



# Open Source Slack Security & Threat Hunting

By: Ashish Bansal  
~AshishSecDev

# Introduction

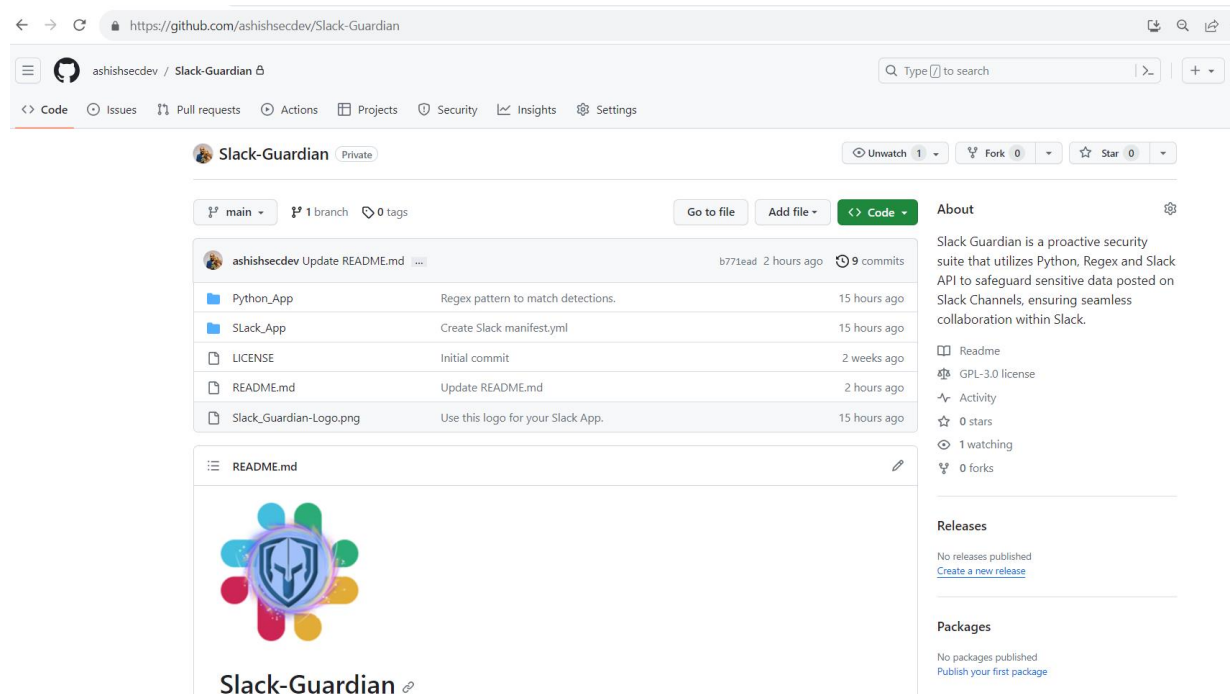
## Slack Guardian Slack Security Suite

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.

