Open Source
Slack Security & Threat Hunting

By: Ashish Bansal
~AshishSecDev

Github: https://github.com/ashishsecdev/Slack-Guardian

Introduction

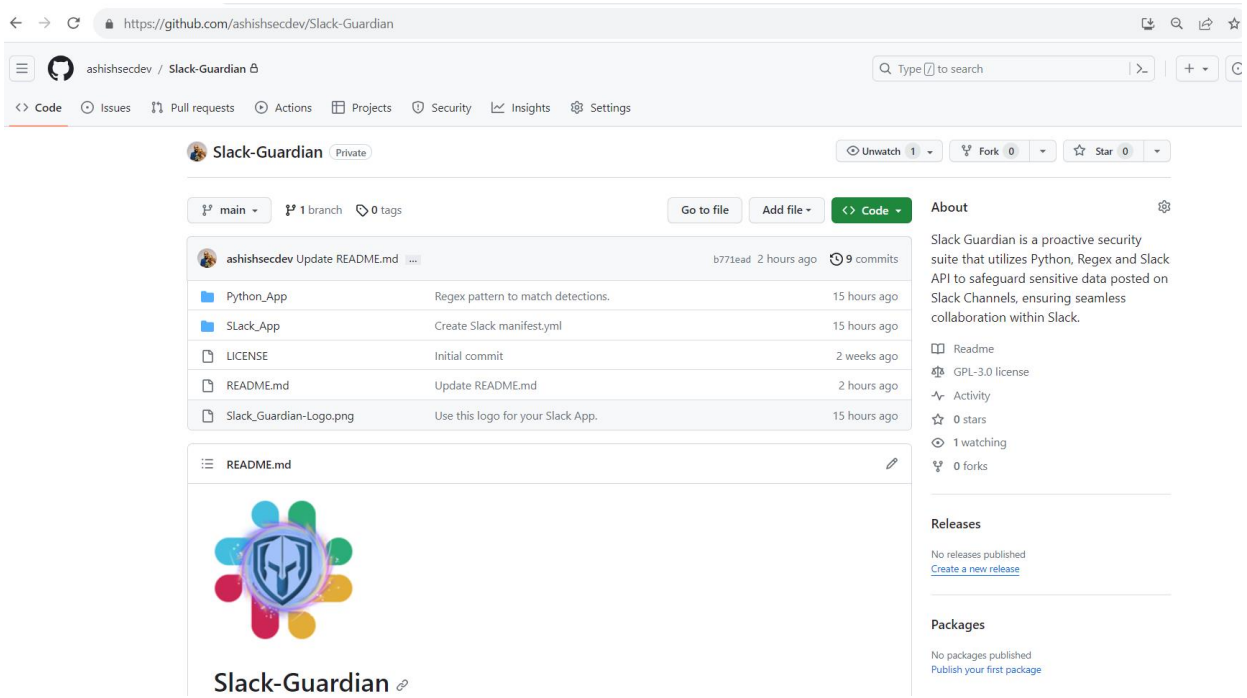
Slack Guardian Slack Security Suite

Slack Guardian, a powerful app designed to give you enhanced control over your Slack channels. With Slack Guardian, you can now monitor your channels for any sensitive information that may have been shared by mistake like confidential data such as code snippets with hardcoded credentials, pre-signed URLs, and PII.

Slack Guardian identifies potential violations based on the specific regex patterns it promptly notifying users about these violations. Additionally, it maintains a detailed record of these violations, providing you with valuable insight about the violations.

