**Федеральное государственное автономное образовательное учреждение**

**высшего образования   
«Национальный исследовательский университет   
«Высшая школа экономики»**

**Московский институт электроники и математики им. А.Н.Тихонова**

Направление подготовки

**«10.03.01 Информационная безопасность»**

Образовательная программа **«Информационная безопасность»**

**О Т Ч Е Т**

**По лабораторной работе «JWT»**

Проверил:

преп. Башун В.В.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Выполнил:

Новиков В. С. МКБ 241

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

**Москва, 2025**

# Задание 1 – JWT: Обход аутентификации через не проверяемую подпись (уровень – Apprentice) (2,5 балла)

Лабораторная работа демонстрирует критическую уязвимость: сервер принимает JWT токены без проверки подписи, полагаясь только на содержимое payload. Это позволяет злоумышленнику подделать токен и повышать свои привилегии. Постановка задачи: Авторизуйтесь в своём аккаунте (wiener:peter), извлеките JWT-токен из сессионной cookie и измените поле sub (subject) с wiener на administrator. Используйте поддельный токен для доступа к админ-панели /admin и удалите пользователя carlos.

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-unverified signature

## Решение:

Наши данные wiener:peter

1. Используем Burpe Suite -> Proxy -> HTTP history
2. В браузере переходим в My account
3. Вводим наши учетные данные

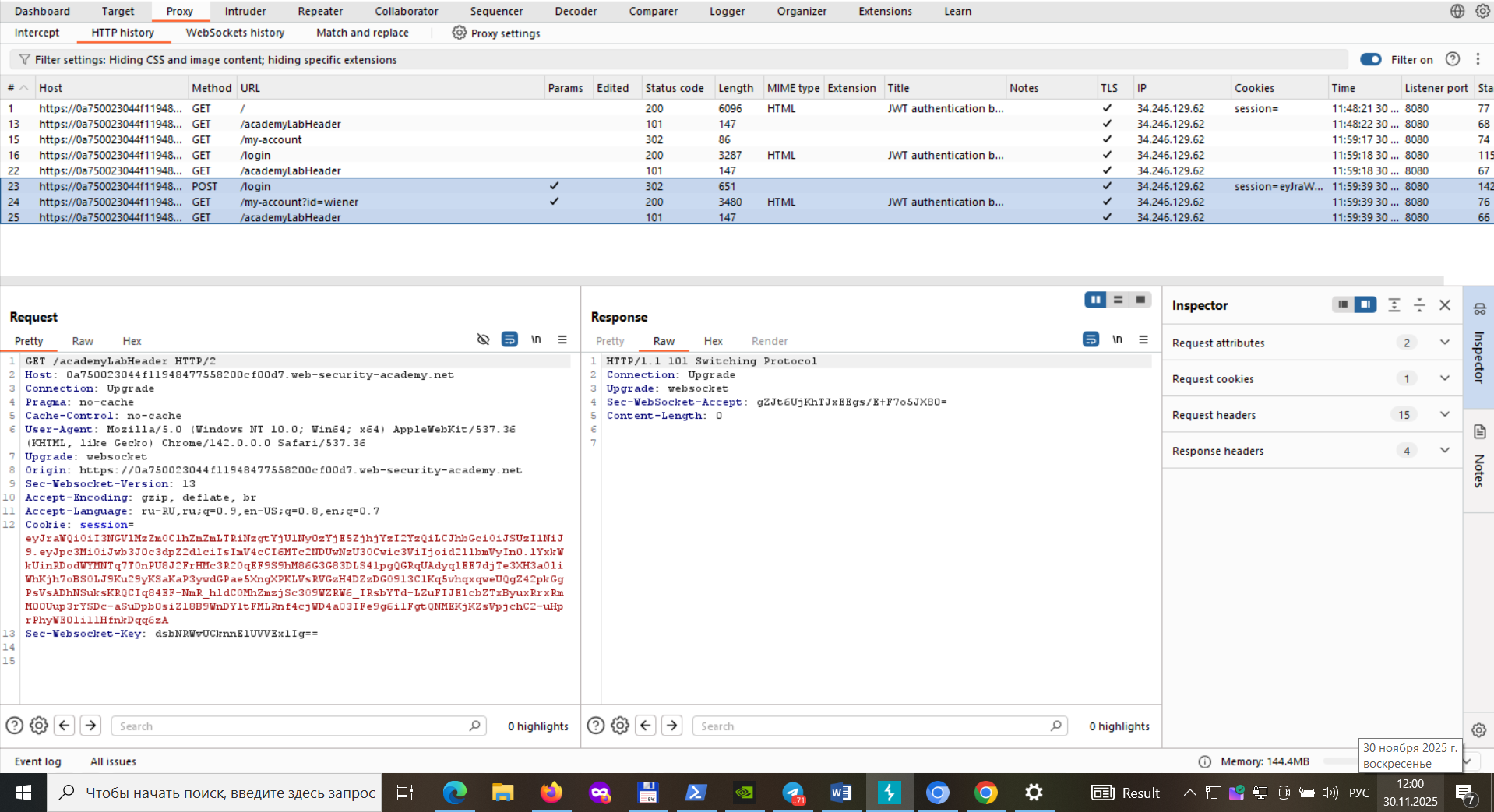


Рисунок 1. «HTTP history»

