**МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ**

**Государственное бюджетное профессиональное образовательное учреждение Московской области «Люберецкий техникум имени Героя Советского Союза, летчика-космонавта Ю.А.Гагарина»**

**ОТЧЕТ**

**ПО УЧЕБНОЙ ПРАКТИЧЕСКОЙ ПОДГОТОВКЕ**

Ефремов Егор Михайлович

(Фамилия, имя, отчество студента)

по профессиональному модулю

**ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**

Специальность

\_\_\_\_\_\_\_\_\_\_10.02.05 Обеспечение информационной безопасности\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_автоматизированных систем\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Код, название*

Курс \_3\_ Группа № 204ОИБ

Период практической подготовки

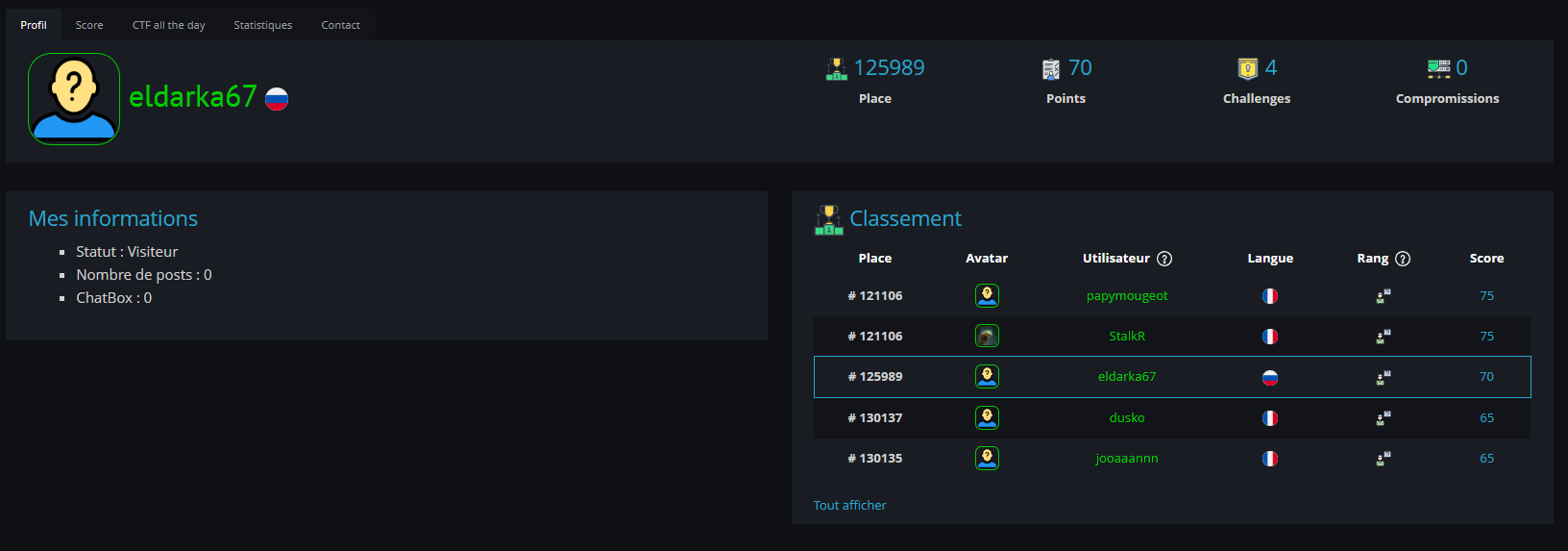
с *«\_11\_»\_\_мая\_\_ 2023 г.* по *«\_31\_»\_\_мая\_\_ 2023 г.*

