# **Keylogger Project**

--- PAVAN

**Project Purpose :**

The keylogger.py script is a Python-based keylogger that captures user keyboard input and periodically sends the logged keystrokes to a specified email address using Gmail SMTP. This project is intended for educational use and authorized lab environments only.

**Features :**

* Keystroke Logging : Records all keyboard inputs, including special keys.[1]
* Automated Email Reporting : When the keystroke buffer reaches 100 characters, the captured data is emailed to a specified address using secure SMTP.[1]
* Configurable Trigger:\*\* Change buffer size to modify reporting frequency.[1]

**Requirements :**

* Python 3.x installed on the system.[1]
* pynput
* smtplib (standard library)
* email.mime (standard library)

**Script Workflow :**

1.Keystroke Capture

* Uses `pynput.keyboard.Listener` to listen for all keyboard events.
* Processes each keystroke for readability:
* Spaces recorded as `" "`
* Enter as newline (`"\n"`)
* Shift is ignored
* Backspace represented as `"<"`.[1]

2. Buffer and Trigger

* Logged keystrokes are stored in a global variable.
* When the count reaches 100 characters, the buffer is emailed and then reset.[1]

3. Email Sending Routine

* Utilizes Gmail SMTP (`smtp.gmail.com: 587`) for sending.[1]
* Credentials and recipient are hardcoded in the script:
* \*\*Sender address:\*\* `anonymous3.in@gmail.com`
* \*\*Recipient address:\*\* `anonymous3.in@gmail.com`
* \*\*App Password:\*\* `"nglb wazj mhsp dgxq"` (use environment/import for production)[1]
* The email contains the captured keystrokes as plain text in the message body.[1]

4. Continuous Listener

* The script runs indefinitely, capturing and reporting keystrokes in real time until manually **stopped.[1]**

**Usage Instructions :**

1. Configure Gmail Account:

- Enable "App Passwords" within Gmail security settings.

- Replace the provided password with a secure app password for the account.[1]

2. Edit the Script (Optional) :

- Change the sender/recipient emails and buffer size in the appropriate variables.[1]

3. Run the Script:

- Open a terminal and execute:

```bash

keylogger.py

```

- The listener will begin capturing keystrokes and sending emails automatically.[1]

4. Stop the Script:

- Go to cmd administater then see the running process using cmd is tasklist /v

- then kill the process using cmd : : taskkill /IM keylogger.exe /F

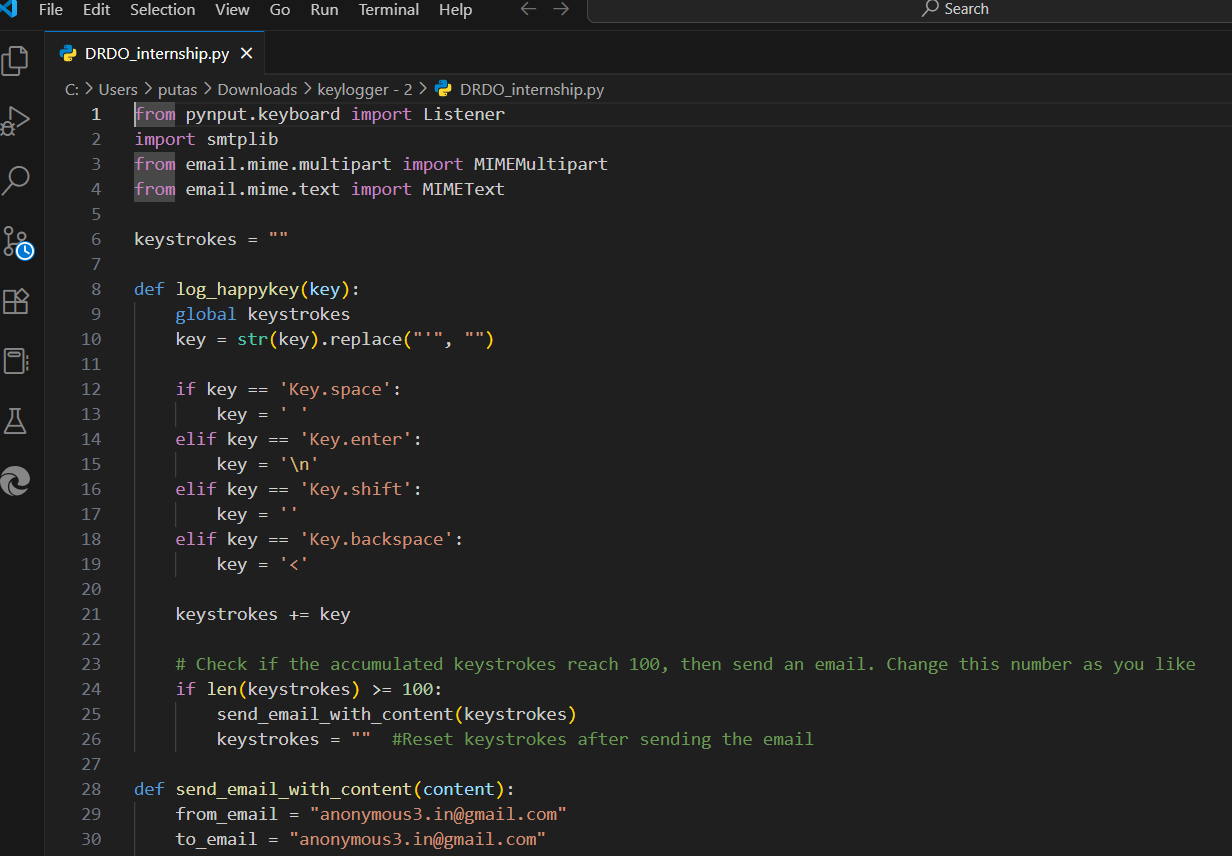
Configuration Guide :

