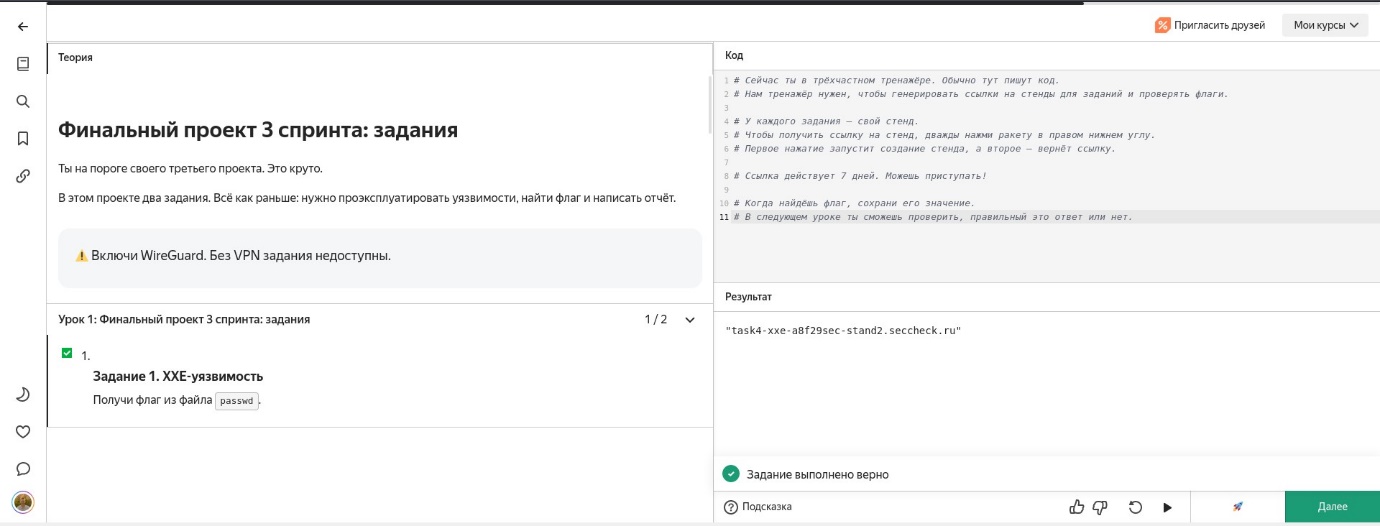
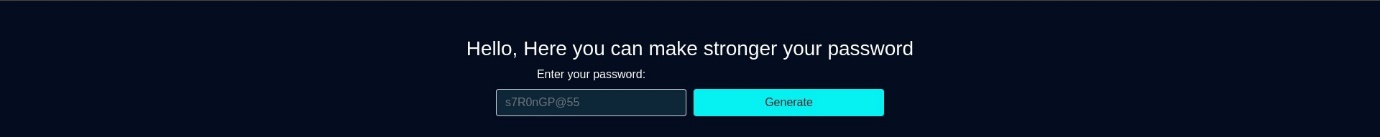
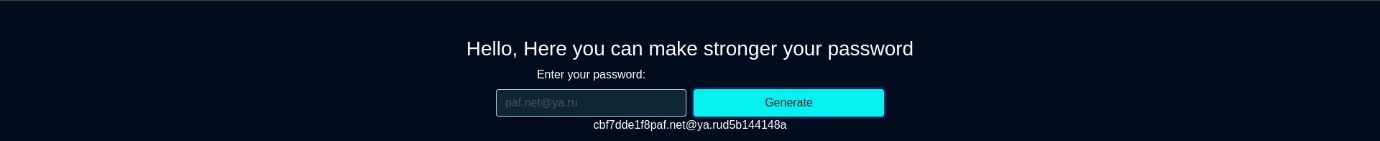
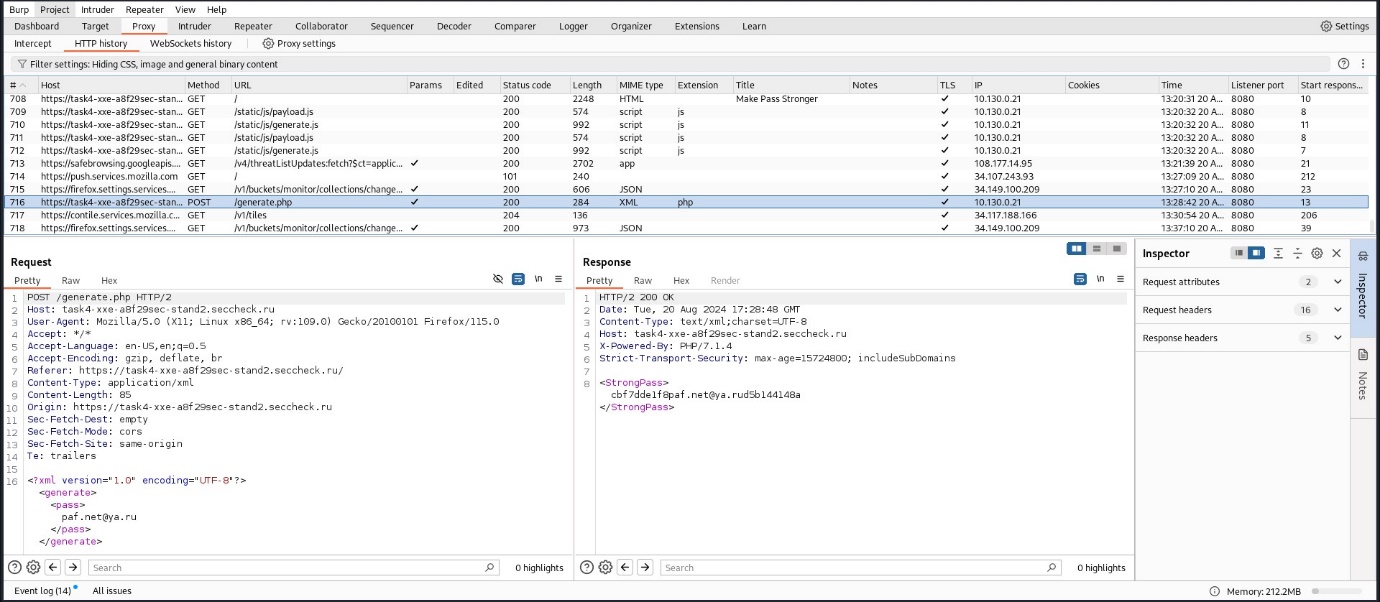
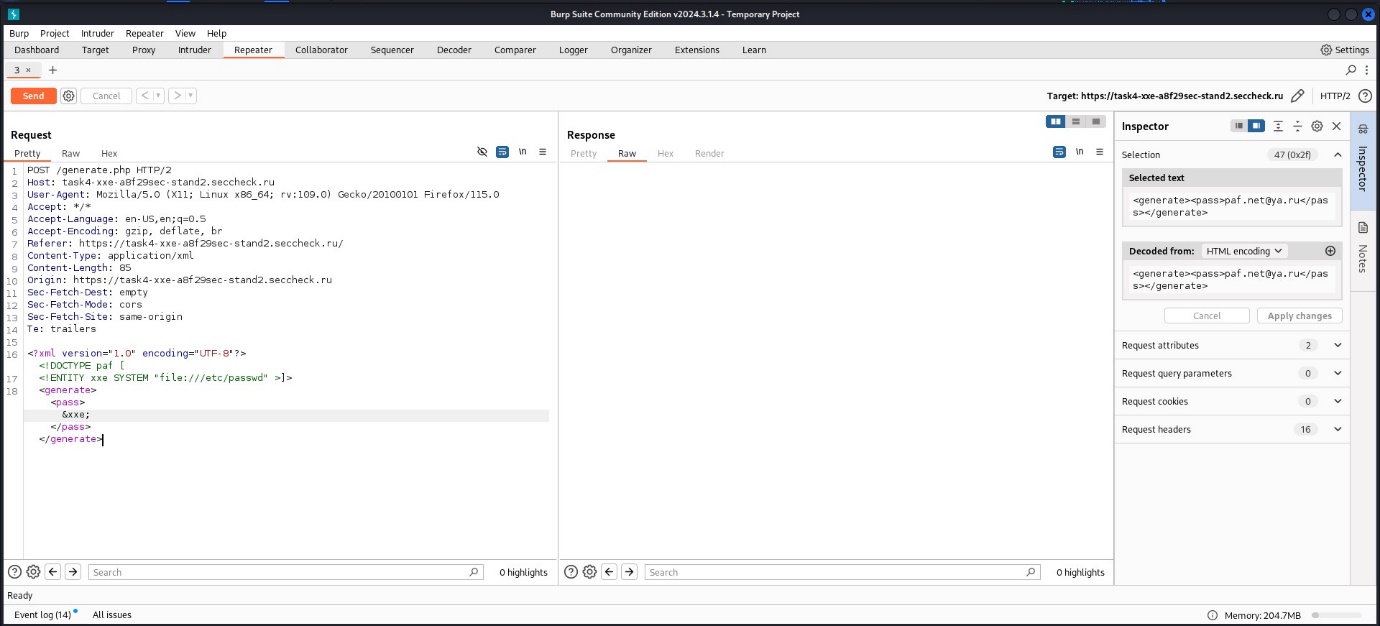
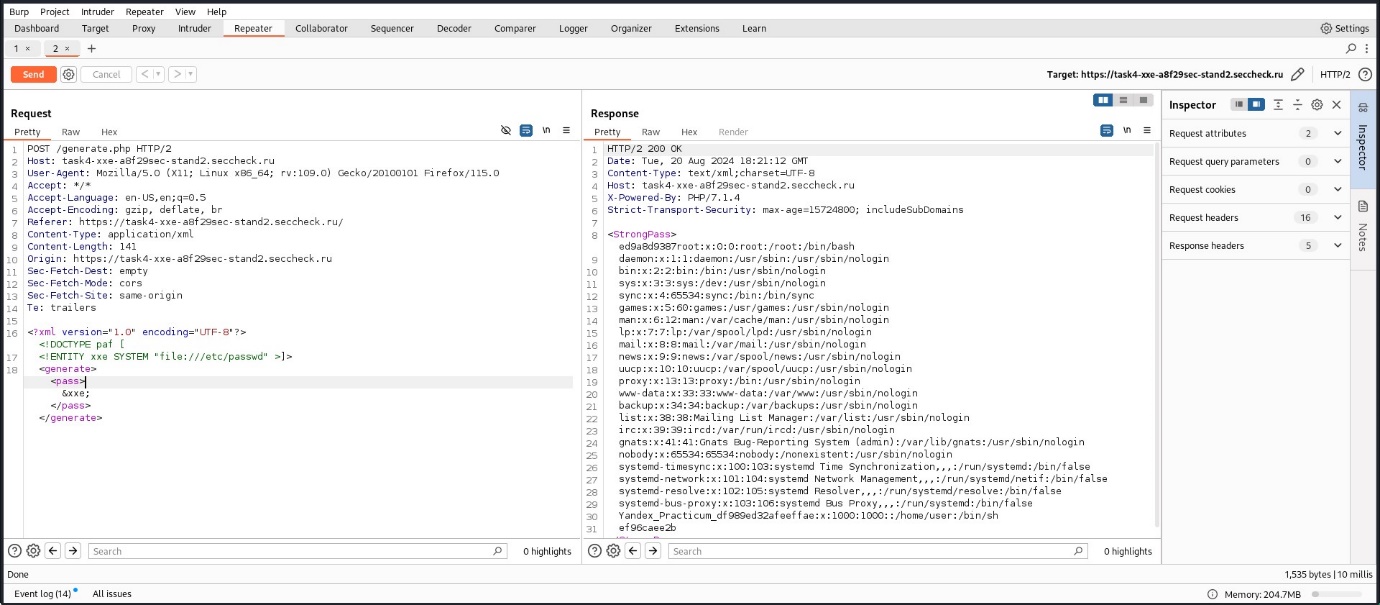
Отчёт выполнения финального проекта 3 спринта

# **Задание 1**

## Флаг: { Yandex\_Practicum\_df989ed32afeeffae }

## Отчёт:

1. Ознакомился с заданием и запустил стенд
2. Открыл в браузере этот сайт и обнаружил там всего одно доступное пользователю поле для ввода пароля 
3. Ввожу произвольный пароль 
4. Затем открываю HTTP history в Burp Suite и вижу, что данные из этого поля методом POST передаются на сайт в формате XML
