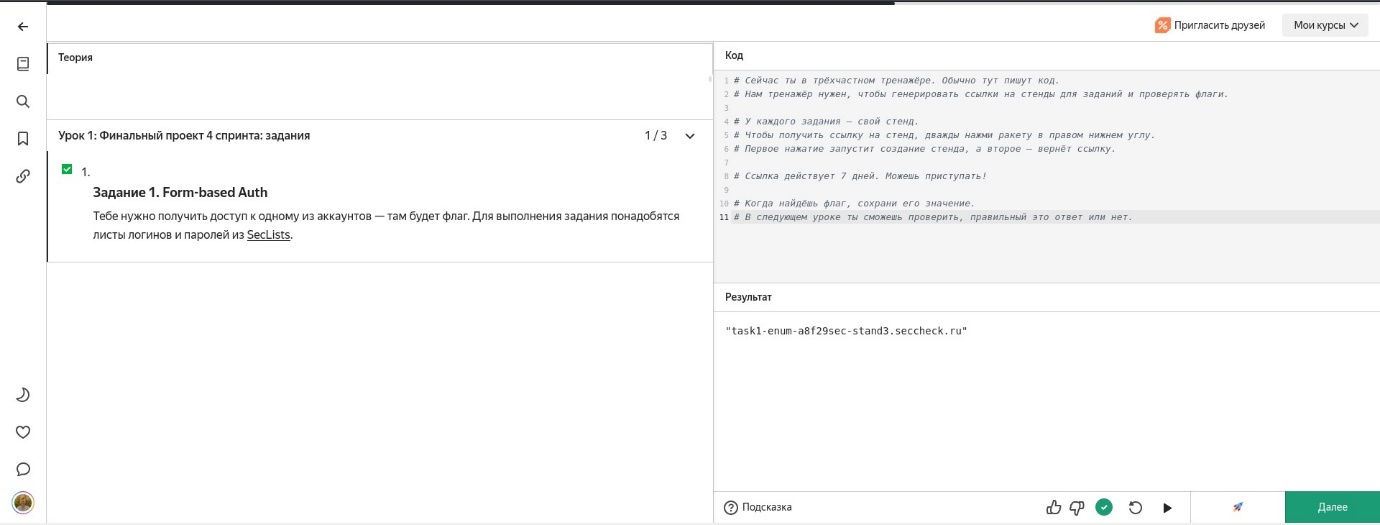
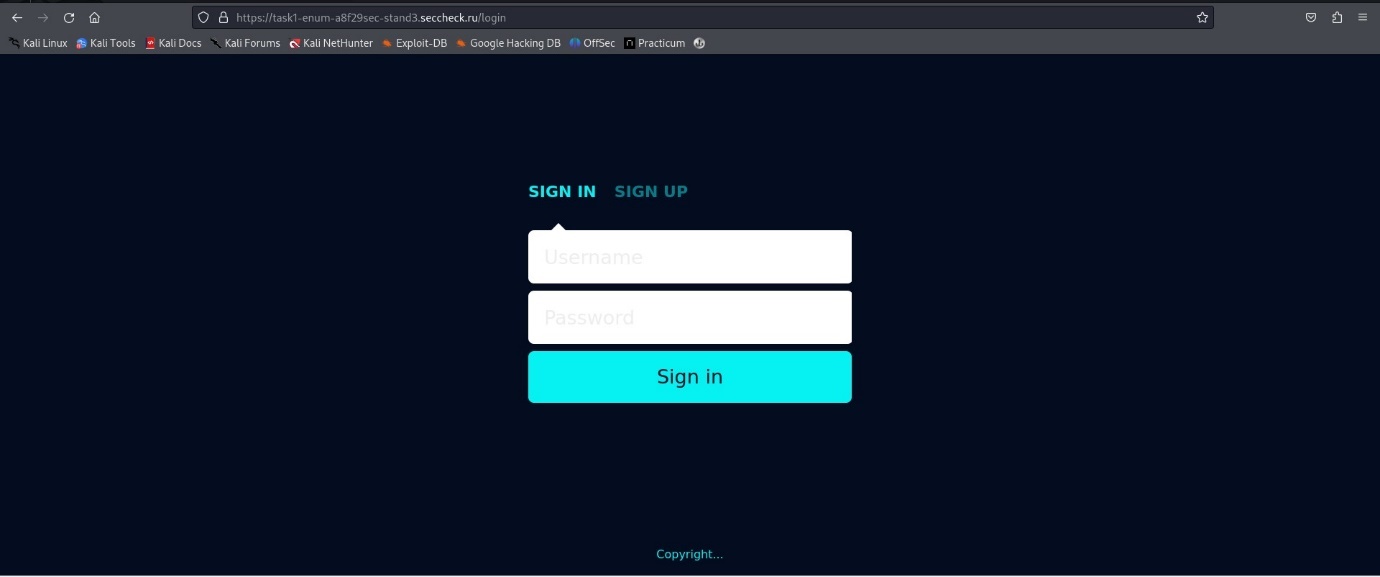
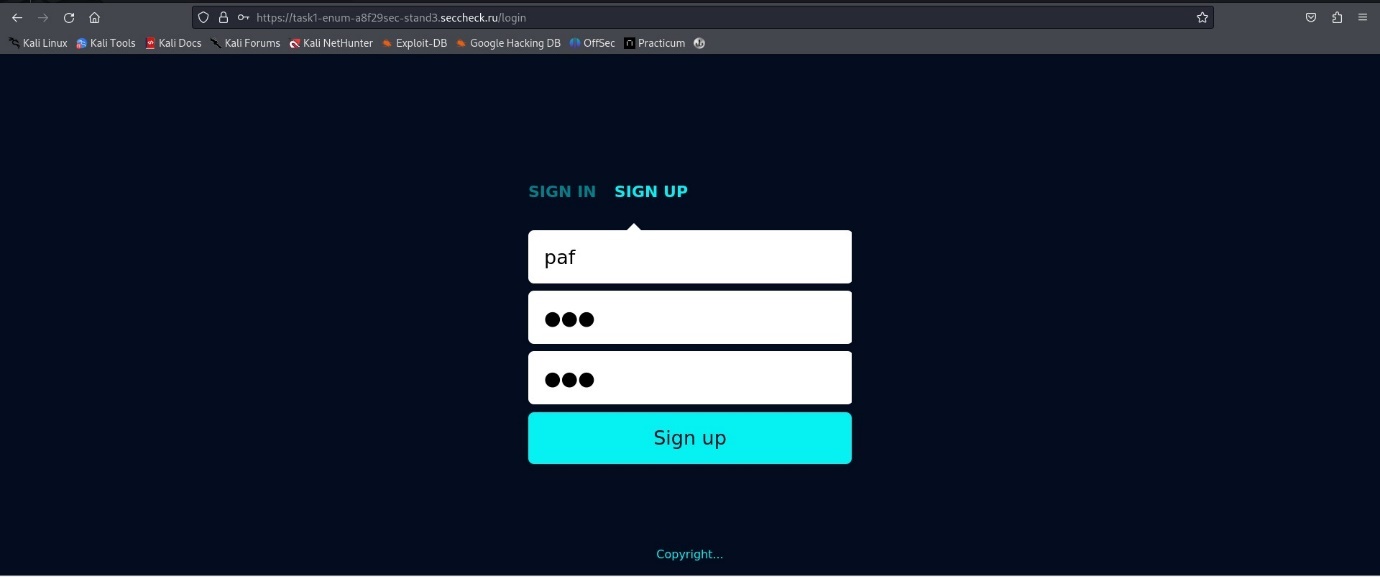
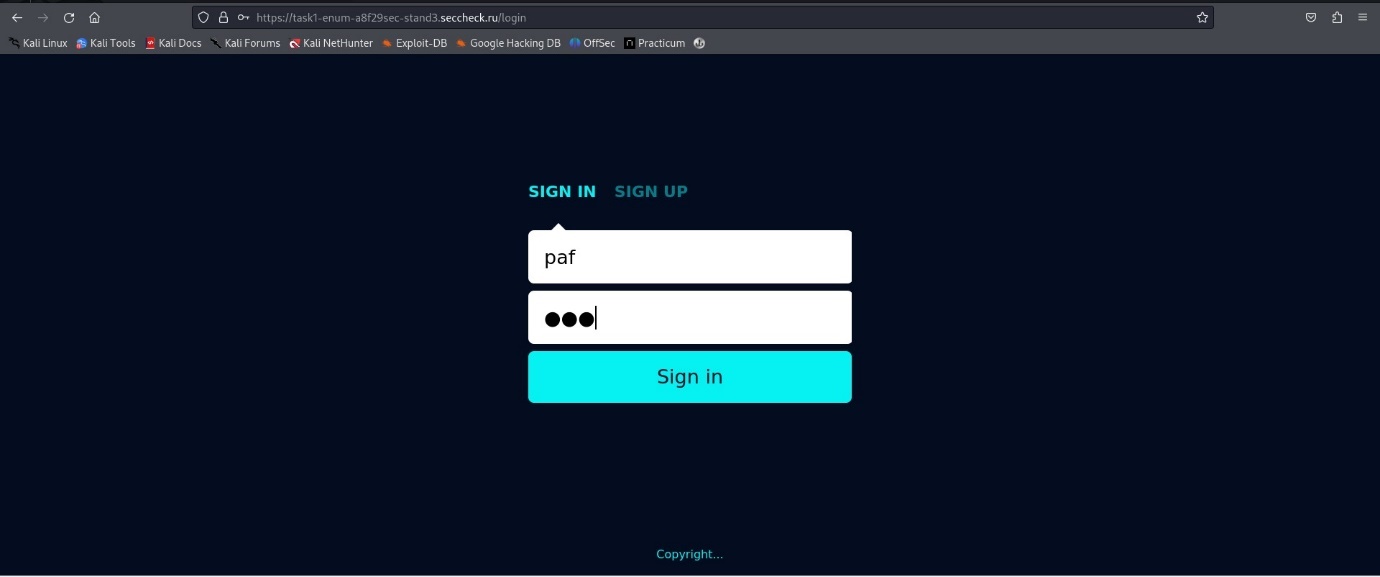
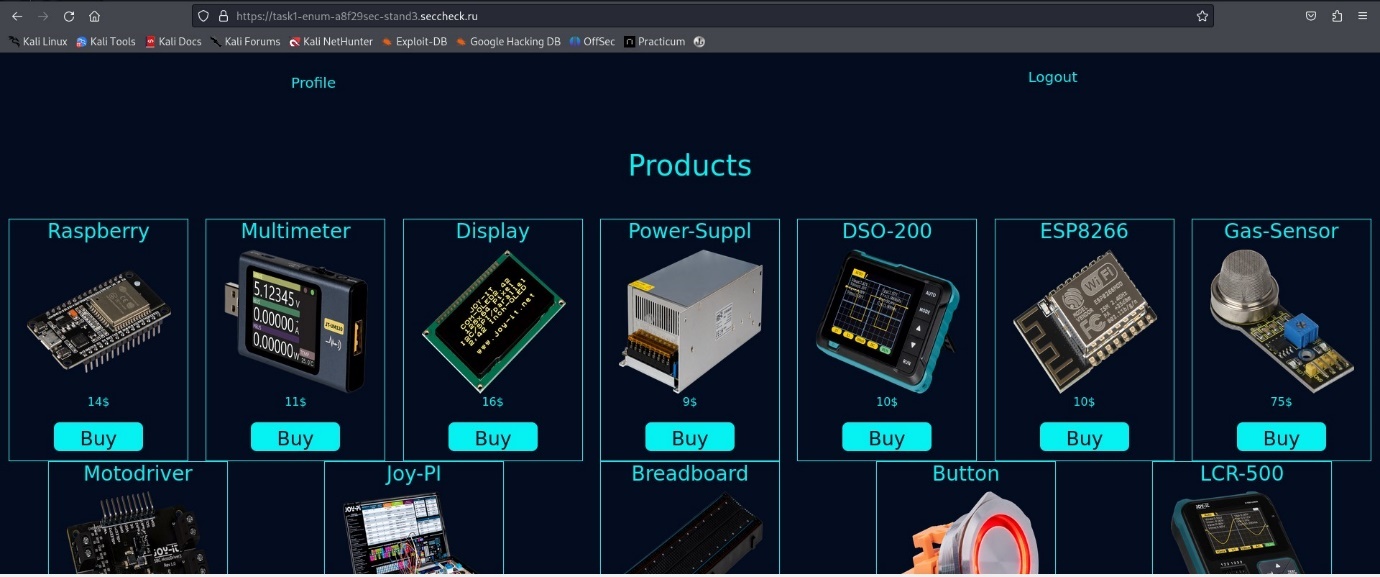
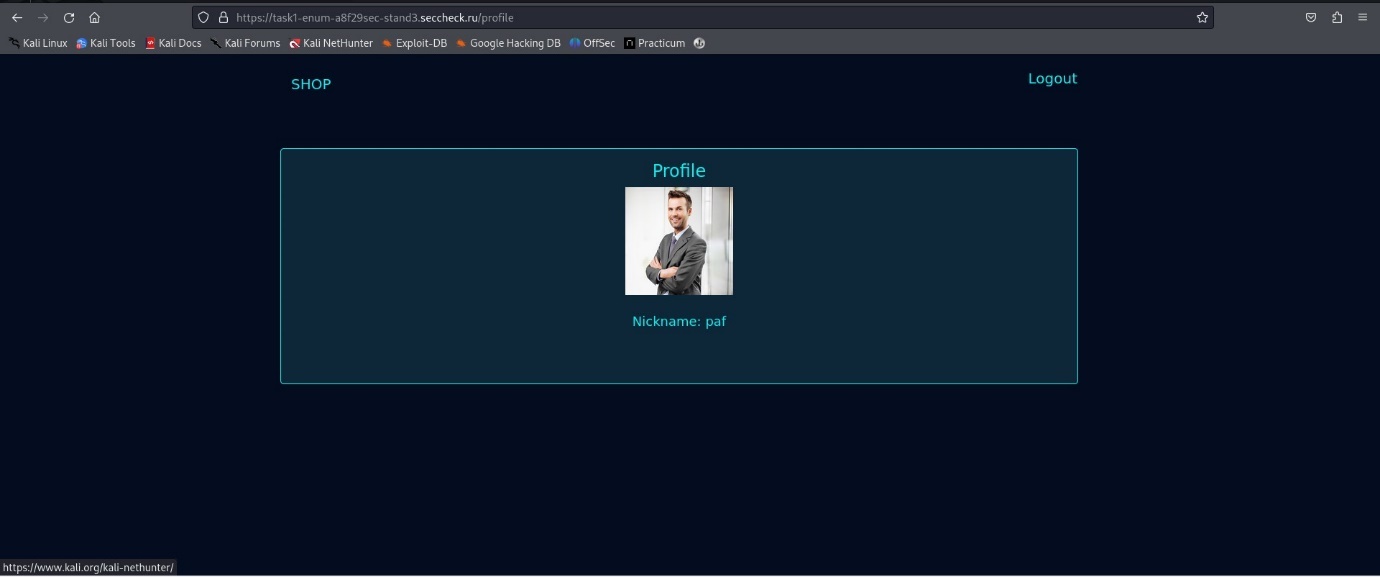
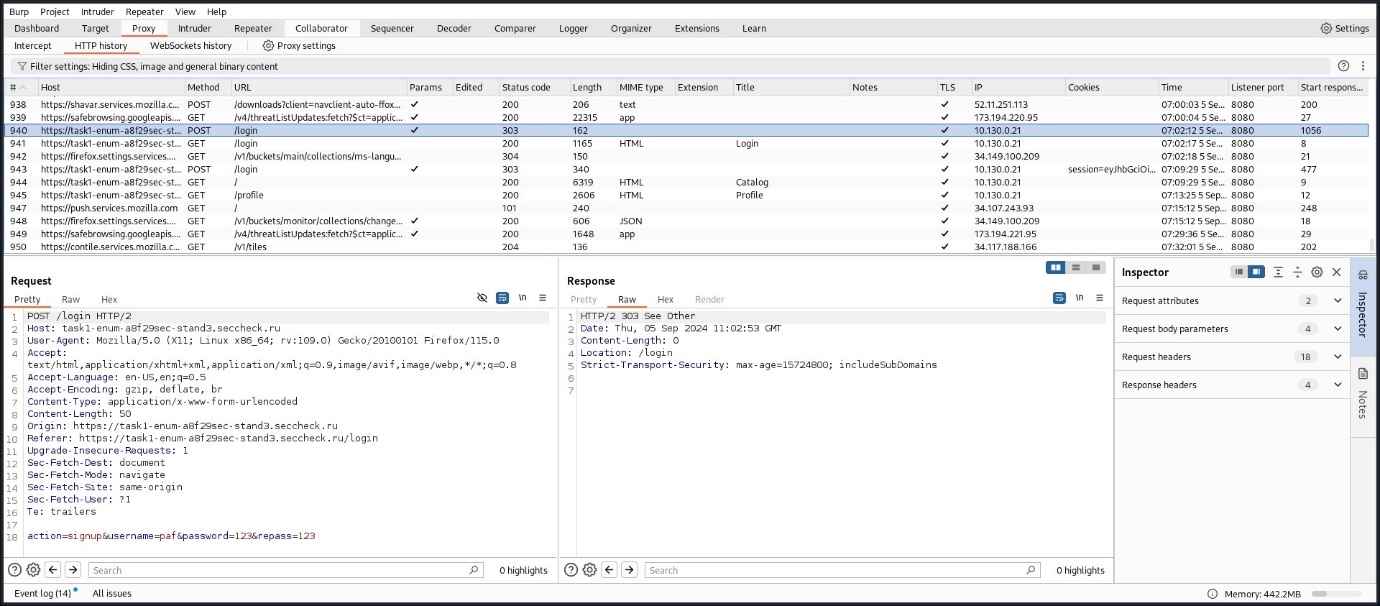
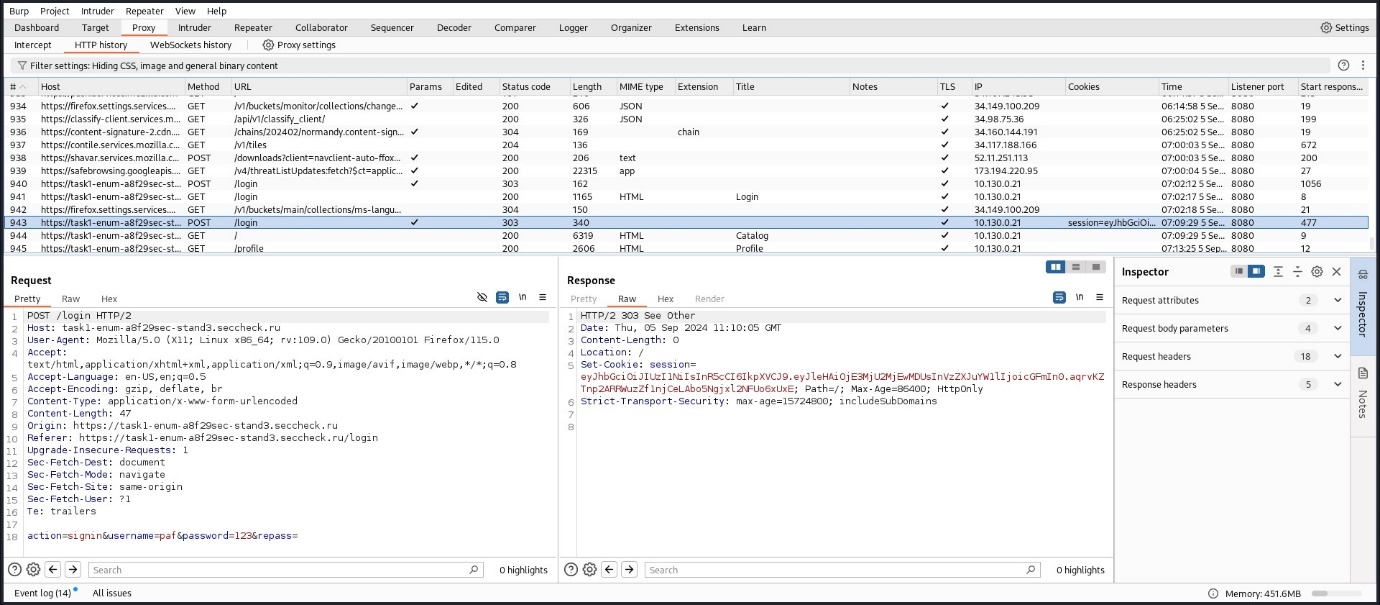
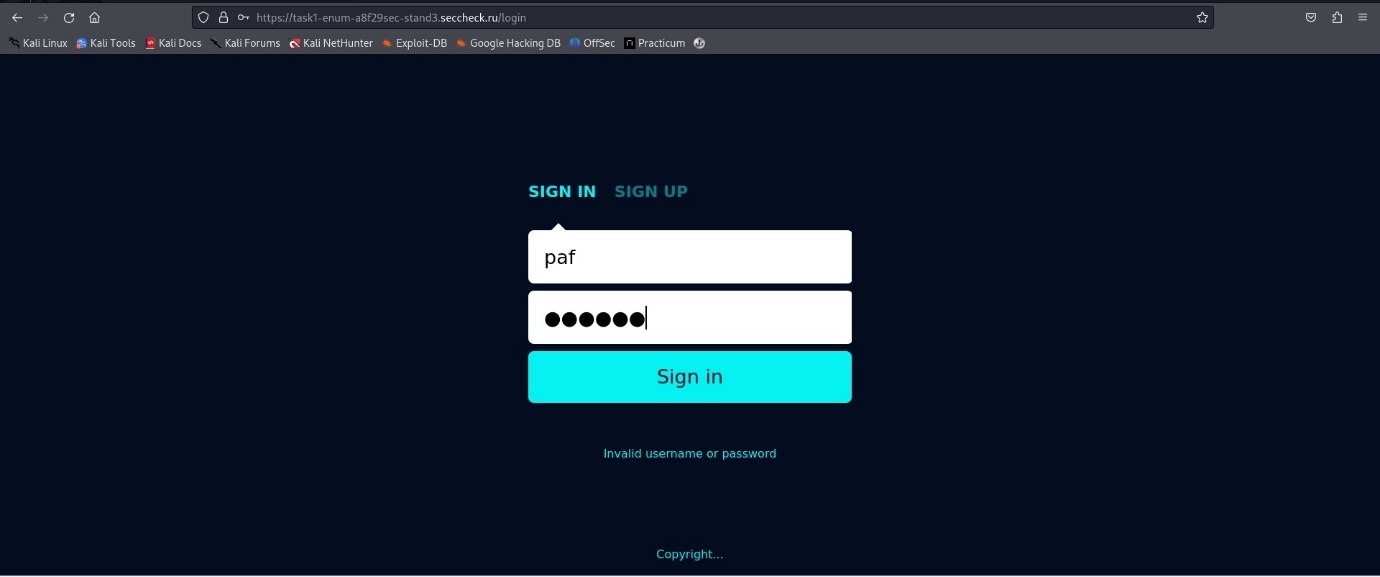
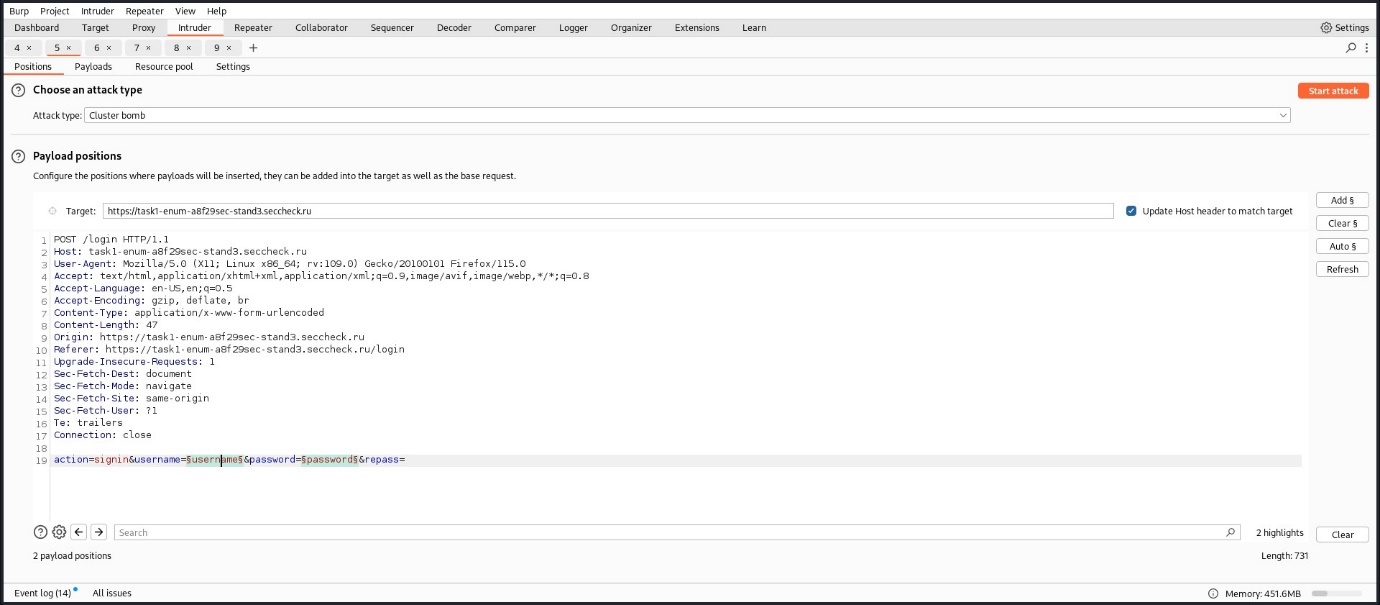
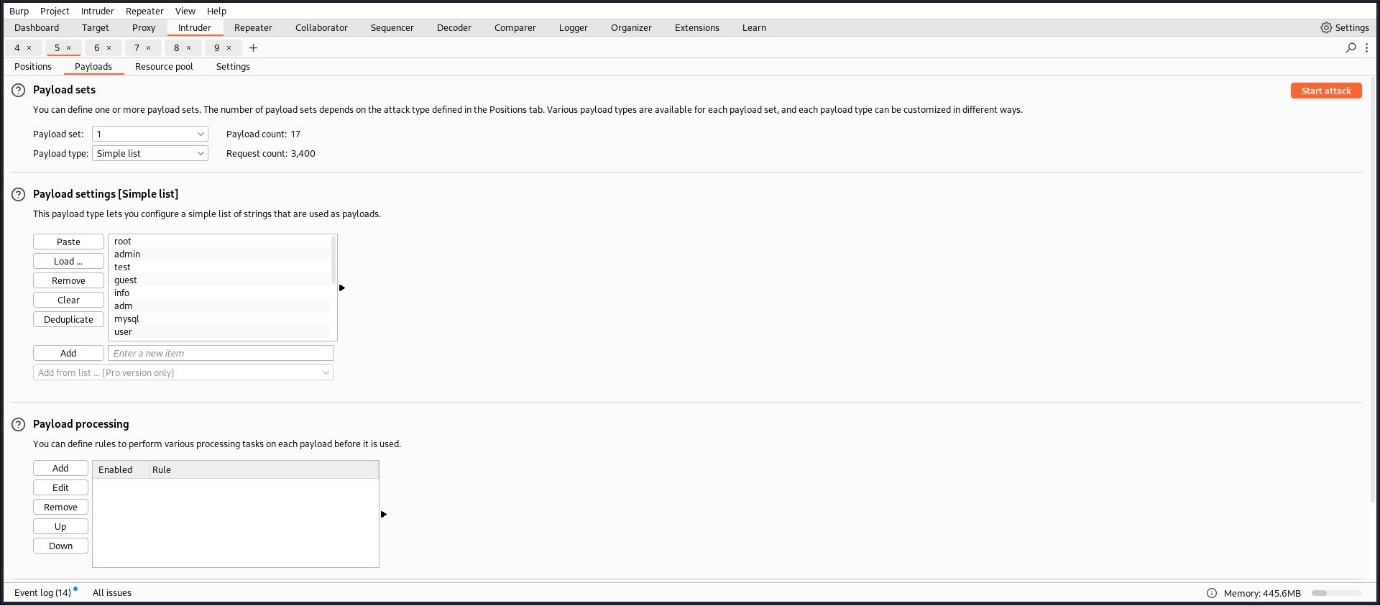
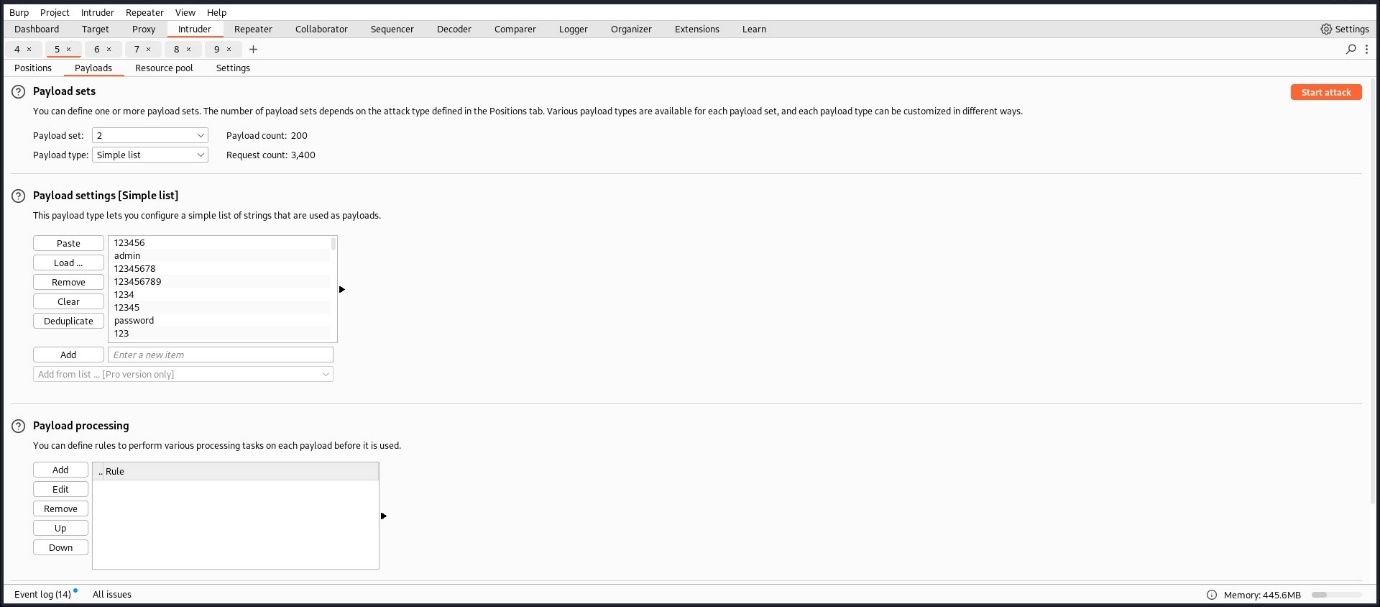
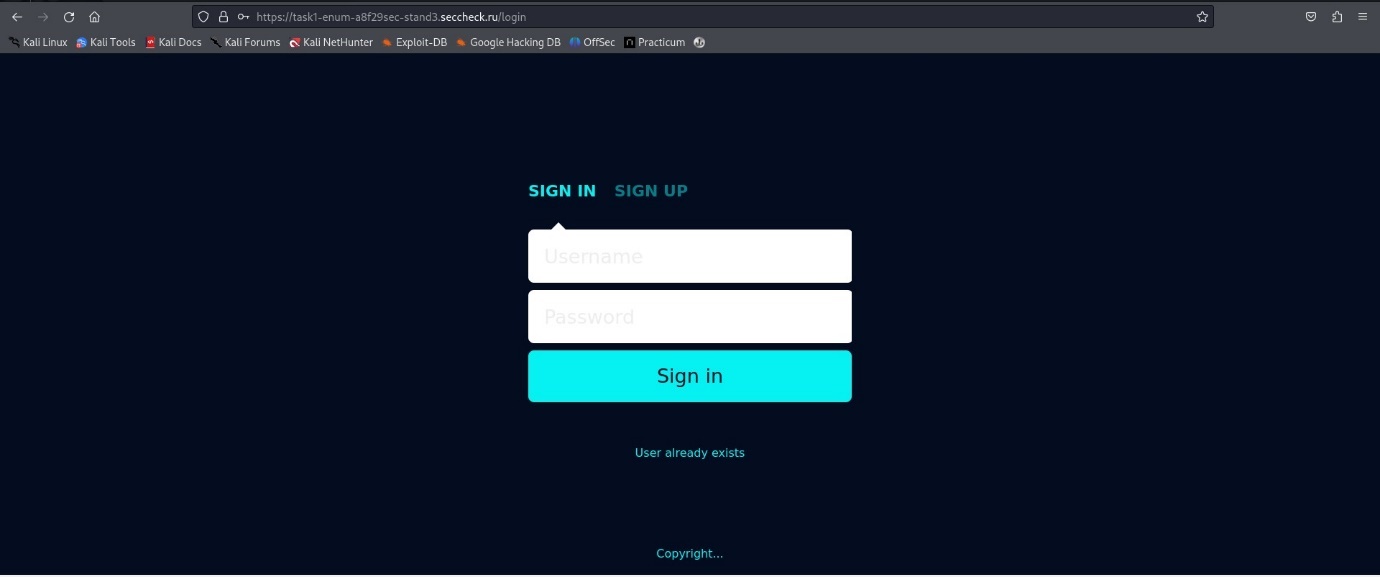
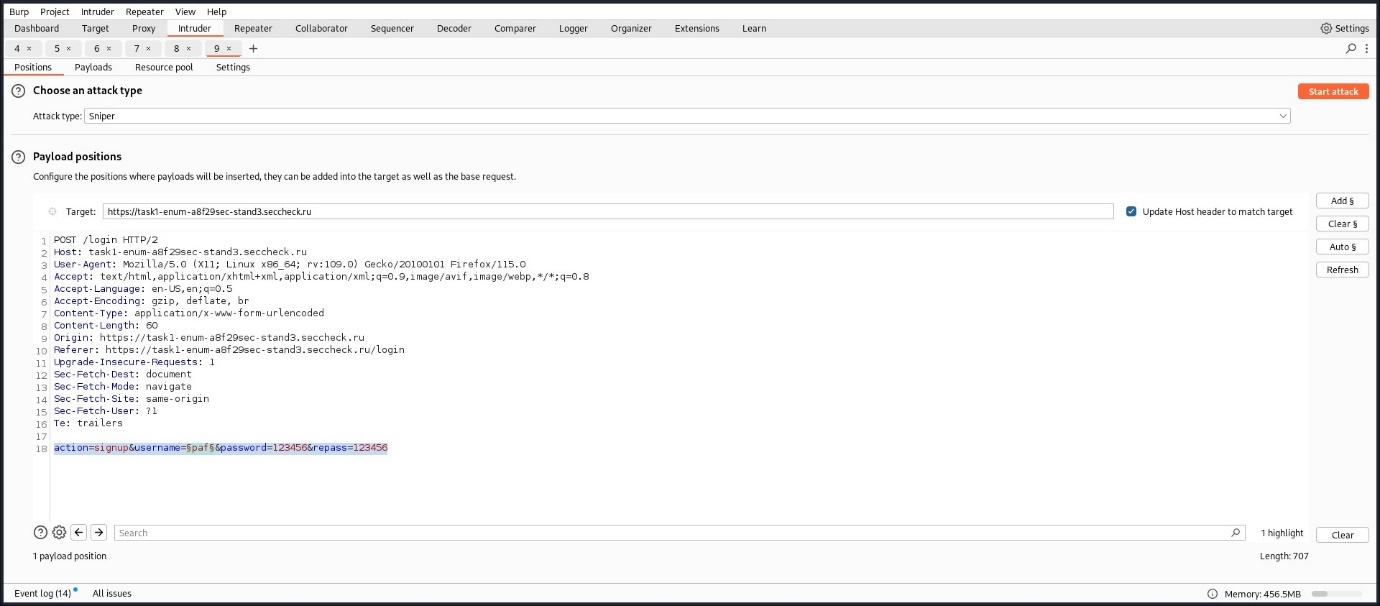
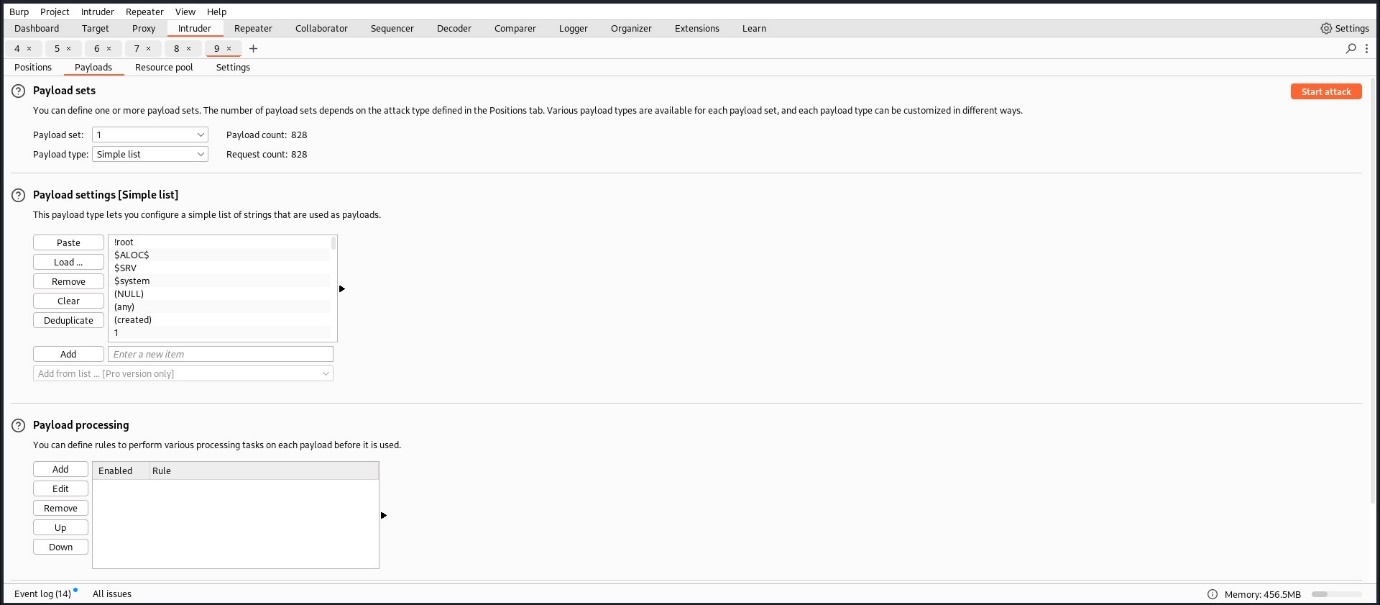
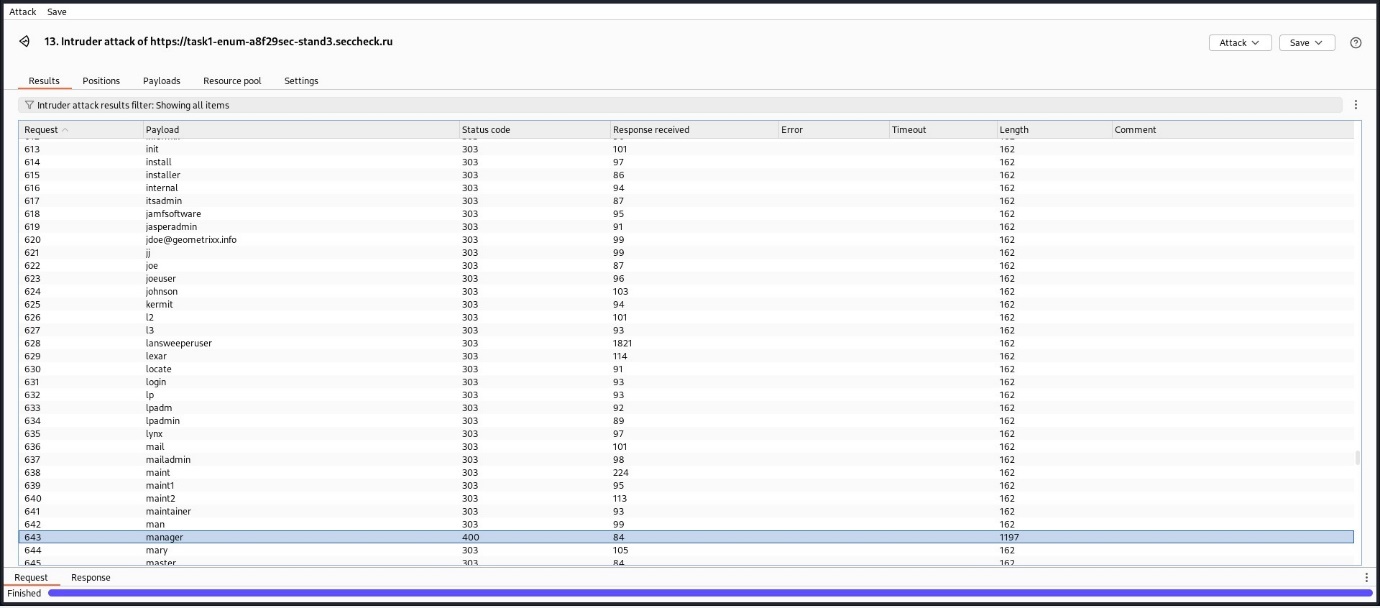
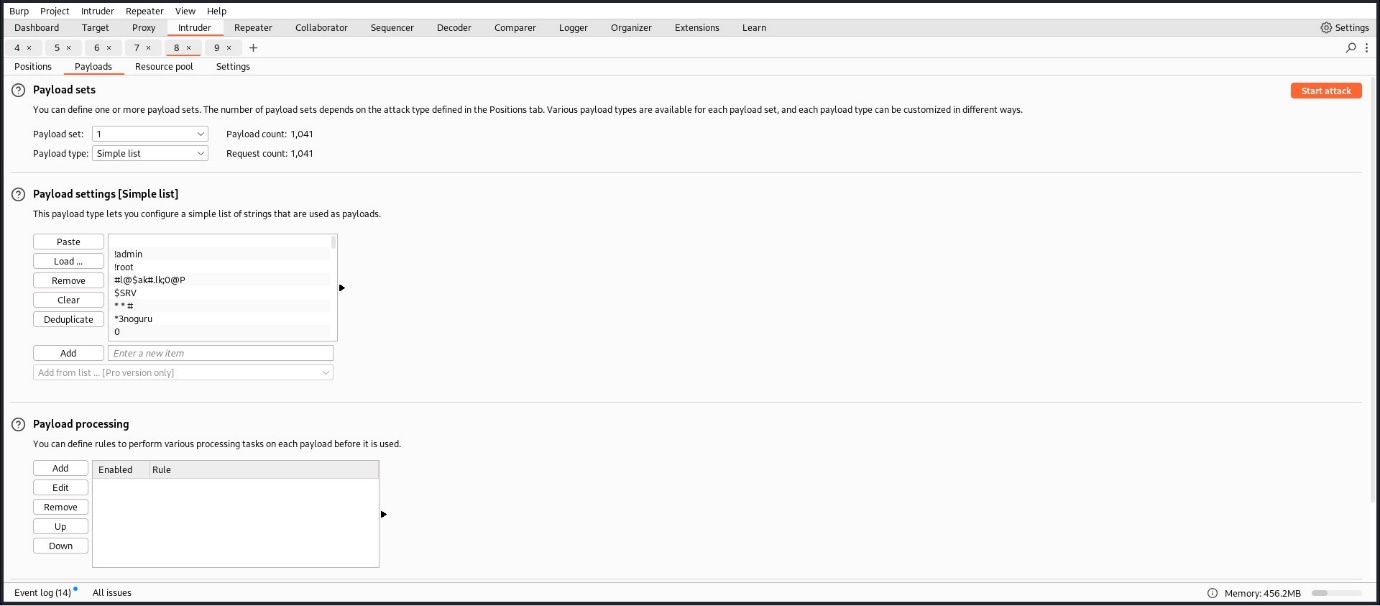
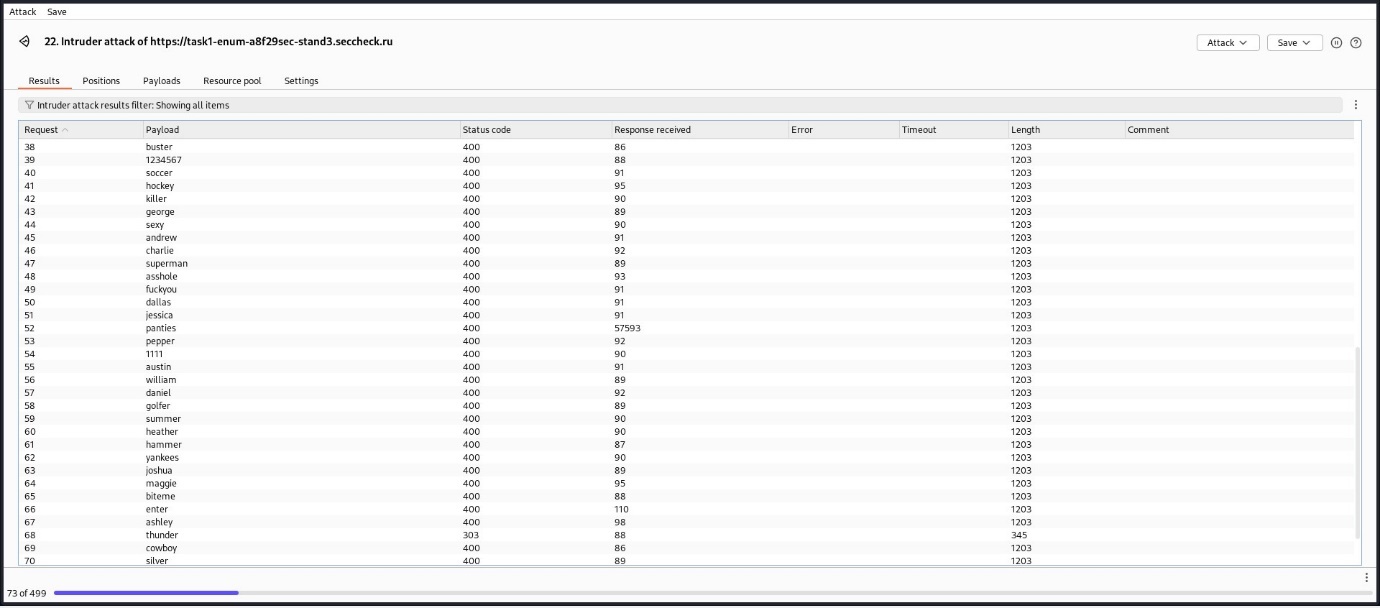
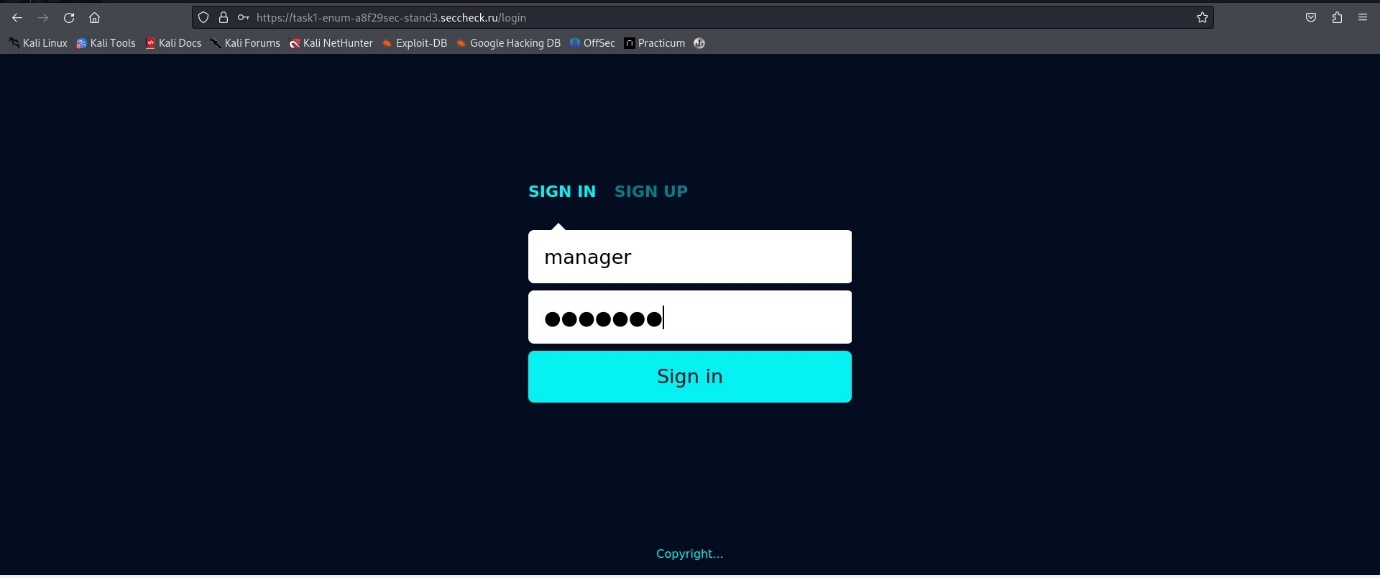
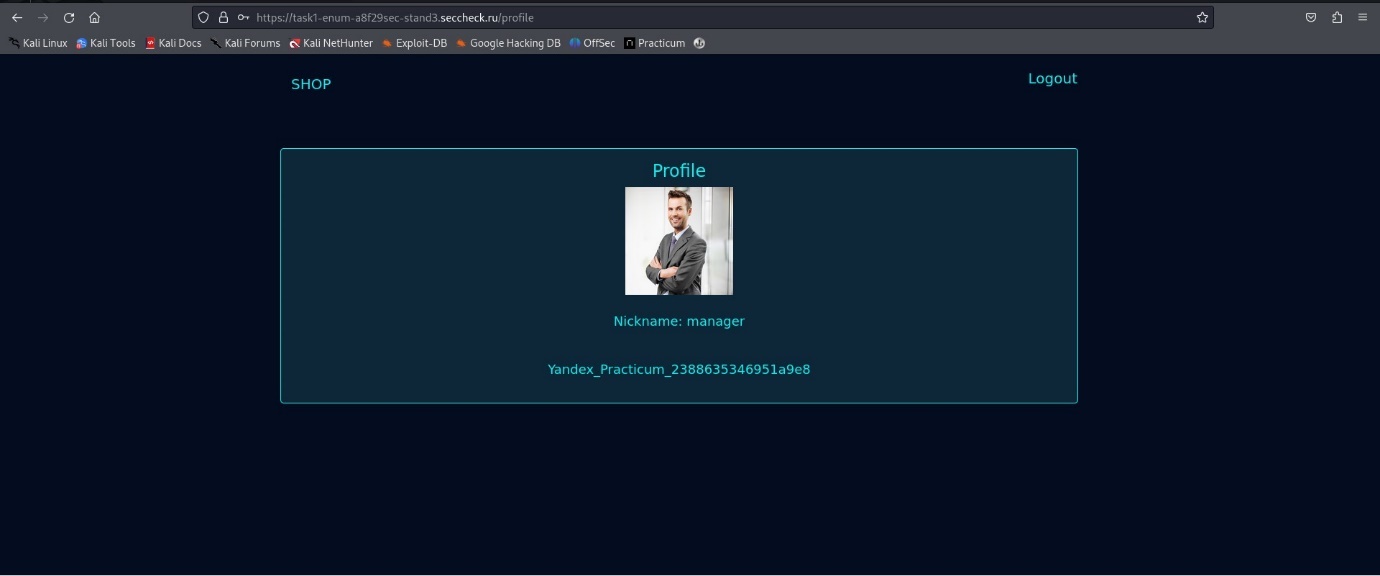
Отчёт выполнения финального проекта 4 спринта

# **Задание 1**

## Флаг: { Yandex\_Practicum\_2388635346951a9e8 }

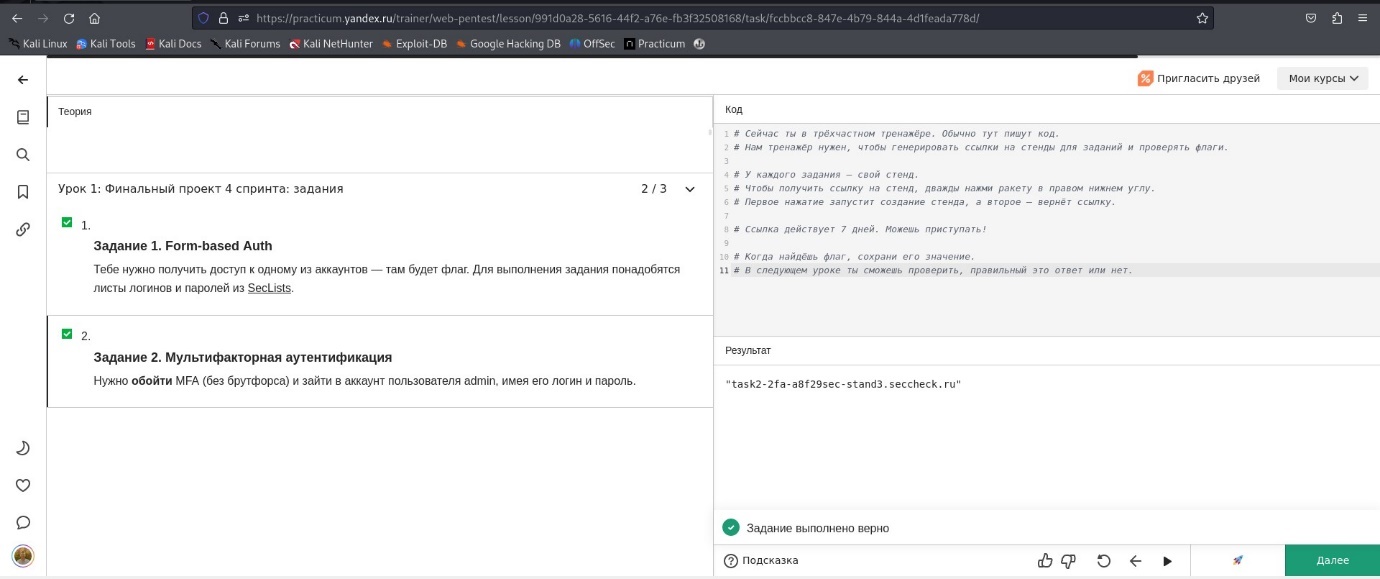
