**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 семинару «Разработка защищенных приложений»**

**Студент:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Новиков В. М. |  |  |
|  | Фамилия И.О. |  | Подпись |

**Преподаватель:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ведущий программист МИЭМ НИУ ВШЭ |  | Башун В.В. |  |  |
| должность и место работы |  | Фамилия И.О. |  | подпись |

**Отчет защищен с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва, 2025**

# Задание 1 – PortSwigger — IDOR (по названию) (уровень - Apprentice)

Ссылка на задание:

<https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>

Решение:

1. Запуск Burp Suite Community Edition / ZAP
2. Перейти Proxy -> Open browser -> вставить ссылку на задание
3. На сайте перейти в [Live chat](https://0aea004e03e9081b80c07bd2001f00f8.web-security-academy.net/chat) -> ввести любой текст -> View transcript
4. HTTP history -> найти переход на View transcript

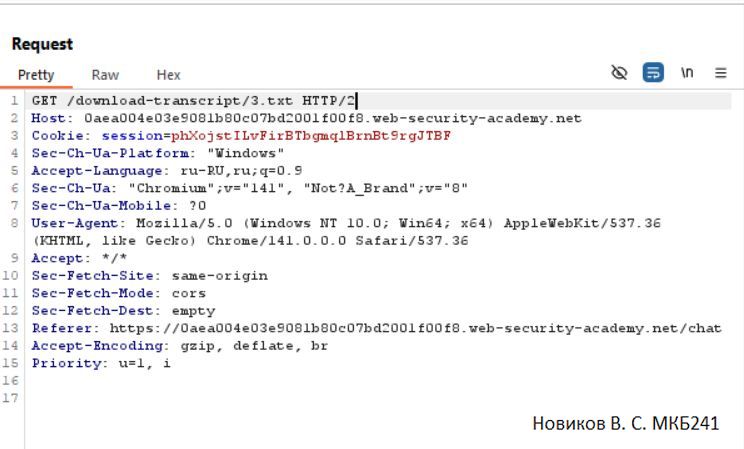


Рисунок 1. Оригинальный запрос.

