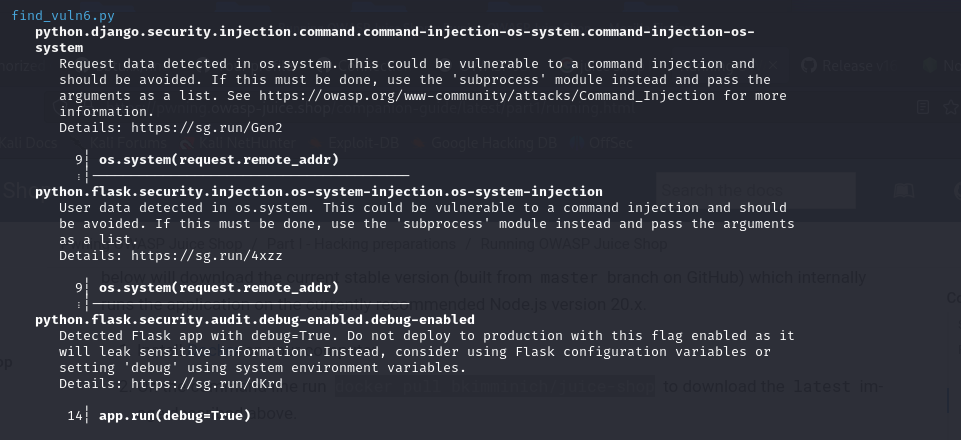
Сканирование файлов с помощью Semgrep

Все файлы с домашнего задания были загружены в одну директорию и использовалась команда **/snap/bin/semgrep --config auto**

**Find\_vuln6.py**

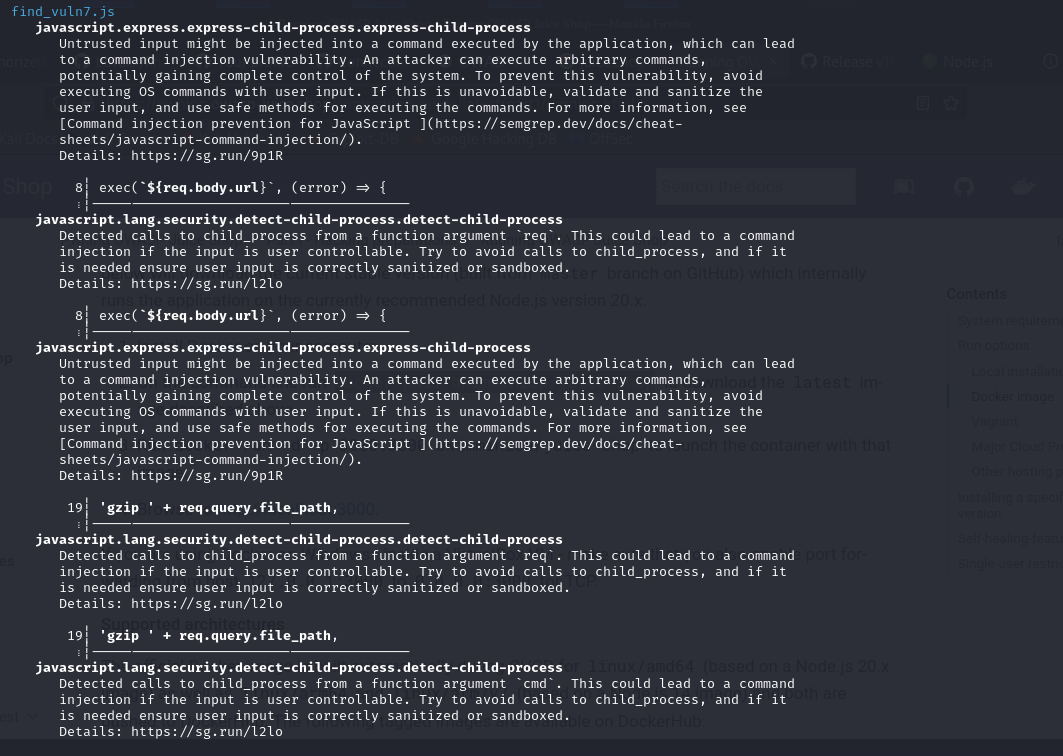


Semgrep обнаружил две ошибки в коде:

