Список OWASP Top 10

Список включает следующее:

- Инъекция
- Нарушенная аутентификация
- Раскрытие чувствительных данных
- Внешние сущности XML (XXE)
- Нарушенный контроль доступа
- Неправильная конфигурация системы безопасности
- Межсайтовый скриптинг (XSS)
- Небезопасная десериализация
- Использование компонентов с известными уязвимостями
- Недостаточное протоколирование и мониторинг

Для прохождения практического задания, выберем первые три уязвимости OWASP
- Инъекция
- Нарушенная аутентификация
- Раскрытие чувствительных данных

Введение — описание приложения juice-shop

Web-приложение juice-shop - это проект с открытым исходным кодом. В приложении огромное количество предполагаемых уязвимостей безопасности. Его цель повешение осведомлённости, обучения, демонстрации рисков безопасности в современных условиях. Это полигон для тренировки и пентеста.

Рекомендации по устранению уязвимостей

Наименование уязвимости	Рекомендации по устранению уязвимостей
Инъекция	- Использование подготовленных инстансов с параметризированными запросами - Использование хранимых процедур - Осуществление проверок и насацию ввода - Экранировать все вводимые пользователем данные
Нарушение аутентификации	- Ввести таум-аут после трёх неудачных попыток ввода логина или пароля. - Использовать при создании пользователей сильный пароли (не менее 8-ми символов с разными регистрами и спец.символами) - Использовать систему многофакторной аутентификации
Раскрытие чувствительных данных	- Зашифровывать конфиденциальные данные.

Описание эксплуатации: что нужно сделать, чтобы воспроизвести уязвимость

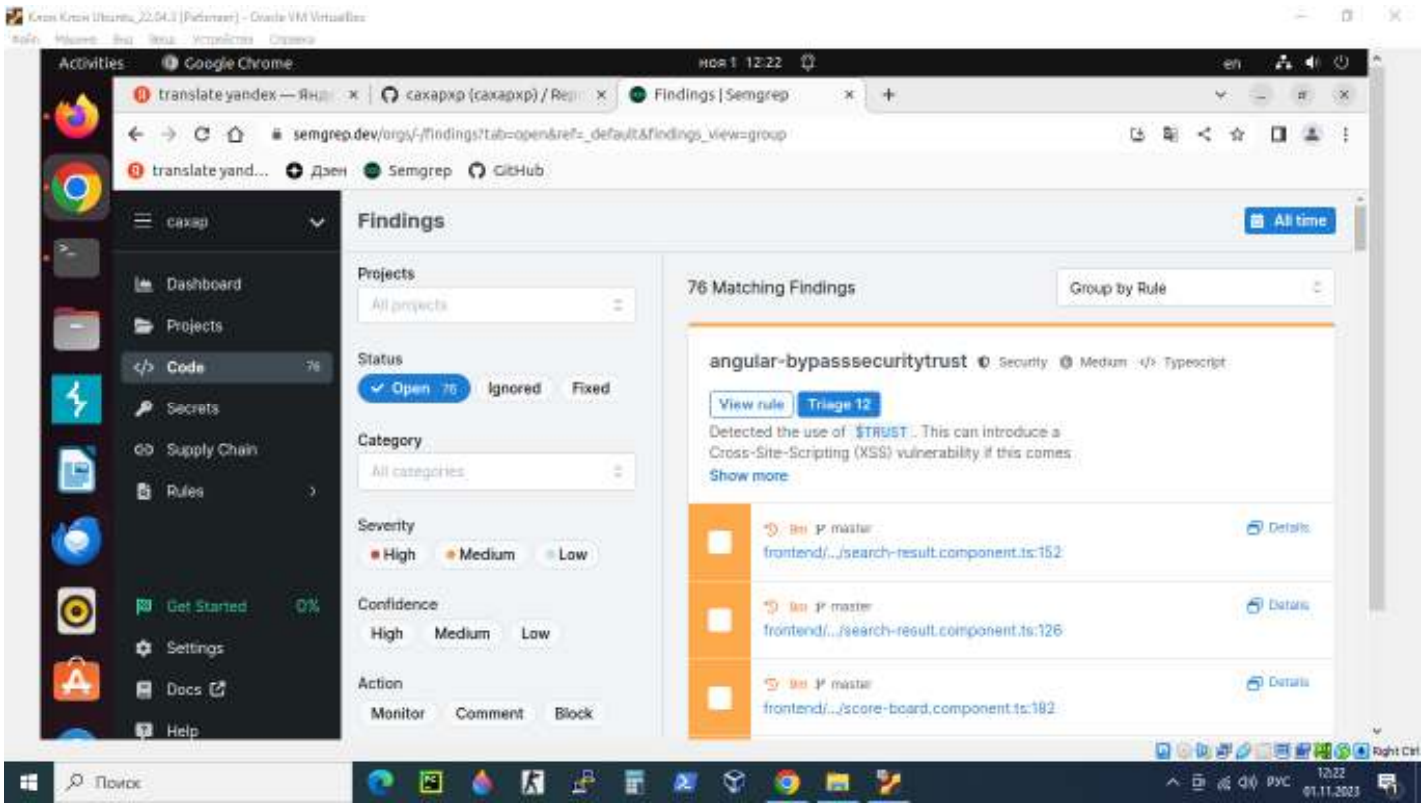
1. **Инъекция**. В браузере зайти в приложение на страницу, где перечислены товары. Сверху справа нажать на значок «Поиск» и ввести любой запрос, например «банан». Заходим в приложение Burp Suite на вкладку Proxy => HTTP history и видим наш запрос