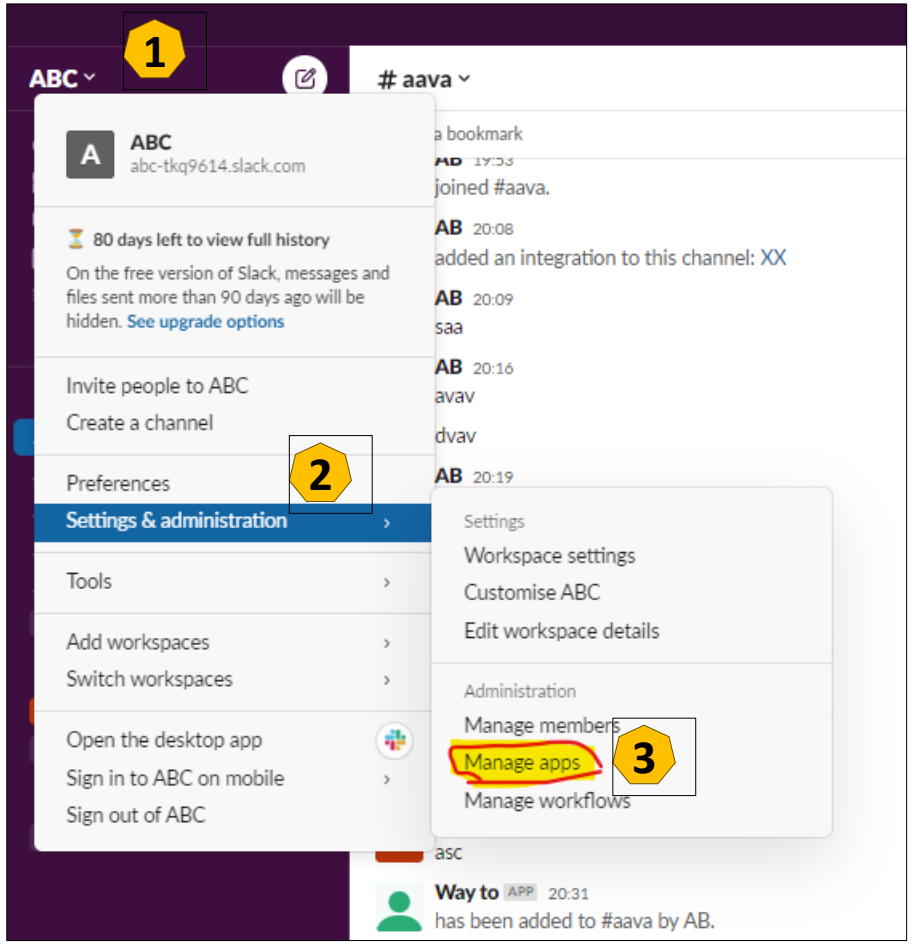
Finally, Slack Guardian automatically removes any identified violations, ensuring your Slack channels remain secure and compliant.

Must have security toolkit for Blue Teams, Security Operations, Threat Hunters and Detection engineers.



Github: https://github.com/ashishsecdev/Slack-Guardian

Setting up your “Slack Guardian Slack App” - I



1. Click on the name of your **“Slack workspace”**, example: **“ABC”**

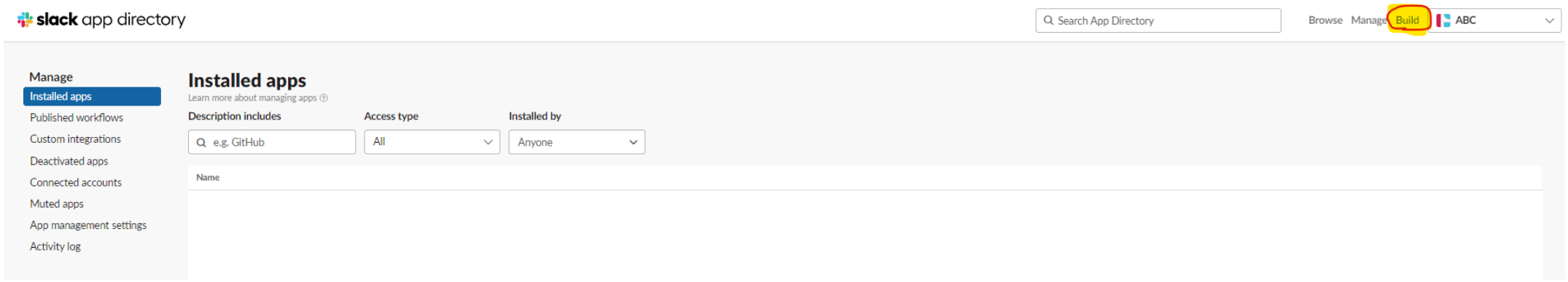
2. Look for **“Settings & administration”**

