IT'S NOT PRONOUNCED 'JOT'

WTH IS A JWT

Auth0

IT'S NOT PRONOUNCED 'JOT'

WTH IS A JWT

Auth0

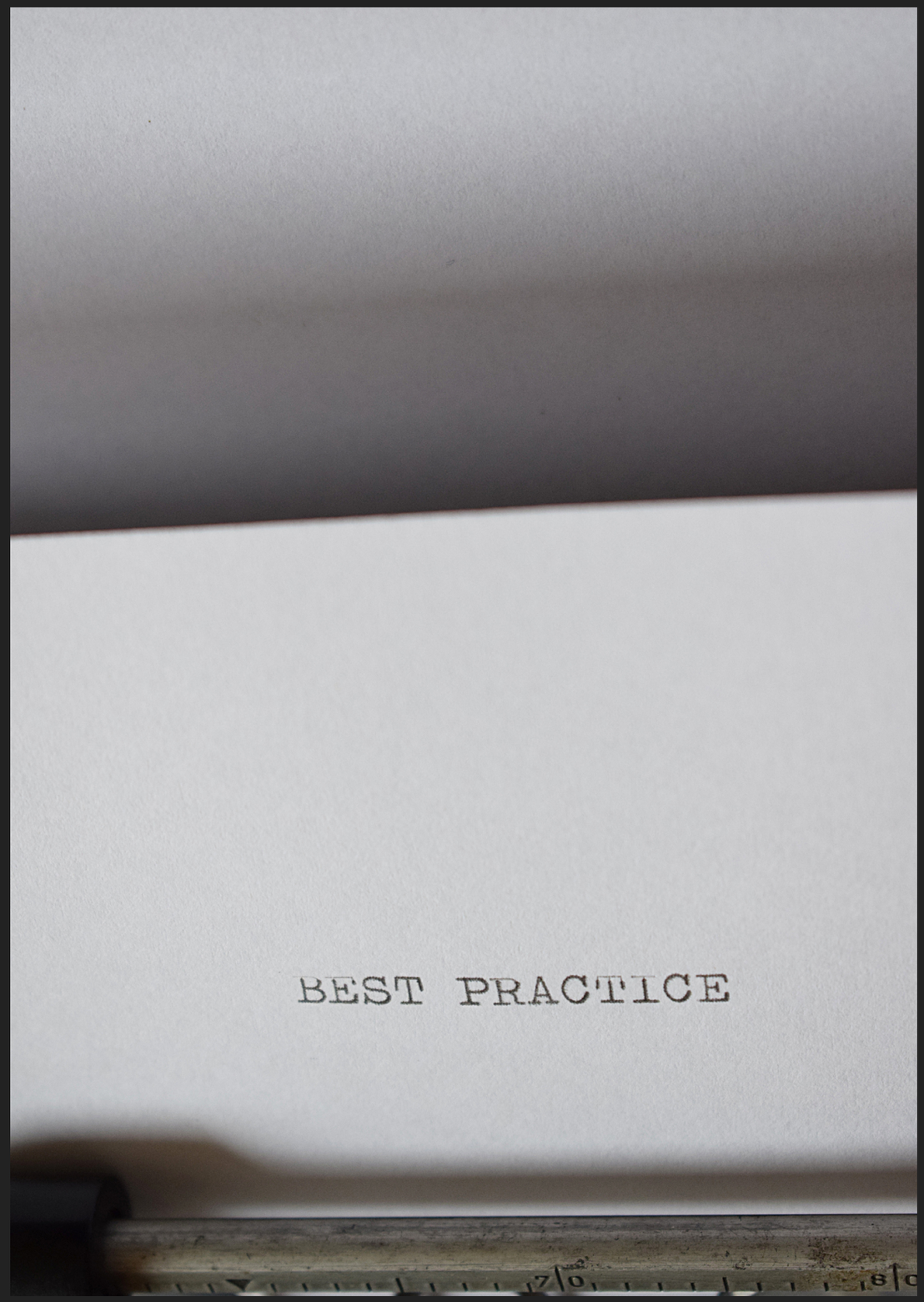
ABOUT ME

Auth0

@joel__lord

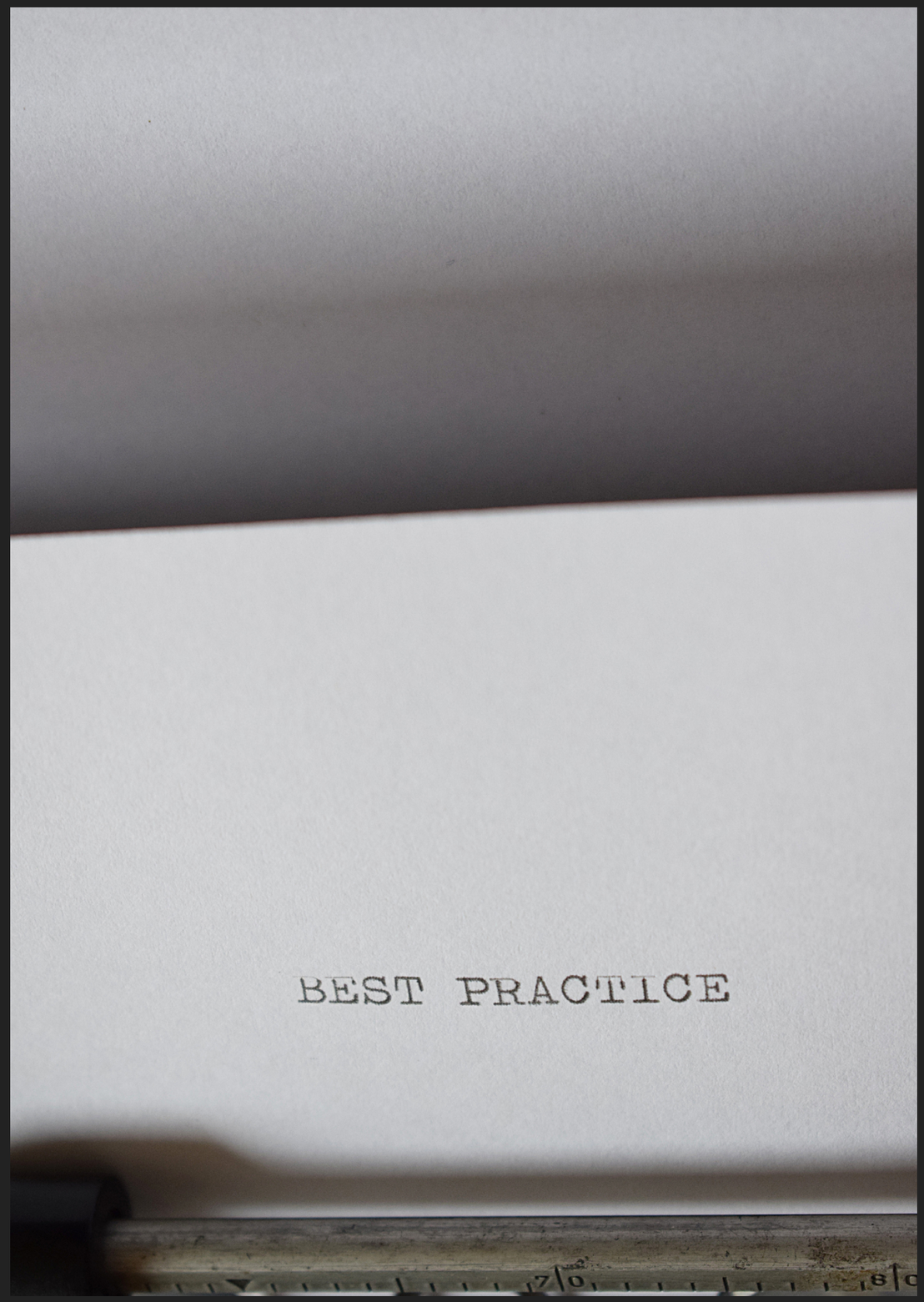
joellord

SPA BEST PRACTICES



SPA BEST PRACTICES

- ...



