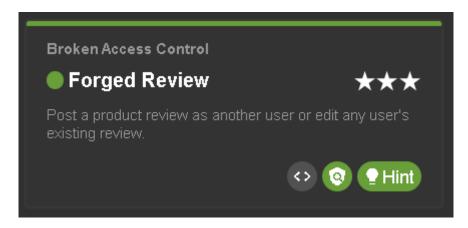
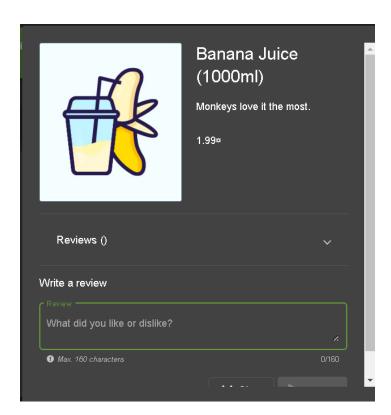
Broken Access Control in OWASP Juice Shop

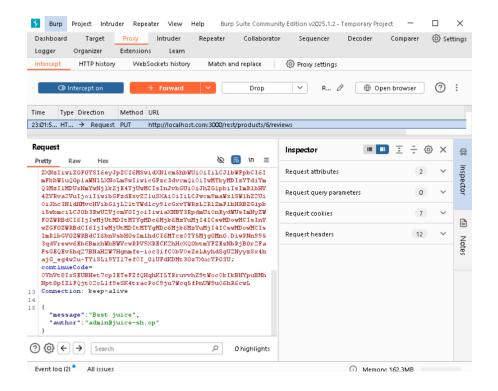


Here we need to post a review for an item as another user by exploiting the Broken access control vulnerability

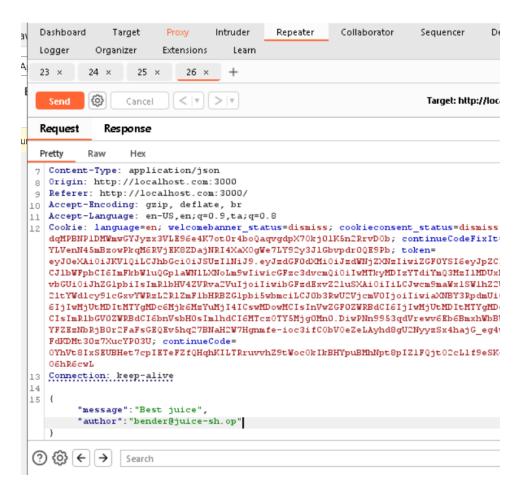
Go to the review section of an item



write an review and intercept the request using burp suite



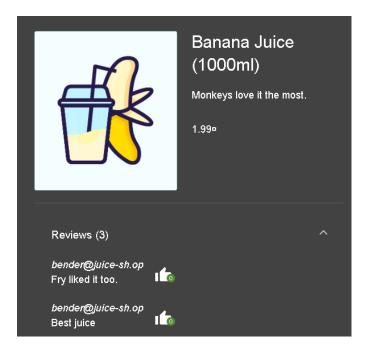
sending the request to the repeater,



Here changing the name of the author with any existing username and forwarding the request.

```
Cancel
  Request
             Response
 Pretty
          Raw
                 Hex
                         Render
 1 HTTP/1.1 201 Created
 2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
 4 X-Frame-Options: SAMEORIGIN
 5 Feature-Policy: payment 'self'
 6 X-Recruiting: /#/jobs
 7 Content-Type: application/json; charset=utf
8 Content-Length: 20
9 ETag: W/"14-Y53wuE/mmbSikKcT/WualL1N65U"
10 Vary: Accept-Encoding
11 Date: Sun, 23 Feb 2025 17:32:22 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
        "status": "success"
```

we got a success response



The review is updated on the server with another user's name

Pote	ntial	Dam	age.
ı Oto	nuat	Daiii	ugo.

The attacker can send forged reviews to any item on behalf of any other user's name.

To Prevent:

Proper Authorization should be carried out before executing the request