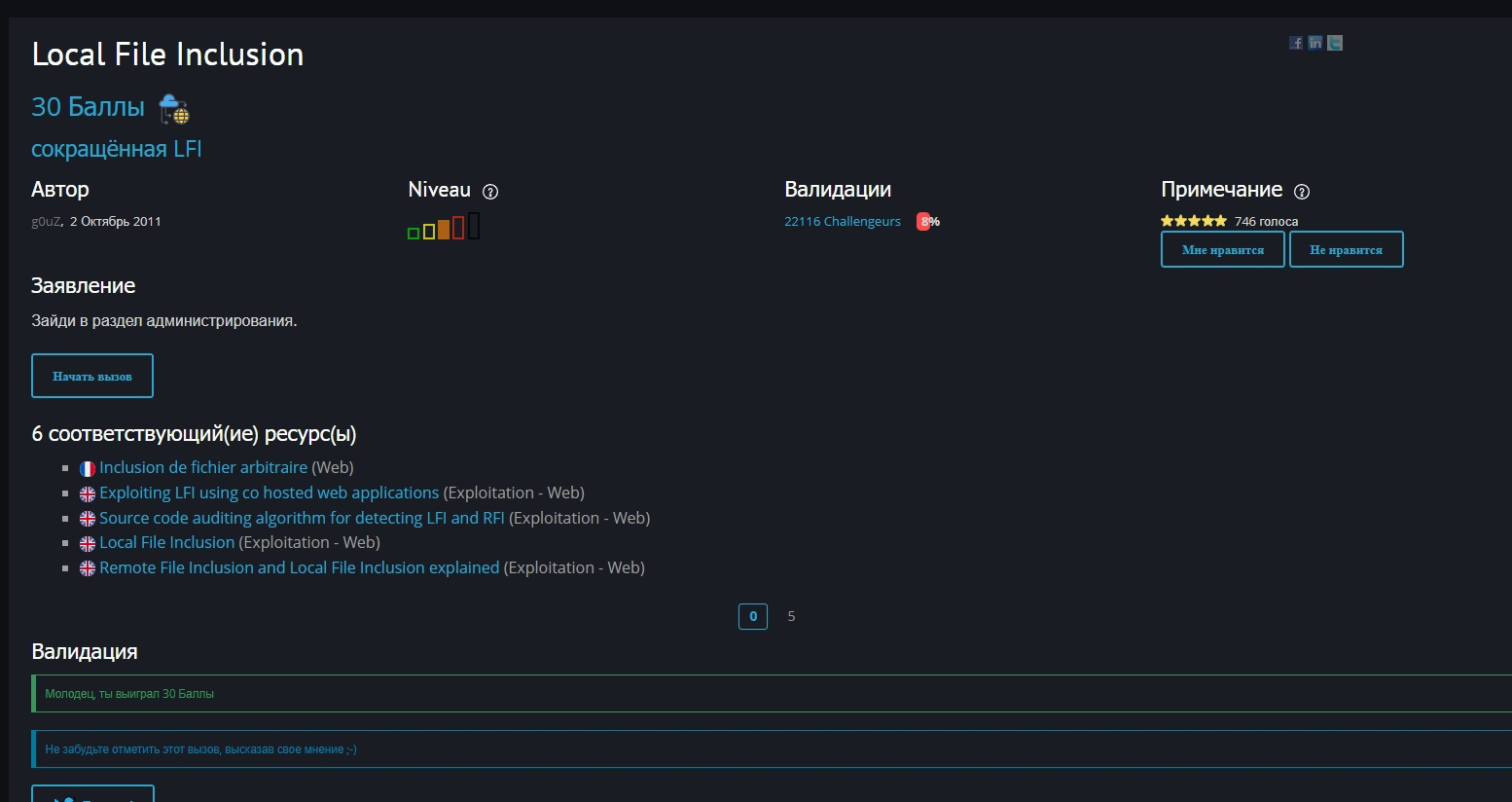
Руководитель практической

подготовки от техникума \_\_\_\_\_\_\_\_\_ (*Тарджиманян Лия Николаевна*)

Люберцы 2023

**Root Me:** обучающая платформа, посвященная взлому и информационной безопасности, на которой более 500 испытаний доступны для обучения взлому. В рамках учебной и производственной практик по профессиональному модулю ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении были выполнены следующие задания:

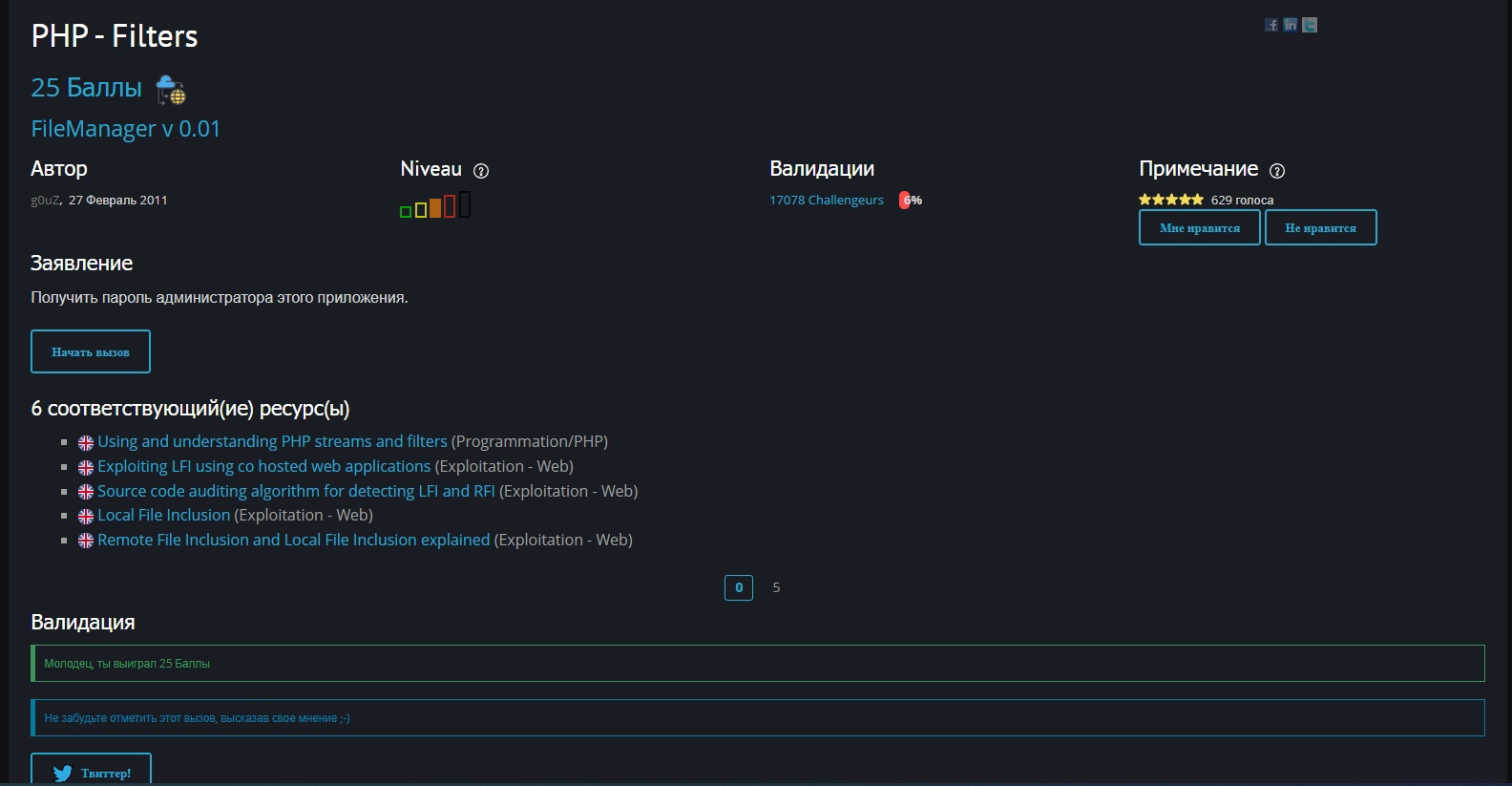
