**Отчет по пентесту-номер задания 15.x модуля 15**

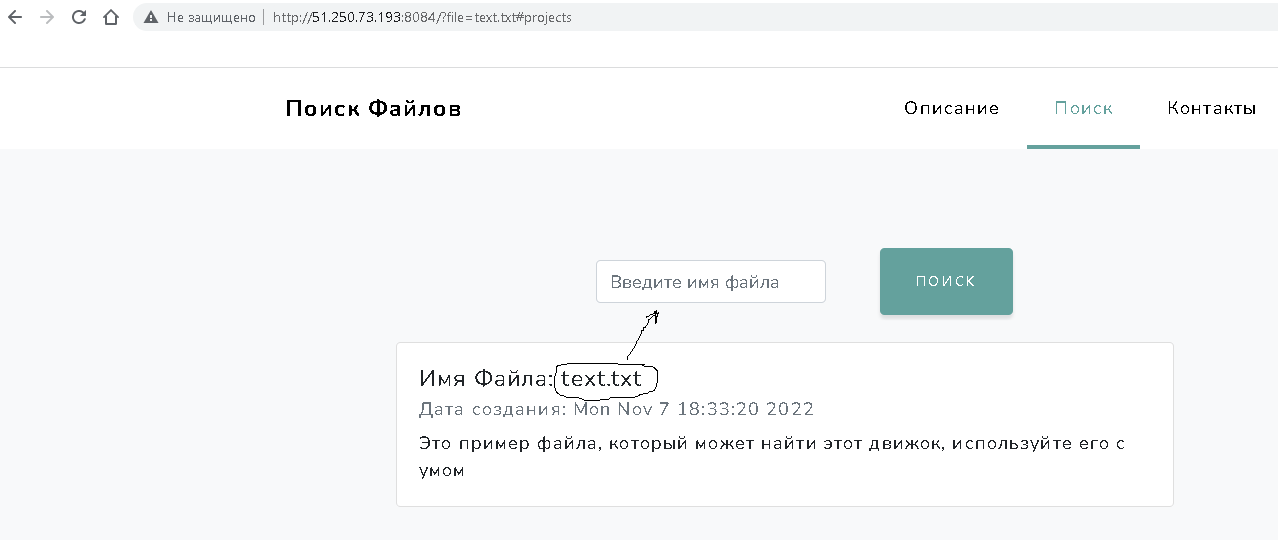
**Персонализация:** Ермакова Наталья Олеговна (natalysoliton@mail.ru)

**LFI Задание 15.7.1**

Мы создали сервис по поиску файлов в наших хранилищах. Мы надеемся, что наш эффективный поиск данных поможет нашим клиентам. Мы быстро растущая компания. Надеемся на сотрудничество.