1. /my-account?id=wiener -> Send to Repeater
2. Переходим в Repeater
3. Меняем /my-account?id=wiener HTTP/2 на /admin HTTP/2

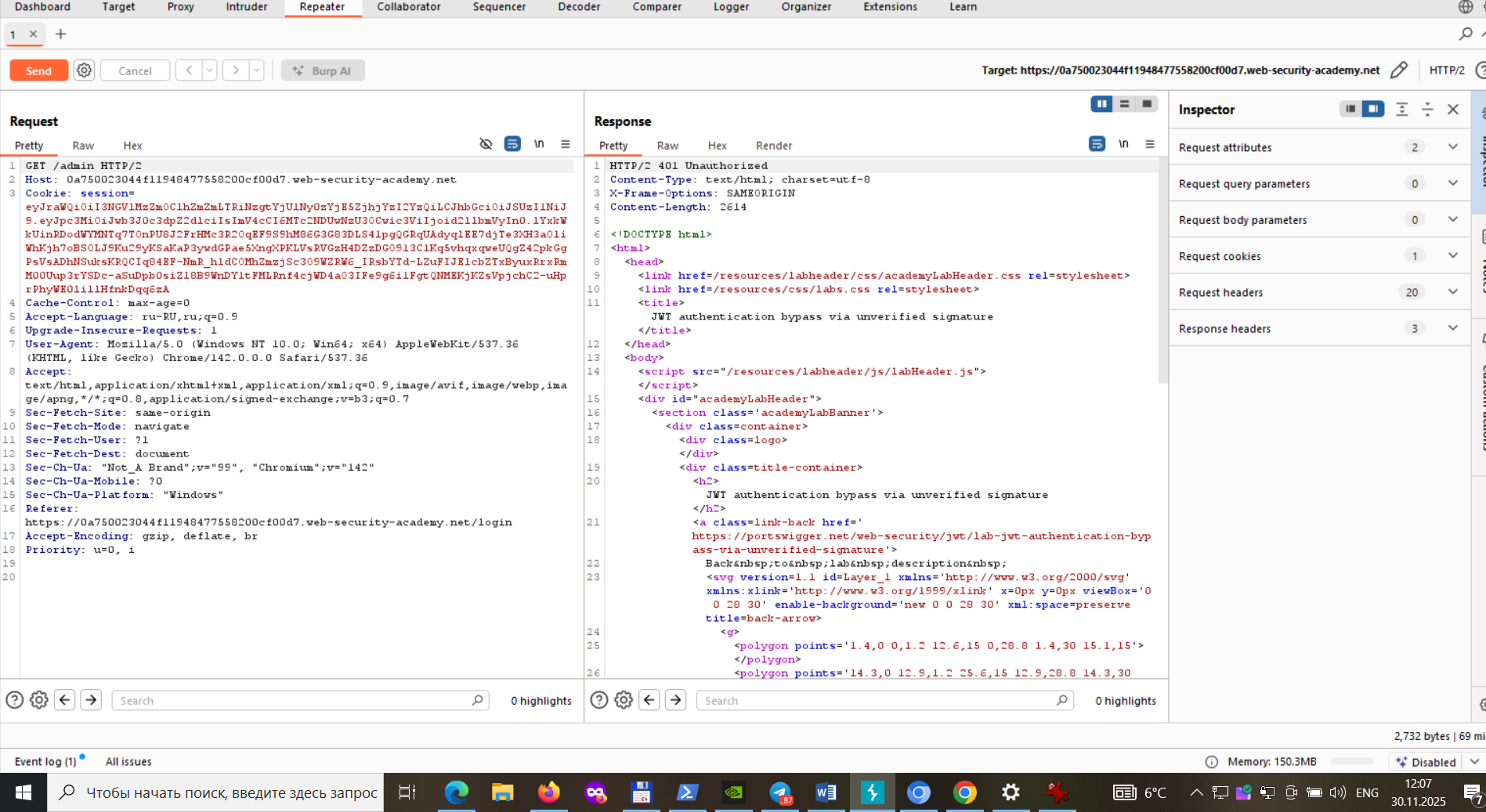


Рисунок 2. «Repeater. /admin»

