ОТЧЕТ

**Практическое задание. Анализ защищённости веб-приложений**

**Описание Приложения**

OWASP Juice Shop, современное и сложное небезопасное веб-приложение.

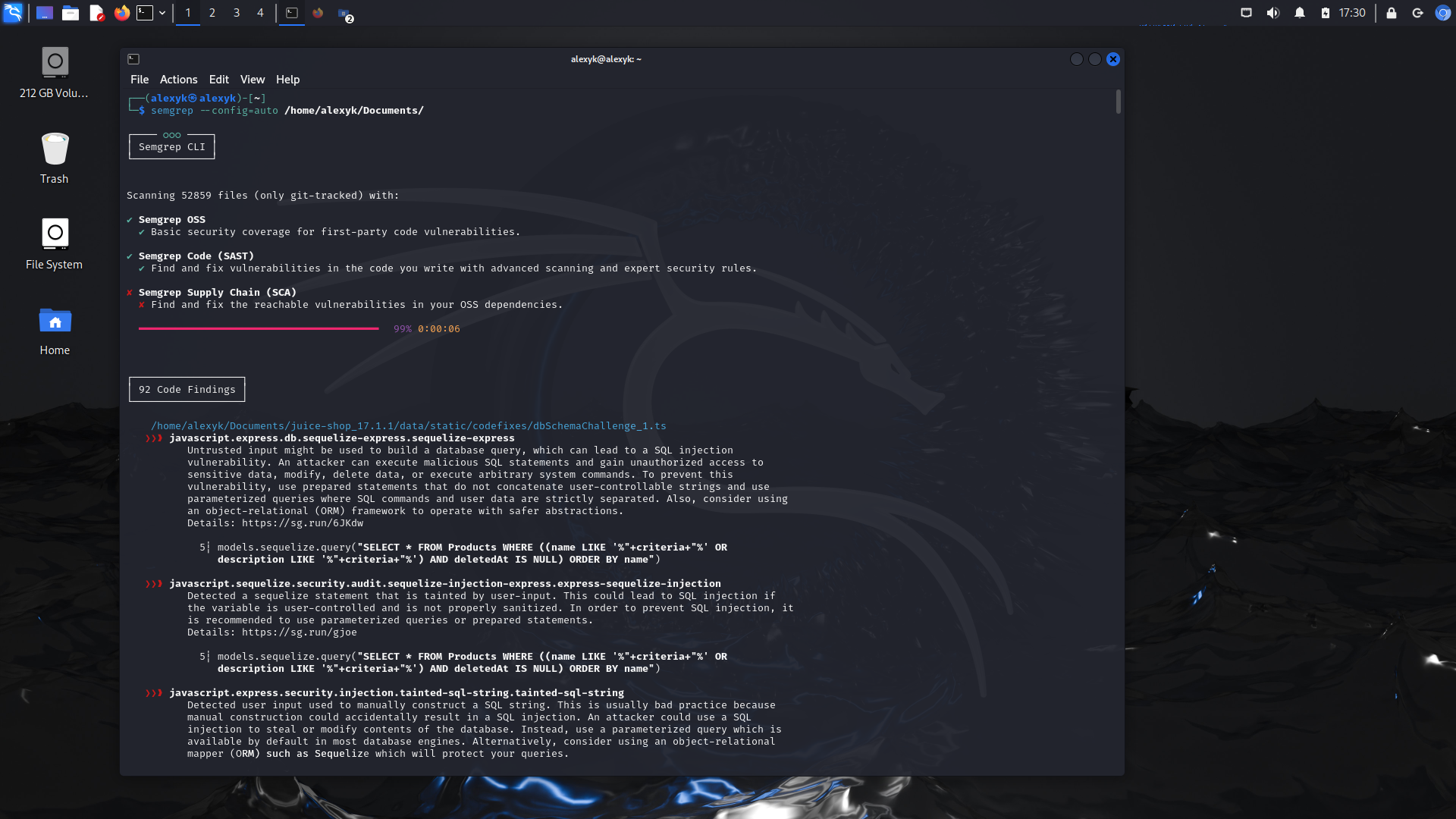
Используется на тренингах по безопасности, демонстрациях осведомленности, CTF и в качестве подопытного кролика для инструментов безопасности.

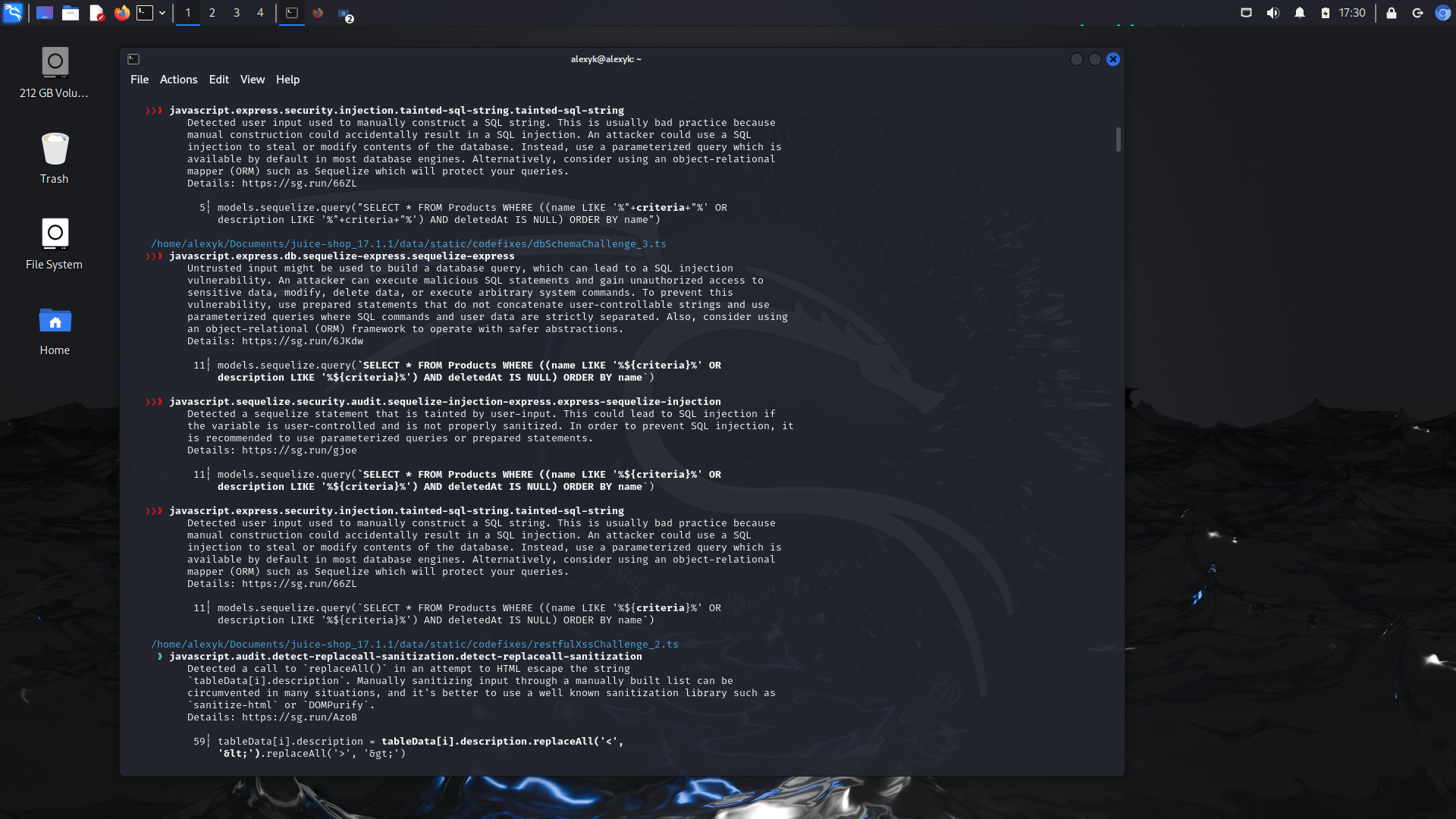
Juice Shop охватывает уязвимости из всей десятки OWASP, а также многие другие недостатки безопасности, обнаруженные в реальных приложениях.

