OWASP Juice Shop pentest

tested by: Rahib
Test conducted: 6/8/2023
Client: TCM Acafemy

Scope

- `http://pwst-server:8002`
    - All paths in scope

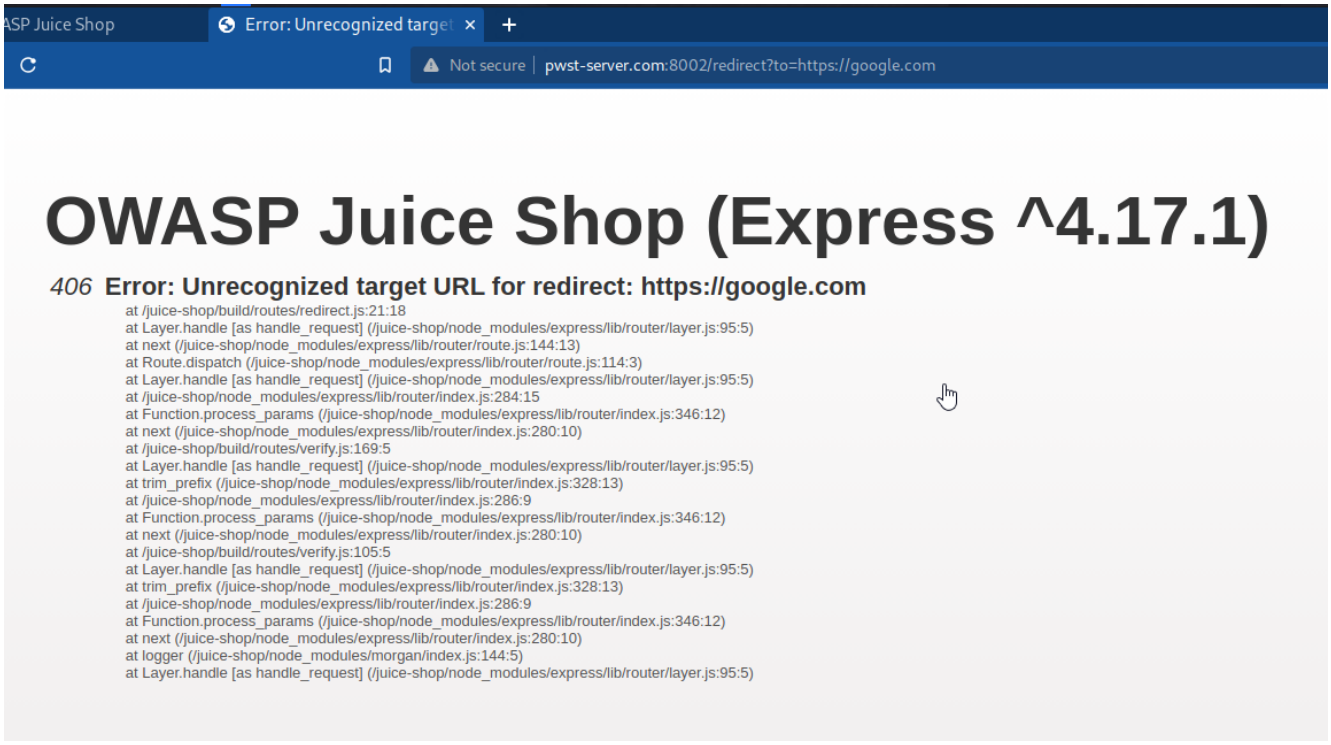
Enumeration

- Base Application is Angular

Found URIs outside of Angular

- http://pwst-server.com:8002/profile
- http://pwst-server.com:8002/ftp
- http://pwst-server.com:8002/video
- http://pwst-server.com:8002/rest
- http://pwst-server.com:8002/metrics
- http://pwst-server.com:8002/assets
- http://pwst-server.com:8002/redirect
- http://pwst-server.com:8002/api
- http://pwst-server.com:8002/Video
- http://pwst-server.com:8002/restaurants
- http://pwst-server.com:8002/assets/public/images/JuiceShop_Logo.png
- http://pwst-server.com:8002/assets/public/favicon_js.ico
- http://pwst-server.com:8002/promotion
- http://pwst-server.com:8002/Profile
- http://pwst-server.com:8002/apis
- http://pwst-server.com:8002/restore
- http://pwst-server.com:8002/restoration
- http://pwst-server.com:8002/apidocs

Potential redirect `/redirect?to=`



-

Anguler Paths

- "administration",
- "accounting",
- "about",
- "address/select",
- "address/saved",
- "address/create",
- "address/edit/:addressId",
- "delivery-method",
- "deluxe-membership",
- "saved-payment-methods",
- "basket",
- "order-completion/:id",
- "contact",
- "photo-wall",
- "complain",
- "chatbot",
- "order-summary",
- "order-history",
- "payment/:entity",
- "wallet",

- "login",
- "forgot-password",
- "recycle",
- "register",
- "search",
- "hacking-instructor",
- "score-board",
- "track-result",
- "track-result/new",
- "2fa/enter",
- "privacy-security",
- "privacy-policy",
- "change-password",
- "two-factor-authentication",
- "data-export",
- "last-login-ip",
- "403",
  "**",

Eploitation

`/ftp`

- Information Leakage: confidential document
- Filter bypass: `package.json.bak`
  - Null byte poisning `\ftp\package.json.bak%2500.md`