THANK YOU

All Things Open, Raleigh, NC
October 23th, 2018

 @joel__lord

 joellord

@joel__lord #AllThingsOpen

https://myserver.com

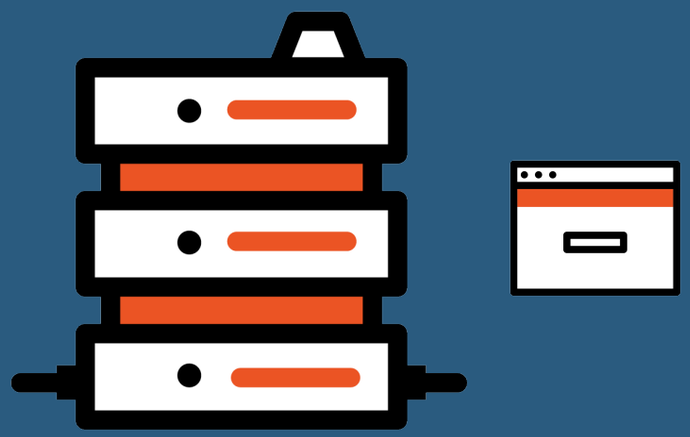
https://myserver.com

https://myserver.com

User

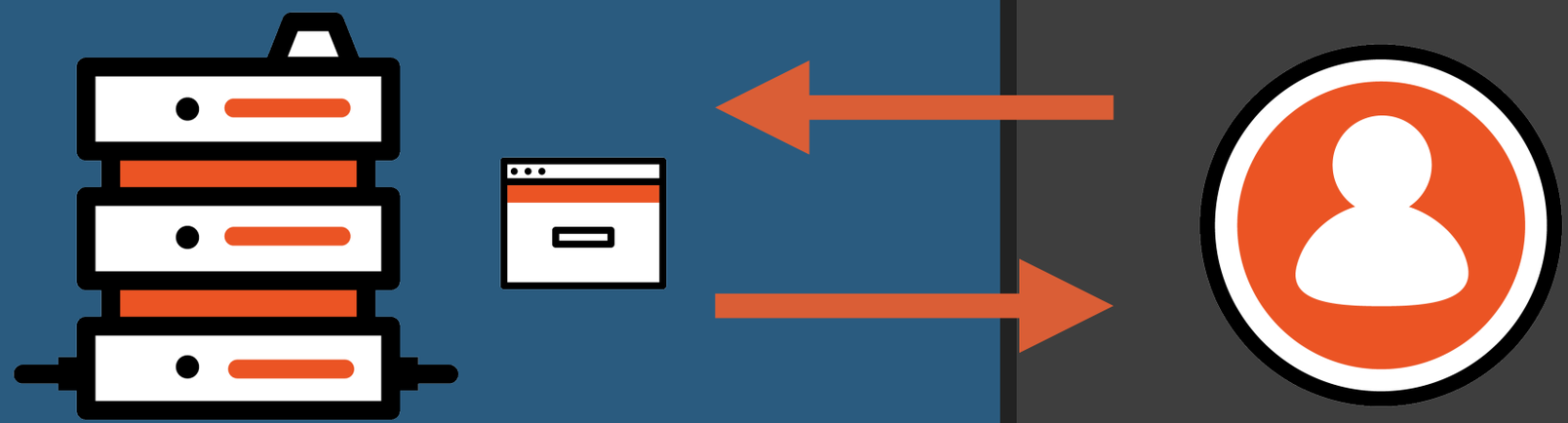
https://myserver.com

User



https://myserver.com

User

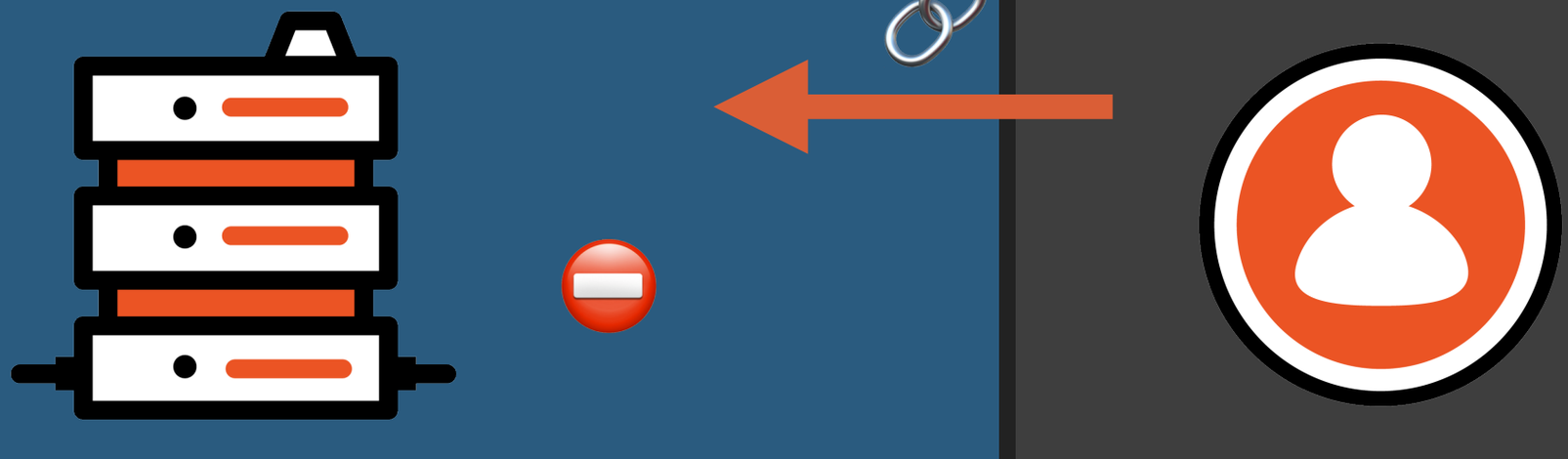


https://myserver.com

User

https://myserver.com

User

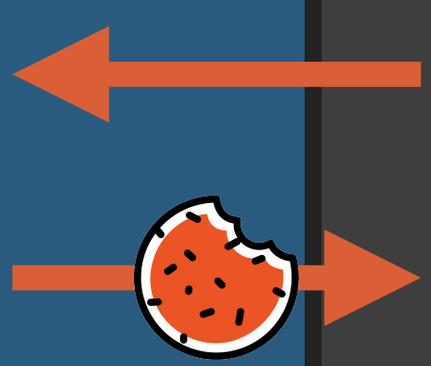


https://myserver.com

User

https://myserver.com

User



https://myserver.com

User

https://myserver.com

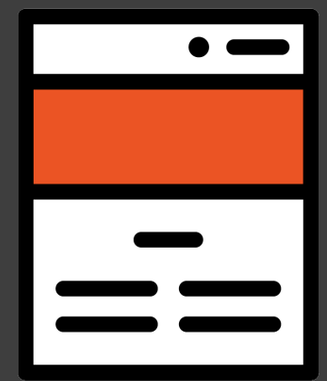
User

https://myserver.com

User

https://api.myserver.com

https://api.myserver.com

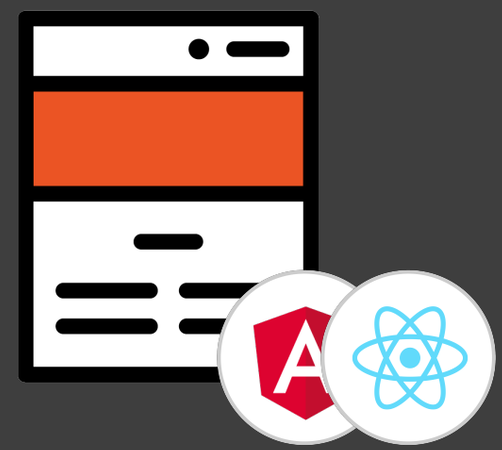


https://myapplication.com

https://api.myserver.com

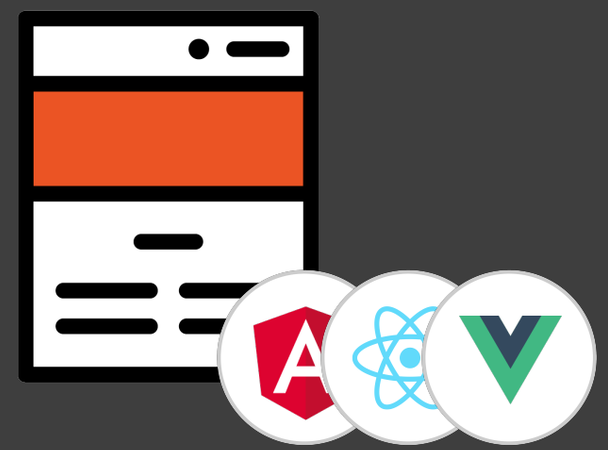
https://myapplication.com