/rest/products/search?q= Нажимаем на наш запрос и в нижней части экрана, во вкладке Request => Raw видим наш развёрнутый запрос. Нажимаем правой кнопкой мыши в текст развёрнутого запроса и выбираем Send to Repeater. Далее заходим на вкладку Repeater=>Request=>Raw и в левом окне видим наш развёрнутый запрос. В этот запрос вписываем /rest/products/search?q=banana'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite_master-- Далее сверху слева жмём на кнопку Send и в левом окне видим результат sql-инъекции

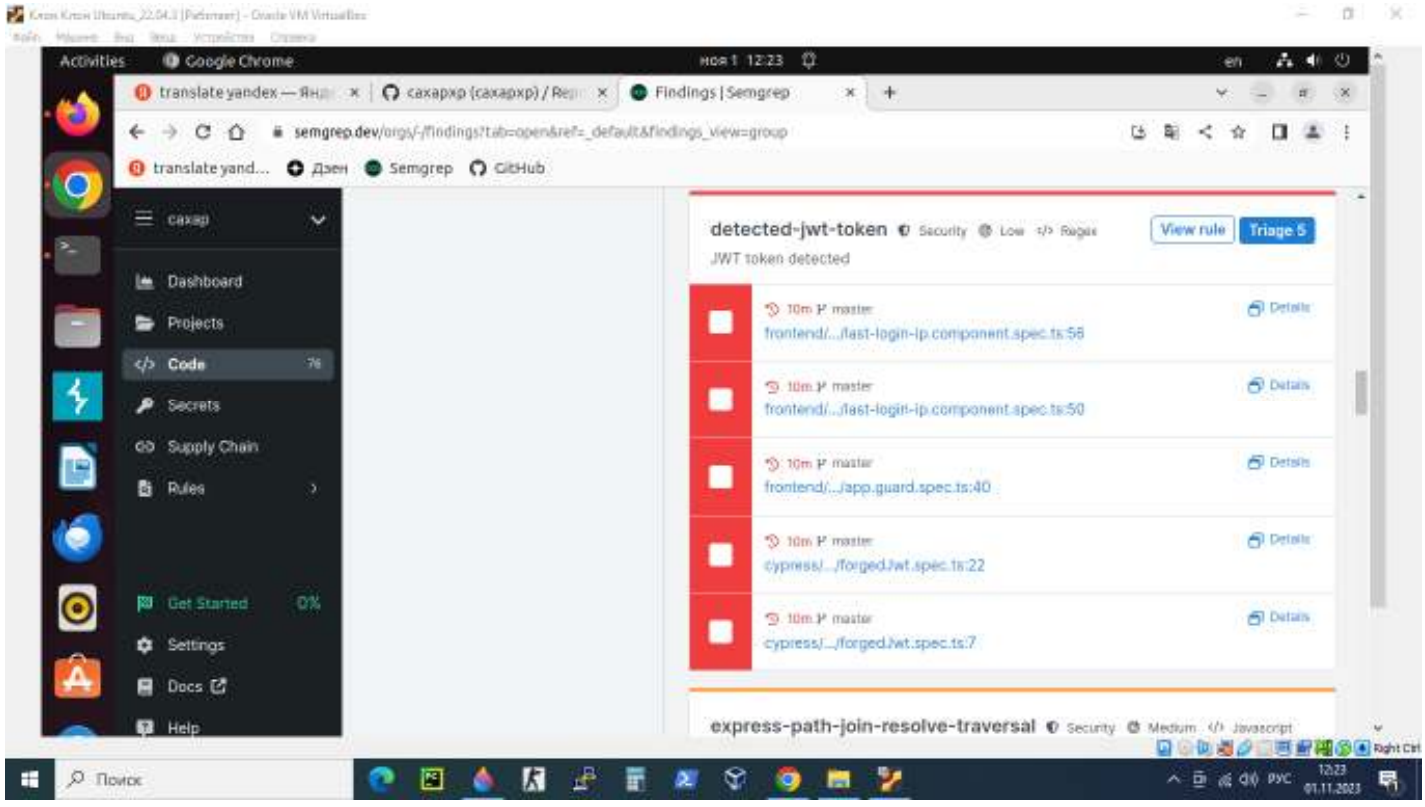
2. **Нарушение аутентификации**. Браузере в приложении можно легко узнать логин пользователей (например их емеилы указаны на товарах в комментариях). Узнав логин, например админа, заходим авторизироваться в приложении. В графе логин – вводим admin@juice-sh.op а в графе пароль – любое значение, например «12345». Заходим в приложение Burp Suite на вкладку Proxy => HTTP history и видим наш запрос /rest/user/login. Нажимаем на наш запрос и в нижней части экрана, во вкладке Request => Raw видим наш развёрнутый запрос. Нажимаем правой кнопкой мыши в текст развёрнутого запроса и выбираем Send to Intruder. Заходим во вкладку Intruder => Positions и снизу видим наш запрос и последней строчкой вводимые данные {"email":"admin@juice-sh.op","password":"12345"}. Выделяем текст (пароль) 12345 и справа нажимаем на кнопку «Add $». Сверху заходим на вкладку Payloads. В окошке Payload settings [Simple list] можно написать варианты паролей, для перебора. Либо, если на компьютере есть текстовый файл с множеством вариантов слов (варианты паролей), можно чтобы данные для подбора брались из этого файла, нажав на кнопку Load и указав до него путь. Далее нажать на кнопку Start attack сверху справа. Откроется окно с перебором паролей. Когда закончится операция перебора паролей. В графе Status code будут ошибки 401 (пароли которые не подходят), и статус 200 (пароли который подходят).