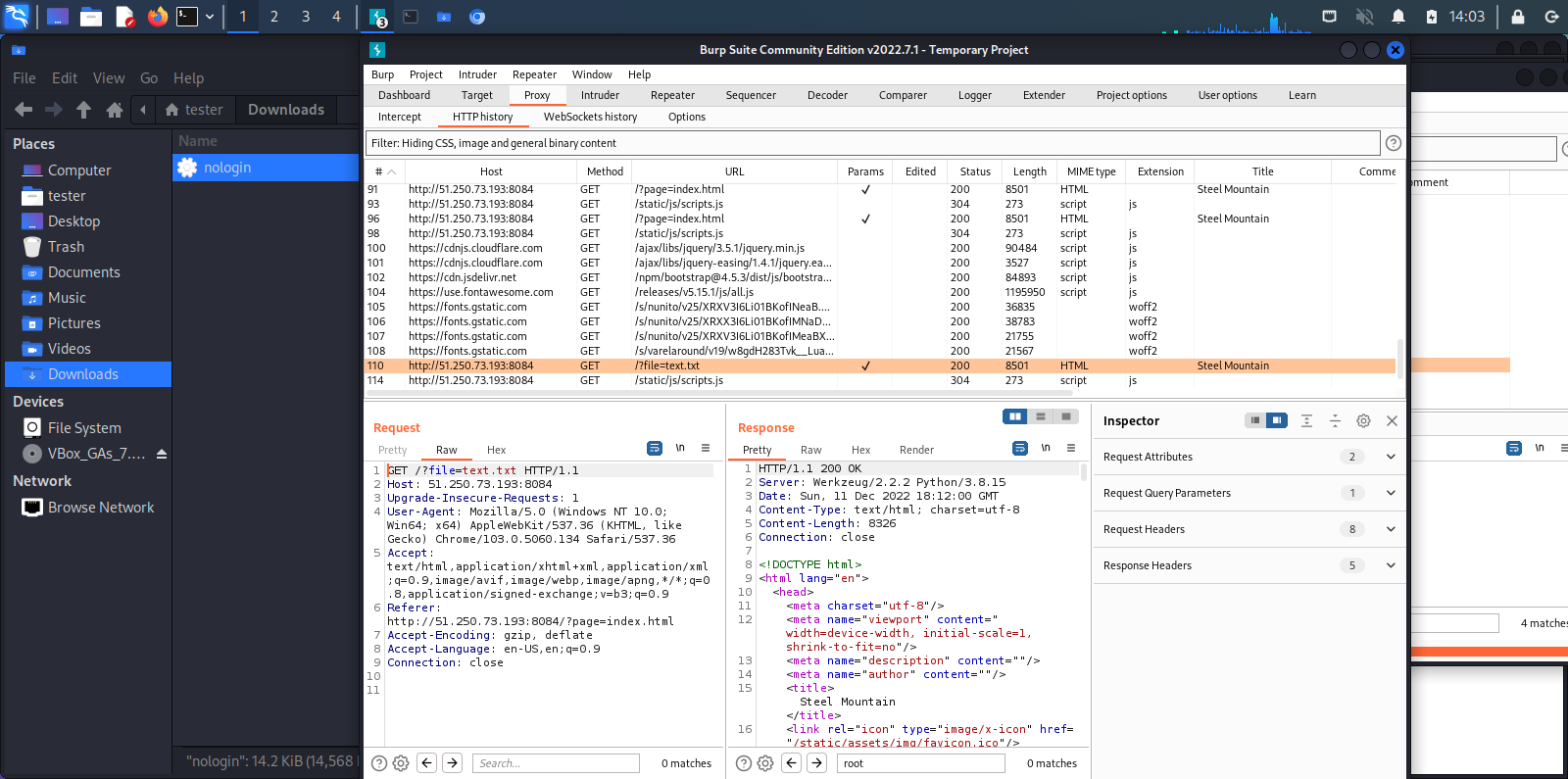
* Общая информация:
  + Период тестирования: 11.12.2022
  + Объект тестирования: [http://51.250.73.193:8084](http://51.250.73.193:8084/)
* Описание действий:

Открыла веб-страницу [http://51.250.73.193:8084](http://51.250.73.193:8084/) и ввела имя файла text.txt, чтобы при передачи запроса увидеть параметр метода GET в Burp Suite.

