МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
**Санкт-Петербургский государственный электротехнический
университет “ЛЭТИ” им. В. И. Ульянова (Ленина) (СПбГЭТУ «ЛЭТИ»)**

Кафедра: МО ЭВМ

ДОКЛАД

по учебной практике

ТЕМА: «ДИНАМИЧЕСКАЯ АВТОМАТИЗАЦИЯ СКАНИРОВАНИЯ ПЕРИМЕТРА ДЛЯ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ С ПОМОЩЬЮ OPENSOURCE ИНСТРУМЕНТОВ»

Студент гр. 8306, ФКТИ Занин Д.С.

Санкт-Петербург
2023 г.

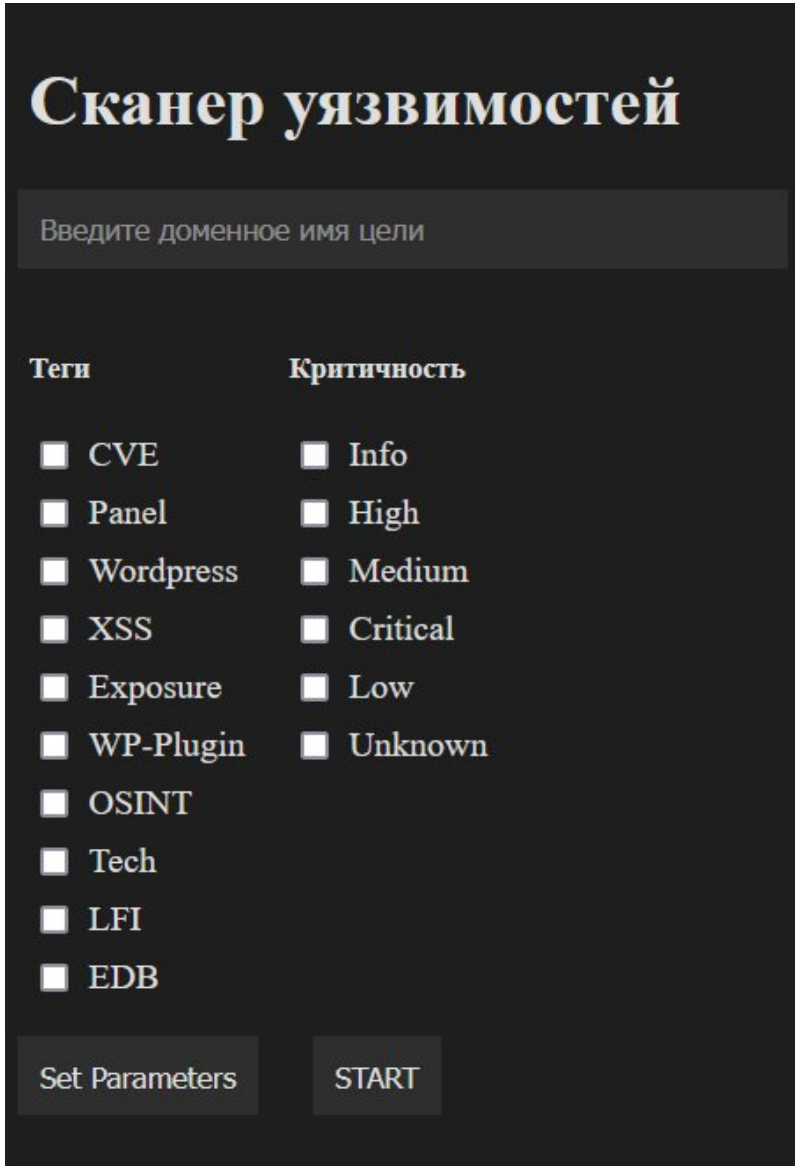
Цели практики

Создать программу которая соответствует следующим пунктам:

- Основная задача состоит в написании программного продукта, который позволяет автоматизировать сканирование сетевого периметра с использование известных OpenSource инструментов.
- Добавить динамический графический интерфейс в программу автоматизации сканирования периметра для обнаружения уязвимостей.