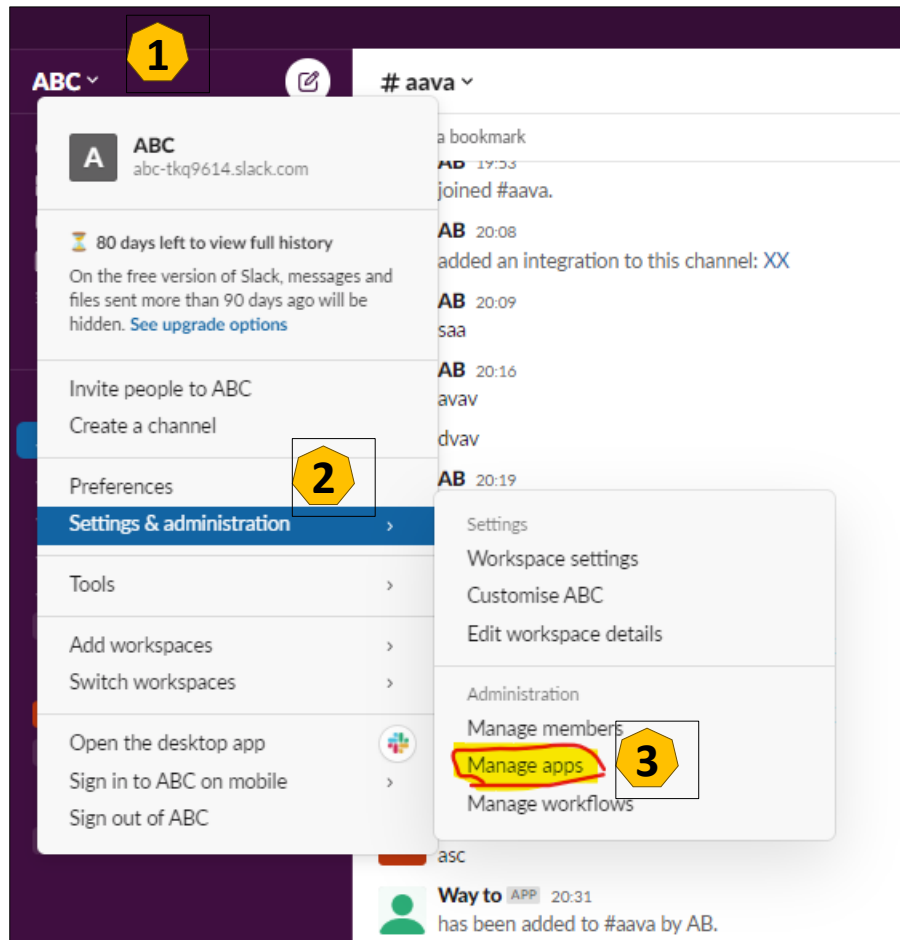
Finally, Slack Guardian automatically removes any identified violations, ensuring your Slack channels remain secure and compliant.

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





# 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”**

slack app directory

Search App Directory

Browse Manage **Build** ABC

Manage

**Installed apps**

Learn more about managing apps

Description includes Access type Installed by

Q e.g. GitHub All Anyone

Name

- Click on **“Create New App”**

https://api.slack.com/apps/

slack api

Search

Documentation Tutorials Your Apps

Start learning

Automation

Authentication

Messaging

Metadata

**Your Apps**

Filter apps by name or workspace

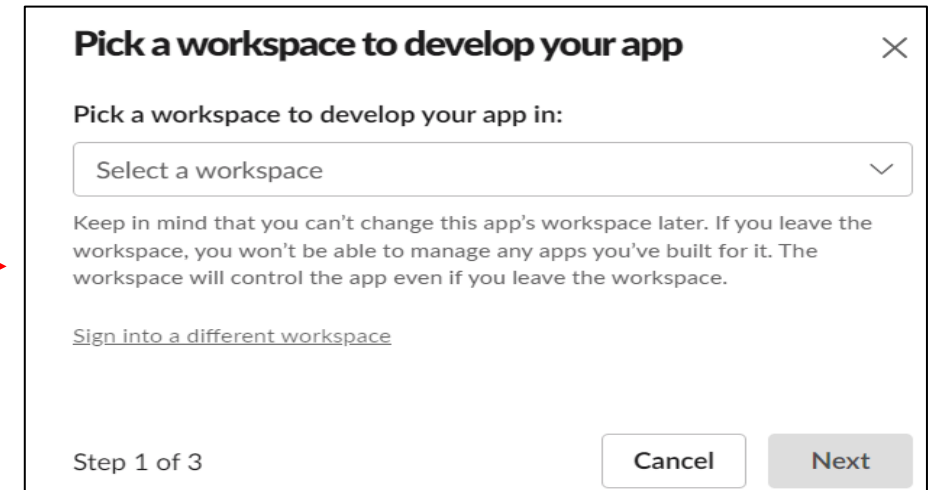
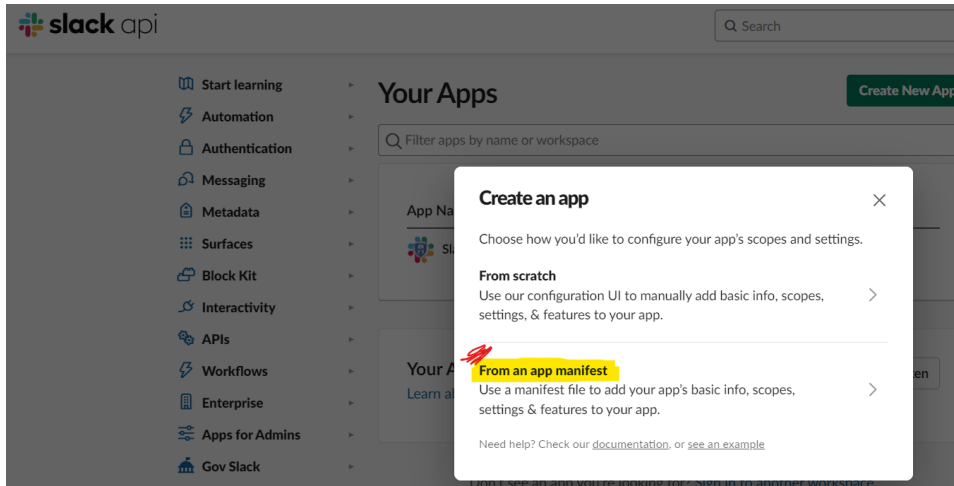
App Name Workspace Distribution Status