3. **Раскрытие чувствительных данных.** В браузере заходим во вкладку «О нас». На страничке присутствует текст «Корпоративная история и политика», в тексте есть гиперссылка на скачивание текстового файла, нажимаем на гиперссылку. Заходим в приложение Burp Suite на вкладку Proxy => HTTP history и видим наш запрос /ftp/legal.md. Нажимаем на наш запрос и в нижней части экрана, во вкладке Request => Raw видим наш развёрнутый запрос. Нажимаем правой кнопкой мыши в текст развёрнутого запроса и выбираем Send to Repeater. Далее заходим на вкладку Repeater=>Request=>Raw и в левом окне видим наш развёрнутый запрос GET /ftp/legal.md HTTP/1.1. Мы видим, что есть некая директория ftp из которой нам предлагается скачать файл. Исправляем запрос на GET /ftp HTTP/1.1 и нажимаем кнопку Send. В правой части экрана, Response, мы видим результат запроса, нам выдало директорию ftp и её содержимое. Пробуем скачать конфиденциальный файл acquisitions.md вставив в гет-запрос GET /ftp/acquisitions.md HTTP/1.1. В правой части экрана, Response, мы видим результат запроса, текст этого конфиденциального файла.

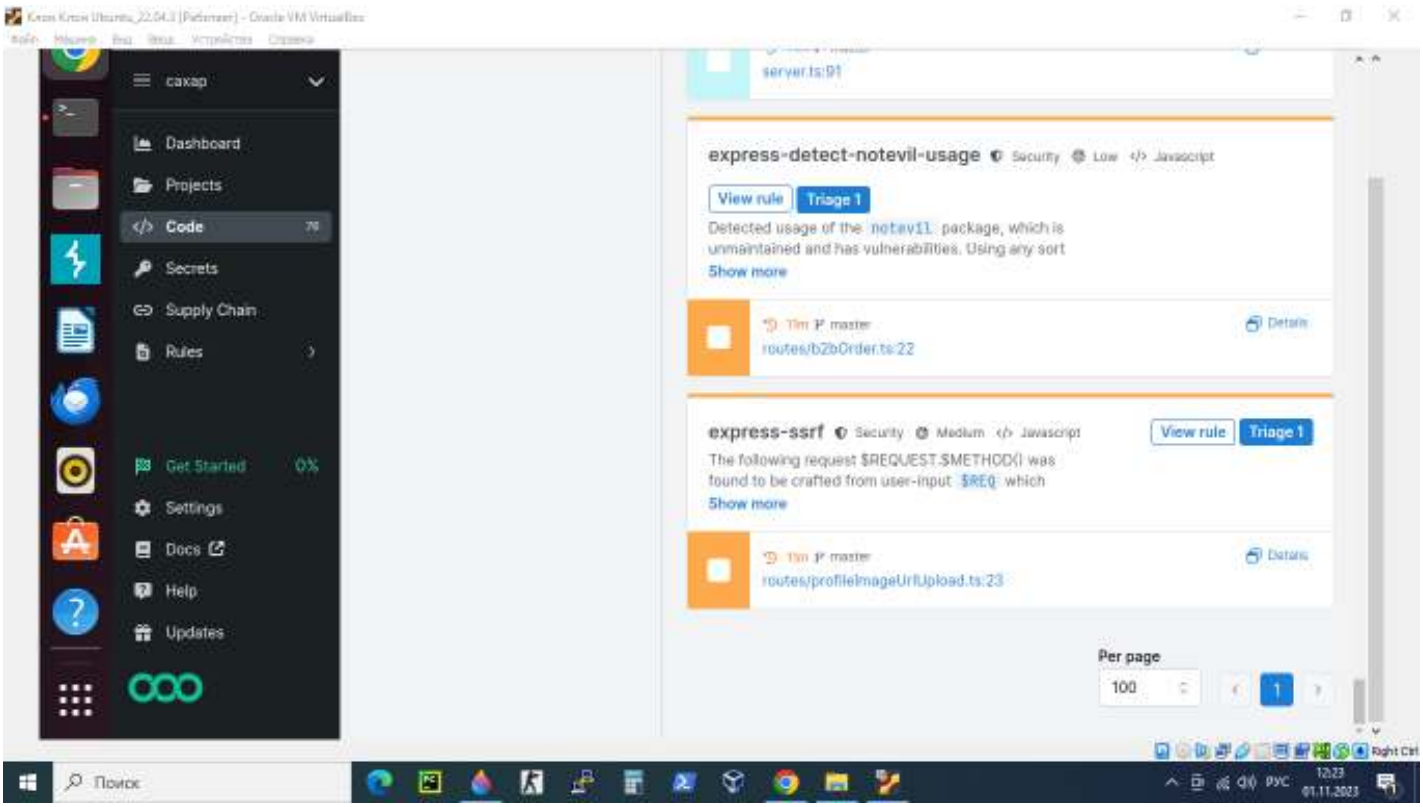
Пункт 2 Результаты статического анализа 1 скриншот



