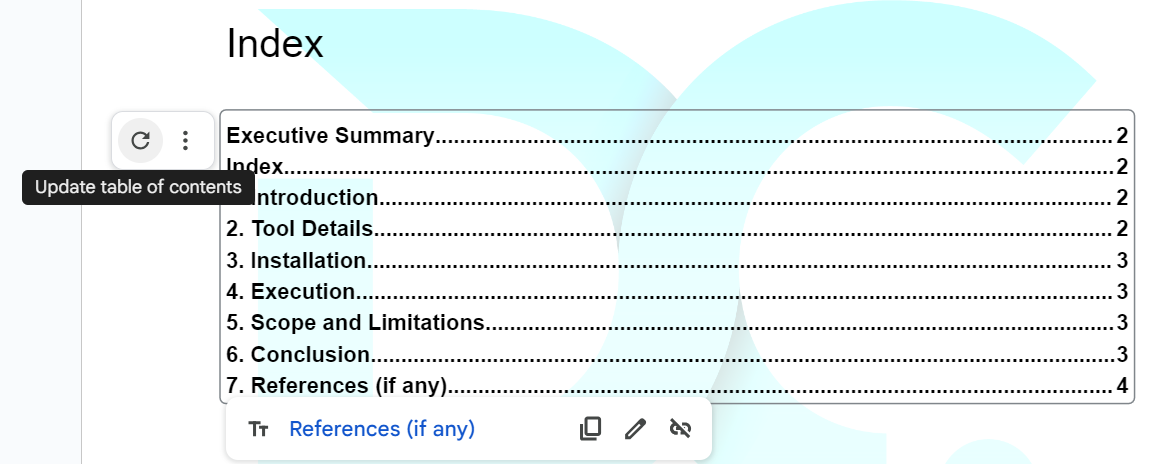
# DEEPCYTES REPORT FORMAT

**General rules: (to be followed on the backend)**

* Name the folder as ‘Report/ToolName\_Vertical\_YYYYMM\_YourName’
* Folder should contain 3 files:
  + Documentation for the work done.
    - The documentation to be named as ‘Doc\_ToolName\_Vertical\_YYYYMM\_YourName’
  + .txt file of script for installation
    - The script file to be named as ‘Script\_ToolName\_Vertical\_YYYYMM\_YourName’
    - Should include a readme/comments section at the top of the script. (FORMAT TBD)
    - To update the index, click the ‘Update table of contents’ button. 
    - Format: Section Headers: Heading 1, Subheaders: Heading 2
  + Demo Video
    - The demo video to be named as ‘Demo\_ToolName\_Vertical\_YYYYMM\_YourName’
    - Video format: .mp4
    - Video should include all the use cases as stated in the use cases section in the document.
    - A VO explaining the working must be included.
* Access for this folder should be shared with your Team Manager, [info@deepcytes.io](mailto:info@deepcytes.io) , and any other IDs if mentioned.
* To start editing this document, make a copy and start Page 2 onwards.

**Gitrob**

**Cyber Intel | Gitrob | 24th September 2023**

# Executive Summary

Gitrob is an open-source tool designed to help security professionals and penetration testers identify sensitive files that may have been inadvertently exposed in public GitHub repositories

# Index

[DEEPCYTES REPORT FORMAT 1](#_Toc146474771)

[Executive Summary 2](#_Toc146474772)

[Index 2](#_Toc146474773)

[1. Introduction 2](#_Toc146474774)

[2. Tool Details 3](#_Toc146474775)

[3. Installation 3](#_Toc146474776)

[4. Execution 4](#_Toc146474777)

[5. Scope and Limitations 6](#_Toc146474778)

[6. Conclusion 6](#_Toc146474779)

[7. References 6](#_Toc146474780)

# Introduction

Gitrob is a tool to help find potentially sensitive files pushed to public repositories on Github. Gitrob will clone repositories belonging to a user or organization down to a configurable depth and iterate through the commit history and flag files that match signatures for potentially sensitive files. The findings will be presented through a web interface for easy browsing and analysis.

