METASCAN

ООО «МЕТАСКАН» ОГРН: 1175024028772
ИНН: 5024179758 КПП: 502401001
Телефон: +7(495) 152-1337

Программное обеспечение для электронно-вычислительных машин «METASCAN»

Инструкция по работе в пользовательском интерфейсе

Листов 15

г. Красногорск, 03 мая 2023 г.

СОДЕРЖАНИЕ

АННОТАЦИЯ

Программное обеспечение для ЭВМ «METASCAN» (Далее - ПО «METASCAN») - это ПО распространяемое по модели SaaS (от англ. Software as a Service, Программное обеспечение как сервис), представляющее собой оркестратор набора специализированных программных средств.

ПО «METASCAN» предоставляется исключительно юридическим лицам и предназначено для инвентаризации корпоративных информационных активов (ресурсов) доступных из сети Интернет, а также обнаружения известных уязвимостей связанных с устареванием ПО, либо вызванных ошибками конфигурирования.

Область применения - инвентаризация и контроль ресурсов доступных из сети Интернет на отсутствие уязвимостей или ошибок конфигурации.

Функциональные возможности позволяют проводить проверку неограниченного количества ресурсов в течении не более одних суток (24 часа) с проведением проверок на сетевых уровнях от L3 до L7, идентифицировать доступные сетевые порты в диапазоне 0-65535 работающих по протоколам TCP или UDP, обнаруживать уязвимости и ошибки конфигурации системных и веб-сервисов, автоматический генерировать скрипт для ручной проверки выявленных уязвимостей.

Предоставляется компанией ООО «МЕТАСКАН» на облачной платформе по подписке, стоимость которой зависит от количества проверяемых ресурсов. Заказчик получает личный кабинет в свое пользование на весь срок подписки.

ПО «METASCAN» позволяет в автоматическом режиме:

- проводить поиск ресурсов доступных из сети Интернет;
- регулярно проверять доступность каждого порта внешнего сетевого периметра и контролировать их соответствие на соответствие списку разрешенных портов на внешнем сетевом периметре;
- для всего программного и программно-аппаратного обеспечения доступного из сети Интернет определять отсутствующие обновления безопасности;
- ранжировать уязвимости ПО по критичности;
- подбирать пароли для ssh, ftp, ftps, ms-sql, mysql, postgresql, vnc. Подбираются пароли для сетевого оборудования - snmp, cisco-telnet, winbox;
- выявлять ошибки администраторов и разработчиков в настройке прав на файлы и папки на веб-серверов приводящие к утечке критичных данных;
- обнаруживать уязвимости в веб-приложениях позволяющие захватить контроль над приложением или сервером, атаковать посетителей сайтов (используется классификация по OWASP-TOP-10. Обнаружение XSS, SQLi, NoSQLi, RCE, XXE и других).
- выявлять уязвимости в используемых компонентах веб-фреймворков и CMS. Поддерживается Magento, Wordpress, Bitrix. Находим уязвимости в js-библиотеках используемых веб-приложением.
- генерировать скрипт для ручной проверки эксплуатации уязвимости.

1. Размещение Системы

ПО «METASCAN» размещено на ресурсах арендованных в ЦОД ООО "Яндекс.Облако" (Yandex Cloud), которые размещаются в трех дата-центрах Яндекса, расположенных во Владимирской, Рязанской и Московской областях:

- г. Мытищи, ул. Силикатная 19.
- г. Владимир, ул. Энергетиков 37, корп. 2.
- г. Сасово, ул. Пушкина 21.

При сканировании ресурсов клиентов, доступных из сети Интернет, используются IP-адреса из следующих диапазонов:

- 51.250.124.64/26
- 217.28.236.96/27
- 217.28.236.80/28
- 178.154.239.240/28

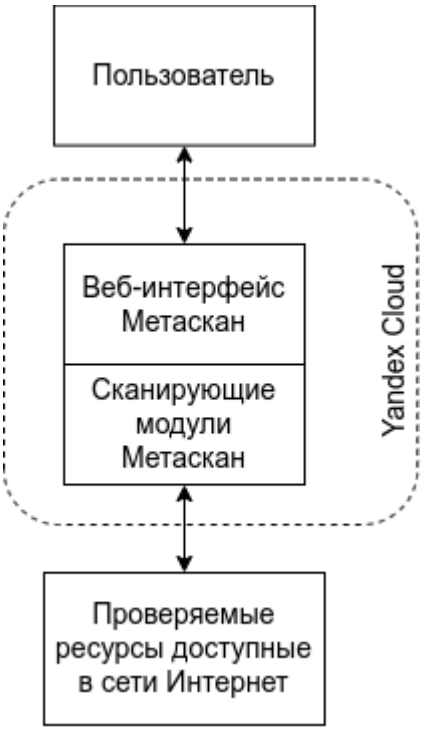

Рисунок 1. Схема работы Системы

2. Технические рекомендации для работы с сервисом

Для получения достоверных результатов работы сервиса необходимо внести следующие адреса в списки исключения на периметровых средствах защиты информации (WAF, antiDDoS, NGFW/UTM):

- 51.250.124.64/26
- 217.28.236.96/27
- 217.28.236.80/28
- 178.154.239.240/28

Веб-браузер должен иметь возможность выполнять JavaScript коды и быть совместим с React 18. Поддерживается последними версиями браузеров:

Edge 15 или новее,

Firefox 59 или новее,

Opera 12.10 или новее,

Google Chrome 66 или новее;

Для корректной работы системы рекомендуется регулярно обновлять браузер.

Неподдерживаемые веб-браузеры: Internet Explorer, Opera версий до версии 12.02, прочие браузеры.

Пакет офисного ПО (например, LibreOffice или Microsoft Office) для удобства работы с техническими отчетами выгружаемыми из интерфейса в формате CSV.

3. Вход в систему

Все функции системы доступны через панель управления:

https://service.metascan.ru

Логин и пароль для первого входа можно получить при самостоятельной регистрации или его предоставляет выделенный аккаунт-менеджер, их необходимо ввести в систему для авторизации (Рис.1).