https://api.myserver.com



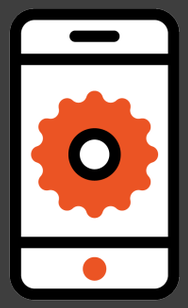
https://myapplication.com

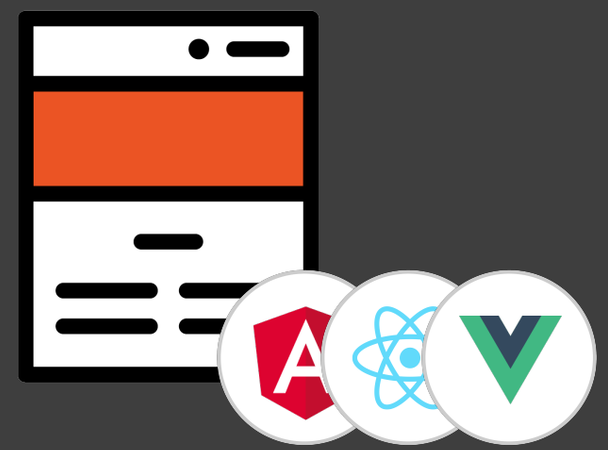
https://api.myserver.com



https://myapplication.com

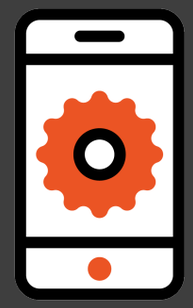
https://api.myserver.com

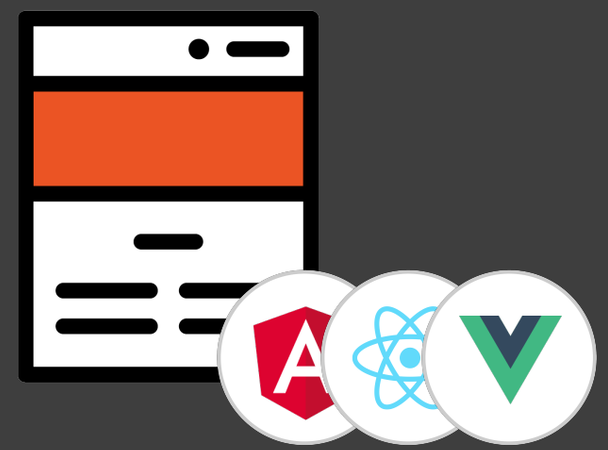




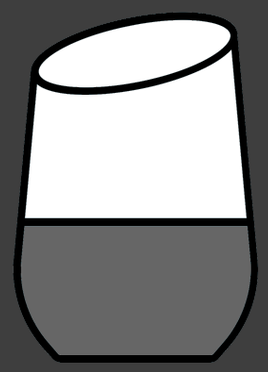
https://myapplication.com

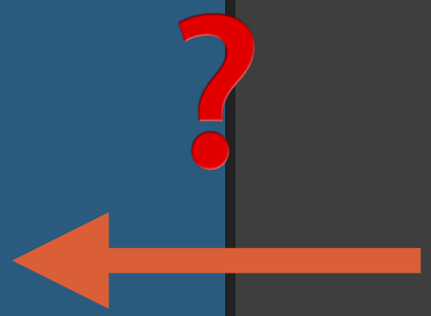
https://api.myserver.com

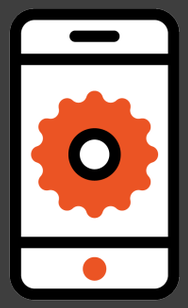


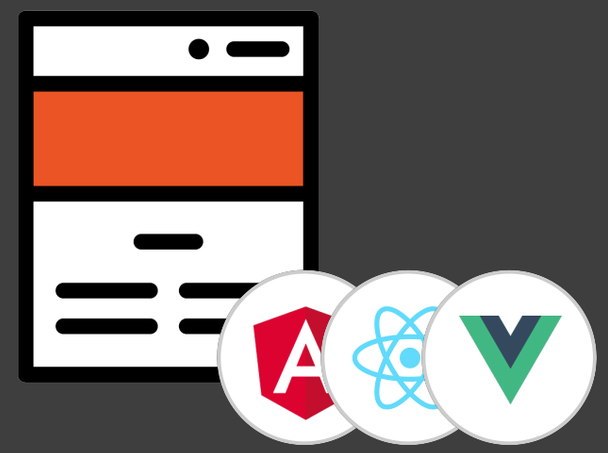


https://myapplication.com



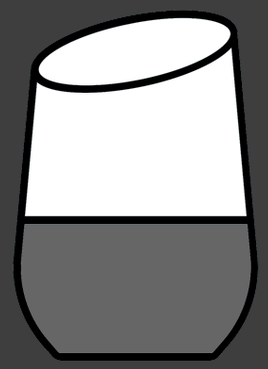






https://api.myserver.com

https://myapplication.com



INTRODUCING

JSON WEB TOKENS

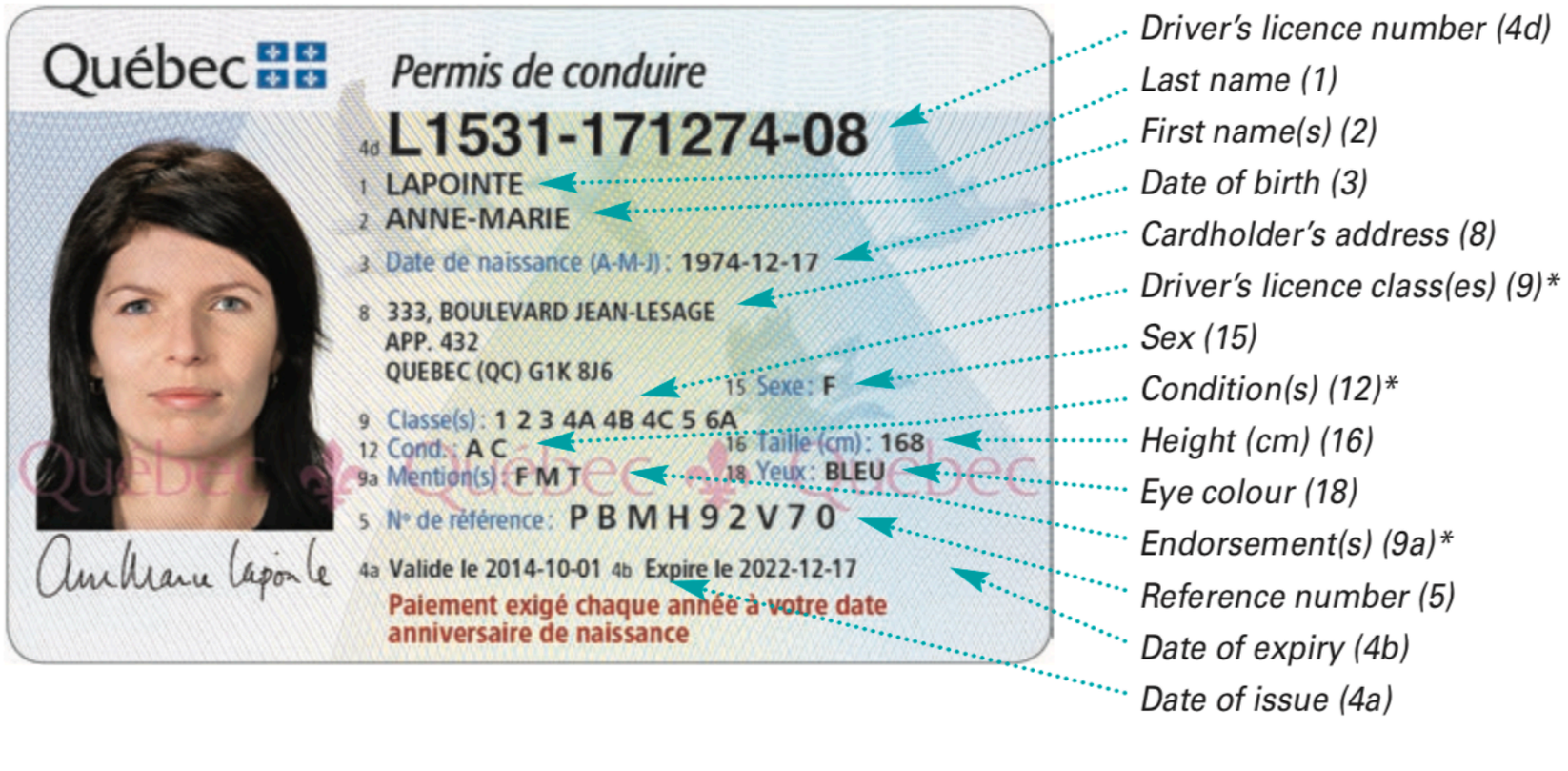
JSON WEB TOKENS

- JWT's (RFC 7519) are an open industry standard method for representing claims securely between two parties.

