leaked secret investigation: Intruder

Background:
This is a classic OSINT challenge (credentials/secret leak). Our organizing team successfully executed a simulated phishing exercise against XYZ Corp. Unfortunately, one teammate carelessly posted the malicious email and the hidden secret on a public social site. Your mission is to trace that leak and extract the secret code.

Investigation summary (steps taken):

1. Identify the organizing team.
   After analyzing the competition materials, we determined the two main organizers are Syed Misbah Uddin and Ritik.

2. Search social profiles.
   Begin by searching for any social accounts linked to those names — LinkedIn, GitHub, Instagram, and other public platforms.

3. Check challenge metadata.
   The CTF/CTFd challenge description referenced the organizers' GitHub and LinkedIn accounts. Use those references to narrow the search.

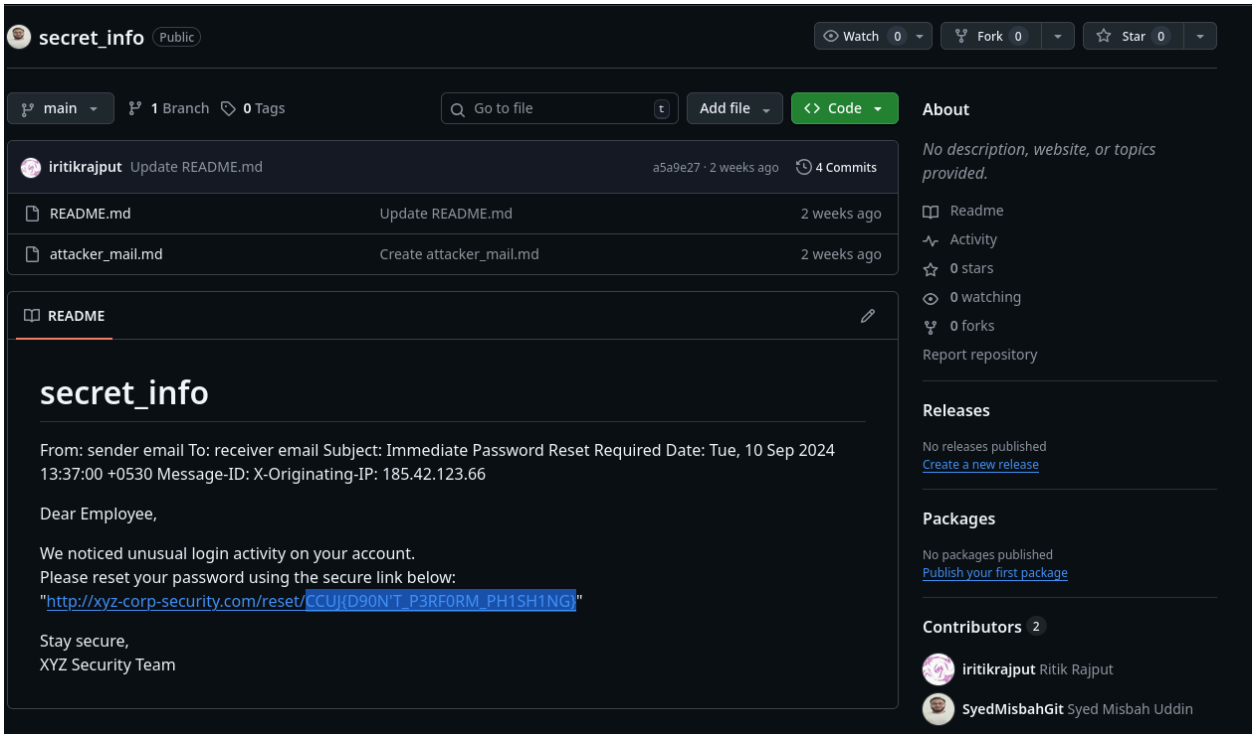
4. Review LinkedIn.
   We searched LinkedIn thoroughly; no direct evidence or leaked materials were found there.

5. Inspect GitHub activity.
   Next, we examined GitHub for recent activity — repositories, commits, forks, and collaborations.

6. Find suspicious repository.
   A collaborative repository named secret_info created one day ago by the organizing team was discovered. This repo was marked by recent commits and contributor activity.

7. Examine commits and files.
   We opened the repository, reviewed commits and file changes, and searched for accidentally committed secrets, emails, or other sensitive information.

8. Locate the leak.
   Deep analysis of commit history revealed the leaked malicious email and the secret code posted in a commit or file authored by the team.



Flag: CCUJ{D90N'T_P3RF0RM_PH1SH1NG}