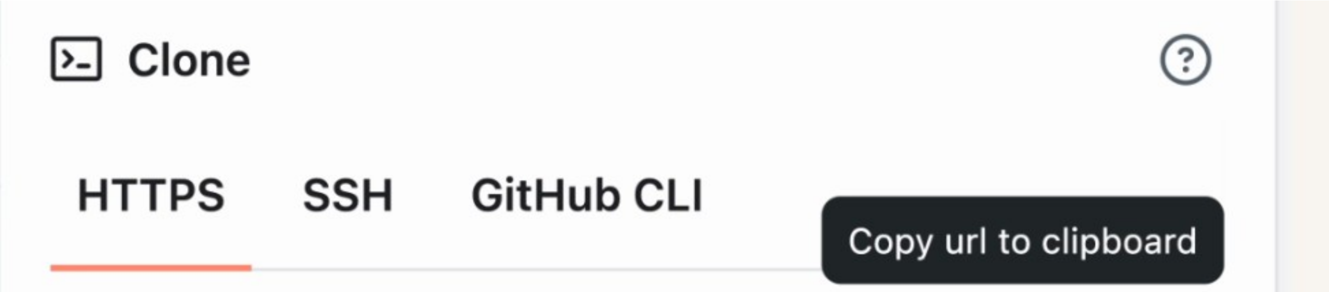
config.py – Hard-coded credentials



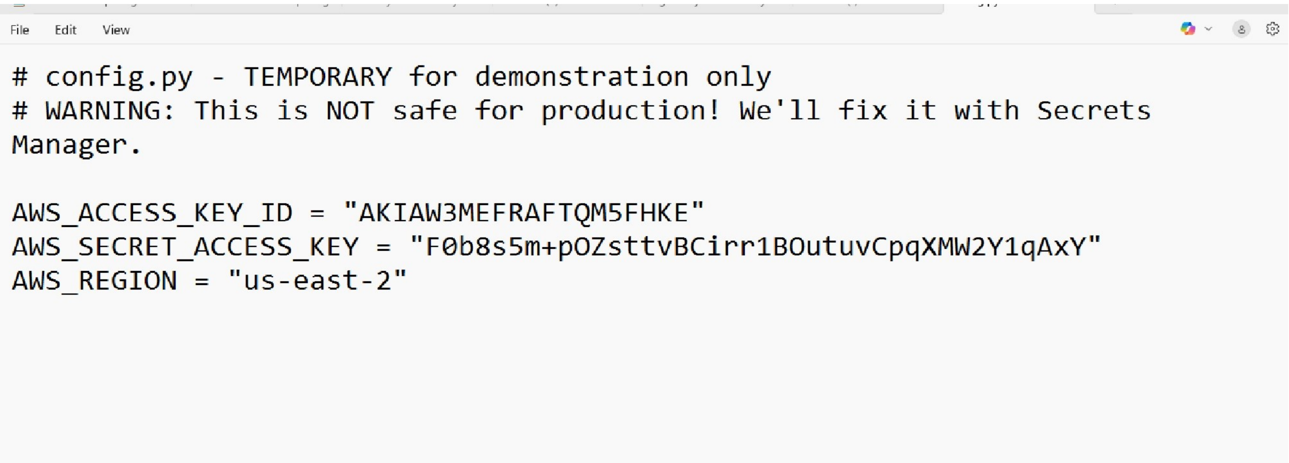
6 lines (5 loc) · 256 Bytes

```
# config.py - TEMPORARY for demonstration only
# WARNING: This is NOT safe for production! We'll fix it with Secrets Manager.

AWS_ACCESS_KEY_ID = "YOUR_ACTUAL_ACCESS_KEY_ID"
AWS_SECRET_ACCESS_KEY = "YOUR_ACTUAL_SECRET_ACCESS_KEY"
AWS_REGION = "us-east-2"
```