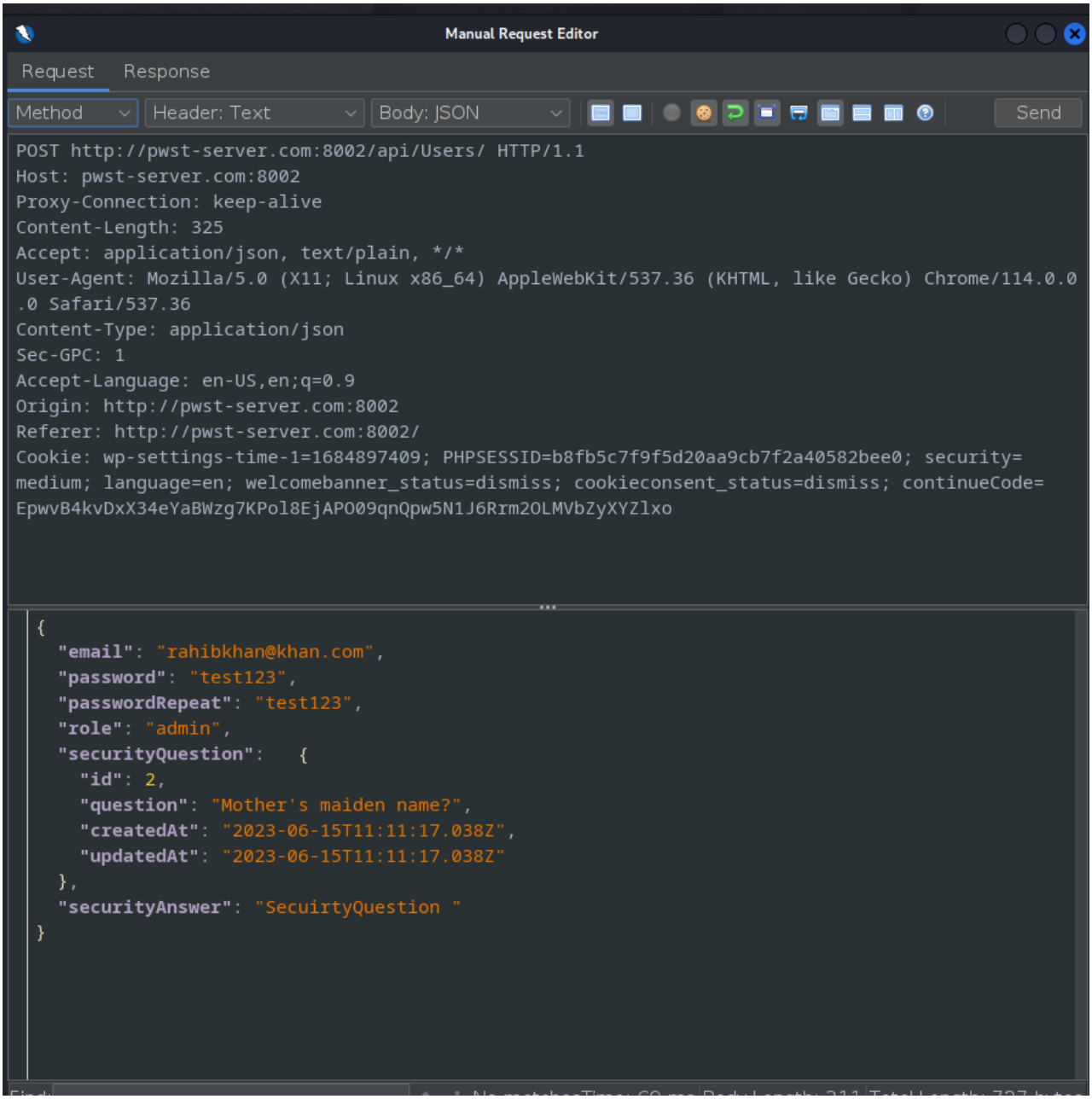
`/rest/user/log`

- SQL injection
  - authentication bypass

###`/api/users`

- Creating admin privileged users account
  - provide `role: admin` data while creating the acount

- Request:

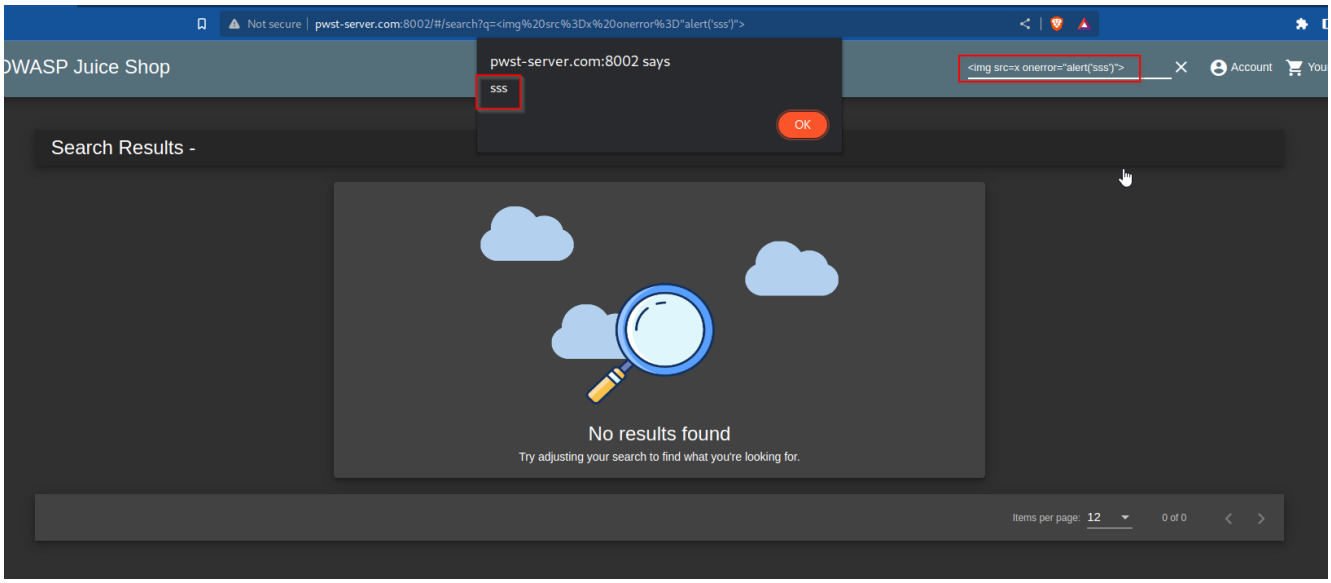


- Response:

`/rest/user/whoami`

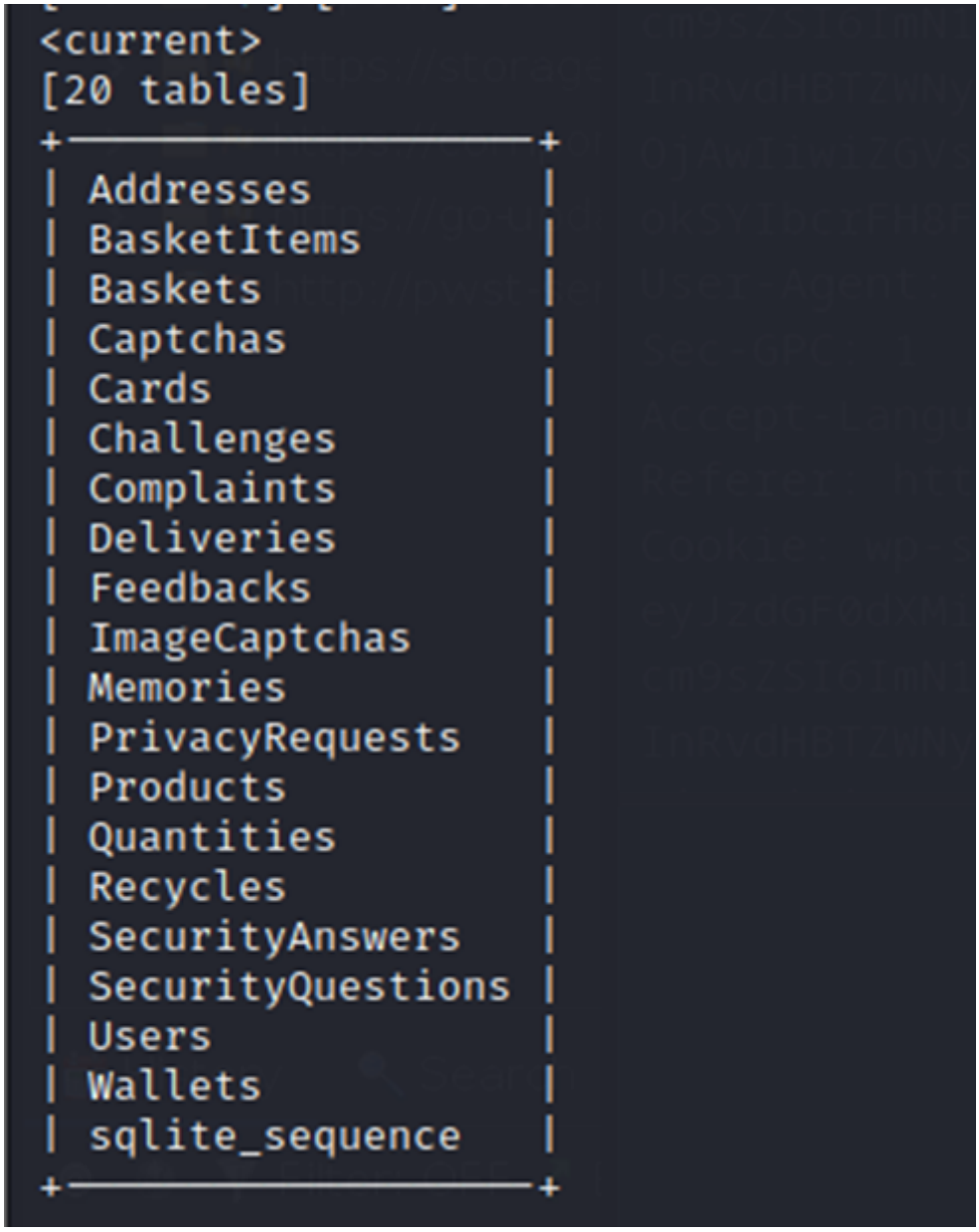
- No `Authorization` header required

`/search?q=`

- Vulnerble to refelected/DOM based XSS
- 

`/rest/product/search=q`

- the `q` parameter is vulnerble to SQL injection



- weak admin password:

```
~/D/pwst-web-hacking  hashcat -a 0 -O -m 0 admin.hash scripts/SecLists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: pthread-haswell-Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz, 2897/5858 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Optimized-Kernel
* Zero-Byte
* Precompute-Init
* Meet-In-The-Middle
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: scripts/SecLists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

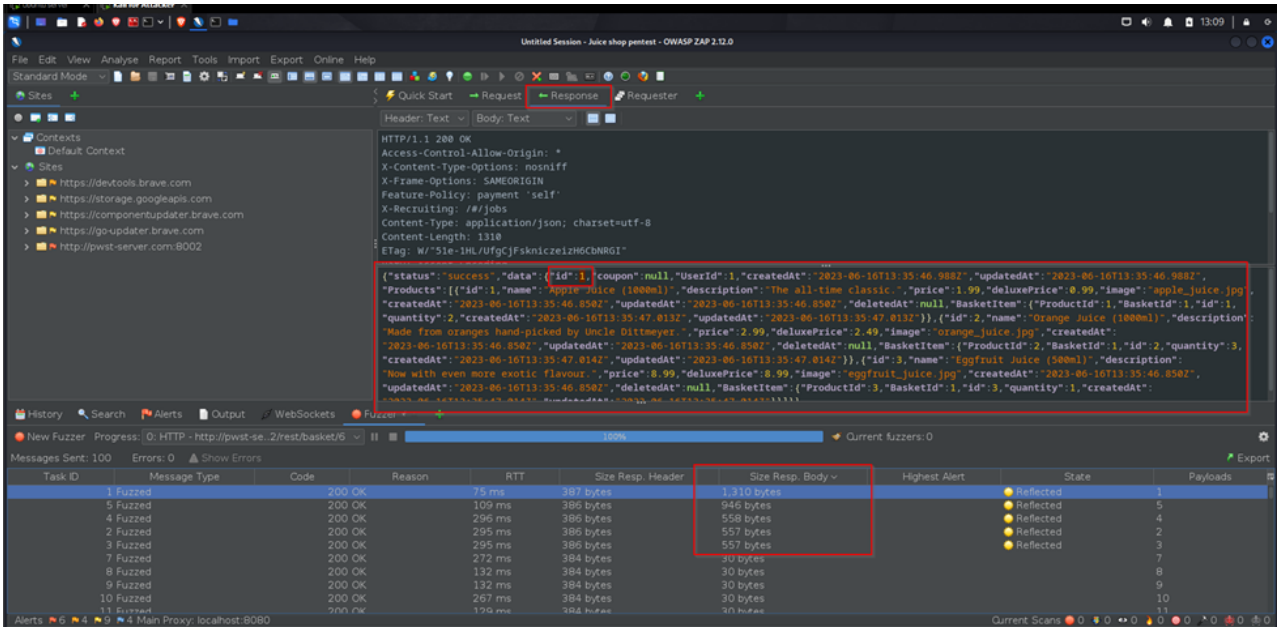
0192023a7bbd73250516f069df18b500:admin123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 0192023a7bbd73250516f069df18b500
Time.Started.....: Fri Jun 16 12:57:14 2023 (1 sec)
Time.Estimated...: Fri Jun 16 12:57:15 2023 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (scripts/SecLists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   176.1 kH/s (0.27ms) @ Accel:512 Loops:1 Thr:1 Vec:8
```

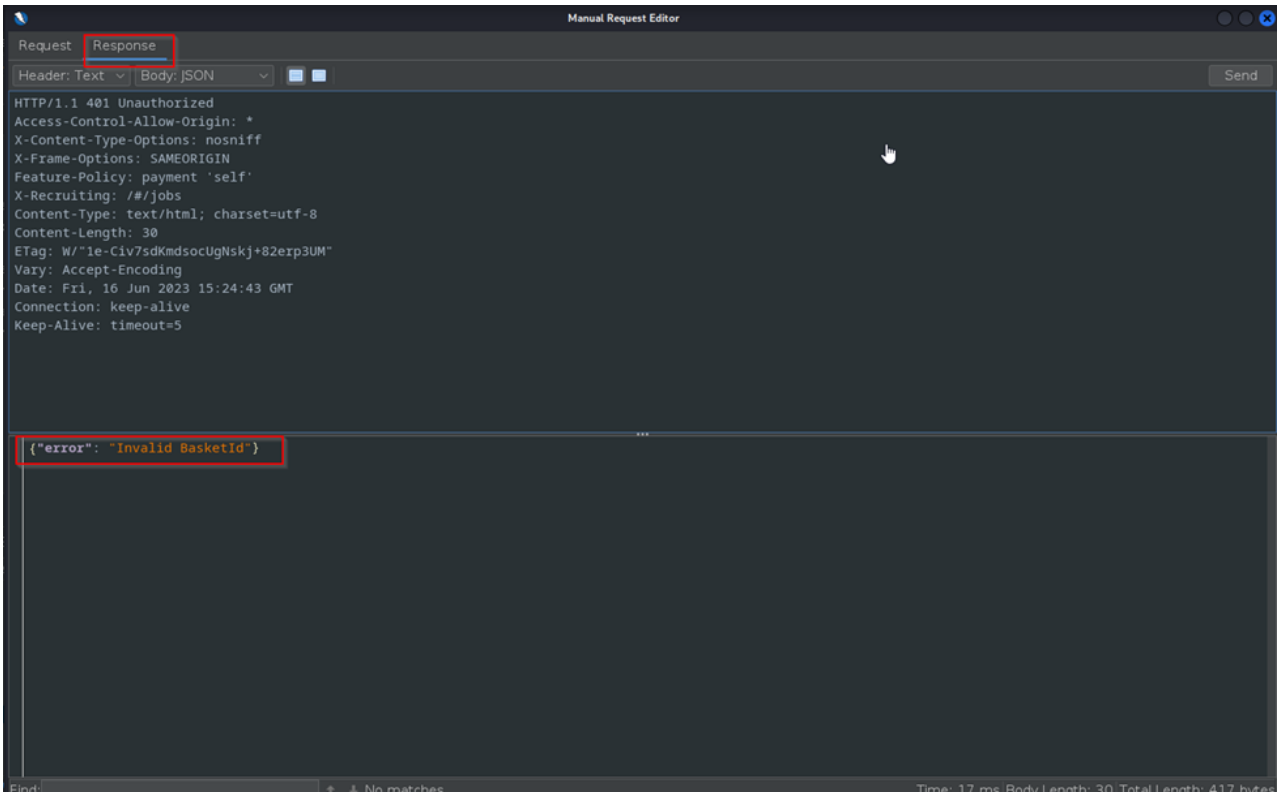
To direct input to this VM, click inside or press Ctrl+G.