**Key Features:**

1. **Repository Scanning**: Gitrob scans public GitHub repositories for potentially sensitive information. It does this by analyzing the contents of repositories and identifying patterns that match common filenames or file contents associated with sensitive data.
2. **Token Detection**: Gitrob can identify tokens and credentials that developers may have mistakenly included in their code, such as API keys, passwords, and authentication tokens.
3. **File Content Analysis**: The tool can also search for specific patterns or regular expressions within file contents. This is useful for identifying code comments or configuration files that contain sensitive information.
4. **Collaborator Analysis**: Gitrob can analyze the list of collaborators and contributors to a repository to identify individuals who may have access to sensitive data.
5. **Organization and User Profiles**: Gitrob provides a way to profile organizations and individual users on GitHub. This can help security professionals build a better understanding of an organization's exposure to risk.

# Tool Details

Link to git repo: <https://github.com/michenriksen/gitrob>

Dependencies: NA

Use Cases List:

* Security Assessment
* Risk Assessment
* Compliance Audits

Version worked on in the report: 2.0.0

Date of installation and run: 24th September

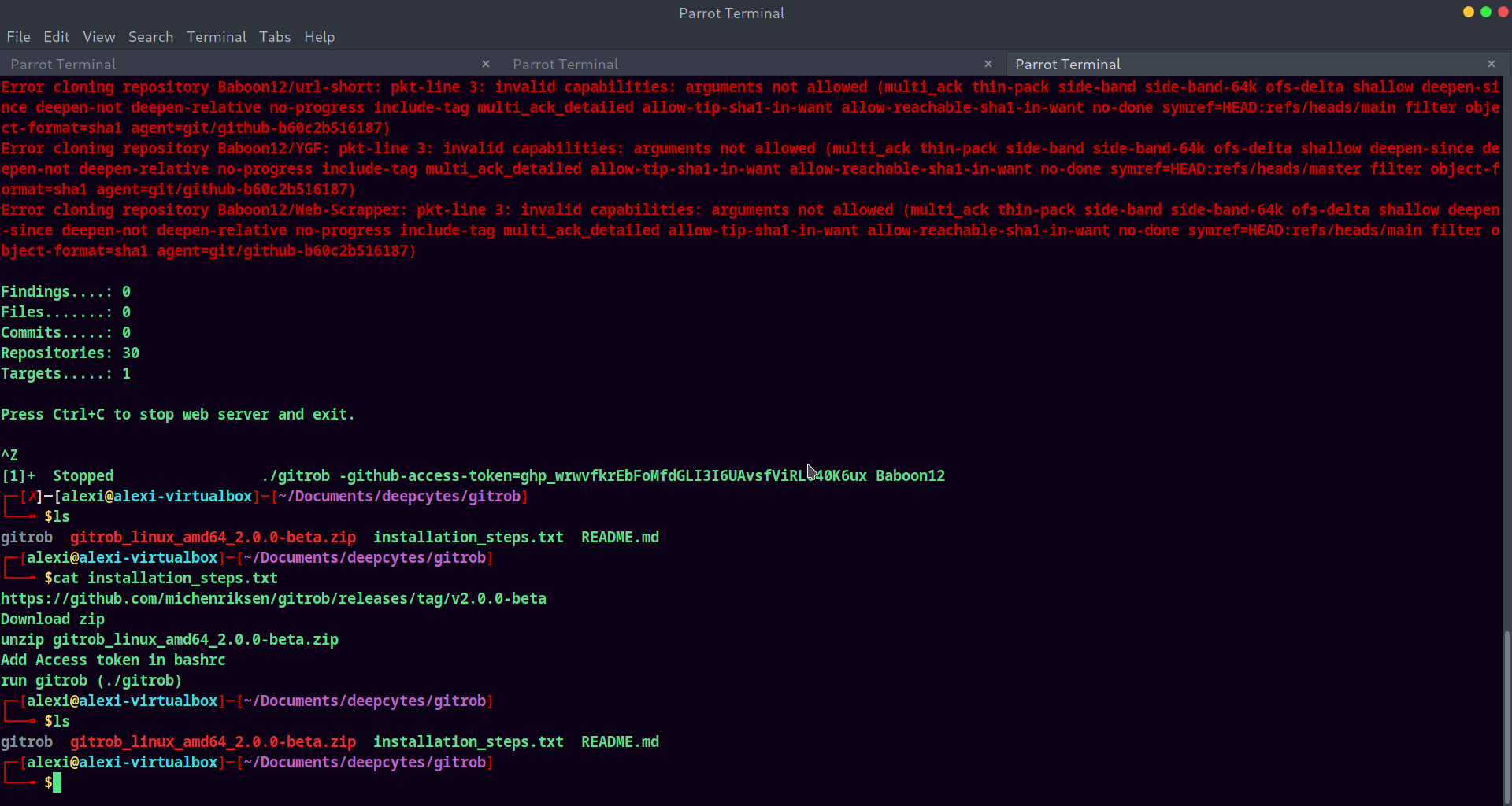
OS used: Kali Linux/Parrot OS

GUI/CLI/Web: CLI

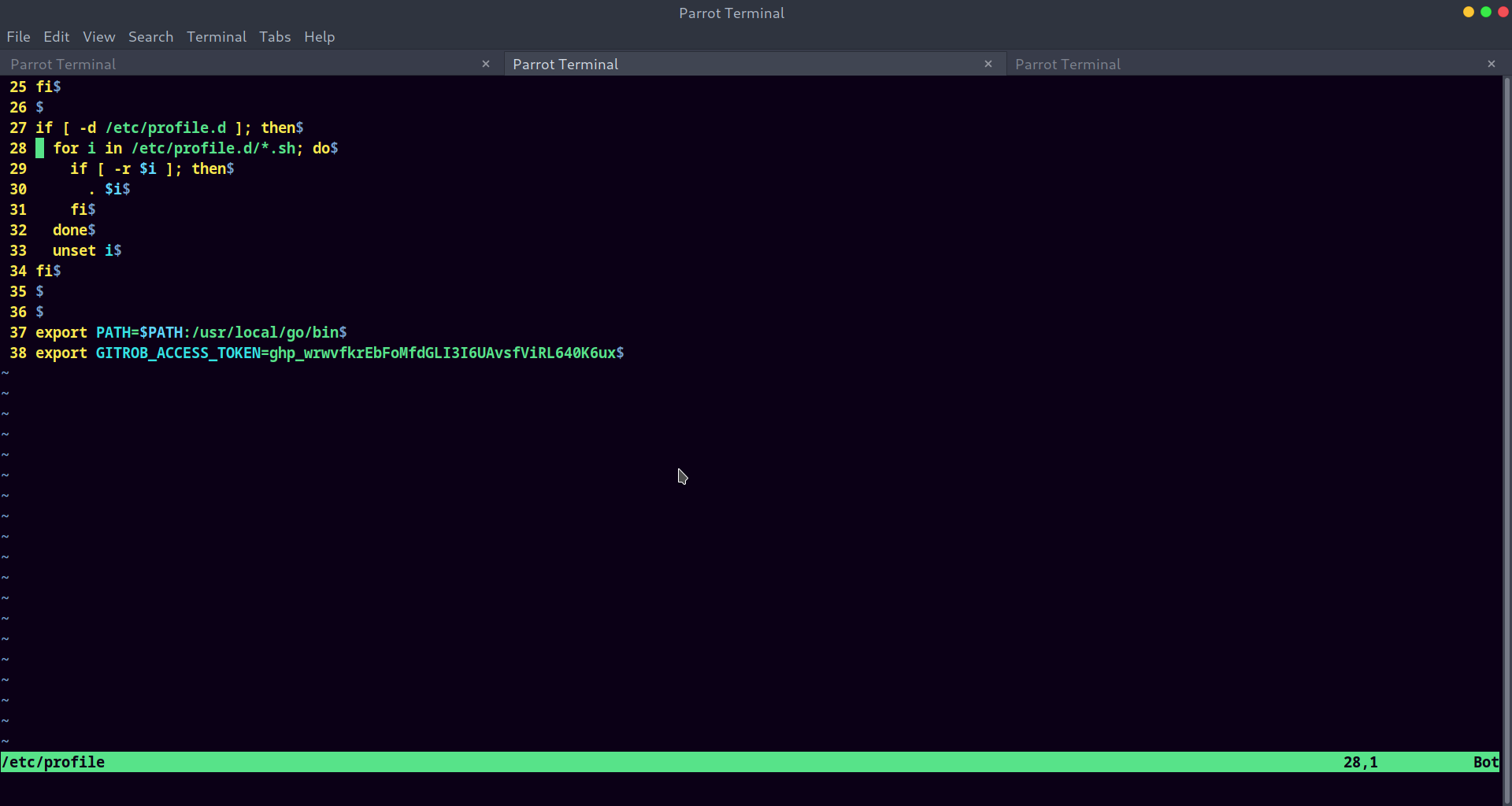
# Installation

**Step 1.** Download the zip file from <https://github.com/michenriksen/gitrob/releases/tag/v2.0.0-beta>

**Step 2.** Unzip the zip file unzip gitrob\_linux\_amd64\_2.0.0-beta.zip



**Step 3.** Add the github access token in /etc/profile file



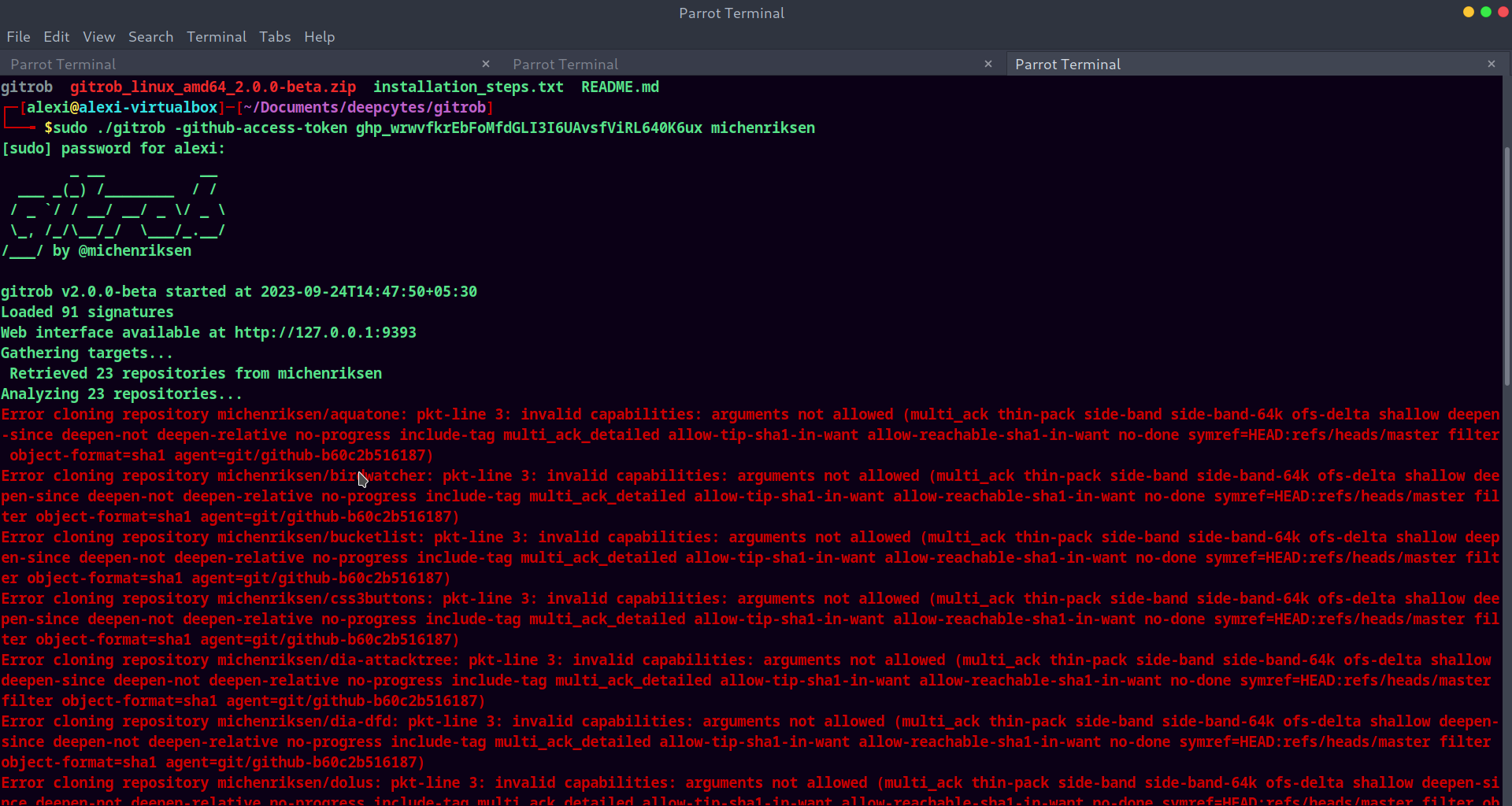
# Execution

To run the tool

./gitrob username

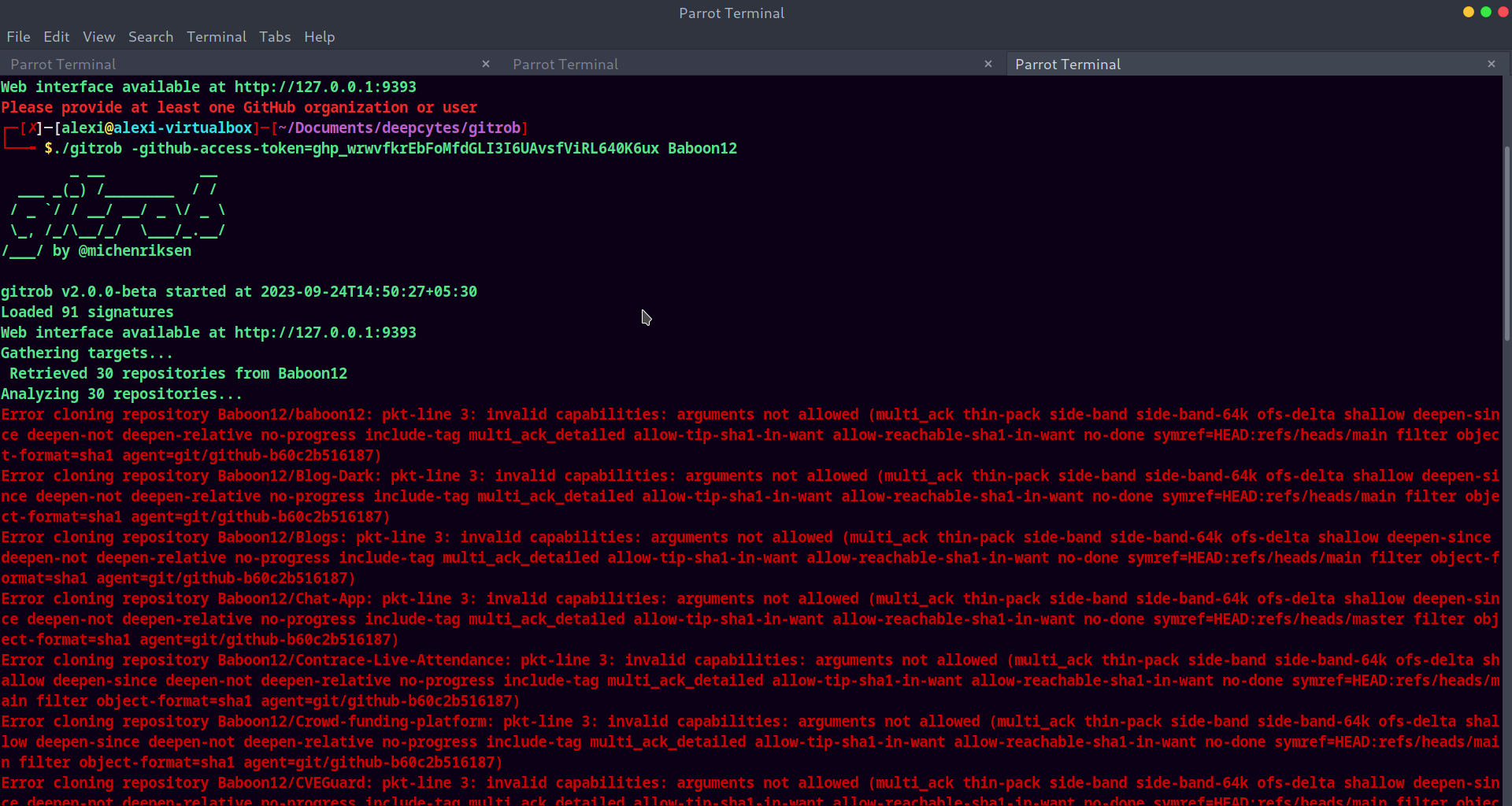