Get the copy of the URL

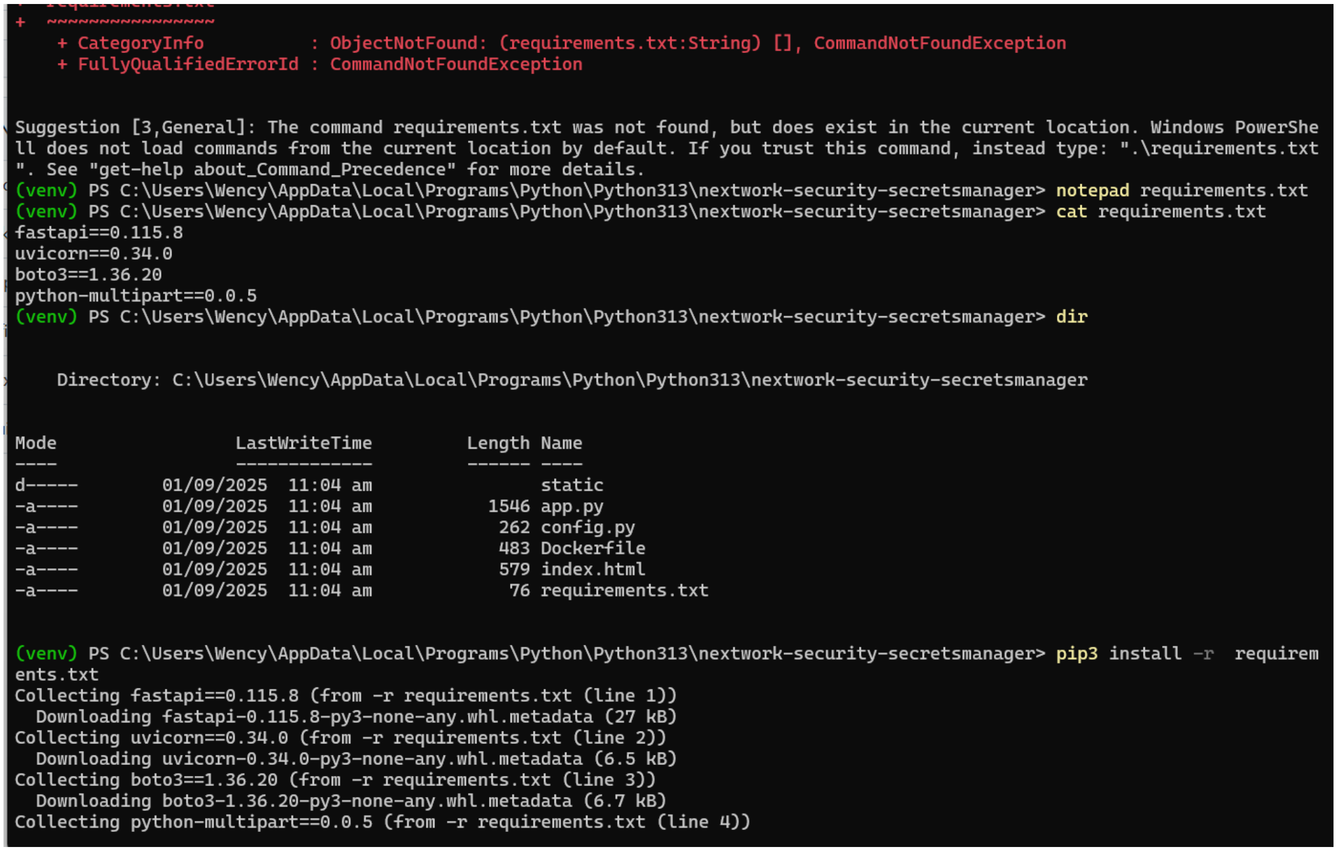


config.py edited credentials



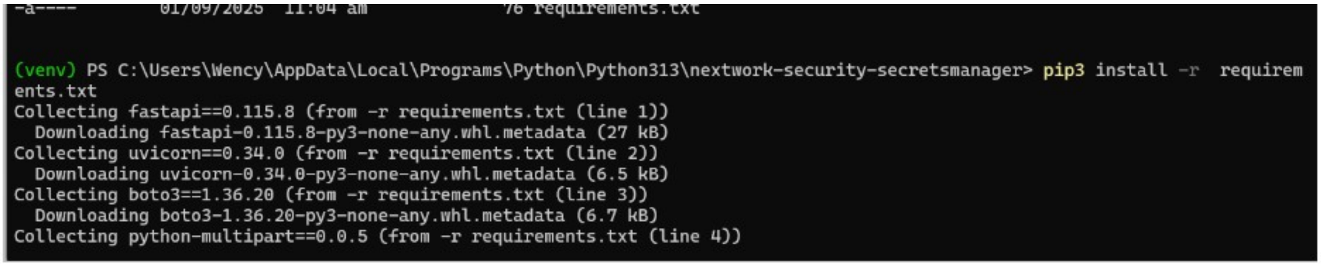
```
# config.py - TEMPORARY for demonstration only
# WARNING: This is NOT safe for production! We'll fix it with Secrets
Manager.

AWS_ACCESS_KEY_ID = "AKIAW3MEFRAFTQM5FHKE"
AWS_SECRET_ACCESS_KEY = "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"
AWS_REGION = "us-east-2"
```