1. Send to Repeater -> переходим в Repeater
2. Перейти Repeater
3. Заменить GET /download-transcript/3.txt HTTP/2 на:

GET /download-transcript/1.txt HTTP/2

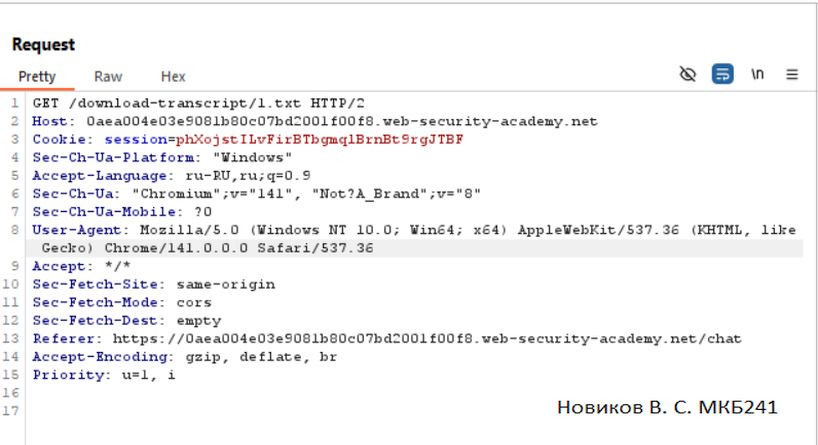


Рисунок 2. Новый запрос GET /download-transcript/1.txt HTTP/2

1. Отправит новый измененный запрос и проверить ответ

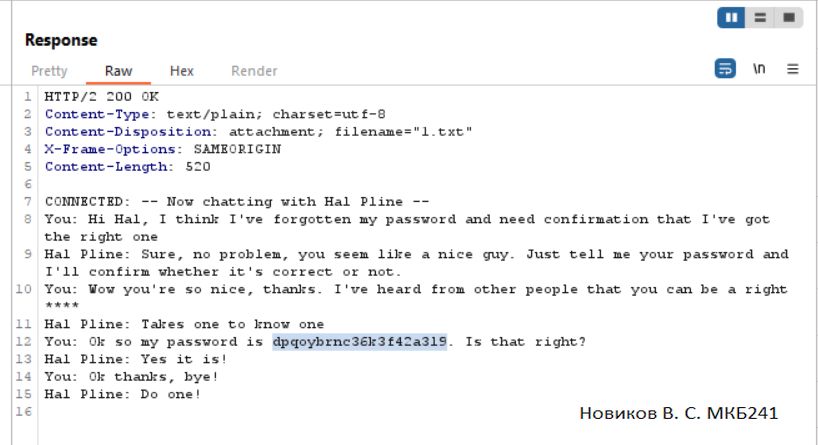


Рисунок 3. Ответ на запрос GET /download-transcript/1.txt HTTP/2

1. В ответе мы видим историю переписки где указан пароль пользователя

carlos

dpqoybrnc36k3f42a3l9

# Задание 2 – PortSwigger. Модификация user id через параметр запроса (уровень - Apprentice)

Ссылка:

<https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids>

1. Запуск Burp Suite Community Edition / ZAP
2. Перейти Proxy -> Open browser -> вставить ссылку на задание
3. HTTP history -> переходим на View post -> ищем carlos
4. Нажать на carlos -> в ссылке будет указан его ID

https://0a3200dd03a0d053803c71a2001f0093.web-security-academy.net/blogs?userId=ad55ff10-ef5b-4091-a52c-64f685fcb579

1. Возвращаемся в начало -> My account
2. Burp Suite -> Proxy -> HTTP history -> ищем наш вход My account