JSON WEB TOKENS

- eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp
  XVCJ9.eyJzdWIiOjEsInNjb3BlIjoiY
  XBpOnJlYWQiLCJ1c2VybmFtZSI6I
  mpvZWxsb3JkIiwiaXNzIjoibXktc21
  hbGwtYXV0aC1zZXJ2ZXIiLCJhdW
  QiOiJteS1yYW5kb20tY2xpY2tiYW
  l0LWFwaSIsImlhdCI6MTUzNzg5M
  TQyOCwiZXhwIjoxNTM3ODkyMDI
  4fQ.gEY3pRSdrnK5VtJI6E9vgada
  OQuLNWILBvvGasR4CRk

Front


Québec
Permis de conduire
4d L1531-171274-08
1 LAPOINTE
2 ANNE-MARIE
3 Date de naissance (A-M-J) : 1974-12-17
8 333, BOULEVARD JEAN-LESAGE
APP. 432
QUEBEC (QC) G1K 8J6
15 Sexe : F
9 Classe(s) : 1 2 3 4A 4B 4C 5 6A
12 Cond. : A C
16 Taille (cm) : 168
9a Mention(s) : F M T
18 Yeux : BLEU
5 N° de référence : P B M H 9 2 V 7 0
4a Valide le 2014-10-01 4b Expire le 2022-12-17
Paiement exigé chaque année à votre date anniversaire de naissance
Driver's licence number (4d)
Last name (1)
First name(s) (2)
Date of birth (3)
Cardholder's address (8)
Driver's licence class(es) (9)*
Sex (15)
Condition(s) (12)*
Height (cm) (16)
Eye colour (18)
Endorsement(s) (9a)*
Reference number (5)
Date of expiry (4b)
Date of issue (4a)

Back


CLASSE(S) : Tous les types de véhicules routiers. Toute motocyclette.
CONDITION(S) : A : Lunettes ou lentilles cornéennes, C : Appareil auditif, classe 2, 4A, 4B ou 4C.
MENTION(S) : F : Freinage pneumatique, M : Transmission manuelle, T : Train routier.
Apposer l'autocollant de votre nouvelle adresse.
Pour tout renseignement
1 800 361-7620
Pour vérifier la validité d'un permis
1 900 565-1212 (frais exigés)
Services aussi disponibles au www.saaq.gouv.qc.ca
Société de l'assurance automobile
Québec
(2009-10)
Definitions of the licence classes, conditions and endorsements listed on the front
Bar code
The bar code corresponds to the driver's licence number.
Telephone number for more information
Telephone number to check the validity of a licence (fees apply)
Two-dimensional bar code
The two-dimensional bar code (2D) contains all licence information except the photo and signature.

A SIMPLE ANALOGY

- How is a Drivers License like a JSON Web Token?
- eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp
  XVCJ9.eyJzdWIiOjEsInNjb3BlIjoiY
  XBpOnJlYWQiLCJ1c2VybmFtZSI6I
  mpvZWxsb3JkIiwiaXNzIjoibXktc21
  hbGwtYXV0aC1zZXJ2ZXIiLCJhdW
  QiOiJteS1yYW5kb20tY2xpY2tiYW
  l0LWFwaSIsImlhdCI6MTUzNzg5M
  TQyOCwiZXhwIjoxNTM3ODkyMDI
  4fQ.gEY3pRSdrnK5VtJI6E9vgada
  OQuLNWILBvvGasR4CRk

A SIMPLE ANALOGY

- How is a Drivers License like a JSON Web Token?
- eyJhbGciOiJIUzI1NiIsInR5cCI6Ikp
  XVCJ9.eyJzdWIiOjEsInNjb3BlIjoiY
  XBpOnJlYWQiLCJ1c2VybmFtZSI6I
  mpvZWxsb3JkIiwiaXNzIjoibXktc21
  hbGwtYXV0aC1zZXJ2ZXIiLCJhdW
  QiOiJteS1yYW5kb20tY2xpY2tiYW
  l0LWFwaSIsImlhdCI6MTUzNzg5M
  TQyOCwiZXhwIjoxNTM3ODkyMDI
  4fQ.gEY3pRSdrnK5VtJI6E9vgada
  OQuLNWILBvvGasR4CRk

HEADER

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

HEADER

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

- Drivers Licence

HEADER

- Drivers Licence
- Province of Quebec

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

HEADER

- Drivers Licence
- Province of Quebec

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

HEADER

- Drivers Licence
- Province of Quebec

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

- atob("eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9");

HEADER

- Drivers Licence
- Province of Quebec

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

PAYLOAD

- Picture

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

PAYLOAD

- Picture
- Name

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

PAYLOAD

- Picture
- Name
- Date of Birth

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

PAYLOAD

- Picture
- Name
- Date of Birth
- Restrictions

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

PAYLOAD

- Picture
- Name
- Date of Birth
- Restrictions

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ

PAYLOAD

- Picture
- Name
- Date of Birth
- Restrictions

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

atob("eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ");

PAYLOAD

- Picture
- Name
- Date of Birth
- Restrictions

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

```
{
  "sub": 1,
  "scope": "api:read",
  "username": "joellord",
  "iss": "my-small-auth-server",
  "aud": "my-random-clickbait-api",
  "iat": 1537891428,
  "exp": 1537892028
}
```

SIGNATURE

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

SIGNATURE

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

- Holograms

SIGNATURE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

- Holograms
- Signature

SIGNATURE

- Holograms
- Signature

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

SIGNATURE

- Holograms
- Signature

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

HMACSHA256(
  `${header}.${payload}`,
  “mysupersecret”
);

SIGNATURE

- Holograms
- Signature

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

HMACSHA256(
  `${header}.${payload}`,
  “mysupersecret”
);

SIGNATURE

- Holograms
- Signature

- eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOjEsInNjb3BlIjoiYXBpOnJlYWQiLCJ1c2VybmFtZSI6ImpvZWxsb3JkIiwiaXNzIjoibXktc21hbGwtYXV0aC1zZXJ2ZXIiLCJhdWQiOiJteS1yYW5kb20tY2xpY2tiYWl0LWFwaSIsImlhdCI6MTUzNzg5MTQyOCwiZXhwIjoxNTM3ODkyMDI4fQ.gEY3pRSdrnK5VtJI6E9vgadaOQuLNWILBvvGasR4CRk

HMACSHA256(
  `${header}.${payload}`,
  “mysupersecret”
);

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

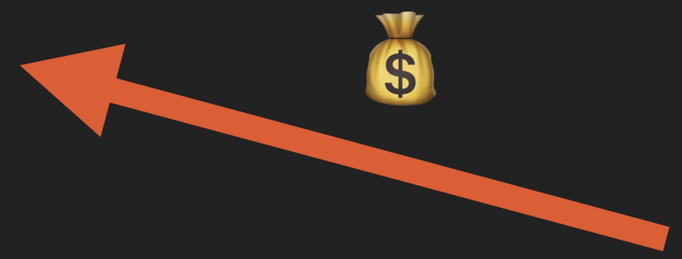
A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR



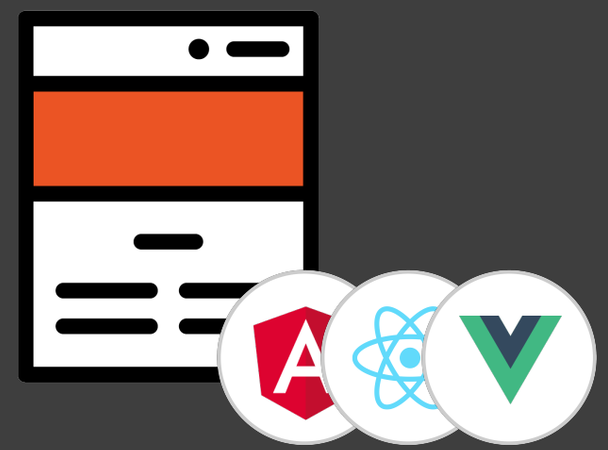
A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

