SolidPoint DAST

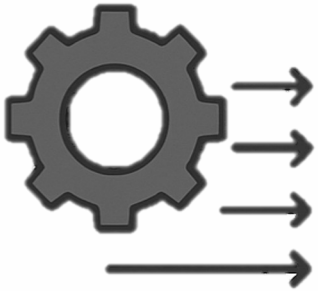
Управление динамическим анализом безопасности веб приложений и сервисов

solidpoint

Что такое динамический анализ веб-приложений и API?

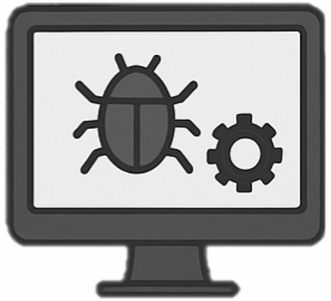
Динамический анализ имитирует атаки на работающие веб-приложения или сервисы, чтобы выявить уязвимости, которые реально можно эксплуатировать.

Дает всестороннее представление о безопасности веб приложения



Может быть интегрирован в этапы разработки тестирования и эксплуатации

Позволяет управлять рисками в масштабе портфеля



Тестирует работающее приложение

Динамический анализ веб-приложений и API

solidpoint

Основные вызовы

- Анализ поверхности атаки с учетом клиентского кода
- Обнаружение критических уязвимостей и минимум FP
- Автоматизация и управление процессом сканирования в сценариях разработки и для решения оперативных задач ИБ
- Масштабирование (организационно и технически)
- Актуальность технологий

solidpoint

Dynamic Analysis
for Security Testing

Объект сканирования

Цель сканирования

Описывает сканируемое приложение:

- URL
- Лимит нагрузки
- OpenAPI спецификация
- Аутентификация

Информация о цели

Адрес	http://vampi.stands.appsecuritytesting.fun
Описание	Vulnerable REST API https://github.com/erev0s/VAmPI

Спецификация API

Спецификация OpenAPI	vampi.yml

Ограничения

Ограничение запросов	20 запросов в секунду
Ограничения URL-адресов	• `/api/auth`

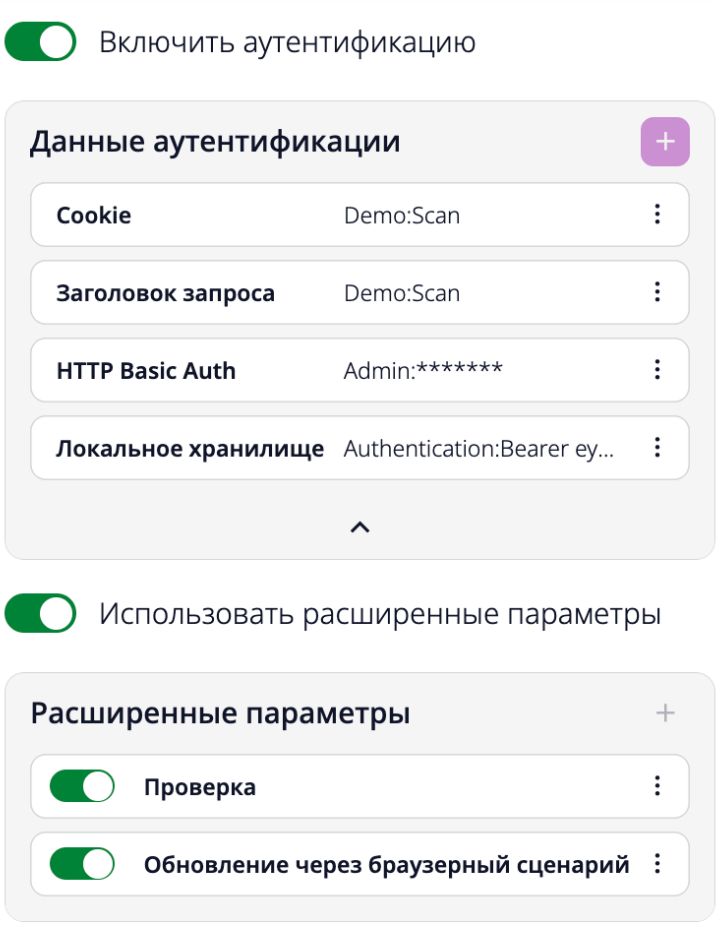
Аутентификация

Базовые технологии:

- Cookie
- Заголовок запроса
- HTTP Basic Auth
- Локальное хранилище
- Клиентский TLS-сертификат

Расширенные (JWT, Record/replay сценария. Проверка сессии):

- Проверка
- Обновление через HTTP-запрос
- Обновление через браузерный сценарий

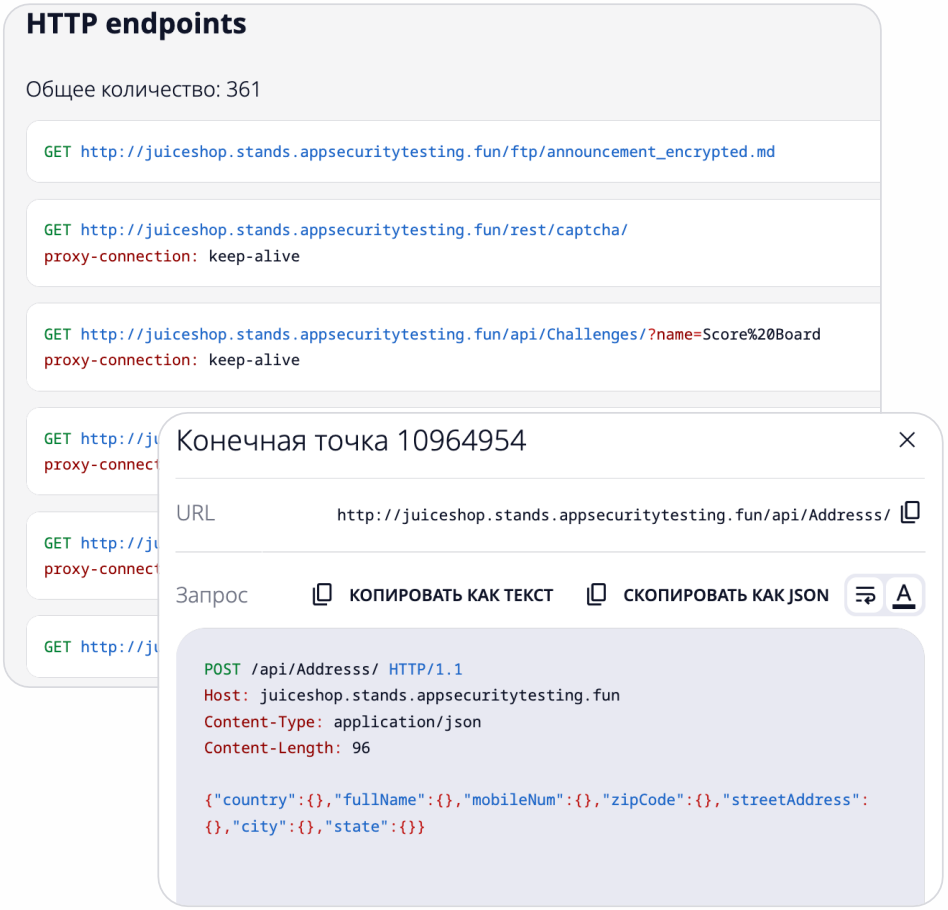


Фаза сканирования:
Анализ поверхности атаки

Обнаружение поверхности атаки

Применяемые методы и инструменты

- Обнаружение поверхности атаки
  - Статический и динамический краулер
  - Перебор директорий
  - Статико-динамический анализ клиентского JS кода
  - Импорт OpenAPI спецификации и SOAP API
  - Импорт трафика с SolidWall WAF
  - Поиск GraphQL
  - Импорт HAR



Обнаружение поверхности атаки

- Комбинирование методов для повышения покрытия
- Поддержка дедупликации выявленных точек ввода данных
- Уникальные технологии статико-динамического анализа JavaScript кода[1]
  - Возможность анализа закомментированного кода
  - Возможность обойти все ветки кода

