

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

github 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>

GitHub 文档

这篇文章也有[简体中文版本](#)。

在 GitHub 上搜索 / 在 GitHub 上搜索 / 搜索存储库

免费、专业和团队

搜索存储库

您可以在 GitHub 上搜索存储库, 并以任意组合使用这些存储库搜索限定符来缩小结果范围。

您可以在整个 GitHub.com 中全局搜索仓库, 或在特定组织内搜索仓库。更多信息请参阅[关于在 GitHub 上搜索](#)。

要在搜索结果中包含分叉, 您需要在查询中添加 `fork:true` 或 `fork:only`。有关详细信息, 请参阅[在分叉中搜索](#)。

提示:

- 有关可以添加到任何搜索限定符以进一步改进结果的搜索语法列表, 请参阅[了解搜索语法](#)。
- 在多词搜索词周围使用引号。例如, 如果您想搜索带有“进行中”标签的问题, 您可以搜索 `label:"in progress"`。搜索不区分大小写。

按存储库名称、描述或 README 文件的内容搜索

使用 `in` 限定符, 您可以将搜索限制为存储库名称、存储库描述、README 文件的内容或这些的任意组合。当您省略此限定符时, 仅搜索存储库名称和描述。

在本文中

- 按存储库名称、描述或 README 文件的内容进行搜索
- 按创建或上次更新存储库进行搜索
- 按语言搜索
- 按主题搜索
- 按主题数量搜索
- 按许可证搜索
- 按存储库可见性搜索
- 根据仓库是否为镜像进行搜索
- 根据仓库是否归档进行搜索
- 根据 first issue 进行搜索
- 根据赞助能力进行搜索
- 进一步阅读

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