**Create New App**

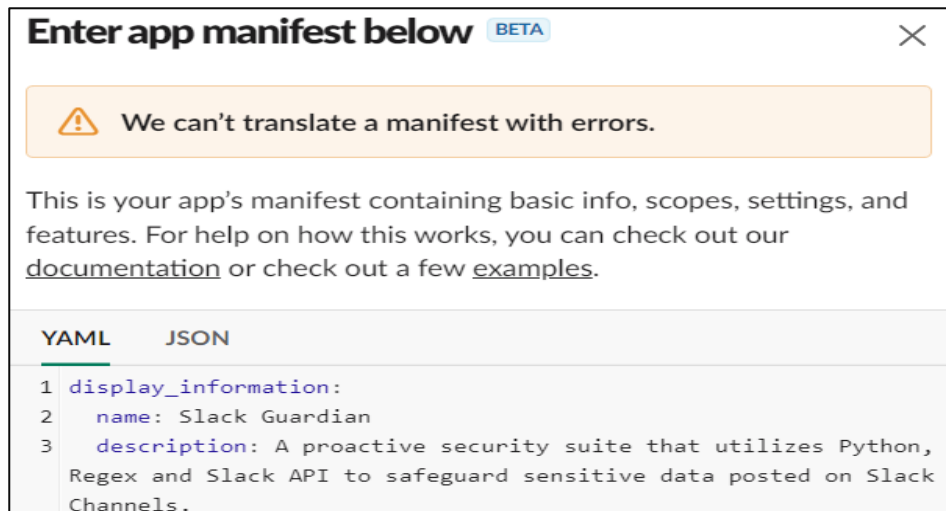


# Setting up your “Slack Guardian Slack App” - III

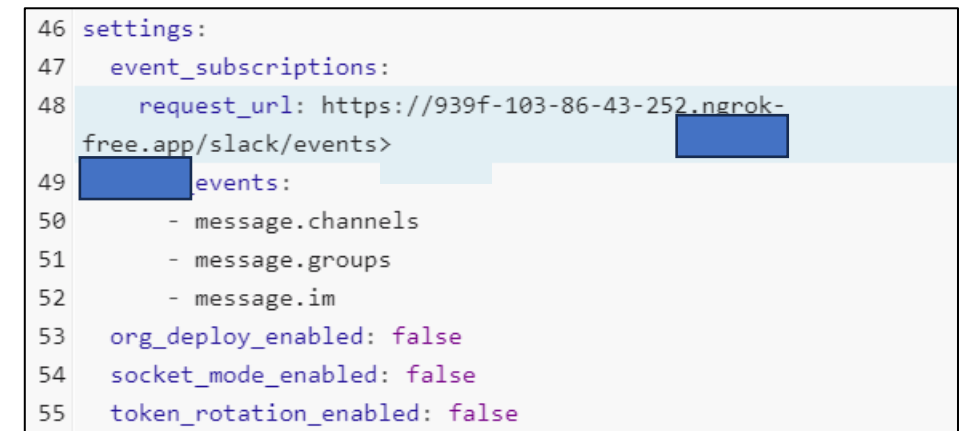
- Click on “**From an app manifest**” and then select your “**workspace**”.



- Enter “**app manifest**” in YAML format by copy pasting from “**manifest.YML**” format and update the 48<sup>th</sup> line under “**event\_subscriptions**” that has “**request\_url**” param with your *Slack Guardian Flask* app endpoint.