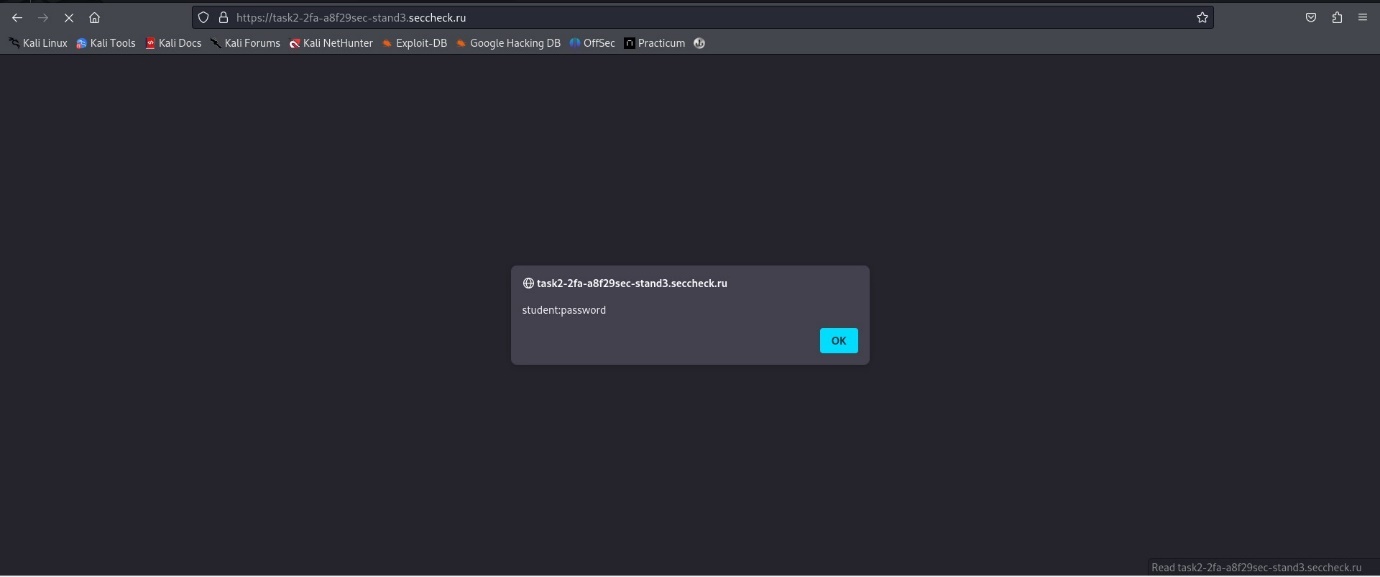
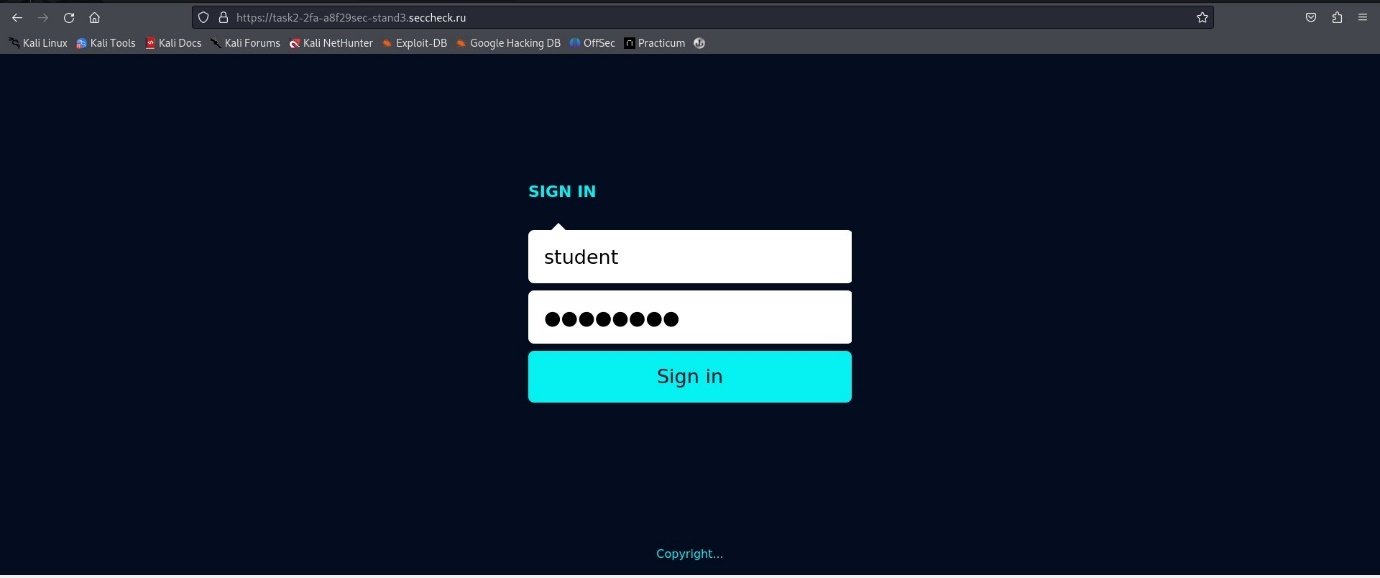
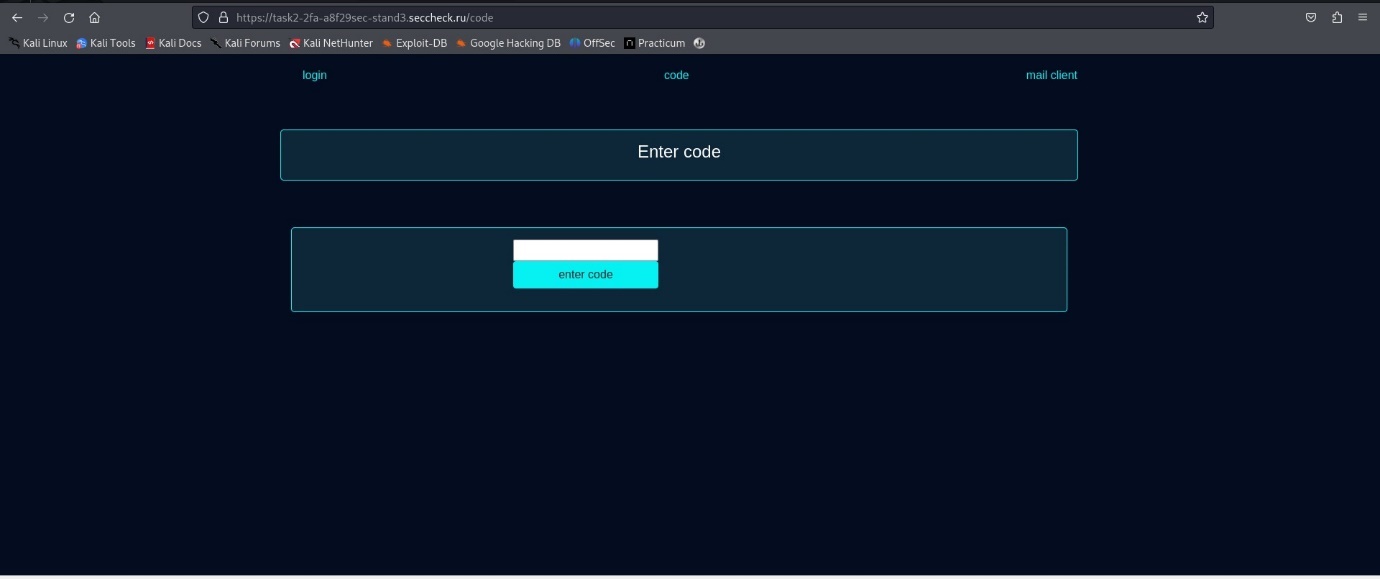
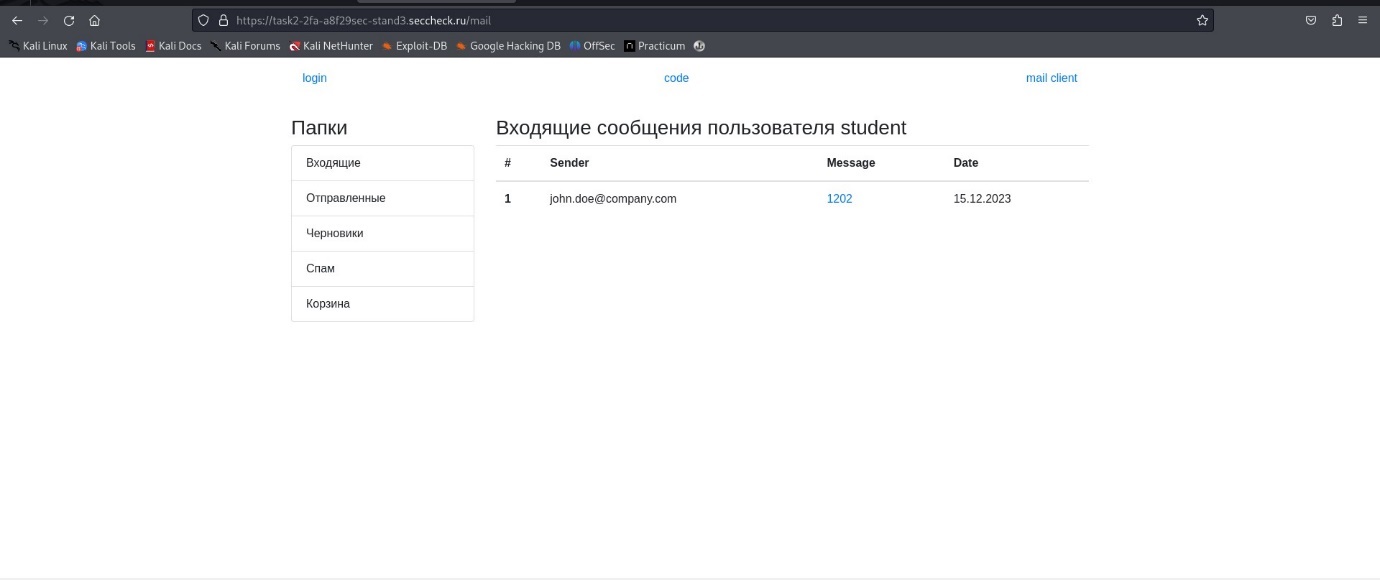
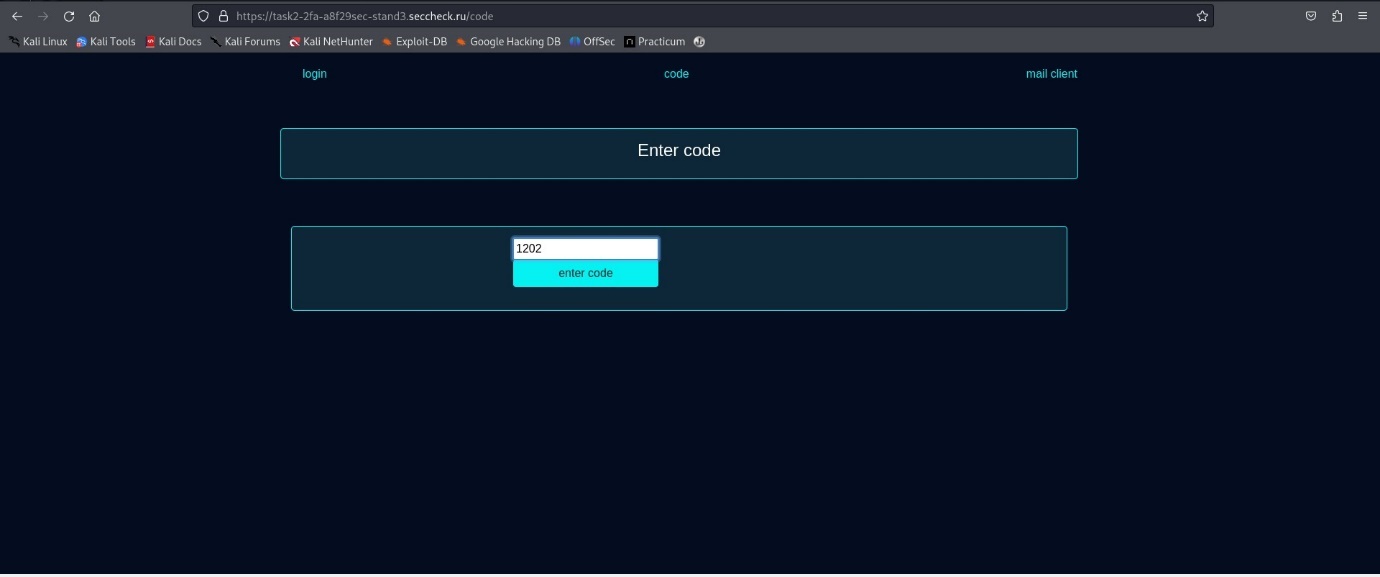
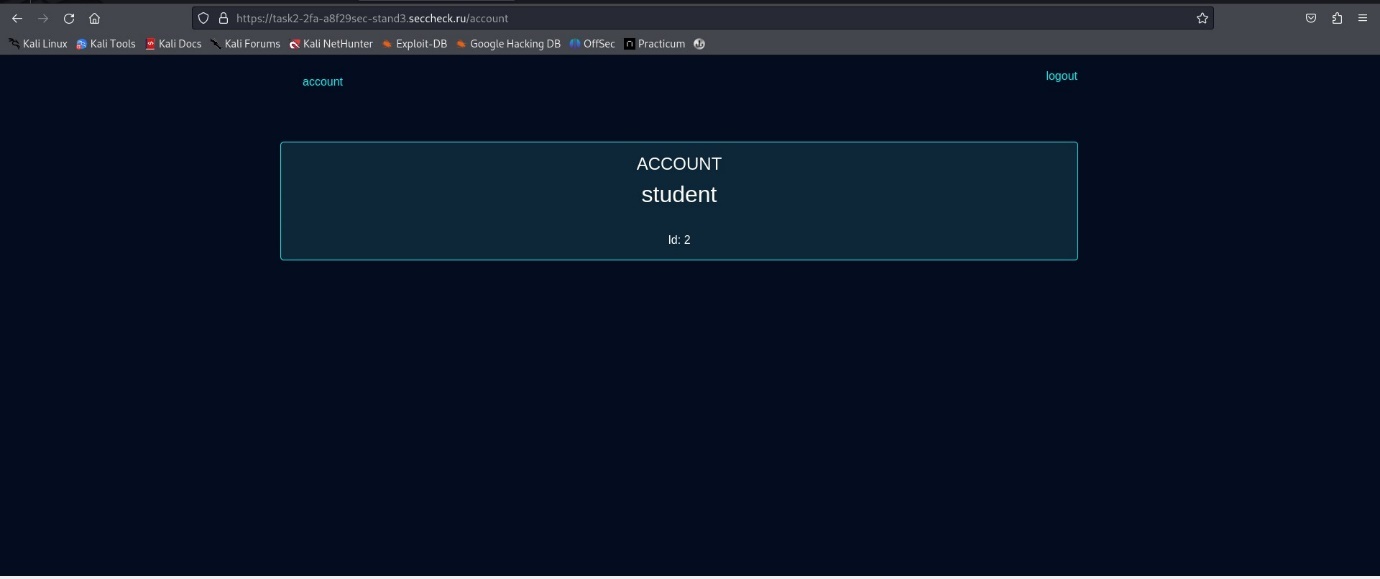
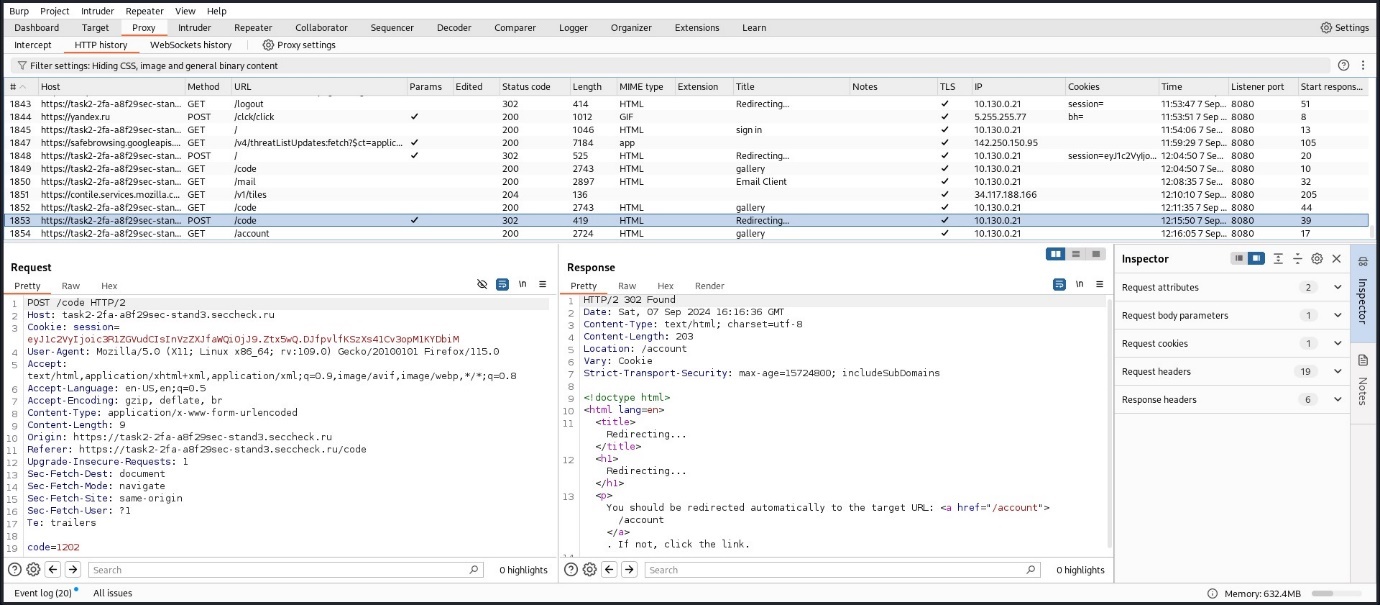
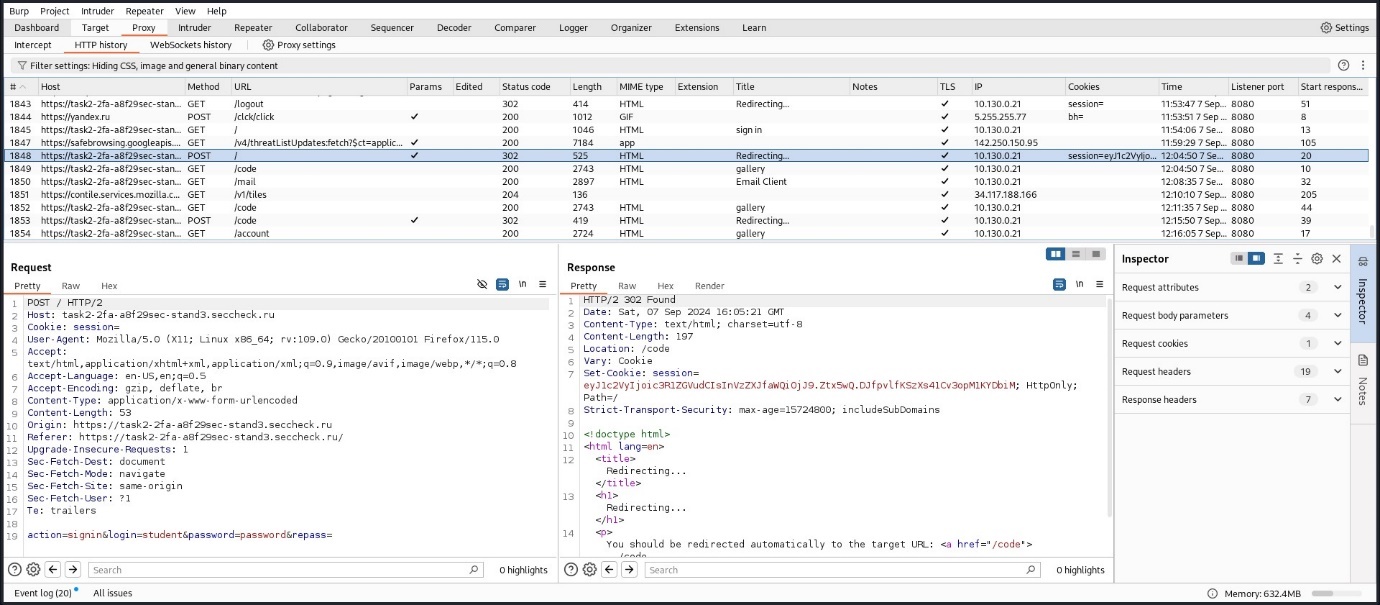
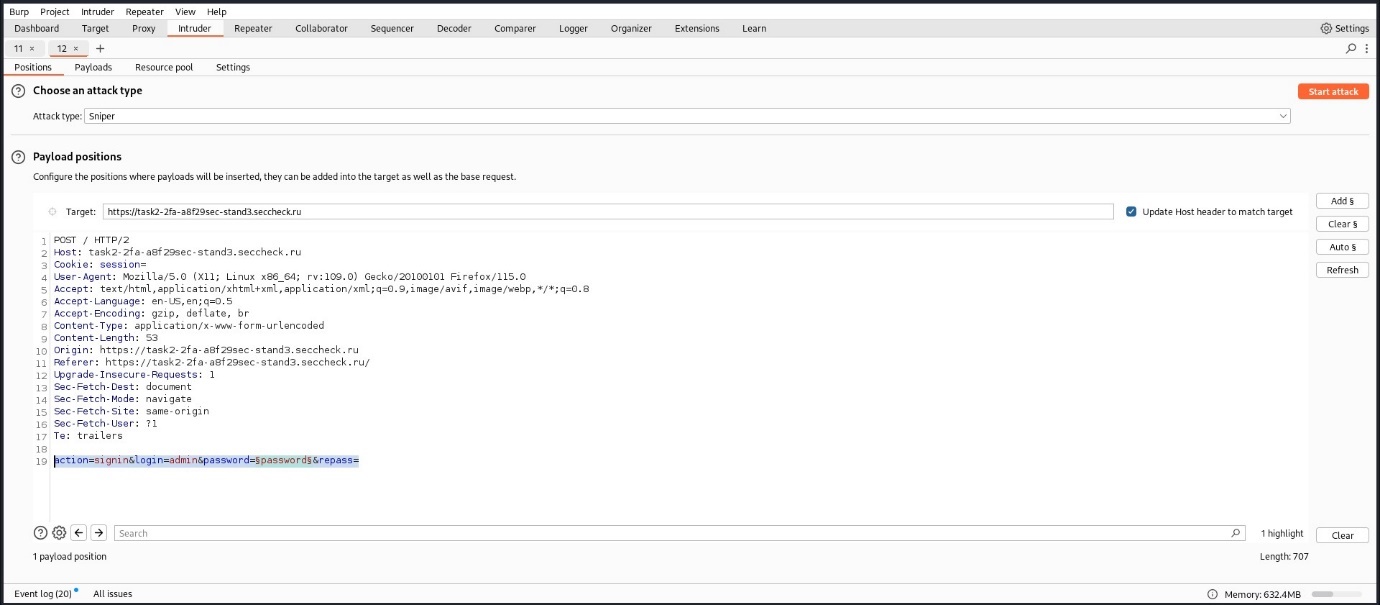
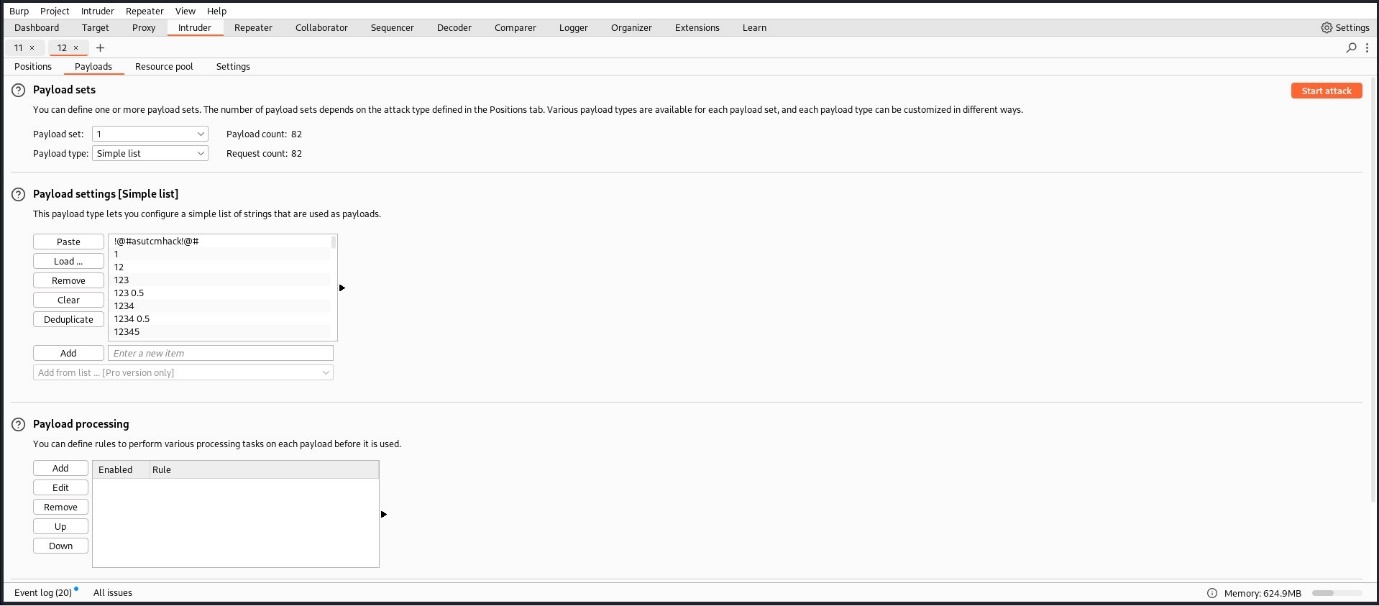
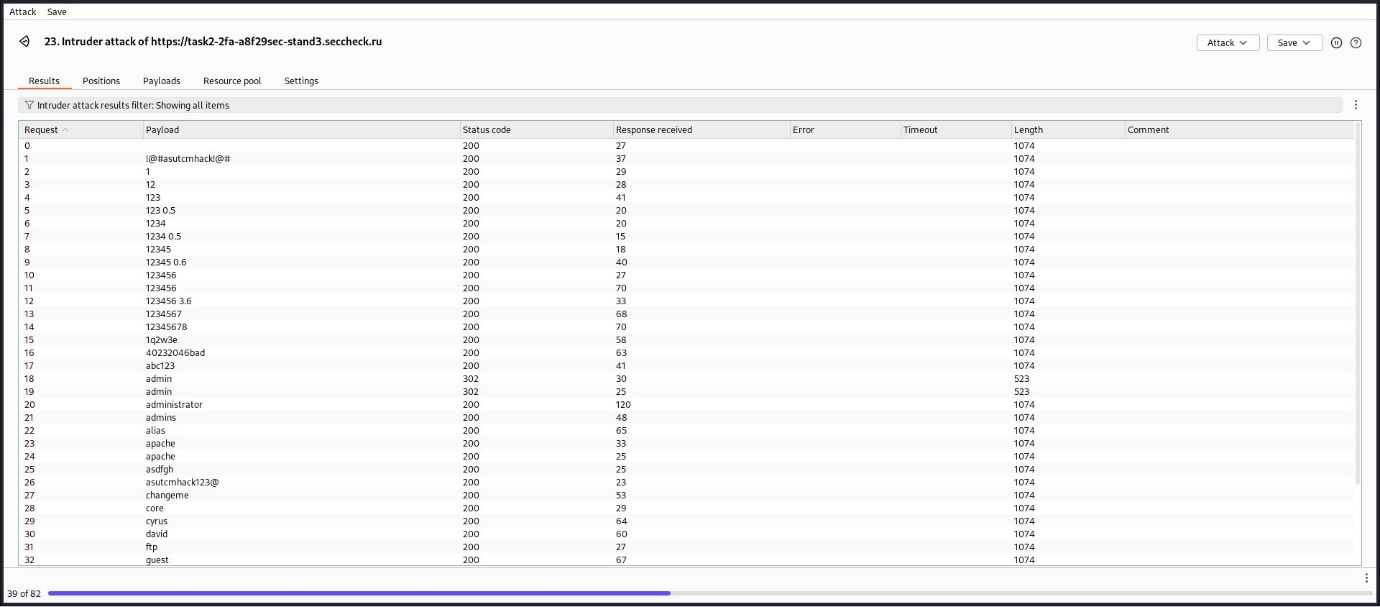
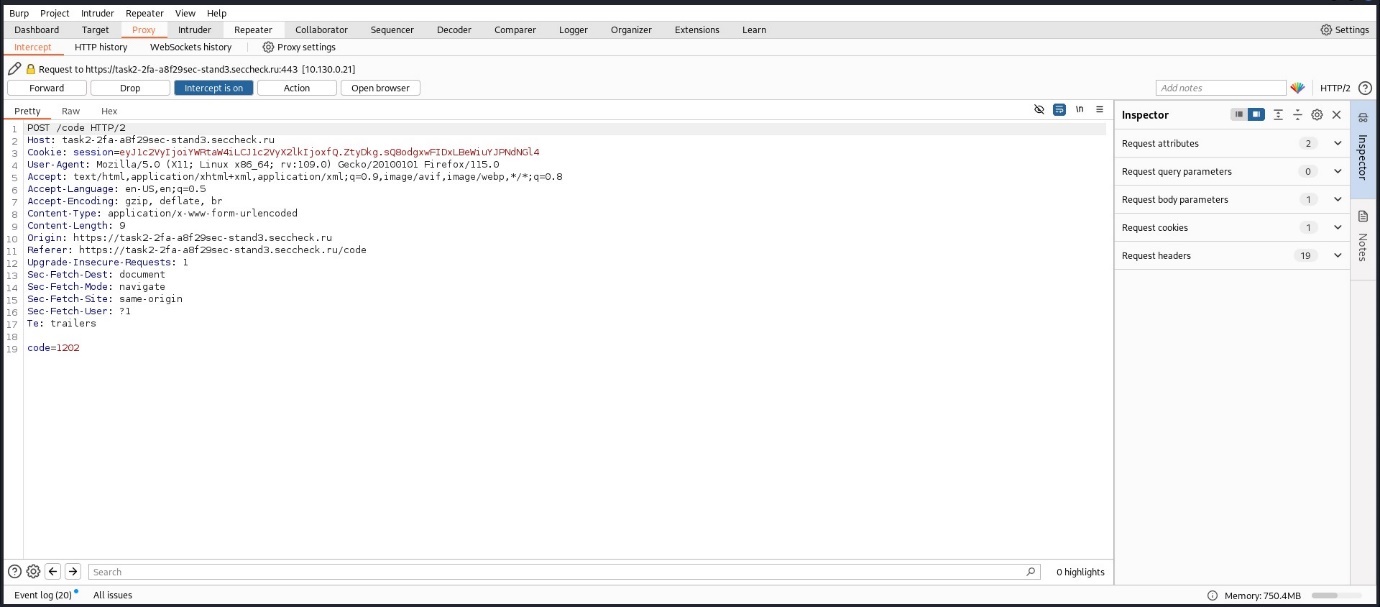
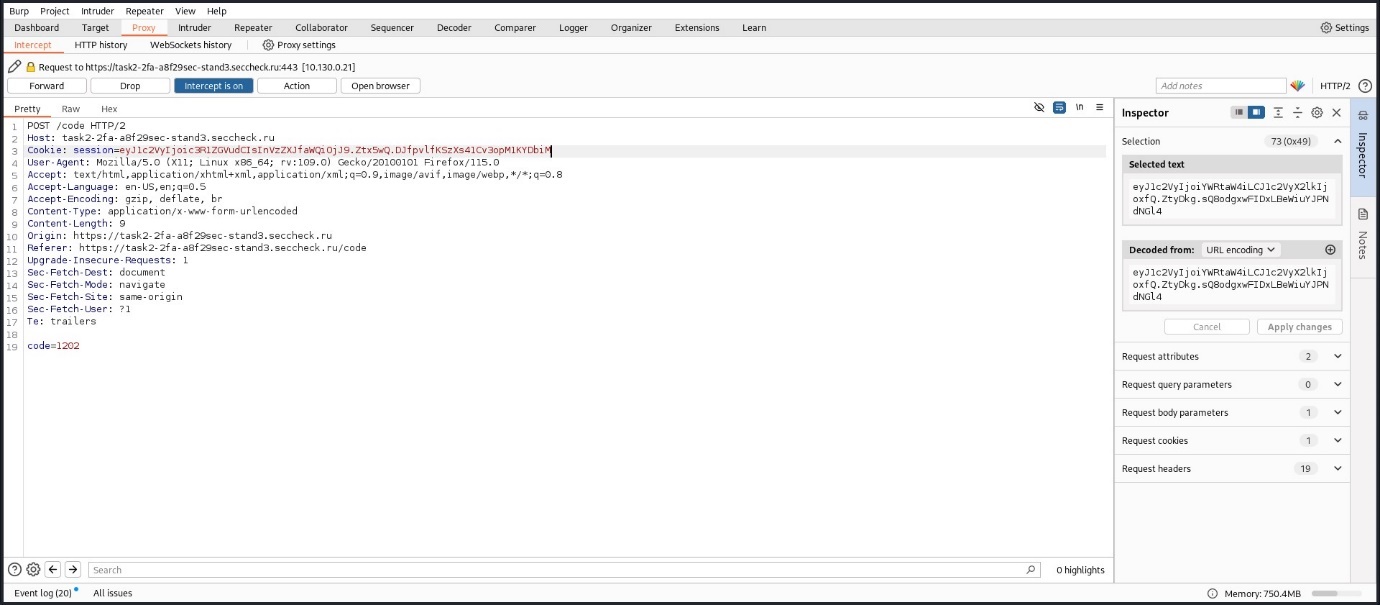
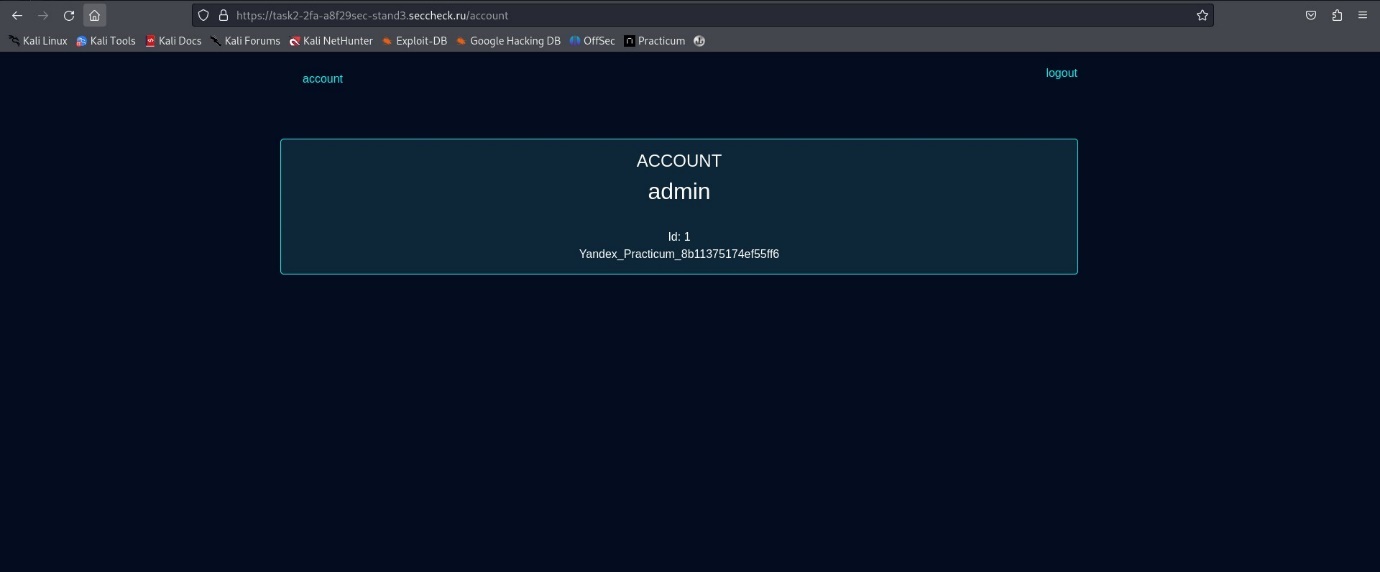
## Отчёт:

1. Ознакомился с заданием и запустил стенд
2. Открыл в браузере этот сайт и обнаружил там форму для регистрации и авторизации пользователя
3. Перехожу в SIGN UP и регистрирую нового пользователя
4. Перехожу в SIGN IN и авторизуюсь
5. Открывается главная страница сайта с каталогом товаров
6. Перехожу по ссылке Profile и не обнаруживаю там какого-либо функционала