Activated Virtual Environment



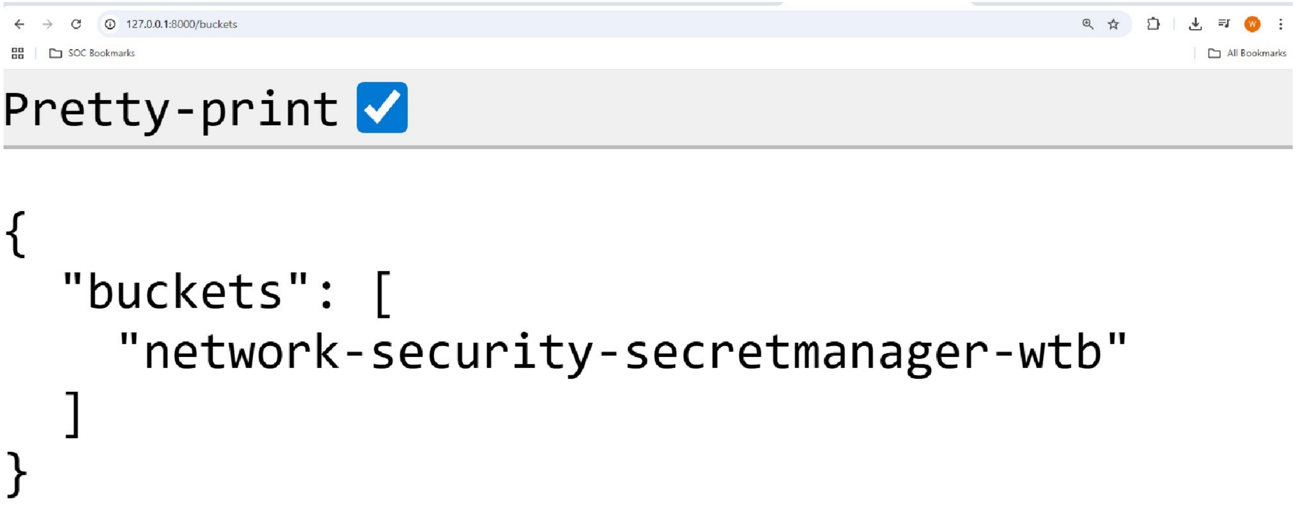
```
+  requirements.txt
+  ~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (requirements.txt:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException


Suggestion [3,General]: The command requirements.txt was not found, but does exist in the current location. Windows PowerShe
ll does not load commands from the current location by default. If you trust this command, instead type: ".\requirements.txt
". See "get-help about_Command_Precedence" for more details.
(venv) PS C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager> notepad requirements.txt
(venv) PS C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager> cat requirements.txt
fastapi==0.115.8
uvicorn==0.34.0
boto3==1.36.20
python-multipart==0.0.5
(venv) PS C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager> dir


    Directory: C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        01/09/2025  11:04 am                static
-a----        01/09/2025  11:04 am           1546 app.py
-a----        01/09/2025  11:04 am            262 config.py
-a----        01/09/2025  11:04 am            483 Dockerfile
-a----        01/09/2025  11:04 am            579 index.html
-a----        01/09/2025  11:04 am             76 requirements.txt


(venv) PS C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager> pip3 install -r  requirem
ents.txt
Collecting fastapi==0.115.8 (from -r requirements.txt (line 1))
  Downloading fastapi-0.115.8-py3-none-any.whl.metadata (27 kB)
Collecting uvicorn==0.34.0 (from -r requirements.txt (line 2))
  Downloading uvicorn-0.34.0-py3-none-any.whl.metadata (6.5 kB)
Collecting boto3==1.36.20 (from -r requirements.txt (line 3))
  Downloading boto3-1.36.20-py3-none-any.whl.metadata (6.7 kB)
Collecting python-multipart==0.0.5 (from -r requirements.txt (line 4))
```

Install required packages boto3, fastapi, uvicorn



```
-a----        01/09/2025  11:04 am             76 requirements.txt


(venv) PS C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager> pip3 install -r  requirem
ents.txt
Collecting fastapi==0.115.8 (from -r requirements.txt (line 1))
  Downloading fastapi-0.115.8-py3-none-any.whl.metadata (27 kB)
Collecting uvicorn==0.34.0 (from -r requirements.txt (line 2))
  Downloading uvicorn-0.34.0-py3-none-any.whl.metadata (6.5 kB)
Collecting boto3==1.36.20 (from -r requirements.txt (line 3))
  Downloading boto3-1.36.20-py3-none-any.whl.metadata (6.7 kB)
Collecting python-multipart==0.0.5 (from -r requirements.txt (line 4))
```