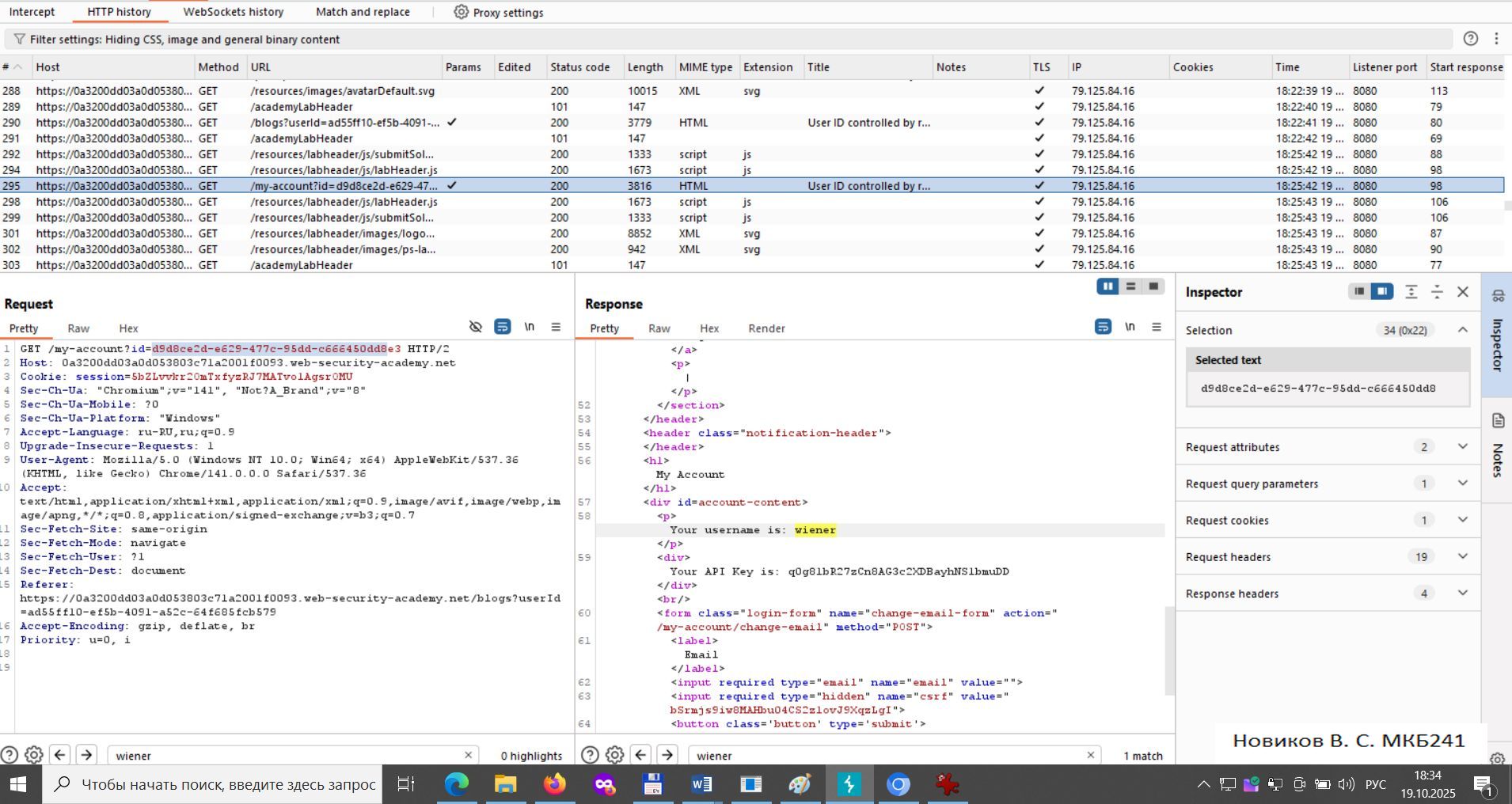


Рисунок 4. History

1. Send to Repeater -> переходим в Repeater

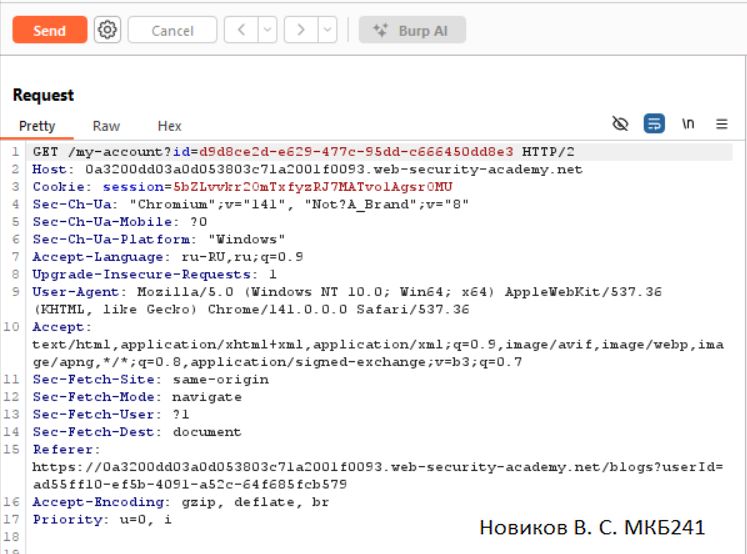


Рисунок 5. Request оригинал

1. Изменяем ID пользователя

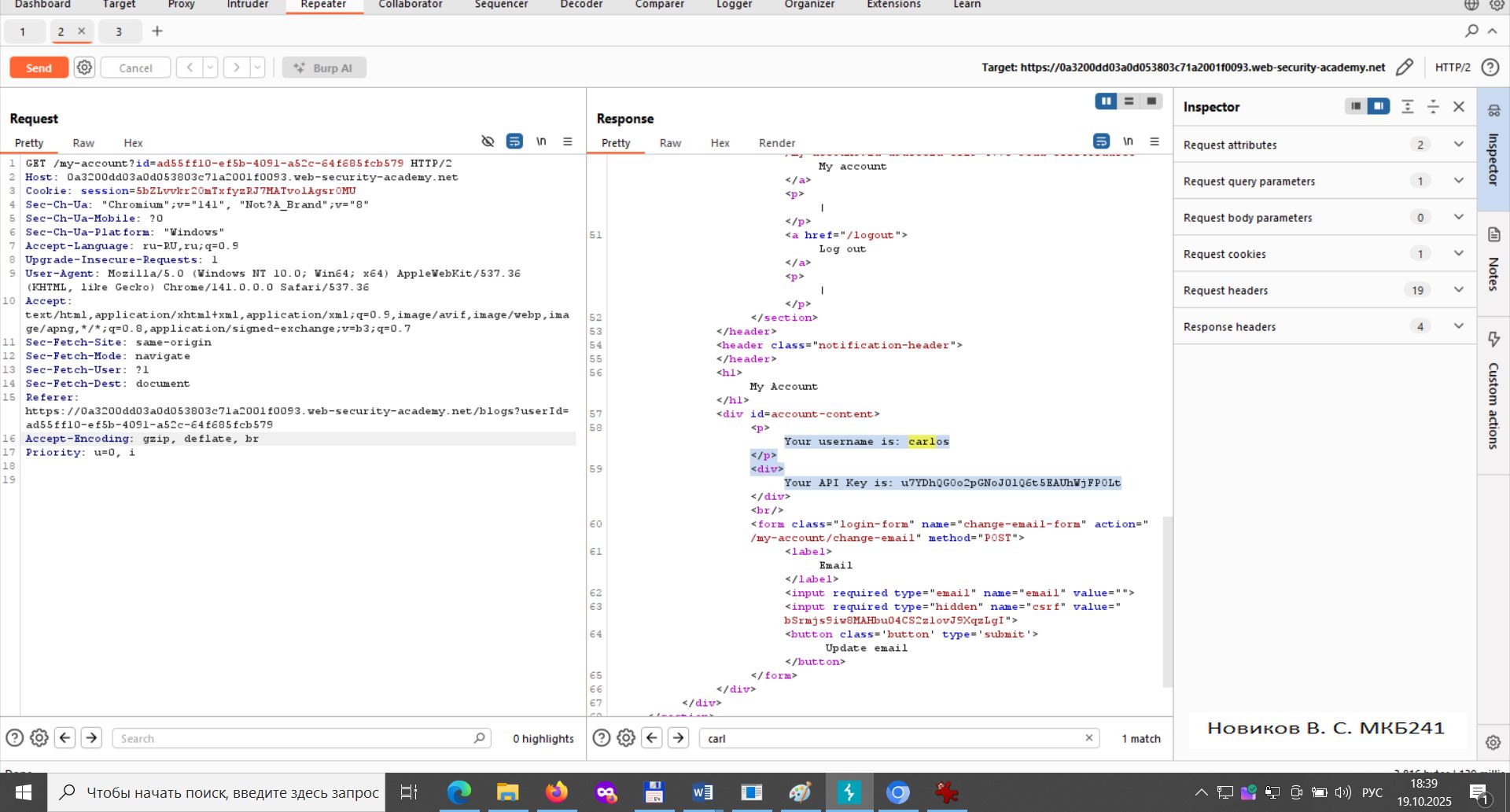


Рисунок 6. Измененный запрос

1. В ответе ищем carlos и видим его ID

carlos

u7YDhQGOo2pGNoJ0lQ6t5EAUhWjFPOLt

# Задание 3 – PortSwigger. Простой пример file path traversal (уровень - Apprentice)

Ссылка:

https://portswigger.net/web-security/file-path-traversal/lab-simple

1. Запуск Burp Suite Community Edition / ZAP
2. Перейти Proxy -> Open browser -> вставить ссылку на задание
3. HTTP history -> включаем фильтр image

