Step 1: Exploring the .git Directory

The `.git` directory is accessible due to a misconfiguration that allows directory listing. An attacker can browse to `http://target.com:8080/.git/` to view the git history.

Tools and Commands:

- **git-dumper** or manual browsing: Tools like `git-dumper` can be used to download the entire `.git` repository locally for further exploration.
  ```
  git-dumper http://target.com:8080/.git/ local_directory
  ```
- **Examine the history**: Use `git log` and `git diff` to review changes, especially look into commits that might contain credentials or sensitive changes.

Step 2: Extracting Credentials

Upon examining the git commit history, file containing flag can be found in the logs where it was added and then removed in subsequent commits.

Commands:

- **Finding commits with credentials**:
  ```
  git log -p
  ```
- This might show something like:
  ```
  commit 1234abc
  +CZ4067{s3cr3t_l0gs_4r3_us3ful}
  ```