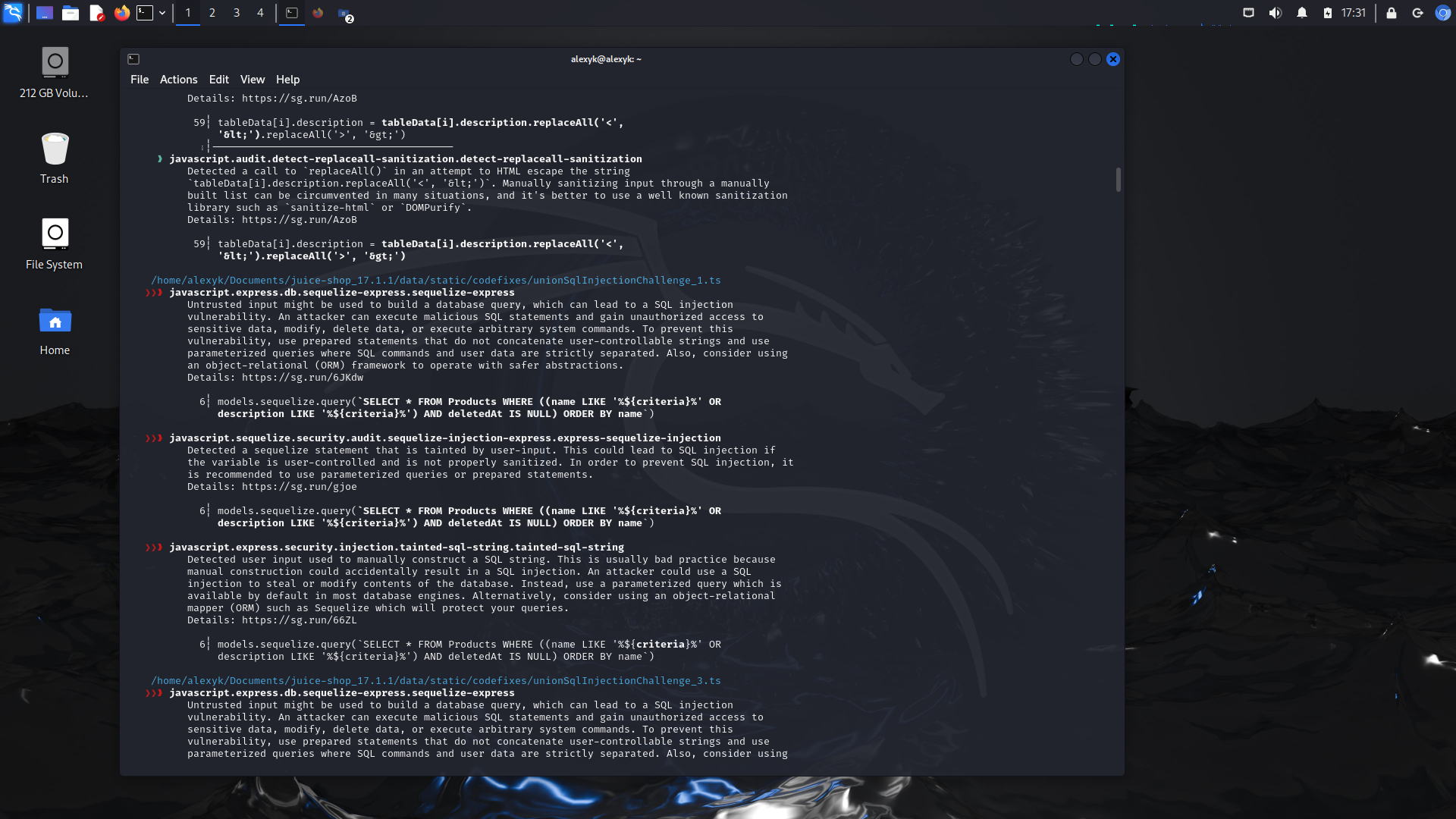
Juice Shop написан на Node.js, Express и Angular. Это было первое приложение, написанное полностью на JavaScript.

Приложение содержит огромное количество хакерских задач разной сложности, в которых пользователю предлагается использовать уязвимости, которые лежат в основе.

Результаты Статического Анализа







Все результаты сканирования на уязвимости расположены в файле: **semgrep res juice.txt**

**Дополнительно:** Проведен статический анализ с помощью Приложения [**NodeJSScan**](https://github.com/ajinabraham/NodeJsScan) ( **GIT** <https://github.com/omerlh/juice-shop-security-tests?tab=readme-ov-file>)

Результаты сканирования расположены в файле: **nodejsscan v4.8 - Scan Results.html**,

в нем также указаны уязвимости найденные в Приложении Juice Shop с указанием уязвимостей по CWE и MITRE

**Демонстрация эксплуатации трёх уязвимостей из OWASP Top-10**

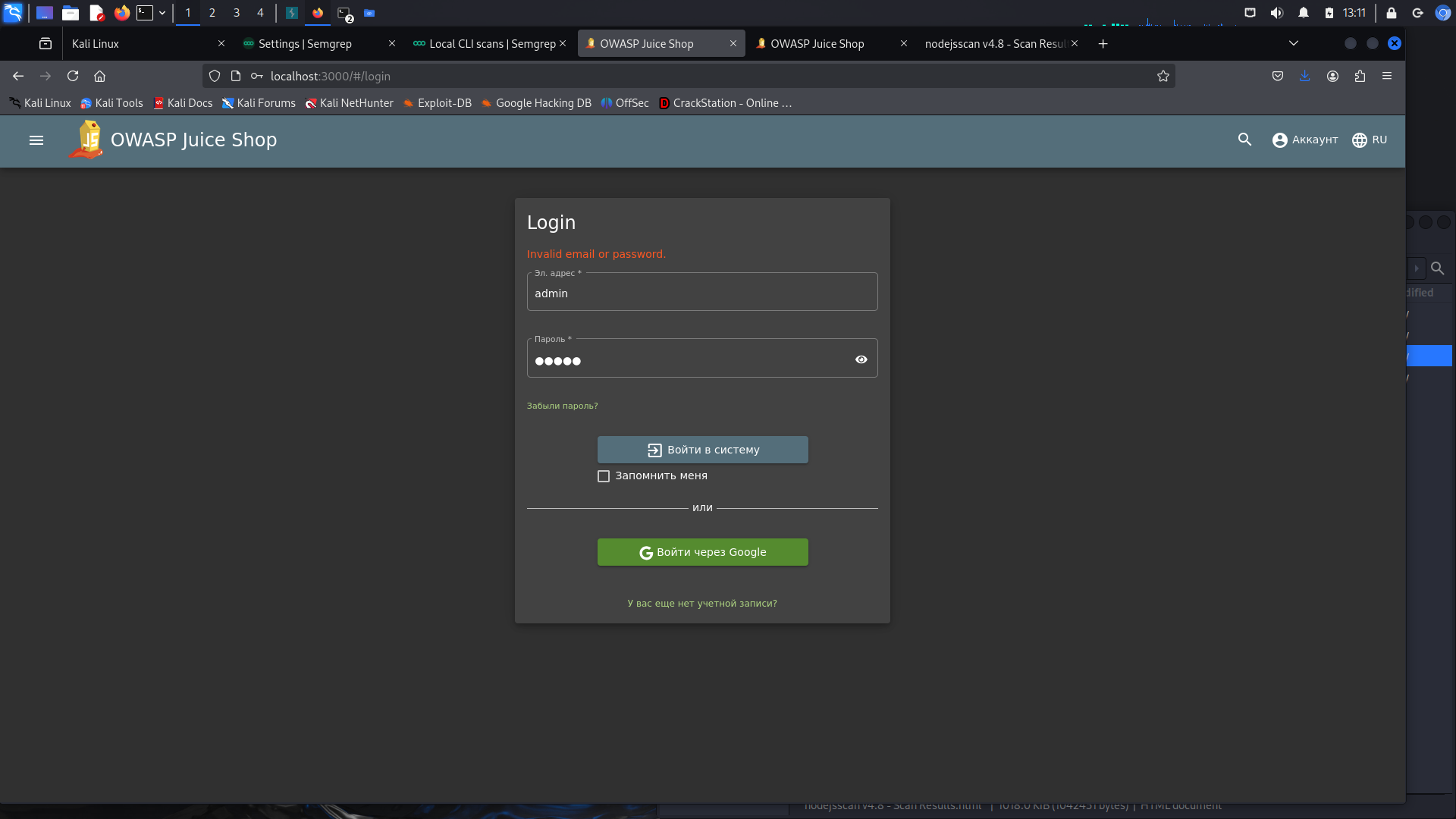
CWE-23, CWE-327, CWE-20, CWE-94, CWE-347