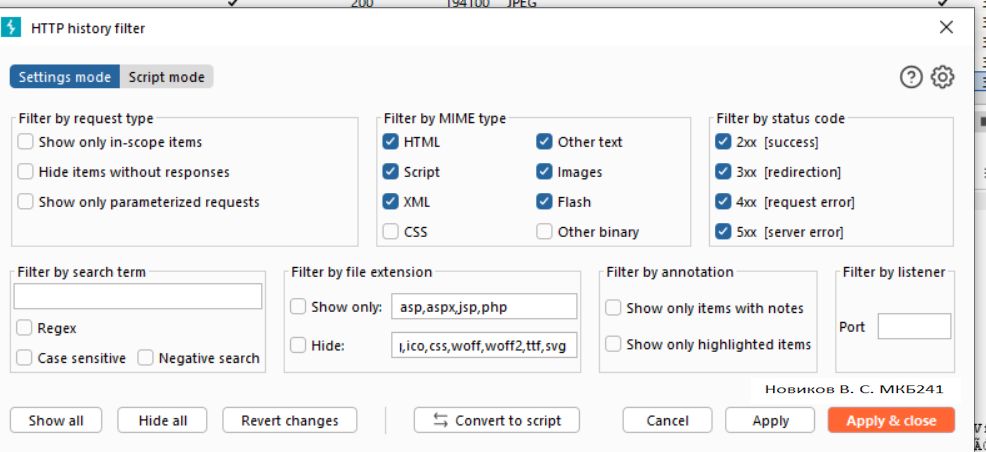


Рисунок 7. Настройка фильтров

1. Находим любую картинку

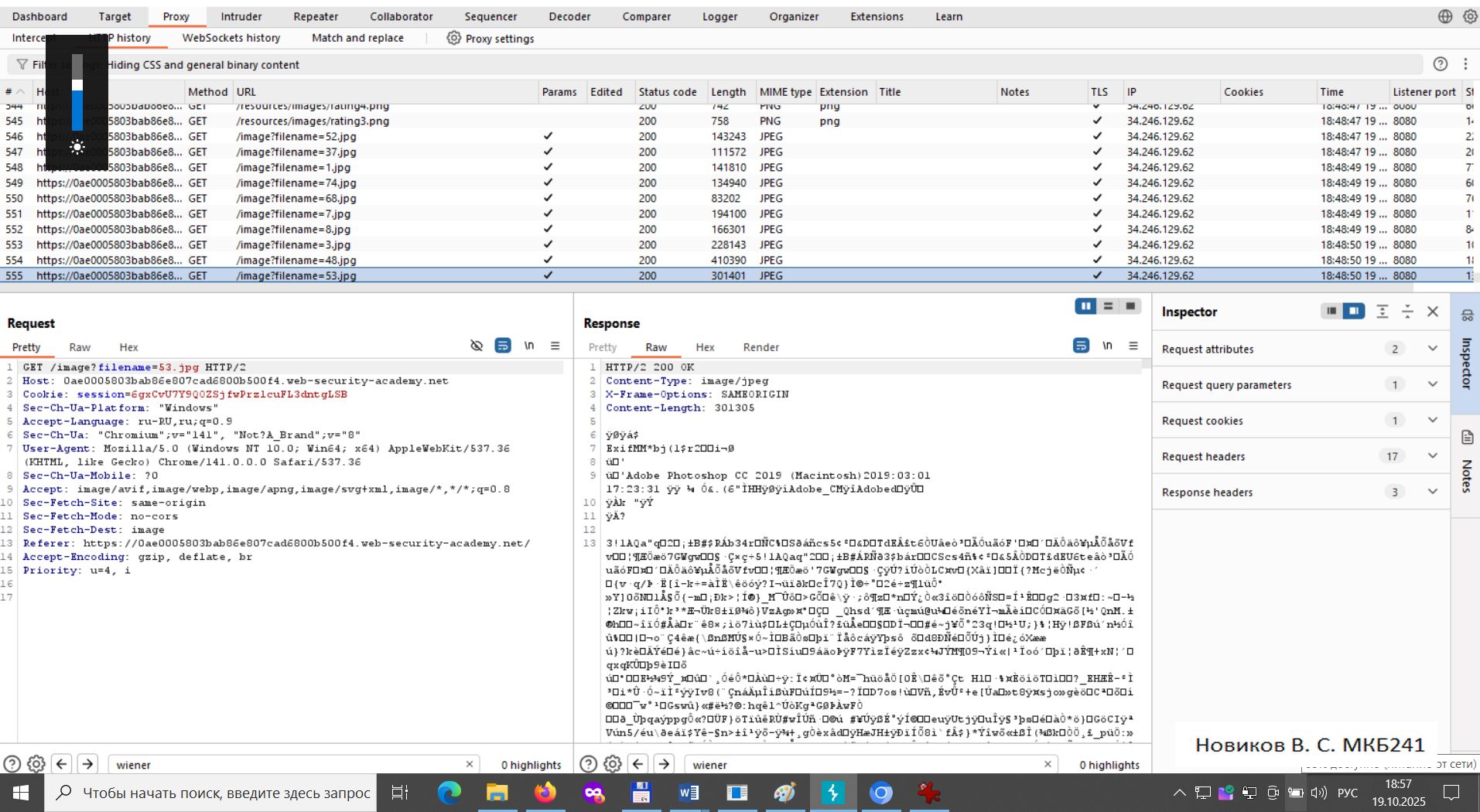


Рисунок 8. Запрос с картинкой, где указан путь

1. Send to Repeater -> переходим в Repeater
2. Меняем запрос GET /image?filename=53.jpg HTTP/2 на:

GET /image?filename=../etc/passwd HTTP/ - проверяем Response