1. В строке 9 используется функция os.system() для выполнения команды с переданным параметром request.remote\_addr. Это может привести к уязвимости командного инъектирования, так как пользовательский ввод не был обработан должным образом. Рекомендуется использовать модуль subprocess и передавать аргументы в виде списка.

2. В строке 14 используется параметр debug=True при запуске Flask-приложения. Это может привести к утечке чувствительной информации в производственной среде. Рекомендуется использовать переменные конфигурации Flask или настройки среды для установки параметра debug.

**Find\_vuln8.js**

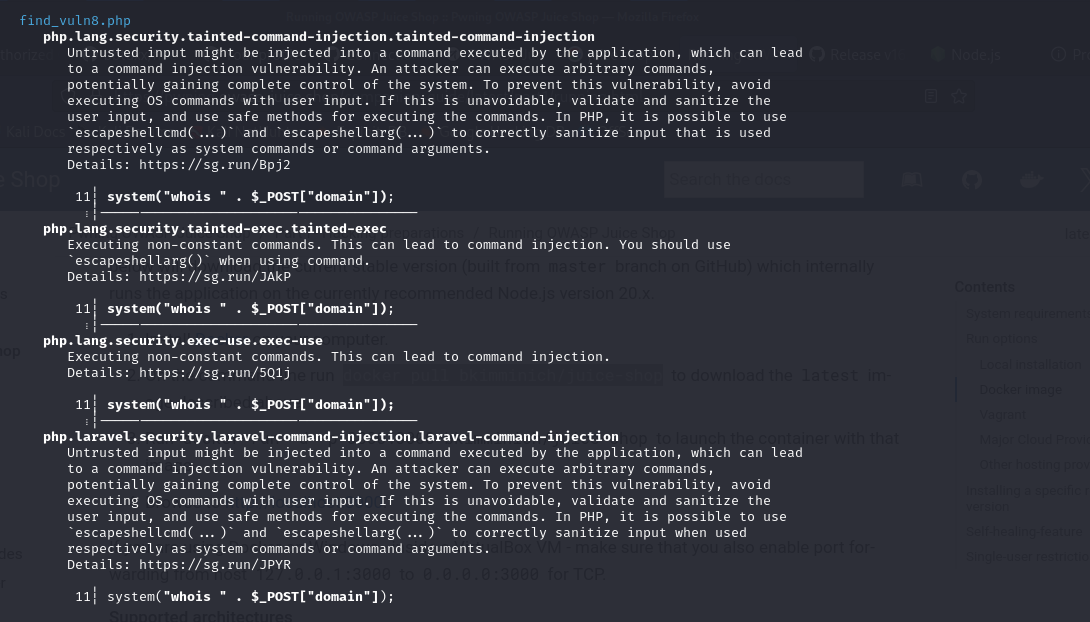


Semgrep обнаружил две ошибки в коде:

1. В строке 8 используется функция exec() с переданным параметром req.body.url, который является пользовательским вводом. Это может привести к уязвимости командного инъектирования, так как пользовательский ввод не был обработан должным образом. Рекомендуется использовать модуль child\_process и передавать аргументы в виде списка.

