介绍:

在漏洞挖掘的过程前期我们进行信息收集，github 和码云搜索相关的信息，代码库，运气好的话可以在库中发现一些重要配置如数据库用户密码等

手工方法

gtihub 搜索语法:

| | |
|---|---|
| in:name baidu | #标题搜索含有关键字 baidu |
| in:descripton baidu | #仓库描述搜索含有关键字 |
| in:readme baidu | #Readme 文件搜索含有关键字 |
| stars:>3000 baidu | #stars 数量大于 3000 的搜索关键字 |
| stars:1000..3000 baidu | #stars 数量大于 1000 小于 3000 的搜索关键字 |
| forks:>1000 baidu | #forks 数量大于 1000 的搜索关键字 |
| forks:1000..3000 baidu | #forks 数量大于 1000 小于 3000 的搜索关键字 |
| size:>=5000 baidu | #指定仓库大于 5000k(5M)的搜索关键字 |
| pushed:>2019-02-12 baidu | #发布时间大于 2019-02-12 的搜索关键字 |
| created:>2019-02-12 baidu | #创建时间大于 2019-02-12 的搜索关键字 |
| user:name | #用户名搜索 |
| license:apache-2.0 baidu | #明确仓库的 LICENSE 搜索关键字 |
| language:java baidu | #在 java 语言的代码中搜索关键字 |
| user:baidu in:name baidu | #组合搜索,用户名 baidu 的标题含有 baidu 的 |

等等..

github 文档:

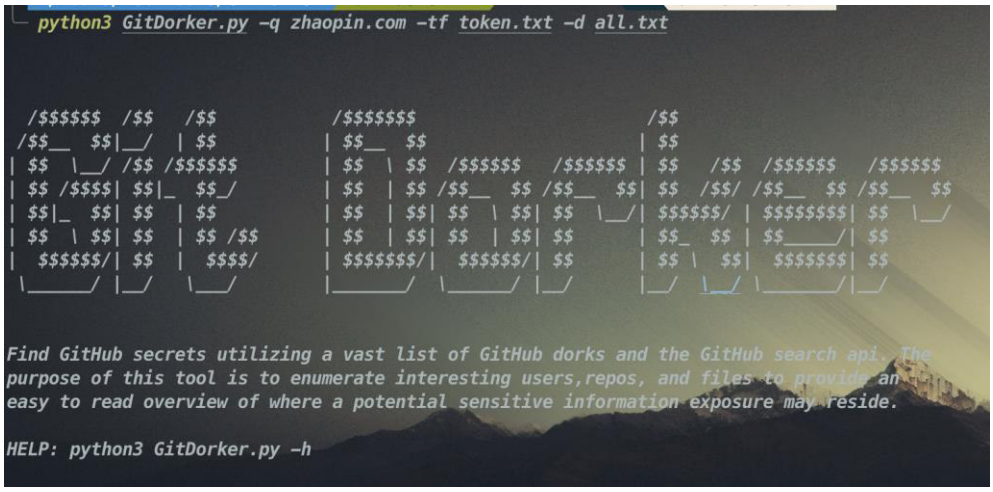
https://docs.github.com/en/search-github/searching-on-github/searching-for-repositories

fcmit.cc


自动化工具

GitDorker: https://github.com/obheda12/GitDorker

GitDorker 是一款 github 自动信息收集工具，它利用 GitHub 搜索 API 和作者从各种来源编译的大量 GitHub dorks 列表，以提供给定搜索查询的 github 上存储的敏感信息的概述

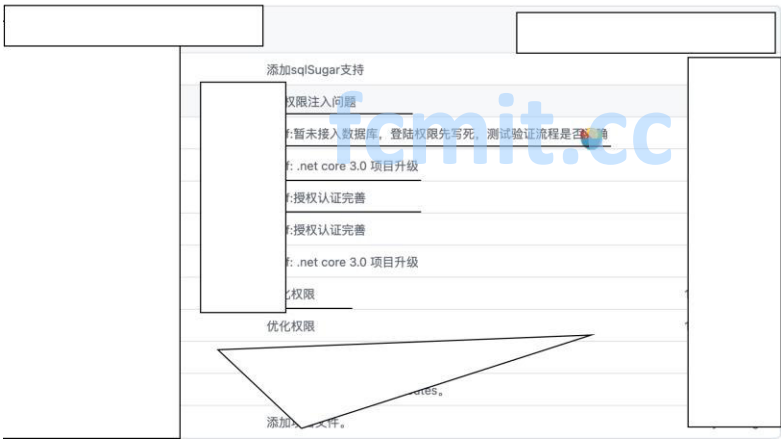



挖掘泄漏方法:

可以从域名开始找比如：xxx.com 我们就使用 github.com 等平台等搜索语法对包含 xxx.com 进行搜索，再一一进行逐个排查或者直接使用上方等自动化工具，直接跑也可以

高危案例:

某某某.com 存在敏感信息泄露，数据库用户名密码等泄露




通过查看库内文件找到了 数据库配置等信息