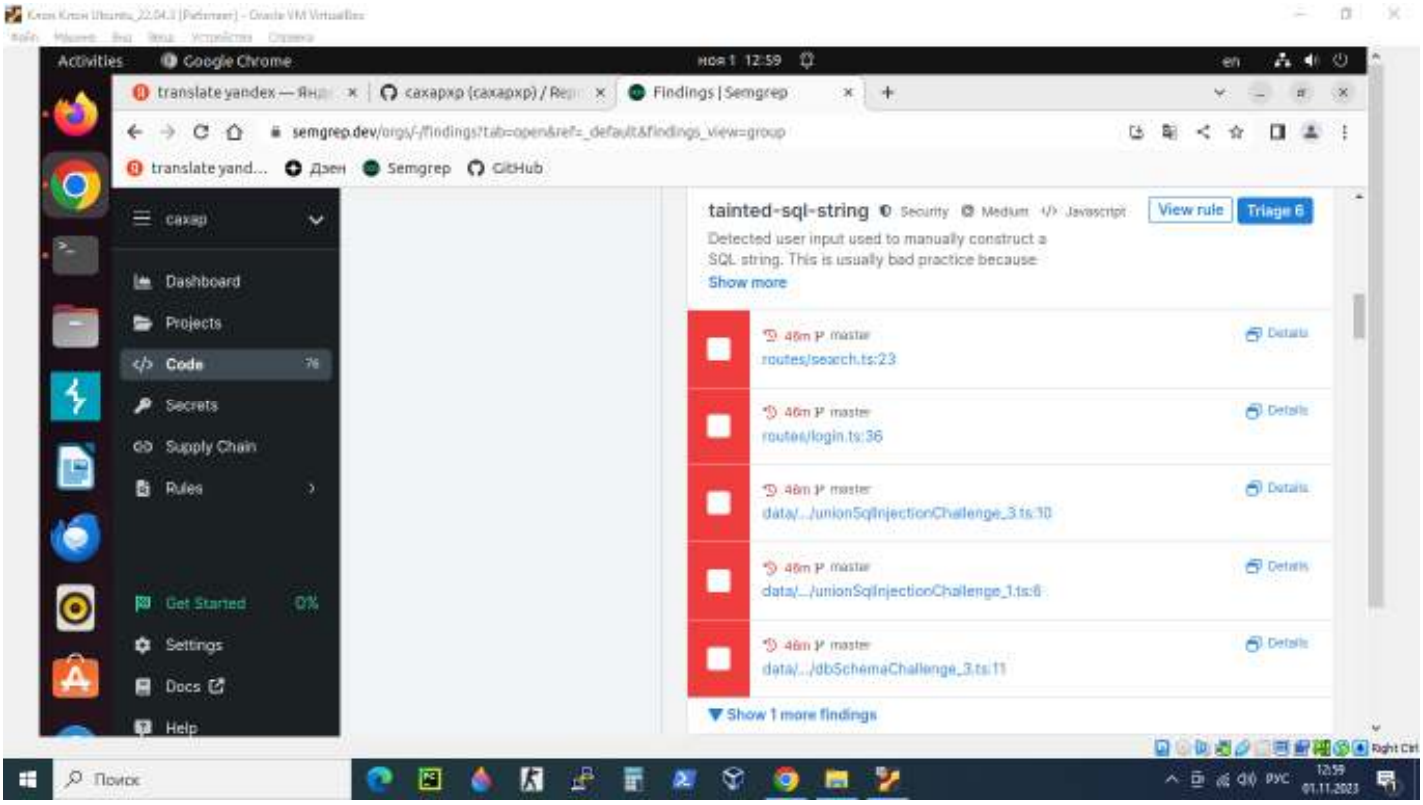
Пункт 2 Результаты статического анализа 2 скриншот



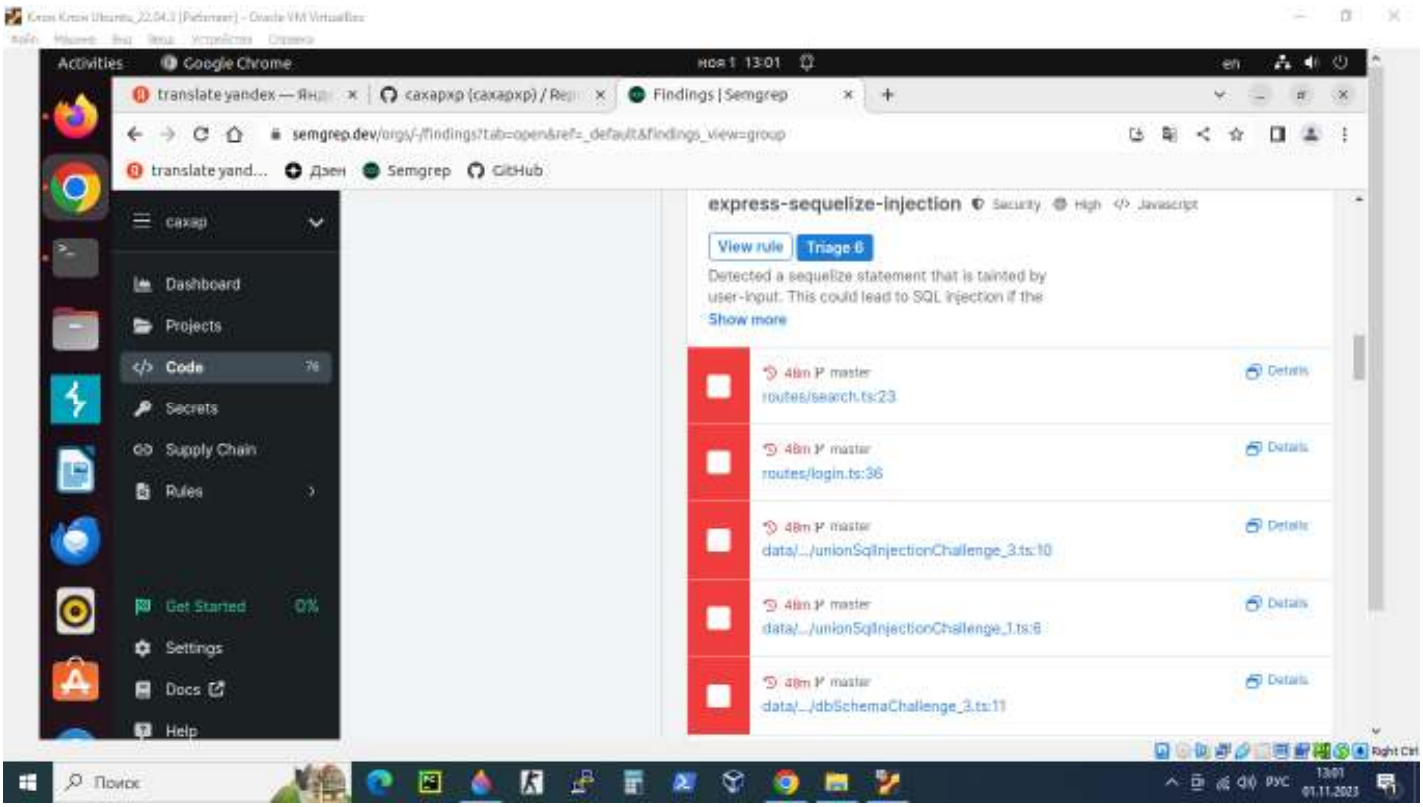
Пункт 2 Результаты статического анализа 3 скриншот