Login Admin (Injection)

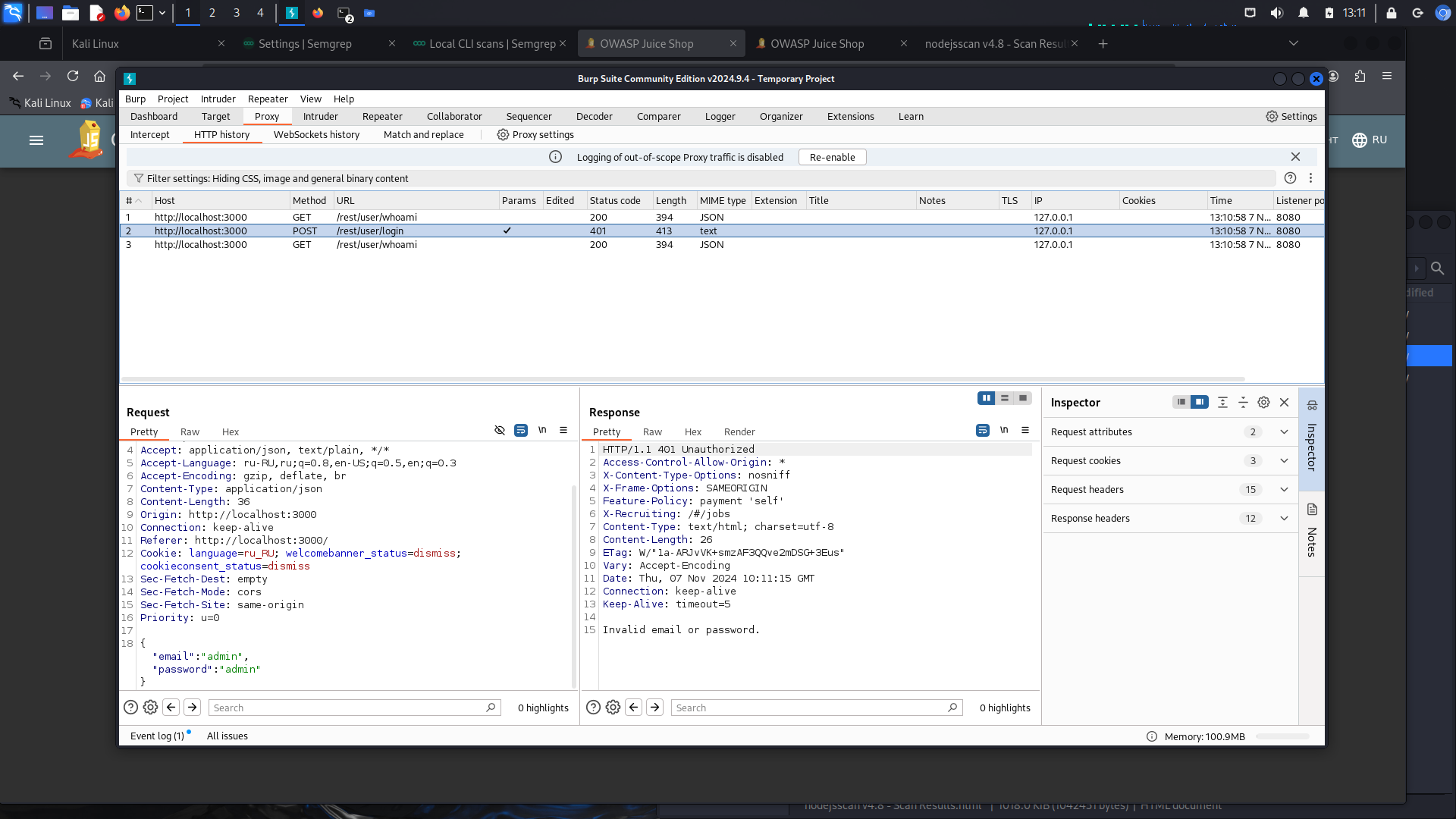
Методы обнаружения(противодействия):

