

Documentation for GoLang Script to identify and validate any AWS IAM keys embedded in the provided repository's code:

The submitted code is working and able to provide the required results. Please note the following points:-

1. The code works for the GitHub repositories only. It can be easily scaled up to cover GitLab and Bitbucket by incorporating their respective packages and following the logic used for the GitHub repositories.
2. The code requires GitHub token, AWS Region and repository's author and name in order to provide the results. The token is needed for the authentication purpose and is mandatory.
3. The code has been properly commented on in order to make it readable and understandable. This will also help in understanding the thought process involved in coming up with this solution for the problem.
4. Since I'm writing code in GoLang for the first time, I couldn't touch upon the optional enhancements. They are very interesting but I need time to read and learn about these features and how to include them in my code.

Approach used to find the solution:

The problem has been broken down into parts and then the solution to each one of them provided me with the final result. Following are the parts of the problem:

1. Authentication and creation of GitHub client so that we can access the desired repository
2. Getting the regex pattern for IAM Keys (access key ID and Secret Access Key) so that we can use them for finding possible IAM Keys.
3. Getting the list of branches for the repository and then using loop to for processing each of them:
 - a. Finding the content of each branch and then pattern matching is used to find possible Keys.
 - b. Finding the list of commits and scanning each of them for the IAM Keys patterns
4. Using AWS API for the authentication of found possible matches for IAM Keys.

Running the script:

To find the output of the script, go to the folder containing the code and run the following command on the terminal:-

go run SearchingGit.go

After this, you will be asked for four pieces of information. Kindly enter them:

Enter your GitHub access token:

Enter the repository owner:

Enter the repository name:

Enter the AWS region:

After providing these values the processing will begin and the result will be displayed on the terminal. Here is a peak into what we got when we used the sample GitHub repository provided as the test case.

(1) Scanning branch: leak

Scanning the code for the IAM Keys:--

Possible IAM key(s):access key ID was found in file: leak.js (Branch: leak)

AKIA57VFSPPO3QT5WAXG

AKIAUMNA5JFAU5RDXHEG

Possible IAM key(s):secret access key was found in file: leak.js (Branch: leak)

7k+ptP9Ud9KuwV0Ren28YGpx5hEMjm6IK4ay8US

j3JgkGbF3f7PLALLViCB+mw1W9plkfneqvAFT2B2

-----TESTING Them using AWS APIs-----

-----ERROR: AWS API failed-----

Using accessKeyID: AKIA57VFSPPO3QT5WAXG & secretAccessKey:

7k+ptP9Ud9KuwV0Ren28YGpx5hEMjm6IK4ay8US, Error calling AWS API:

InvalidClientTokenId: The security token included in the request is invalid.

status code: 403, request id: ee9fb50a-1304-41b6-a593-a76b0ad7c9ef

-----ERROR: AWS API failed-----

Using accessKeyID: AKIA57VFSPPO3QT5WAXG & secretAccessKey:

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, Error calling AWS API:

InvalidClientTokenId: The security token included in the request is invalid.

status code: 403, request id: 207c1c7c-e055-4660-9577-700e586bf6a4

-----ERROR: AWS API failed-----

Using accessKeyID: AKIAUMNA5JFAU5RDXHEG & secretAccessKey:

7k+ptP9Ud9KuwV0Ren28YGpx5hEMjm6IK4ay8US, Error calling AWS API:

SignatureDoesNotMatch: The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method. Consult the service documentation for details.

status code: 403, request id: f203772e-3f7a-4d90-8edf-bc10171333fd

-----ERROR: AWS API failed-----

Using accessKeyID: AKIAUMNA5JFAU5RDXHEG & secretAccessKey:

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, Error calling AWS API:

SignatureDoesNotMatch: The request signature we calculated does not match the

signature you provided. Check your AWS Secret Access Key and signing method.
Consult the service documentation for details.

status code: 403, request id: a3cacb66-c5fb-464c-9982-a05a32e5c757

Scanning the commits for the IAM Keys

Scanning commit with SHA : a24771e4678261b3b9ceb3e222eb02539b3d9d05

-----No IAM Key(s) found in this commit-----

Scanning commit with SHA : 94006ad4c1b6432702d0f663e17e2af9f35e91d9

-----No IAM Key(s) found in this commit-----

Scanning commit with SHA : 373b38356967cd38d9b70e3840e41bed0736c21c

-----No IAM Key(s) found in this commit-----

Scanning commit with SHA : d01c9b4c5fe063be55102f30187c6bc45ef7e024

-----No IAM Key(s) found in this commit-----

(2) Scanning branch: main

Scanning the code for the IAM Keys:--

Possible IAM key(s):access key ID was found in file: .config (Branch: main)

AKIAUMNA5JFAXO65BXNJ

AKIAUMNA5JFA62FXEE4F

Possible IAM key(s):secret access key was found in file: .config (Branch: main)

WCCgBZuC19LCJOFlkBgKFoeqYoWzR+7SzfHD04M3

C32AzNrF6ZCZs8fqS82UXisHrrimjB98SDpQ6d5A

-----TESTING Them using AWS APIs-----

-----SUCCESSFUL FINDING-----

IAM key(s) found in file: .config (Branch: main)

AccessKeyID found AKIAUMNA5JFAXO65BXNJ

SecretAccessKey found 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

-----ERROR: AWS API failed-----

Using accessKeyID: AKIAUMNA5JFAXO65BXNJ & secretAccessKey:

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, Error calling AWS API:

SignatureDoesNotMatch: The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method.

Consult the service documentation for details.

status code: 403, request id: 61d6ab4a-b4cf-4b6a-a53a-64b9b8e2a1a3

-----ERROR: AWS API failed-----

Using accessKeyID: AKIAUMNA5JFA62FXEE4F & secretAccessKey:

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, Error calling AWS API:

InvalidClientTokenId: The security token included in the request is invalid.

status code: 403, request id: 9e963ce2-87f5-4f7a-b015-08641c845dd1

-----ERROR: AWS API failed-----

Using accessKeyID: AKIAUMNA5JFA62FXEE4F & secretAccessKey:

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, Error calling AWS API:

InvalidClientTokenId: The security token included in the request is invalid.

status code: 403, request id: 1d6f401f-eb29-42d6-9fe9-f68a73b32efb

Scanning the commits for the IAM Keys

Scanning commit with SHA : 67975c9f71b84901729ccac14162318ec7d5b89d

-----No IAM Key(s) found in this commit-----

Scanning commit with SHA : 373b38356967cd38d9b70e3840e41bed0736c21c

-----No IAM Key(s) found in this commit-----

Scanning commit with SHA : d01c9b4c5fe063be55102f30187c6bc45ef7e024

-----No IAM Key(s) found in this commit-----