Update  
“request\_url”



Slack Guardian



# Setting up your “Slack Guardian Slack App” - IV

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

**Review summary & create your app**

Slack Guardian

OAuth Features Settings

**Bot Scopes (19)**  
channels:history, channels:join, channels:manage, channels:read, channels:write.invites, channels:write.topic, chat:write, chat:write.public, groups:history, groups:read, groups:write, im:history, im:read, im:write, incoming-webhook, mpim:history, mpim:read, mpim:write, chat:write.customize

**User Scopes (1)**  
chat:write

Step 3 of 3

Back Create

- Click on **“Install to Workspace”**

Slack Guardian

**Settings**

- Basic Information
- Collaborators
- Socket Mode
- Install App
- Manage Distribution

**Features**

- App Home
- Org Level Apps
- Incoming Webhooks
- Interactivity & Shortcuts
- Slash Commands
- Workflow Steps
- OAuth & Permissions

**Basic Information**

**Building Apps for Slack**

Create an app that's just for your workspace (or build one that can be used by any workspace) by following the steps below.

**Add features and functionality**

**Install your app**

Install your app to your Slack workspace to test it and generate the tokens you need to interact with the Slack API. You will be asked to authorize this app after clicking an install option.

**Install to Workspace**

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

This app was created by a member of your workspace, ABC.