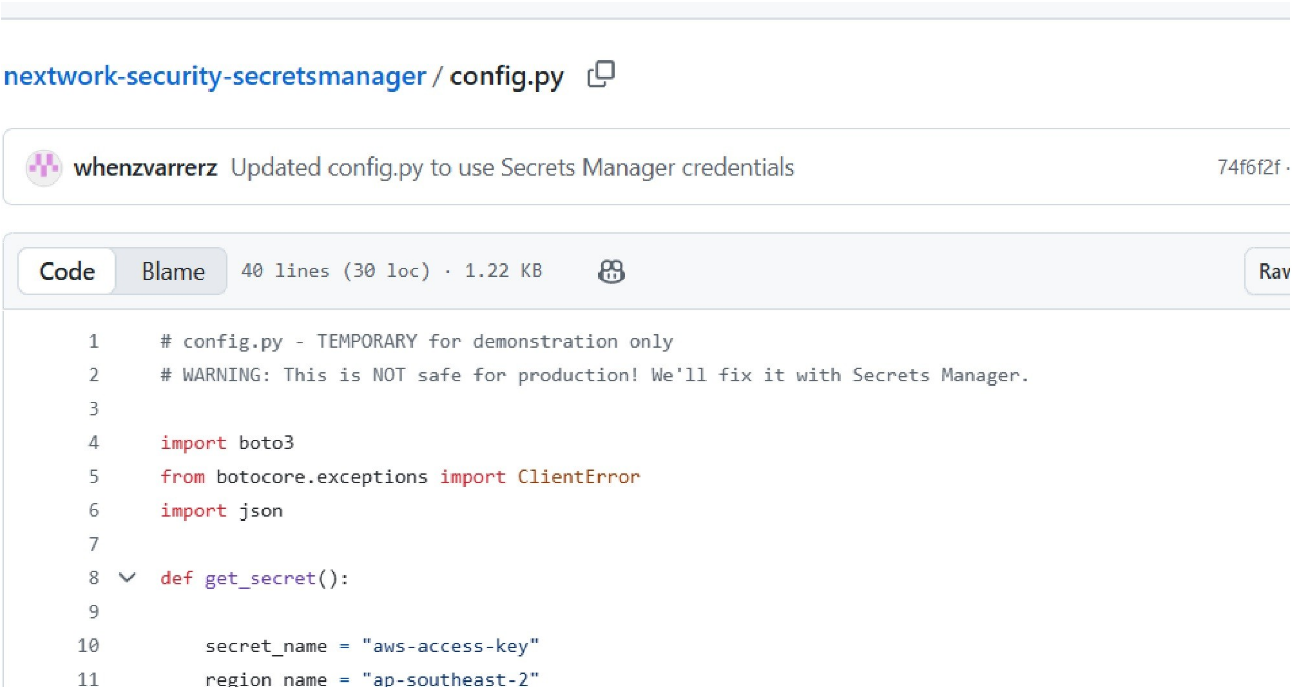
Web app working after configuring the right Access key and Secret access key.



Pretty-print ☑

```
{
  "buckets": [
    "network-security-secretmanager-wtb"
  ]
}
```

Push configuration commit success!

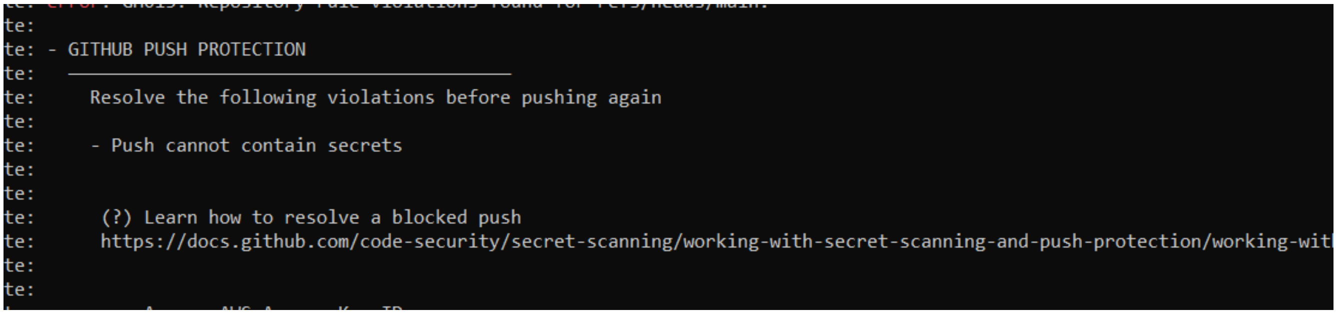


whenzvarrerz Updated config.py to use Secrets Manager credentials 74f6f2f ·

40 lines (30 loc) · 1.22 KB

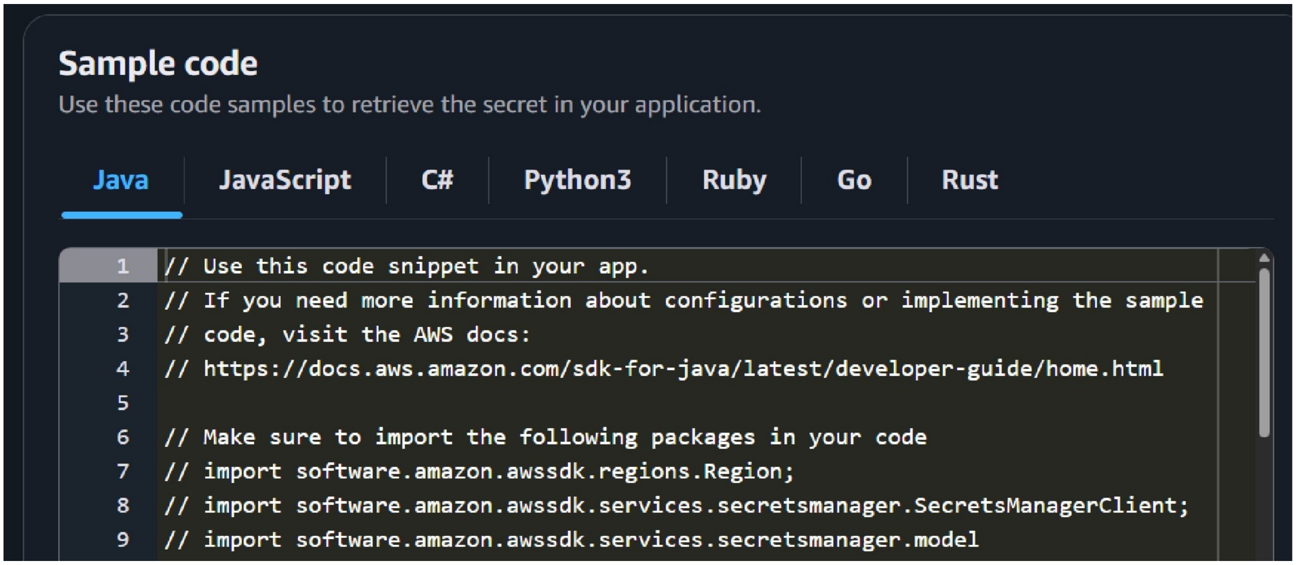
```
# config.py - TEMPORARY for demonstration only
# WARNING: This is NOT safe for production! We'll fix it with Secrets Manager.

import boto3
from botocore.exceptions import ClientError
import json

def get_secret():

    secret_name = "aws-access-key"
    region_name = "ap-southeast-2"
```