3. Click on option **“Manage apps”**

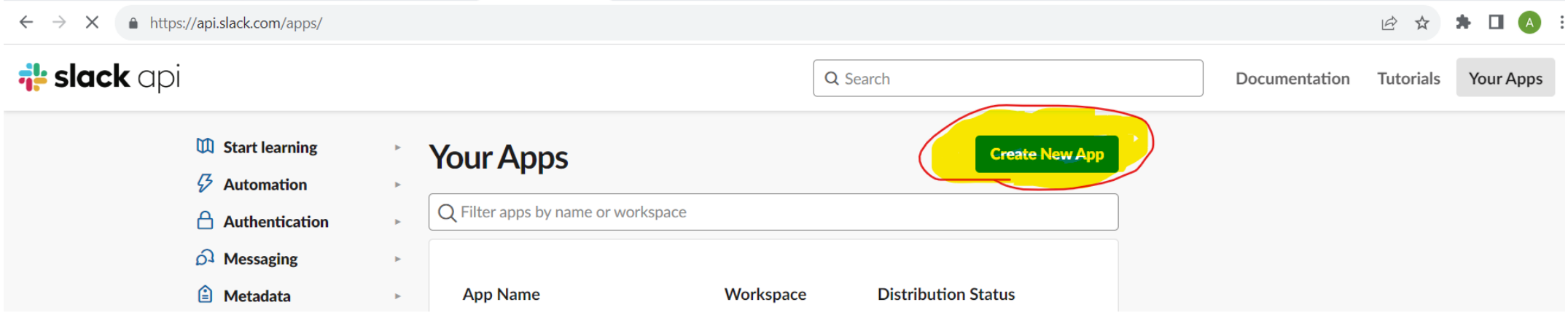
Note: Run Slack Guardian python app with all other required files Slack_Guardian_Detections.csv and violation-audit-report.csv.