Slack Guardian is requesting permission to access the ABC Slack workspace

**What will Slack Guardian be able to view?**

- Content and info about you
- Content and info about channels & conversations

**What will Slack Guardian be able to do?**

- Perform actions as you
- Perform actions in channels & conversations

**Where should Slack Guardian post?**

# Slack Guardian requires a channel to post to as an app

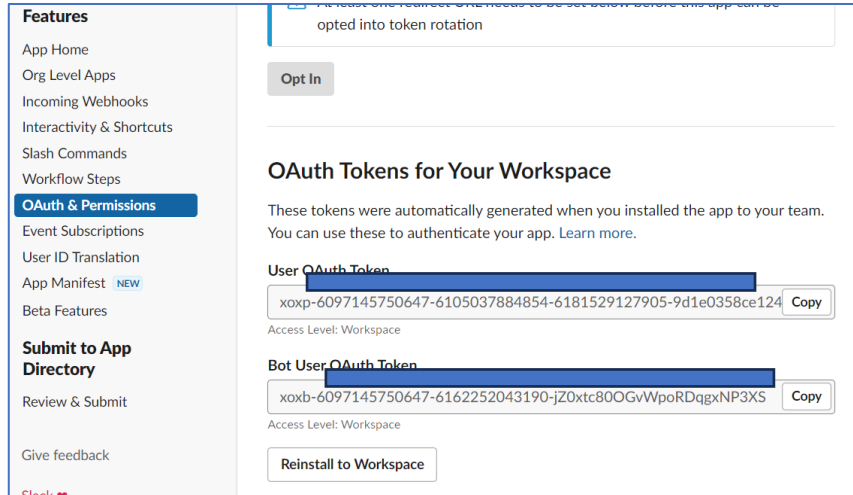
# aava

Cancel Allow



# Setting up your “Slack Guardian Slack App” - V

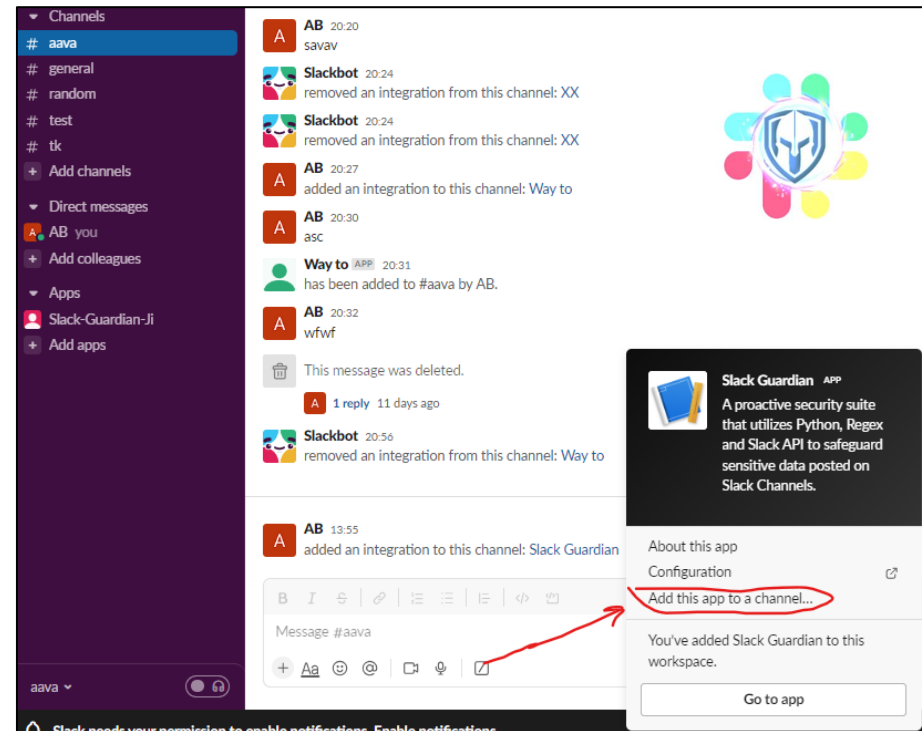
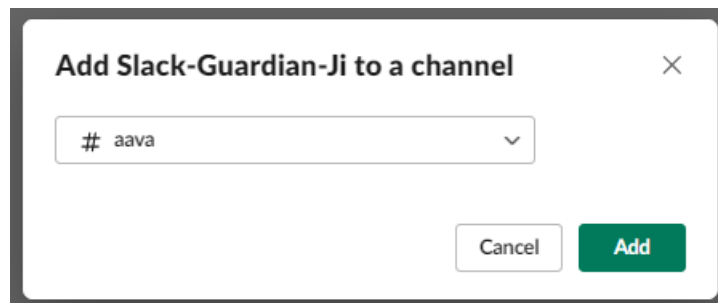
- Copy “User OAuth Token and update it in your Slack Guardian Python App code.



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

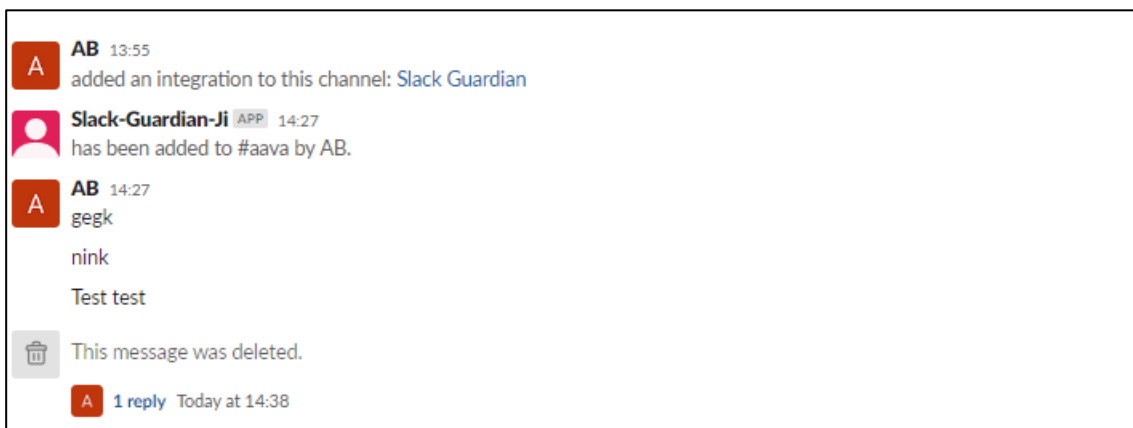


## Test “Slack Guardian Slack App”

- 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 deployment
* 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.







# 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	date	\b\d{2}/\d{2}/\d{4}\b
2	credit_card	\b\d{16}\b
3	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**

```
User ID,Channel ID,Thread ID,Message Time - Epoch,Deleted Message
U0 [REDACTED] U,C [REDACTED] QS,169849 [REDACTED] 139,1 [REDACTED] 4.278139,10, [REDACTED]
U0 [REDACTED] U,C [REDACTED] QS,169849 [REDACTED] 309,1 [REDACTED] 3.082809,10, [REDACTED]
U [REDACTED] U,C [REDACTED] FP,169849 [REDACTED] 299,1 [REDACTED] 5.491299,10, [REDACTED]
U0 [REDACTED] U,C [REDACTED] FP,169849 [REDACTED] 519,1 [REDACTED] 9.848519,10, [REDACTED]
```

# Thank you!

Contact: [ashishsecdev@gmail.com](mailto:ashishsecdev@gmail.com)

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

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