

L'API : une interface comme une autre (qu'on peut tester aussi)



```
{  
  "error": "TooManyRequests",  
  "message": "Trop d'APIs listées en une seule session.",  
  "hint": "Utilisez la pagination... ou buvez un café ☕",  
  "docs": "https://api.my-career.dev/docs/rate-limiting"  
}
```

Anne-Laure Gaillard, Lead QA @Talarian



CGI

COCKTAIL
Système d'information pour les établissements
de l'Enseignement Supérieur et la Recherche

ManoMano

Talarian





**Les API Web sont
devenues omniprésentes**



[Début](#)[Côté client](#)[Côté serveur](#)[Points d'accès](#)[Ressources contre services](#)[Documentation](#)[Croissance et impact](#)[En entreprise](#)[Entreprises privées](#)[Gouvernements](#)[Exemple](#)[Voir aussi](#)[Références](#)[Bibliographie](#)

Croissance et impact [\[modifier \]](#) [modifier le code \]](#)

Le nombre d'API Web disponibles n'a cessé d'augmenter au cours des dernières années, à mesure que les entreprises réalisent les opportunités de croissance associées à l'exécution d'une plate-forme ouverte, avec laquelle tout développeur peut interagir. ProgrammableWeb suit plus de 24 000 API Web disponibles en 2022, contre 105 en 2005⁷.

Les API Web sont devenues omniprésentes. Il existe peu d'applications/services logiciels majeurs qui n'offrent pas une certaine forme d'API Web. L'une des formes les plus courantes d'interaction avec ces API Web consiste à intégrer des ressources externes, telles que des tweets, des commentaires Facebook, des vidéos [YouTube](#), etc. En fait, il existe des entreprises très prospères, telles que [Disqus](#), dont le service principal est de fournir des outils intégrables, tels qu'un système de commentaires riche en fonctionnalités⁸. Tout [site Web](#) du TOP 100 des sites Web classés par [Alexa Internet](#) utilise des API et/ou fournit ses propres API, ce qui est un indicateur très distinct de l'échelle prodigieuse et de l'impact des API Web dans leur ensemble⁹.

À mesure que le nombre d'API Web disponibles augmentait, des outils [open source](#) ont été développés pour fournir une recherche et une découverte plus sophistiquées.

APIs ison fournit une description lisible par machine d'une API et de ses opérations, et le



CGI

COCKTAIL
Système d'information pour les établissements
de l'Enseignement Supérieur et la Recherche

ManoMano

Talarian

atbdx



PARISTESTCONF



Rechercher

Menu

L'engagement tout *simplement*

Bienvenue sur la plateforme pour créer,
participer, s'engager ou soutenir une
association.



Un mouvement 100%
financé par les citoyens

[En savoir plus](#)

