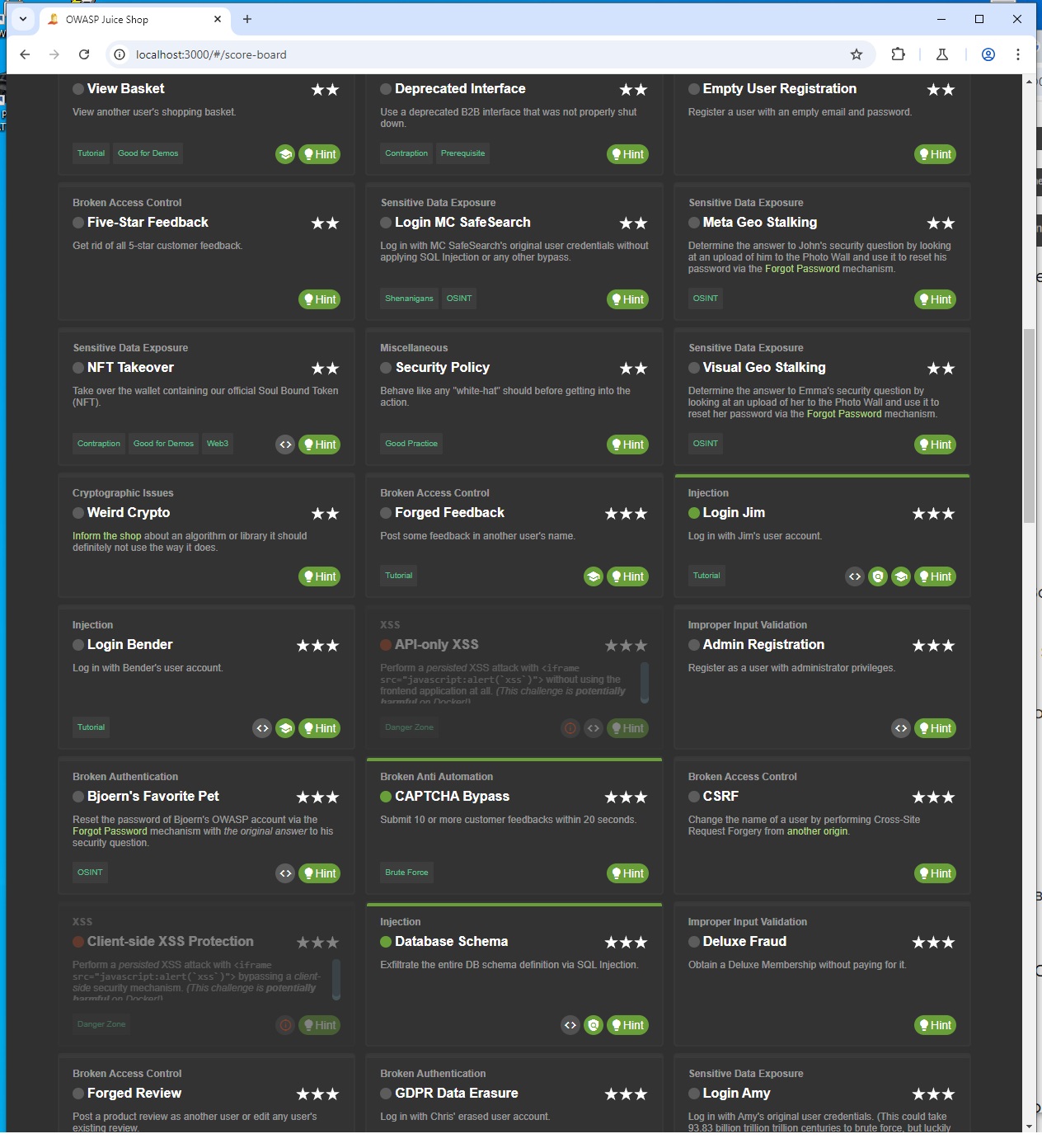
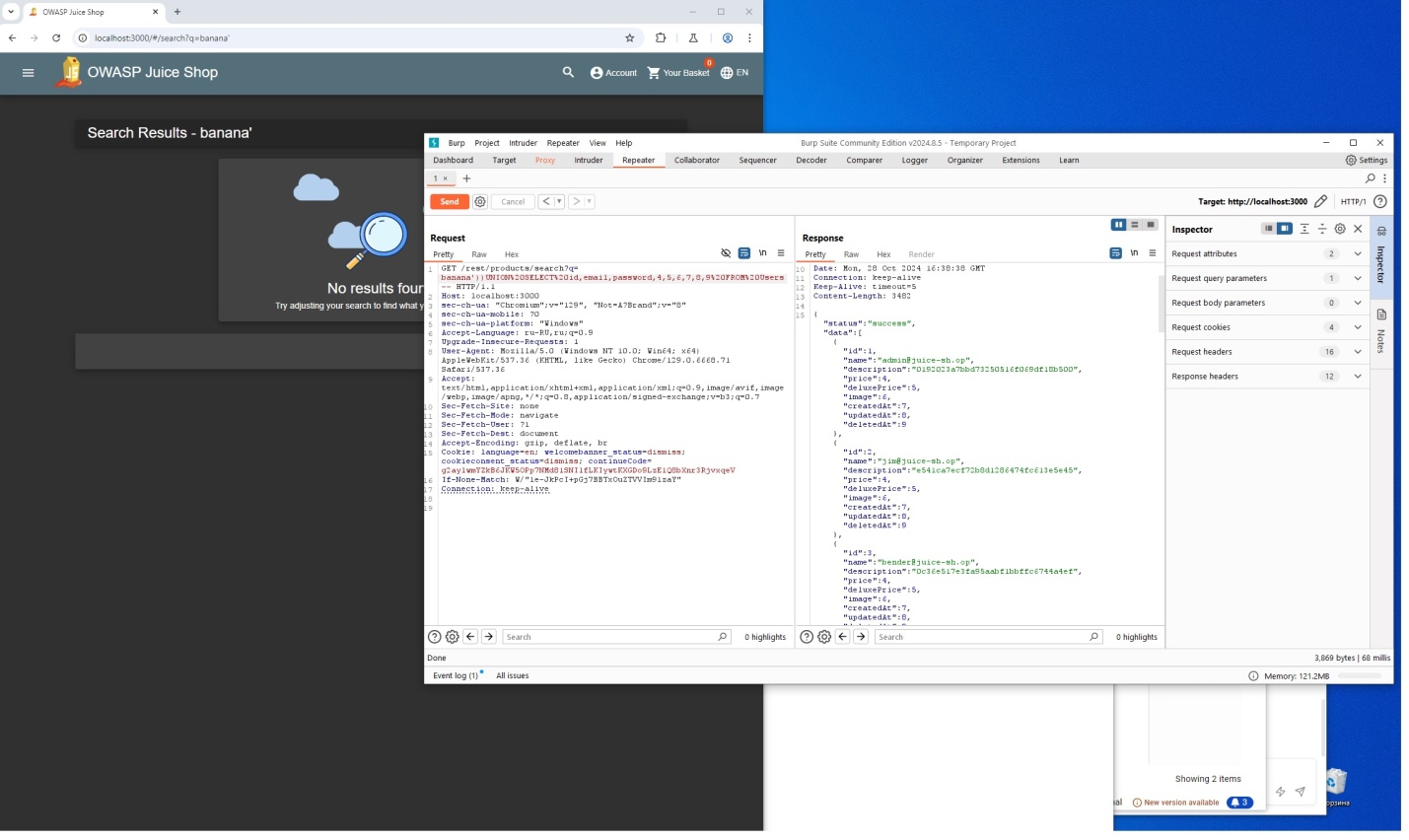
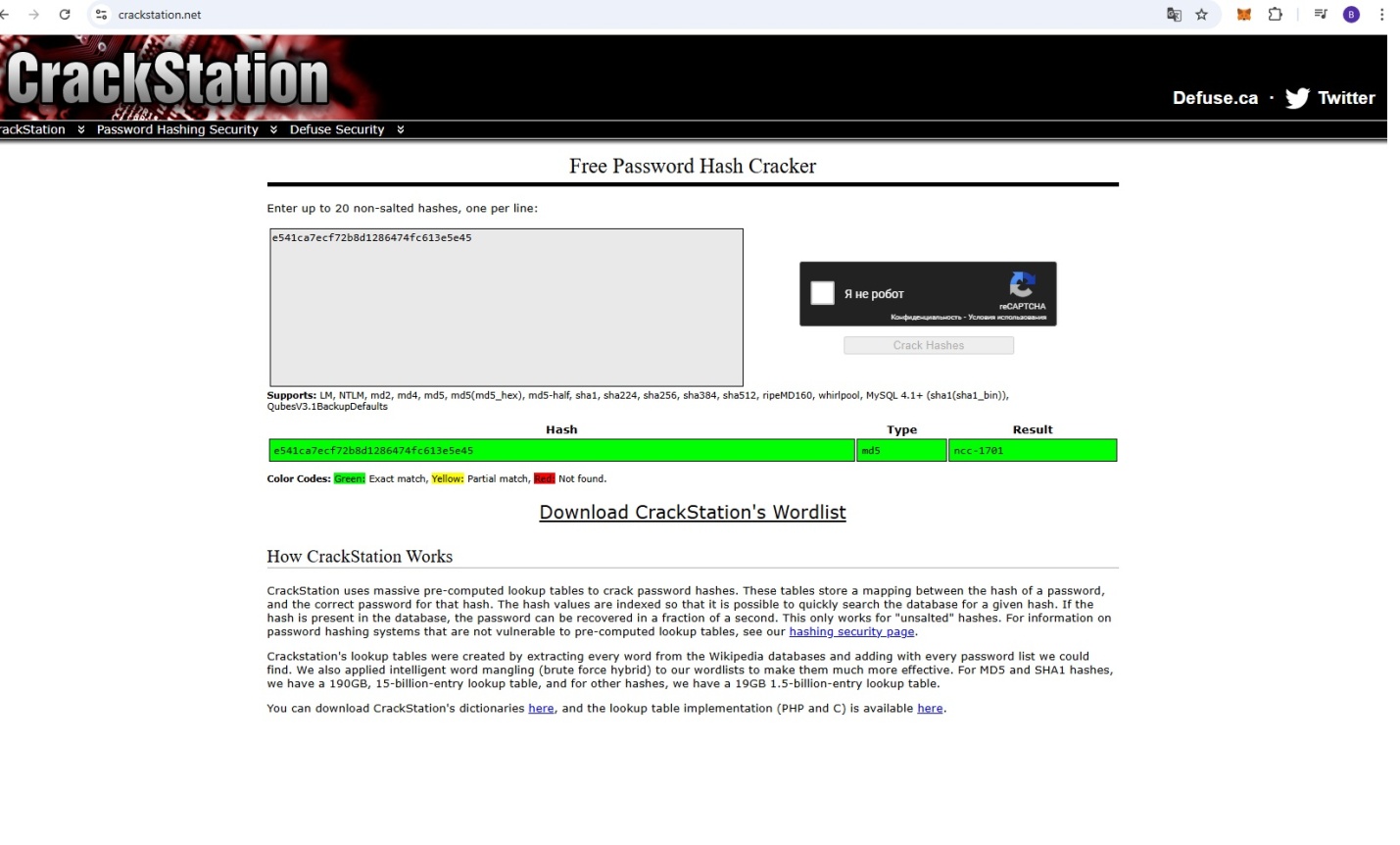
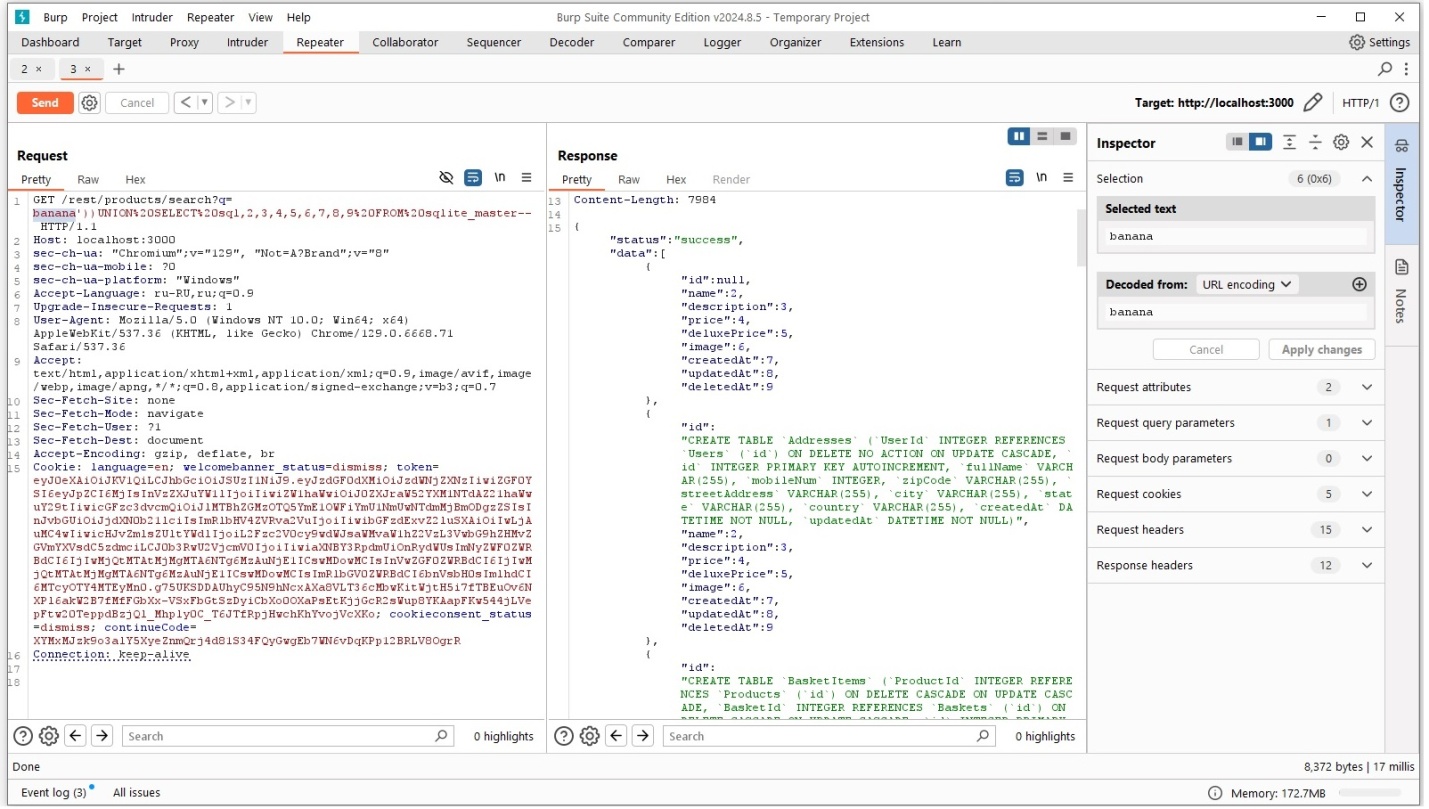
1. **Скриншот выполненной работы CAPTCHA Bypass из таблицы Scoreboard Juice Shop. Скриншот выполненной работы Database Schema из таблицы Scoreboard Juice Shop. Скриншот выполненной работы Login Jim из таблицы Scoreboard Juice Shop**

****

****

1. **Скопировав примеры кода в локальную папку и скачав свежие правила сканирования для semgrep – запустил сканирование(статический анализ). В результате чего semgrep выдал информацию о 8ми возможных проблемах безопасности кода. Проанализировав полученную информация я определил что:**

- **find\_vuln6.py** существует серьезная уязвимость, связанная с выполнением произвольного кода, что может привести к удаленному выполнению команд os.system()

**- find\_vuln7.js** код демонстрирует две разные уязвимости, которые связаны с выполнением произвольных команд в операционной системе на основе данных, предоставленных пользователями exec, gzip, spawn.

**- find\_vuln8.php** в коде представлено несколько примеров уязвимостей, связанных с выполнением команд: PHP-код, который выполняет команду whois с параметром из POST-запроса, а также код для выполнения системных команд. system(),exec, spawn.