1. Видим ответ HTTP/2 401 Unauthorized
2. Меняем wiener на administrator

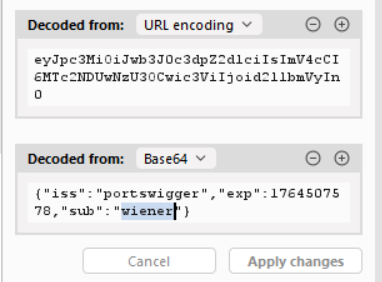


Рисунок 3. «Inspector. Decoded from base64. administrator »

1. Repeater жмем Send и получаем ответ OK



Рисунок 4. «Send. 200 OK»

1. Находим запрос на удаление carlos : /admin/delete?username=carlos

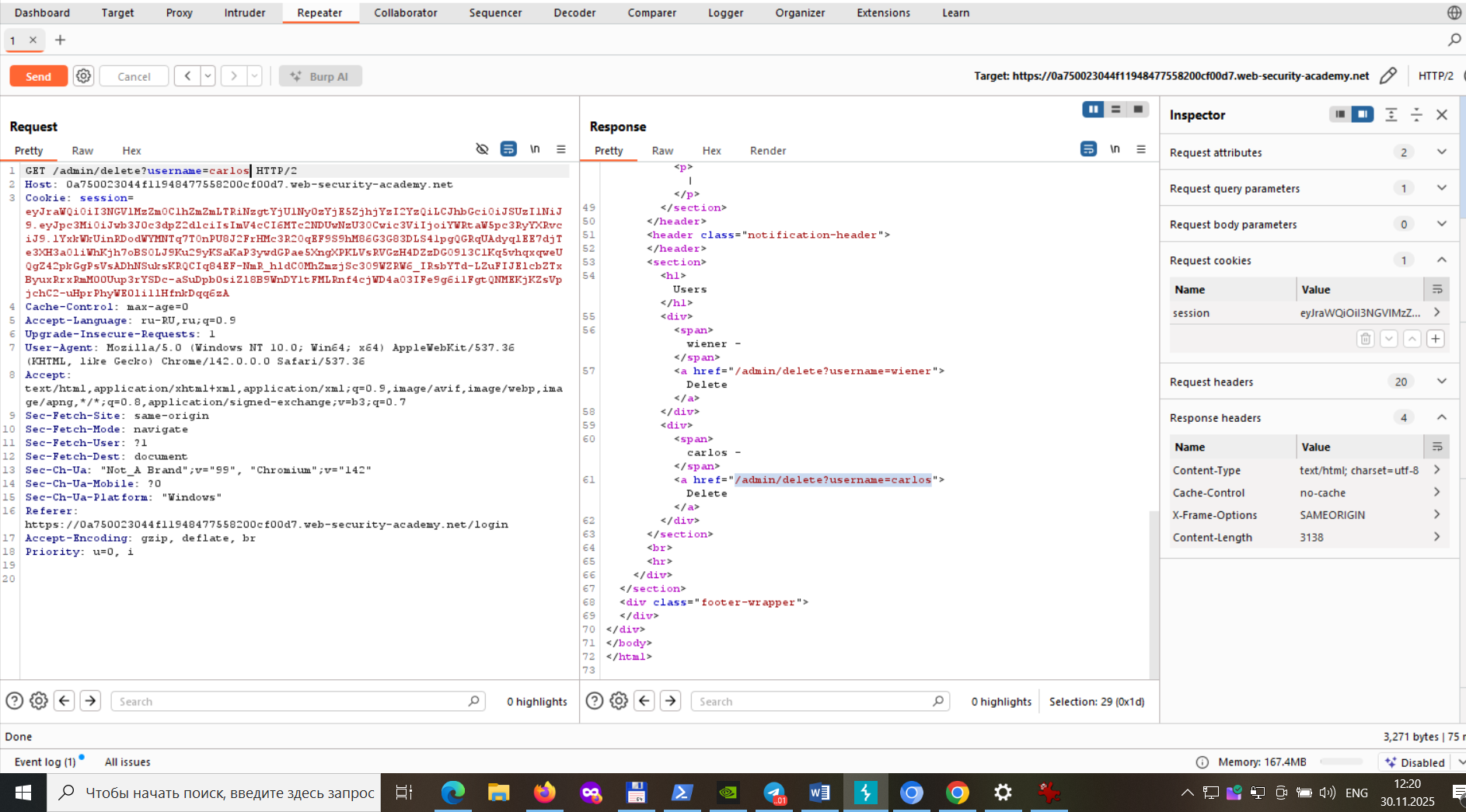


Рисунок 5. «Send. /admin/delete?username=carlos»