[1] Статья: http://journals.tsu.ru/engine/download.php?id=223281&area=files

Выступление: https://www.youtube.com/watch?v=vG0EzOr81pE

Блог: https://blog.secsem.ru/ru/mining-requests-from-js-with-static-analysis/

JS-Analyzer

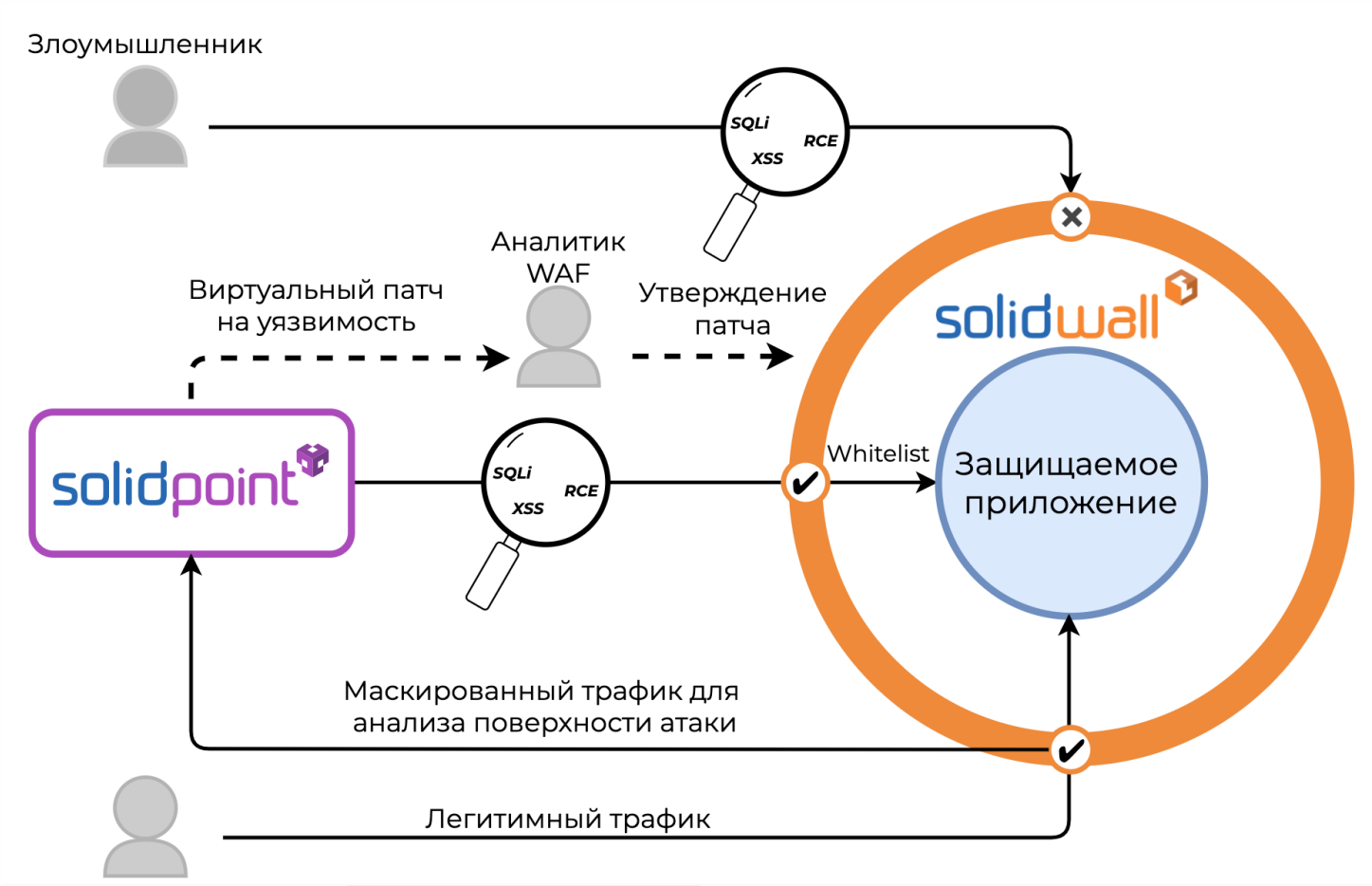
Выявление DEP

- Анализ клиентского кода статическими методами
- Анализ DEP из кода вне зависимости от наличия авторизации
- Не зависит от логики сайта или страницы, проанализированы будут все вариации переходов

```
<script type="text/javascript">
        function saveLike(articleID) {
            $.ajax({
                method: 'POST'
                url: '/api/like/add',
                data: {
                    id: articleID
                }
            });
        }
        function getNewsList(cb) {
            $.getJSON('/api/get-data?type=news_list', cb);
        }
  </script>
</head>
<body>
  <a href="/user/profile?id=18">Article author</a>
  <a href='/article/text?id=84932">Read full text</a>
  <form method="POST" action="/news/search">
    <input type="text" name="query">
    <input type="text" name="sort_by">
    <input type="submit" name="Искать">
```