A TOKEN WALKS INTO A BAR

DEMO

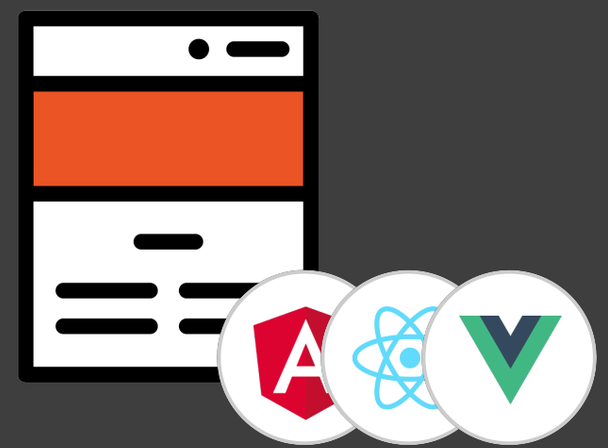
https://api.myserver.com



https://myapplication.com

https://api.myserver.com

/api/cats



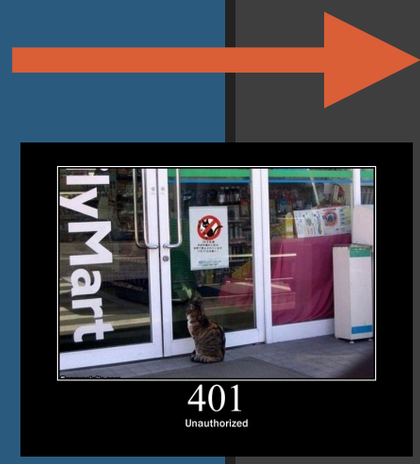
https://myapplication.com

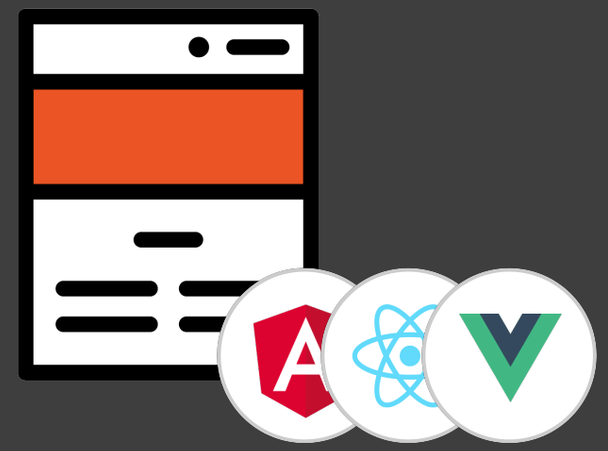
https://ap

ation.com

https://api.myserver.com

/api/cats



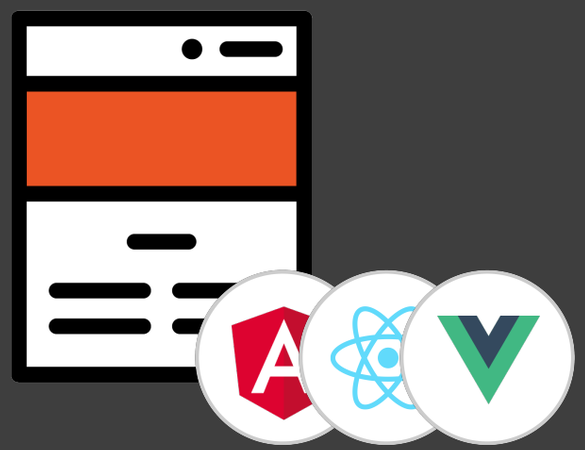


https://myapplication.com

@joel__lord #AllThingsOpen

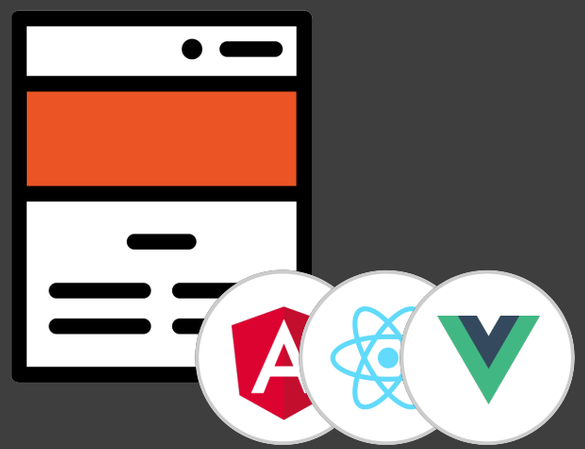
https://api.myserver.com

https://api.myserver.com



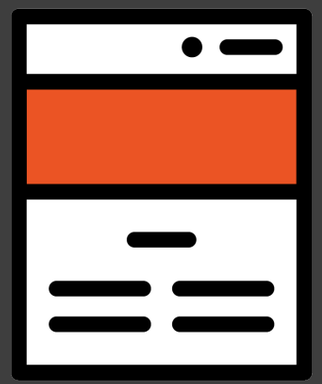
https://myapplication.com

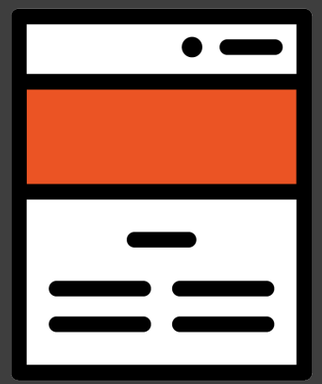
https://api.myserver.com



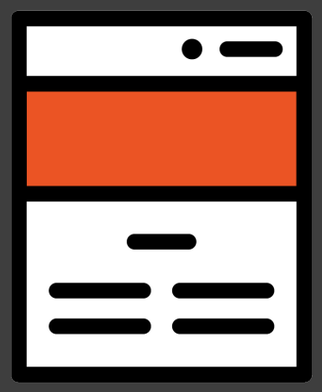
https://myapplication.com

https://login.myserver.com