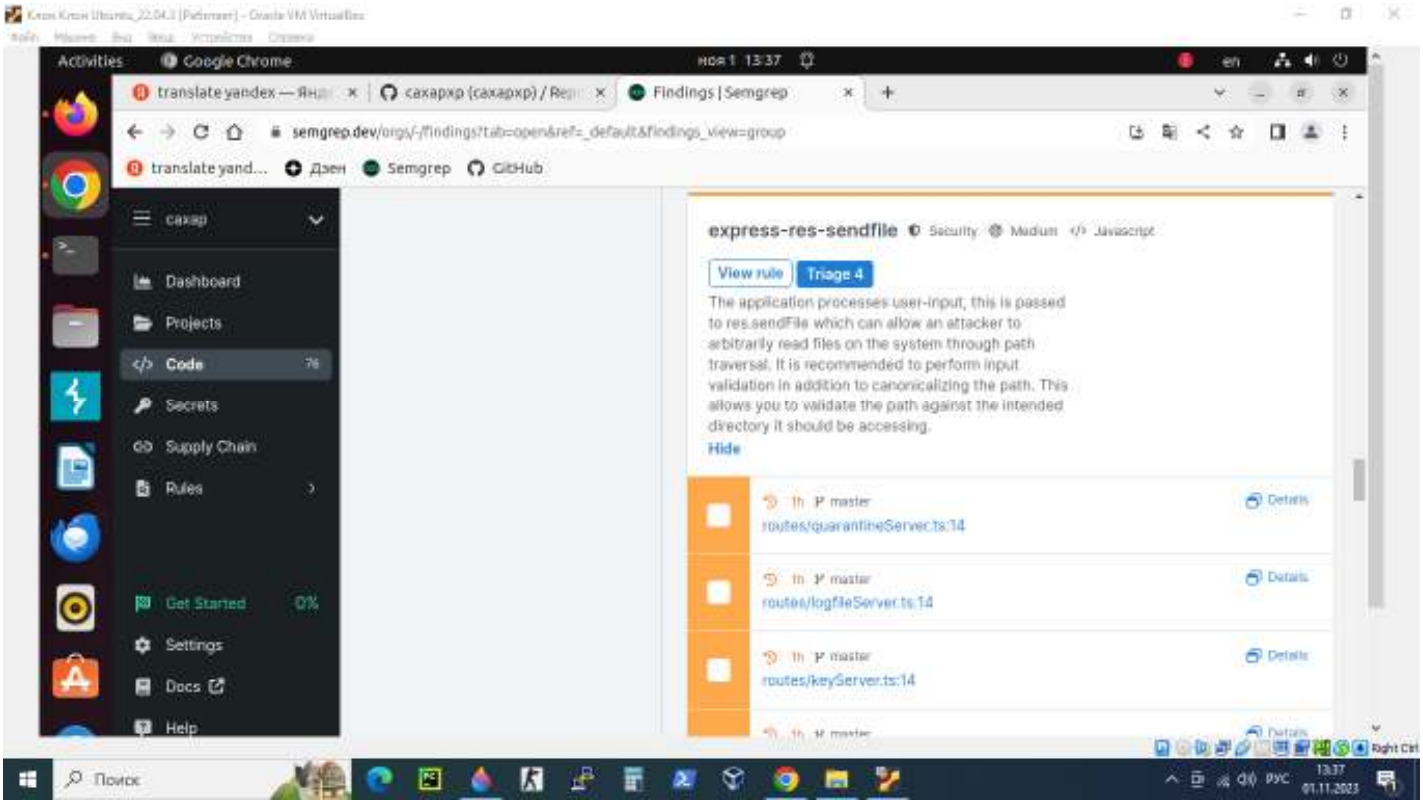
Пункт 3 Уязвимости из OWASP Top-10 1 скриншот