Обнаружение поверхности атаки

Интеграция с WAF

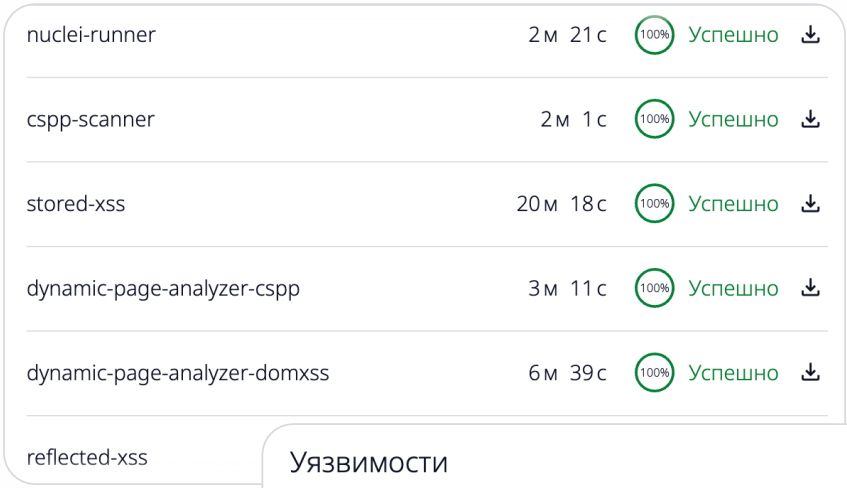


Фаза сканирования:
Взлом

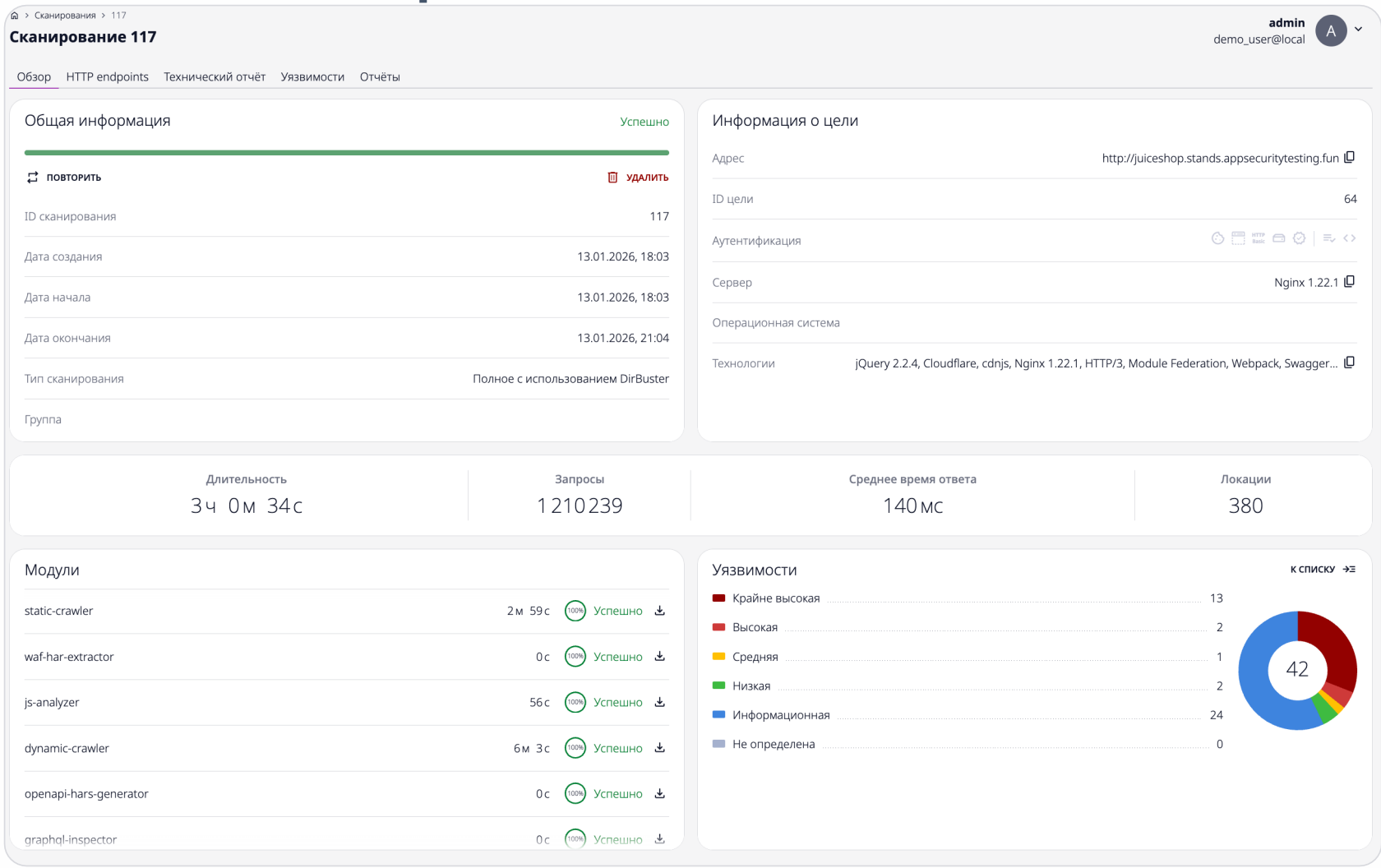
Сканеры безопасности

Применяемые методы выявления уязвимостей

- Переборные проверки
  - Перебор паролей
  - Перебор директорий
- Сигнатурные
  - Пассивный сигнатурный анализ
  - Активный сигнатурный анализ
- Фаззеры
  - Insecure Deserialization
  - Reflected XSS
  - DOM Based XSS
  - Stored XSS
  - XXE
  - NoSQLi
  - SQLi
  - SSTI
  - Path Injection
  - Shell Injection
  - HTTP Smuggling
  - File Upload
  - Prototype Pollution
- Поддержка Out-of-Band метода