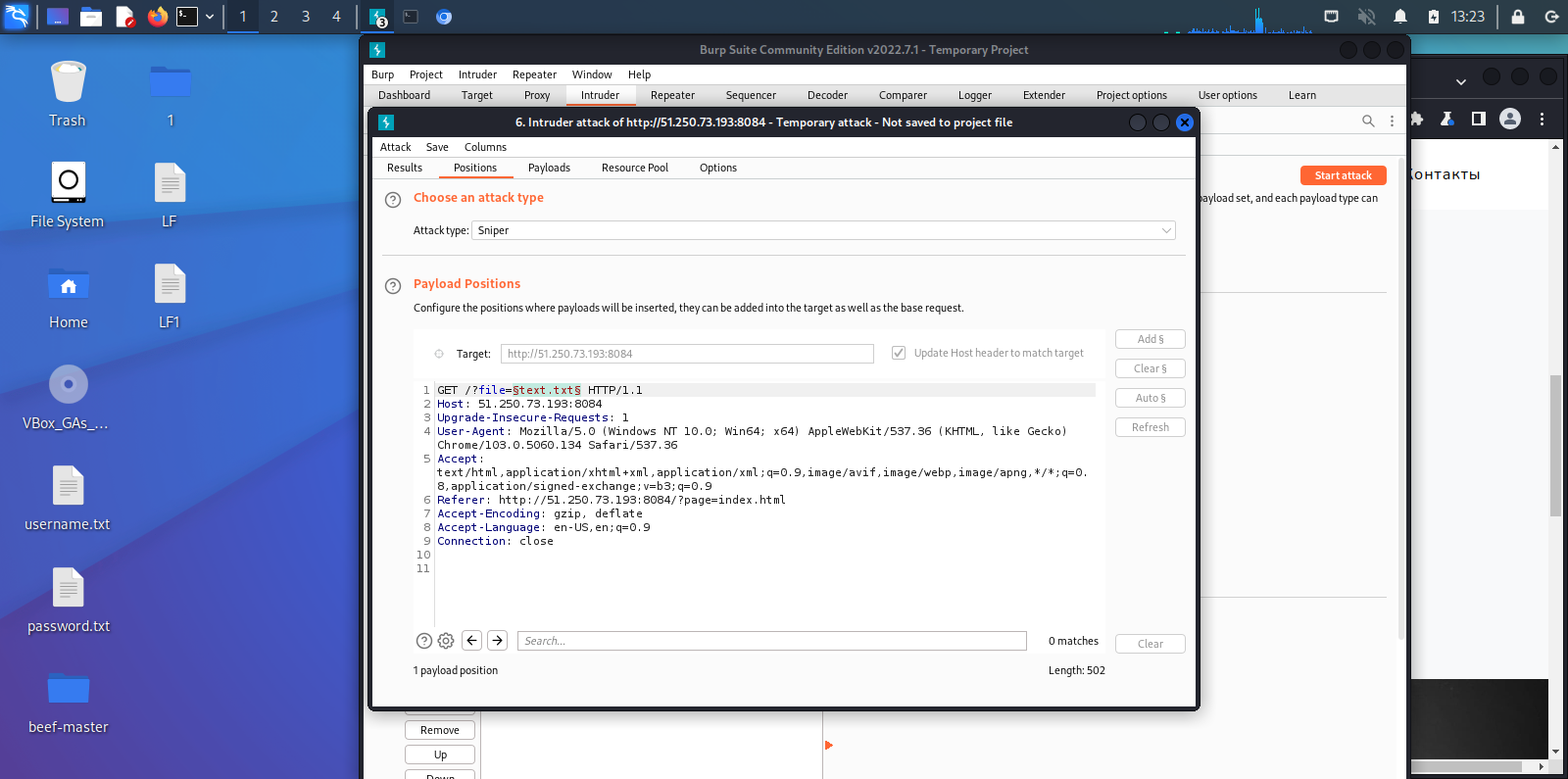


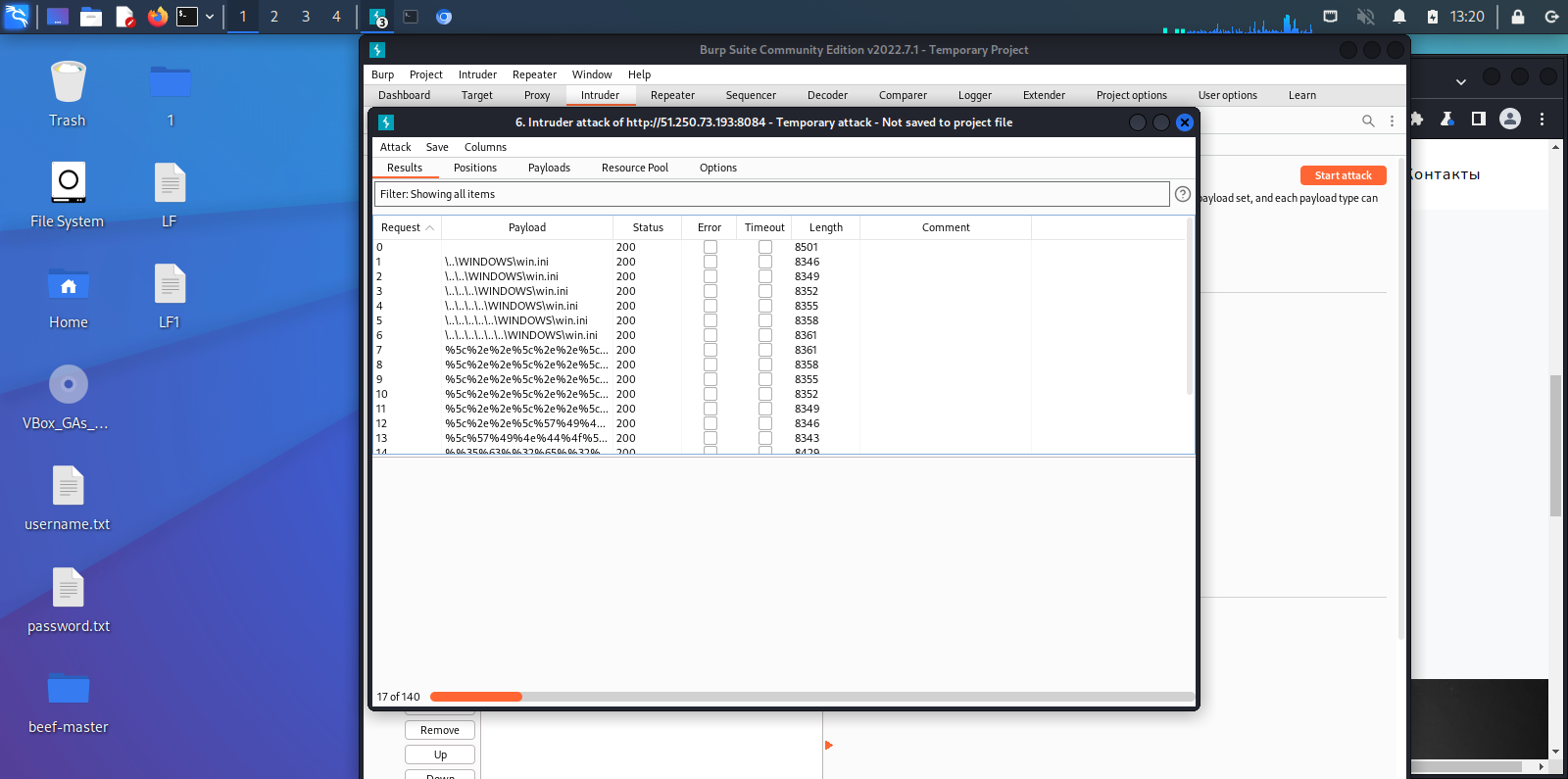
(Intercept is off).

Далее на закладке HTTP History видим наш запрос:



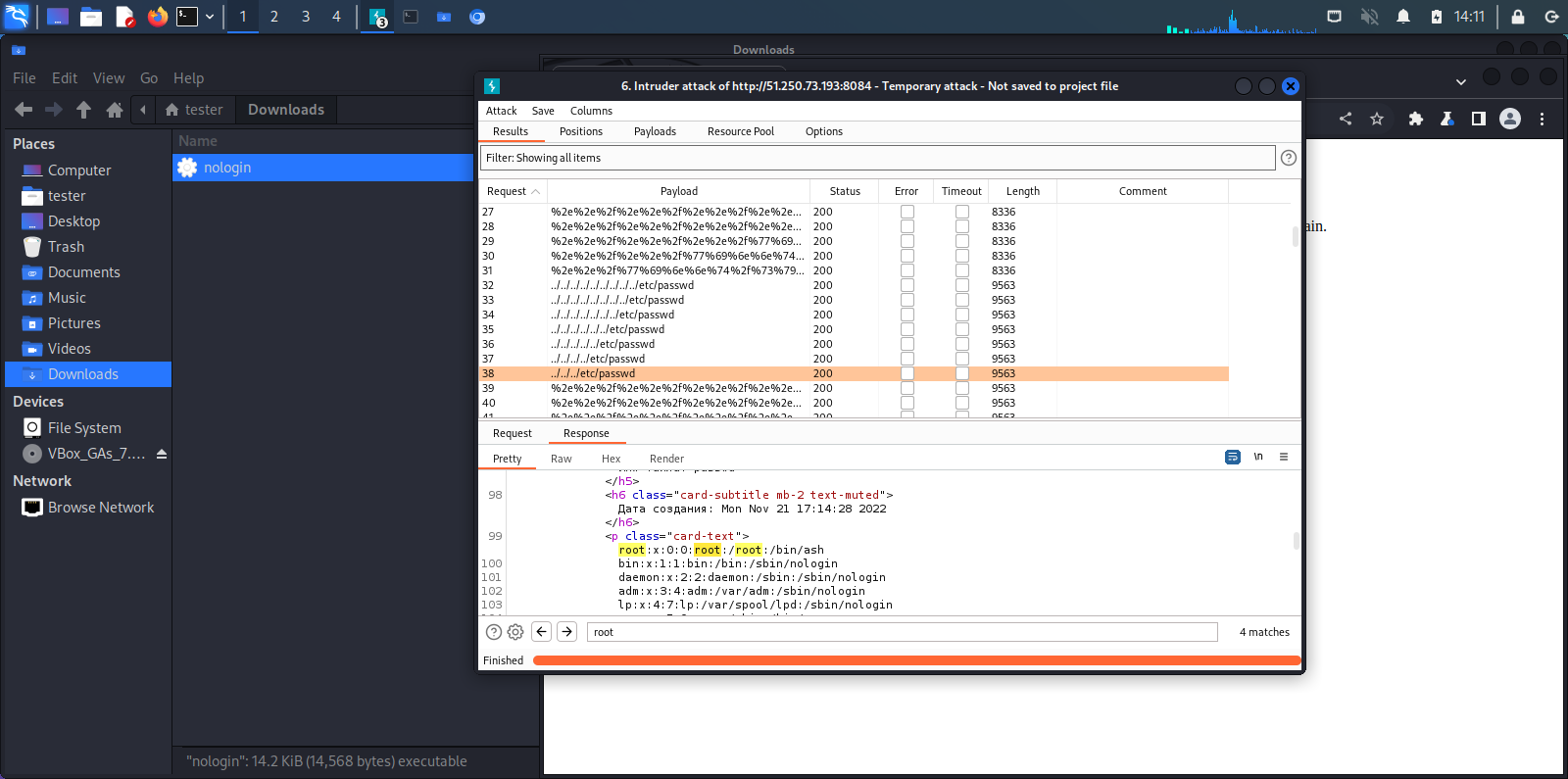
Через контекстное меню выбрала Send to Intruder и зашла на закладку Intruder. Скачала словарь https://github.com/SkillfactoryCoding/HACKER-Webinars-PayloadsAllTheThings/blob/master/Directory%20Traversal/Intruder/directory\_traversal.txt