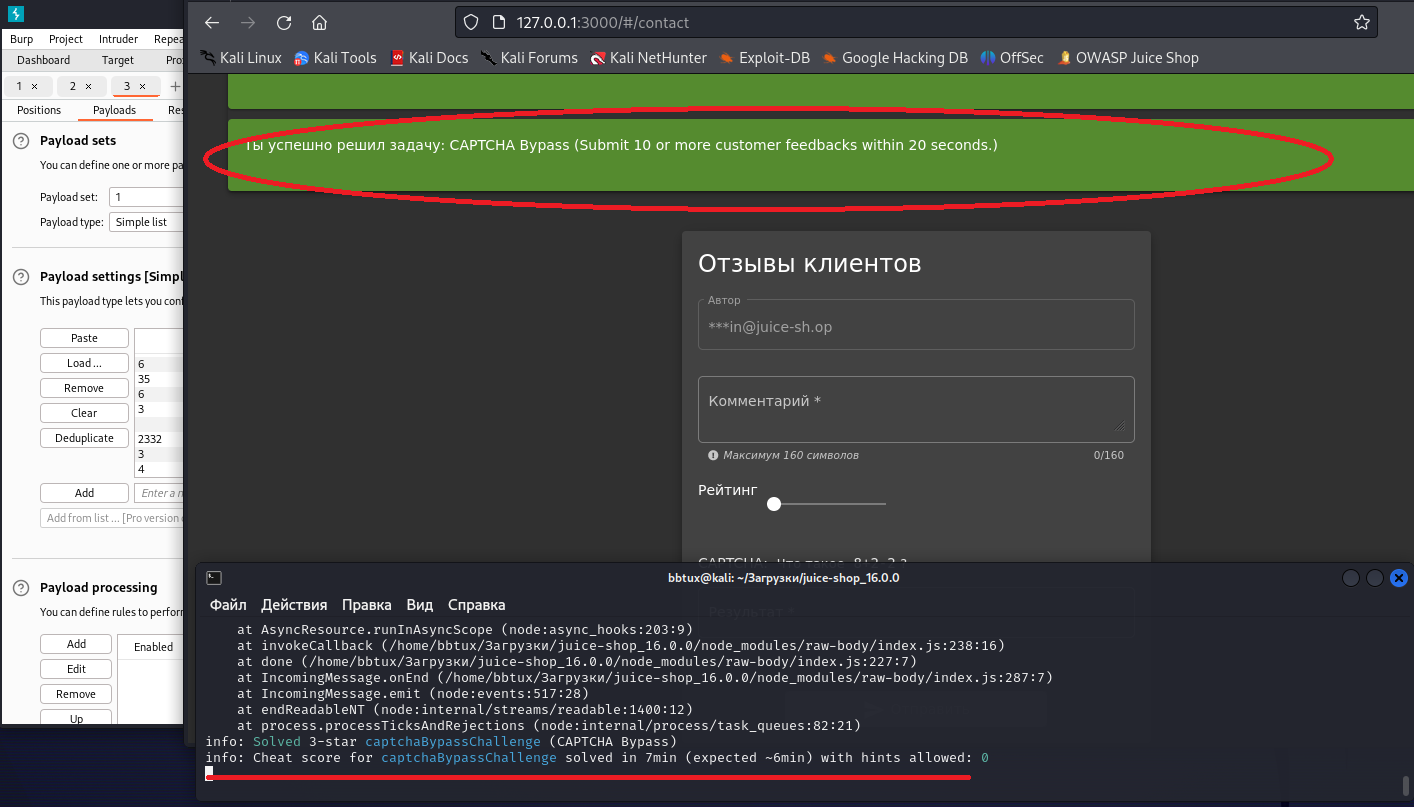
2. В строке 19 используется функция exec() с переданным параметром req.query.file\_path, который является пользовательским вводом. Это может привести к уязвимости командного инъектирования, так как пользовательский ввод не был обработан должным образом. Рекомендуется использовать модуль child\_process и передавать аргументы в виде списка