Автоматизированный статический анализ

Вводим запрос на авторизацию



Перехват пакета авторизации в Burp Suite

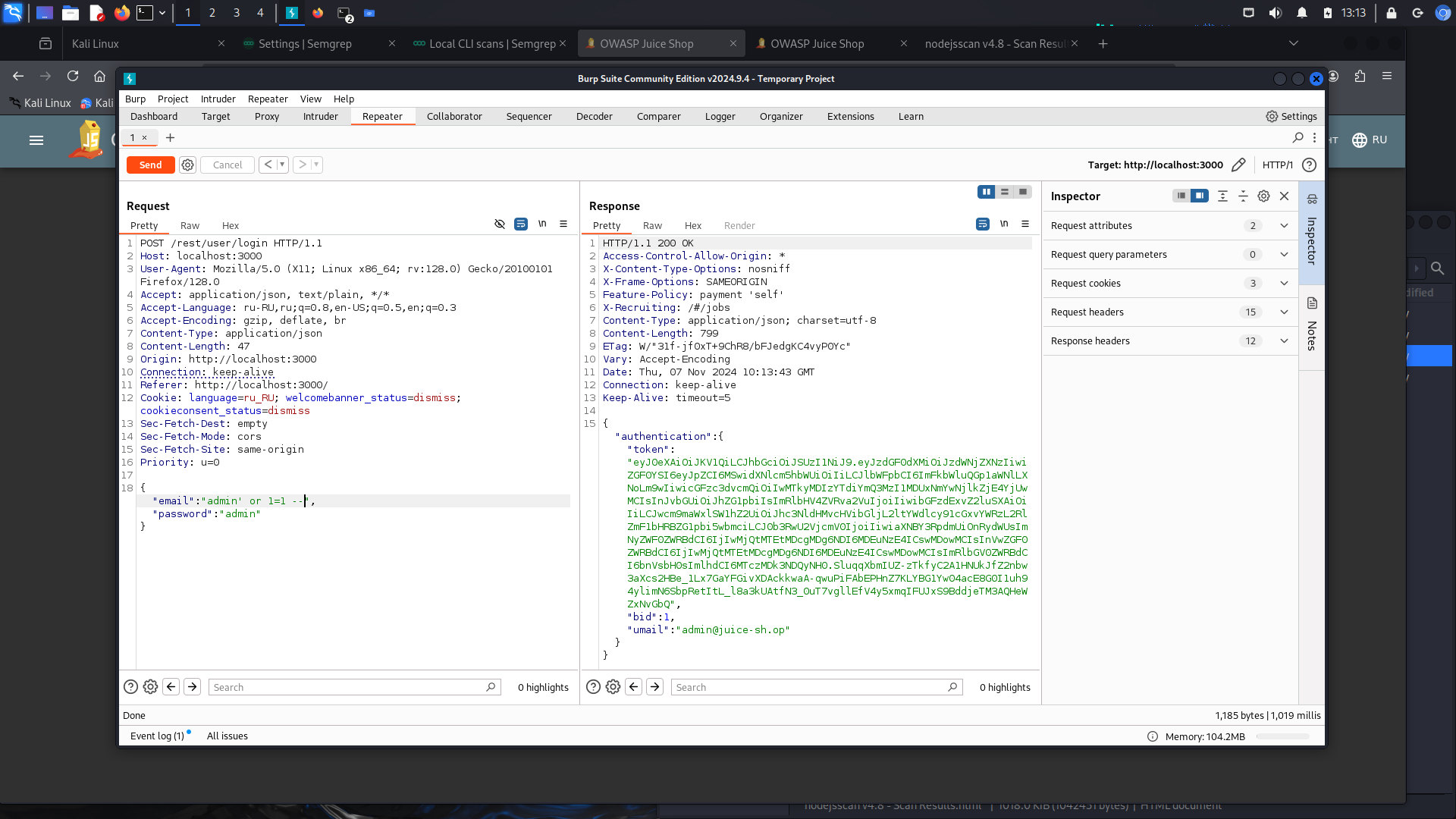




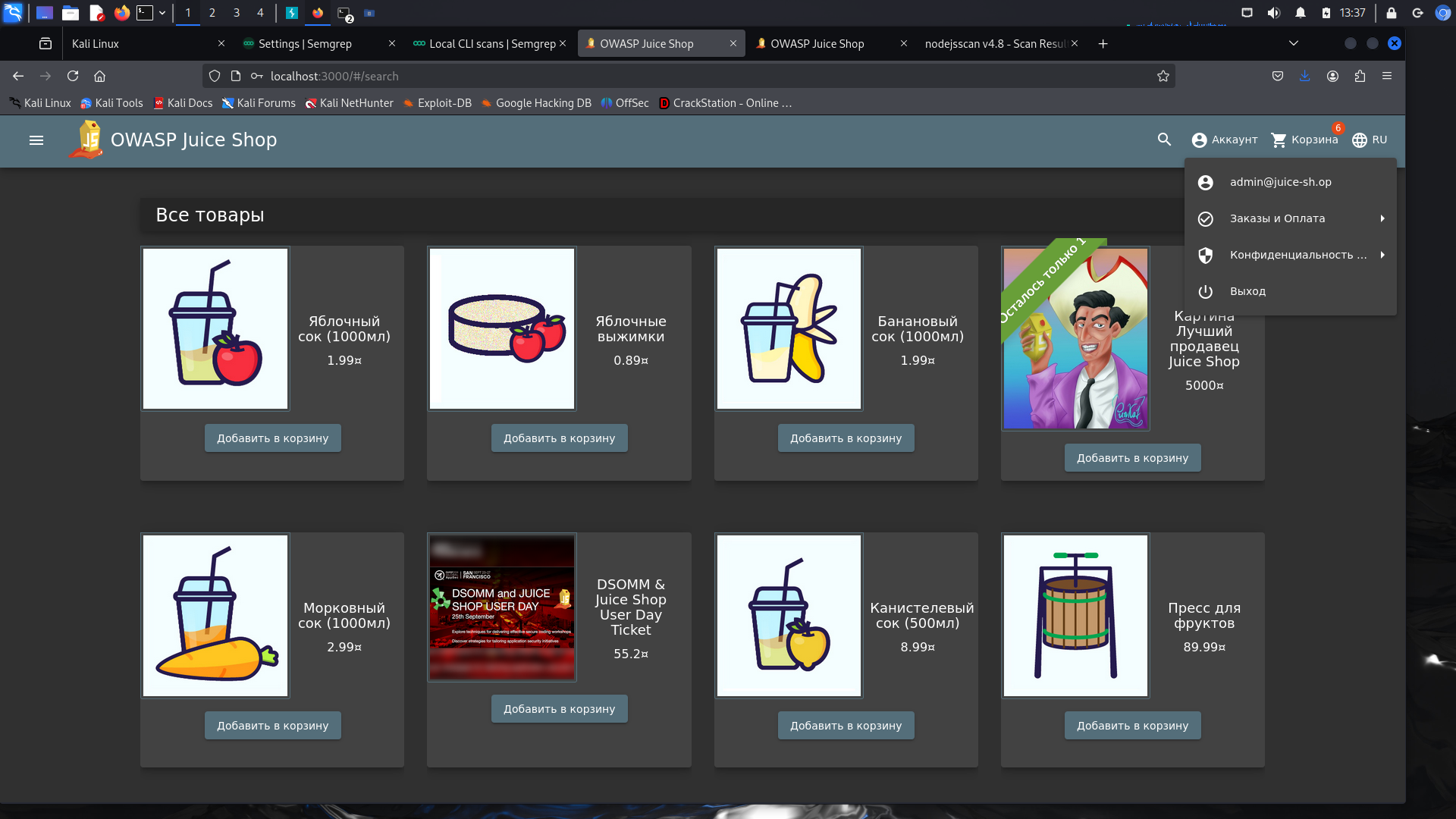
Отправка запроса с апострофом анализ реагирования



Отправка запроса с инъекцией, получение адреса администратора и вход



Проверка входа



Admin Registration (Improper Input Validation)

Методы обнаружения(противодействия):

Автоматизированный статический анализ

Ручной статический анализ

Фаззинг

Автоматизированный статический анализ — двоичный или байт-код

Ручной статический анализ — двоичный или байт-код

Динамический анализ с автоматизированной интерпретацией результатов

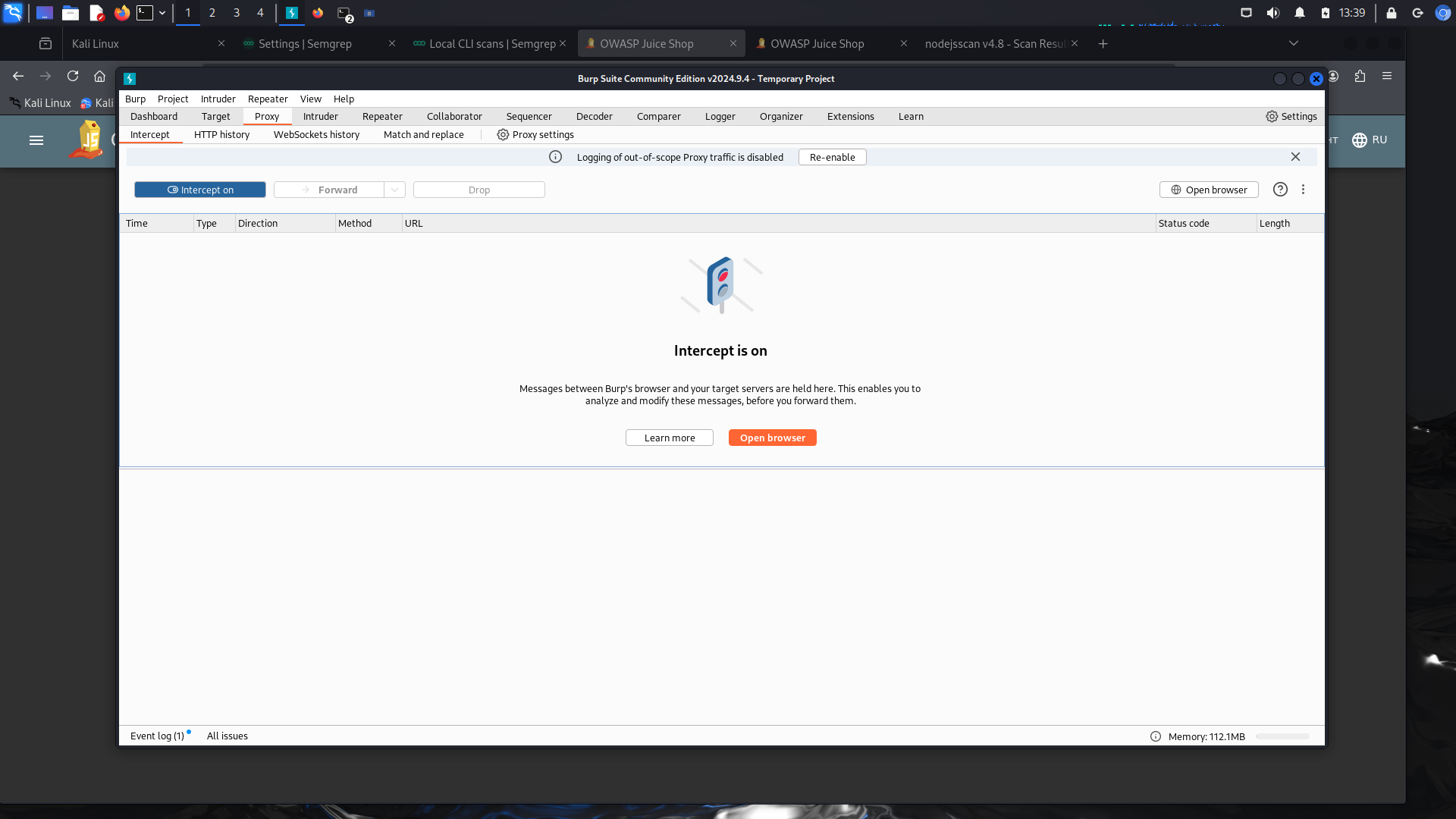
Динамический анализ с ручной интерпретацией результатов