GitHub Secret Scanning Block



```
te: error: GH013: Repository rule violations found for refs/heads/main.
te:
te: - GITHUB PUSH PROTECTION
te:   ——————————————————————————————————————————
te:     Resolve the following violations before pushing again
te:
te:     - Push cannot contain secrets
te:
te:
te:      (?) Learn how to resolve a blocked push
te:      https://docs.github.com/code-security/secret-scanning/working-with-secret-scanning-and-push-protection/working-wit
te:
te:
              Amazon AWS Access Key ID
```

Sample code for retrieval

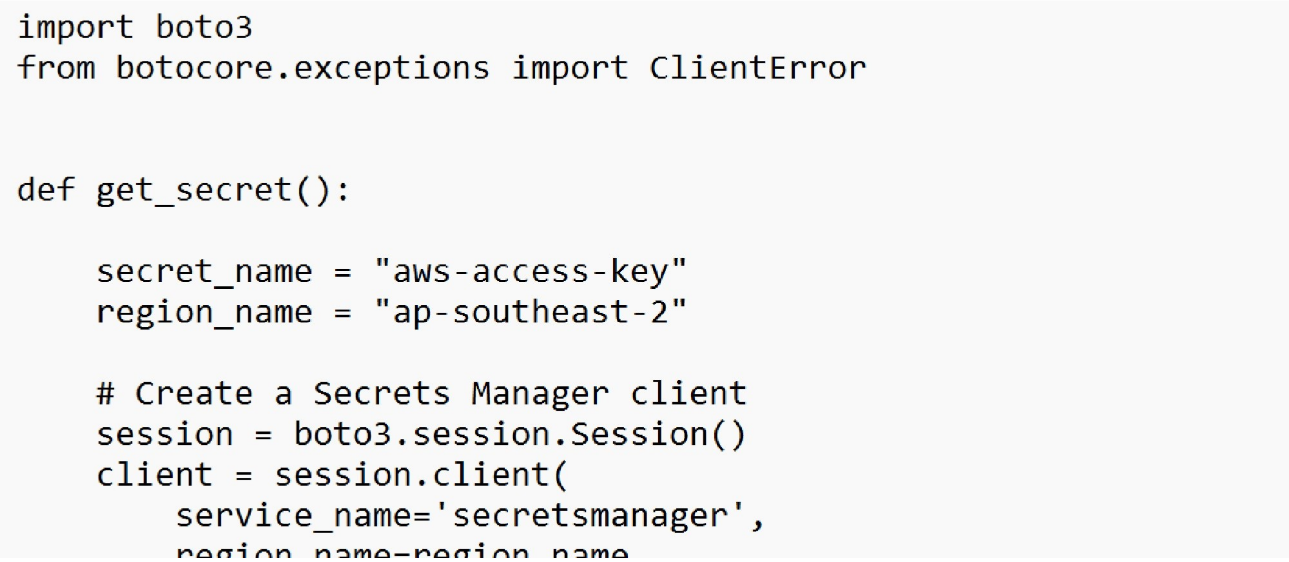


Sample code

Use these code samples to retrieve the secret in your application.

