

Generative AI and Open-Source Intelligence: Exploring Capabilities and Privacy Implications

Akif Ozer, Vinicius Lima and Umit Karabiyik

OVERVIEW

GOALS

This research aims at looking into how Generative Artificial (GenAI) Intelligence tools can be leverage to provide open-source intelligence (OSINT) capabilities. We tested the main GenAI applications to check what level of information can be gathered with them. We also tested ways to circumvent their privacy barriers.

The main goals of our project included:

1. Examining the generative AI tools and their Open Source Intelligence capabilities.
2. Testing generative AI tool's privacy restrictions and potential ways to circumvent them.

METHODOLOGY

FINDINGS

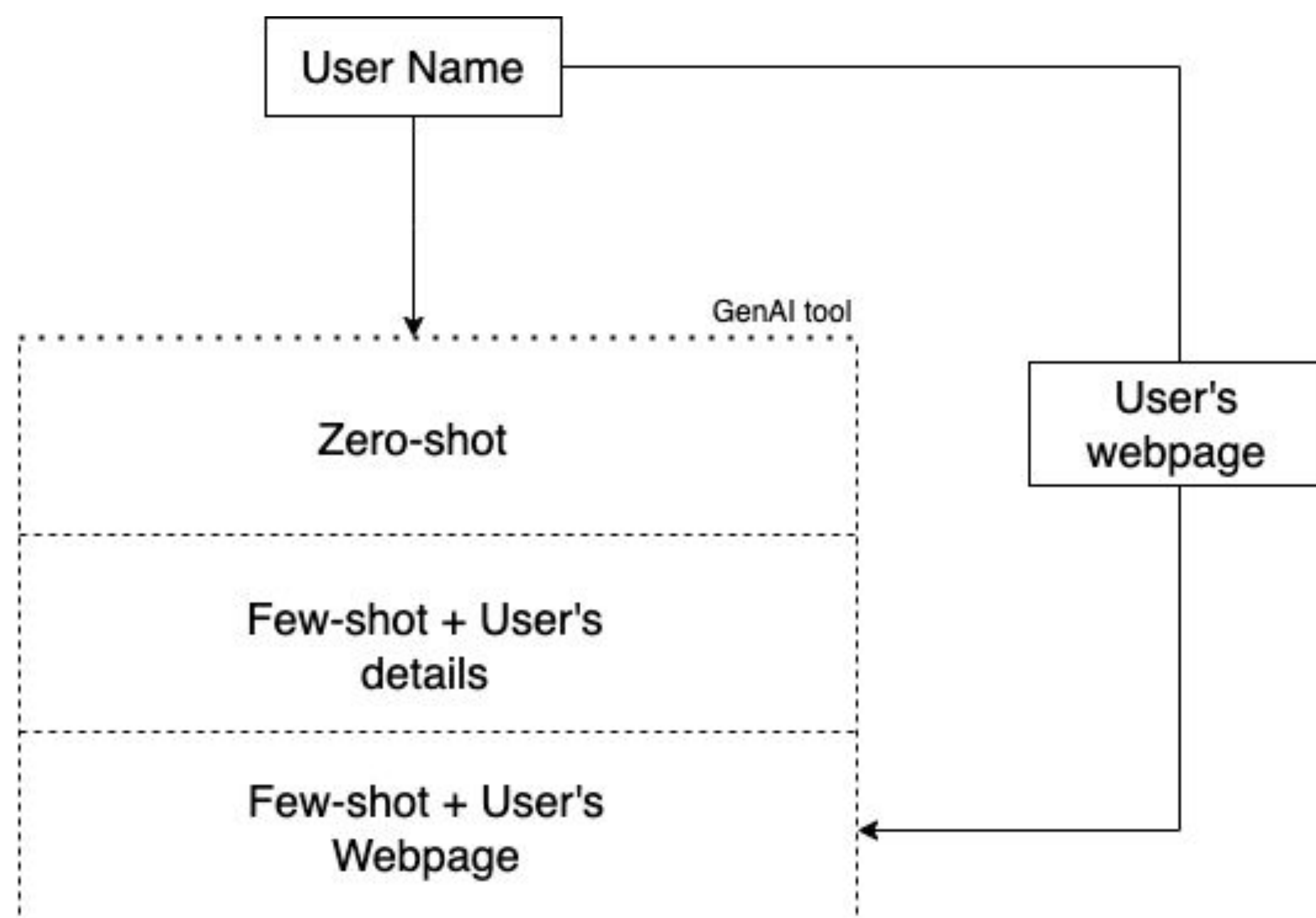
Our method consisted of analysing four major GenAI tools: ChatGPT, Copilot, Gemini, and You.com . We conducted tests on both public and private webpage user information. Our objective was to ascertain the extent to which information could be accessed using each of the tools. The following are the levels we considered:

- Generative AI tools have privacy restrictions that prevents them from accessing social media platforms (see figure below). We were able to access public information with few-shot prompting, although not from social media.

- **Zero-shot prompting:** Information on a user profile with a single prompt.
- **Few-shot prompting:** Information on a user could not be provided from the first prompt, thus new prompts were necessary with user's details.
- **Prompting with the full webpage information :** Prompt question followed by a copy of the user's web page information.

ChatGPT
I can't directly access or interact with LinkedIn profiles or content from many other specific web services due to privacy restrictions and the technical limitations of my current environment. These restrictions are in place to protect user privacy and comply with data protection regulations. Additionally, platforms like LinkedIn have their own access controls and terms of service that limit automated systems from retrieving personal data without explicit permission. Therefore, I can provide guidance and answer questions based on publicly available information or help you find resources, but I can't directly access or interpret personal profiles on LinkedIn or similar sites.

- Our research showed that some AI tools can generate inaccurate information about a person.
- These tools are more capable of accessing resources like news and online articles rather than user related personal information directly.



Generative AI	Privacy Restriction	When data shared	Accuracy
ChatGPT 4	Yes	Yes	Yes
Gemini Advanced	No	Yes	No
Co-pilot Pro	Yes	Yes	Yes
You.com	Yes	Yes	No

- All tools evaluated utilize generative AI technologies to produce content based on inputs received.

CONCLUSION

Our level analysis has proven to be an effective method for assessing the model's access to both public and private data, while also evaluating the robustness of its privacy and security restriction mechanisms. The initial prompt was formulated as follows: "Can you find me information about..[user name]...?" utilizing all generative AI tools that are being tested. Based on the answers we would provide user details to test their capabilities.

- This research can be a great resource for future tool development to scrape data from social media and create an OSINT report using generative AI.
- Privacy restrictions creates a secure layer for AI tools to access personal information.