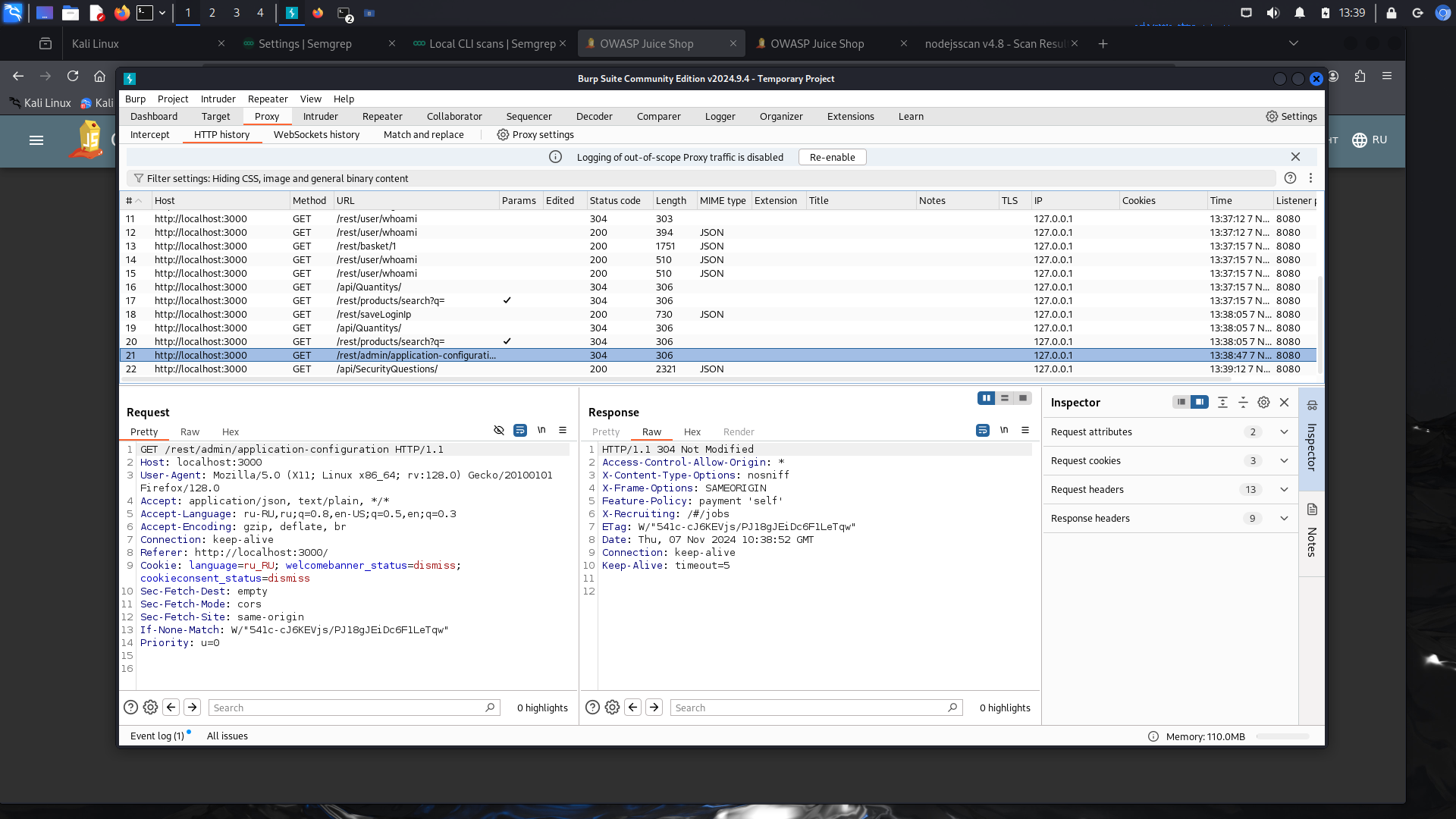
Ручной статический анализ - Исходный код