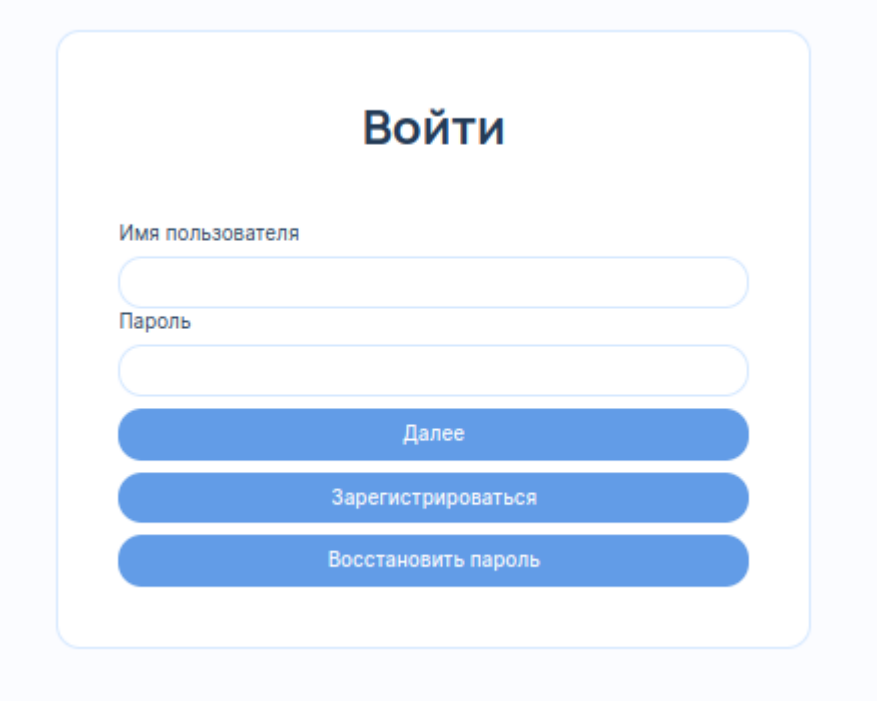

Рисунок 1. Форма авторизации и регистрации

После авторизации станет доступен личный кабинет.

4. Навигация

В личном кабинете размещены следующие функциональные разделы: «Главная», «Мои сайты», «Профили сканера», «Инфраструктура», «Порты», «Уязвимости», «Галерея», «Разведка» «Граф», «Расписание», «История проверок», «Мой аккаунт» и «Dorks».

Они располагаются последовательно друг за другом. В окне веб-браузера они располагаются в левой части панели управления (Рис. 2).

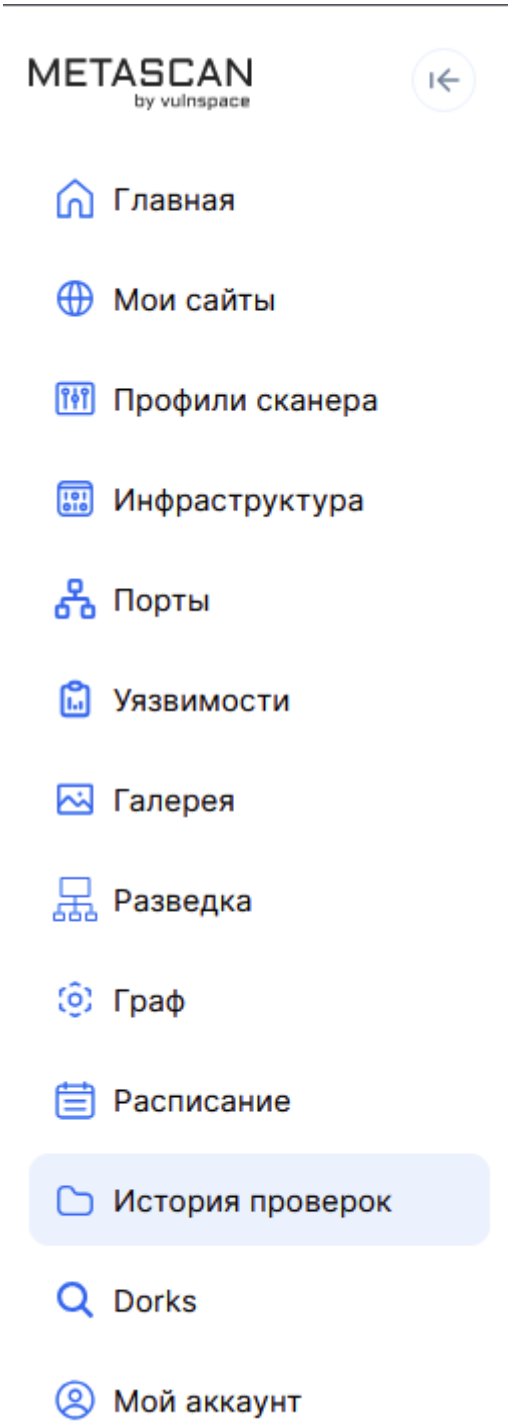

Рисунок 2. Разделы навигации

4.1. Раздел «Главная»

Этот раздел представляет общую, статистическую информацию по аккаунту. На представленных в разделе дашбордах (Рис. 3) вы можете получить информацию:

- о динамике изменения количества уязвимостей
- о текущем количестве угроз критического, высокого и среднего уровня.
- об открытых портах доступных из сети Интернет;
- о количестве проверяемых ресурсов и количестве проведенных проверок.

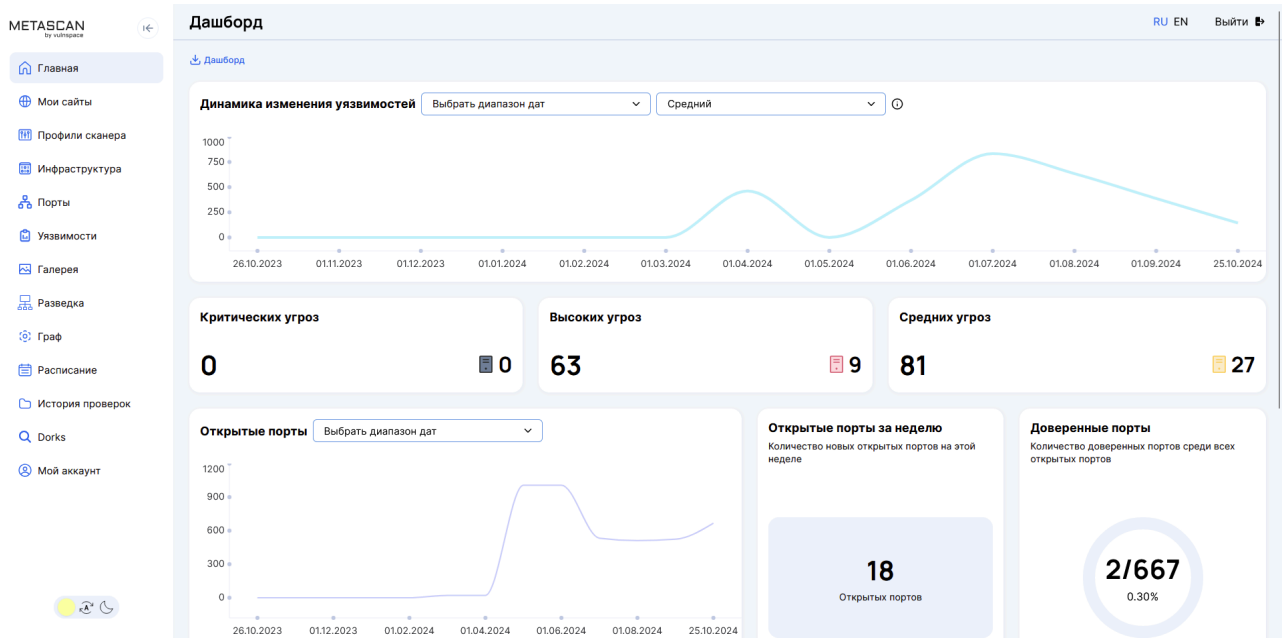

Рисунок 3. Личный кабинет пользователя - Главная

4.2. Раздел «Мой аккаунт»