**Find\_vuln8.php**

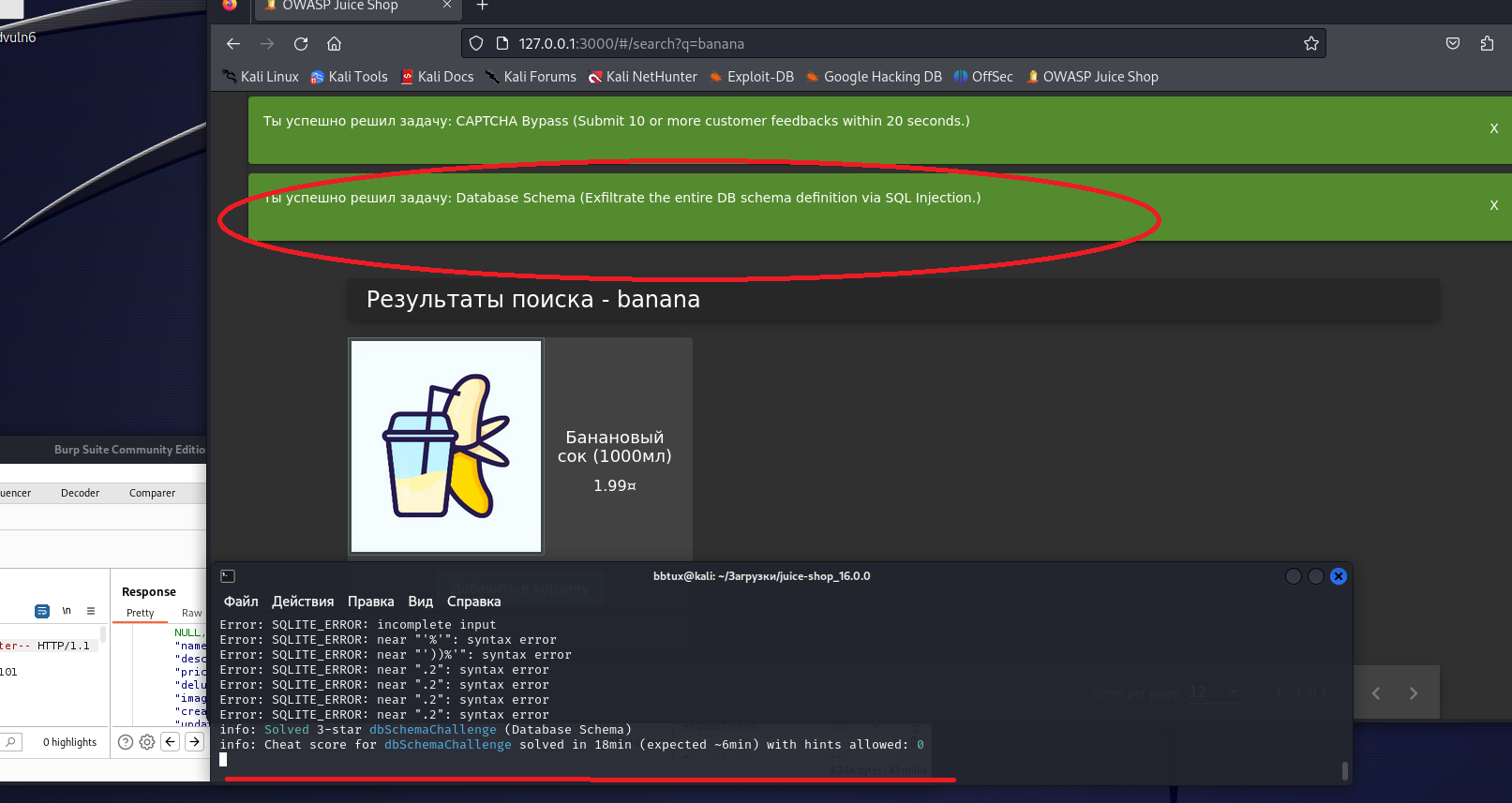


В строке 11 используется функция system() с переданным параметром $\_POST["domain"], который является пользовательским вводом. Это может привести к уязвимости командного инъектирования, так как пользовательский ввод не был обработан должным образом. Рекомендуется использовать функцию escapeshellarg() для корректной обработки пользовательского ввода при использовании команд.