1. После отправки запроса – carlos будет удален

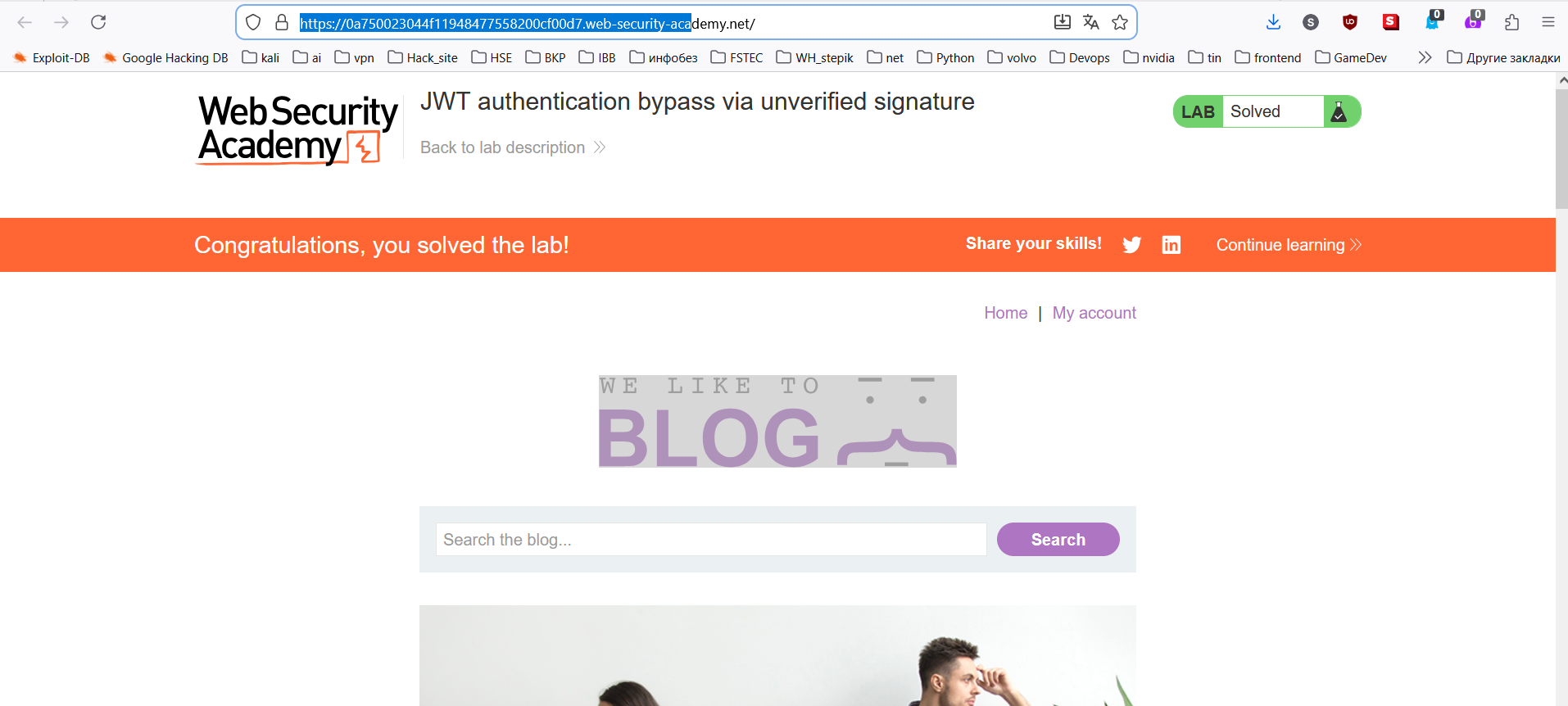


Рисунок 6. «Решение лабораторной»

# Задание 2 – JWT: Обход аутентификации через некорректную проверку подписи (alg=none) (уровень – Apprentice) (2,5 балла)

Лабораторная работа иллюстрирует классическую уязвимость конфигурации JWT: сервер принимает токены с алгоритмом none, интерпретируя их как подписанные, хотя на самом деле подпись отсутствует. Это позволяет подделать токен, удалив подпись и указав alg: none.

Постановка задачи: Авторизуйтесь в аккаунте wiener:peter, извлеките JWT из сессионной cookie, измените значение поля sub на administrator, установите алгоритм none в заголовке и удалите подпись (оставив точку после payload). Используйте модифицированный токен для доступа к /admin и удаления пользователя carlos.

https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature verification

## Решение:

Наши данные wiener:peter

1. Используем Burpe Suite -> Proxy -> HTTP history
2. В браузере переходим в My account
3. Вводим наши учетные данные