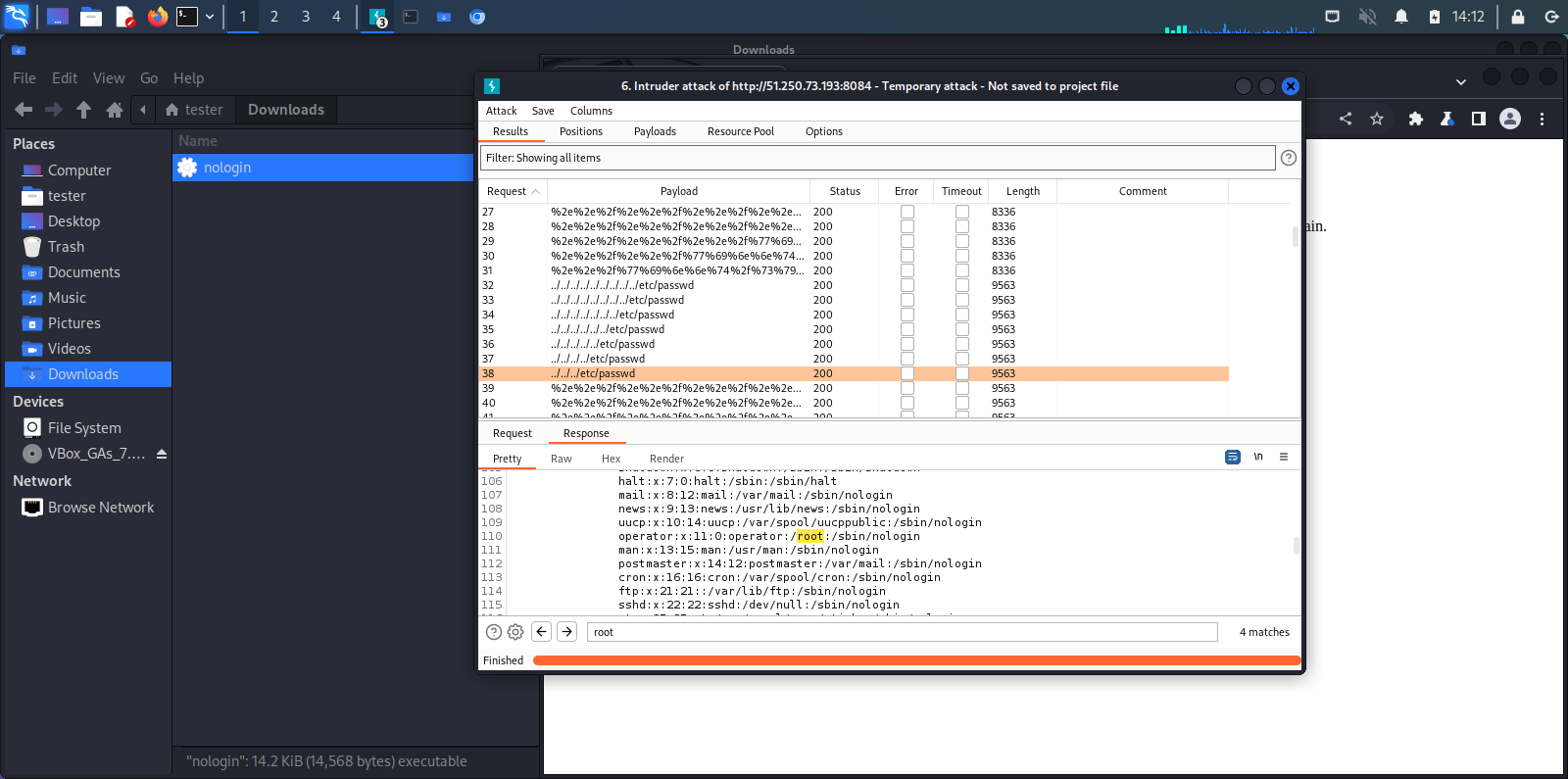




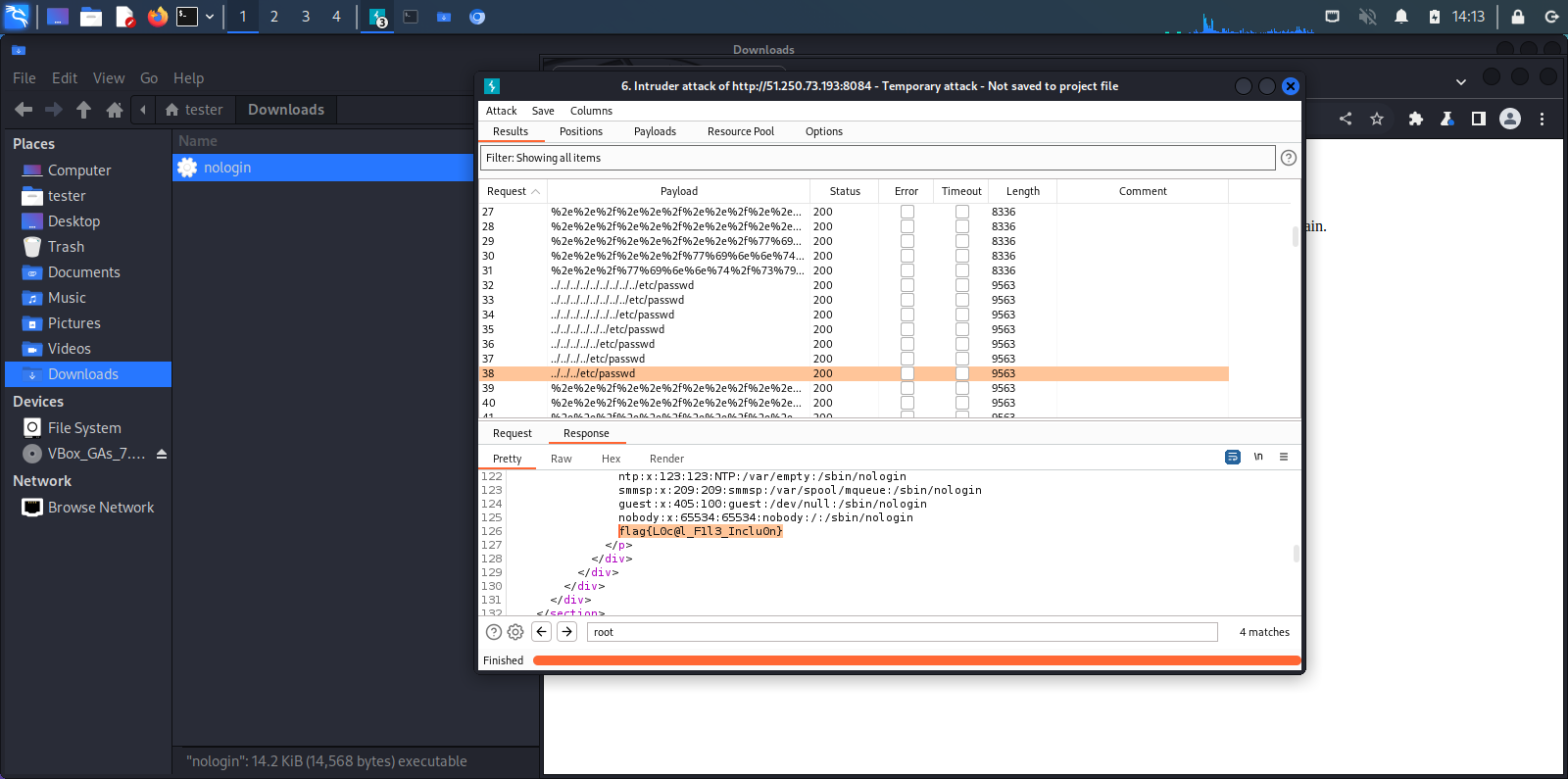
и подключила, выбрала атаку Sniper. Запустила атаку.