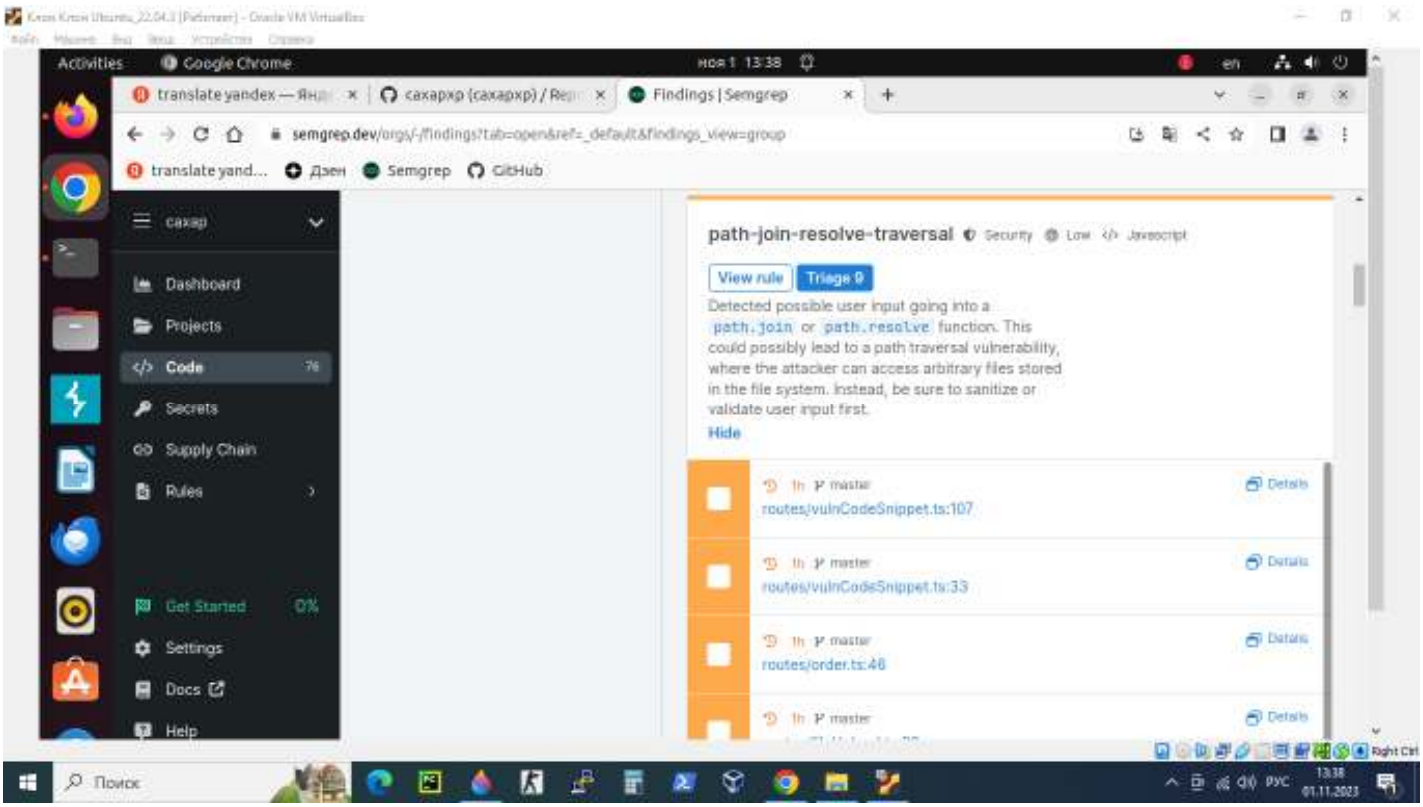
Пункт 3 Уязвимости из OWASP Top-10 2 скриншот



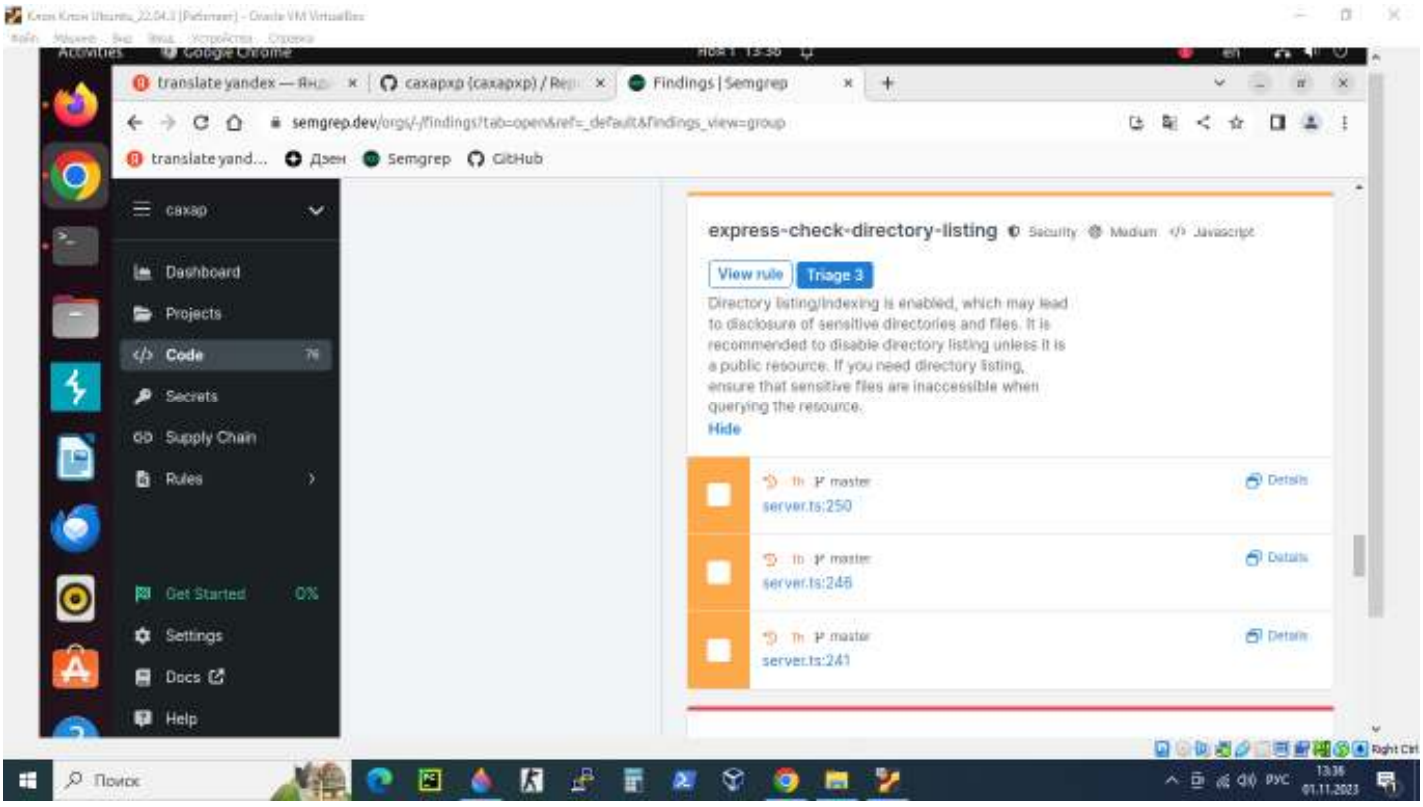
Пункт 3 Уязвимости из OWASP Top-10 3 скриншот