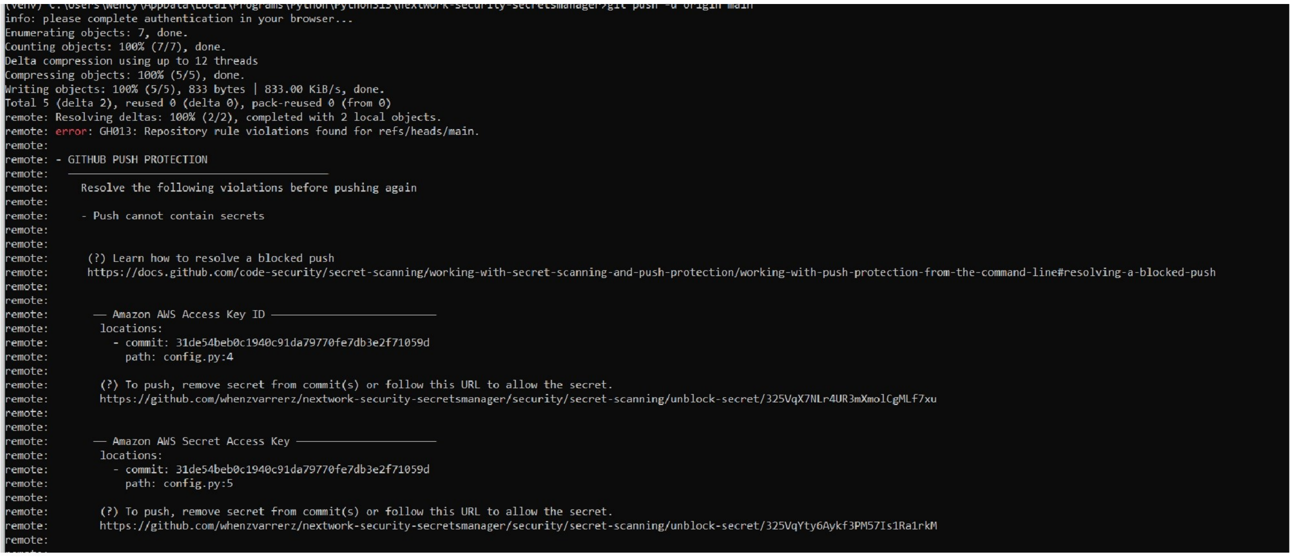
```
// Use this code snippet in your app.
// If you need more information about configurations or implementing the sample
// code, visit the AWS docs:
// https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/home.html

// Make sure to import the following packages in your code
// import software.amazon.awssdk.regions.Region;
// import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
// import software.amazon.awssdk.services.secretsmanager.model
```

Updated configuration file



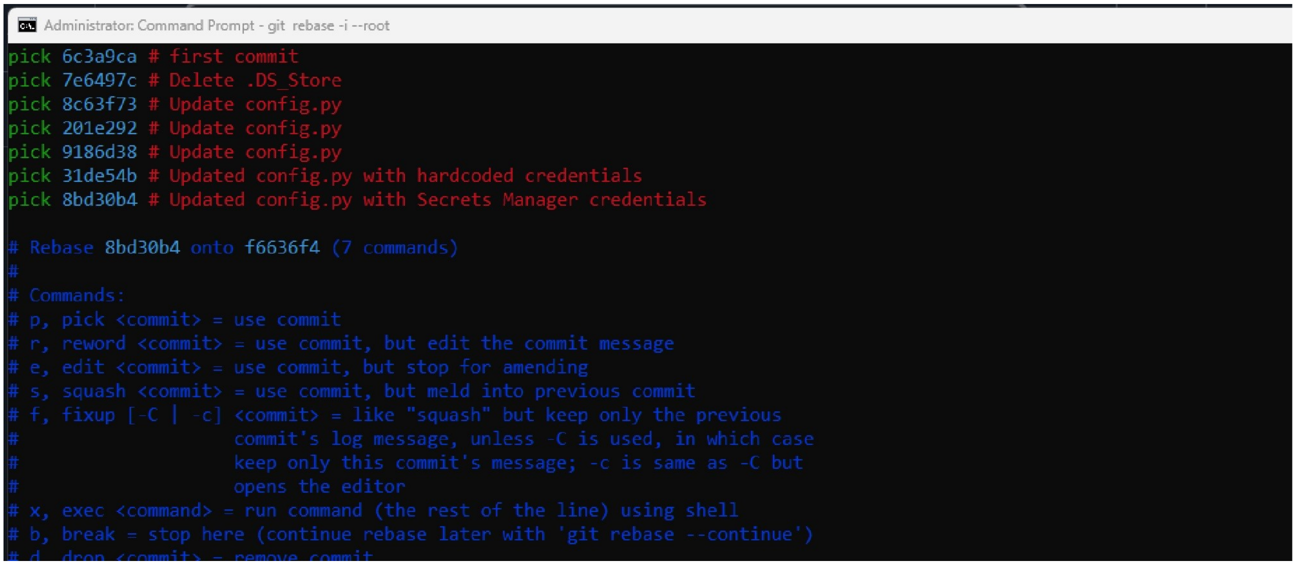
```
import boto3
from botocore.exceptions import ClientError


def get_secret():

    secret_name = "aws-access-key"
    region_name = "ap-southeast-2"

    # Create a Secrets Manager client
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=region_name
```