**Je soutiens
HelloAsso**



Elements Console Sources **Network** Performance >> 2

Filter ☐ Invert More filters

All Fetch/XHR Doc CSS JS Font Img Media Manifest Socket Wasm Other

20,000 ms 40,000 ms 60,000 ms 80,000 ms 100,000 ms

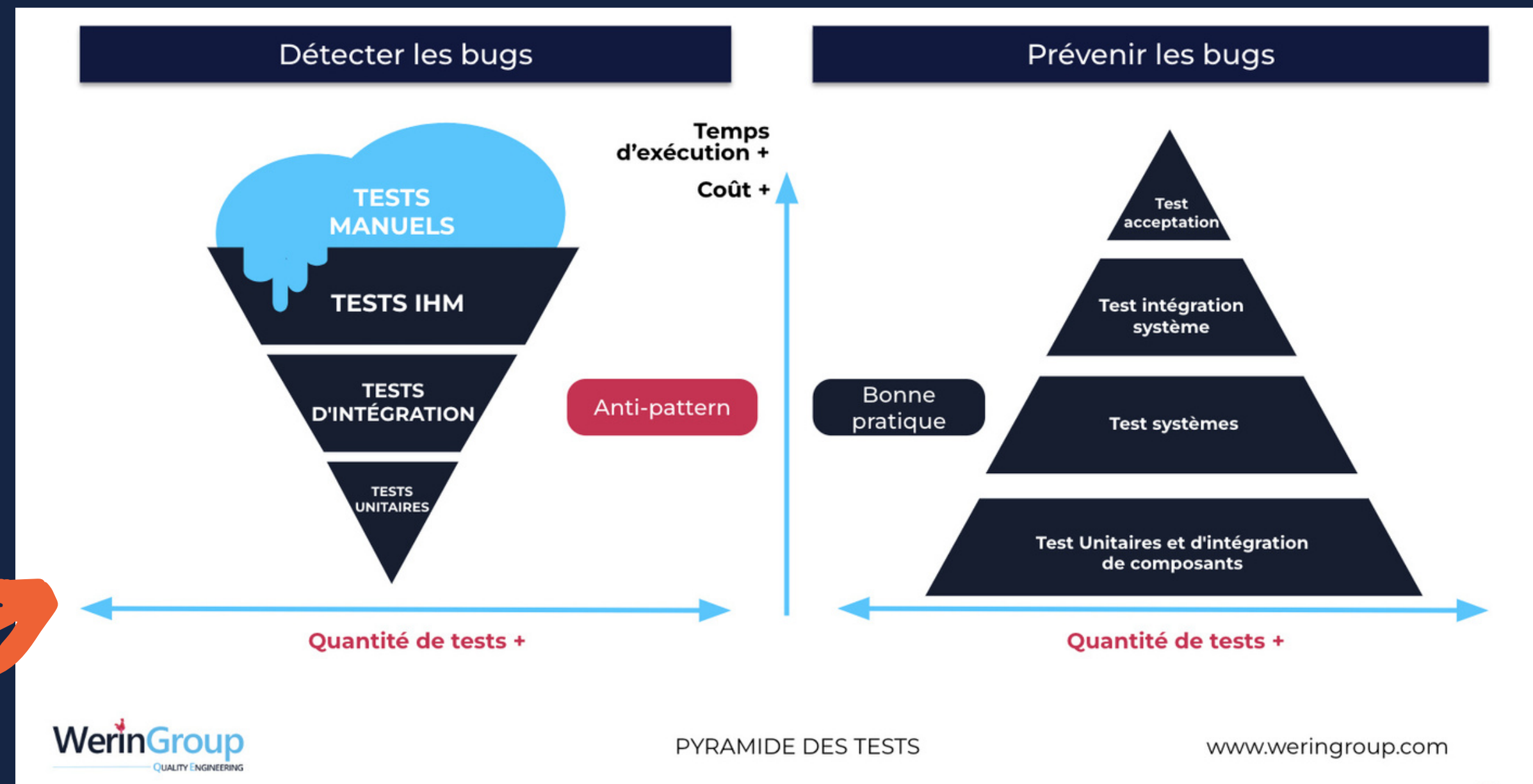
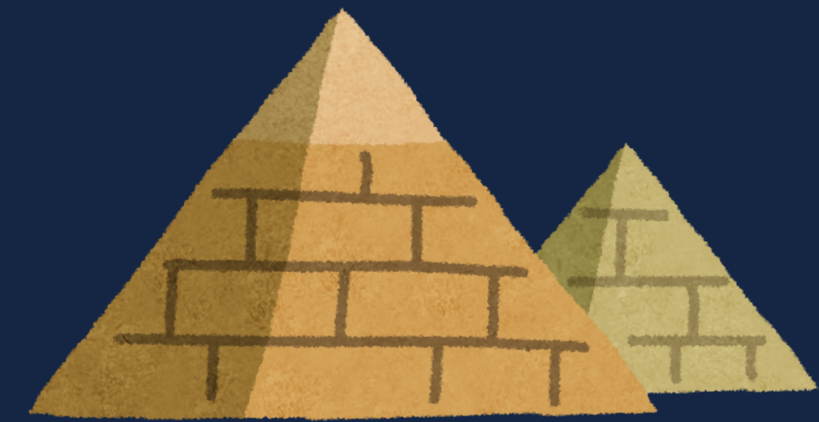
Name	Headers	Preview	Response	Initiator	Timing
611231a1c0ecb69e28e6768.js...	General				
user	Request URL https://api.helloasso.com/v5/agg/user				
settings	Request Method GET				
p	Status Code 200 OK				
i	Remote Address [2606:4700::6812:d5e]:443				
attribution_trigger?pid=377121...	Referrer Policy strict-origin-when-cross-origin				
collect	Response Headers (15)				
wa/?medium=fetch&fmt=g	Request Headers (19)				
collect					
m					
collect					
collect					
collect					
collect					