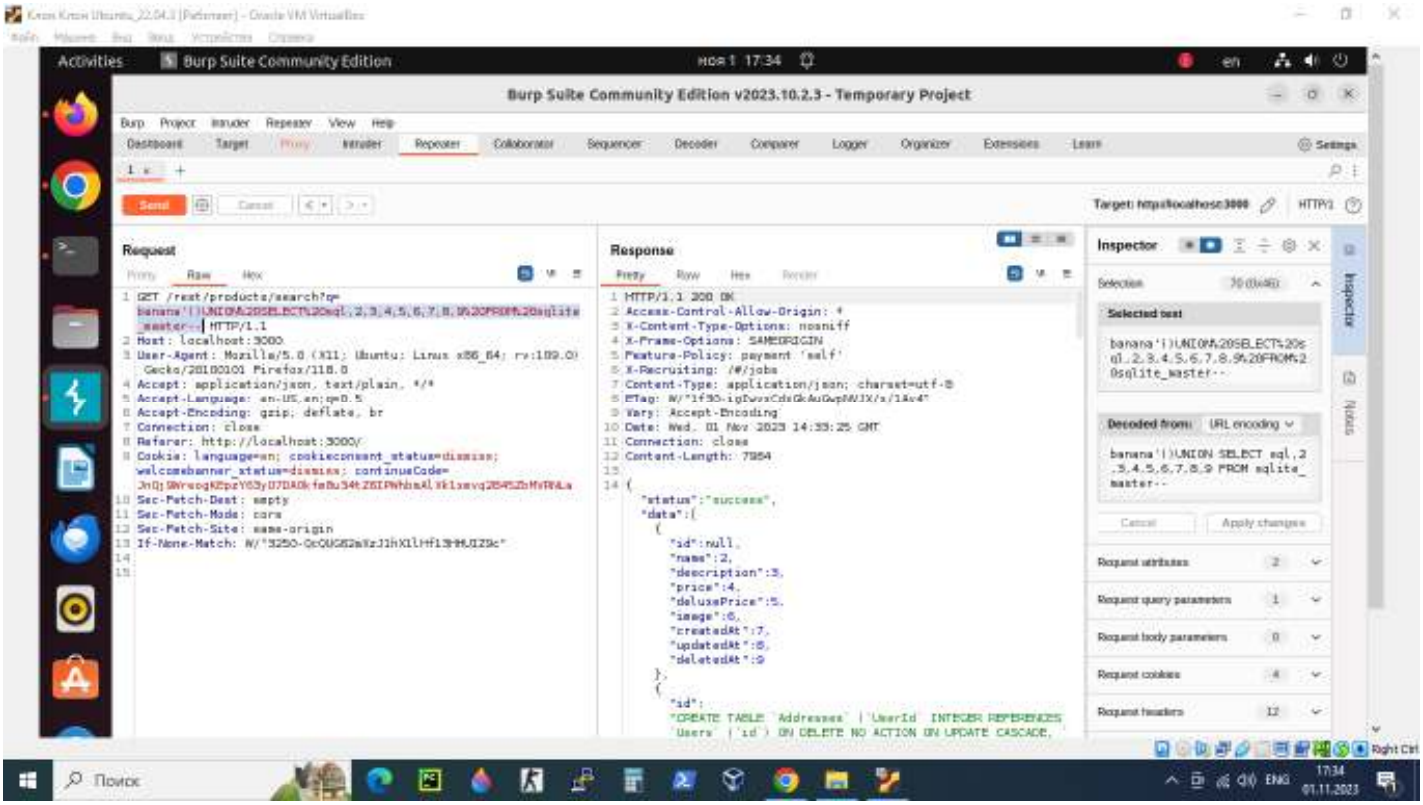
Пункт 3 Уязвимости из OWASP Top-10 4 скриншот