Setting up your “Slack Guardian Slack App” - II

- Click on **“Build”**

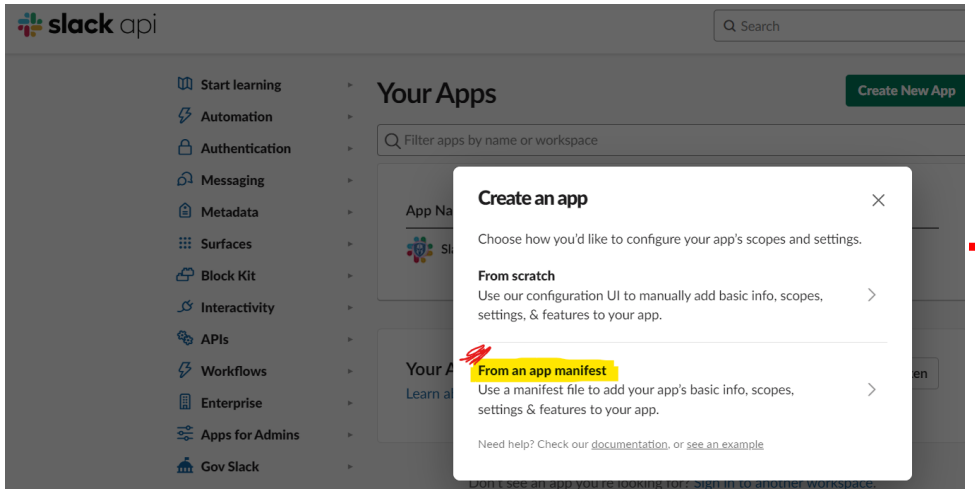


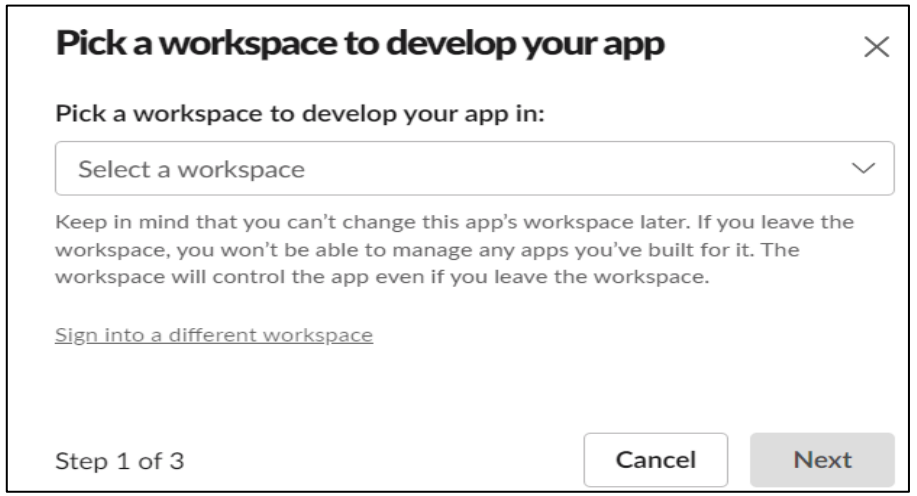
- Click on **“Create New App”**



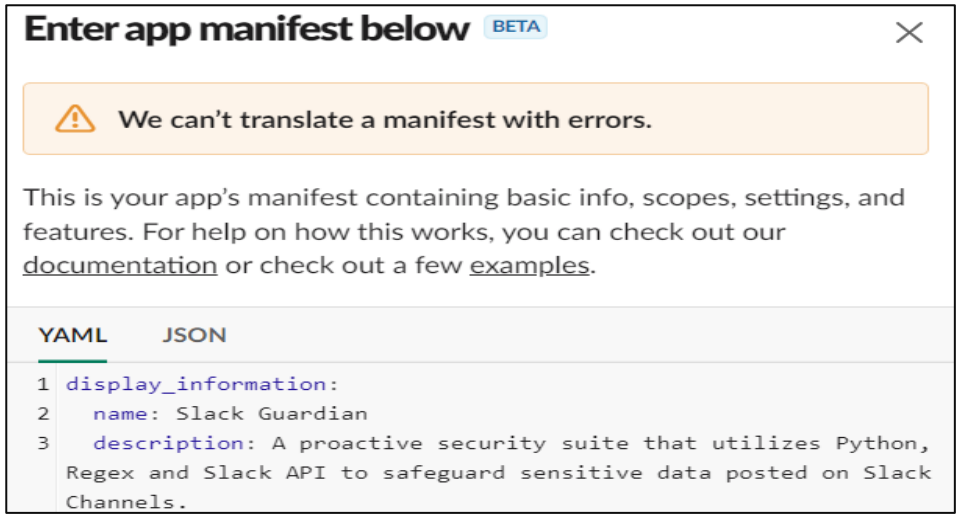
Setting up your “Slack Guardian Slack App” - III

- Click on **“From an app manifest”** and then select your **“workspace”**.

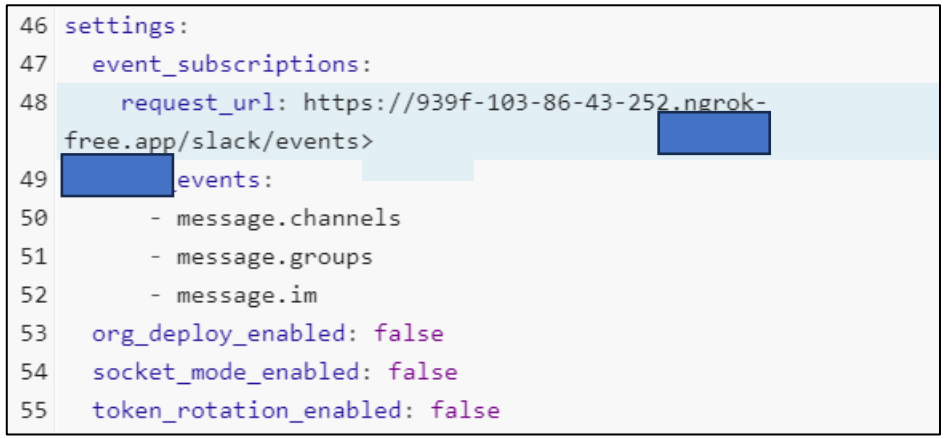




- Enter **“app manifest”** in YAML format by copy pasting from **“manifest.YML”** format and update the 48th line under **“event_subscriptions”** that has *“request_url”* param with your *Slack Guardian Flask* app endpoint.



