**Задание**

Установите на свой компьютер инструмент semgrep ([https://semgrep.dev](https://semgrep.dev/)) для анализа исходного кода на наличие уязвимостей. Напишите собственные правила для поиска одного из класса уязвимостей по OWASP Top 10 (<https://owasp.org/www-project-top-ten/>). Чем больше вы покроете вариантов реализации уязвимости в коде, тем лучше. На одном из языков программирования напишите программу, которая в качестве входных параметров будет принимать путь к директории с исходным кодом, а также имя выходного файла, в который запишется результат сканирования. Программа должна запускать инструмент semgrep, дожидаться завершения сканирования, после чего записывать результат сканирования в выходной файл в определенном формате.

Формат выходного файла:

<порядковый номер уязвимости>. <путь к файлу с уязвимостью> <номер строки, в которой была найдена уязвимость> <номер столбца, в котором была найдена уязвимость>

Пример:

**report.txt**

1. ./src/secrets.py 3 1

2. ./config/settings.yaml 5 4