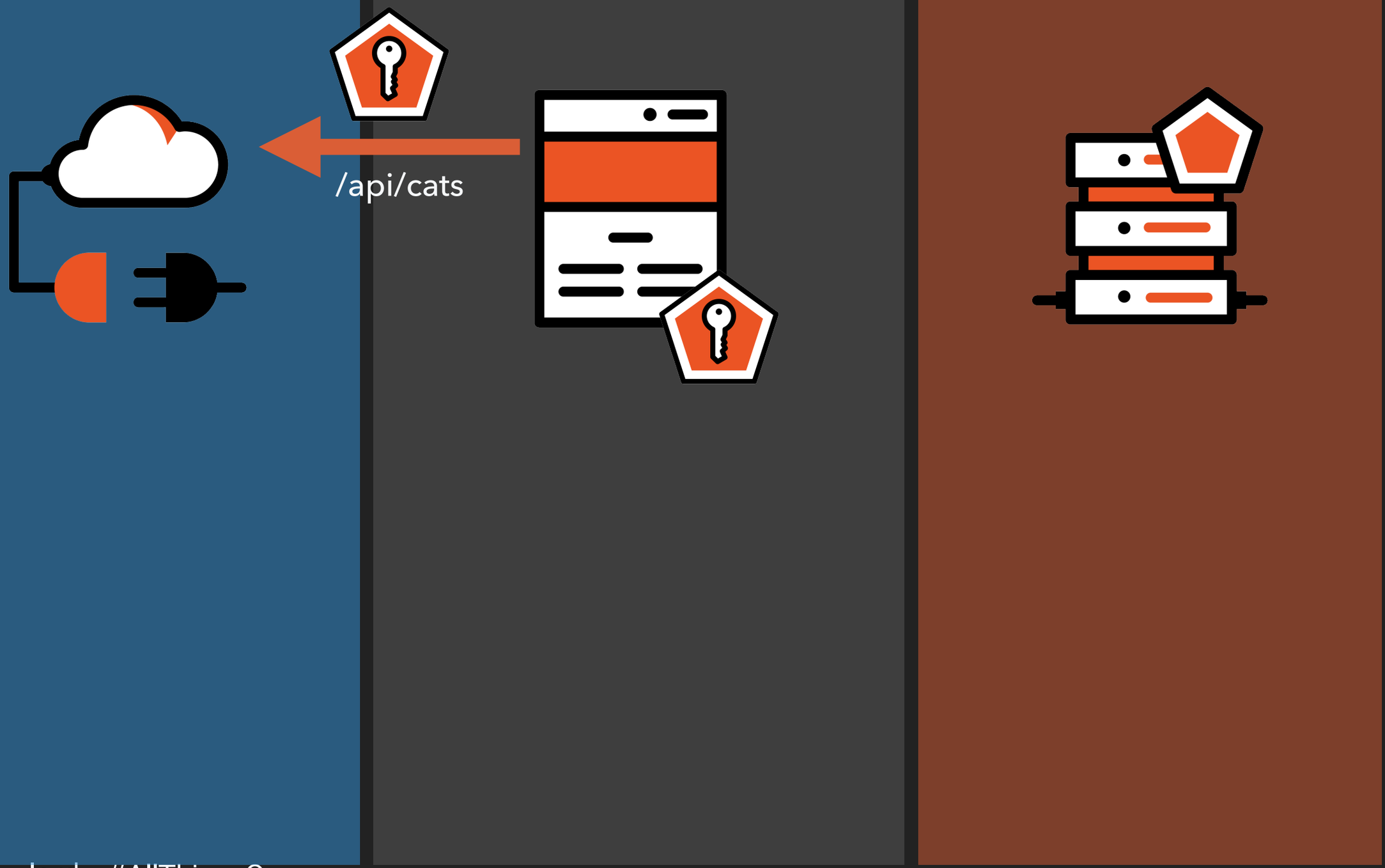





/authorize

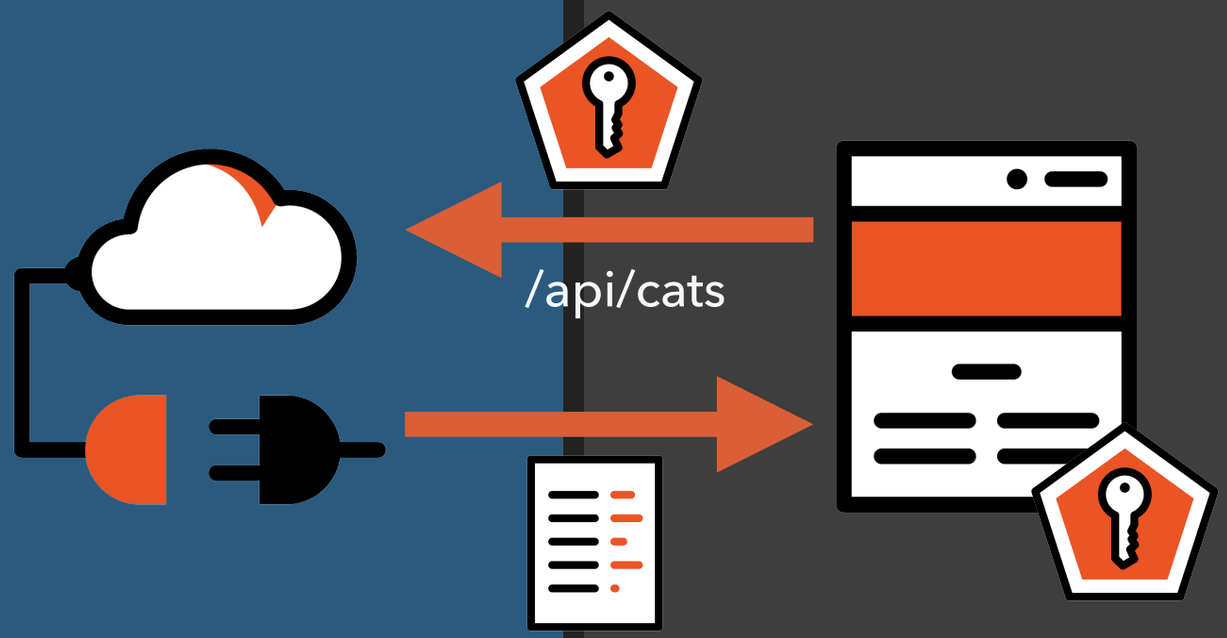


/authorize


/api/cats

200

OK


/api/cats

SENDING THE TOKEN TO THE API

- Using Axios

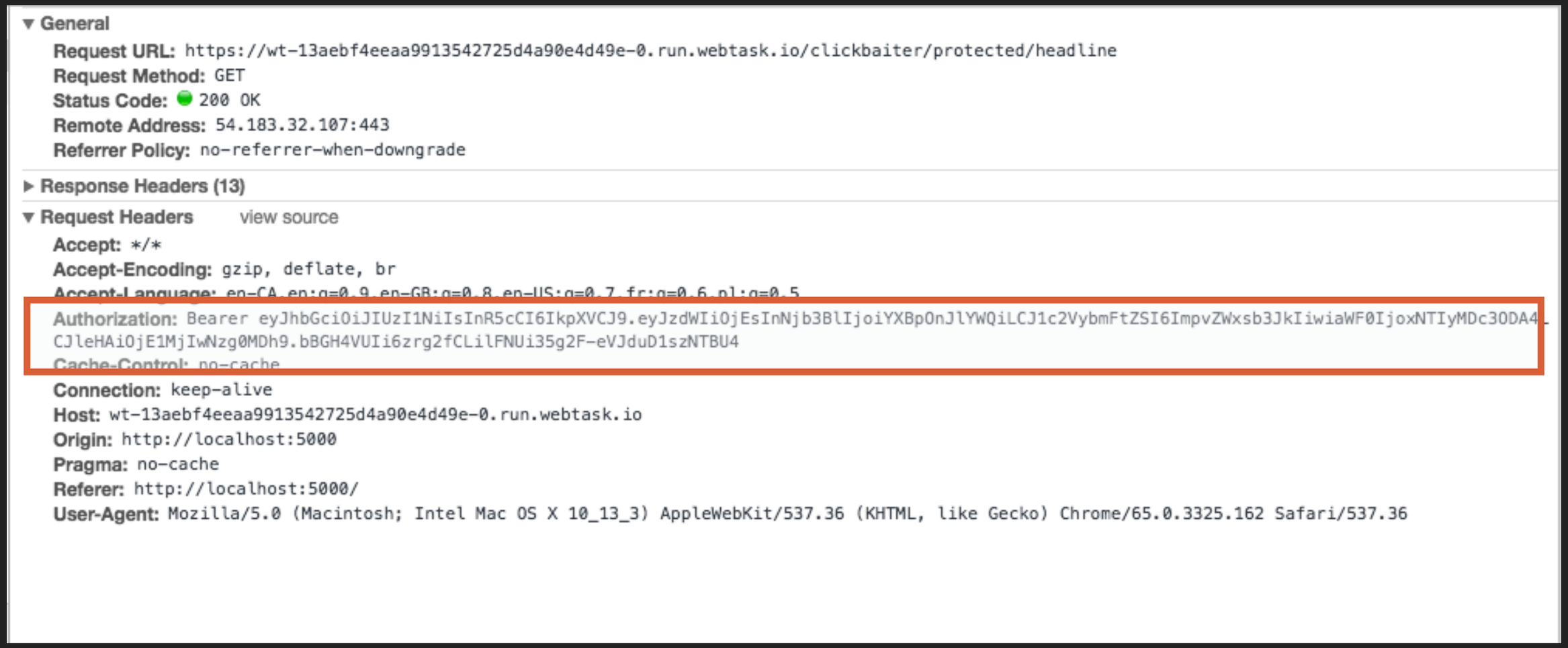
```
axios.post(
  `${API_URL}/api/cats`,
  {
    headers: {
      Authorization: `Bearer ${token}`
    }
  }
).then((data) => {
  console.log(data); // {message: "ok", cats: "cute"}
});
```

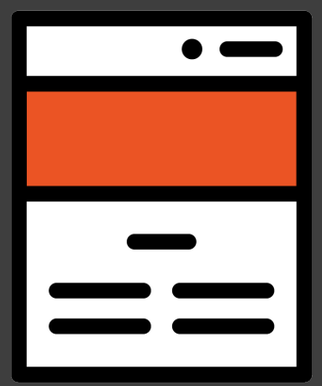
SENDING THE TOKEN TO THE API

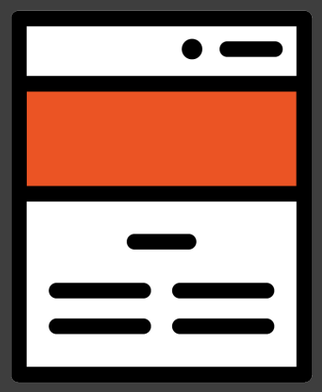
- Using Fetch

```
1 fetch(
2   `${API_URL}/api/cats`,
3   {
4     method: "POST",
5     headers: {
6       Authorization: `Bearer ${token}`
7     }
8   }
9 ).then((data) => {
10   console.log(data); // {message: "ok", cats: "cute"}
11 });
```

