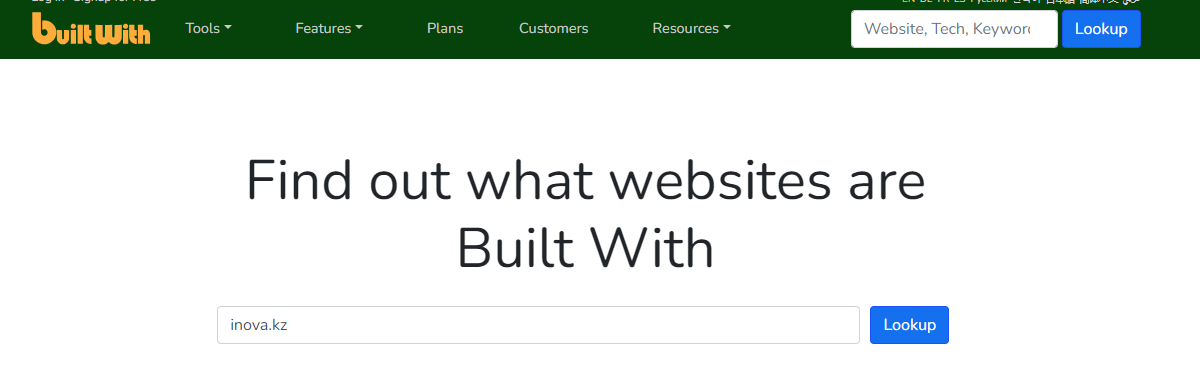
**Исследование технологий сайта с помощью Builtwith**

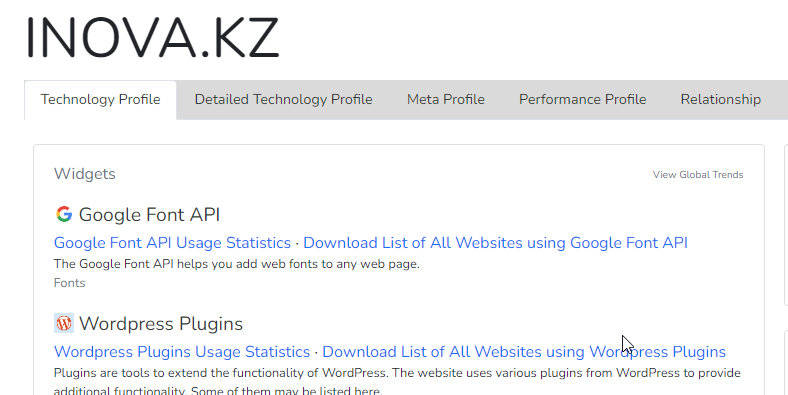
BuiltWith: Он предоставляет информацию о технологиях, которые используются на веб-сайте, таких как CMS, серверы, скрипты и другие технологии.

Запустите веб-браузер и перейдите на сайт Builtwith, введя адрес https://builtwith.com/.

В строке поиска введите домен inova.kz и запустите поиск.

Изучите и анализируйте используемые технологии на сайте.





**Задание 1:** Перейдите во вкладку "Задание" и укажите какую систему управления контентом (CMS) использует сайт inova.kz?

**Использование SHODAN для исследования**

SHODAN: Это поисковик для интернет-устройств. Он может искать устройства, серверы, камеры и многие другие вещи на основе их характеристик и служб.

**Примеры фильтров:**

title: Поиск контента, извлеченного из HTML-тега.

html: Поиск полного HTML-контента возвращаемой страницы.

product: Поиск названия программного продукта или обнаруженного в баннере программного обеспечения.

net: Поиск в заданном блоке сети (например, 204.51.94.79/18).

version: Поиск определенной версии продукта.