GET /image?filename=../../etc/passwd HTTP/ - пусто

GET /image?filename=../../../etc/passwd HTTP/ - есть файл etc/passwd

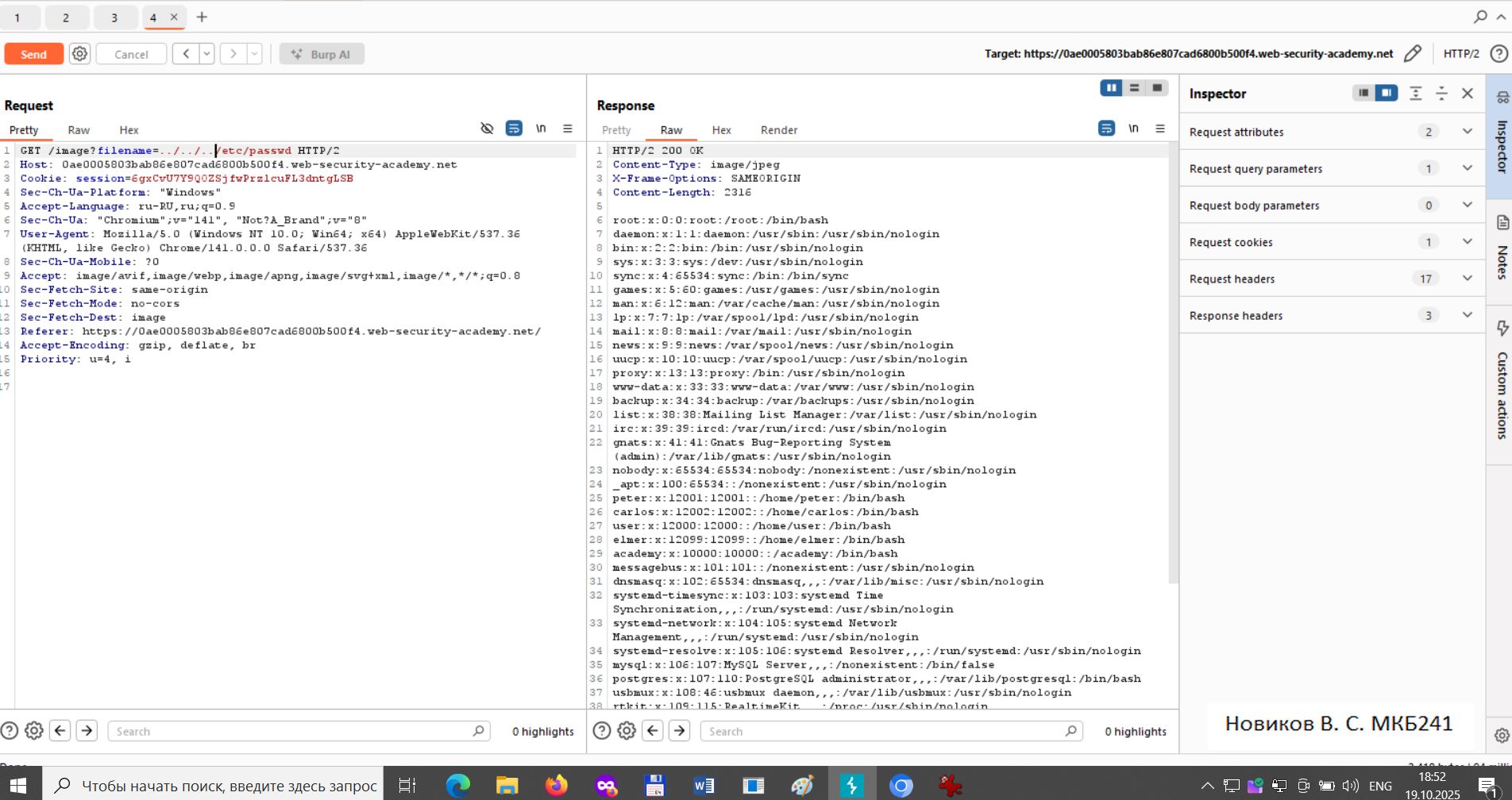


Рисунок 9. Response etc/passwd

Задание 4 – PortSwigger. File path traversal с обходом простой защиты

Ссылка:

https://portswigger.net/web-security/file-path-traversal/lab-sequences-stripped-non-recursively