Update “request_url”

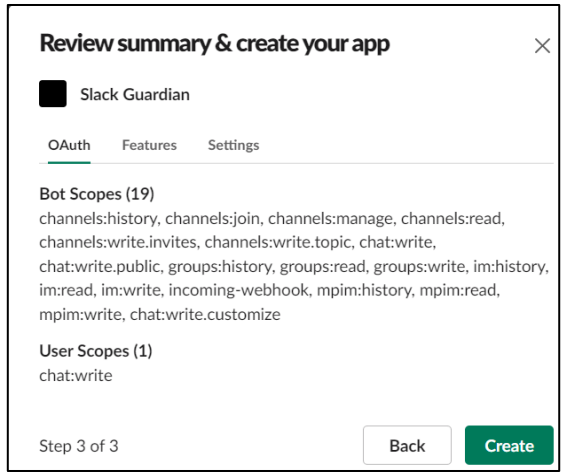


Slack Guardian

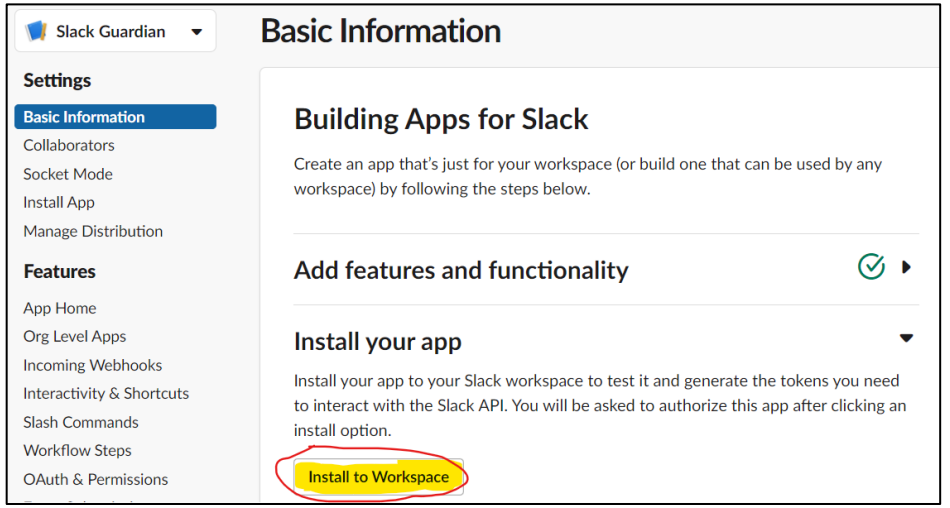
Github: https://github.com/ashishsecdev/Slack-Guardian

Setting up your “Slack Guardian Slack App” - IV

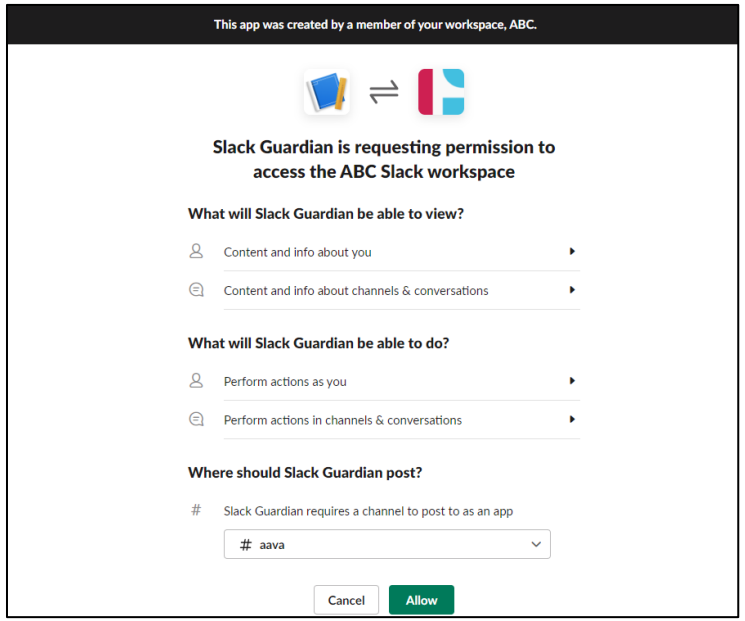
- Review summary of the app and click **“Create”.**