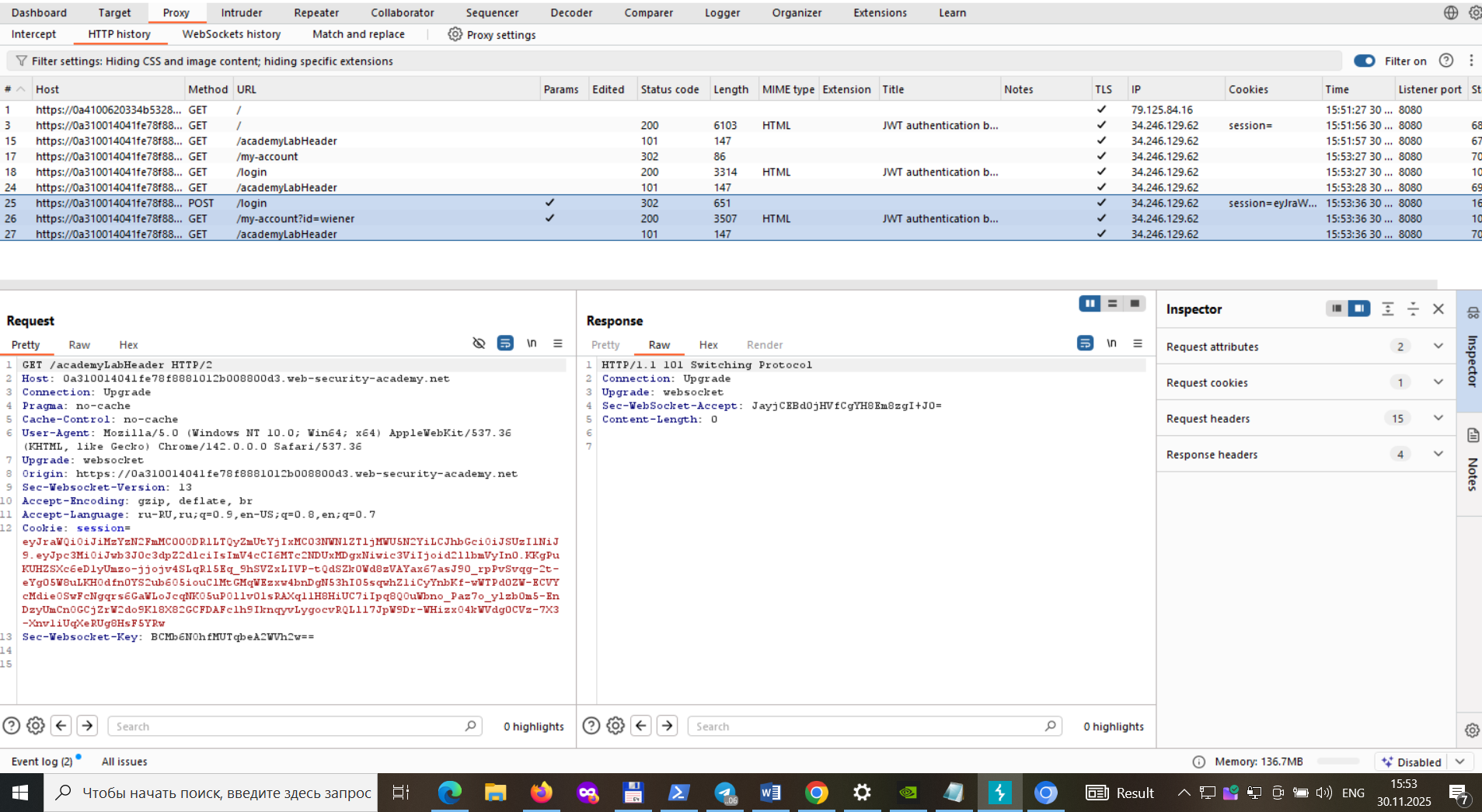


Рисунок 7. «HTTP history»

1. /my-account?id=wiener -> Send to Repeater
2. Переходим в Repeater
3. Меняем /my-account?id=wiener HTTP/2 на /admin HTTP/2