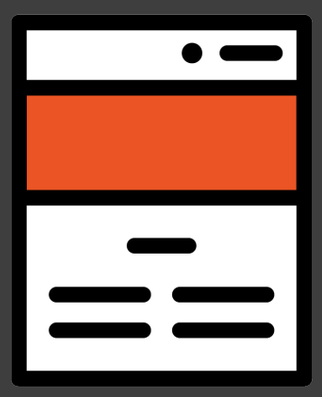
SENDING THE TOKEN TO THE API



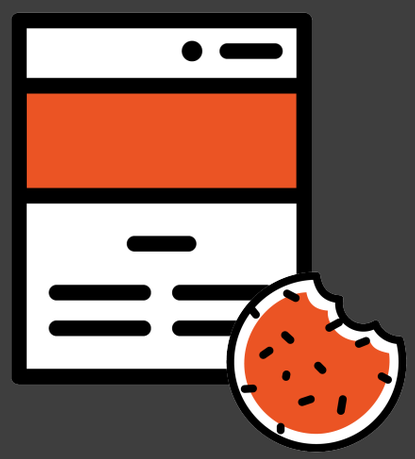


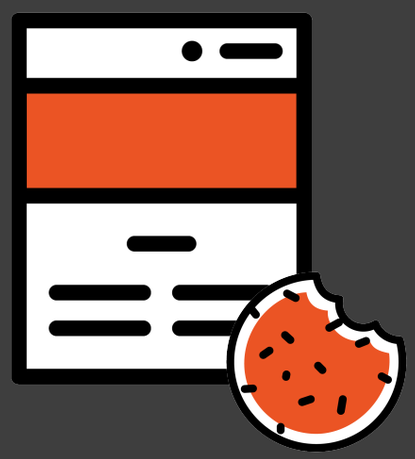


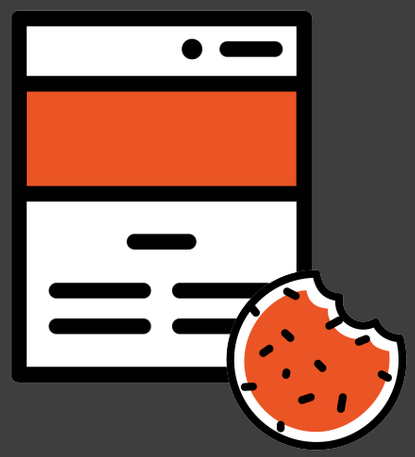
/authorize

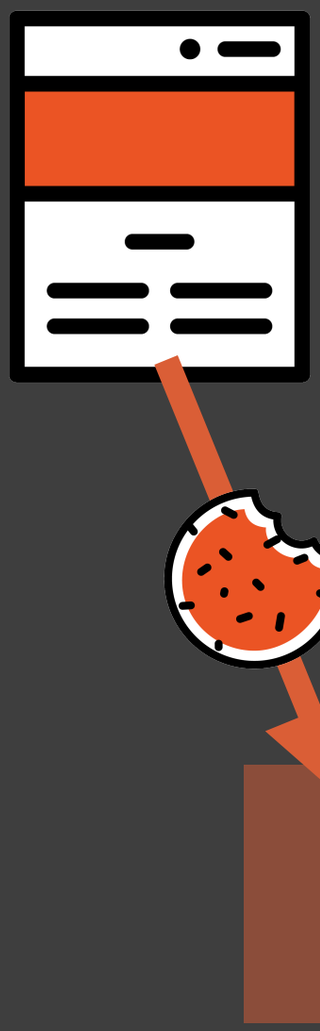


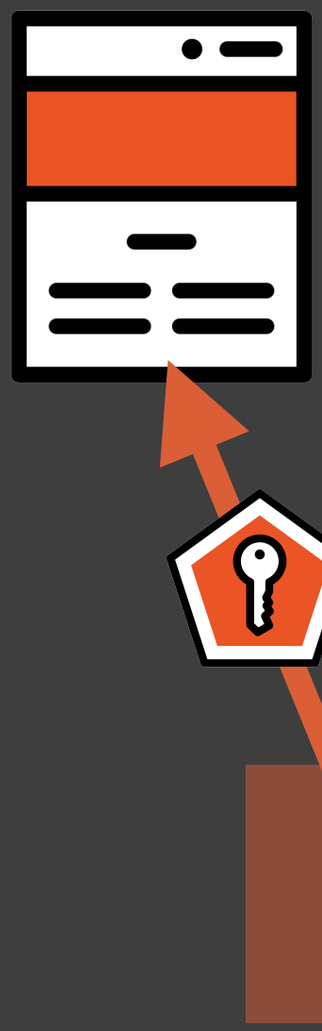
/authorize

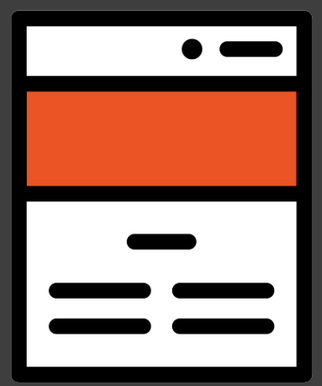












"SECURING" YOUR SPA

- You can never completely secure your front-end using JWTs
- You can "hide" some routes

“SECURING” YOUR SPA

```
Router.routes = [
  {name: "home", path: "#", public: true},
  {name: "secret", path: "#secret", public: false}
];

window.addEventListener("hashchange", () => {
  let route = window.location.hash;
  let isLoggedIn = Auth.isLoggedIn();

  hideAllSections();

  selectedRoute = Router.routes.find(r => r.path === route));

  if (selectedRoute.public) {
    displaySection(selectedRoute.name);
  } else if (isLoggedIn) {
    displaySection(selectedRoute.name);
  } else {
    displaySection("unauthorized");
  }
});
```

@joel__lord

“SECURING” YOUR SPA

```
Router.routes = [
  {name: "home", path: "#", public: true},
  {name: "secret", path: "#secret", public: false}
];

window.addEventListener("hashchange", () => {
  let route = window.location.hash;
  let isLoggedIn = Auth.isLoggedIn();

  hideAllSections();

  selectedRoute = Router.routes.find(r => r.path === route));

  if (selectedRoute.public) {
    displaySection(selectedRoute.name);
  } else if (isLoggedIn) {
    displaySection(selectedRoute.name);
  } else {
    displaySection("unauthorized");
  }
});
```

@joel__lord

“SECURING” YOUR SPA

```
Router.routes = [
  {name: "home", path: "#", public: true},
  {name: "secret", path: "#secret", public: false}
];

window.addEventListener("hashchange", () => {
  let route = window.location.hash;
  let isLoggedIn = Auth.isLoggedIn();

  hideAllSections();

  selectedRoute = Router.routes.find(r => r.path === route));

  if (selectedRoute.public) {
    displaySection(selectedRoute.name);
  } else if (isLoggedIn) {
    displaySection(selectedRoute.name);
  } else {
    displaySection("unauthorized");
  }
});
```

@joel__lord

“SECURING” YOUR SPA

```
Router.routes = [
  {name: "home", path: "#", public: true},
  {name: "secret", path: "#secret", public: false}
];

window.addEventListener("hashchange", () => {
  let route = window.location.hash;
  let isLoggedIn = Auth.isLoggedIn();

  hideAllSections();

  selectedRoute = Router.routes.find(r => r.path === route));

  if (selectedRoute.public) {
    displaySection(selectedRoute.name);
  } else if (isLoggedIn) {
    displaySection(selectedRoute.name);
  } else {
    displaySection("unauthorized");
  }
});
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

“SECURING” YOUR SPA

```
1 Router.routes = [
2   {name: "home", path: "#", public: true},
3   {name: "secret", path: "#secret", public: false}
4 ];
5
6 window.addEventListener("hashchange", () => {
7   let route = window.location.hash;
8   let isLoggedIn = Auth.isLoggedIn();
9
10  hideAllSections();
11
12  selectedRoute = Router.routes.find(r => r.path === route));
13
14  if (selectedRoute.public) {
15    displaySection(selectedRoute.name);
16  } else if (isLoggedIn) {
17    displaySection(selectedRoute.name);
18  } else {
19    displaySection("unauthorized");
20  }
21 });
```

@joel__lord

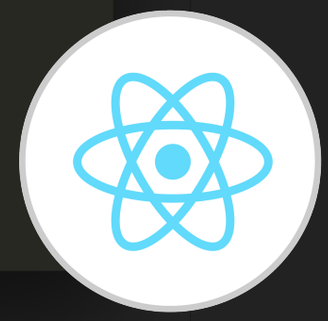
```
import Vue from "vue";
import Router from "vue-router";
Vue.use(Router);

function requireAuth(to, from, next) {
  if (!isLoggedIn()) {
    next({
      path: "/unauthorized",
      query: { redirect: to.fullPath }
    });
  } else {
    next();
  }
}

export default new Router({
  mode: "history",
  routes: [
    {
      path: "/",
      name: "Home",
      component: Home
    },
    {
      path: "/secret",
      name: "Secret",
      beforeEnter: requireAuth,
      component: Secret
    }
  ]
});
```

@joel__lord #AllThingsO

```
import Vue from "vue";
import Router from "vue-router";
Vue.use(Router);

function requireAuth(to, from, next) {
  if (!isLoggedIn()) {
    next({
      path: "/unauthorized",
      query: { redirect: to.fullPath }
    });
  } else {
    next();
  }
}

export default new Router({
  mode: "history",
  routes: [
    {
      path: "/",
      name: "Home",
      component: Home
    },
    {
      path: "/secret",
      name: "Secret",
      beforeEnter: requireAuth,
      component: Secret
    }
  ]
});
```

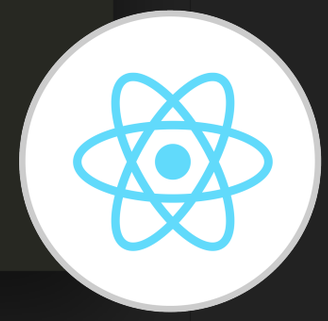
```
1  import Vue from "vue";
2  import Router from "vue-router";
3  Vue.use(Router);
4
5  function requireAuth(to, from, next) {
6    if (!isLoggedIn()) {
7      next({
8        path: "/unauthorized",
9        query: { redirect: to.fullPath }
10     });
11   } else {
12     next();
13   }
14 }
15
16 export default new Router({
17   mode: "history",
18   routes: [
19     {
20       path: "/",
21       name: "Home",
22       component: Home
23     },
24     {
25       path: "/secret",
26       name: "Secret",
27       beforeEnter: requireAuth,
28       component: Secret
29     }
30   ]
31 });
32
```