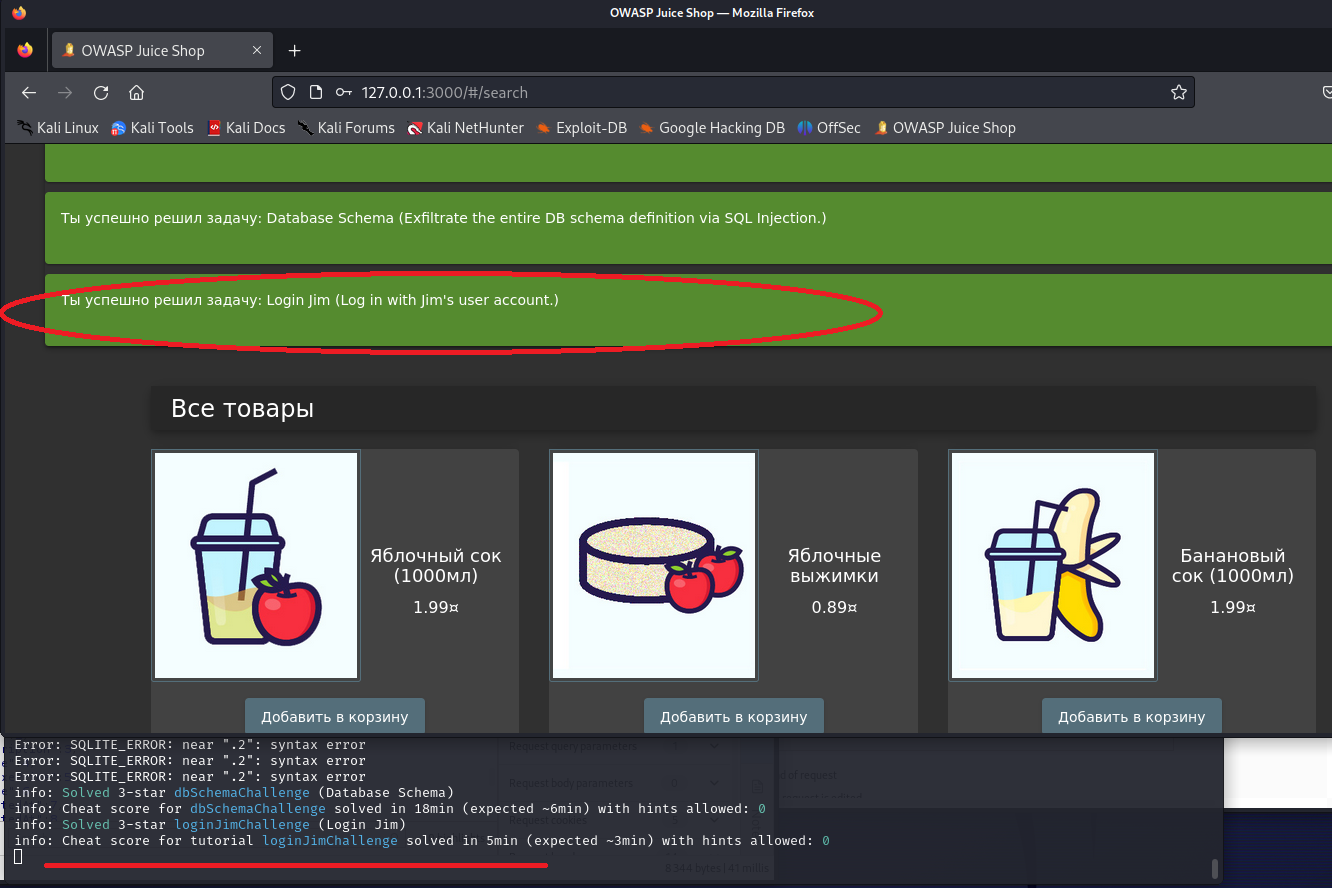
Juice Shop

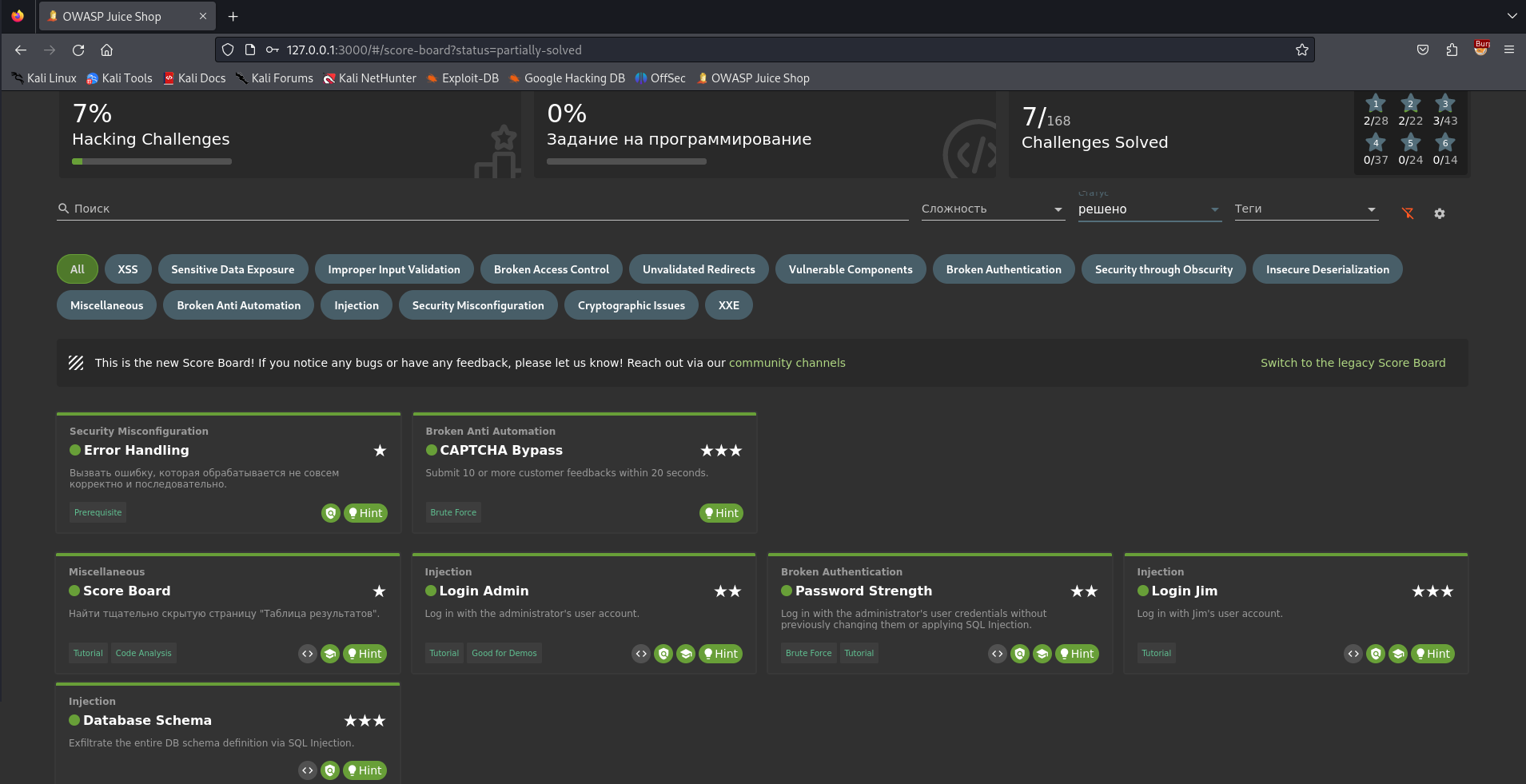
**Captcha\_Bypass**   


**Database SCHEMA**



**Login Jim**

****

****