Push cannot contain secrets



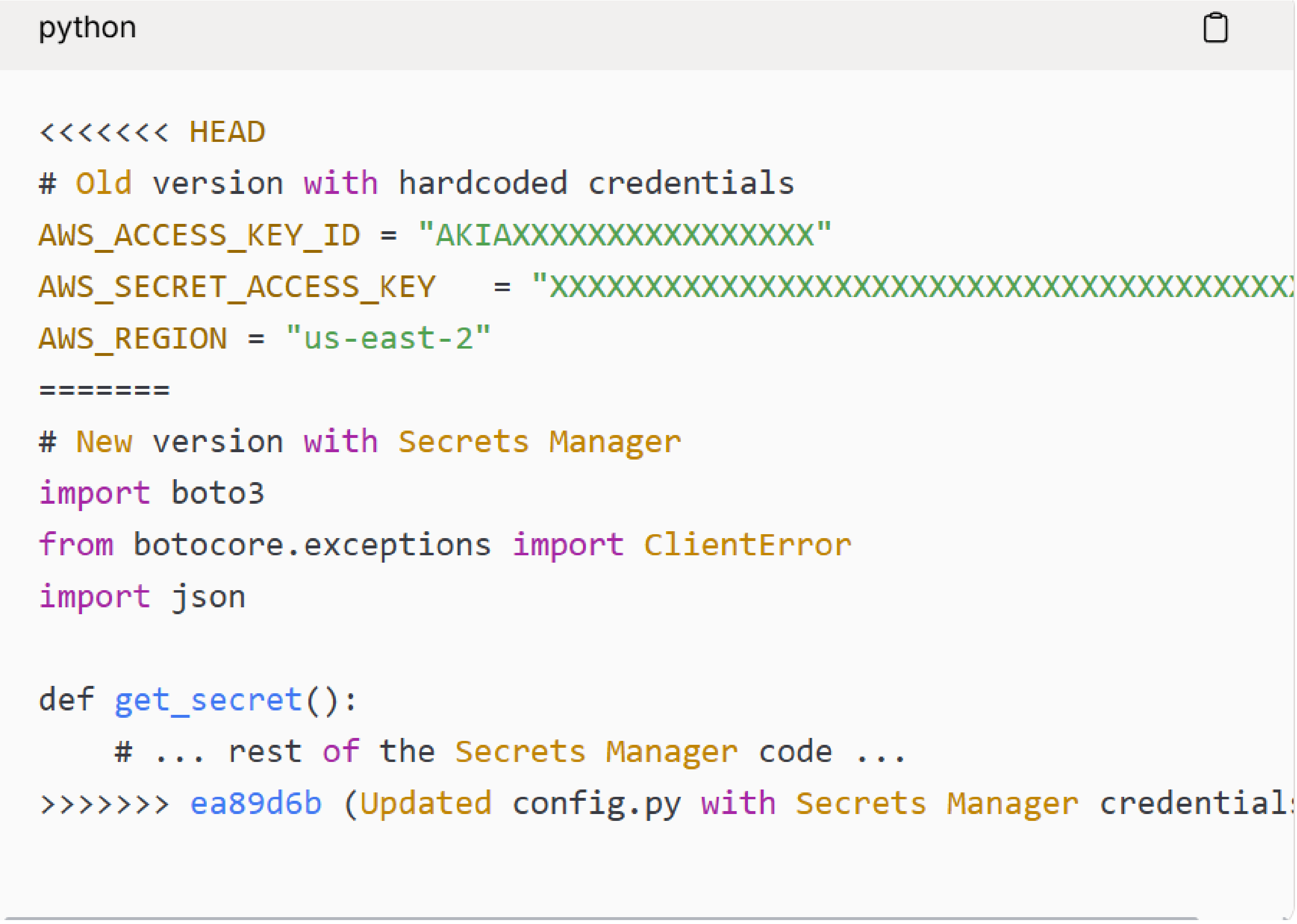
```
(venv) C:\Users\Wency\AppData\Local\Programs\Python\Python313\nextwork-security-secretsmanager>git push -u origin main
info: please complete authentication in your browser...
Enumerating objects: 7, done.
Counting objects: 100% (7/7), done.
Delta compression using up to 12 threads
Compressing objects: 100% (5/5), done.
Writing objects: 100% (5/5), 833 bytes | 833.00 KiB/s, done.
Total 5 (delta 2), reused 0 (delta 0), pack-reused 0 (from 0)
remote: Resolving deltas: 100% (2/2), completed with 2 local objects.
remote: error: GH013: Repository rule violations found for refs/heads/main.
remote:
remote: - GITHUB PUSH PROTECTION
remote:   ————————————————————————————————————————
remote:     Resolve the following violations before pushing again
remote:
remote:     - Push cannot contain secrets
remote:
remote:
remote:      (?) Learn how to resolve a blocked push
remote:      https://docs.github.com/code-security/secret-scanning/working-with-secret-scanning-and-push-protection/working-with-push-protection-from-the-command-line#resolving-a-blocked-push
remote:
remote:
remote:       —— Amazon AWS Access Key ID ——————————————————————————
remote:        locations:
remote:          - commit: 31de54beb0c1940c91da79770fe7db3e2f71059d
remote:            path: config.py:4
remote:
remote:        (?) To push, remove secret from commit(s) or follow this URL to allow the secret.
remote:        https://github.com/whenzvarrerz/nextwork-security-secretsmanager/security/secret-scanning/unblock-secret/325VqX7NLr4UR3mXmolCgMLf7xu
remote:
remote:
remote:       —— Amazon AWS Secret Access Key ——————————————————————
remote:        locations:
remote:          - commit: 31de54beb0c1940c91da79770fe7db3e2f71059d
remote:            path: config.py:5
remote:
remote:        (?) To push, remove secret from commit(s) or follow this URL to allow the secret.
remote:        https://github.com/whenzvarrerz/nextwork-security-secretsmanager/security/secret-scanning/unblock-secret/325VqYty6Aykf3PM57Is1Ra1rkM
remote:
```

