

Shodan.io, Google

Shodan.io

Требуется регистрация, платный сервис. Позволяет фильтровать поиск по:

ФИЛЬТР ПОИСКА	ОПИСАНИЕ	ПРИМЕР
Port	Номера портов	Port:80
Product	Имя продукта	Product: "Apache"
Org	Название организации. На латинице.	Org: "Target company name."
Country	Двухбуквенное обозначение страны	Country:RU
City	Город	City:Montreal
hostname	Доменное имя	Hostname: "domain-name.com"
os	Операционная система	os: "Linux"
http:title	Заголовок веб-страницы	http.title:"Dashboard"

И еще порядка 50 параметров.

Пример карточки объекта:

Regular View Raw Data Timeline Whois

Максимовщина Привольная Худькова Hot Springs

© OpenMapTiles Satellite | © MapTiler | © OpenStreetMap contributors

// LAST SEEN: 2025-10-08

General Information

Country **Russian Federation**

City **Irkutsk**

Organization

ISP

ASN

Open Ports

21 22 111 137 139 445 2049 4949 5900 5901

// 21 / TCP

-569280712 | 2025-10-04T20:49:41.023915

```
220 (vsFTPd 2.3.5)
228 login successful.
214 The following commands are recognized.
ABOR ACCT ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MKD
MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR
RNTD SITE SIZE SHUT STAT STOR STOU STRU SYST TYPE USER XCUP XCMD XMKD
XPWD XXRD
... ..
```

Google

Этот способ использования google называют Google Dorks. Генерация запросов dorks через ИИ <https://www.dorkgpt.com/>

site:github.com ключевые_слова	Слова на сайте. Много на github.
inurl:[критерий]	Поиск текста внутри URL. Поиск возможных мест SQL-инъекций на сайте: site:[домен] inurl:?id=
intitle:[критерий]	Поиск текста внутри заголовка веб-страницы. Поиск видеокамер: intitle:"index of" "cctv"
filetype:[расширение файла]	Поиск файлов по их расширениям. Поиск файлов, связанных с доменом, который является вашей целью: Site:[домен] filetype:"xls xlsx doc docx ppt pptx pdf"
intext:	Слова должны быть в теле страницы. intext:"Ошибка базы данных"
cache:	Показывает сохраненную в кеше Google версию страницы. cache:bobrobotirk.ru
define:	Быстрое определение термина. define:SQL injection.
link:	Показывает (не все) сайты, которые ссылаются на указанный URL.
related:	Поиск сайтов, похожих на указанный.

Комбинация запросов

"точная фраза"	Поиск страниц, содержащих точную фразу в кавычках. "логин или пароль неверен" (идеально для поиска конкретных сообщений об ошибках).
OR (или)	Логическое "ИЛИ". Найдет страницы, содержащие хотя бы одно из слов. python OR javascript tutorial
- (минус)	Исключает слово из поиска. python -snake (найдет все про язык Python, но исключит результаты про змей).
* (звездочка)	Подстановочный знак, заменяет любое слово или часть слова. Пример: "Используйте * для" (найдет фразы типа "Используйте Python для", "Используйте наш сервис для" и т.д.).
() — Группировка для сложных запросов.	Пример: (python OR java) site:github.com "beginner tutorial"

На сайте <https://www.exploit-db.com/google-hacking-database> размещена база с интересными запросами.

Revision #4

Created 8 October 2025 03:13:01 by Admin

Updated 6 November 2025 09:34:09 by Admin