7. Открываю Burp Suite и проверяю историю запросов. Первым обращением к серверу был POST-запрос с данными, которые необходимы для регистрации 
8. Далее последовал POST-запрос с данными, которые необходимы для авторизации 
9. Для выполнения задания попытался пройти процедуру авторизации повторно, чтобы проверить реакцию сервера на неправильный пароль при верном имени пользователя. Для этого перешёл по ссылке [Logout](https://task3-jwt-a8f29sec-stand3.seccheck.ru/logout) и заново ввёл в SIGN IN своё имя пользователя с другим паролем, но получил сообщение о том, что неверными могут быть оба значения
10. Возвращаюсь в историю Burp Suite и отправляю POST-запрос на авторизацию в Intruder. Отмечаю там символом § поля username и password для перебора значений, и выбираю тип атаки Cluster Bomb, который подбирает значения сразу для двух параметров
11. Открываю вкладку Payloads и загружаю в Payload set 1 лист с именами пользователей top-usernames-shortlist.txt из SecLists 
12. Загружаю в Payload set 2 лист с паролями 2023-200\_most\_used\_passwords.txt из SecLists 
13. Запускаю подбор имени пользователя и пароля, но не получаю ожидаемого ответа с кодом перенаправления 303. Такой способ подбора длится очень долго, поскольку требует использования двух больших списков одновременно и результат может быть достигнут уже после крайнего срока сдачи задания на проверку. По этой причине я вернулся к POST-запросу на регистрацию нового пользователя, ведь если я указываю своё имя пользователя, но с другим паролем, то вижу в браузере ошибку User already exists 
14. Отправляю POST-запрос на регистрацию нового пользователя в Intruder. Отмечаю там символом § поле username, а password и repass оставляю с произвольным значением 123456. Тип атаки на этот раз выбираю Sniper 
15. Открываю вкладку Payloads и загружаю в Payload set 1 лист с именами пользователей cirt-default-usernames.txt из SecLists 