В разделе можно посмотреть более детальную информацию об учетной записи, ограничения лицензии и получить API-ключ для проведения интеграции со сторонними решениями (Рис. 3).

Документация на API доступна по адресу: https://service.metascan.ru/api/v1/docs/

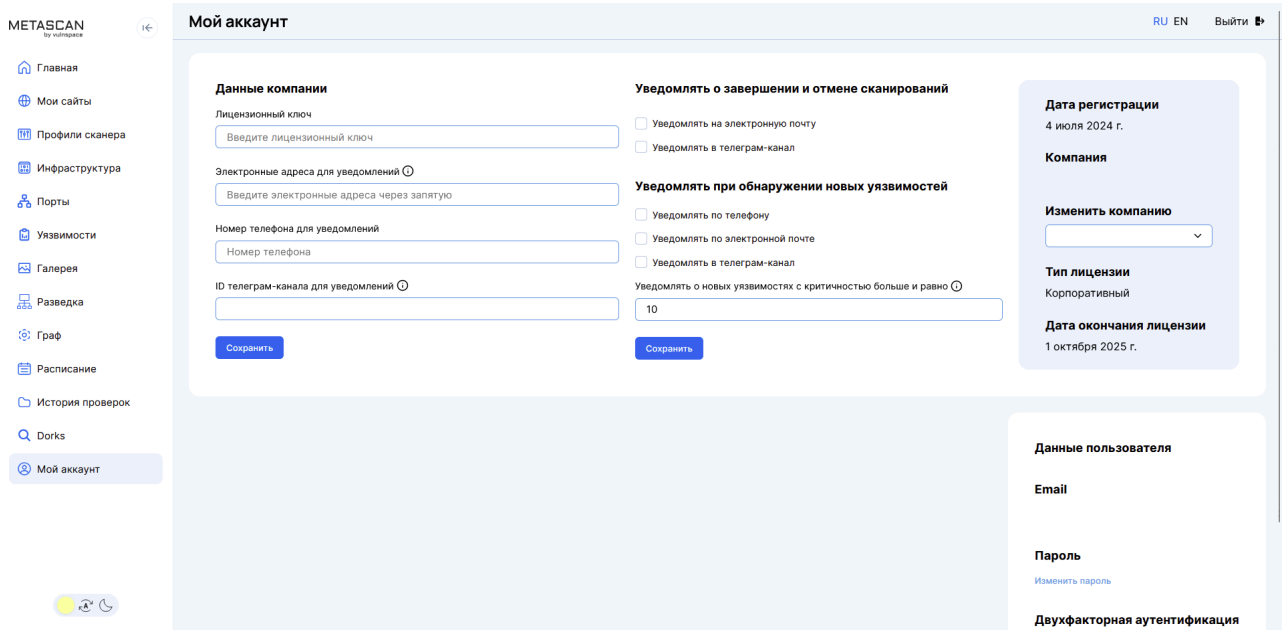

Рисунок 3. Детальная информация об учетной записи

4.2.1. Активация аккаунта

Для активации лицензии, на вкладке «Мой аккаунт» введите в поле «Лицензионный ключ» номер вашего лицензионного сертификата. При успешной проверке ключа ваша лицензия будет активирована.

4.2.2. Получение ключа API

Для интеграции ваших внутренних систем с Метаскан, воспользуйтесь API-ключем (Рис. 4), его можно получить наведя мышкой на поле «Ключ API». При необходимости сменить ключ или отказаться от использования ранее полученного ключа - воспользуйтесь соответствующими иконками в этом же поле, справа от надписи «Ключ API».

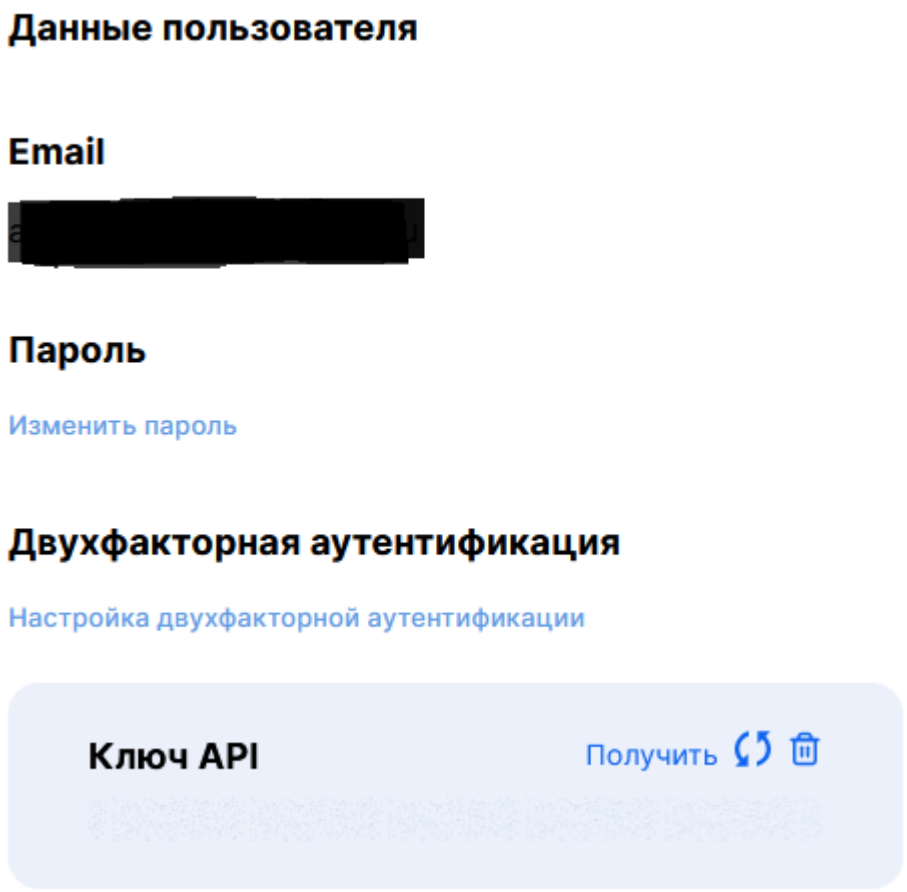

Рисунок 4. Ключ API

4.3. «Мои сайты»

Раздел «Мои сайты» содержит информацию о группах активов, активах, инвентаризационной информации и об обнаруженных уязвимостях (Рис. 5).