Автоматизированный статический анализ - Исходный код

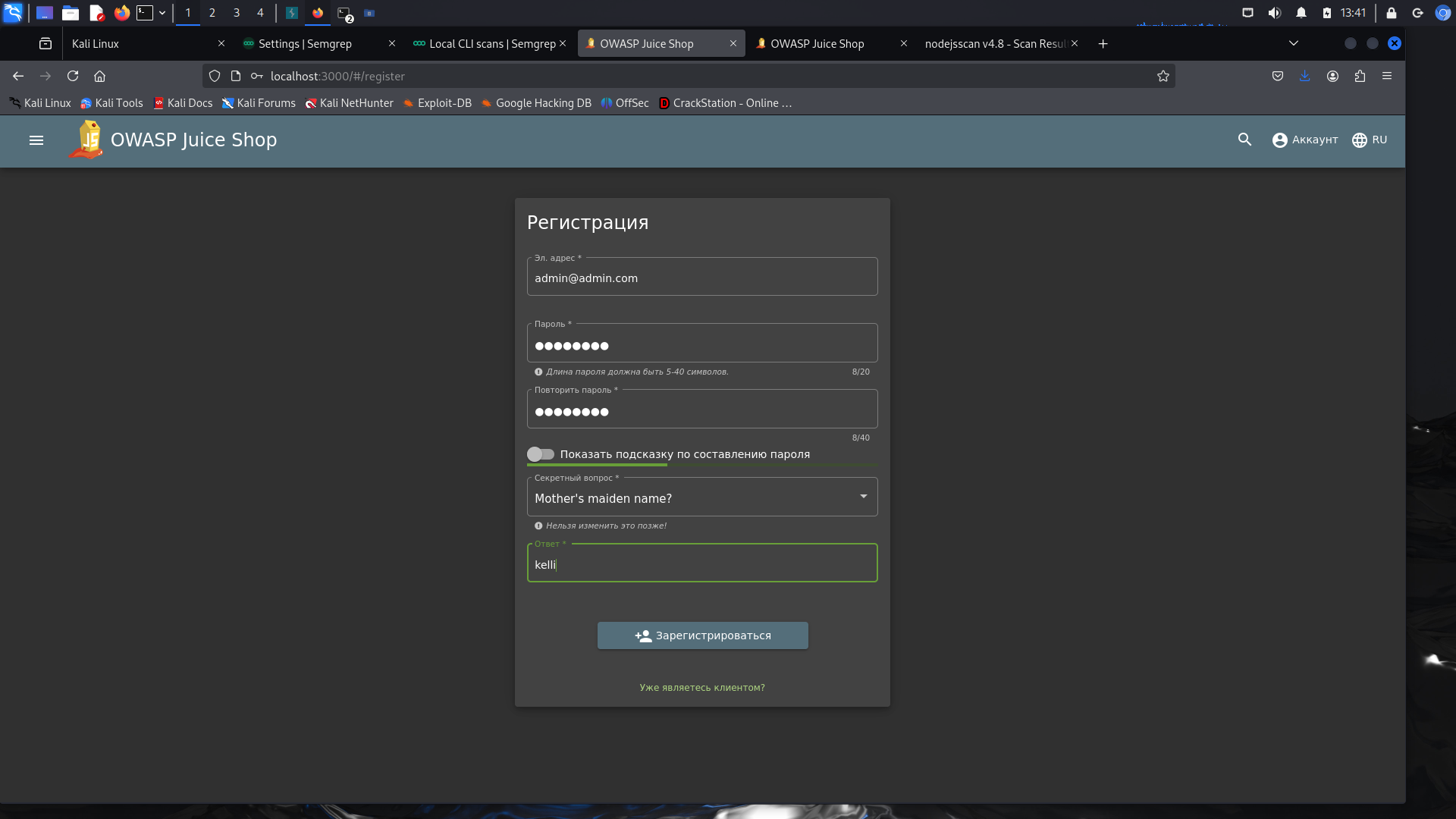
Обзор архитектуры или дизайна

Включение перехвата Burp Suite

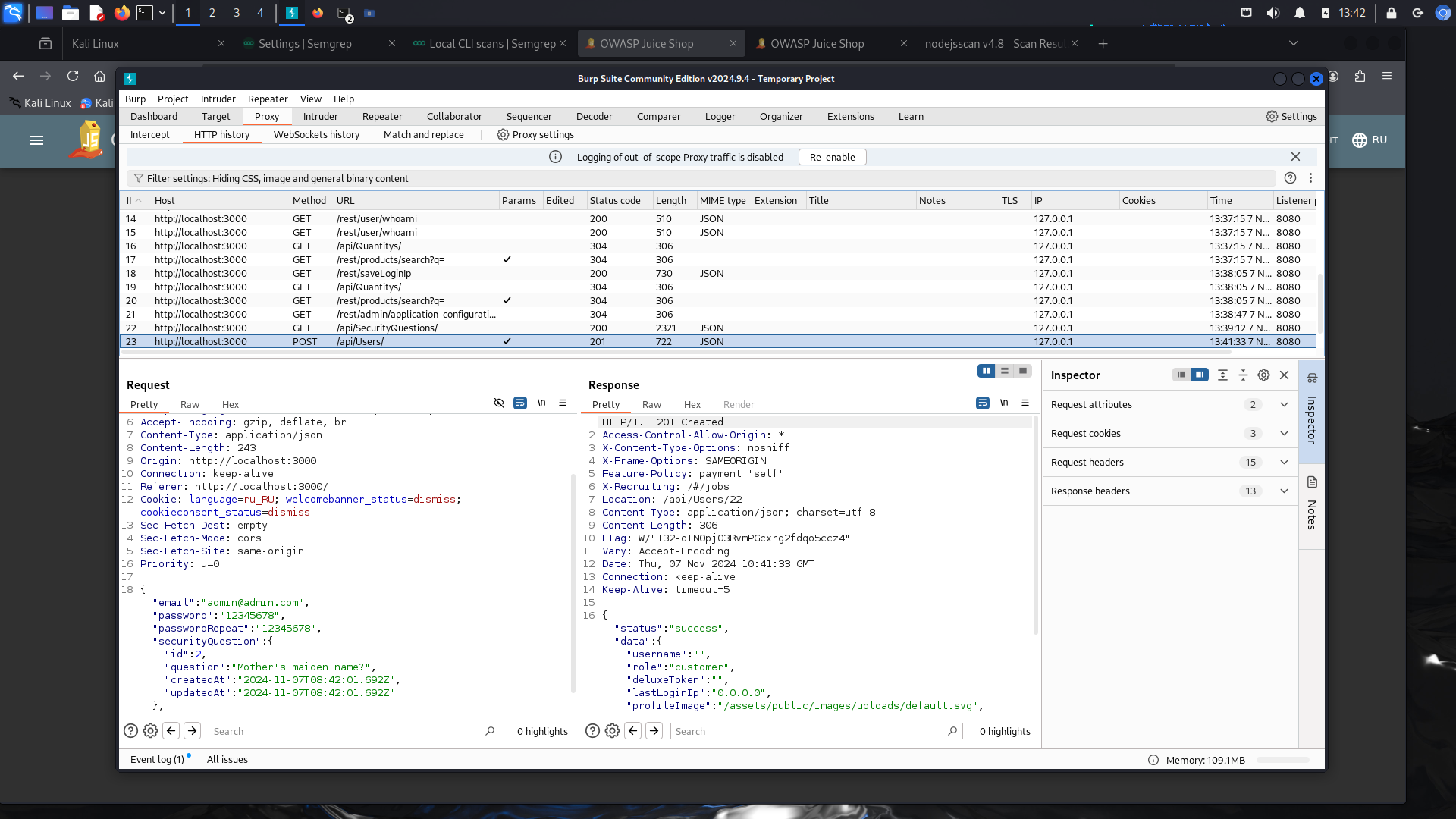


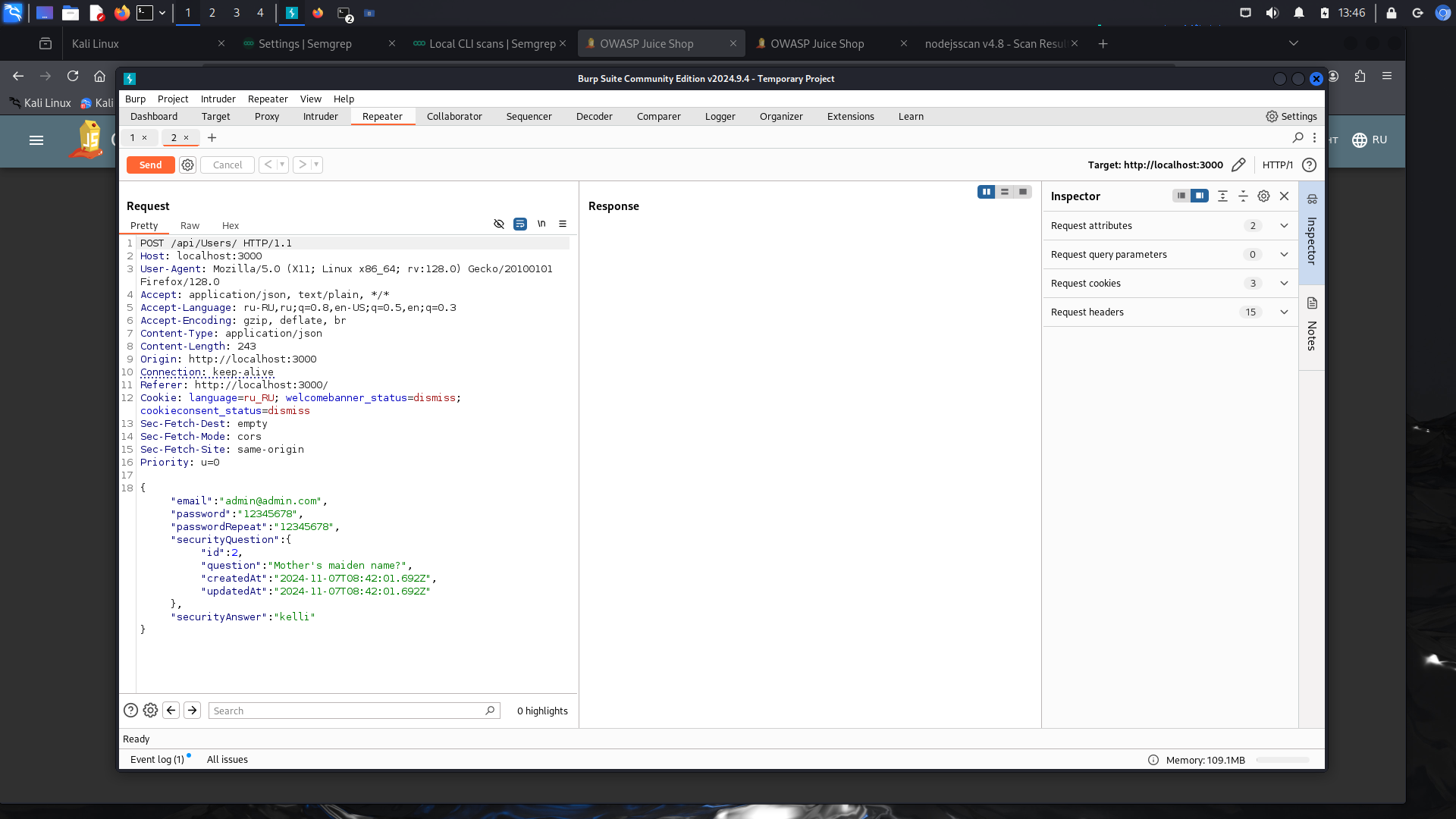


Регистрация нового пользователя с перспективой админа



Перехват пакета с запросом на регистрацию нового пользователя

