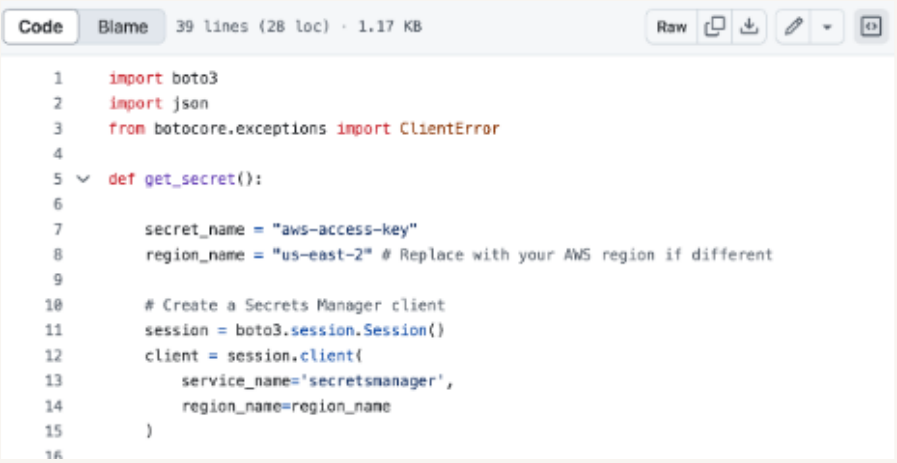
nextwork.org

Secure Secrets with Secrets Manager

Russell Geisler



R
Russell Geisler
NextWork Student

Introducing Today's Project!

In this project I will demonstrate how to store code securely using AWS Secrets Manager

Tools and concepts

I learned about GitHub and AWS Secrets Manager

Project reflection

This project took about 3 hours

I did this projet to learn more about AWS Secrets Manager

Hardcoding credentials

Credentials in code can leave you open to attackers easily being able to access and change or delete your resources

In the config file I put my own credentials

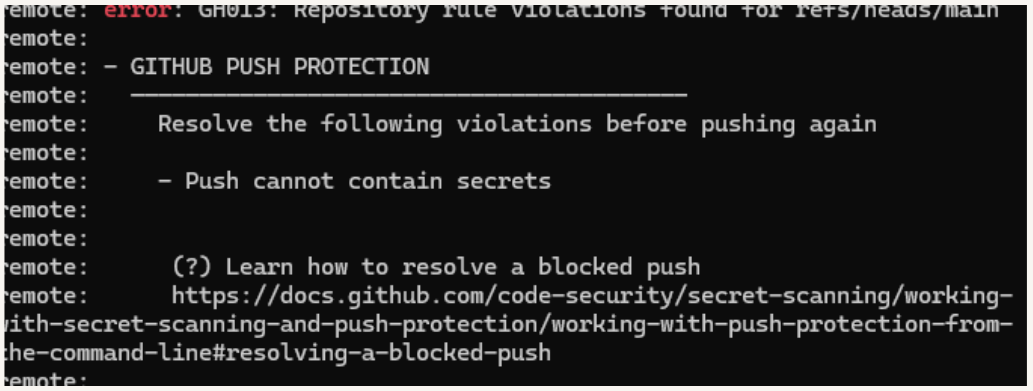
```
# config.py - TEMPORARY for demonstration only
# WARNING: This is NOT safe for production! We'll
fix it with Secrets Manager.

AWS_ACCESS_KEY_ID = "AKIAW3MEFRAFTQM5FHKE"
AWS_SECRET_ACCESS_KEY =
"F0b8s5m+pOZsttvBCirr1BOutuvCpqXMW2Y1qAxY""YOUR_ACT
UAL_SECRET_ACCESS_KEY"
AWS_REGION = "us-east-2"
```

Pushing Insecure Code to GitHub

I fork the original repository so i can add my own edits to it. Cloning would have made an offline copy

I used git remote add origin <my URL> to add repository, git commit adds the changes, git push -u origin main pushes the changes to the repositiory

Github blocked the request because it detected some sensitive credentials

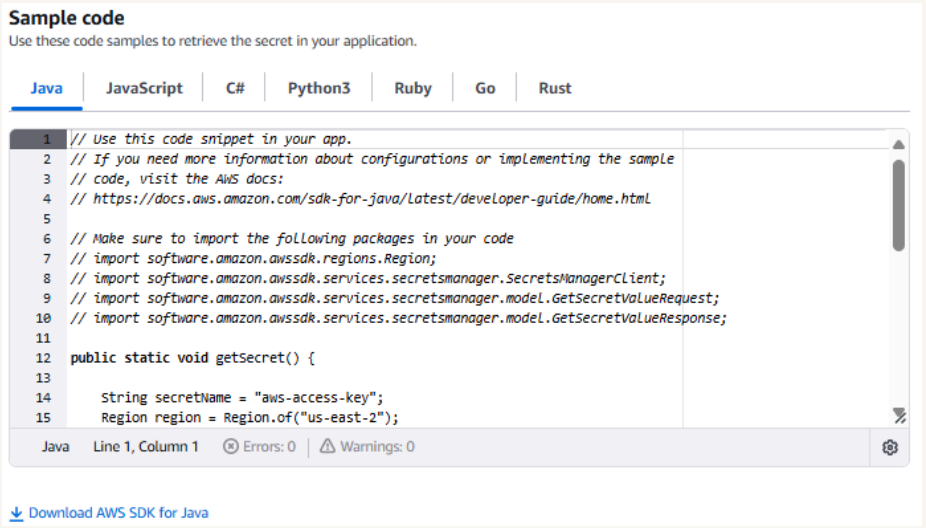


Secrets Manager

Secrets Manager is used for keeping credentials

Secret rotation is the process of automatically changing your secrets on a regular schedule. This is a security best practice because it reduces the risk of compromised credentials.