- **Click on “Install to Workspace”**



- **Select the Slack channel name and then click “allow”.**

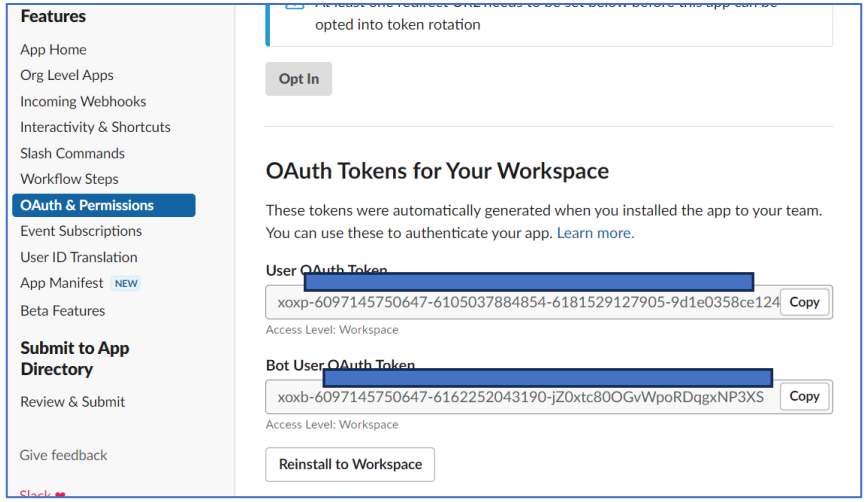


Slack Guardian

Github: https://github.com/ashishsecdev/Slack-Guardian

Setting up your “Slack Guardian Slack App” - V

- Copy “User OAuth Token and update it in your Slack Guardian Python App code.

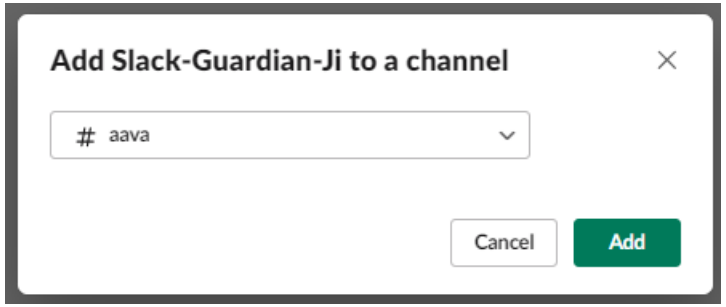


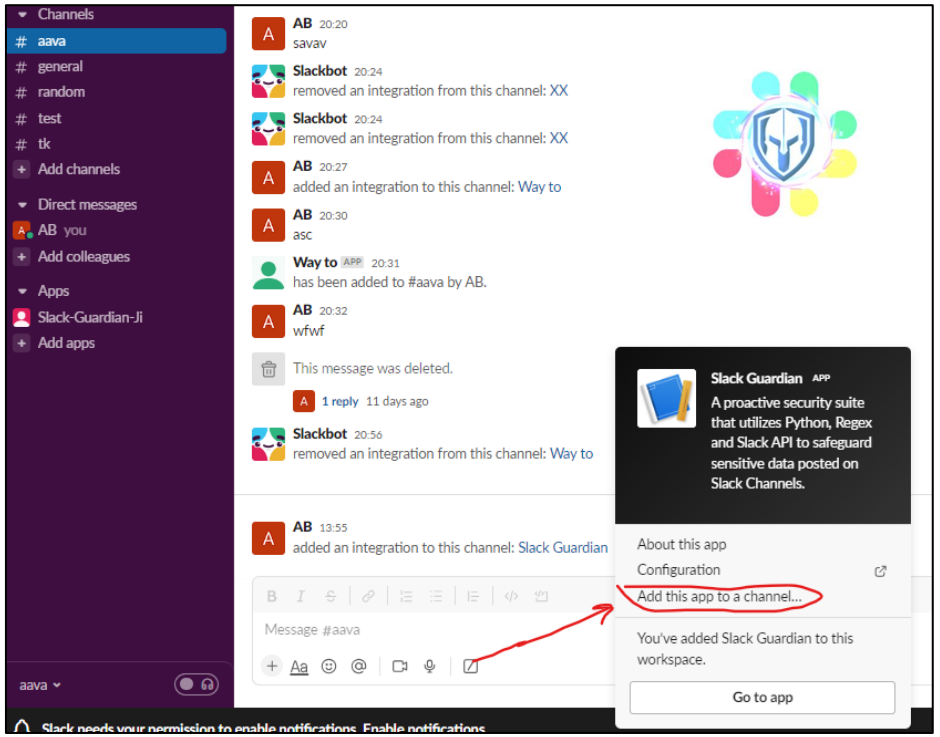
Update Slack Token as per below.

```
app = Flask(__name__)

SLACK_API_TOKEN = "XX"
os.environ['SLACK_API_TOKEN'] = SLACK_API_TOKEN
client = WebClient(token=os.environ['SLACK_API_TOKEN'])
```

