Initial Ethics Review Form

Application # ______

Project Title:

A Large-Scale Empirical Study of Secret Leakage in Hugging Face Spaces

Project Description

Hugging Face Spaces has become a leading platform for hosting AI applications, offering developers seamless integration of Git-based repositories and out-of-the-box web service deployment. However, as its adoption continues to expand, security issues have gradually surfaced. Recent reports have pointed to the accidental exposure of sensitive information, such as API tokens and database credentials, within Spaces-hosted code. Despite these security risks, there is still a lack of comprehensive understanding of the scope and impact of these security threats in the research community. To fill this gap, we conducted the first large-scale, systematic empirical study, using Large Language Models (LLMs) to identify and analyze secret leakage in Hugging Face Spaces and quantify the extent of secret leakage in Spaces.

Project Aims

This project plans to conduct two key-related studies: (1) Space repository data collection: We will collect and analyze the source code and .git commit history of all publicly available Hugging Face Space repositories to assess the performance of our LLM-based method in key identification. (2) Usability testing: By testing various keys through official API interfaces provided by different platforms, we will verify whether the keys are still active and analyze their corresponding permissions to assess the potential risks associated with key leakage.

Research Methods

(1) We use the HFAPI provided by Hugging Face to extract repository names based on the creation date of the repositories. Then, we use an automated script combined with git clone to download the source code from all repositories to the local machine. Afterward, we use a Large Language Model (LLM) to process the collected code and git commit history, identifying and classifying the keys.

(2) To further assess the risks associated with leaked secrets, we conducted a systematic risk evaluation of the detected keys. First, the keys we verified were strictly limited to those already exposed within public code repository files. Second, following established practices in secret scanning and methodologies adopted by tools such as TruffleHog [1-2], we investigated official API interfaces provided by platforms like Hugging Face and GitHub, which are specifically designed to verify key validity and access scopes. To mitigate any potential ethical concerns, we implemented strict data protection

measures during the verification process: no sensitive information returned by the API was recorded, and no actual operations were performed on external systems or services. Furthermore, we adhered to the principle of least privilege, ensuring that only essential validation steps were carried out. This guarantees that the verification process imposes no interference or potential risk to the owners of the keys.

Ref

[1] https://docs.github.com/en/code-security/secret-scanning/enabling-secret-scanning-features/enabling-validity-checks-for-your-repository
[2] https://trufflesecurity.com/blog/research-finds-12-000-live-api-keys-and-passwords-in-deepseek-s-training-data?utm_source=chatgpt.com

Data Management

All data collected during the study will not include any private information related to repository owners or the leaked keys. The data will be securely stored and analyzed locally by the research team only. No data will be shared with third parties.

Funding and External Contractors

N.A.

Project Location(s): [redacted]

Proposed Start Date: 1 DEC 2024

Proposed Finish Date: 15 Mar 2025

Ethical Considerations

Please check the relevant box to answer **Yes** or **No** to each of the following questions. If answering **Yes** to any questions, please ensure further details are provided in the project description above.

1. **Has this project been reviewed and conditionally approved or rejected by another ethics committee?**

   □ Yes ☒ No

2. **Is the project being externally funded or provided with in-kind support by an external party?**

   □ Yes ☒ No

3. **Is the project designed to provide market research or a consultancy service fully paid for by a client?**

   □ Yes ☒ No

4. **Will there be any restrictions (or restrictive procedures) placed on the publication of results from this project as a result of the funding or support arrangements?**

   □ Yes ☒ No

5. **Will any part of the project be undertaken by or outsourced to a third party?**

   □ Yes ☒ No

6. **Are there any potential conflicts of interest for the research team or organisation(s) associated with the project?**
   (e.g., arising from any involvement or role that researchers may have with other projects or external organisations, or an existing relationship between a member of the research team and the potential participants)

   □ Yes ☒ No

8. **Are there any risks (e.g., social, psychological, financial, physical, legal) to participants, the research team or others arising from their involvement in the research which cannot be mitigated / negated through project design?**

   □ Yes ☒ No

9. **Is it likely that the project will involve the disclosure of unlawful conduct, or concealment of a crime, by individuals or definable groups?**

   □ Yes ☒ No

10. **Will this research project involve access to, use, collection or acquisition of culturally sensitive materials or artefacts?**

    □ Yes ☒ No

11. **Will the information to be collected about participants during the project come from any of the following sources?**

    □ Yes ☒ No

If Yes, please specify:

- ☐ Another person about the research participant
- ☐ An agency, authority, or organisation other than [redacted]
- ☐ A data source collected previously by [redacted] for a purpose other than this research project

12. **Will the project involve the collection, handling and/or storage of personal information?**

    ☐ Yes ☒ No

Additional Notes

- If any questions are answered **Yes**, please provide detailed explanations in the **Project Description** section or as an attachment.
- Ensure that all ethical considerations are addressed in the research design and methodology.

Certification

Principal Researcher / Project Leader

Name: [redacted]
Position: [redacted]
Business Unit: [redacted]
Research Group: [redacted]
Location: [redacted]
Phone: [redacted]
Email: [redacted]

Certification:

As Principal Researcher / Project Leader for this research project, I certify that:

- The information provided in this application is correct to the best of my knowledge.
- I wil notify the ethlcs committee of any ethically relevant varlations to the project.
- I will immediately report any adverse events or harm to particlpants.
- Data will be managed and stored in accordance [redacted]'s policies and relevant legislation.

[redacted]

Signed: [redacted]

Name:

Date: 2025.3.15

To comply with the double-blind review policy, we have masked the stamped sections. If required by the reviewers, we are prepared to provide an unmasked version for verification.