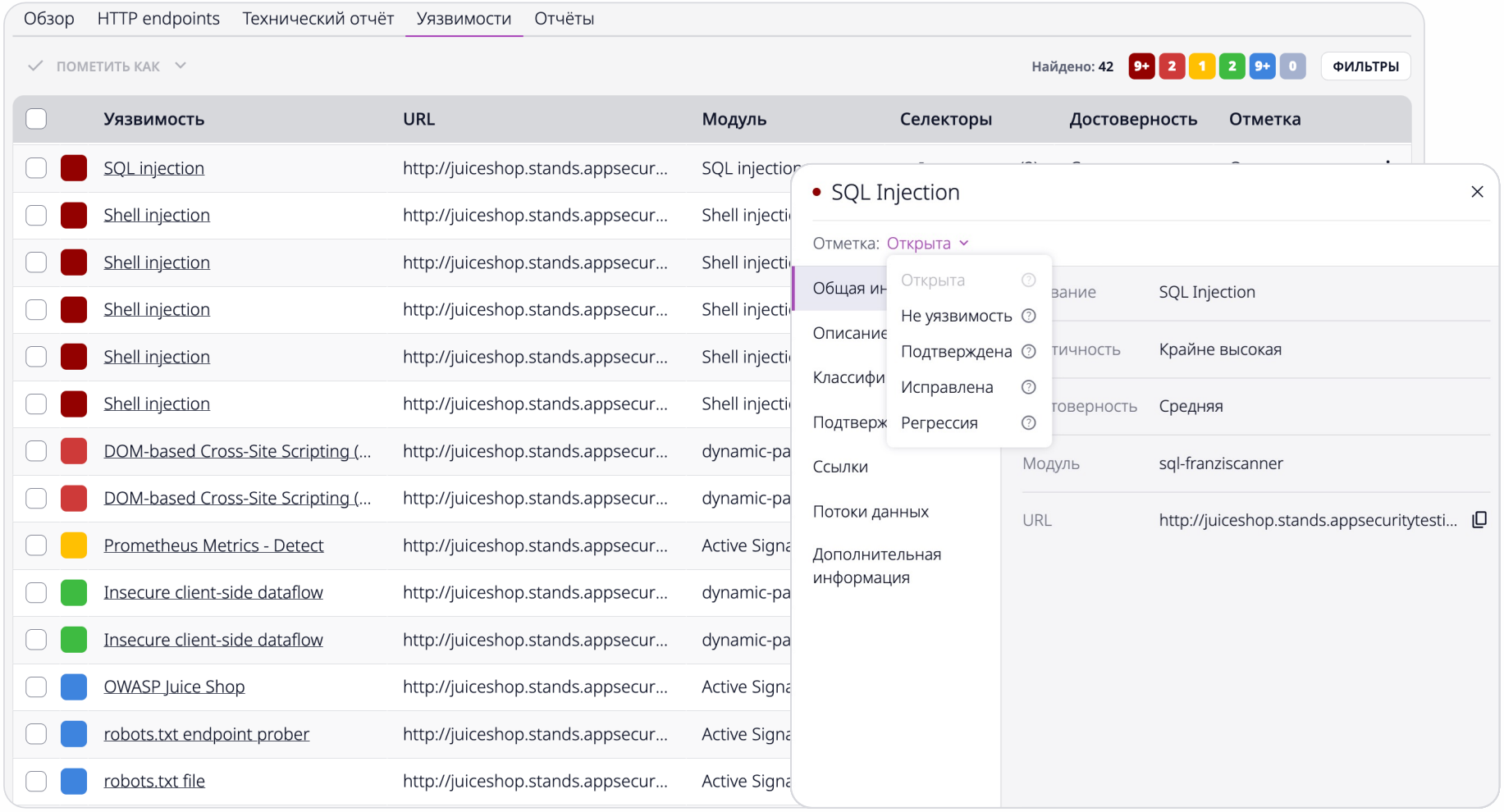


Процесс сканирования



Результаты сканирования

Детальная информация по каждой уязвимости и процесс анализа



solidpoint

Дополнительно о продукте

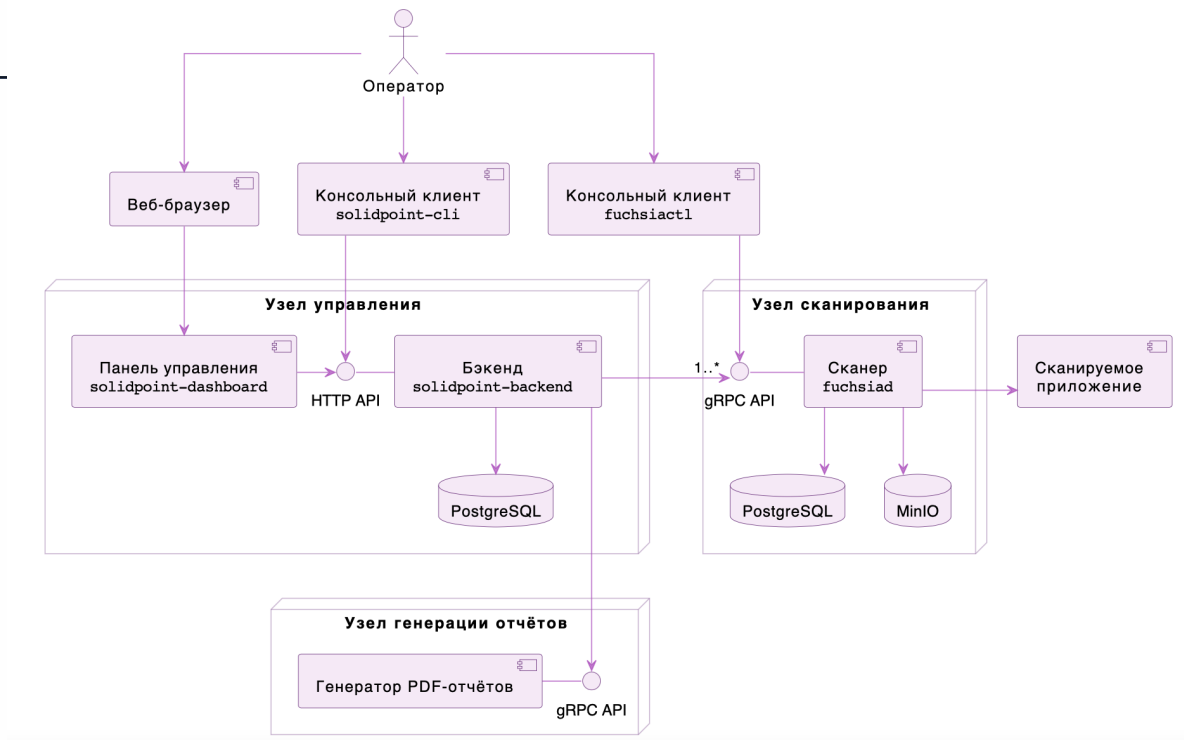
Масштабирование и архитектура

Масштабирование

- Единый сервер управления
- Горизонтальное масштабирование

Типы дистрибутивов

- Apt пакеты (Debian)
- Docker compose
- Kubernetes – helm chart



Промышленные возможности

- LDAP аутентификация
- Экспорт результатов сканирования во внешние системы
  - К Defect Dojo готовый парсер
  - JSON формат
- REST API
  - CLI на базе REST API
  - Интеграция с оркестраторами CI\CD, в различных сценариях
- Журналы сервисных событий, аудита, сканирования
- Типовая архитектура для удобного резервного копирования и восстановления

Отчеты

Информация о цели

Адрес	http://juiceshop.stands.appsecuritytesting.fun
ID цели	110
Сервер	nginx/1.22.1

Информация о сканировании

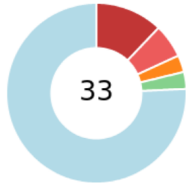
ID сканирования	432
Дата создания	14 октября 2025 г., 10:28 (UTC+0)
Дата начала	14 октября 2025 г., 10:28 (UTC+0)
Дата окончания	14 октября 2025 г., 15:52 (UTC+0)
Тип сканирования	Выборочное с использованием DirBuster

Статистика

Длительность	5 ч 23 м 56 с
Запросы	1 190 411