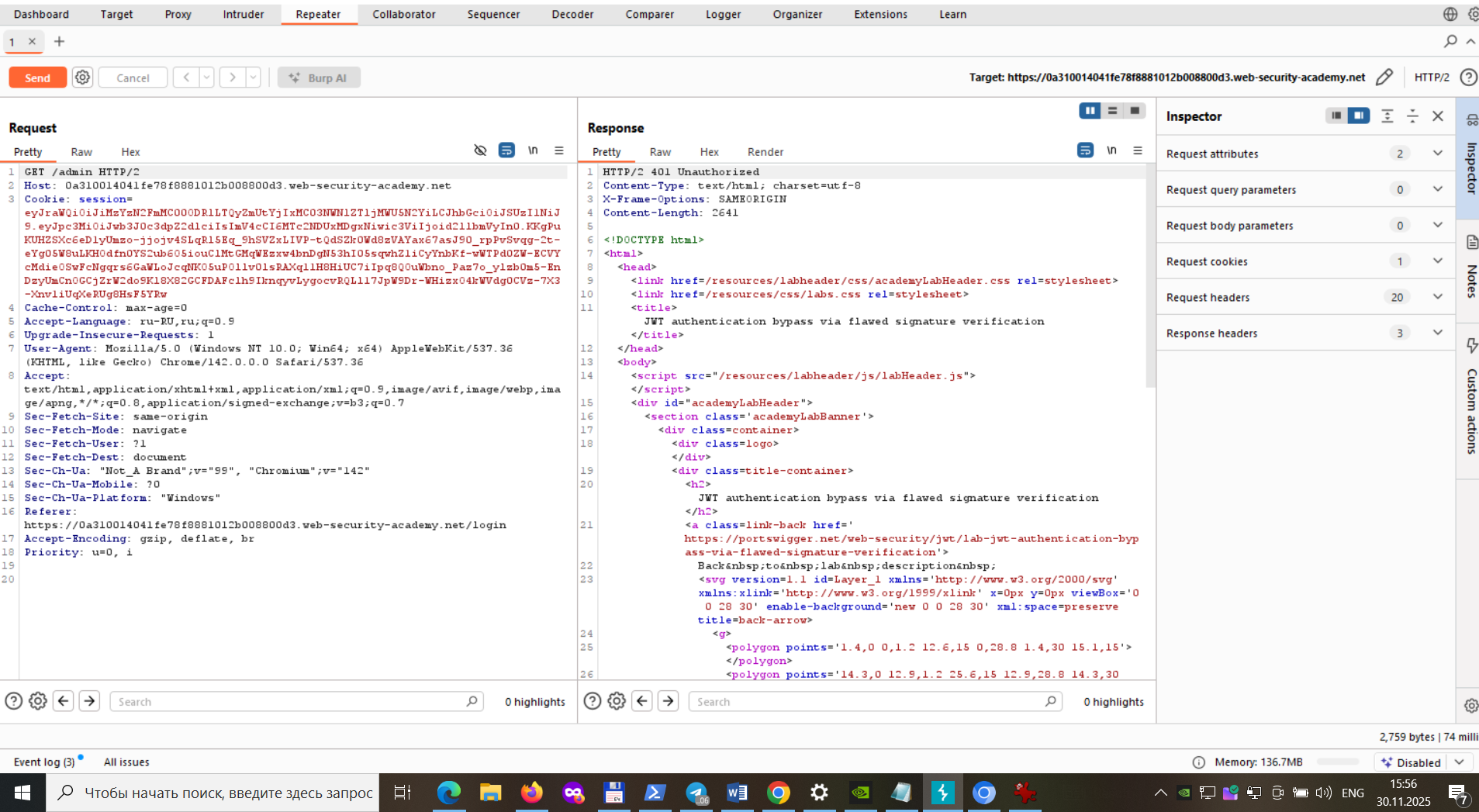


Рисунок 8. «Repeater. /admin»

1. Видим ответ HTTP/2 401 Unauthorized

Меняем в **payload of the JWT** wiener на administrator и **header of the JWT** RS256 на none

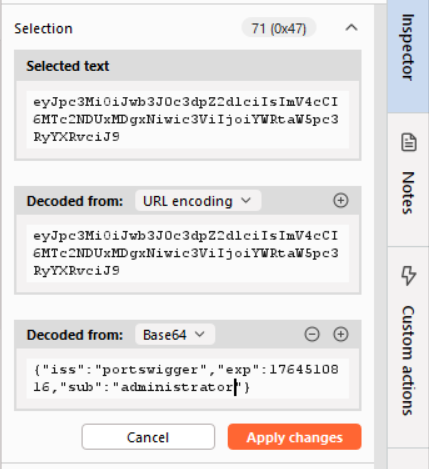
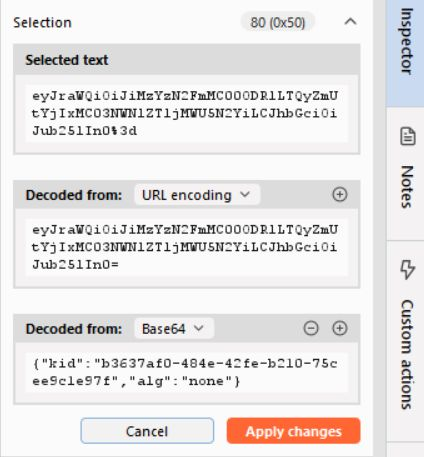
 

Рисунок 9. «Inspector: wiener -> administrator; RS256 -> none»