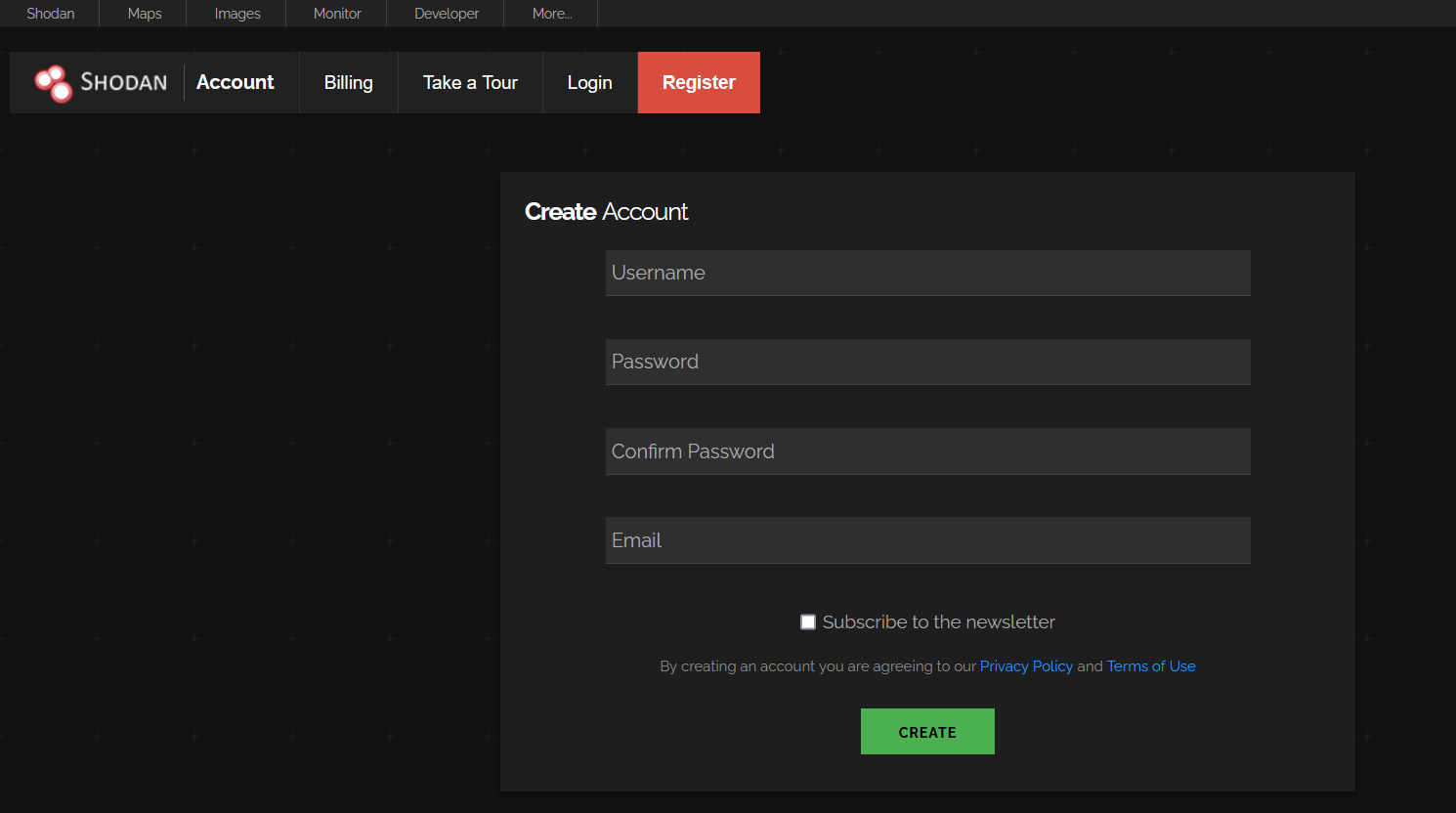
port: Поиск по конкретному порту или портам.

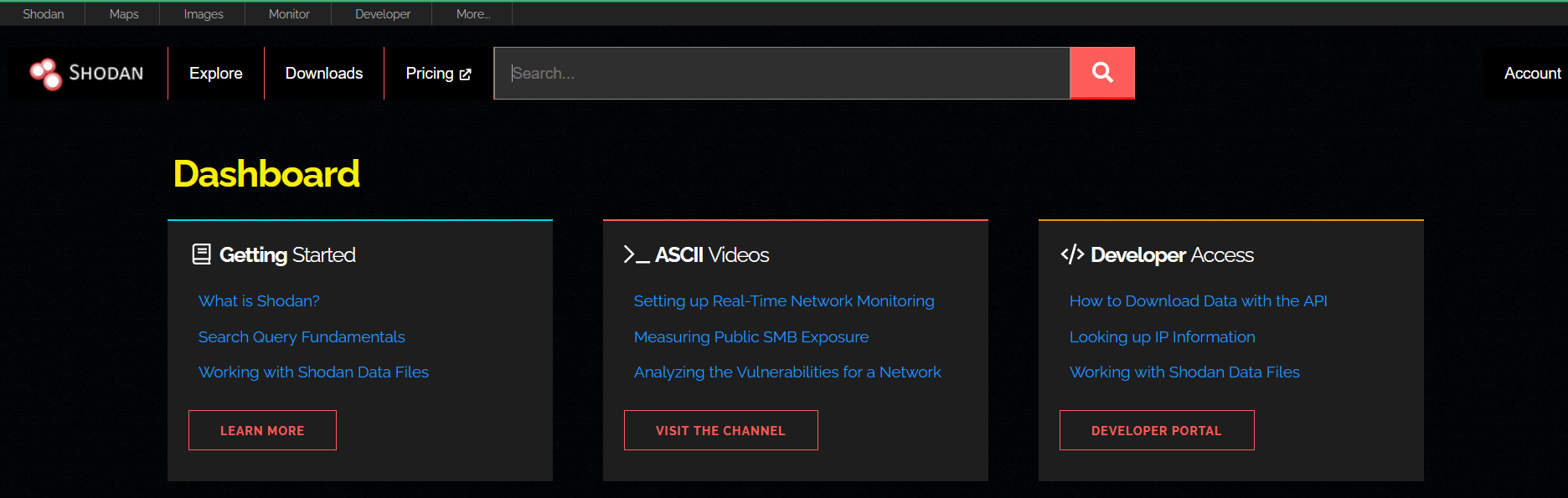
os: Поиск по названию операционной системы.