5. Отправляю этот POST-запрос в Repeater, там добавляю тег DOCTYPE с именем paf, внутри которого будет сущность ENTITY с именем xxe, которая будет заменена содержимым файла passwd 
6. В Burp Suite нажимаю на кнопку Send и приходит ответ с флагом 

Подробно опиши свои действия:

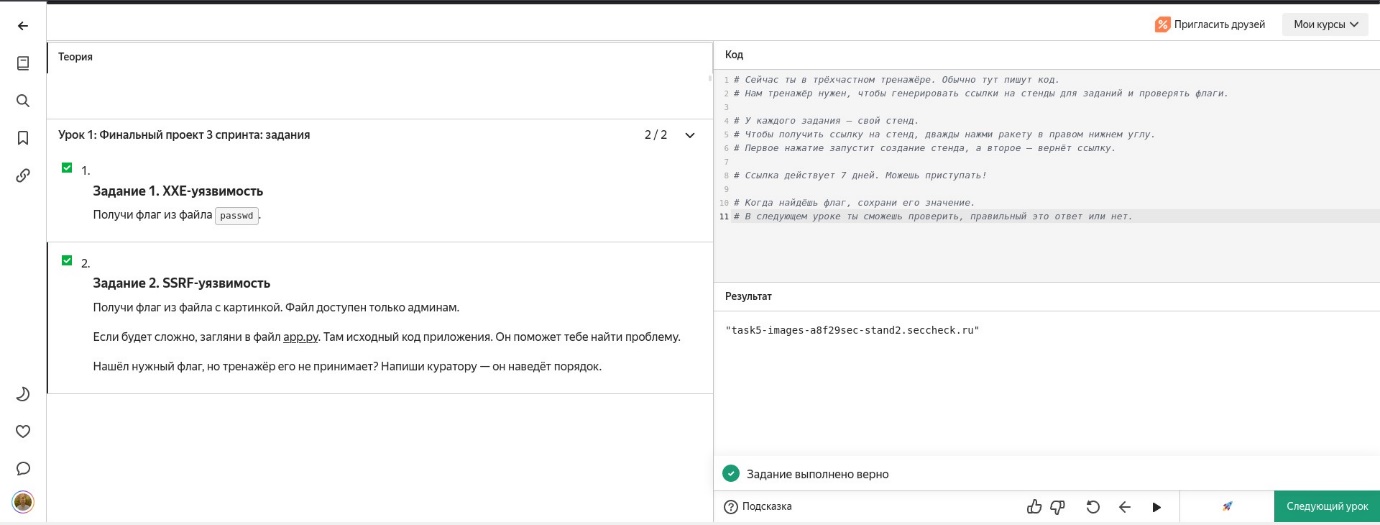
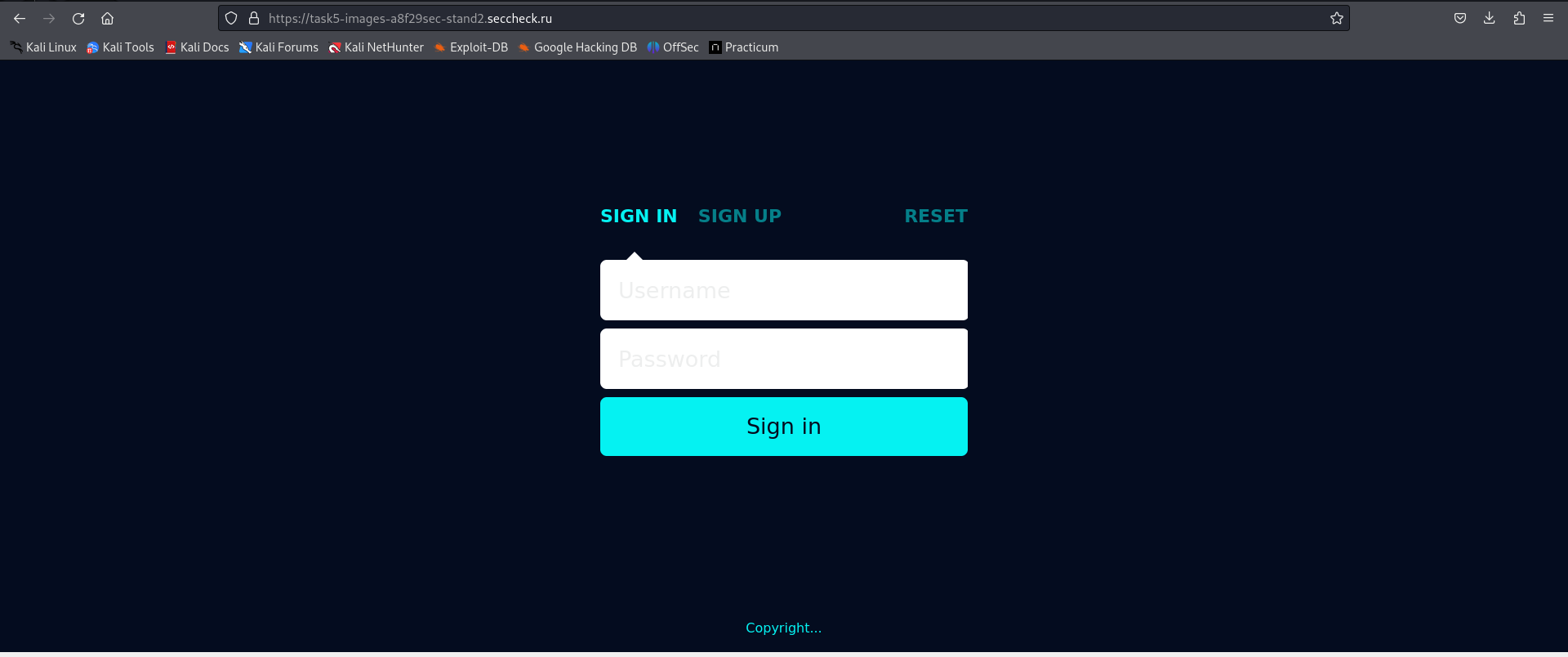
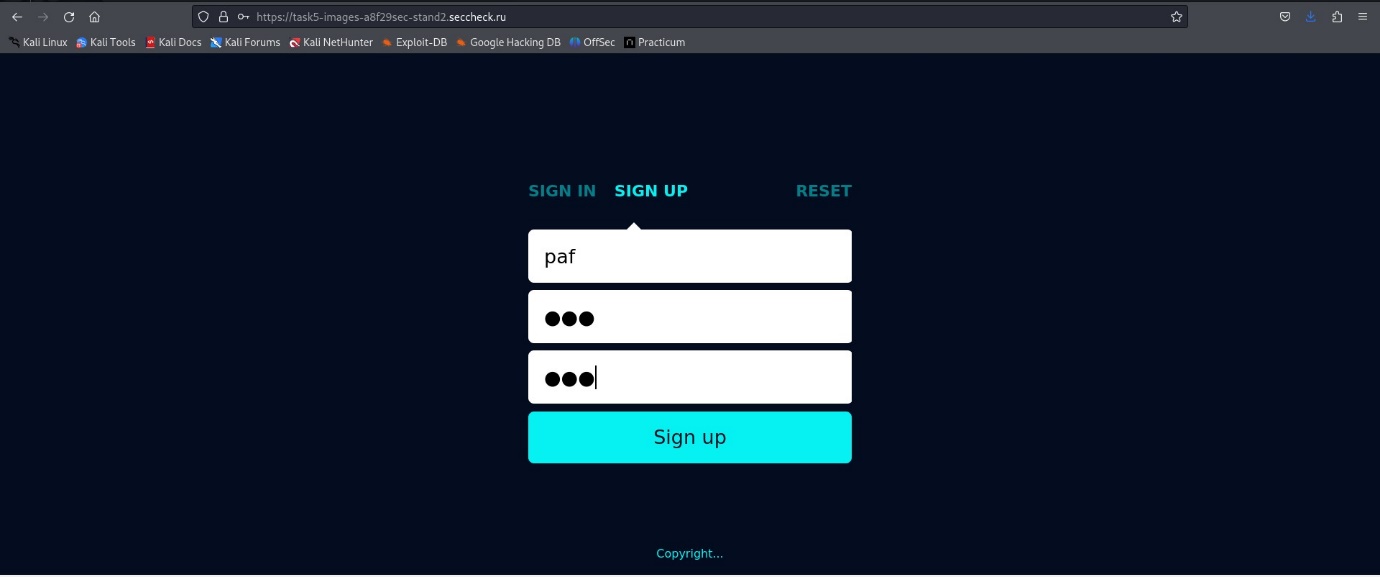
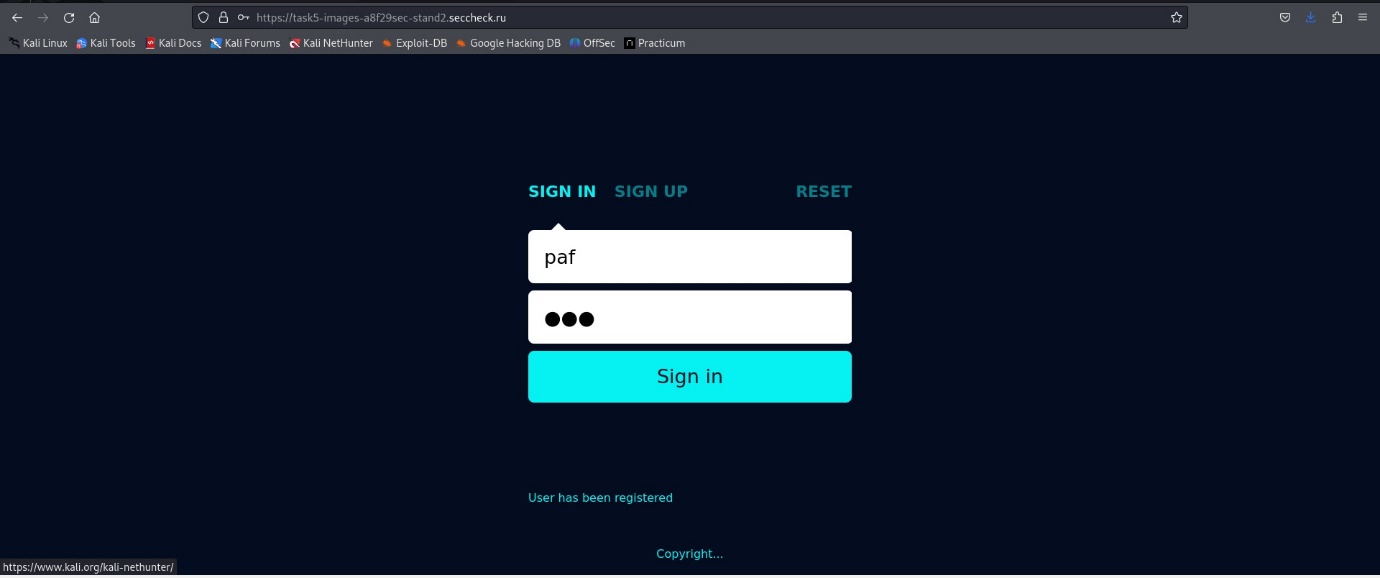
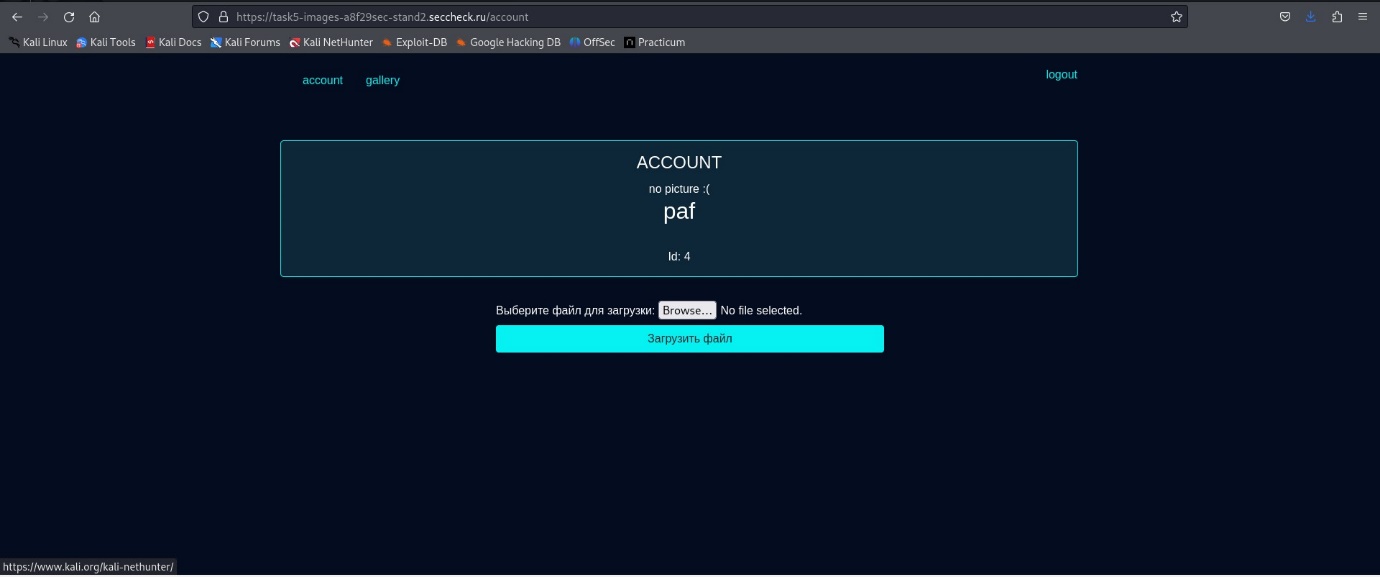
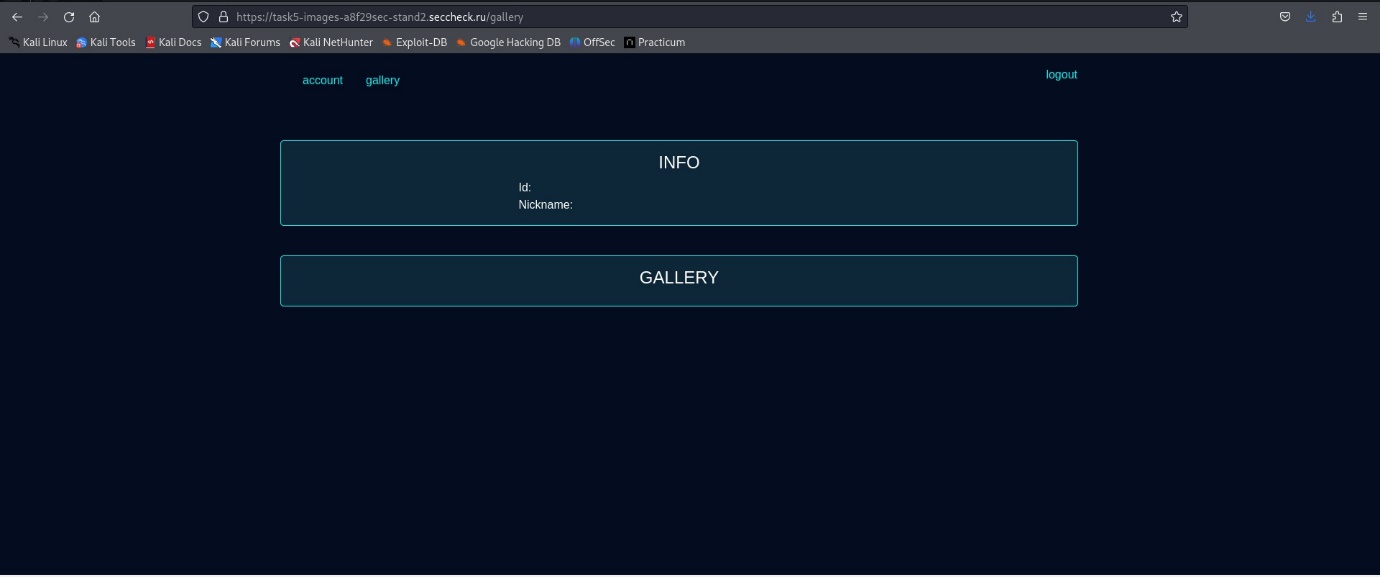
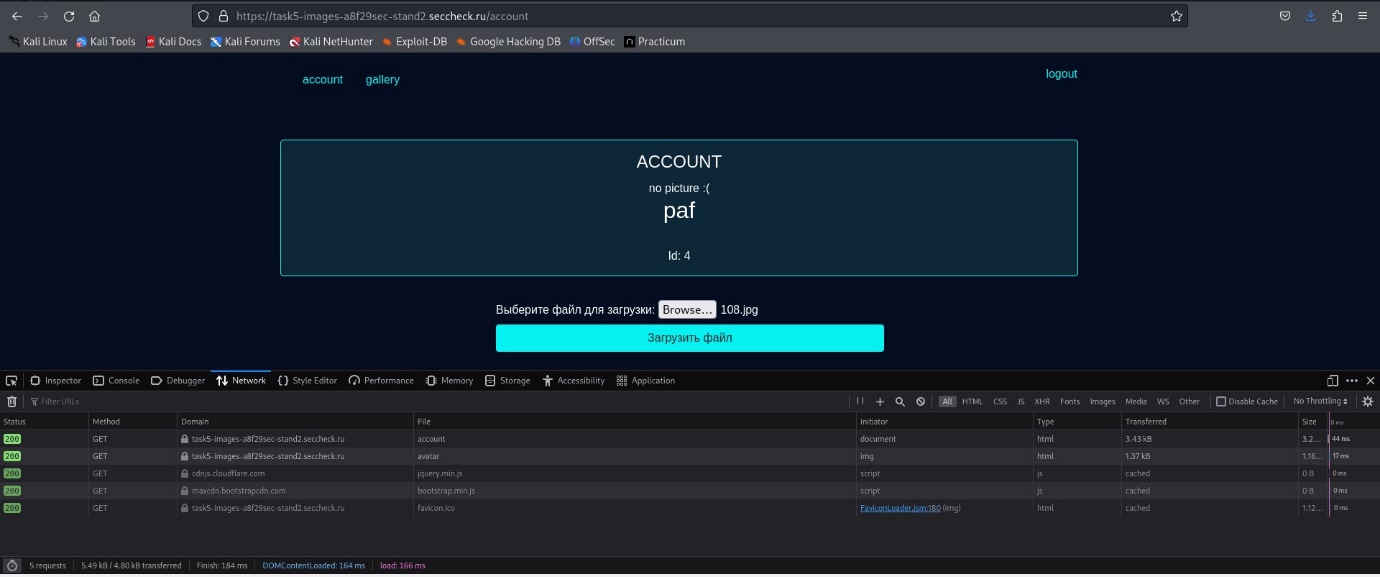
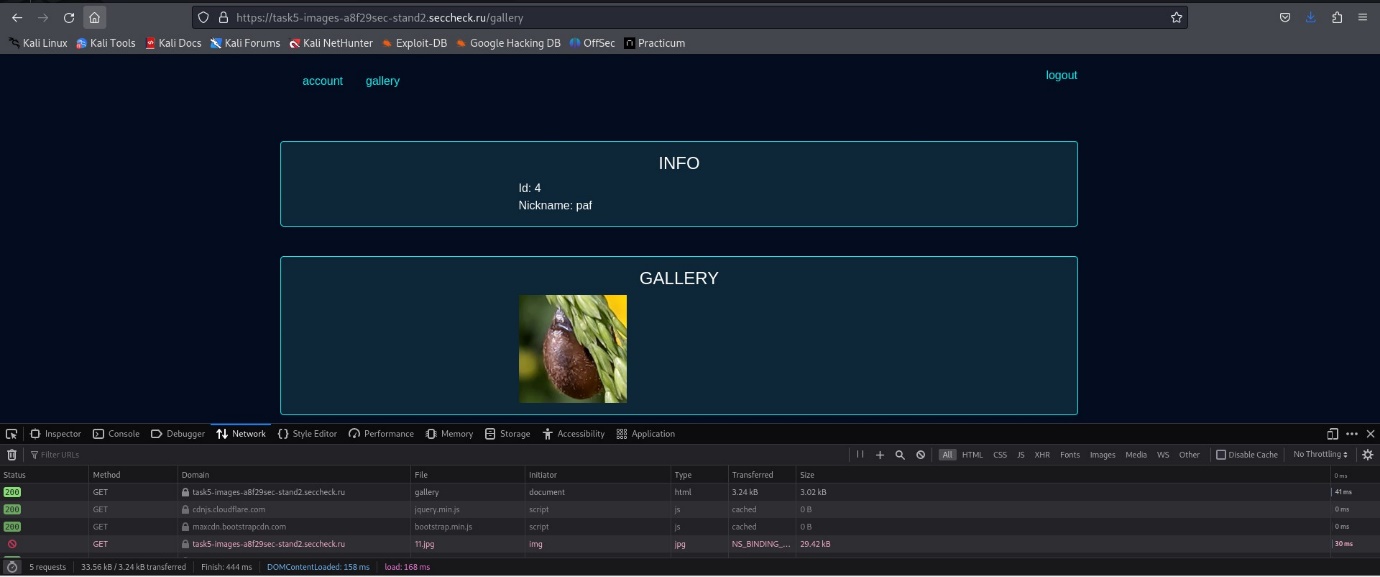
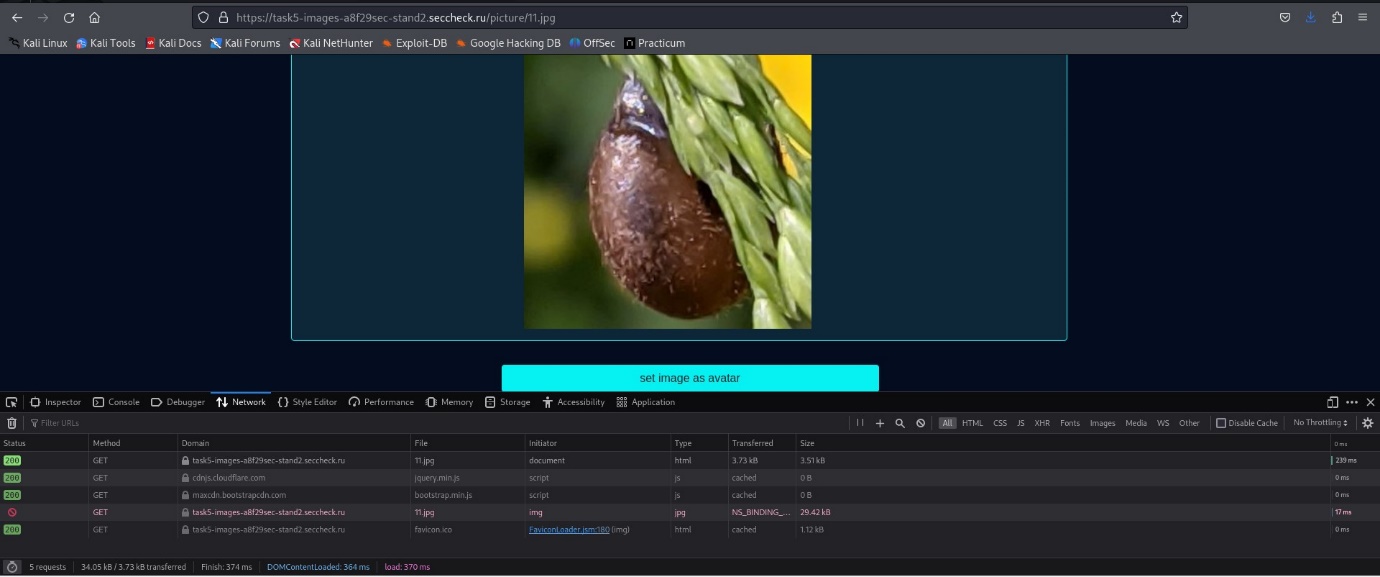
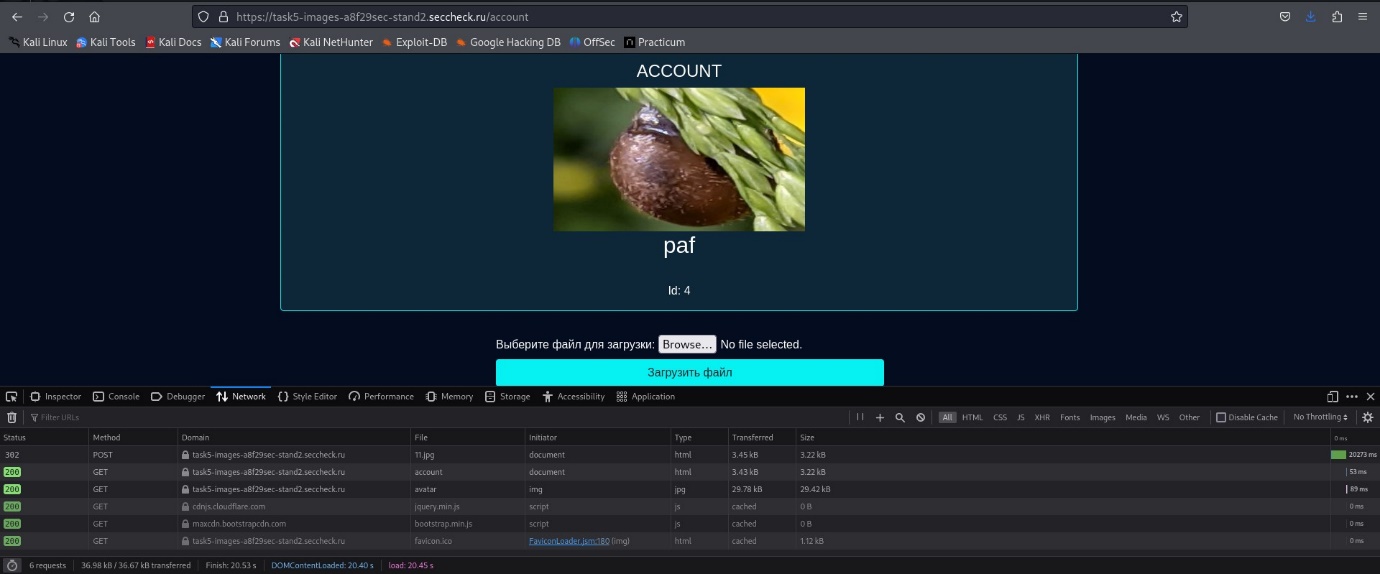