Secret Manager shows sample code which is very helpful! It shows you exactly how to retrieve your secret from Secrets Manager in your application code.



Updating the web app code

I used the sample code and made a new config fle using notepad

These lines are responsible for actually retrieving the credentials from the secret and assigning them to the AWS_ACCESS_KEY_ID, AWS_SECRET_ACCESS_KEY, and AWS_REGION variables that our app.py code expects

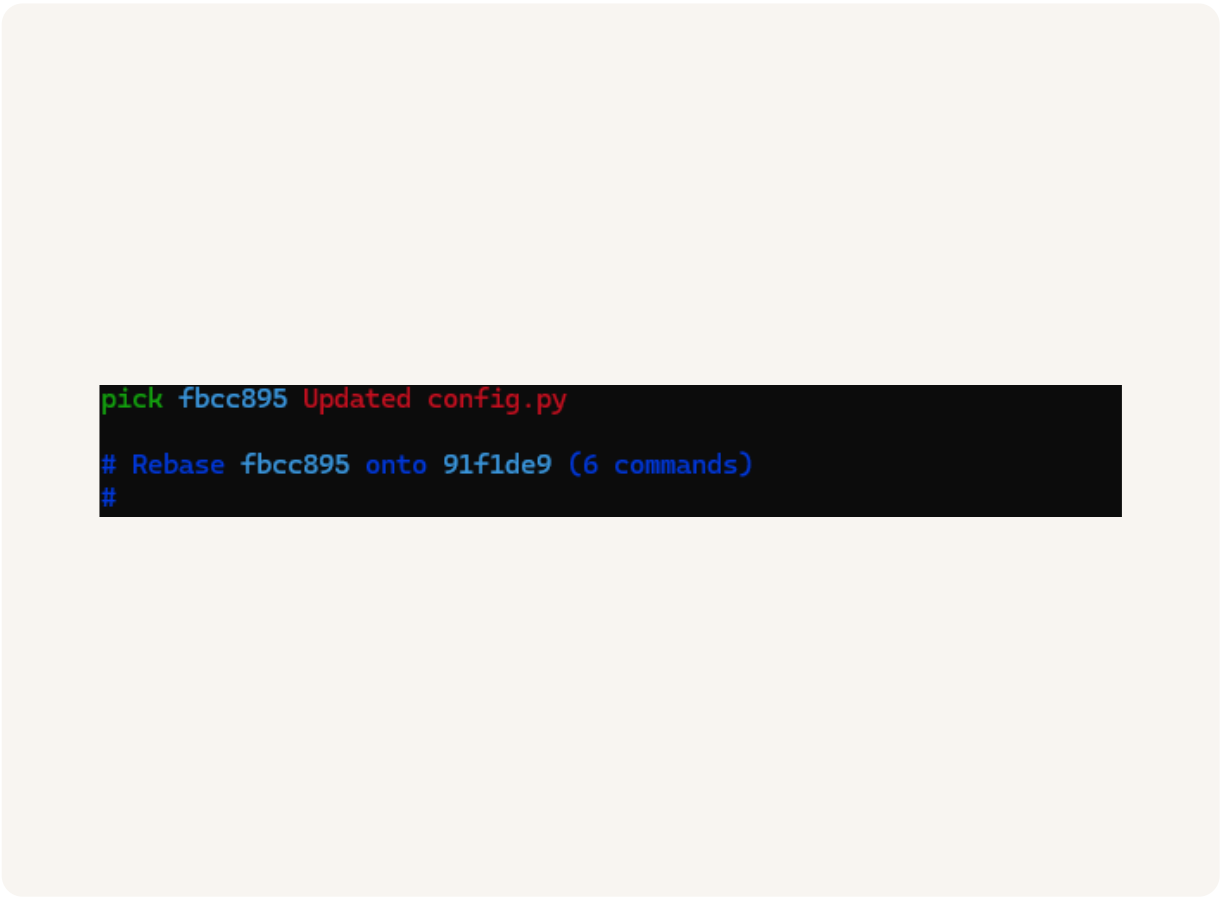
```
def get_secret():

    secret_name = "aws-access-key"
    region_name = "us-east-2"

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

    try:
        get_secret_value_response =
client.get_secret_value(
            SecretId=secret_name
        )
    except ClientError as e:
        # For a list of exceptions thrown, see
        #
https://docs.aws.amazon.com/secretsmanager/latest
/apireference/API_GetSecretValue.html
        raise e

    secret =
get_secret_value_response['SecretString']

    # Your code goes here.
|
```

Rebasing the repository

Git rebasing is used to rewrite commit history

Git detects conflicting changes in a file. I reslved the issue by deleting conflicts

I was able to pull up the config.py filein my respoitory and verify the credntials were not able to be seen



The place to learn & showcase your skills

Check out nextwork.org for more projects