`/rest/baskets/:id`

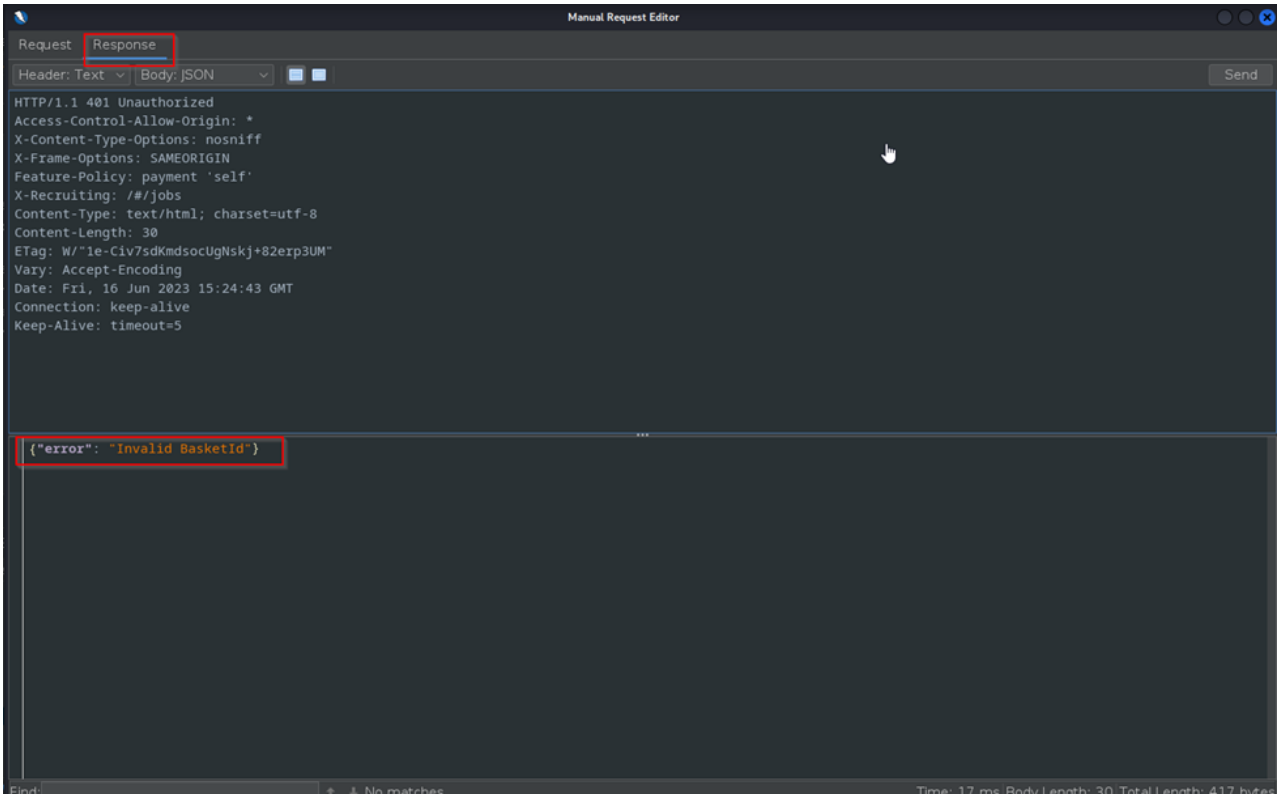
- IDOR: Insecure Direct Object Reference
- Request:
  - ```
    GET http://pwst-server.com:8002/rest/basket/1 HTTP/1.1
    Host: pwst-server.com:8002
    Proxy-Connection: keep-alive
    Accept: application/json, text/plain, */*
    Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
    eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJyYWhpYkByYWhpYi5jb20iLCJwYXNzd29yZCI6IjQyOTdmNDRiMTM5NTUyMzUyNDViMjQ
    5NzM5OWQ3YTkzIiwicm9sZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdX
    Bsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0wNi0xNiAxNTowMToxNy42MjAgKzAwOjAwIiwidXBkYXRlZEF0IjoiM