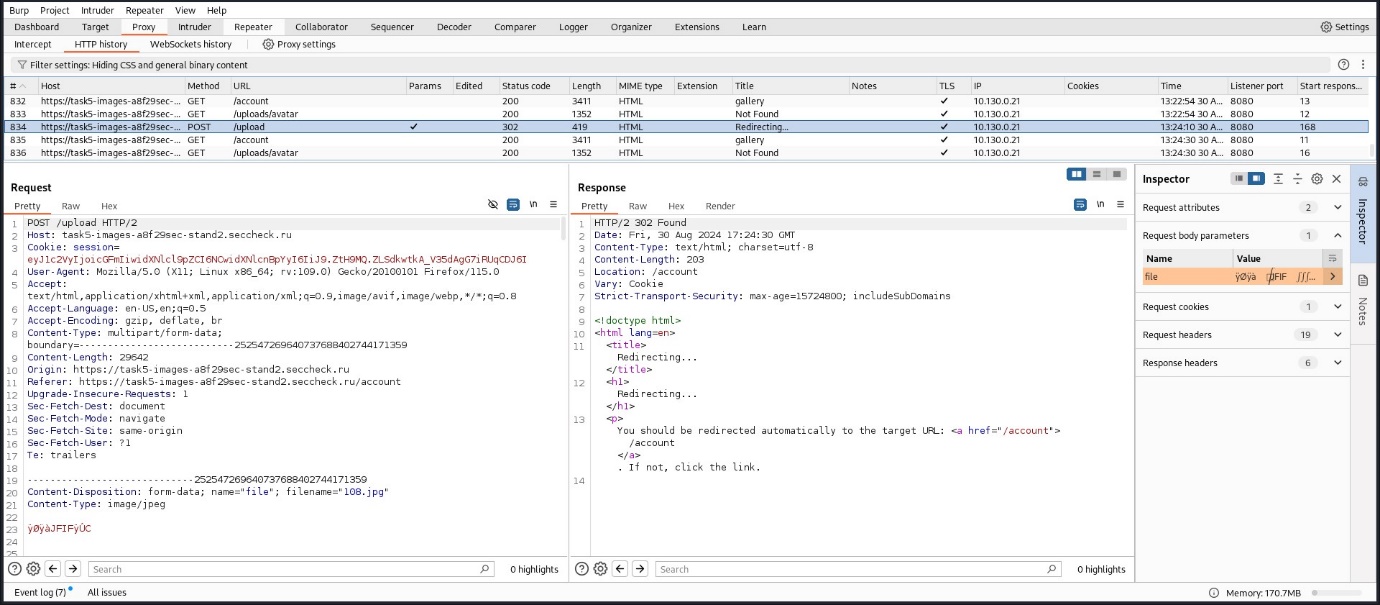
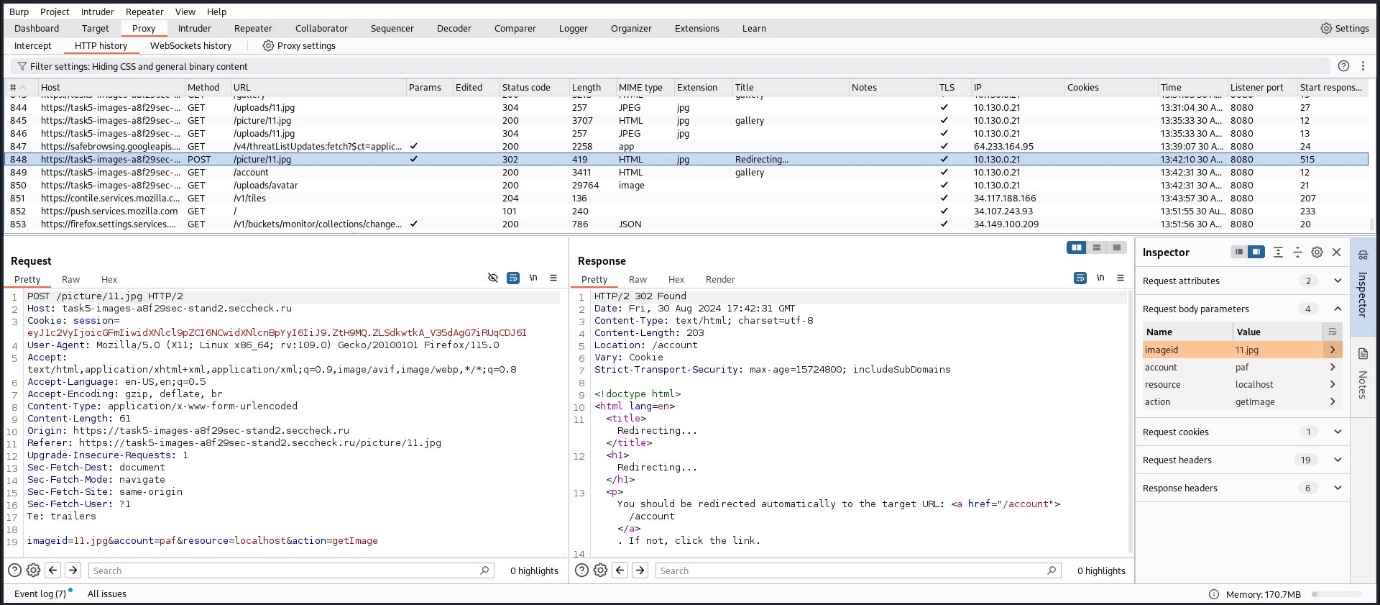
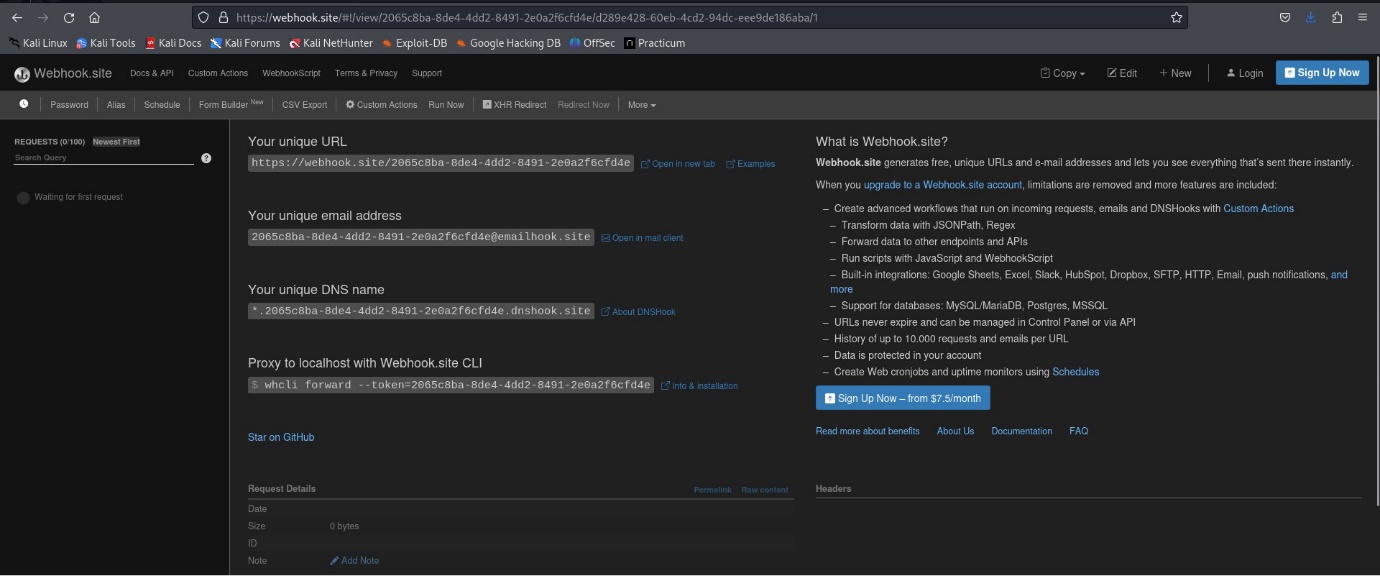
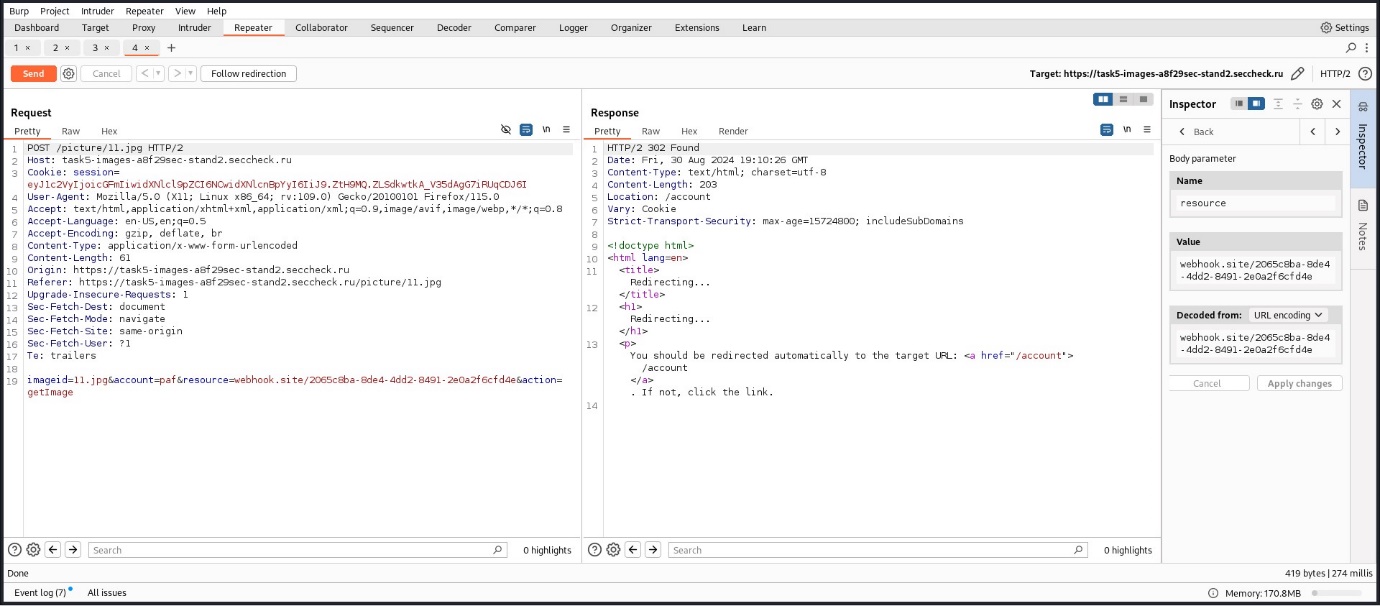
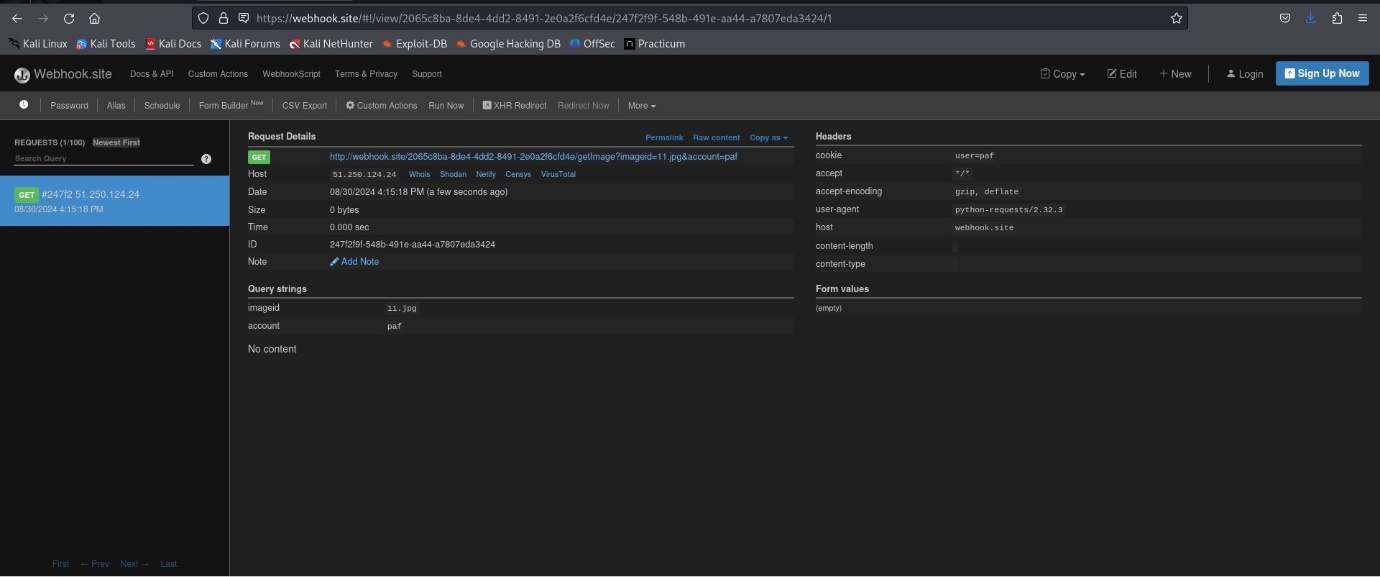
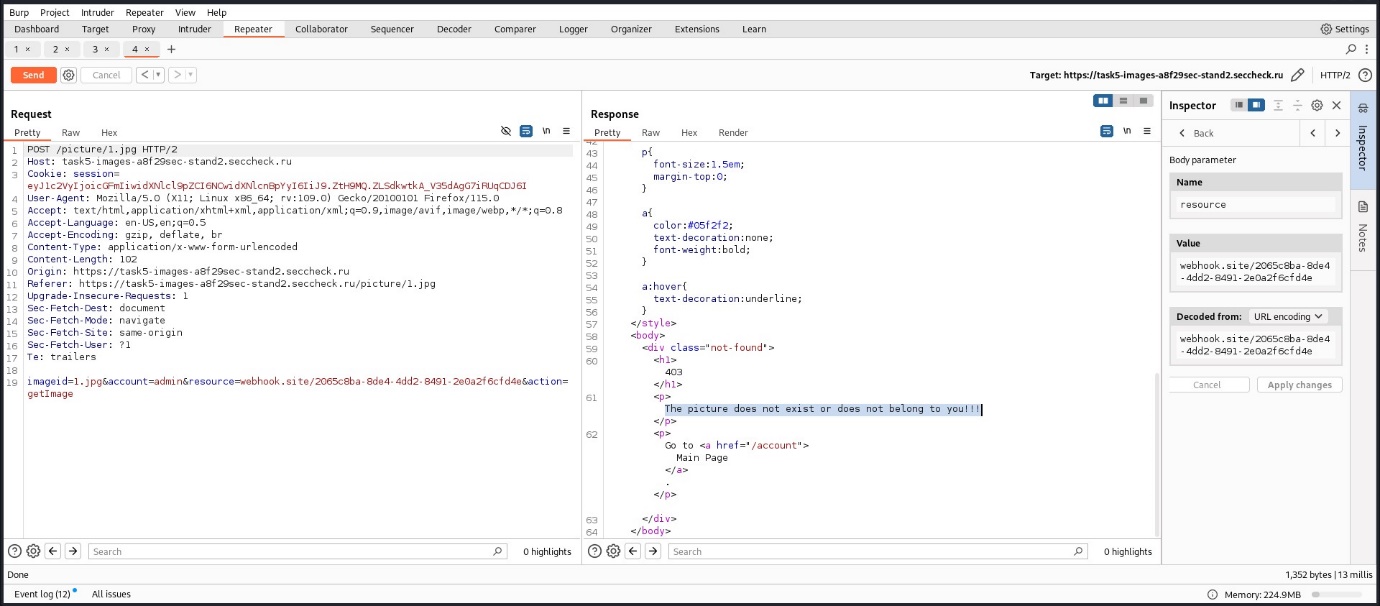
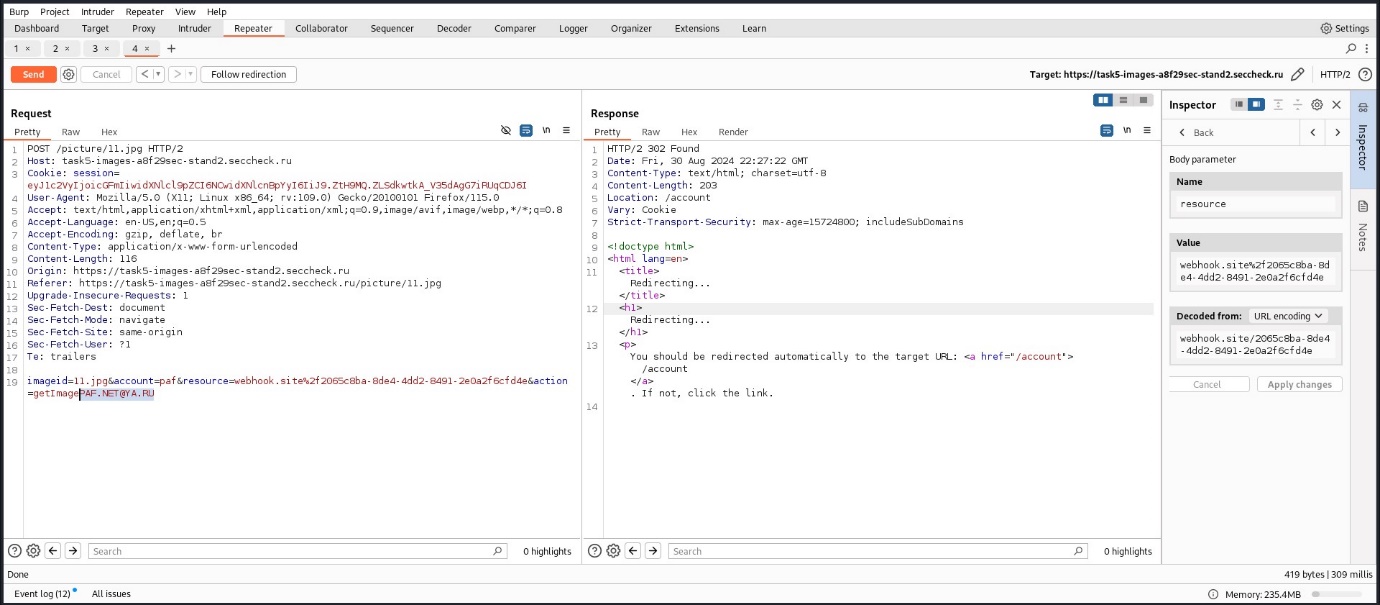
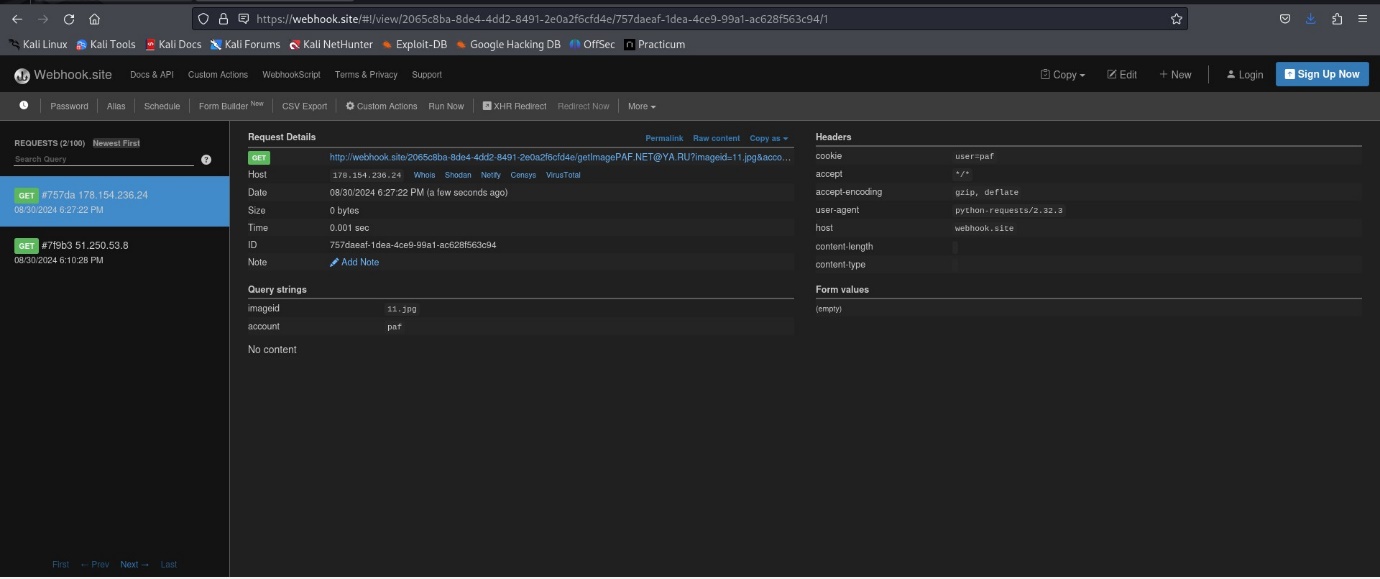
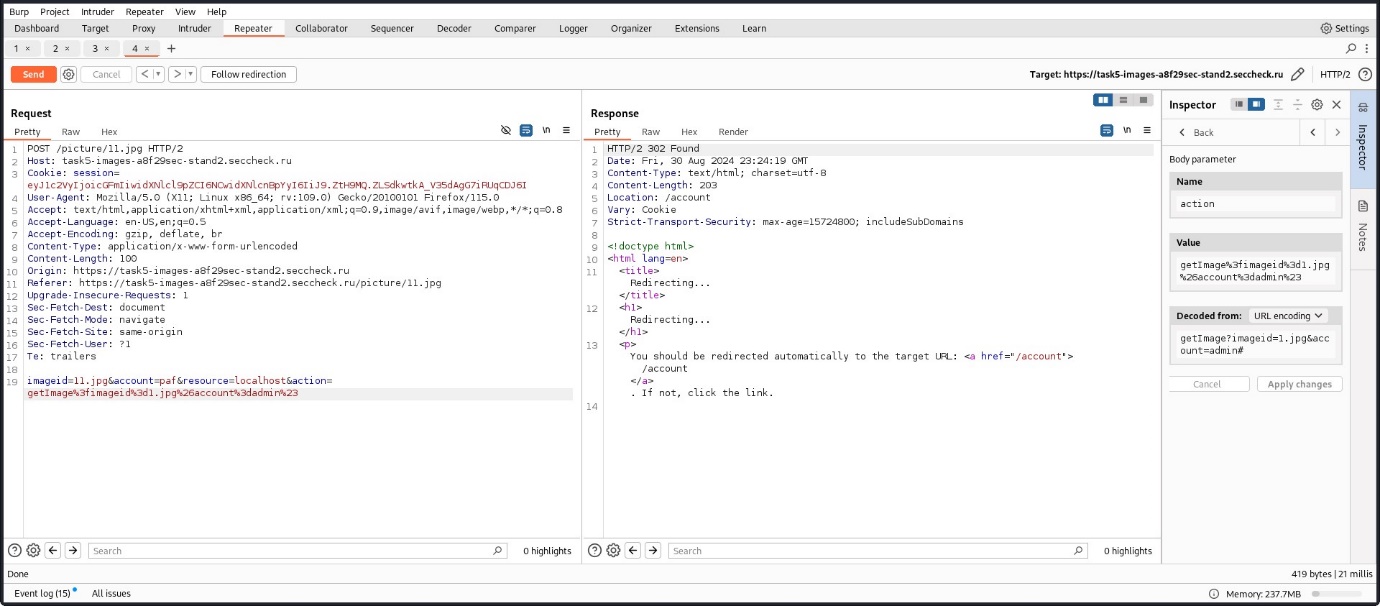
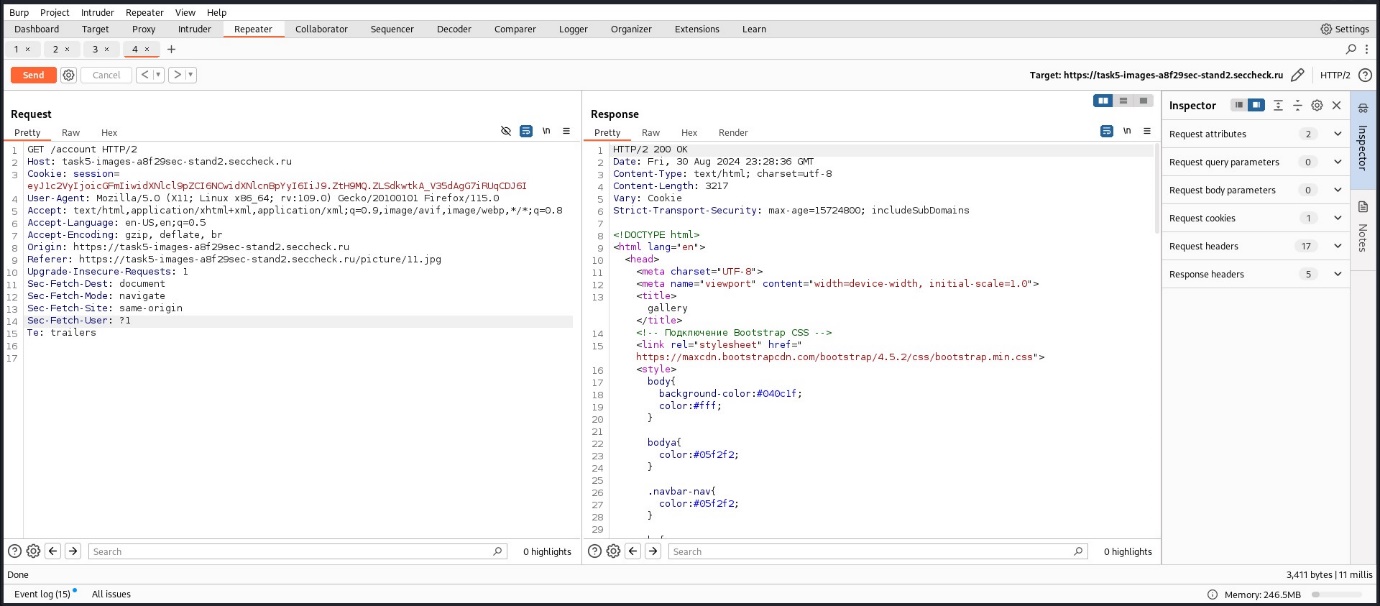
* Что именно сделал — начиная с запуска стенда.
* Что увидел.
* Какие инструменты использовал и чего с ними добился.
* Как удалось получить флаг.

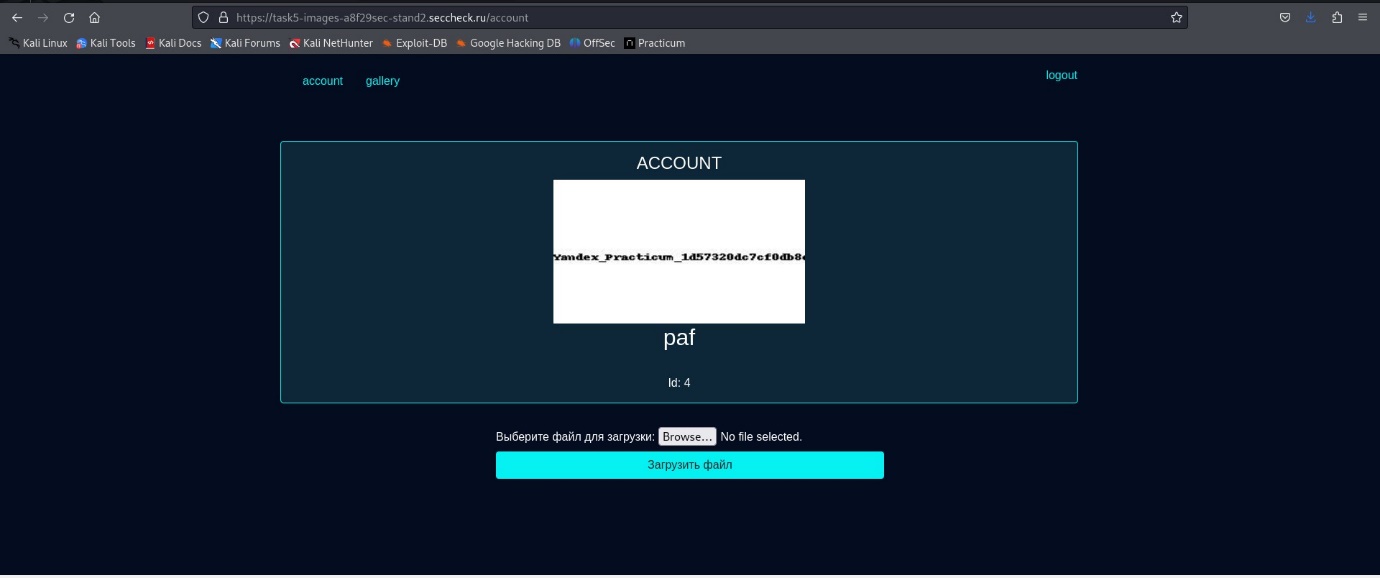
Сделай скриншот каждого действия и приложи его к ответу. Структурируй ответ — опиши каждый шаг, даже если шагов много. Придерживайся правила: один шаг — один скриншот.