```jsx
const PrivateRoute = ({ component: Component, ...rest }) => (
    <Route
        {...rest}
        render={props =>
            isLoggedIn() ? (
                <Component {...props} />
            ) : (
                <Redirect
                    to={{
                      pathname: "/unauthorized",
                      state: { from: props.location }
                    }}
                />
            )
        }
    />
);

class App extends Component {
  render() {
    return (
        <Router>
            <Switch>
              <Route path="/callback" component={Callback} />
              <PrivateRoute path="/secret" component={Secret} />
              <Route path="/unauthorized" component={Unauthorized} />
            </Switch>
        </Router>
    );
  }
}

export default App;
```



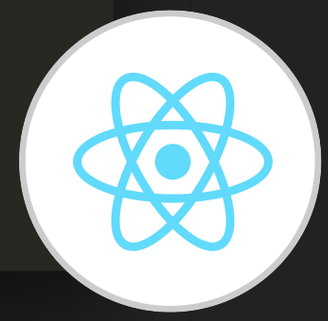
@joel__lord

```jsx
const PrivateRoute = ({ component: Component, ...rest }) => (
    <Route
        {...rest}
        render={props =>
            isLoggedIn() ? (
                <Component {...props} />
            ) : (
                <Redirect
                    to={{
                      pathname: "/unauthorized",
                      state: { from: props.location }
                    }}
                />
            )
        }
    />
);

class App extends Component {
  render() {
    return (
        <Router>
            <Switch>
                <Route path="/callback" component={Callback} />
                <PrivateRoute path="/secret" component={Secret} />
                <Route path="/unauthorized" component={Unauthorized} />
            </Switch>
        </Router>
    );
  }
}

export default App;
```



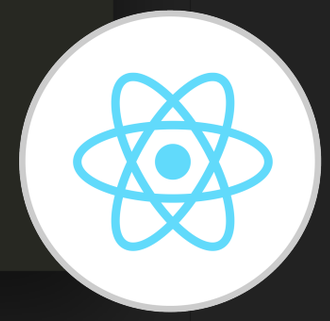
@joel__lord

```jsx
const PrivateRoute = ({ component: Component, ...rest }) => (
    <Route
        {...rest}
        render={props =>
            isLoggedIn() ? (
                <Component {...props} />
            ) : (
                <Redirect
                    to={{
                      pathname: "/unauthorized",
                      state: { from: props.location }
                    }}
                />
            )
        }
    />
);

class App extends Component {
  render() {
    return (
        <Router>
            <Switch>
              <Route path="/callback" component={Callback} />
              <PrivateRoute path="/secret" component={Secret} />
              <Route path="/unauthorized" component={Unauthorized} />
            </Switch>
        </Router>
    );
  }
}

export default App;
```



@joel__lord

```jsx
const PrivateRoute = ({ component: Component, ...rest }) => (
    <Route
        {...rest}
        render={props =>
            isLoggedIn() ? (
                <Component {...props} />
            ) : (
                <Redirect
                    to={{
                      pathname: "/unauthorized",
                      state: { from: props.location }
                    }}
                />
            )
        }
    />
);

class App extends Component {
  render() {
    return (
        <Router>
            <Switch>
              <Route path="/callback" component={Callback} />
              <PrivateRoute path="/secret" component={Secret} />
              <Route path="/unauthorized" component={Unauthorized} />
            </Switch>
        </Router>
    );
  }
}

export default App;
```



@joel__lord

@joel__lord #AllThingsOpen

RESOURCES

- General JWT resource
  - jwt.io

RESOURCES

- General JWT resource
  - jwt.io
- Overview of JWT Signing Algorithms
  - bit.ly/jwt-alg

RESOURCES

- General JWT resource
  - jwt.io
- Overview of JWT Signing Algorithms
  - bit.ly/jwt-alg
- JWT Handbook
  - bit.ly/jwt-book

SUMMARY

- Single Page Application security is mainly concerned with authorization.

SUMMARY

- Single Page Application security is mainly concerned with authorization.
- JSON Web Tokens are excellent for securing SPA applications.

SUMMARY

- Single Page Application security is mainly concerned with authorization.
- JSON Web Tokens are excellent for securing SPA applications.
- Many excellent JWT Libraries exist for all languages and frameworks.

THANK YOU

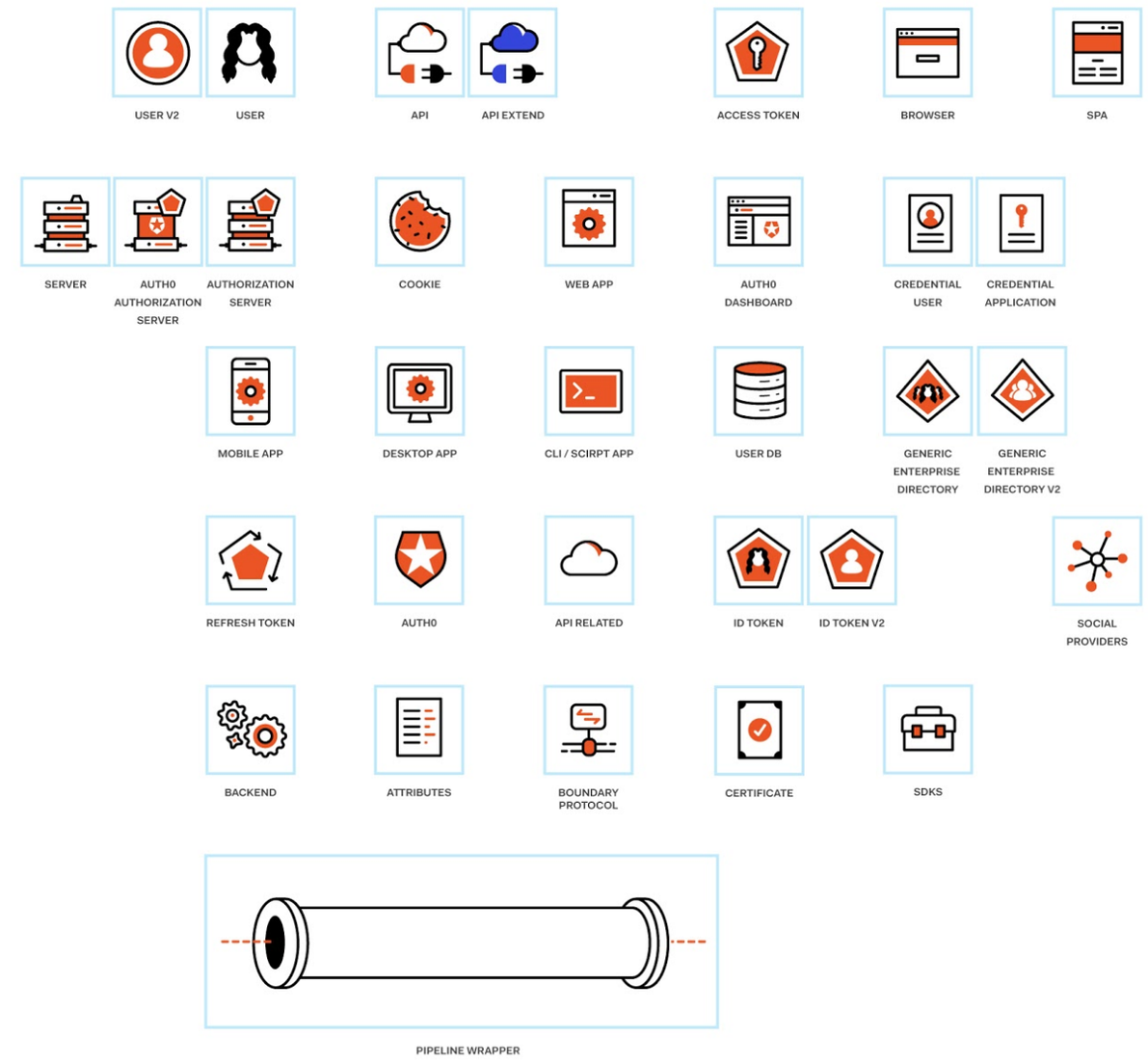
All Things Open, Raleigh, NC
October 23rd, 2018

@joel__lord

joellord

TEXT

Auth0


USER V2
USER
API
API EXTEND
ACCESS TOKEN
BROWSER
SPA
SERVER
AUTH0 AUTHORIZATION SERVER
COOKIE
WEB APP
AUTH0 DASHBOARD
CREDENTIAL USER
CREDENTIAL APPLICATION
MOBILE APP
DESKTOP APP
CLI / SCIRPT APP
USER DB
GENERIC ENTERPRISE DIRECTORY
GENERIC ENTERPRISE DIRECTORY V2
REFRESH TOKEN
AUTH0
API RELATED
ID TOKEN
ID TOKEN V2
SOCIAL PROVIDERS
BACKEND
ATTRIBUTES
BOUNDARY PROTOCOL
CERTIFICATE
SDKS
PIPELINE WRAPPER

Auth0

TEXT