country: Поиск результатов в определенной стране (по 2-буквенному коду).

city: Поиск результатов в определенном городе.

**Примечание:** Чтобы использовать SHODAN, вам необходимо зарегистрироваться на сайте shodan.io.





Настоятельно рекомендуем вам зарегистрироваться и попробовать самостоятельно выполнить следующие задачи:

Поиск серверов, на которых запущен Outlook Web Access на портах, отличных от 80 и 443﻿

Поиск серверов nginx версии 1.14.0 в городе Алматы. Это может указывать на возможное наличие известных уязвимостей, связанных с этой версией nginx

FTP-серверы с возможностью анонимного входа

**Практика с Google Dorks**

Google Dorks — это техника, при помощи которой можно осуществлять более эффективный поиск в Google, используя специальные запросы. С помощью Google Dorks можно находить информацию, которая обычно не доступна при стандартных запросах, например, файлы определенных форматов, страницы с определенным содержимым, информацию на определенных сайтах и т. д.

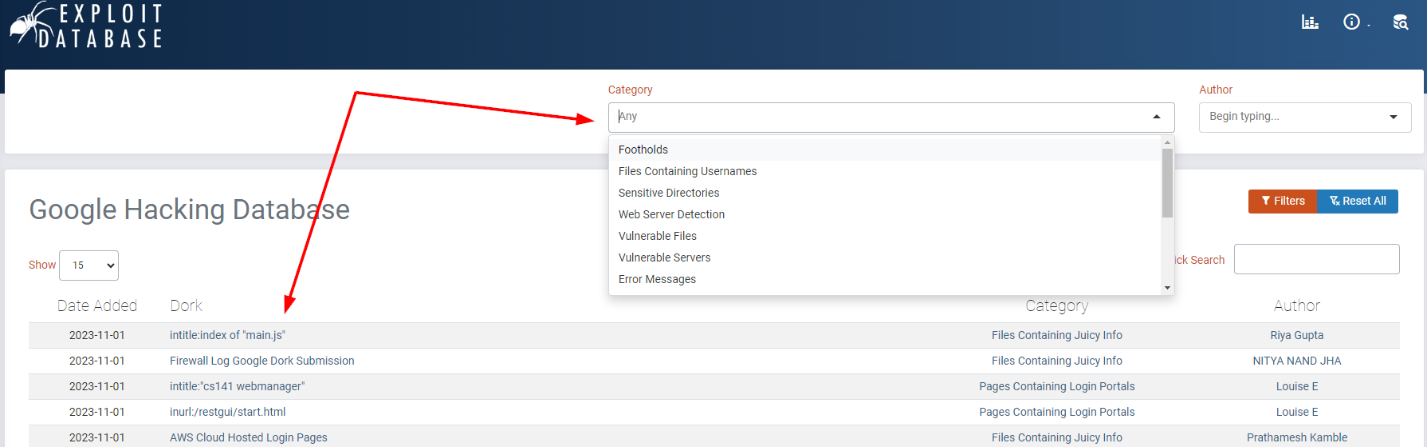
Основная идея заключается в использовании специальных операторов Google для фильтрации результатов поиска. Некоторые примеры таких операторов:

site:example.com filetype:pdf - ищет файлы PDF только на сайте example.com.

intext:"Учетные данные" - ищет страницы, содержащие фразу "Учетные данные".

inurl:admin - ищет страницы, URL которых содержит слово "admin".