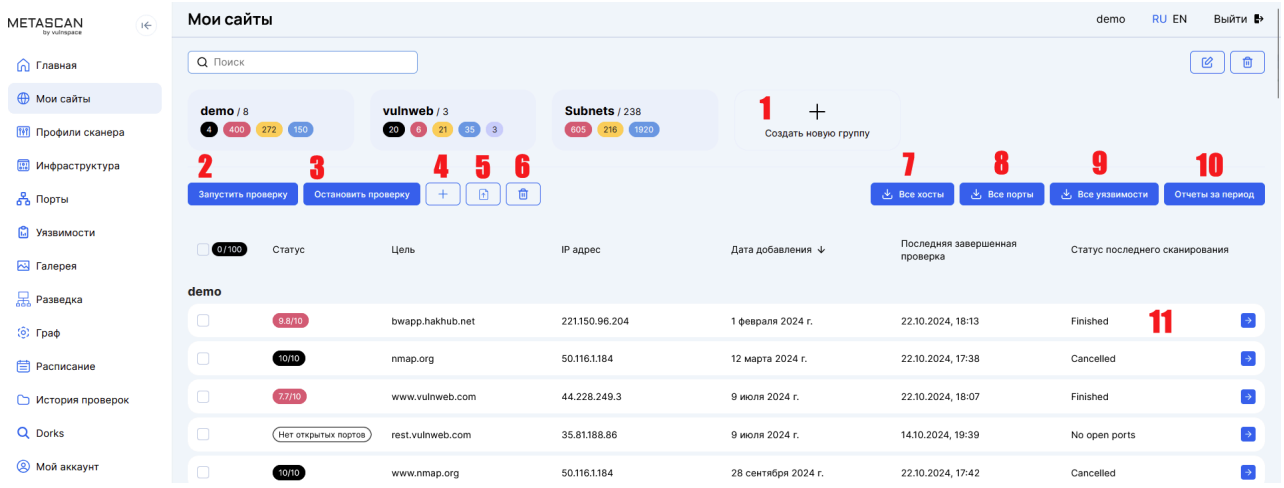

Рисунок 5. Личный кабинет пользователя - Мои сайты

В разделе «Мои сайты» вы можете:

- создать необходимое количество групп активов (цифра 1 на Рис. 5);
- для запуска проверки необходимо нажать на ссылку «Запустить проверку» и выбрать необходимый профиль сканирования (цифра 2 на Рис.5), создание профилей сканирования рассмотрено в разделе 3.3 «Профили сканирования»;
- при необходимости остановить сканирование необходимо воспользоваться кнопкой «Остановить проверку», выбрав перед этим ресурсы по которым необходима остановка (цифра 3 на Рис.5);
- в зависимости от необходимости и внести в них проверяемые ресурсы в виде доменного имени, IP-адреса или подсети, используя запись вида 123.0.0.0/24 (цифра 4 на Рис.5);
- либо загрузить их из текстового файла, где каждая строка будет соответствовать одному ресурсу (цифра 5 на Рис.5);
- либо удалить ресурс или ресурсы пометив необходимое количество и нажав на иконку с корзиной (цифра 6 на Рис.5);
- в разделе присутствует 4 ссылки для выгрузки технических отчетов в формате TXT или CSV, которые позволяют получить следующие отчеты:
    - все ресурсы добавленных в личный кабинет (цифра 7 на Рис.5);
    - все открытые порты (цифра 8 на Рис.5);
    - все обнаруженные уязвимости (цифра 9 на Рис.5)
    - получить дифференциальный отчет за период (цифра 10 на Рис.5);
- посмотреть подробную карточку ресурса с информацией по открытым портам и уязвимостям (цифра 11 на Рис.5).

4.3.1. Карточка ресурса

В карточке ресурса (Рис. 6) в верхней части присутствует меню навигации состоящего из разделов:

- «Информация» в котором вы можете:
    - получить информацию о статусе последней проверки;
    - получить и отредактировать информацию об открытых портах, их статус - доверенный/не доверенный и комментарии по каждому из них (при наличии);
    - загрузить Cookie-файл для проведения проверки веб-ресурса с авторизацией;
    - внести запись о текущих работах по хосту и их статус.