# **Задание 2**

## Флаг: { Yandex\_Practicum\_1d57320dc7cf0db8с }

## Отчёт:

1. Ознакомился с заданием и запустил стенд 
2. Открыл сайт в браузере и вижу там уже знакомую форму для авторизации
3. Перешёл на SIGN UP и зарегистрировал нового пользователя
4. Перешёл на SIGN IN и авторизовался на этом сайте 
5. Открылась страница моего аккаунта, на которой есть возможность загрузить файл
6. И есть ссылка на галерею, в которой ничего нет 
7. Перехожу обратно в аккаунт и загружаю файл с изображением 108.jpg
8. Захожу в галерею и вижу там свой файл, но он уже переименован в 11.jpg
9. Открываю 11.jpg, вижу там кнопку установки картинки на аватар
10. Кликаю по этой кнопке и вижу, что аватар успешно применился для моего аккаунта
11. Открыл Burp Suite и увидел там всего два POST-запроса. Сначала это был POST /upload, который содержал в теле только один параметр file со значением в виде большого количества символов
12. А далее шёл POST /picture/11.jpg, который представлял больше интереса для задания по теме SSRF, поскольку содержал параметр resource cо значением localhost и какие-то другие параметры 
13. Теперь следует проверить как сервер отрабатывает такой запрос и как фильтрует параметры. Для этого я воспользовался сервисом webhook.site