* Email Credentials : Update `from\_email`, `to\_email`, and `password` in the script for your account.[1]
* Buffer Size : Adjust the `if len(keystrokes) >= 100` line for a different reporting frequency.[1]
* Application Security : Avoid hardcoding sensitive passwords. Use environment variables or configuration files where possible.[1]

**Testing the Script :**

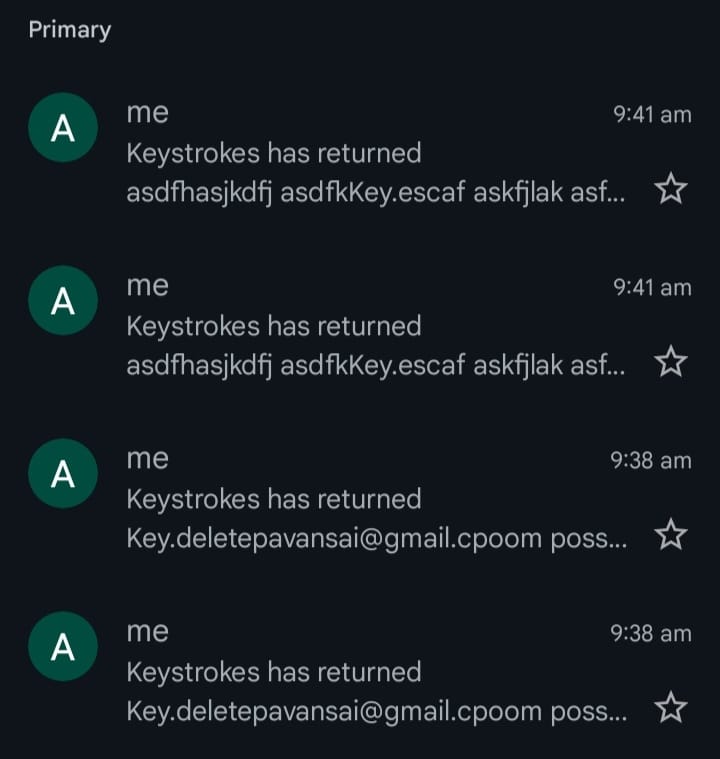
* Run the script and type various keys.
* After every 100 characters, check the specified Gmail inbox for new messages titled `"Keystrokes has returned"`.[1]
* If emails are not received, check for errors regarding authentication, network connectivity, or incorrect credentials.[1]

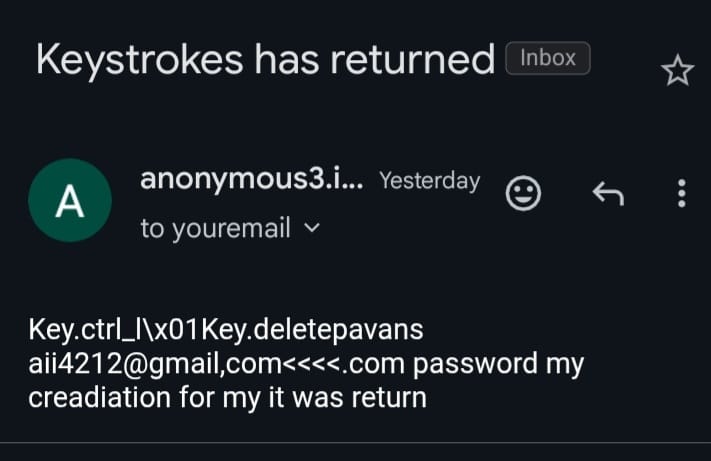
**Source script code :**

****

* **Then execute code it will send the keystocks**
* **To your registrated gmail utpo 100 characters**
* **So stop this using this cmd** taskkill /IM keylogger.exe /F

**Output ::**

****

****

**Ethical and Legal Notice :**

\*\*Warning:\*\*

This software is for legitimate educational, testing, or research use \*\*only\*\*. Unauthorized deployment or use on systems without owner consent is strictly illegal and unethical. Operate strictly within controlled lab environments and adhere to all local laws and institutional guidelines.[1]

1. **Parental Monitoring**
   * Parents may use keyloggers to track their children’s computer usage and protect them from harmful online activities.
2. **Employee Monitoring**
   * Some organizations use keyloggers (with consent or policies in place) to monitor workstations for productivity, insider threats, or policy violations.

**3. Forensic Investigations**

* + In cybersecurity and digital forensics, keyloggers may be used in controlled environments to gather evidence or study attacker behavior.