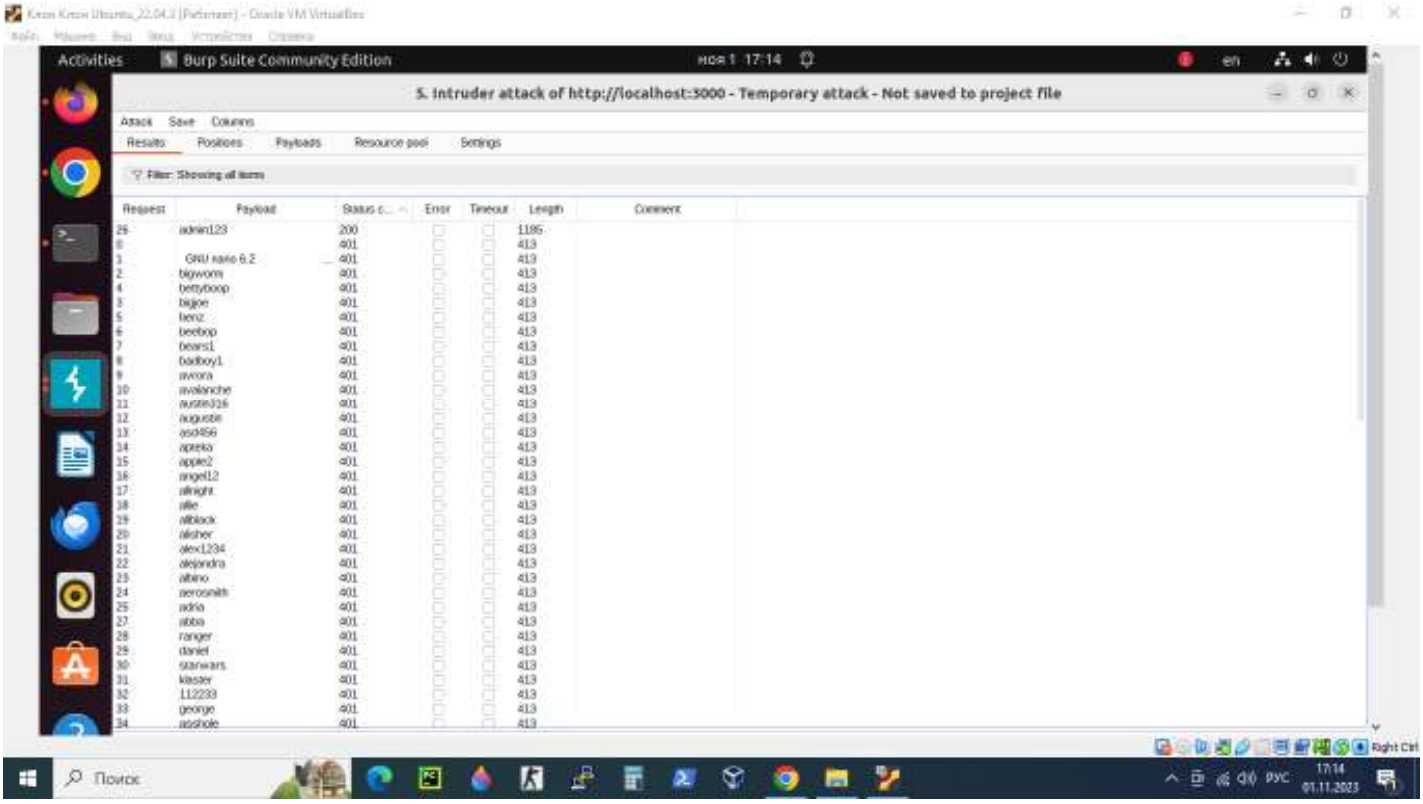
Пункт 3 Уязвимости из OWASP Top-10 5 скриншот



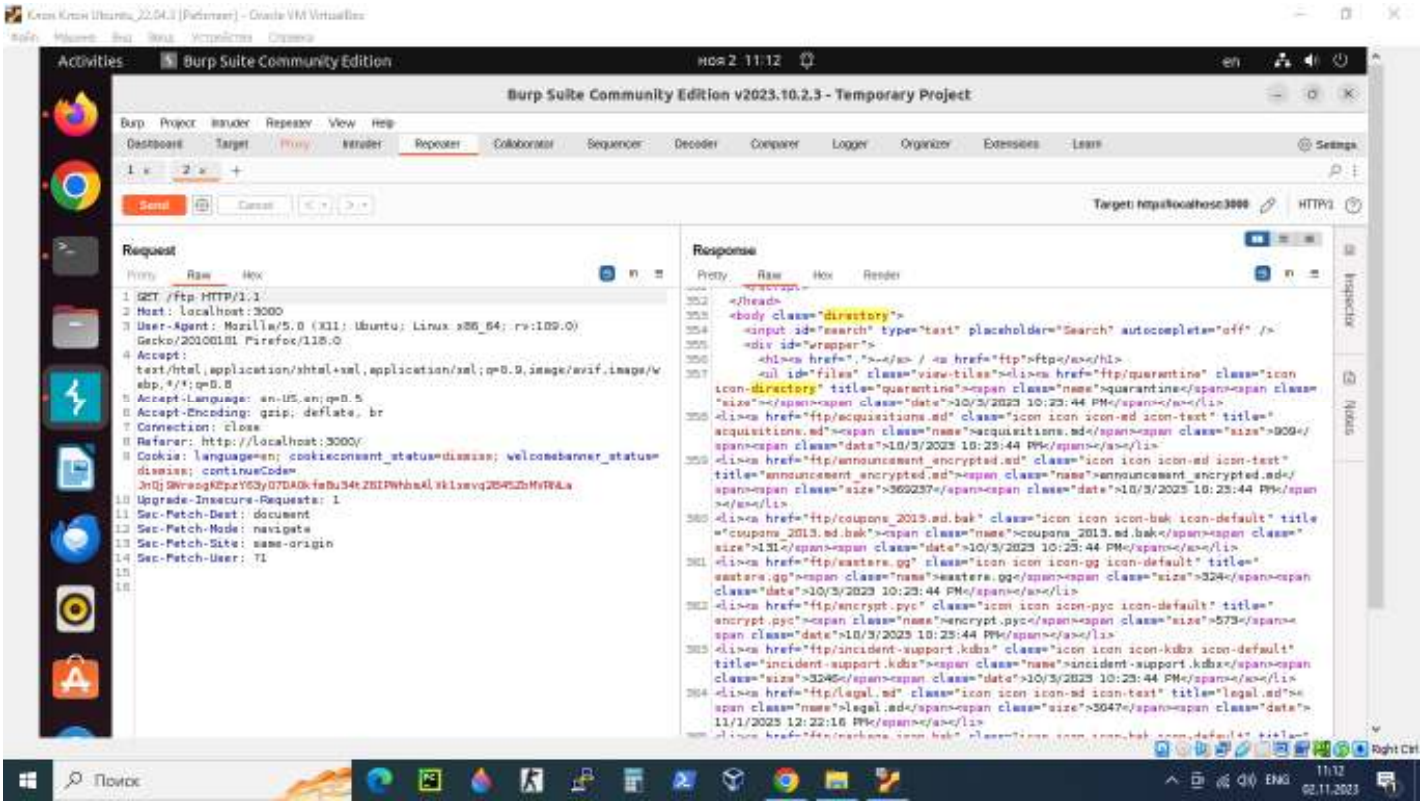
Пункт 4 Sql injection database



Пункт 4 Sql injection password_admin



Пункт 4 запрос и просмотр директории



Пункт 4 получение конфиденциального документа