16. Запускаю подбор имени пользователя и наблюдаю череду успешных регистраций новых пользователей с паролем 123456. У всех приходит ответ с кодом перенаправления 303 и только одно имя пользователя даёт ответ с кодом 400. Это указывает на то, что пользователь manager был зарегистрирован ранее 
17. Теперь с этим именем пользователя можно перейти к подбору пароля. Отмечаю символом § поле password, а в username будет найденное значение manager. Тип атаки снова выбрал Sniper 
18. Открываю вкладку Payloads и загружаю в Payload set 1 лист с паролями 500-worst-passwords.txt из SecLists 
19. Запускаю подбор пароля и наблюдаю, что приходит множество ответов с кодом 400 и только один пароль thunder даёт ответ с кодом перенаправления 303
20. Возвращаюсь на сайт и авторизуюсь с полученными учётными данными 
21. Затем перехожу в профиль этого пользователя и обнаруживаю там флаг 

# **Задание 2**

## Флаг: { Yandex\_Practicum\_8b11375174ef55ff6 }

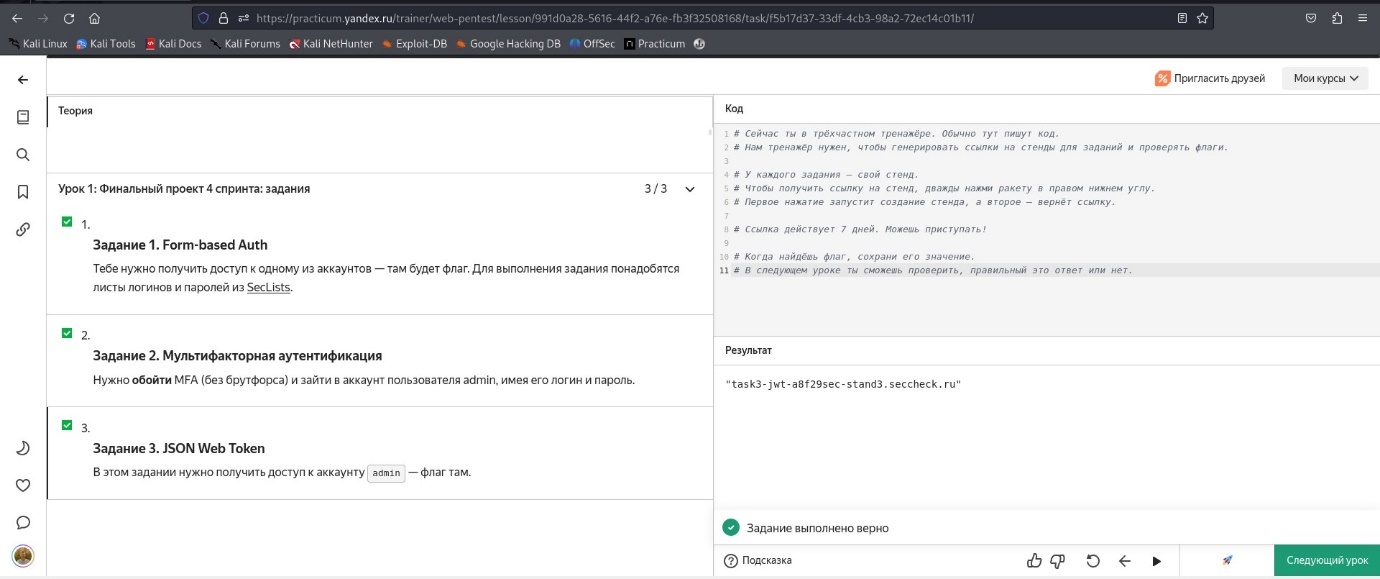
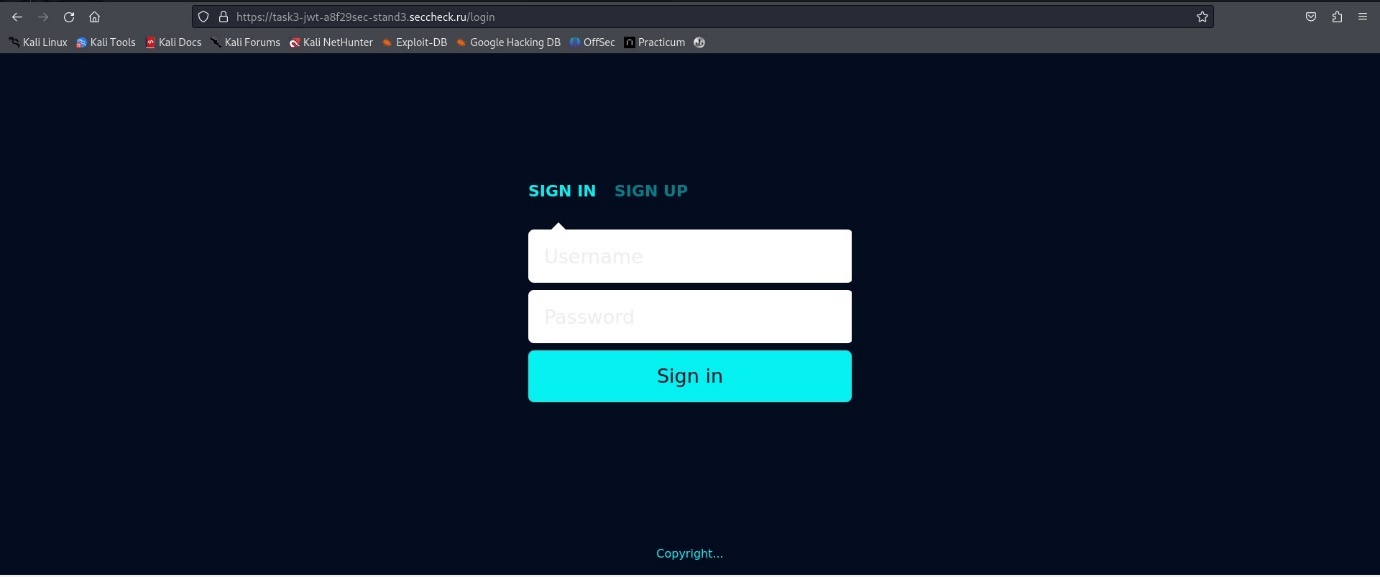
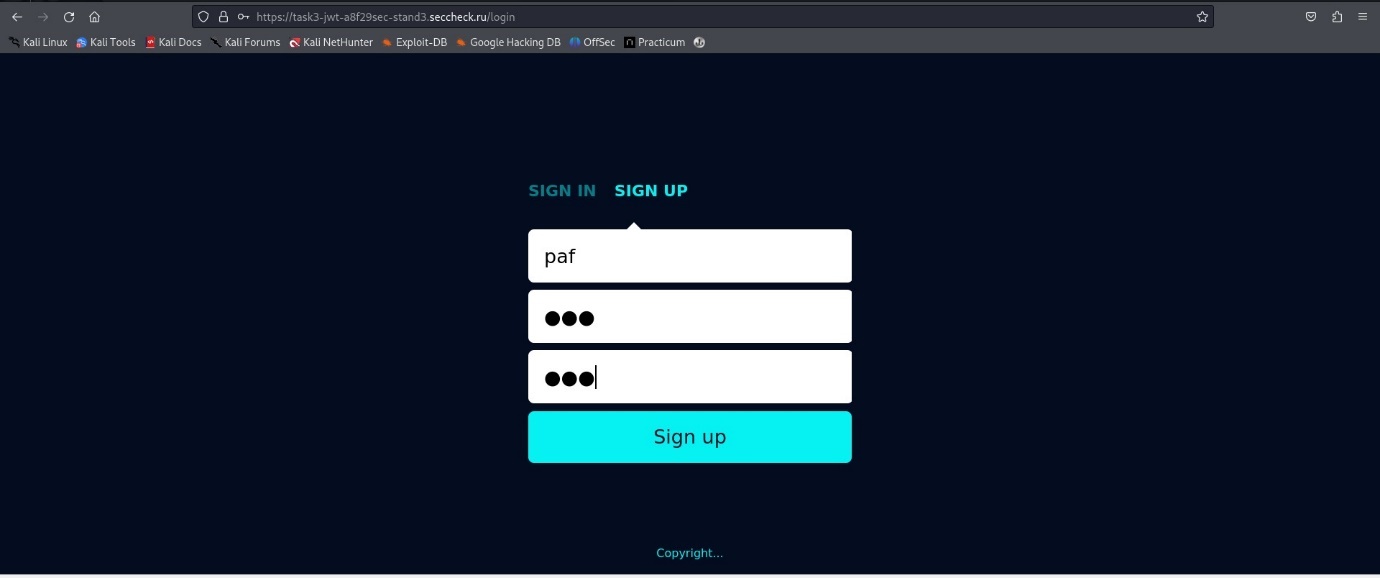
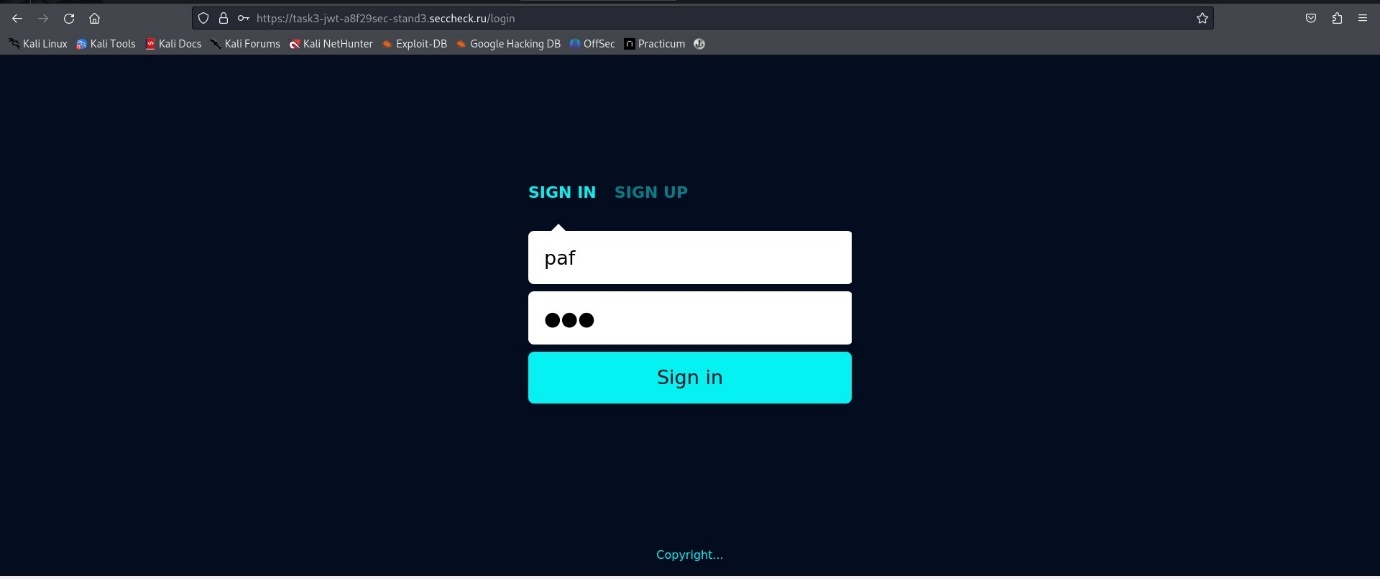