- Click on the message with integration add to channel and click **“Add this app to a channel”**





Github: https://github.com/ashishsecdev/Slack-Guardian

Slack Guardian

Test “Slack Guardian Slack App”

- Post message in the Slack group with app and your Flask app terminal should get 200 response code.

```
 * Serving Flask app 'Save_output_Slack'
 * Debug mode: on
INFO:werkzeug:WARNING: This is a development server. Do not use it in a production deplo
 * Running on http://127.0.0.1:5000
INFO:werkzeug:Press CTRL+C to quit
INFO:werkzeug: * Restarting with stat
WARNING:werkzeug: * Debugger is active!
INFO:werkzeug: * Debugger PIN: 138-863-689
INFO:werkzeug:127.0.0.1 - - [09/Nov/2023 14:01:33] "POST /slack/events HTTP/1.1" 200 -
INFO:werkzeug:127.0.0.1 - - [09/Nov/2023 14:27:24] "POST /slack/events HTTP/1.1" 200 -
INFO:werkzeug:127.0.0.1 - - [09/Nov/2023 14:27:28] "POST /slack/events HTTP/1.1" 200 -
INFO:werkzeug:127.0.0.1 - - [09/Nov/2023 14:27:39] "POST /slack/events HTTP/1.1" 200 -
INFO:werkzeug:127.0.0.1 - - [09/Nov/2023 14:27:45] "POST /slack/events HTTP/1.1" 200 -
```

- Post message that matches violation patterns and see the “Slack Guardian Ji” in action.

Github: https://github.com/ashishsecdev/Slack-Guardian

Customizations “Slack Guardian Slack App”

- Enable or disable message deletion.
- Change the user notification option.

|| Violation Detection Patterns ||

Update the Regex patterns as per **Slack_Guardian_Detections.csv**

Slack-Guardian / Python_App / Slack_Guardian_Detections.csv

ashishsecdev Regex pattern to match detections.

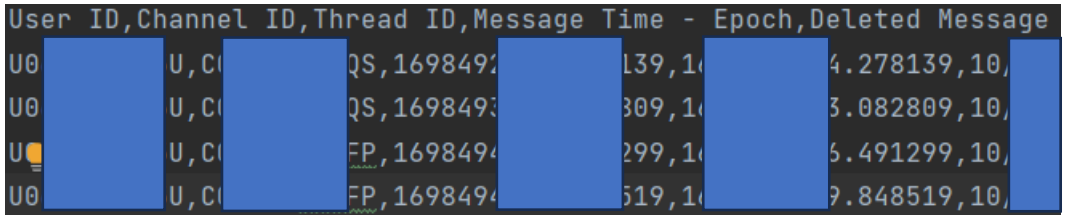
Preview | Code | Blame | 4 lines (4 loc) · 106 Bytes | Code 55% fast

Search this file

	pattern_name	pattern
1		
2	date	\b\d{2}/\d{2}/\d{4}\b
3	credit_card	\b\d{16}\b
4	Mail_Gun	\bkey-[0-9a-zA-Z]{32}\b

|| Violation Records ||

- Update the <**save_to_csv**> function to customise the output records in **violation-audit-report.csv**



Github: https://github.com/ashishsecdev/Slack-Guardian

Thank you!

Contact: ashishsecdev@gmail.com

More articles: https://ashishsecdev.medium.com

Github: https://github.com/ashishsecdev/Slack-Guardian