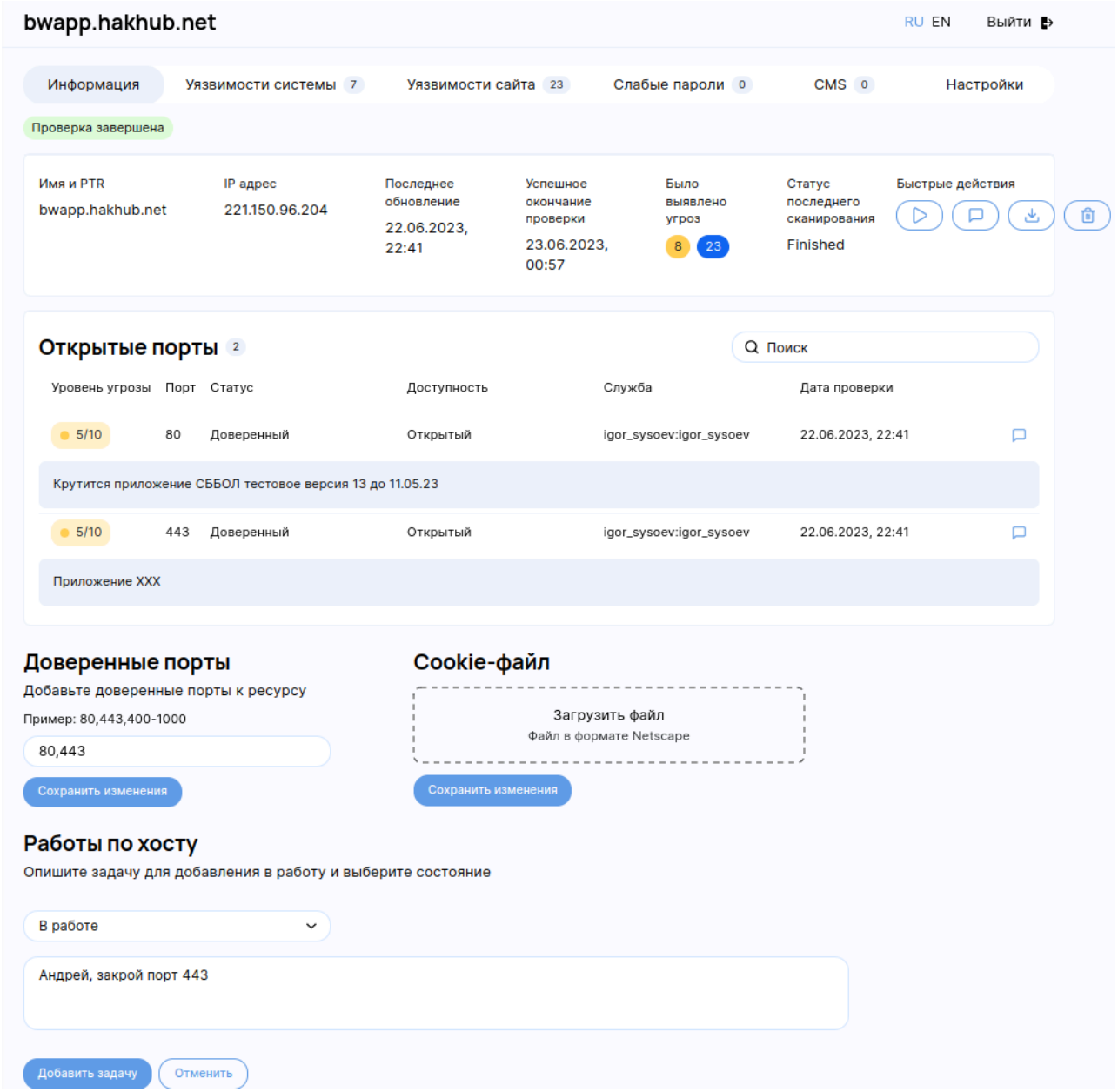

Рисунок 6. Карточка ресурса

- «Уязвимости системы», «Уязвимости сайта» и «CMS» в которых вы можете получить подробную информацию о системных уязвимостях, веб-уязвимостях и уязвимостях CMS соответственно, их критичности и способ устранения. В описании уязвимости содержится строка ручной проверки уязвимости (если применимо). А так же возможность пометить уязвимость специальным статусом: ложное срабатывание или не требующее исправления (won't fix) (Рис. 7). При отметке уязвимости такими статусами оценка риска будет понижена до -1 (из 10), разница между этими статусами в том, что при отметке уязвимости статусом «Ложное срабатывание» дополнительно создана заявка на разработчиков для проверки механизма выявления уязвимости.

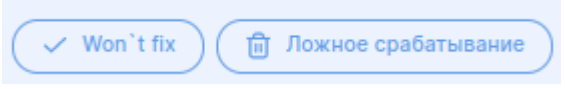

Рисунок 7. Специальные статусы для уязвимости

- «Слабые пароли» в разделе будут отображены все пары логин/пароль, которые были подобраны в результате проведенной проверки;
- «Настройки» в разделе вы можете указать используемые на ресурсе технологии, для ускорения работы сканеров. Сканеры не поддерживающие выбранные технологии будут пропущены при проверке.

4.4. «Профили сканирования»

В разделе «Профили сканирования» вы можете создать необходимое вам количество профилей для проведения инвентаризации или проверок на уязвимости. В профиле сканирования возможно произвести настройку скорости работы сканеров, что позволит регулировать нагрузку на проверяемые ресурсы. Общий вид раздела ниже (Рис. 8).

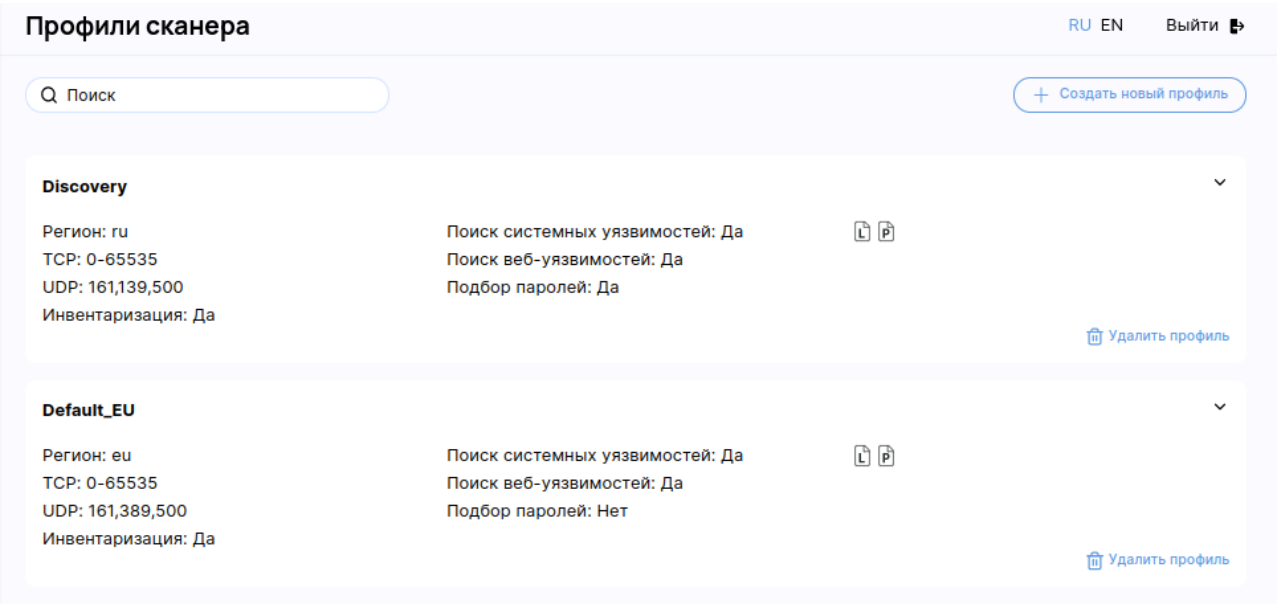

Рисунок 8. Профили сканера

Для настройки профиля необходимо выбрать существующий или создать новый профиль, общий вид профиля приведен ниже (Рис. 9). В котором вы можете:

1. присвоить профилю уникальное имя;
2. выбрать регион сканирования Россия или Европа (в зависимости от этого проверки будут проводиться с ресурсов «МЕТАСКАН» размещенных в соответствующих регионах);
3. указать диапазон или список проверяемых TCP-портов, с разделителем через «-» для диапазона и «,» для списка;
4. указать диапазон или список проверяемых UDP-портов, с разделителем через «-» для диапазона и «,» для списка (не рекомендуется указывать большое количество UDP-портов, это может значительно увеличить время проверки);
5. указать список разрешенных протоколов;
6. указать список нежелательных протоколов;
7. указать скорость проверки веб-приложений (RPS - request per second, запросов в секунду);
8. указать скорость проверки портов для подсети (единиц в секунду);
9. указать скорость проверки портов для хоста (единиц в секунду);
10. загрузить собственный словарь логинов (по умолчанию используется встроенный);
11. загрузить собственный словарь паролей (по умолчанию используется встроенный);

12. включить/выключить поиск поддоменов;
13. в разделе «Поиск системных уязвимостей» доступны следующие настройки:
    a. включить/выключить механизм поиска системных уязвимостей на основе баннерных проверок;
    b. включить/выключить механизм поиска системных уязвимостей на основе скриптов (будут использоваться NSE скрипты);
    c. включить/выключить механизм подбора паролей (используется механизм bruteforce). При включении данного функционала, по умолчанию, будет производиться подбор аутентификационных данных со встроенным словарем;
14. в разделе «Поиск веб-уязвимостей» доступны следующие настройки:
    a. включить/выключить механизм поиска ошибок в HTTP-заголовках;
    b. включить/выключить механизм поиска веб-уязвимостей на основе шаблонов Nuclei в распространенных веб-движках и CMS Bitrix;
    c. указать список непубличных шаблонов Nuclei для выявления веб-уязвимостей;
    d. включить/выключить механизм определения используемых веб-технологий на проверяемых ресурсах;
    e. включить/выключить механизм создания скриншотов страниц при обнаружении HTTP ответа;
    f. включить/выключить механизм поиска скрытых файлов и папок на веб-ресурсах;
    g. включить/выключить механизм рекурсивного перебора доступных каталогов на веб-ресурсах;
    h. включить/выключить механизм определения срабатывания WAF при сканировании ресурса;
    i. включить/выключить механизм поиска уязвимостей основанных на Wordpress;
    j. при наличии собственного токена для wpscan рекомендуется внести его, если оставить поле пустым, будут использованы токены загруженные в платформу разработчиками;
    k. включить/выключить механизм поиска уязвимостей в CMS Magento;
    l. заменить user-agent, который будет использоваться для сканирования, если необходимо.
15. В разделе «Сканер веб-уязвимостей» доступны следующие настройки:
    a. включить/выключить сканер веб-уязвимостей (при выключении любых других проверок связанных с веб-уязвимостями будет отключен). Включение данного функционала, так же включает обнаружение форм аутентификации в веб-приложениях;
    b. включить/выключить сбор информации о страницах на сайте при помощи краулера Katana и статического анализатора JS-файлов, настроить дополнительные опции обхода сайта;
16. В настройках проводимой атаки для «Сканера веб-уязвимостей» доступны следующие настройки:
    a. включить/выключить механизм поиска SQL-injection уязвимостей;
    b. включить/выключить механизм XSS уязвимостей;
    c. включить/выключить механизм поиска CMD-injection уязвимостей;
    d. включить/выключить механизм поиска NoSQL-injection уязвимостей;
    e. включить/выключить механизм поиска XXE уязвимостей;

f. включить/выключить механизм поиска Time-based SQL Injection и Blinde SQL Injection уязвимостей;

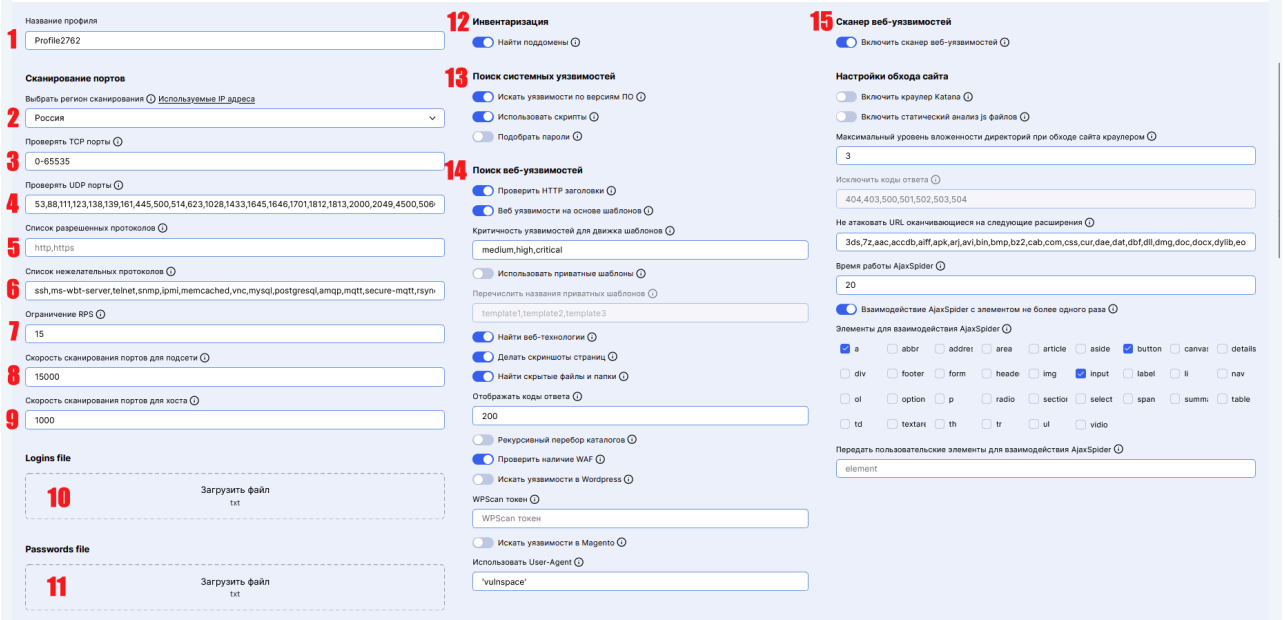

Рисунок 9. Профиль сканера

4.5. «Инфраструктура»

В разделе «Инфраструктура» представлены карточки ресурсов отсортированные по мере убывания уровня критичности обнаруженных на них уязвимостей (Рис. 10). Для отображения критичности используется следующая цветовая кодировка:

- Черный цвет - присутствует минимум одна уязвимость критического уровня (Critical), требующая немедленной реакции по устранению. Уязвимости такого уровня обычно легко эксплуатируются автоматическими системами, злоумышленниками с низким уровнем компетенций и/или имеют публичный эксплойт;
- Красный цвет - присутствует минимум одна уязвимость высокого уровня (High), требующая срочной реакции по устранению. Уязвимости такого уровня обычно легко эксплуатируются злоумышленниками с низким уровнем компетенций;
- Оранжевый цвет - присутствует минимум одна уязвимость высокого уровня (Medium), требующая внимания. Уязвимости такого уровня обычно эксплуатируются злоумышленниками с высоким и средним уровнем компетенций, либо информация получаемая при эксплуатации позволяет получить дополнительную информацию, которая может быть использована для эксплуатации других уязвимостей;
- Синий цвет - уязвимости низкого (Low) и информационного уровня (Information). Данный тип уязвимостей может дать злоумышленникам с высоким уровнем компетенции дополнительную информацию для проведения атак;
- Серый цвет - отмечены узлы на которых отсутствуют уязвимости, либо открытые порты, либо узел по каким-либо причинам не был проверен (например, проверка была заблокирована средствами защиты).