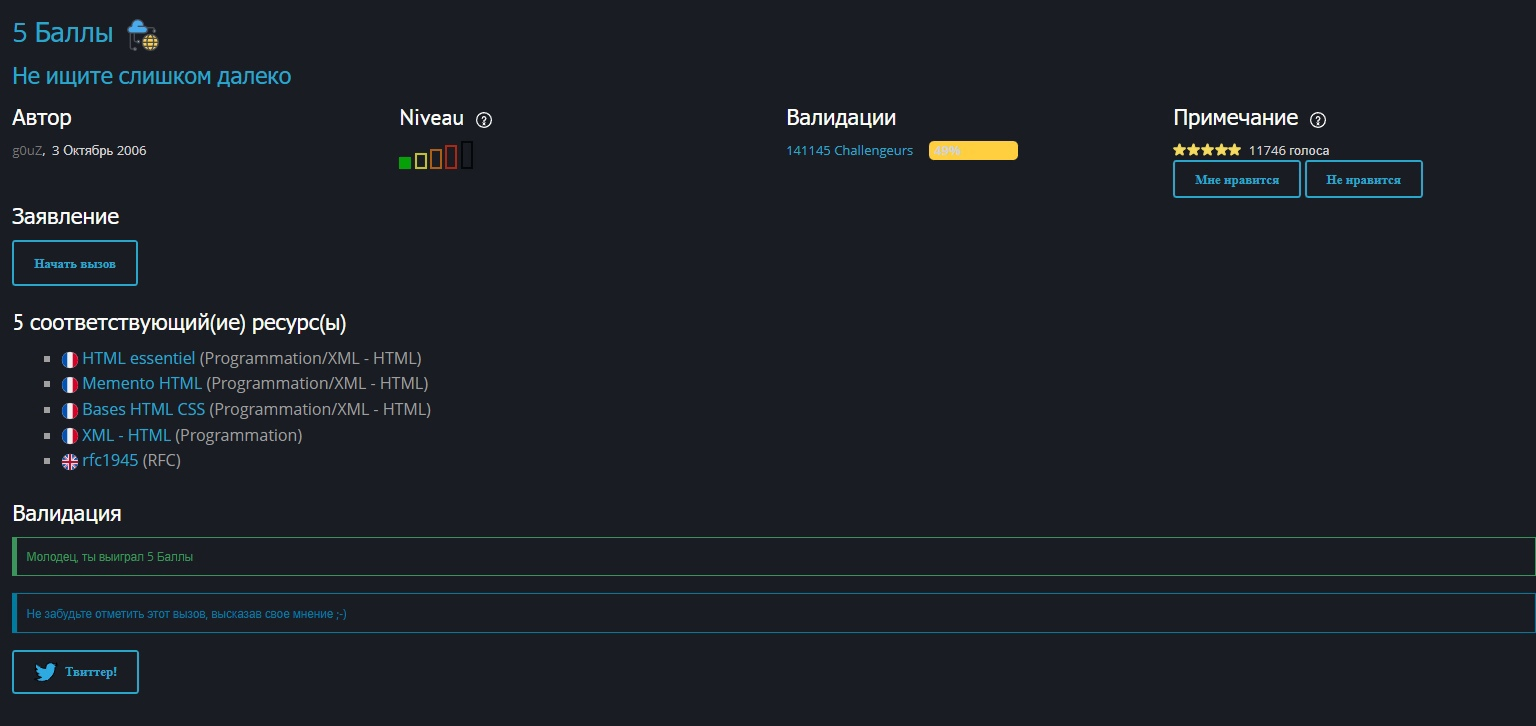