    jAyMy0wNi0xNiAxNTowMToxNy42MjAgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjg2OTI3NjkwfQ.
    oBlmK97pwkNmWm8QBvimMffvtsdyu8a3jHREcG3TqwTASTeHaMq9wXWX8SOq-myCagBUjVy-493cRp0UbZ0Kye97BN2ziv-7bfUjuXTVQyvebDs4ZFaXKE4uu0qDFd_
    dVmLzvlrqGXeF2cSPsVeRQfEEDIkPxuIeeM8gVcItX7Y
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
    Sec-GPC: 1
    Accept-Language: en-US,en;q=0.8
    ```
- Response:
    ```

- 

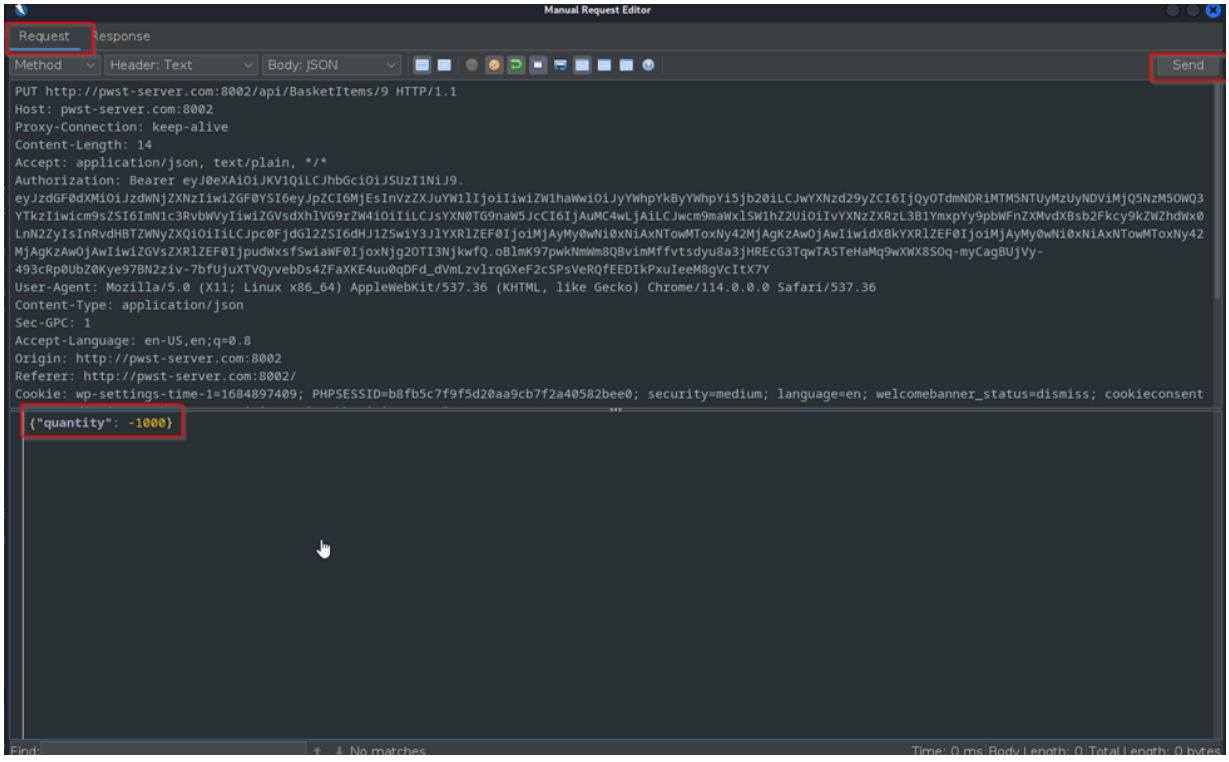
`/api/BasketItems`

- HTTP parameter pollution: POST reqeust
- The Reqeust:
  - 

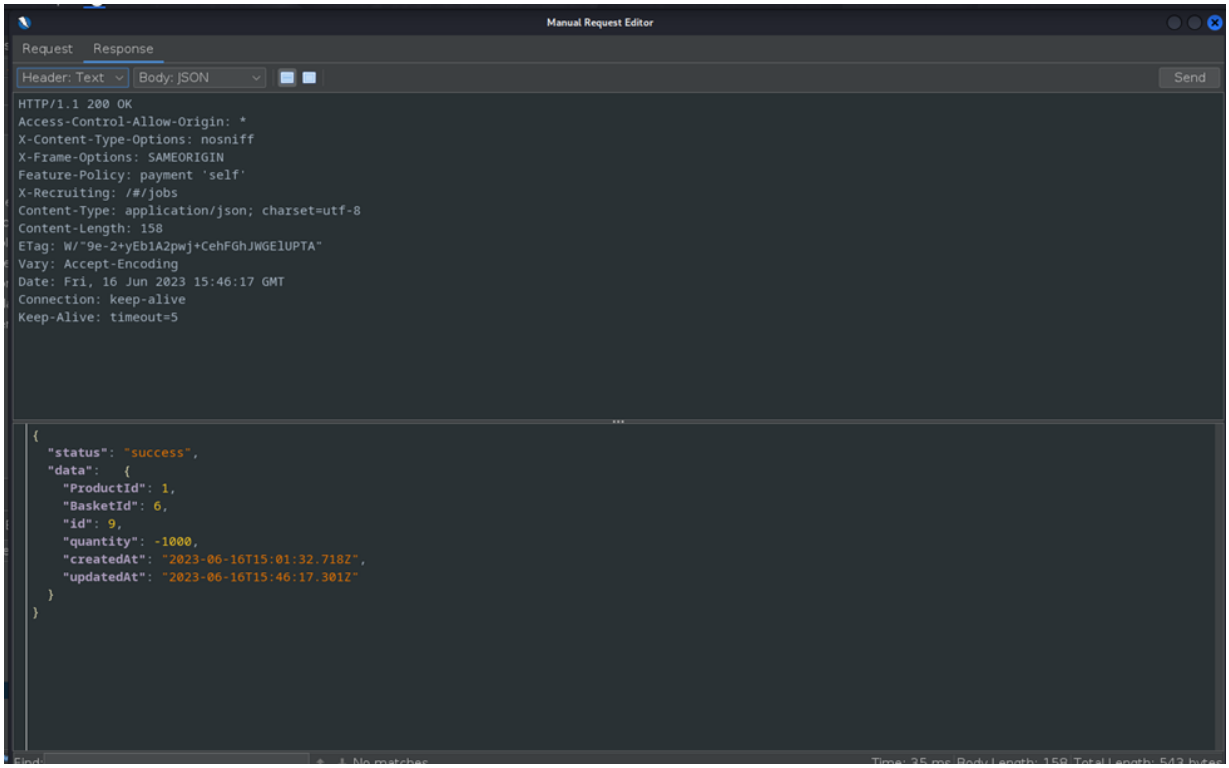
- The Response:



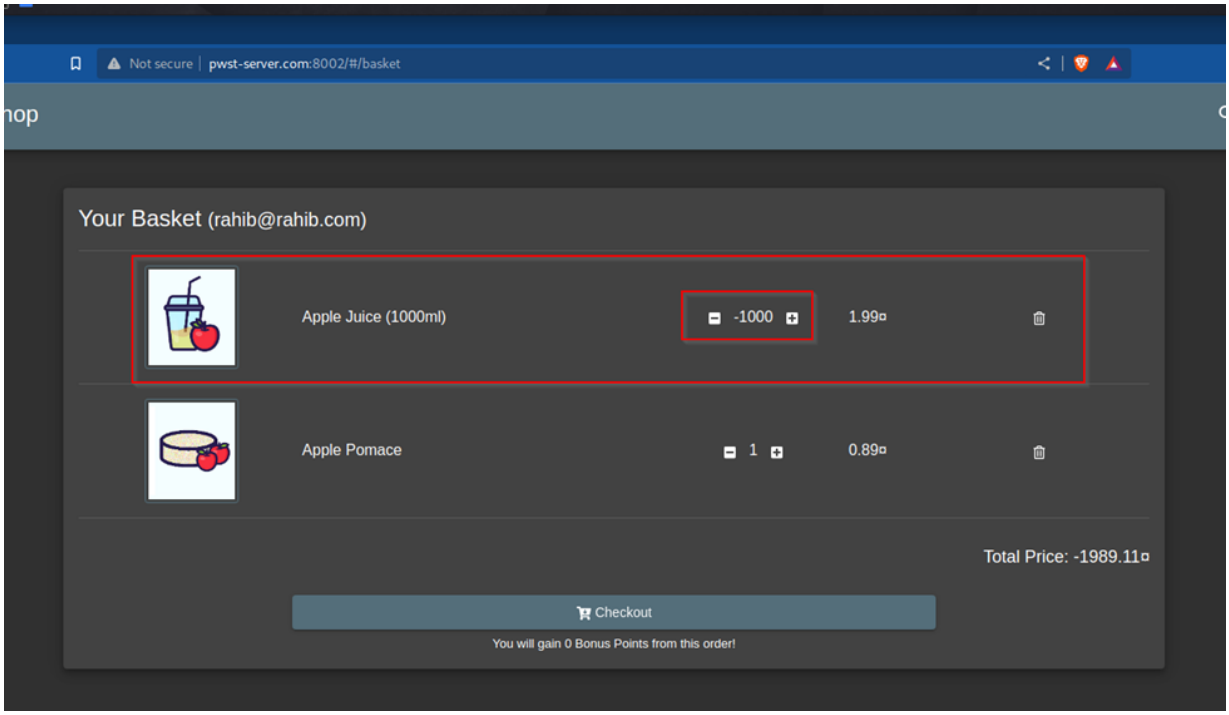