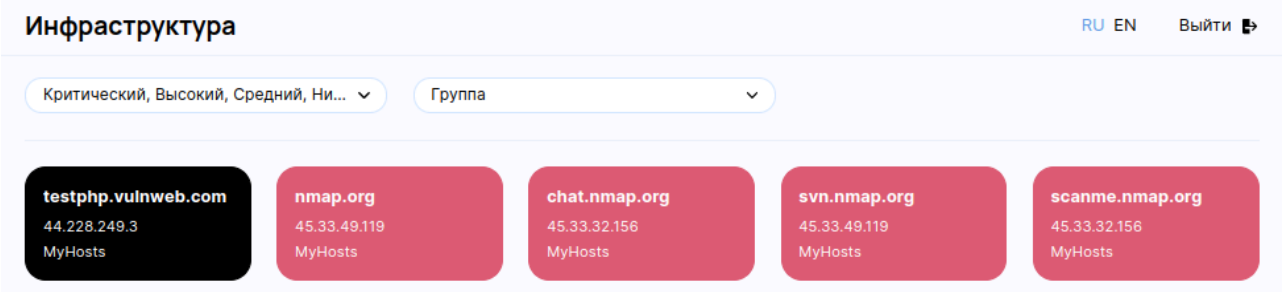

Рисунок 10. Инфраструктура

При клике на выбранный ресурс произойдет автоматическое перенаправление на карточку ресурса.

4.6. «Порты»

Раздел «Порты» позволяет просмотреть информацию об открытых портах выявленных в ходе работы сканера (Рис. 11)

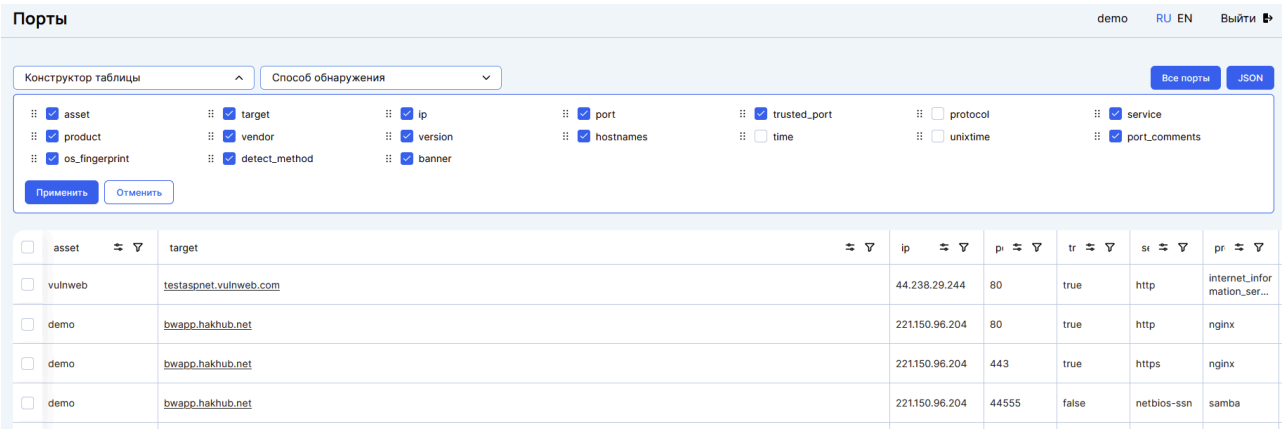

Рисунок 11. Порты

- В данном разделе доступен Конструктор таблицы с помощью которого можно выбрать желаемые столбцы для отображения выявленных портов и дополнительной информации по данным портам
- В разделе «Порты» можно загрузить полный списком портов используя кнопки «Все порты» и «JSON»

4.7. «Уязвимости»

Раздел «Уязвимости» позволяет просмотреть информацию о найденных уязвимостях, выявленных в ходе работы сканера (Рис. 12) Учет уязвимостей производится на основе уровня критичности уязвимости, соответственно черный цвет - критичный, красный - высокий, желтый - средний, синий - низкий или информационный уровень критичности.