В поле поиска ищу в каких директориях словаря встречается слово root. Максимальная частота использования слова root - 4 раза.





Посмотрела в директории /../../etc/passwd, где встретилось 4 раза root, пролистала вниз в поисках флага и нашла. Флаг: flag{L0c@l\_F1l3\_Inclu0n}



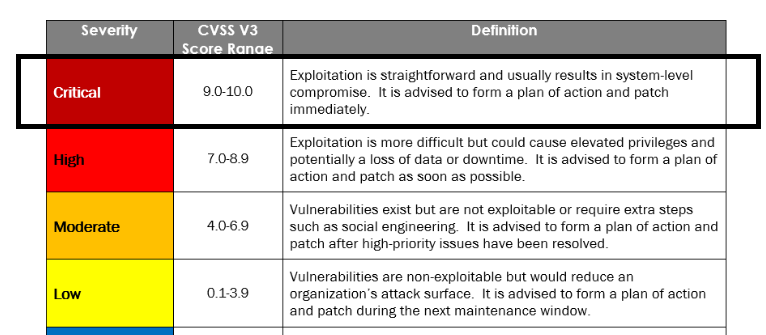
**Вопросы для самопроверки:**

* для декодирования использовала Burp Suite, а остальное-ручное исследование кода
* совет по защите кода: cуть уязвимости кроется в некорректной (небезопасной) обработке пользовательского ввода, поэтому чтобы не допустить такого на своих веб-приложениях следует использовать:

аргументом функции могут быть только числа (0-9) и буквы (a-z), в то время как все остальные символы не принимать и не обрабатывать;

ограничить права API одним каталогом (набором каталогов), таким образом получится избежать выхода из текущего каталога.

* Мне кажется уязвимость высокой опасности 9.0.10.0 по шкале:



## **Security Misconfiguration.** Задание 15.7.2:

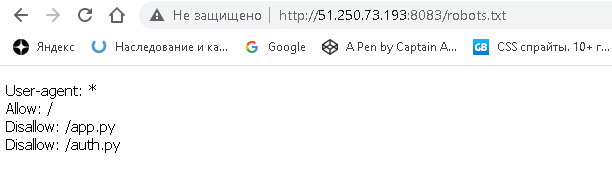
Любой уважающий себя сервис начинает с аутентификации и авторизации, мы знаем как безопасность важна для наших клиентов. Проверьте, удастся ли вам найти наши супер секретные коды.

* Общая информация:
  + Период тестирования: 11.12.2022
  + Объект тестирования: [http://51.250.73.193:8083](http://51.250.73.193:8083/)
* Описание действий:

Сканирую директории с помощью <https://github.com/SkillfactoryCoding/HACKER-WebPentest-pidrila>

Просматриваю конфиги.

