SolidPoint DAST

Интеллектуальный сканер безопасности веб приложений
и сервисов

Валерий Куваев
Менеджер по продукту
Valeriy.kuvaev@solidlab.ru

Sk Сколково

solidpoint

Dynamic Analysis
for Security Testing

Основные задачи

- Обнаружение максимальной поверхности атаки
- Обнаружение критических уязвимостей в первую очередь
- Масштабирование и поддержка мультитенантности
- Интеграция в сценарии CI\CD и возможность интерактивного запуска
- Поддержка специфических технологий Заказчиков

Обнаружение поверхности атаки

- Интеллектуальный инструмент для анализа защищенности веб-приложений методами статико-динамического анализа
- Сканирование сети, выявление уязвимостей в инфраструктуре доставки приложений
- Максимальная эффективность при поиске точек ввода данных в приложение (Data Entry Points)
- Уникальные технологии статико-динамического анализа JavaScript кода[1]

[1] Статья: http://journals.tsu.ru/engine/download.php?id=223281&area=files
Выступление: https://www.youtube.com/watch?v=vG0EzOr81pE

Обнаружение поверхности атаки

Применяемые методы

- Static & Dynamic Crawling
- Dirbusting
- Статико-динамический анализ клиентского JS кода
- OpenAPI import
- FAST (интеграция с SolidWall WAF)
- Импорт HAR*
- Сканирование IP/Диапазона для выявления

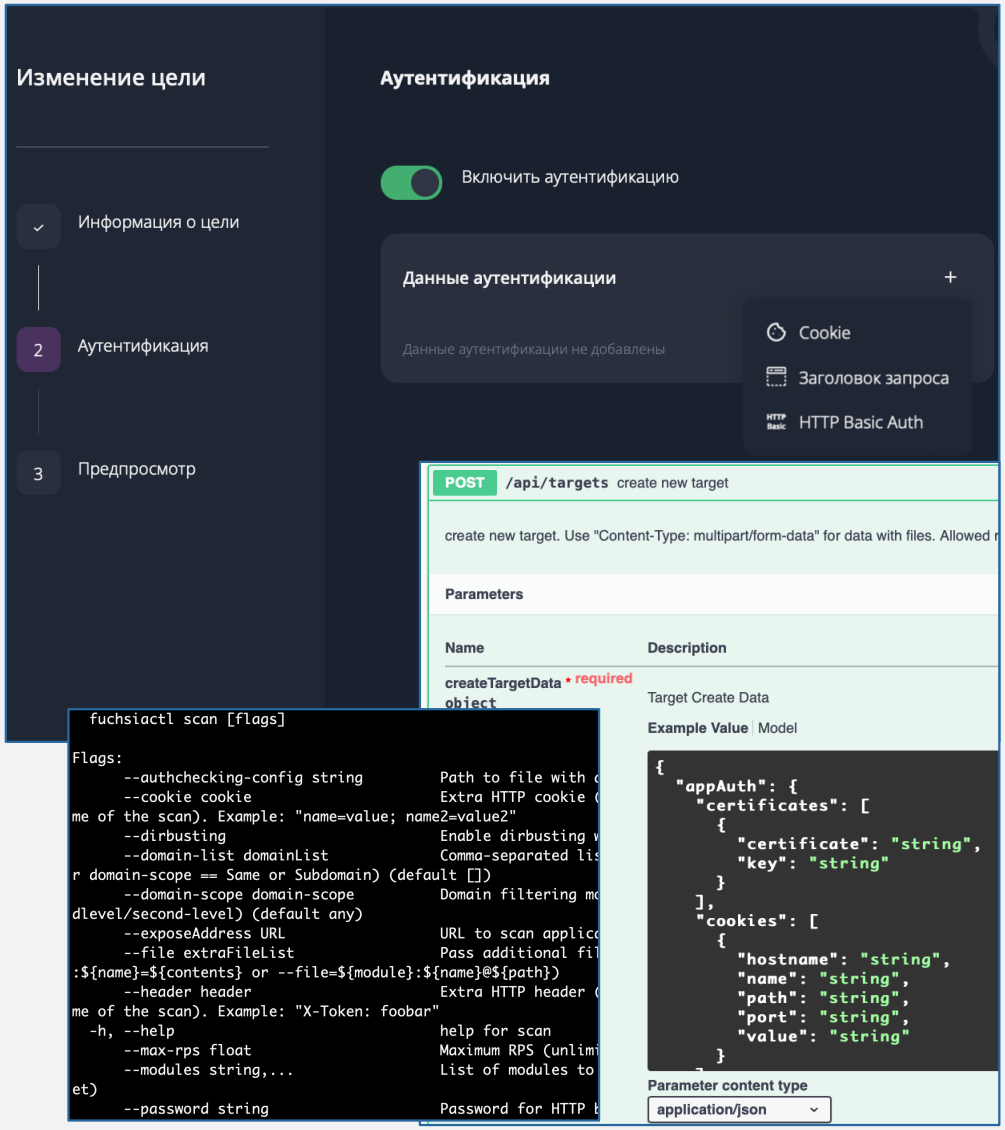
* В разработке

Сканеры безопасности

Критические риски в первую очередь

Insecure Deserialization
Reflected XSS
XXE
NoSQLi
SQLi
Path Injection*
HTTP Smuggling
File Upload
Prototype Pollution
DOM Based XSS
Пассивный сигнатурный анализ
Активный сигнатурный анализ
Перебор паролей

*В разработке



Аутентификация

Используется MITM Proxy

Технологии:

- HTTP Basic Authentication
- Header
- Cookies
- X.509

Активный рефреш сессий*

Использование сценария автоматической аутентификации*

*В разработке

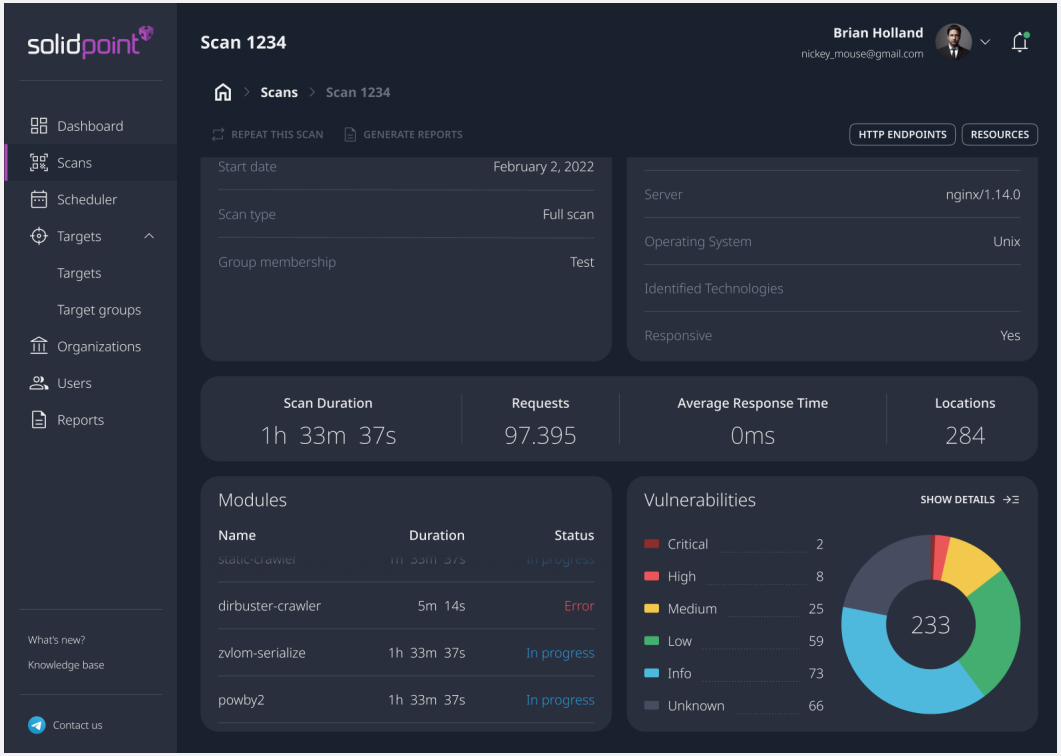
solidpoint

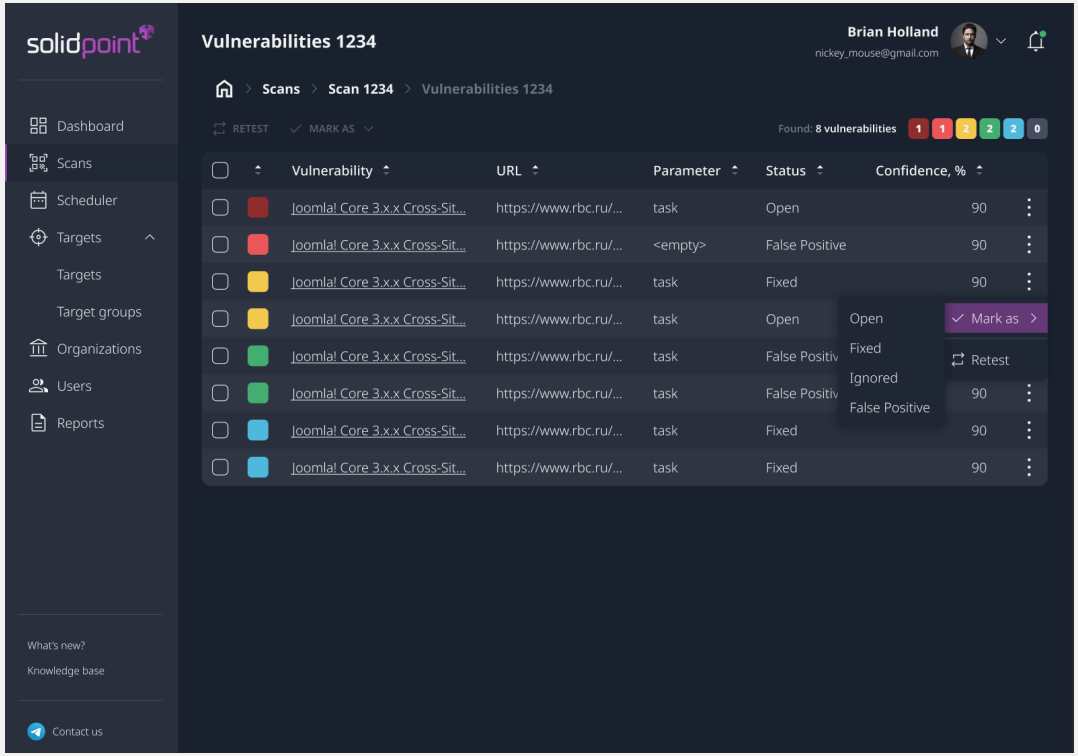
Развертывание и масштабирование

- Apt пакеты (Ubuntu\Debian)
- Docker контейнеры и Docker-compose.yml
- Kubernetes*

*В разработке

Планируется добавление результатов анализа в Q124





Демо

Q&A