****Local file:

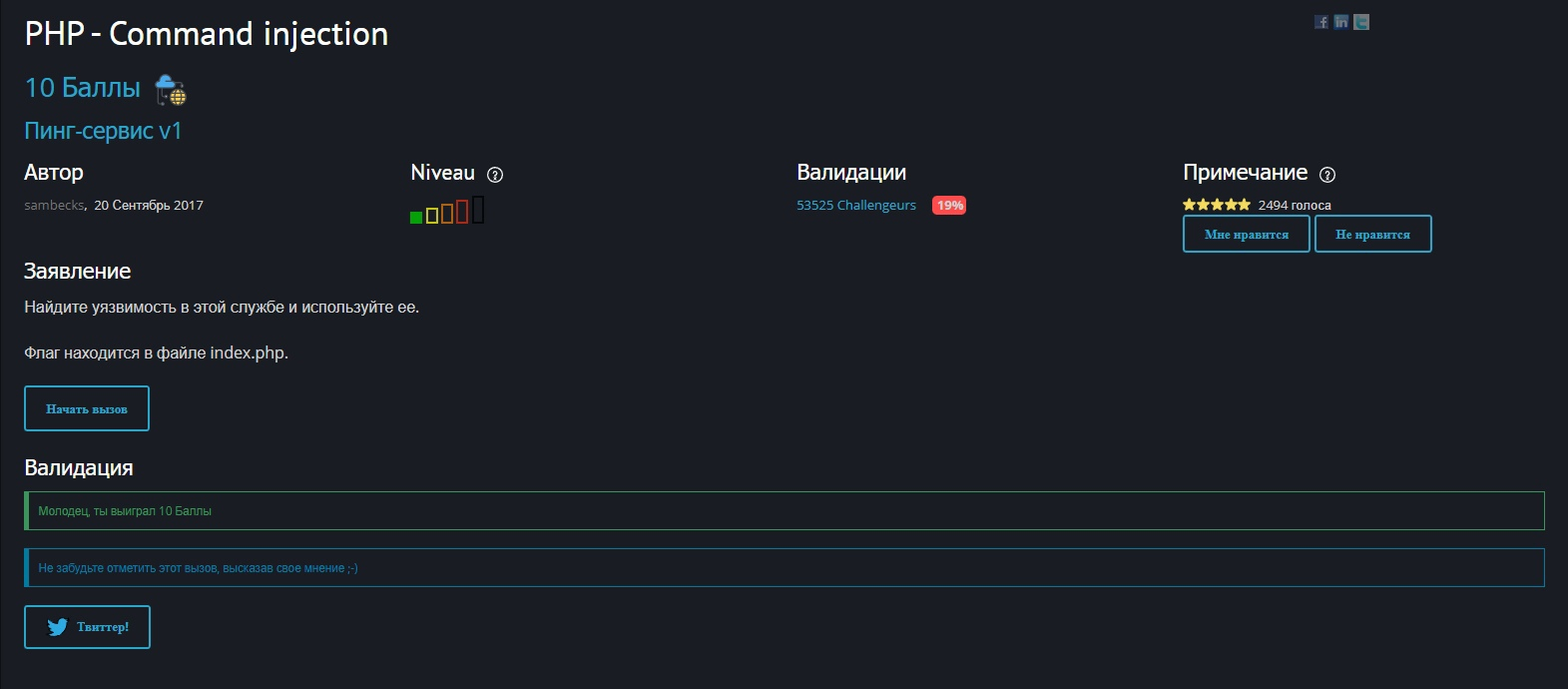
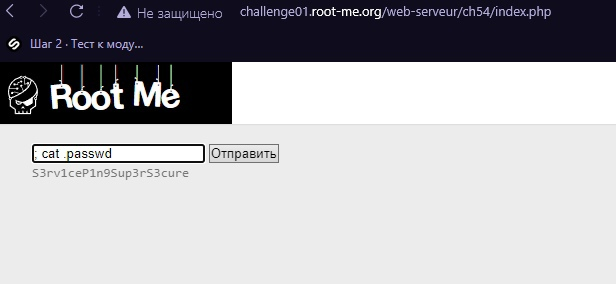
При заходе на сайт мы обнаруживаем список файлов и папок, доступных для перехода. Если перейти по одной из ссылок, мы увидим внутри папки файлы, и устанавливается параметр files с названием папки. При чтении файла внутри папки мы можем увидеть его содержимое и появится параметр f, который отвечает за файл в данной папке.



При просмотре правой части сайта мы замечаем, что находимся на сайте как гость, но есть возможность авторизоваться как администратор. При попытке авторизоваться вылезает окно авторизации, однако, если его закрыть, мы можем увидеть, что существует папка admin. Пытаясь прочитать ее содержимое, мы находим один файл, который содержит имя пользователя admin и пароль. Попробовав использовать это для авторизации, мы успешно входим на сайт.

**  
**Php filters:

Параметр "inc", принимающий название скрипта, привлекает внимание и напоминает LFI. Однако, есть проблема - файл, по всей видимости, выполняется на сервере при загрузке, но его полный исходный код недоступен. Чтобы решить эту проблему, можно закодировать вывод файла в base64 с помощью php-фильтров. После декодирования полученного вывода, можно получить ответ.

**  
  
  
**