14. Указал этот URL вместо значения localhost в параметре resource, отправил запрос и получил ответ с кодом перенаправления 302 Found, который означает, что запрошенный ресурс был перемещён в /account 
15. Перехожу на webhook.site и вижу, что сервером был сформирован и отправлен GET-запрос с параметрами, которые были представлены в POST-запросе - imageid, account, action. Переданы они были таким URL: getImage?imageid=11.jpg&account=paf
16. Поскольку названия файлам с изображениями присваивались по номерам в порядке возрастания и начинались с 2.jpg, то можно предположить, что 1.jpg уже был создан заранее и может содержать флаг. Сделал проверку, заменив значения в параметре imageid на 1.jpg, а в параметре account на admin. Получил ответ с сообщением о том, что изображение недоступно мне:  
    The picture does not exist or does not belong to you!!! 
17. Осталось проверить только параметр action. Для этого я возвращаю параметрам imageid и account первоначальные значения и добавляю к значению параметра action произвольные данные 
18. Перехожу на webhook.site и вижу, что сервером был сформирован точно такой же GET-запрос, но в параметр action попали дополнительные данные
19. Поскольку параметр action не фильтруется должным образом, то в него можно поместить параметры, которые необходимы для получения доступа к файлу с флагом. Для этого я возвращаю в репитере первоначальный запрос, который был передан из HTTP history и в параметр action ставлю значение getImage?imageid=1.jpg&account=admin#  
    где для обозначения фрагмента URL используется символ # 
20. Отправляю запрос с SSRF в параметре action и следую за перенаправлением
21. Перехожу в браузер, обновляю страницу стенда и вижу на ней изображение с флагом



Подробно опиши свои действия:

* Что именно сделал — начиная с запуска стенда.
* Что увидел.
* Какие инструменты использовал и чего с ними добился.
* Как удалось получить флаг.

Сделай скриншот каждого действия и приложи его к ответу. Структурируй ответ — опиши каждый шаг, даже если шагов много. Придерживайся правила: один шаг — один скриншот.