GITHUB DORKING ?

Let's hunt for bugs, not for bounty!!

WHAT IS GITHUB DORKING

GitHub is a Git repository hosting service, but it adds many of its own features. While Git is a command line tool, GitHub provides a Web-based graphical interface.

Apart from this it also contains API keys, passwords, customer data etc. Basically it contains a lot of sensitive information which can be useful for an attacker. This sensitive information leaks can cost a company thousand dollars of damage. Let’s see the basic concept first of github recon.

GitHub Dork List :

1. GitHub Dorks for Finding Files

- filename:manifest.xml
- filename:travis.yml
- filename:vim_settings.xml
- filename:database
- filename:prod.exs
- filename:prod.secret.exs
- filename:.npmrc_auth
- filename:.dockercfg
- filename:WebServers.xml
- filename:.bash_history
- filename:settings.py
- filename:credentials.xml
- filename:sftp-config.json
- filename:sftp.json
- filename:secrets.yml
- filename:.esmtprc
- filename:passwd
- filename:LocalSettings.php
- filename:.sqlite
- filename:.psafe3
- filename:secret_token.rb
- filename:carrierwave.rb
- filename:database.yml
- filename:.keychain

GitHub Dork List :

2. GitHub Dorks for Finding Languages

- language:python username
- language:php username
- language:sql username
- language:html password
- language:perl password
- language:shell username
- language:java api

GitHub Dork List :

3. GiHub Dorks for Finding API Keys, Tokens and Passwords

- api_key
- “api keys”
- authorization_bearer:
- oauth
- auth
- authentication
- client_secret
- api_token:
- “api token”
- client_id
- password
- user_password
- user_pass
- passcode
- client_secret
- secret
- password hash
- OTP
- user auth

GitHub Dork List :

4. GitHub Dorks for Finding Usernames

- user:name (user:admin)
- org:name (org:google type:users)
- in:login (<username> in:login)
- in:name (<username> in:name)
- fullname:firstname lastname (fullname:<name> <surname>)
- in:email (data in:email)

GitHub Dork List :

5. GitHub Dorks for Finding Information using Dates

- created:<2012-04-05
- created:>=2011-06-12
- created:2016-02-07 location:iceland
- created:2011-04-06..2013-01-14 <user> in:username

GitHub Dork List :

6. GitHub Dorks for Finding Information using Extension

- extension:pem private
- extension:ppk private
- extension:sql mysql dump
- extension:sql mysql dump password
- extension:json api.forecast.io
- extension:json mongolab.com
- extension:yaml mongolab.com
- [WFClient] Password= extension:ica
- extension:avastlic “support.avast.com”
- extension:json googleusercontent client_secret