Добавляю у url robots.txt:

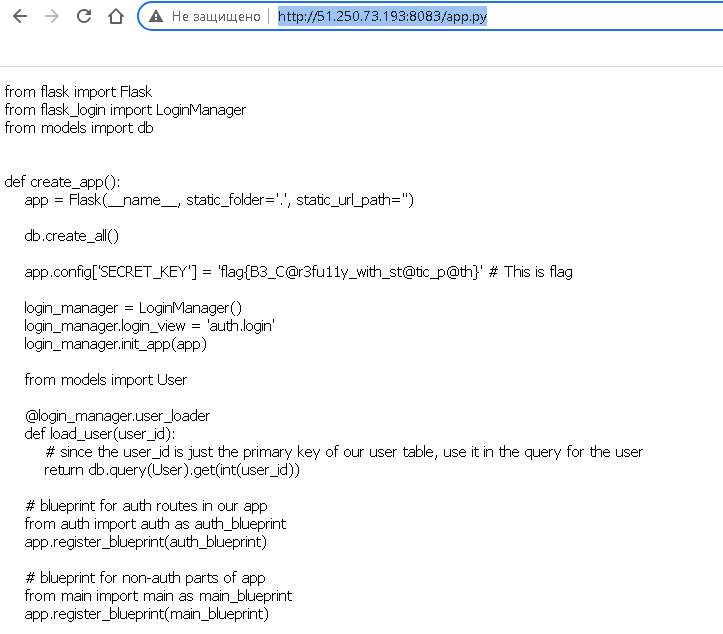


Просматриваю каждый файл на наличие флага, добавляя в урл auth.py, потом app.py.

Введу в адресную строку

<http://51.250.73.193:8083/app.py>

Получаю



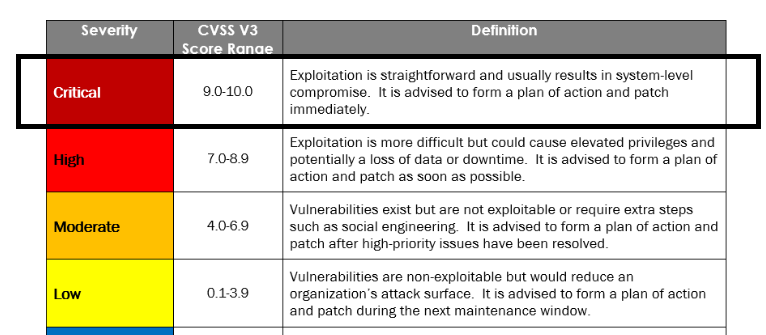
flag{B3\_C@r3fu11y\_with\_st@tic\_p@th}

**Вопросы для самопроверки:**

* для декодирования использовала Pidrila, а остальное-ручное исследование кода
* совет по защите кода:

1. проводить ревизию конфигов приложения (не оставлять учётные данные в конфигах, если такое возможно, внимательно отнестись к тому, что закомментировано или что включено по умолчанию),
2. настроить редиректы со стандартных страниц (например, приветственная страница apache),
3. отключить вход пользователей по умолчанию (например, admin:admin),
4. ограничить права пользователя и службы, от чьего имени работает приложение и его компоненты (плохо: веб-сервер и база данных работает от имени администратора; хорошо: у каждого компонента свой пользователь с максимально ограниченными правами, которых достаточно для полноценного функционирования приложения),
5. постоянно обновлять компоненты приложения.

* Мне кажется уязвимость высокой опасности 9.0.10.0 по шкале:



### Задание 15.6.1

Вы нашли *RCE*, и выполнили команду id на *Linux* сервере. Сервер вернул очень большой (объёмный) ответ, например, ~ 10 мбайт. Опишите, с помощью поиска каких слов (регулярок) вы будете искать успешно выполненную команду (например, в *BurpSuite*, либо в сыром трафике, либо в самом браузере, либо как-то иначе). **Решение: grep id <file>**

### Задание 15.6.2

Вы нашли *RCE*, и выполнили команду dir на *Windows* сервере. Сервер вернул очень большой (объёмный) ответ, например, ~ 10 мбайт. Опишите, с помощью поиска каких слов (регулярок) вы будете искать успешно выполненную команду (например, в *BurpSuite*, либо в сыром трафике, либо в самом браузере, либо как-то иначе).

**Решение: grep dir <file>**