- able to add Negative items
  - reqeust:



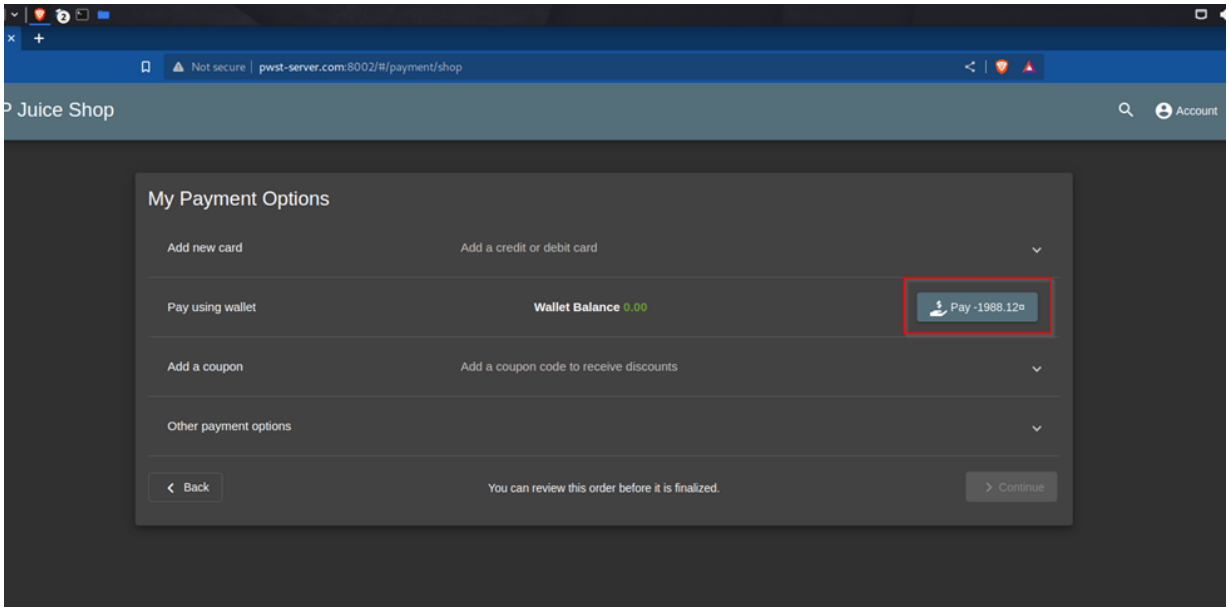
  - Response:



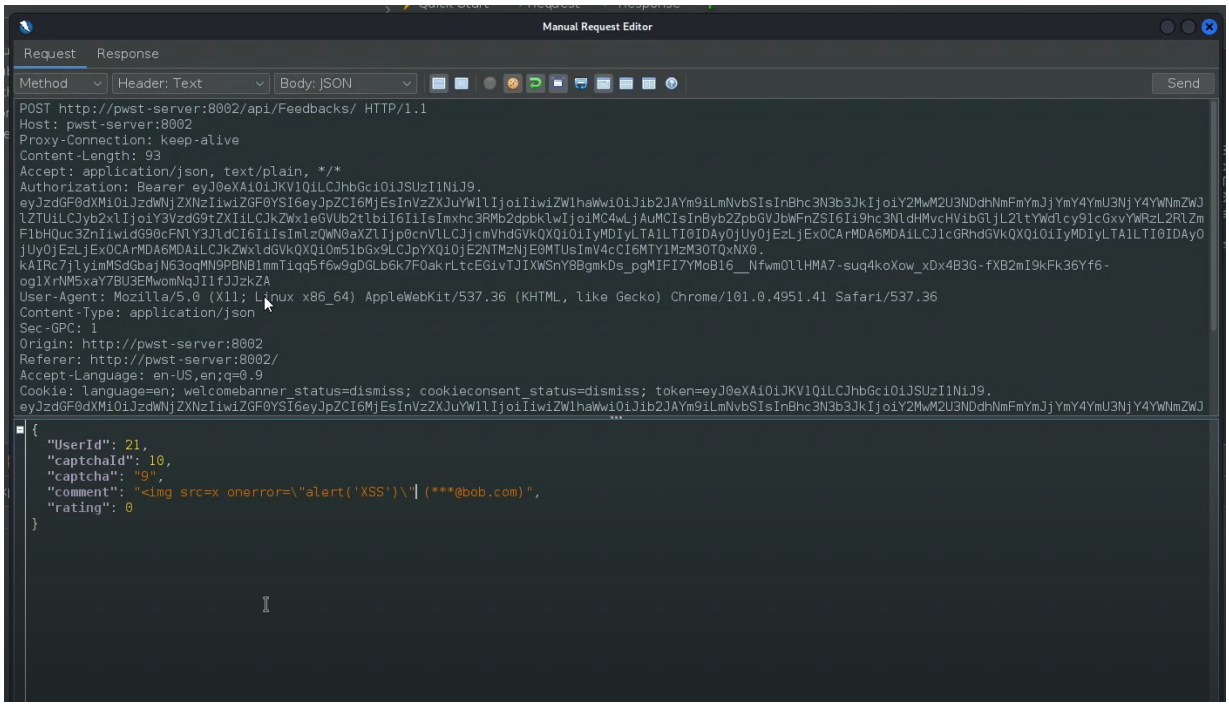
- result: here we have - 1000 orders :



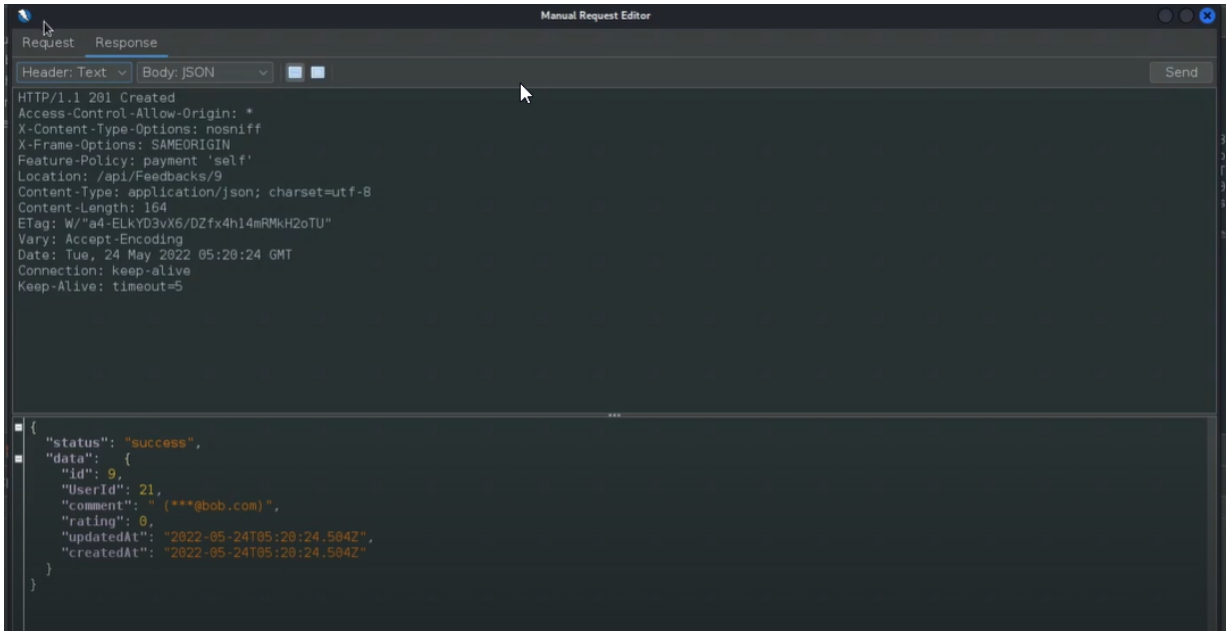
- it resulted in ordering with no money and added money to our wallet:

- 

`/api/Feedback`

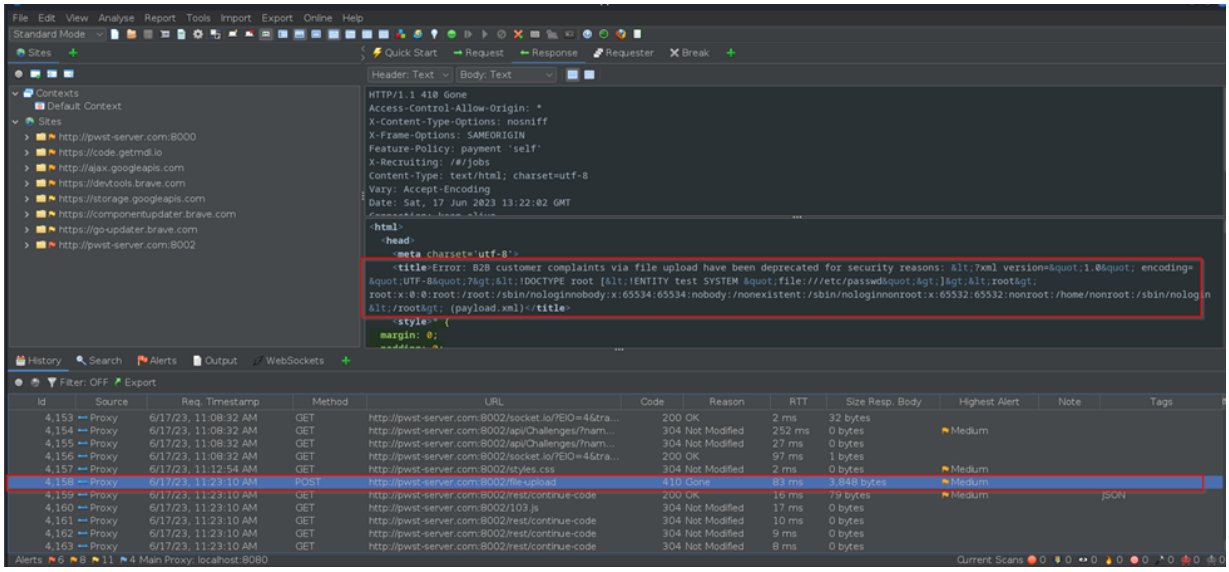
- Ability to give 0 stars:
- Reqeust:
  - 

- the Response:



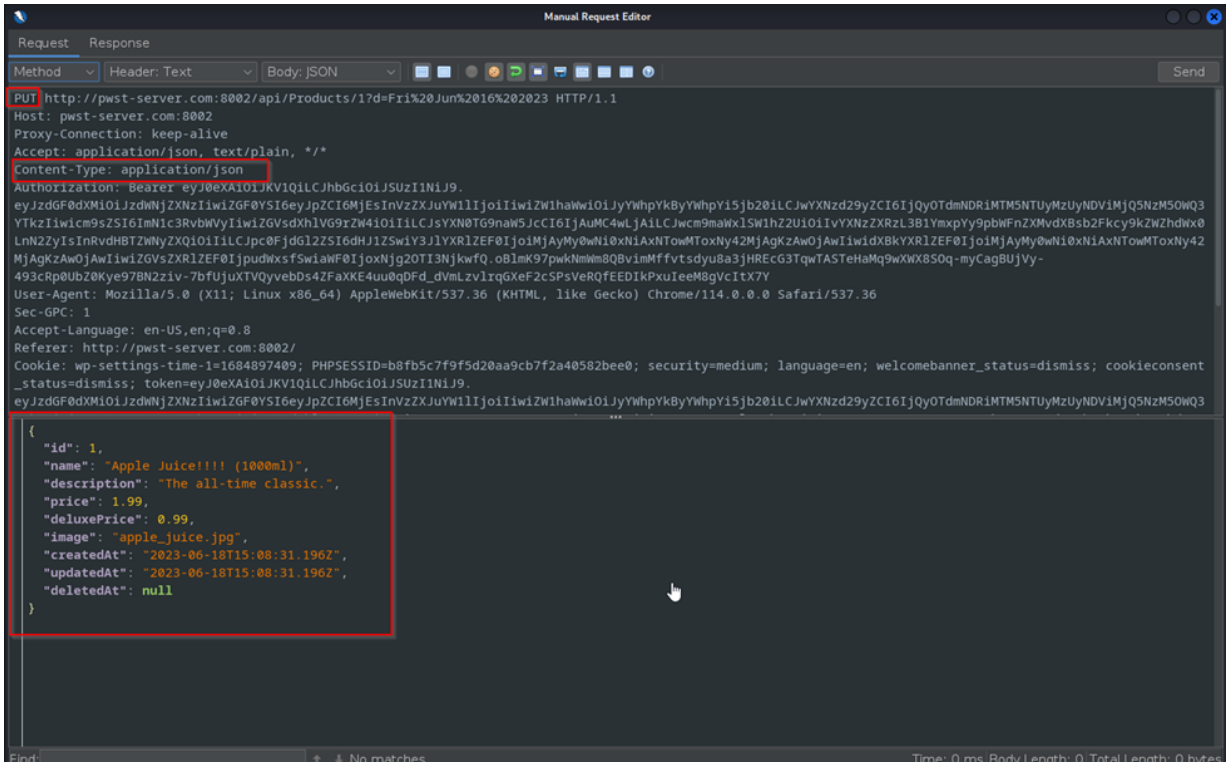
`/complain`

- XXE: can upload xml file that resulted in read /etc/passwd

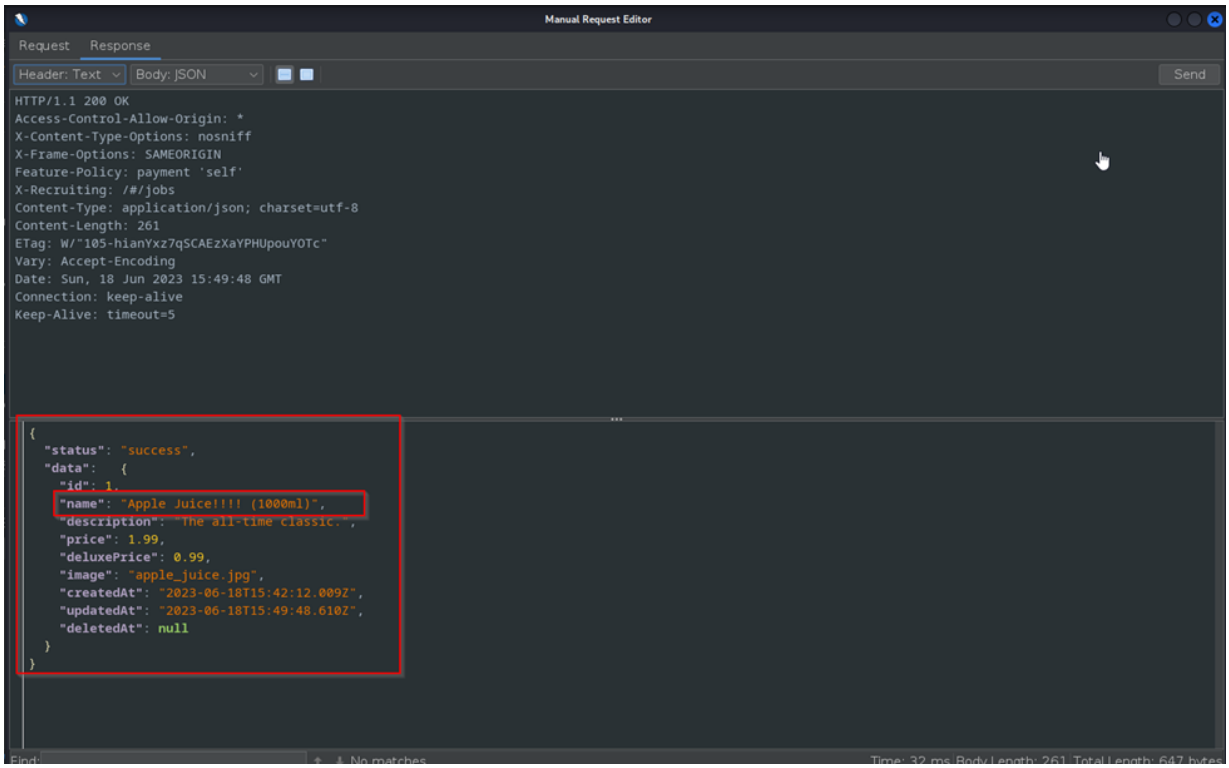


`/api/Products`

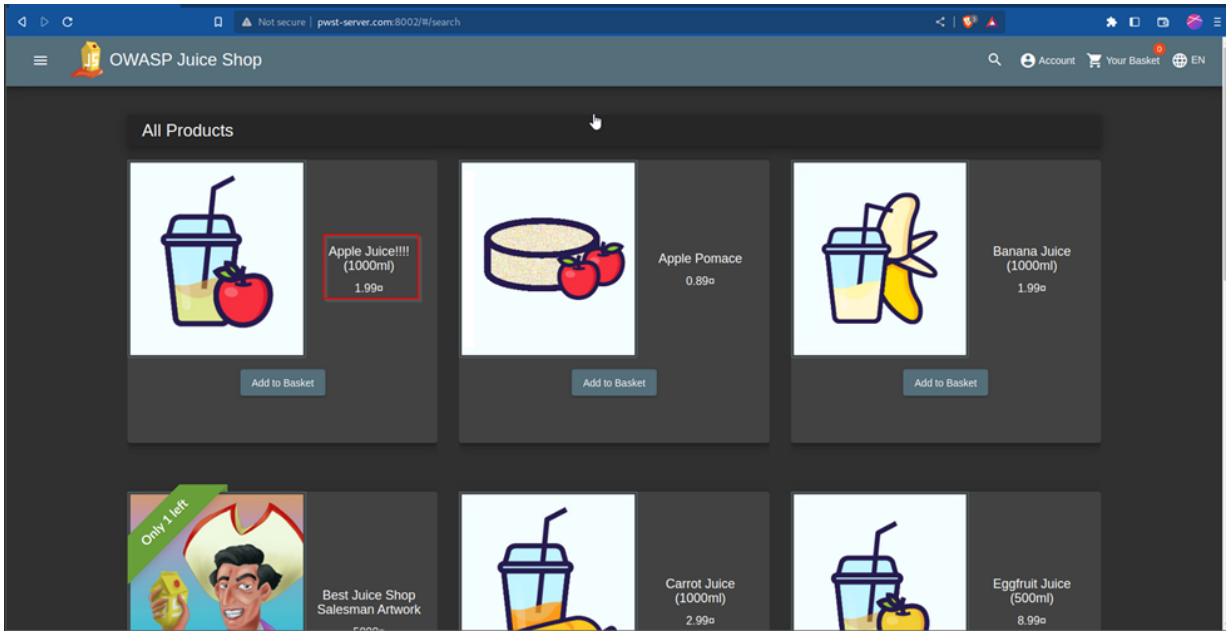