1. Удаляем подпись с JWT

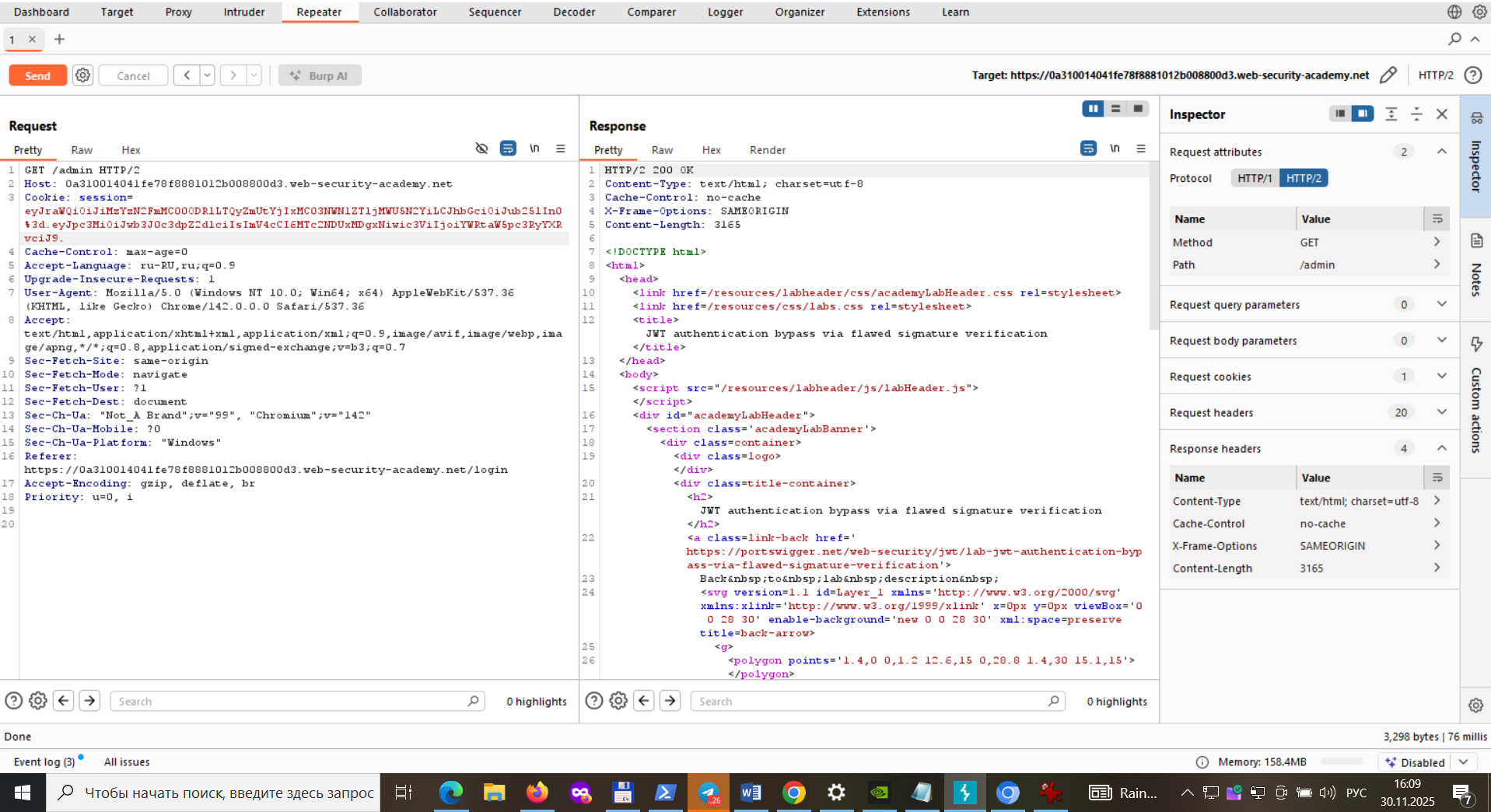


Рисунок 10. «JWT без подписи»

1. Получаем ответ HTTP/2 200 OK
2. Находим запрос на удаление carlos : /admin/delete?username=carlos