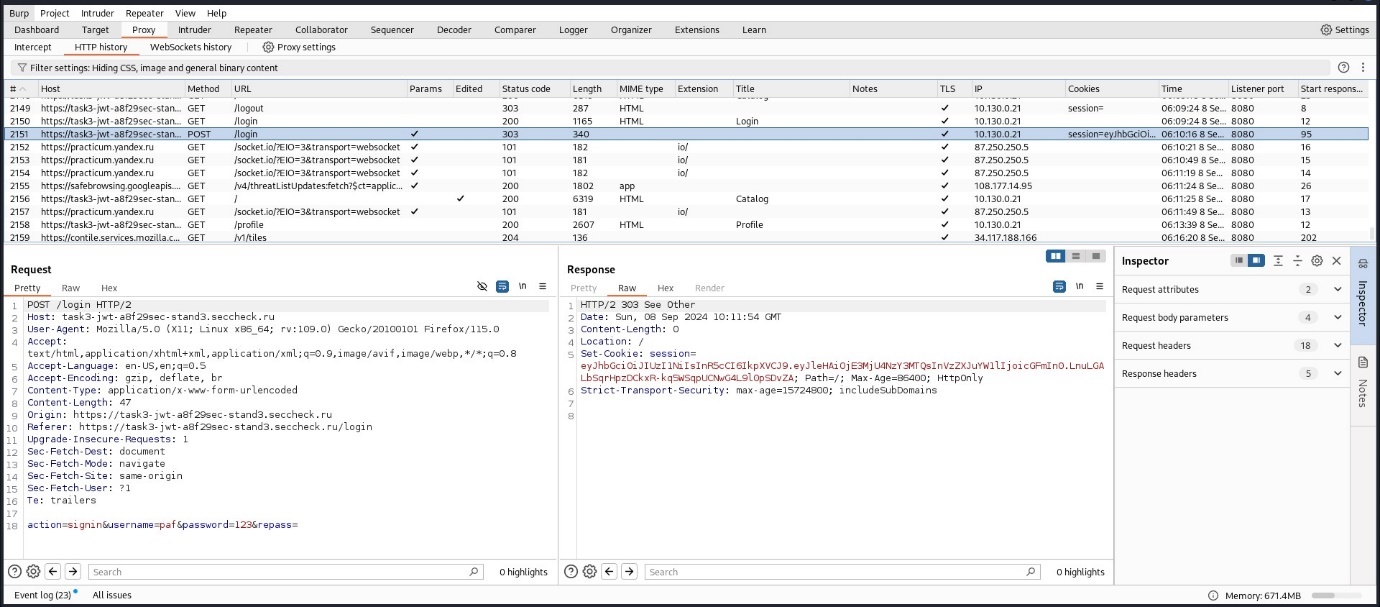
## Отчёт:

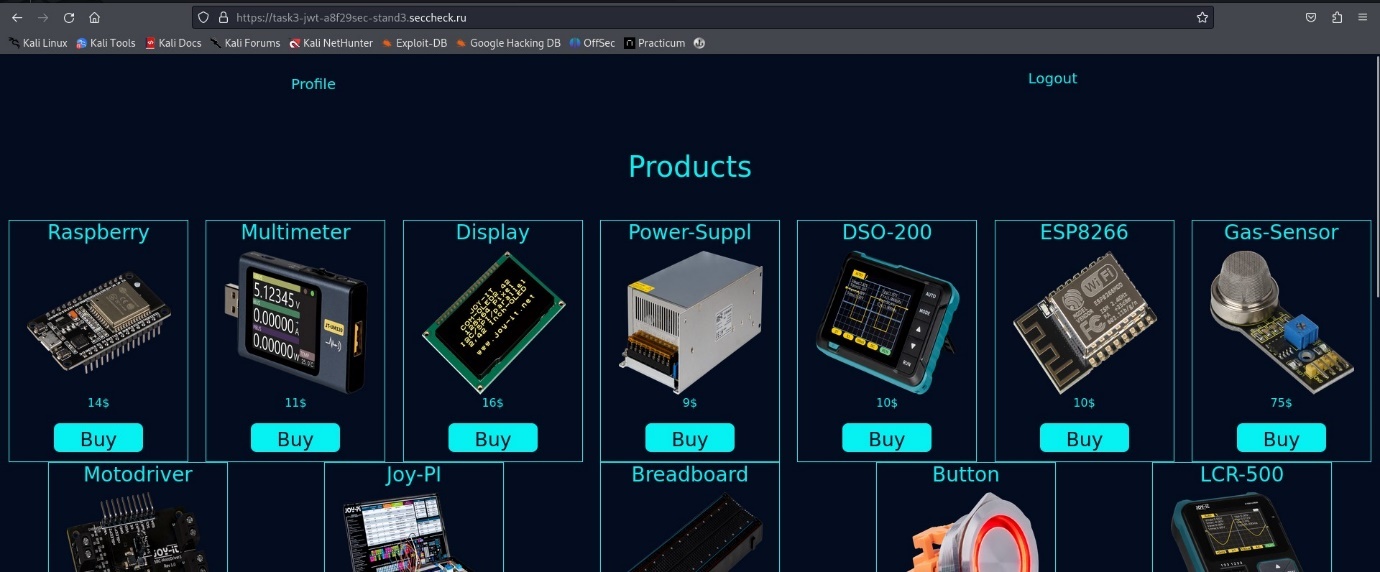
1. Ознакомился с заданием и запустил стенд 
2. Открыл сайт в браузере и обнаружил там вплывающее окно с учётными данными пользователя 
3. Кликаю на OK и открывается форма для авторизации, в которой указываю данные из всплывающего окна 
4. После этого вижу поле для ввода кода MFA 
5. Открываю [mail client](https://task2-2fa-a8f29sec-stand3.seccheck.ru/mail) и вижу там тот самый код MFA 
6. Перехожу по ссылке [code](https://task2-2fa-a8f29sec-stand3.seccheck.ru/code) и ввожу код 
7. Открывается страница аккаунта student 
8. Открываю Burp Suite и вижу в истории POST-запрос c кодом
9. Далее я возвращаюсь к POST-запросу на авторизацию пользователя 
10. И отправляю его в Intruder для подбора пароля пользователя admin 
11. Перехожу в Payloads, загружаю лист с паролями clarkson-university-82.txt и запускаю подбор пароля
12. Быстро нахожу простой пароль admin с кодом перенаправления 302 в ответе 