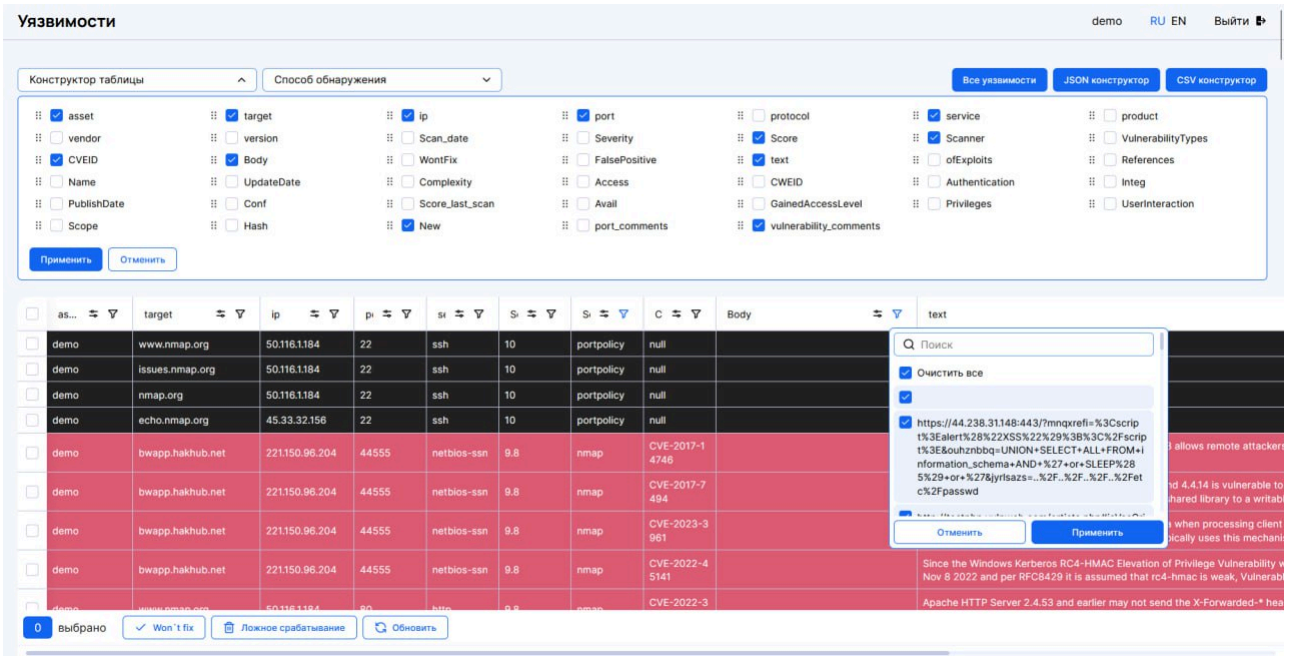

Рисунок 12. Уязвимости

- В данном разделе доступен Конструктор таблицы с помощью которого можно выбрать желаемые столбцы для отображения выявленных уязвимостей и дополнительной информации по ним
- Кнопка “Все уязвимости” позволит вам скачать csv-файл с полным отчетом по всем уязвимостям.
- Кнопка “JSON конструктор” позволяет получить данные по уязвимостям в формате JSON в соответствии с выставленными колонками в Конструкторе таблиц
- Кнопка “CSV конструктор” позволяет скачать csv с отчетом по уязвимостям в соответствии с выставленными колонками в Конструкторе таблиц
- Каждую колонку можно сортировать по возрастанию\убыванию\скрыть, а также выбрать конкретные значения в ней
- По умолчанию уязвимости отсортированы по уровню критичности от 10 и ниже

4.8. «Галерея»

Раздел «Галерея» содержит скриншоты всех заглавных страниц, обнаруженных при проведении последней проверки. Скриншоты производятся по каждому веб порту, найденному на том или ином ресурсе (доменное имя или ip адрес)

4.9. «Разведка»

Раздел «Разведка» содержит в себе результаты работы модуля “Поиск поддоменов”. Его можно включить в профиле сканирования. Вы можете добавить ресурсы в группы сканирования из раздела “Мои сайты”, нажав на соответствующую кнопку. Выбирая фильтр “по подсети”, вы можете посмотреть к какой подсети и кому принадлежит ip адрес, на котором нашелся тот или иной поддомен.

4.10. «Граф»

Раздел «Граф» содержит графическое представление сетевой связанности ресурсов внесенных в личный кабинет, а также графическое представления возможных векторов распространения рисков на взаимосвязанные ресурсы Заказчика.

4.11. «Расписание»

Раздел «Расписание» позволяет настроить расписание запуска задач на сканирование и выпуск отчетов.

Внимание! Все времена старта задач указываются по UTC, -3 часа от Московского времени.

4.12. «История проверок»

Раздел «История проверок» позволяет получить информацию о дате запуска, завершения и статусе задач на сканирование.

В разделе можно остановить сканирование по выбранному ресурсу и скачать отчет.

4.13. «Dorks»

Модуль дорков представляет собой специально отобранный список поисковых запросов в поисковые системы с использованием логических операторов.

О каждом из представленных запросов можно сказать, что они являются шаблоном запроса (Рис. 13) в который подставляется искомый домен. В качестве искомого домена можно использовать домен первого уровня (пример: abc.ru), используемые операторы автоматически будут искать утечки на всех поддоменах.

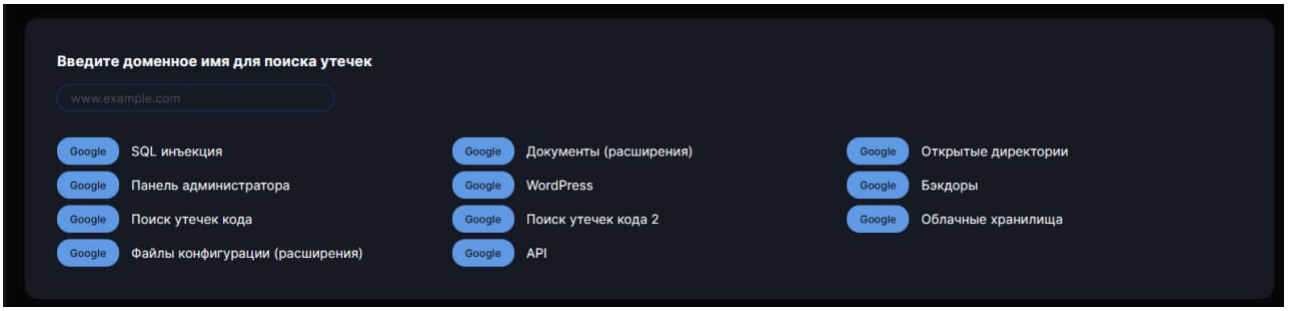

Рисунок 13. Dorks

Порядок действий для использования модуля:

1. Ввести доменное имя в поле.
2. Нажать на кнопку интересующего шаблона для перехода на поисковый запрос.
3. Вручную проанализировать результаты поиска.

Совет: рекомендуется в конце списка результатов поиска нажать на ссылку "Показывать повторяющиеся результаты", т.к. иногда при одинаковых названиях документов могут выводиться документы с уникальным содержанием.

5. Часто задаваемые вопросы

5.1. Как настроить автоматизированную выгрузку DNS-зоны?

- Инструкция для Cloudflare: https://community.cloudflare.com/t/export-the-dns-files-globally-for-all-my-domains/97697
- Инструкция для Nic.ru: https://www.nic.ru/help/upload/file/API_DNS-hosting.pdf

- Инструкция для Selectel: https://docs.selectel.ru/api/dns-actual/#tag/Zones/operation/create_zone_zones_post

5.2. Как работает скорость сканирования портов по подсети / хосту?

- При запуске сканирования по ресурсу сначала проверяется какой тип ресурса сканируется:

  Подсеть: 192.168.1.0/24

  Хост: 192.168.1.1
- Если сканируемый ресурс - это подсеть, то при установленном значении скорости сканирования подсети 10000 на каждый адрес в подсети не будет приходить больше чем 10000/255=39 пакетов
- Если сканируется несколько подсетей, на каждую будет приходить 10000 пакетов / сек
- Если в подсети только 4 адреса, то на каждый будет приходить не больше значения установленного в скорости сканирования одного хоста