Rebase commit editor dropping



```
pick 6c3a9ca # first commit
pick 7e6497c # Delete .DS_Store
pick 8c63f73 # Update config.py
pick 201e292 # Update config.py
pick 9186d38 # Update config.py
pick 31de54b # Updated config.py with hardcoded credentials
pick 8bd30b4 # Updated config.py with Secrets Manager credentials

# Rebase 8bd30b4 onto f6636f4 (7 commands)
#
# Commands:
# p, pick <commit> = use commit
# r, reword <commit> = use commit, but edit the commit message
# e, edit <commit> = use commit, but stop for amending
# s, squash <commit> = use commit, but meld into previous commit
# f, fixup [-C | -c] <commit> = like "squash" but keep only the previous
#                    commit's log message, unless -C is used, in which case
#                    keep only this commit's message; -c is same as -C but
#                    opens the editor
# x, exec <command> = run command (the rest of the line) using shell
# b, break = stop here (continue rebase later with 'git rebase --continue')
# d, drop <commit> = remove commit
```

Merge conflicts. Resolve by choosing which version to keep and remove markers.

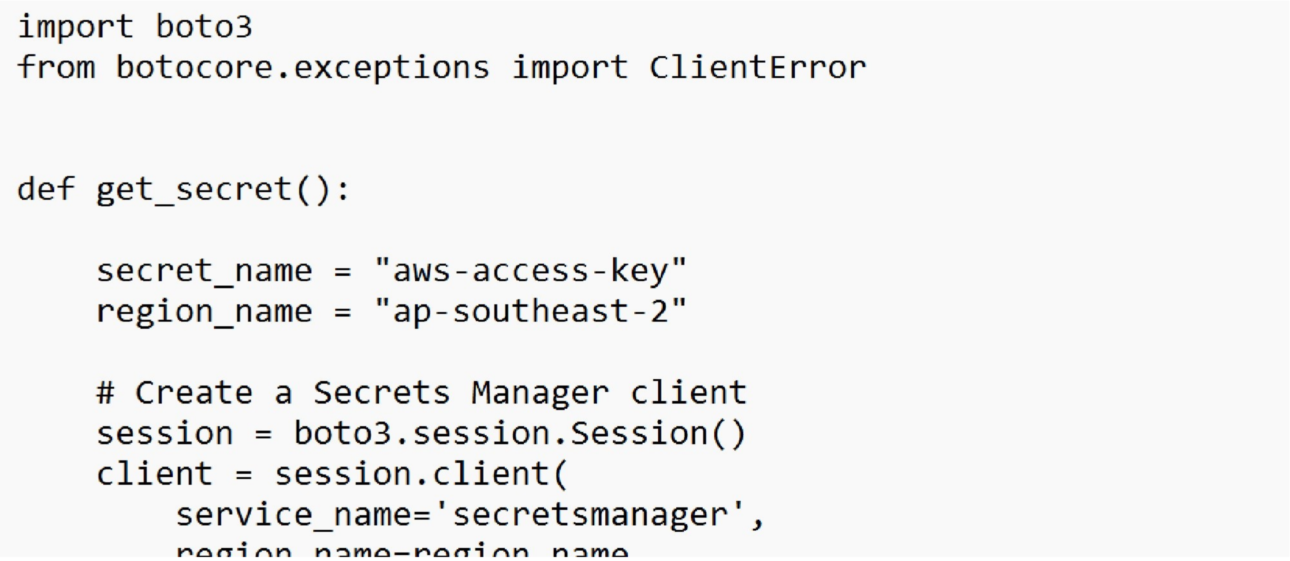


```python
<<<<<<< HEAD
# Old version with hardcoded credentials
AWS_ACCESS_KEY_ID = "AKIAXXXXXXXXXXXXXXXX"
AWS_SECRET_ACCESS_KEY   = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
AWS_REGION = "us-east-2"
=======
# New version with Secrets Manager
import boto3
from botocore.exceptions import ClientError
import json

def get_secret():
    # ... rest of the Secrets Manager code ...
>>>>>>> ea89d6b (Updated config.py with Secrets Manager credential
```

- Delete:

entire section <<<<< HEAD ==== for hard-coded credentials.
===== end of file line
>>>>> feature-branch

Updated config.py clean of any hard-coded credentials
Show only code to retrieve credentials from AWS



```
import boto3
from botocore.exceptions import ClientError


def get_secret():

    secret_name = "aws-access-key"
    region_name = "ap-southeast-2"

    # Create a Secrets Manager client
    session = boto3.session.Session()
    client = session.client(
        service_name='secretsmanager',
        region_name=region_name
```