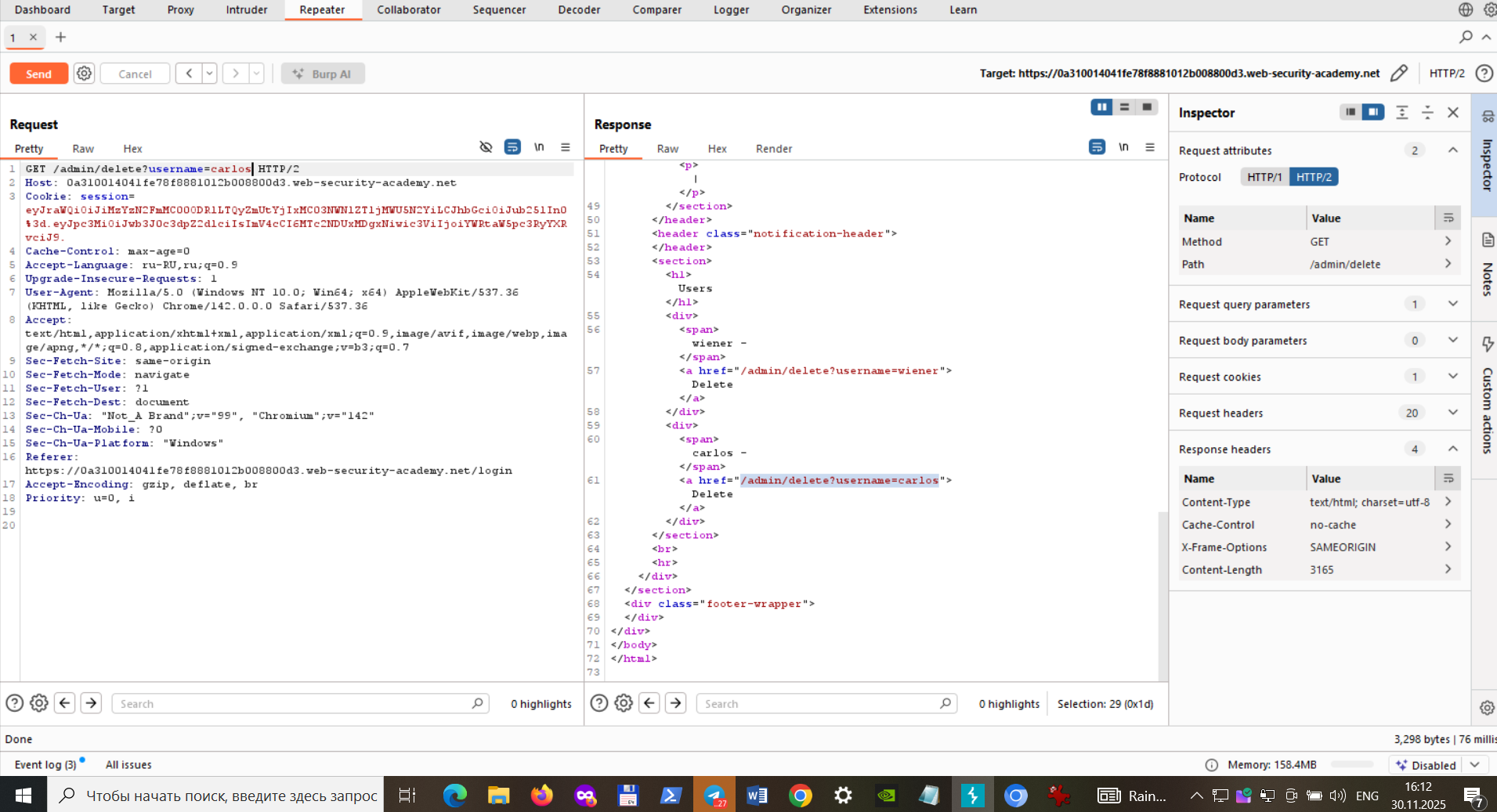


Рисунок 11. «удаление carlos»

1. После отправки запроса – carlos будет удален

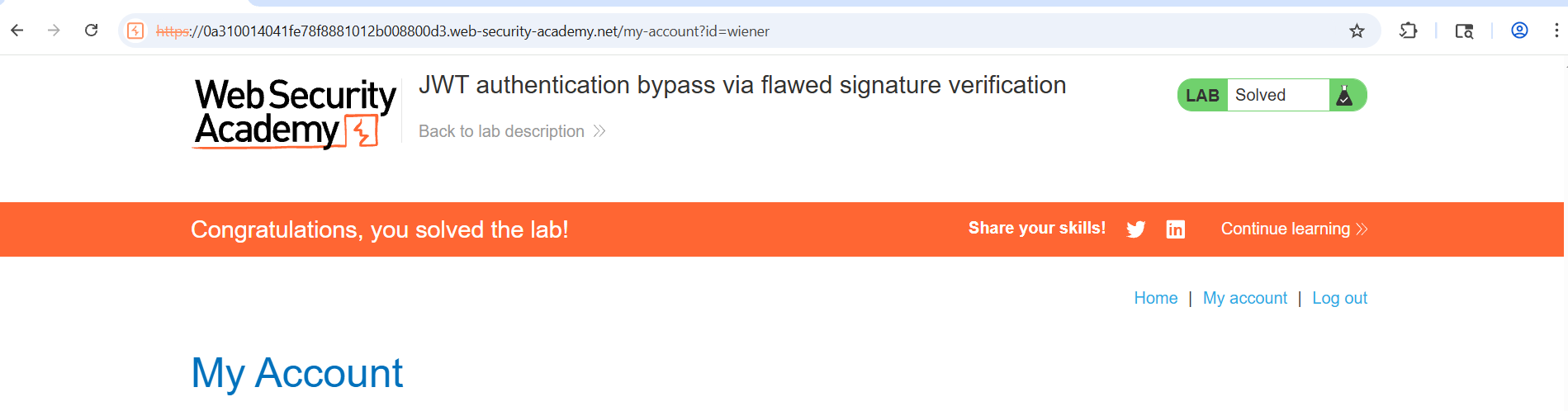


Рисунок 12. «Решение лабораторной»