13. Возвращаюсь на страницу авторизации и использую имя пользователя admin с паролем admin 
14. Перехожу в Burp Suite и вижу в истории запрос на авторизацию admin
15. Включаю Intercept, возвращаюсь к форме ввода кода MFA, указываю в ней тот же код 1202 и перехватываю запрос 
16. Открываю HTTP history, нахожу там POST-запрос на авторизацию пользователя student (пункт 8), копирую оттуда токен eyJ1c2VyIjoic3R1ZGVudCIsInVzZXJfaWQiOjJ9.Ztx5wQ.DJfpvlfKSzXs41Cv3opM1KYDbiM   
    и вставляю его в перехваченный запрос на авторизацию пользователя admin 
17. Нажимаю Forward, перехожу в браузер и вижу там аккаунт admin с флагом 

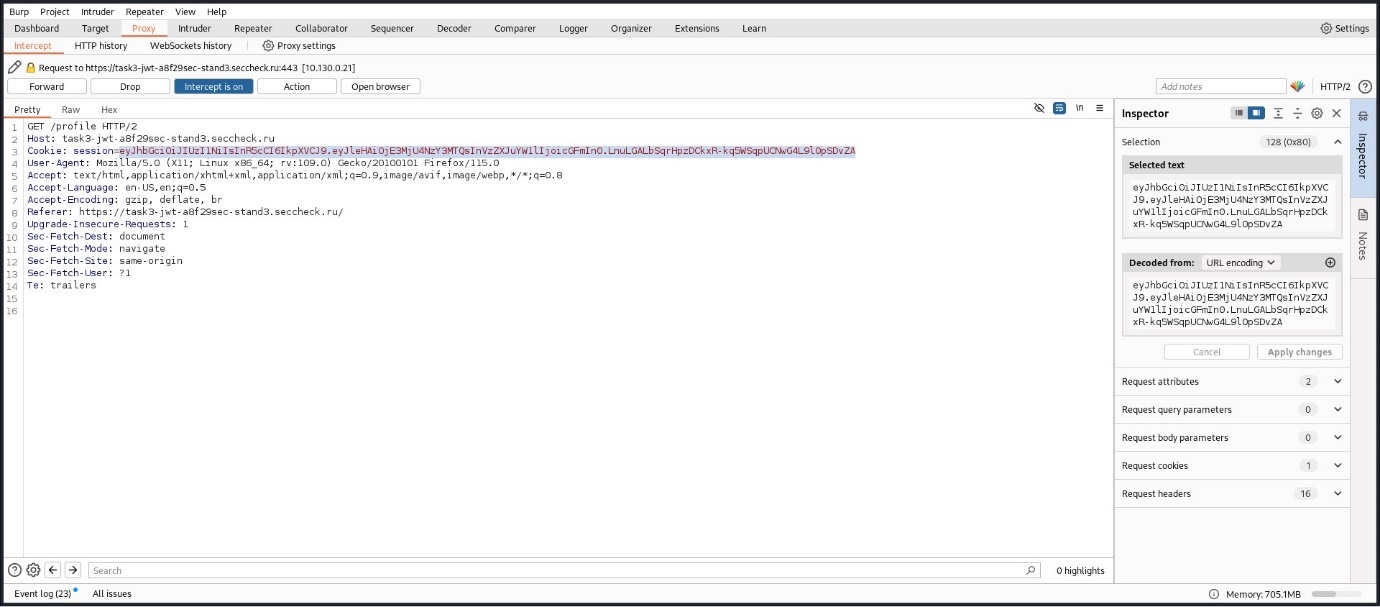
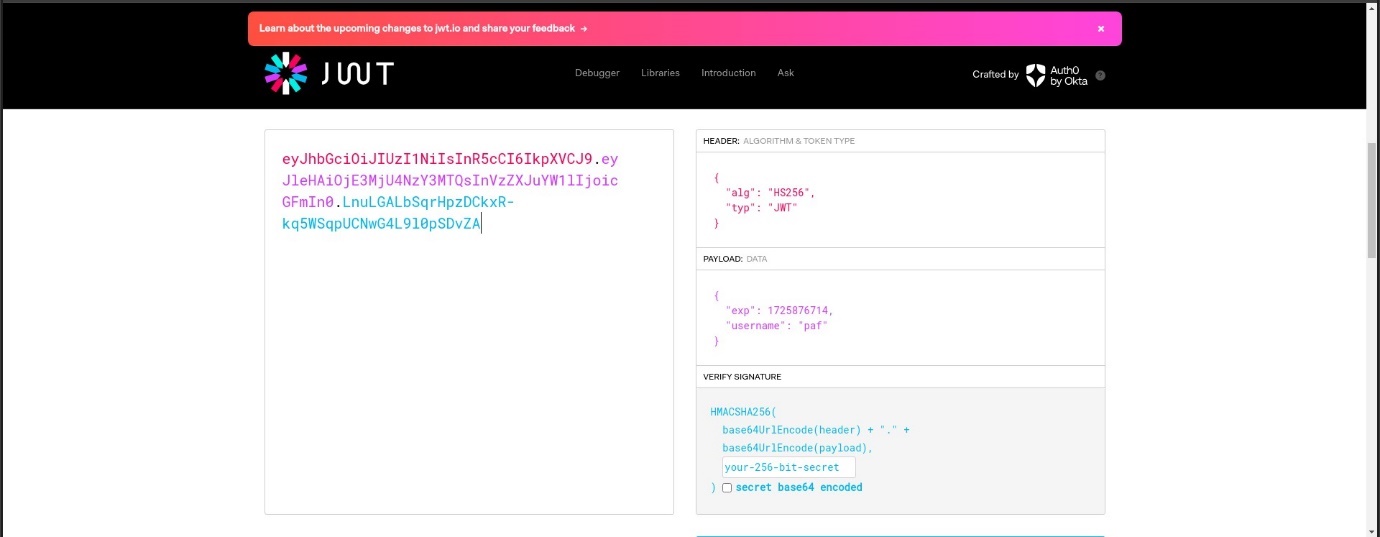
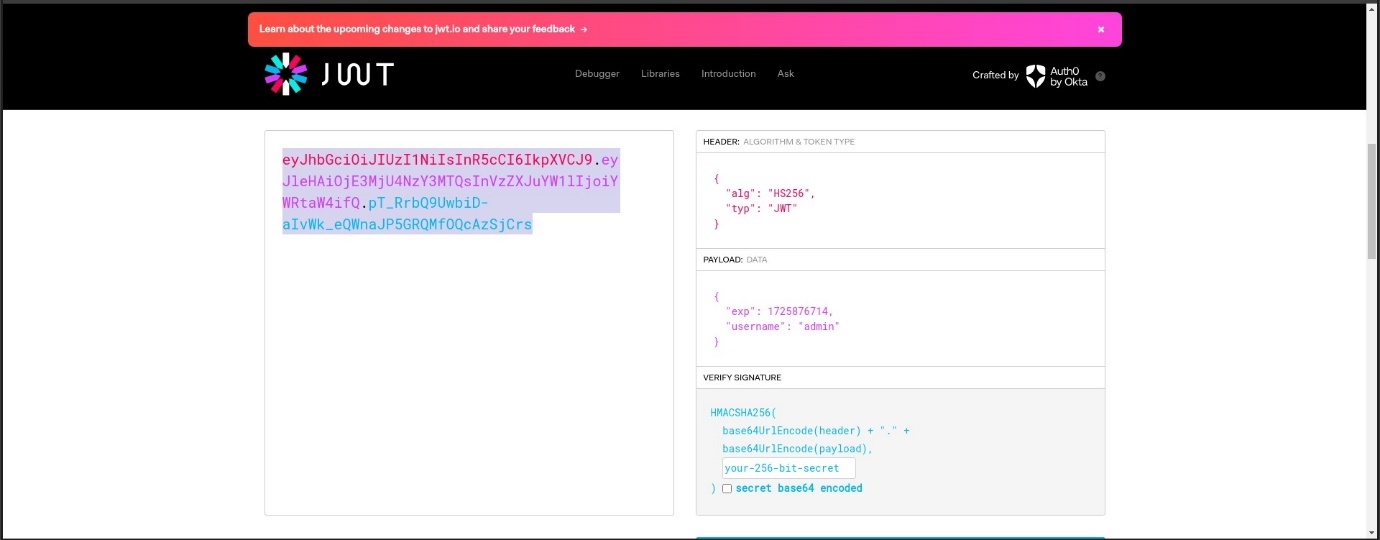
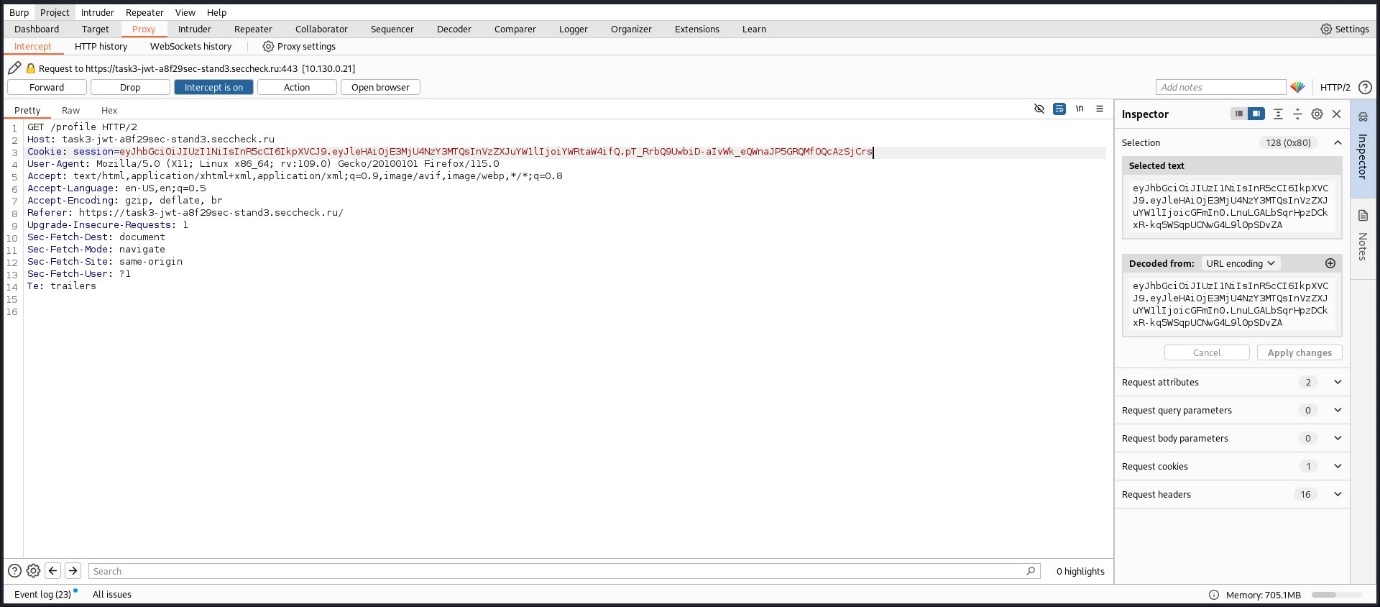
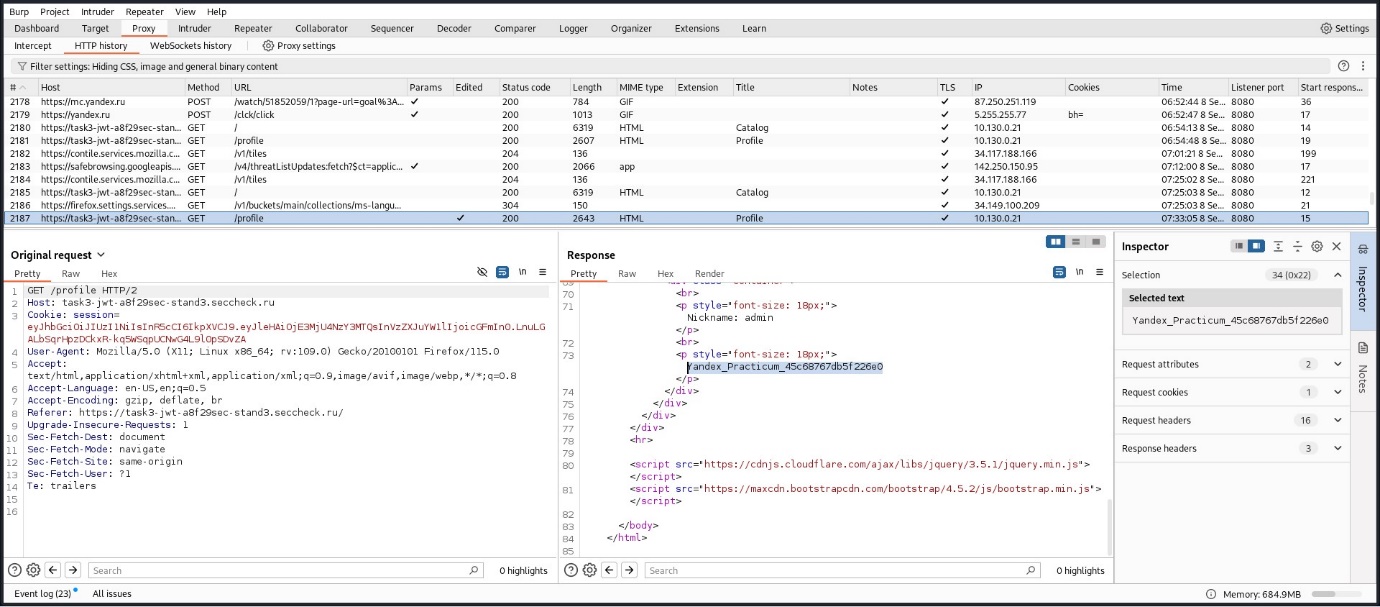
# **Задание 3**

# Флаг: { Yandex\_Practicum\_45c68767db5f226e0 }

## Отчёт:

1. Ознакомился с заданием и запустил стенд 
2. Открыл в браузере этот сайт и обнаружил там форму для регистрации и авторизации пользователя 
3. Перехожу в SIGN UP и регистрирую нового пользователя 
4. Перехожу в SIGN IN и авторизуюсь 
5. Затем перехожу в историю Burp Suite и проверяю порядок авторизации, в результате которой был получен токен eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjU4NzY3MTQsInVzZXJuYW1lIjoicGFmIn0.LnuLGALbSqrHpzDCkxR-kq5WSqpUCNwG4L9l0pSDvZA 
6. Возвращаюсь в браузер, включаю Intercept в Burp Suite и кликаю по ссылке [Profile](https://task3-jwt-a8f29sec-stand3.seccheck.ru/profile)



1. Перехватываю GET-запрос, в котором вижу этот токен. Копирую его в буфер обмена 
2. Открываю в браузере новую вкладку с сервисом jwt.io и вставляю туда скопированный токен 
3. Подменяю paf на admin, получаю новый токен и копирую его 
4. Возвращаюсь в Intercept, вставляю туда токен с пользователем admin вместо токена с пользователем paf и нажимаю Forward 
5. Возвращаюсь в браузер и вижу там флаг от админа 