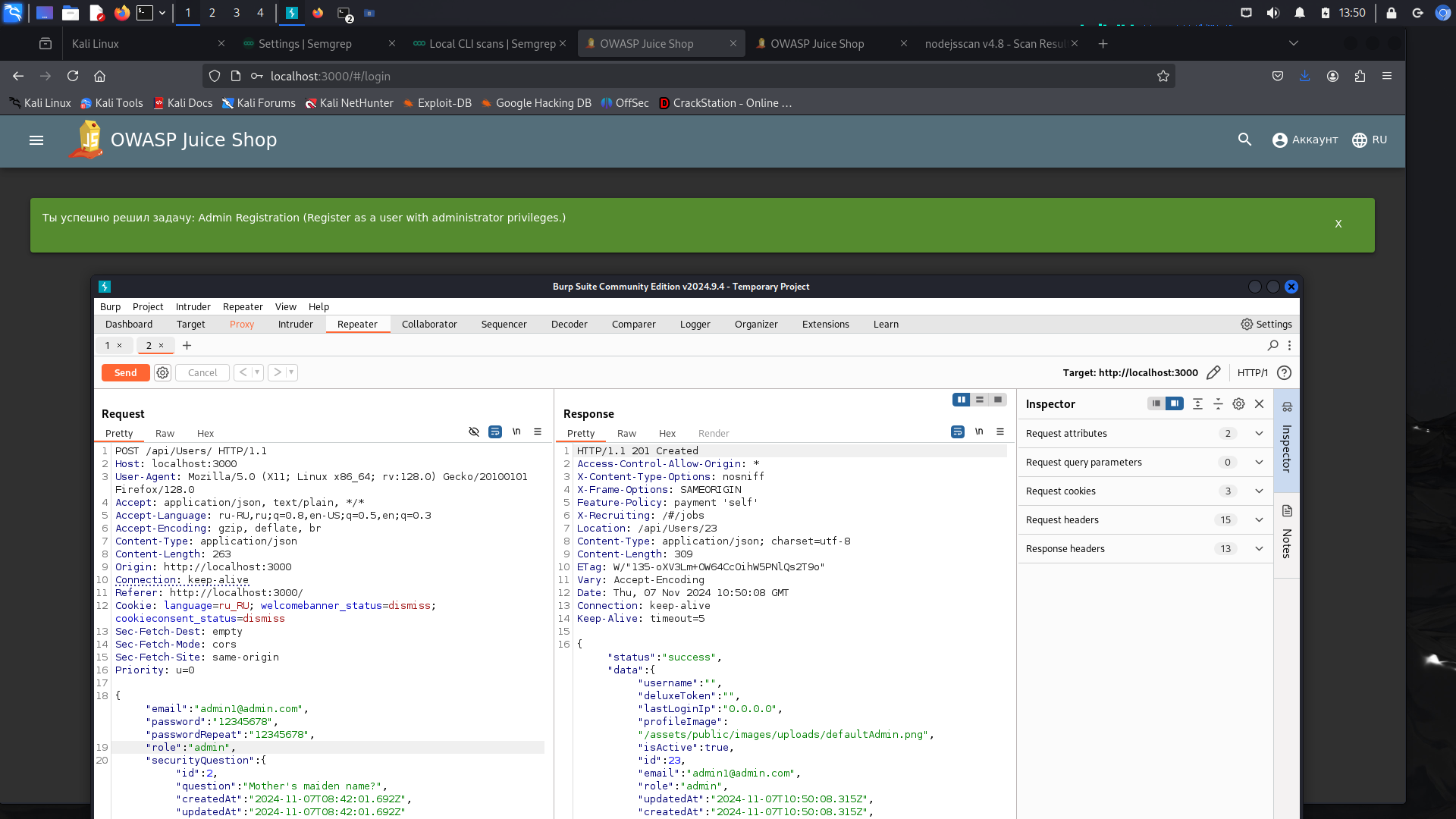




Добавление в запрос строки роли нового пользователя и изменение имени пользователя



Отправление запроса и прописывание роли администратора в ответе роль прописана

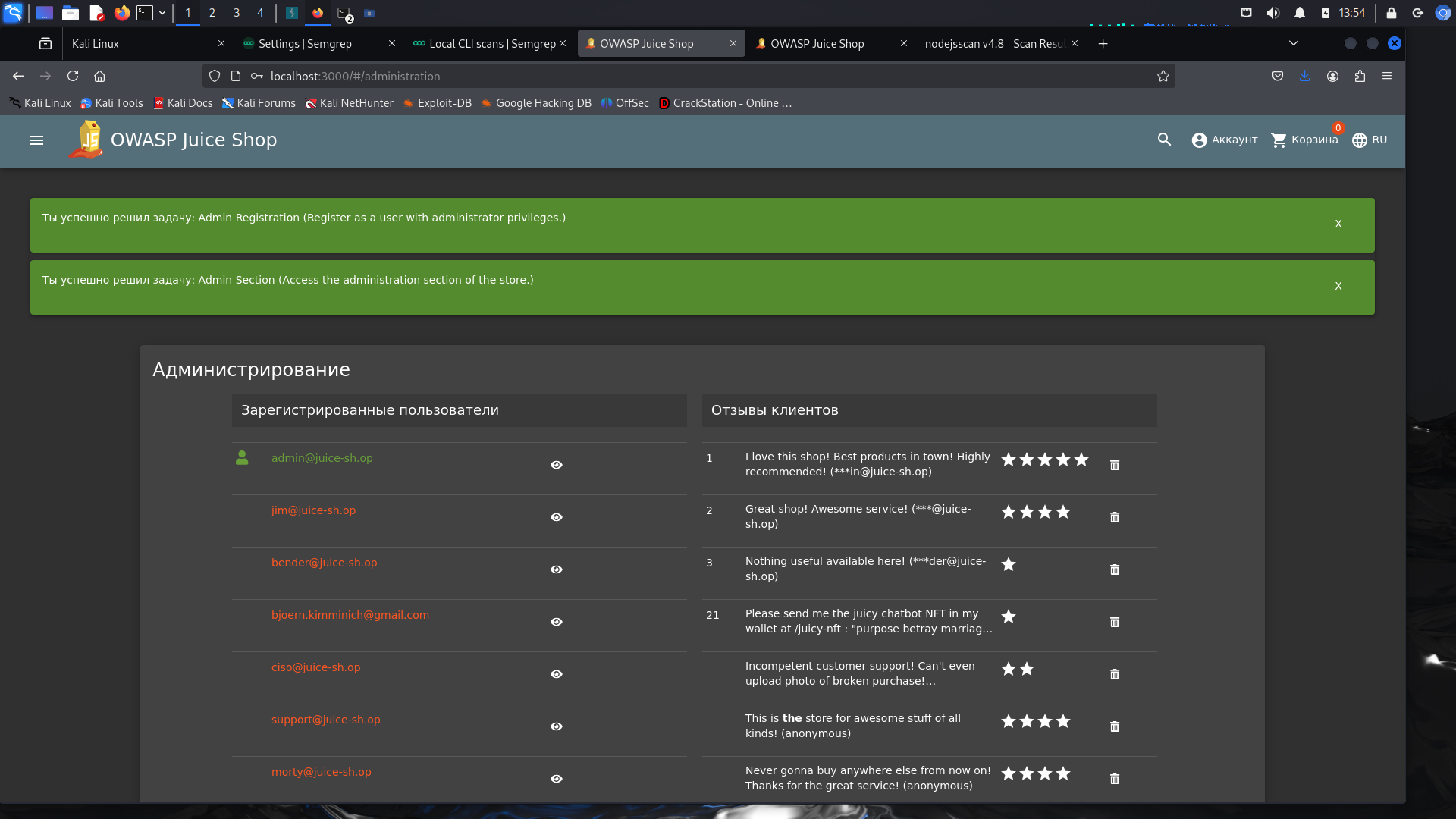


вход под пользователем с ролью администратора



+ Admin Section (Broken Access Control)