Exploit Database (Exploit-DB) — это онлайн-платформа, которая предоставляет информацию о различных уязвимостях и эксплойтах. Это стало одним из самых популярных ресурсов среди исследователей безопасности, этических хакеров и специалистов по информационной безопасности. Особый раздел на этом сайте, известный как Google Hacking Database (GHDB), предоставляет коллекцию так называемых "Google Dorks".



Запустите веб-браузер и перейдите на сайт google.com. Используйте предоставленные Google Dorks для улучшения ваших навыков:

**Поиск PDF-файлов на сайте inova.kz:**

**Запрос:**

site:inova.kz filetype:pdf

Этот запрос поможет вам найти все PDF-файлы, которые расположены на сайте inova.kz. Это может пригодиться, если вы ищете конкретные документы или публикации на этом сайте.

**Поиск почтовых адресов на сайте inova.kz:**

**Запрос:**

site:inova.kz intext:\*@\*.kz

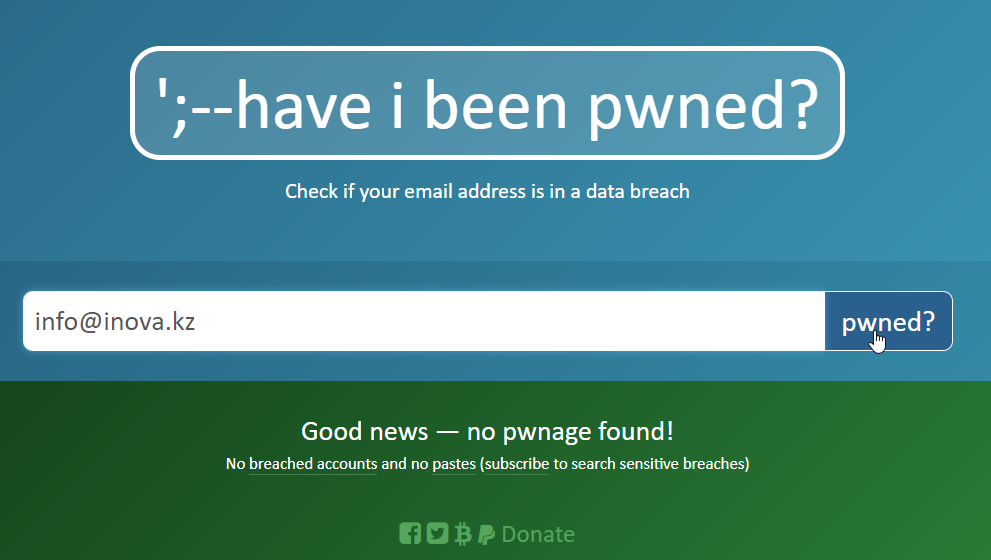
С помощью этого запроса вы можете обнаружить различные электронные адреса, которые указаны на веб-страницах сайта inova.kz.

**Задание 2:** Определите БИН компании.

**Задание 3:** Какие почтовые адреса выдает поиск? (Укажите один)

**Проверка на наличие утечек с помощью HaveIBeenPwned**

Сервис позволяет пользователям проверять, были ли их личные данные, в частности, электронные адреса, скомпрометированы в результате известных утечек данных.



1.Перейдите по адресу https://haveibeenpwned.com.

2.Заполните поле своим электронным адресом.

3.Узнайте, попадал ли ваш email в базы утечек данных.

4.Рекомендуем проверить также другие свои электронные ящики.

intelx.io: Платформа для сбора развед-данных (OSINT). Он собирает и анализирует информацию из разных источников.

Дополнительно, перейдите на сайт https://intelx.io/, чтобы узнать, каким студентам университетов Казахстана предоставляется ограниченный бесплатный доступ.

**Поиск контактной информации через hunter.io**

hunter.io: Этот сервис позволяет пользователям искать адреса электронной почты, связанные с определенным доменом.

1. Зайдите на сайт https://hunter.io/

2. Введите доменное имя inova.kz в поле поиска.

3. Изучите результаты, чтобы узнать электронные адреса, связанные с этим доменом.

**Задание 4:** Укажите электронный адрес, который вы обнаружили с помощью hunter.io.

**Проверка наличия вашего имени пользователя на различных платформах с whatsmyname.app**

1. Перейдите на https://whatsmyname.app/.

2. Введите ваше имя пользователя (username) в предоставленное поле.

3. Оцените результаты, чтобы узнать, на каких платформах это имя пользователя занято или свободно.