# Authentication/authorization

## 1.1 Brute force

We were able to brute force passwords.

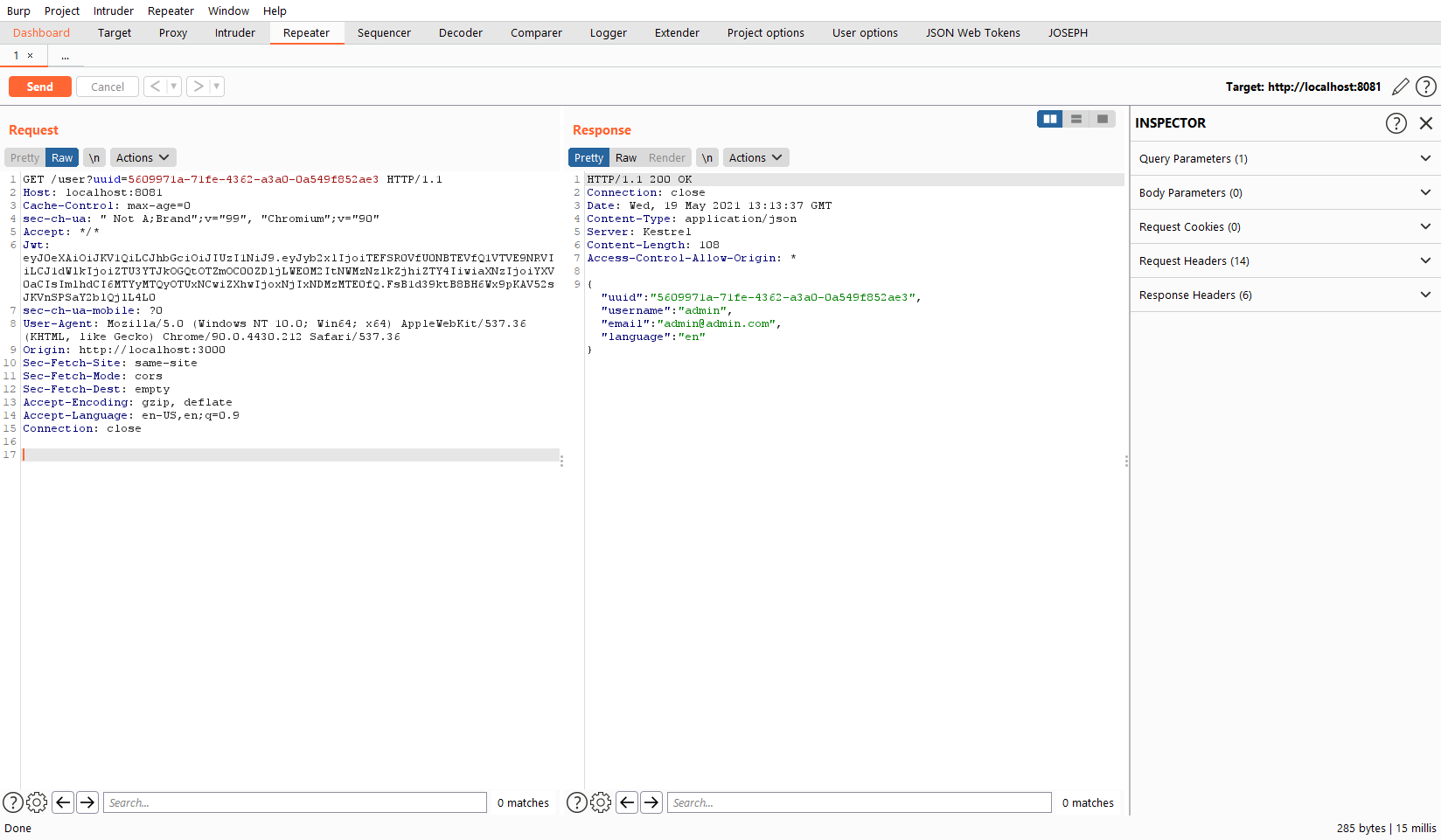
## 1.2 JWT Signature validation

There was no validation on the JWT. This allowed us to mess with the JWT, including giving ourselves a different role.

It is also possible to get the user details of another user by changing the uuid in the JWT.

## 1.3 General authorization

Only the front-end looked at the token. The other services didn’t check if there was a valid token. Leaving all information as public information, not sure if this is intended.



# Cookie flags

The JWT was not flagged with HttpOnly which leaves it vulnerable to XSS attacks.