**Use Case 1.**

./gitrob -github-access-token=ACCESS\_TOKEN michenriksen



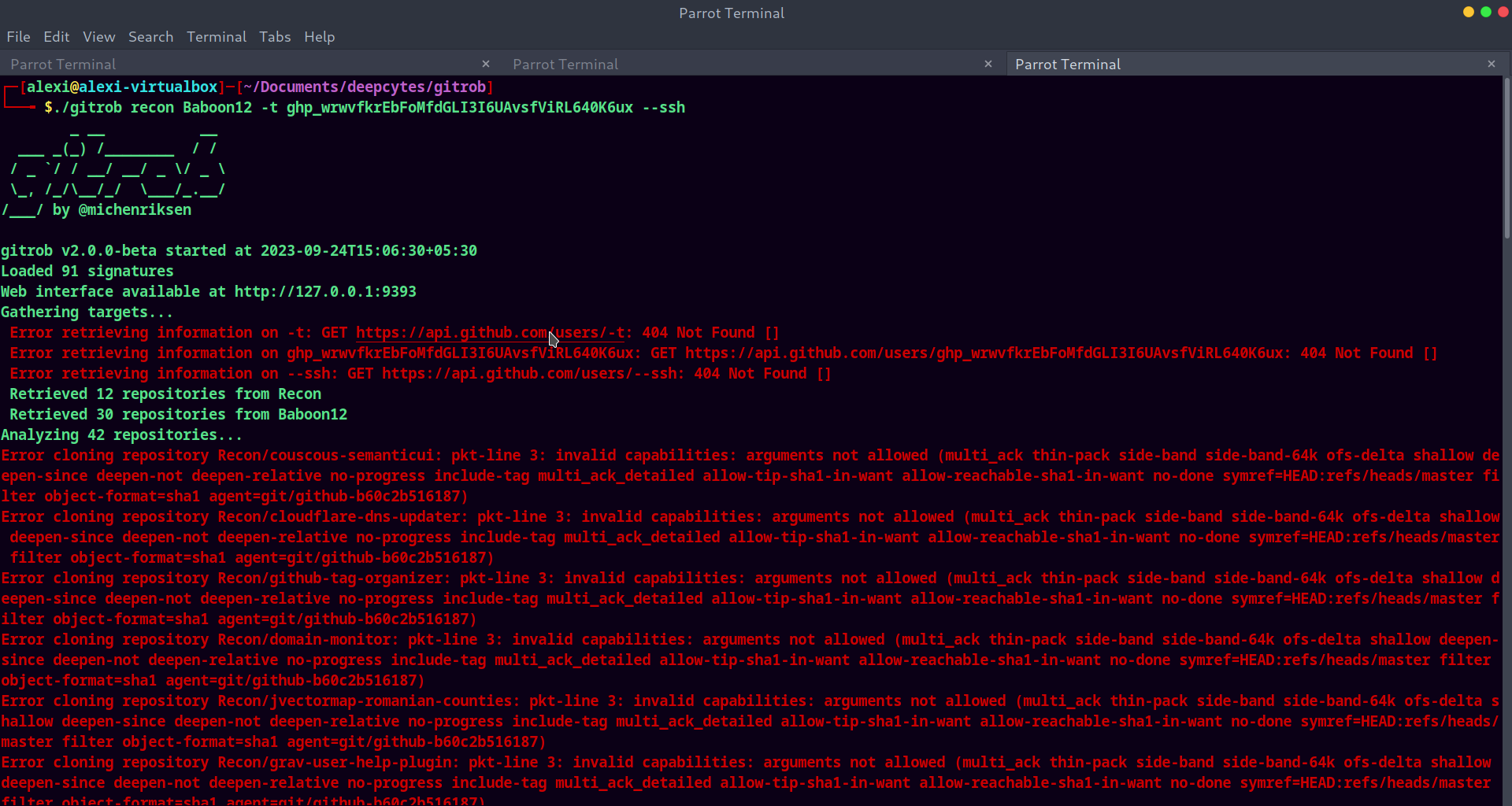
**Use Case 2.** Extract usernames

./gitrob -github-access-token=Access\_Token Baboon12



**Use Case 2.** Extract usernames

./gitrob recon Baboon12 -t Access\_Token --ssh



# Scope and Limitations

* Gitrob can only scan public repositories on GitHub. It cannot be used to scan private repositories unless you have proper authorization to access them. This means that sensitive information in private repositories may go undetected.
* Like any automated scanning tool, Gitrob may produce false positives (identifying data as sensitive when it's not) and false negatives (missing sensitive data). Users need to review the results carefully and manually verify findings
* GitHub imposes rate limits on API requests, which can affect the speed and efficiency of Gitrob scans, especially if you are scanning a large number of repositories

# Conclusion

Thus, we can say that, Gitrob is a valuable open-source tool for security professionals, penetration testers, and organizations concerned about identifying sensitive data exposure in public GitHub repositories

# References

<https://github.com/michenriksen/gitrob>