Просмотор административных функций

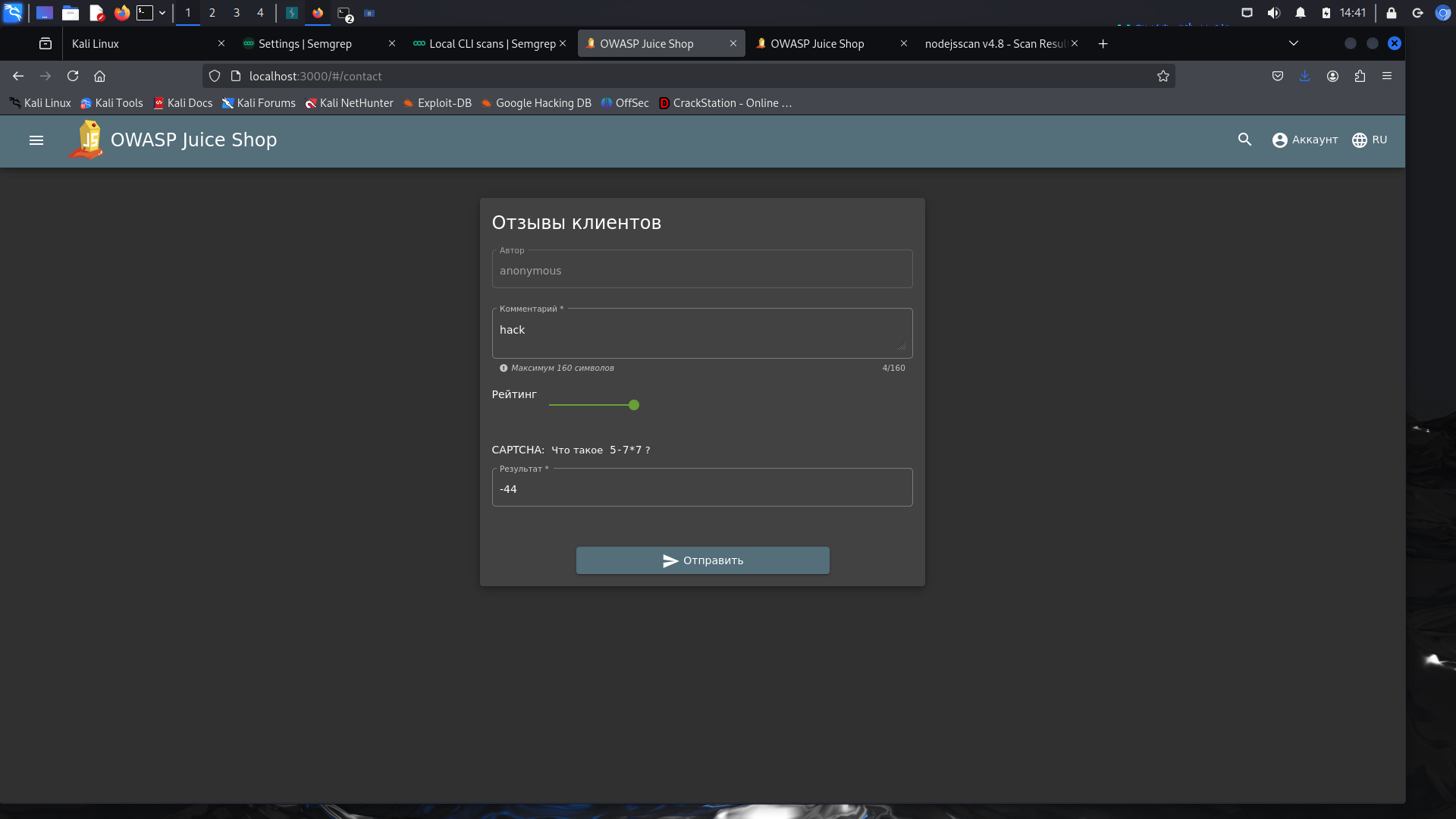


Weird Crypo (Cryptographic)

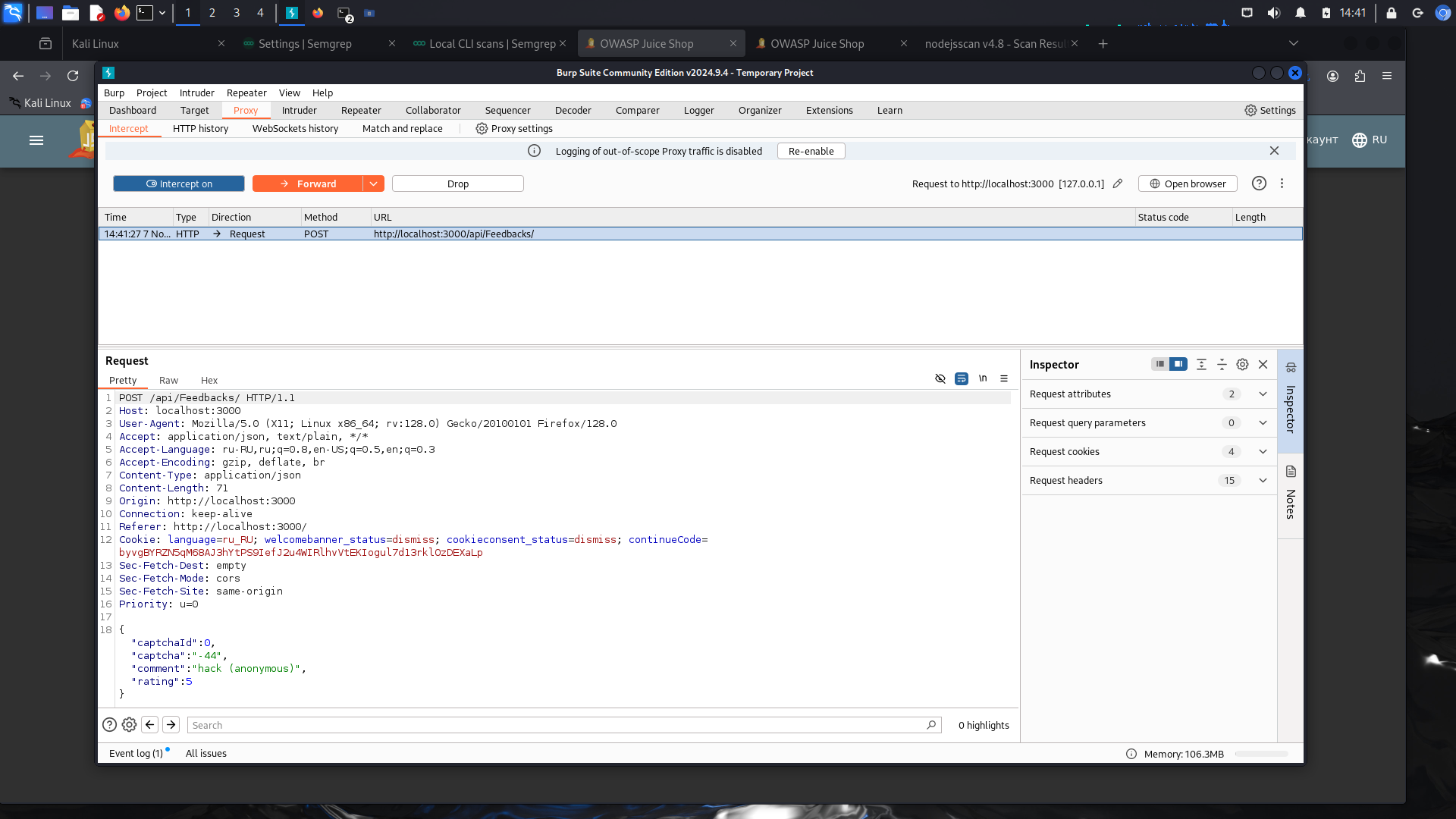
Методы обнаружения(противодействия):

Автоматизированный статический анализ

написание отзывов клиента



Перехват пакета запроса с отзывом клиента



внесение функции в комментарий, отправка пакета