- Modify products via `PUT` reqeust as normal user:
- The Reqeust:



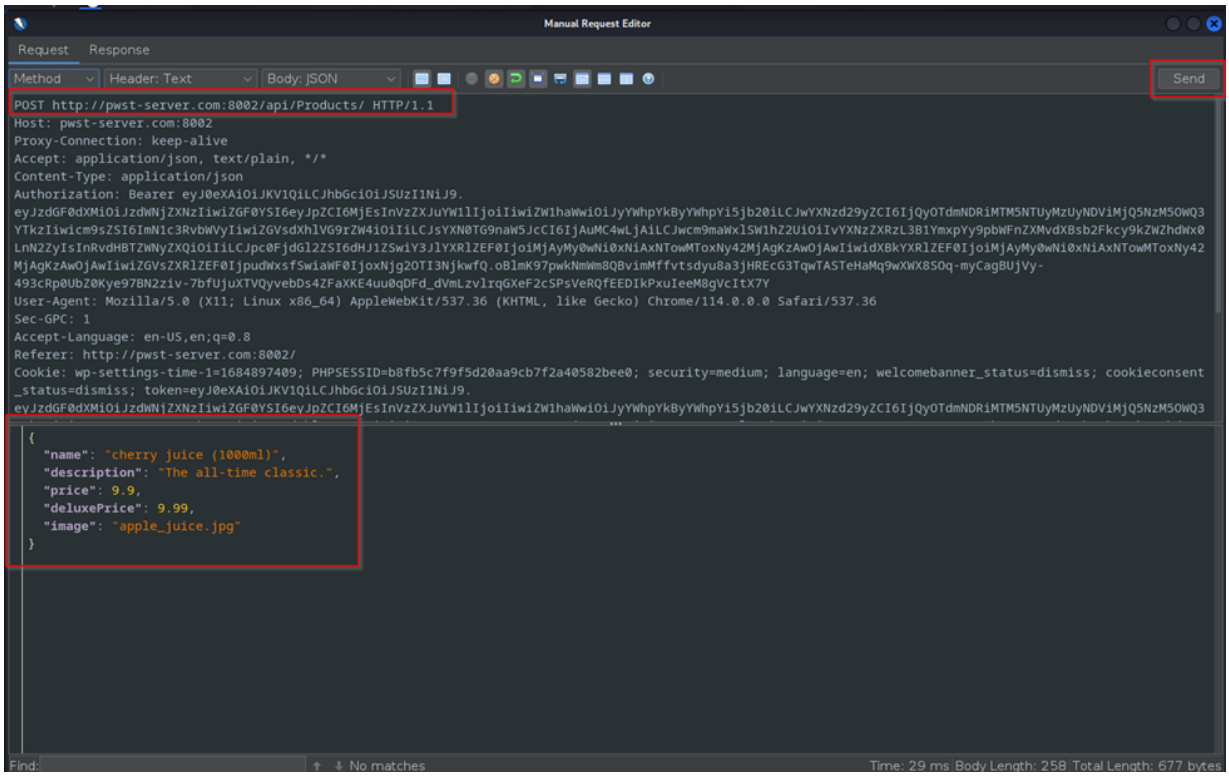
- The Response:



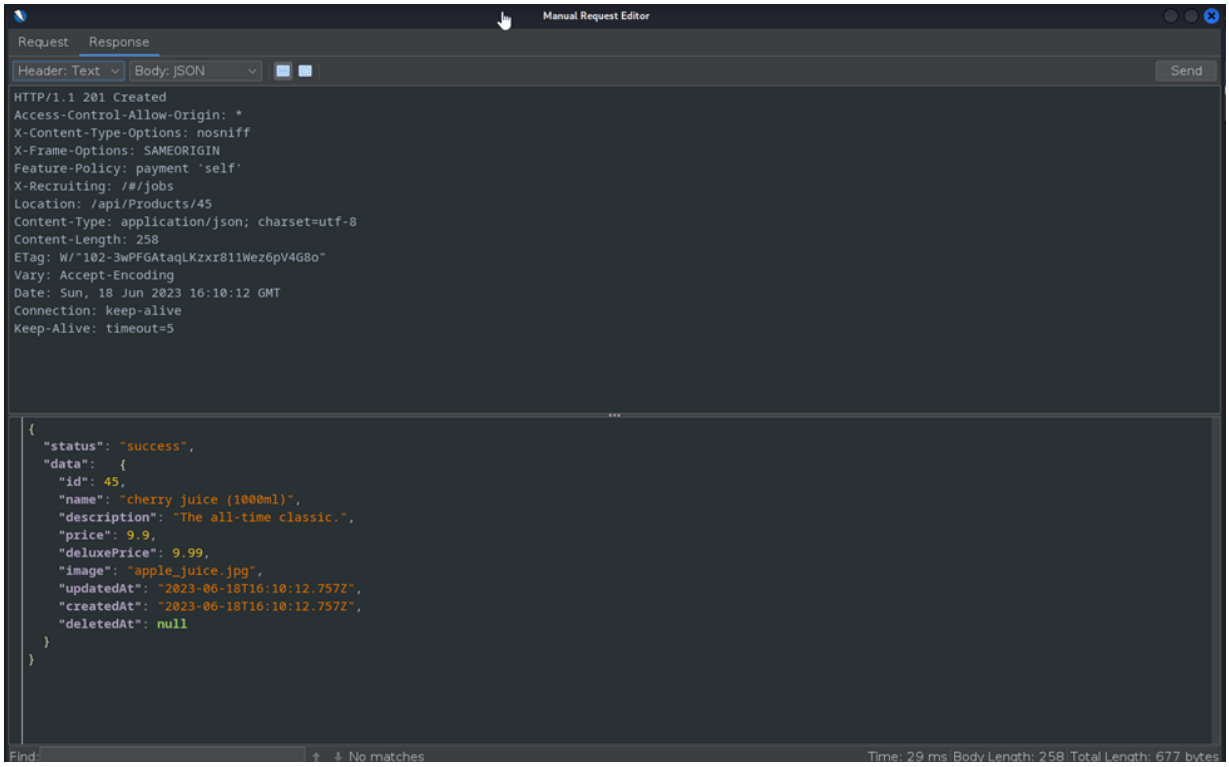
- Resulted in changing the name of the product:



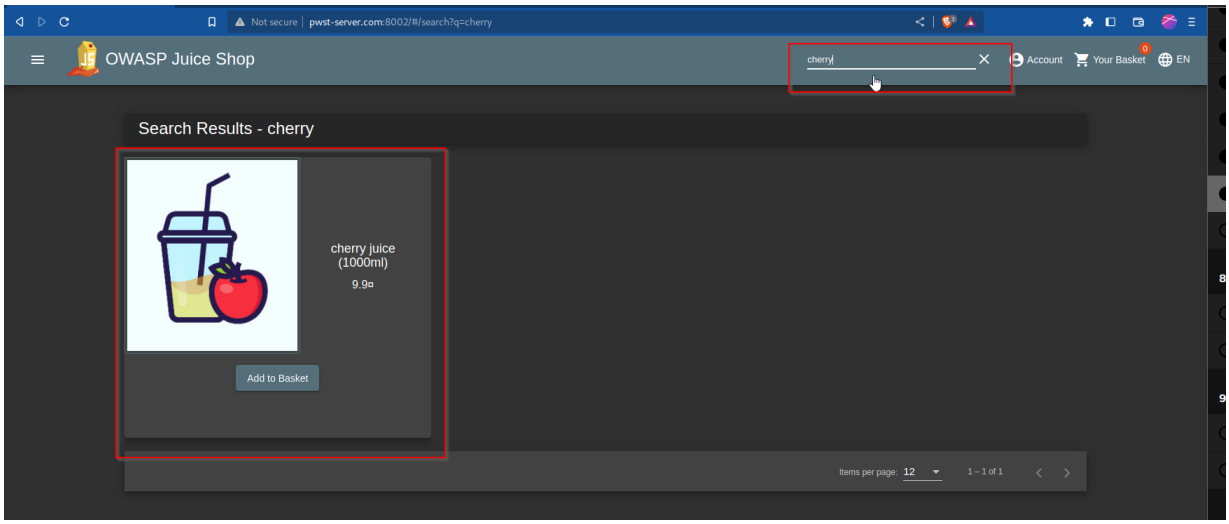
- and we can also change the price, image,...
- we can also add new products using `POST` request:
- the reqeust:



- the response:


Manual Request Editor
Request
Response
Header: Text
Body: JSON
Send
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Products/45
Content-Type: application/json; charset=utf-8
Content-Length: 258
ETag: W/"102-3wPFGAtaqLKzxr811Wez6pV4G8o"
Vary: Accept-Encoding
Date: Sun, 18 Jun 2023 16:10:12 GMT
Connection: keep-alive
Keep-Alive: timeout=5
{
"status": "success",
"data": {
"id": 45,
"name": "cherry juice (1000ml)",
"description": "The all-time classic.",
"price": 9.9,
"deluxePrice": 9.99,
"image": "apple_juice.jpg",
"updatedAt": "2023-06-18T16:10:12.757Z",
"createdAt": "2023-06-18T16:10:12.757Z",
"deletedAt": null
}
}
Find:
No matches
Time: 29 ms Body Length: 258 Total Length: 677 bytes

- resulted:


Not secure
pwst-server.com:8002/#/search?q=cherry
OWASP Juice Shop
cherry
Account
Your Basket
EN
Search Results - cherry
cherry juice (1000ml)
9.9¤
Add to Basket
Items per page: 12
1 – 1 of 1