Среднее время ответа	42 мс
Локации	415

Уязвимости

Крайне высокая	4
Высокая	2
Средняя	1
Низкая	1
Информационная	25
Не определена	0



1. XML eXternal Entity

1.1. Общая информация

Название	XML eXternal Entity
Критичность	Крайне Высокая
Достоверность	Высокая
Модуль	xxe-franziscanner
URL	http://juiceshop.stands.appsecuritytesting.fun/file-upload

1.2. Описание

XML External Entity attack, or simply XXE attack, is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, DoS attacks, server-side request forgery, port scanning from the perspective of the machine where the parser is located, and other system impacts.

Участие в Bug Bounty

HackerOne, BIZONE

solidpoint

Найдено в продуктивной среде 100+ уязвимостей, среди них:

amazon

showmax

IBM

Alibaba

Лицензирование и развертывание

Модель лицензирования

- По количеству целей сканирования

Модель развертывания

- Облачная версия
- On-premise

Тип лицензий

- Срочные лицензии (Подписка)
- Постоянные лицензии с ежегодной поддержкой

Поставляется в составе

- SolidPoint DAST* **
- Сервис SolidLab SDP (Модуль DAST)
- Сервис SolidLab VMS (Модуль AVM)

* Сертификат соответствия ОАЦ № BY/112 02.02. TP027 036.01 02404
** Входит в реестр Российского ПО. Реестровая запись №20542 от 14.12.2023

Вопросы и ответы