Графический интерфейс

- Set Parameters – Загружает выбранные параметры сканирования цели в текстовые файлы.
- START – запускает процесс сканирования в docker контейнере с использованием загруженных параметров сканирования.



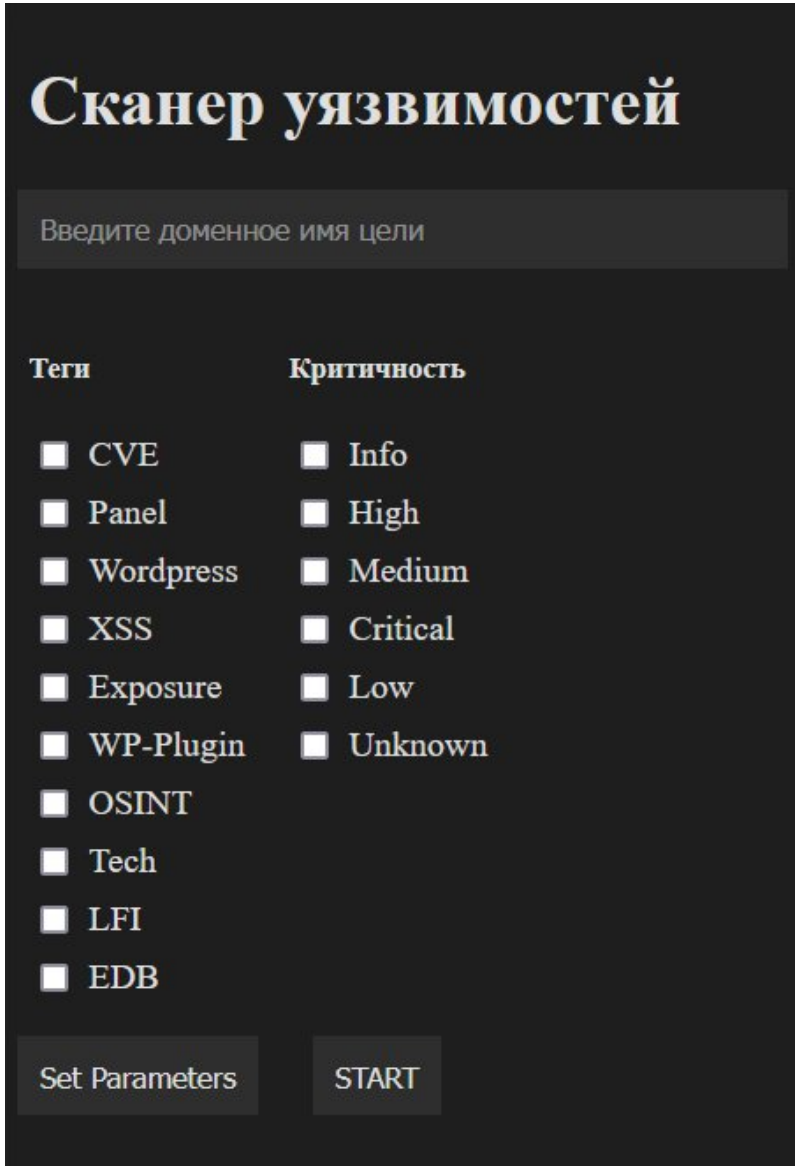
Разработка графического интерфейса.

Используемые языки:

- html
- css
- js
- python

Фреймворк:

- flask



Замена OpenSource инструмента

Замена инструмента:

- Amass – удалён
- Subfinder – добавлен

Прирост в скорости:

$$\frac{3*60+58}{7} = 34 \text{ раз}$$

Прирост в скорости сканирования цели на наличие поддоменов:

- Amass сканировал цель за **3 мин. 58 сек**. с использованием passive.
- Subfinder сканировал цель за **6 - 7 сек.**

Прирост в скорости сканирования составил 3 мин. 51 сек.

Спасибо за внимание !

Контакты: etu.zanin@yandex.ru

Ссылка на репозиторий GitHub с проектом:

https://github.com/JackoPrograms/automated_scanning.git