1. Запуск Burp Suite Community Edition / ZAP
2. Перейти Proxy -> Open browser -> вставить ссылку на задание
3. HTTP history -> включаем фильтр image
4. Send to Repeater -> переходим в Repeater

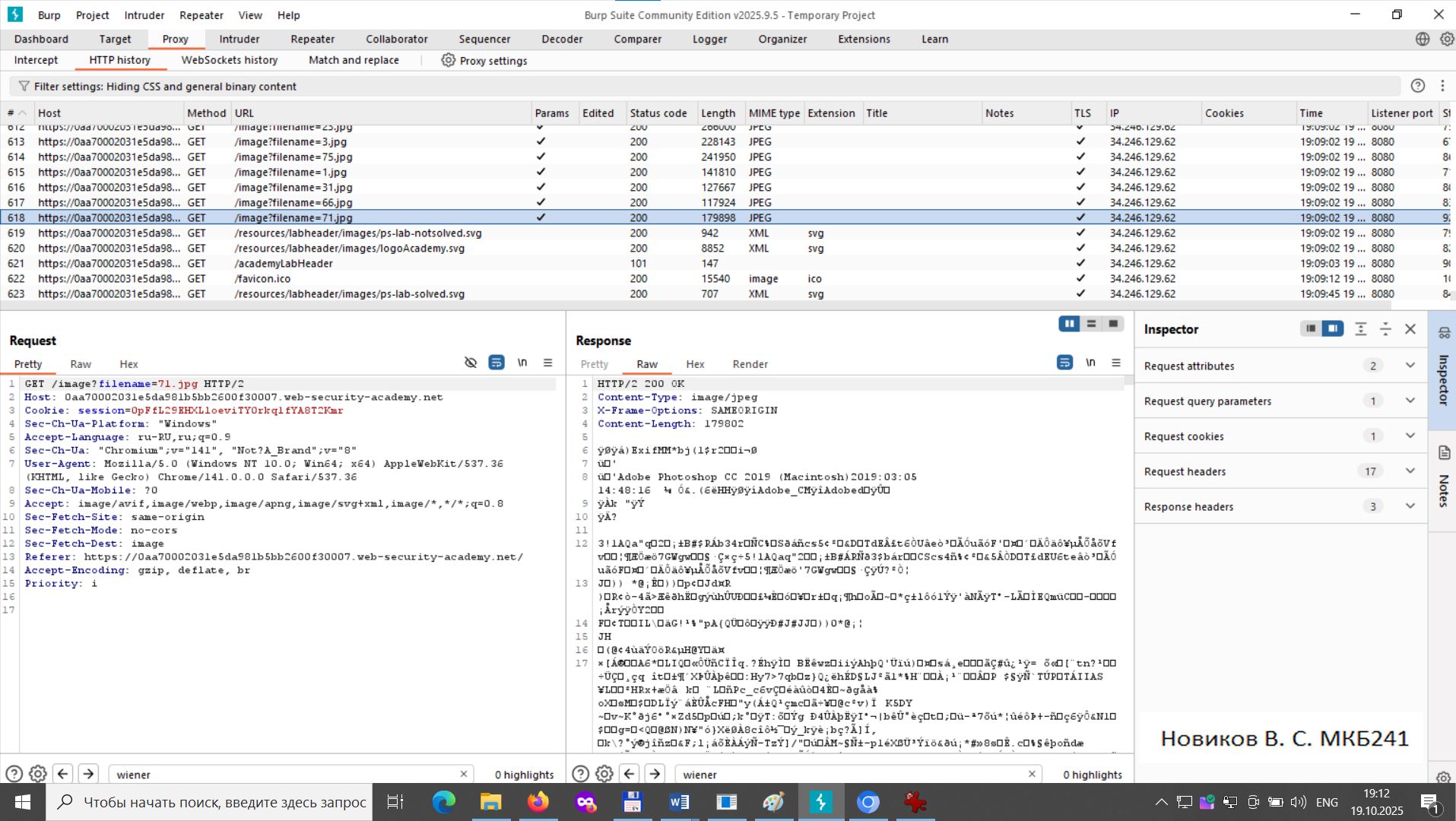


Рисунок 10. Запрос с картинкой, где указан путь

1. Меняем запрос GET /image?filename=71.jpg HTTP/2 на:

GET /image?filename= ....//etc/passwd HTTP/ - проверяем Response

GET /image?filename= ....//....//etc/passwd HTTP/ - пусто

GET /image?filename= ....//....//....//etc/passwd HTTP/ - есть файл etc/passwd

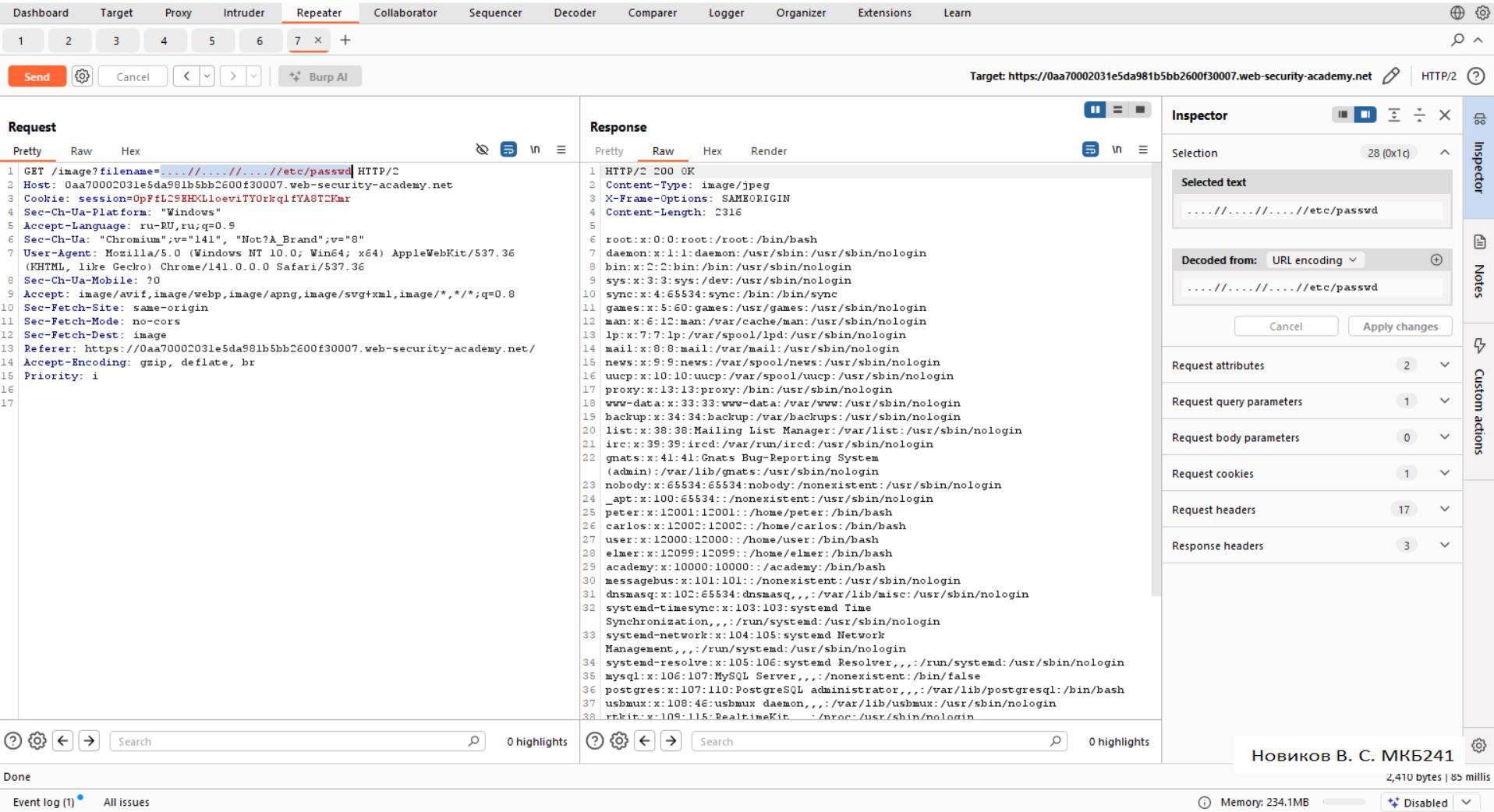


Рисунок 11. Response etc/passwd