Secret Breach Detection in Issue Reports

Suppose there is an individual, Mr. X, who uses GitHub. One day, he posts an issue report stating: ***"I am having trouble with my database connection. Here is the connection string I am using: postgres://username:password @localhost:5432/mydatabase."*** This is an example of a secret breach in an issue report. Despite the availability of tools to detect such breaches in source code, detecting secret breaches (sensitive information like API keys and passwords) in software issue reports on code-sharing platforms like GitHub remains largely unexplored. To address this issue, we have created this survey to understand the severity and likelihood of secret breach in issue reports.

Thank you very much for your participation.

* Indicates required question

1. Email *

2. Please provide your Github username *

3. How likely you are to encounter secret breach in issue reports of Github? *

Mark only one oval.

	1	2	3	4	5
	○	○	○	○	○

4. What do you think of the severity of secret sharing in issue reports?

5. What scenarios could influence your sharing of secret in issue reports?