**On teste déjà
l'interface
graphique**

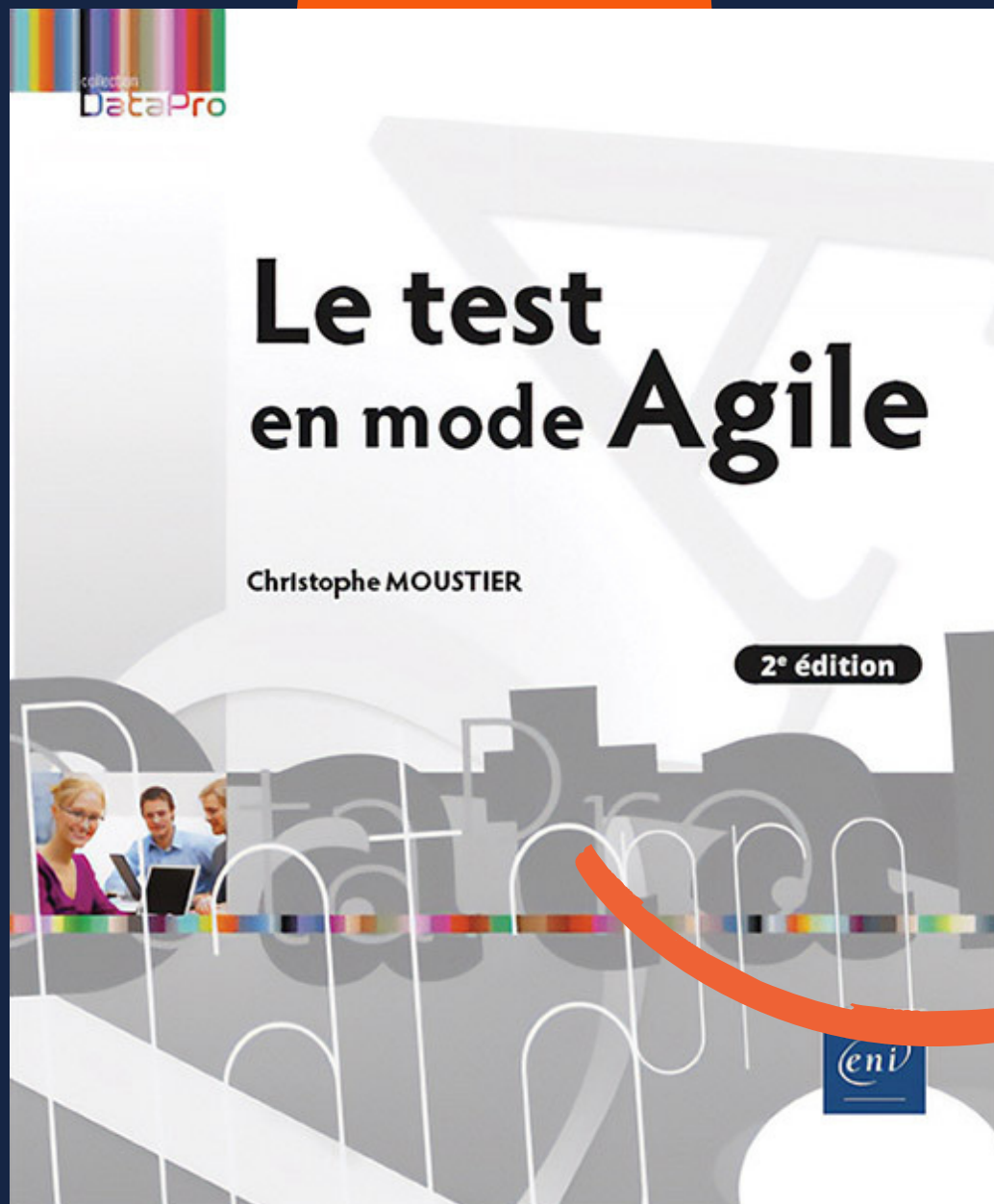
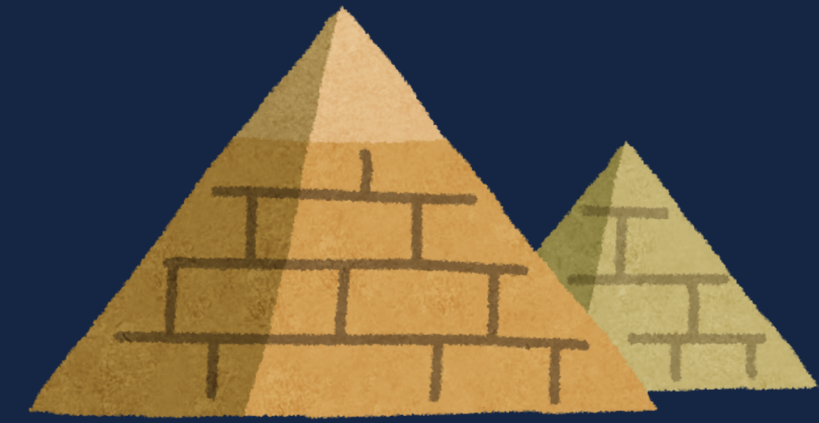


On teste déjà l'interface graphique





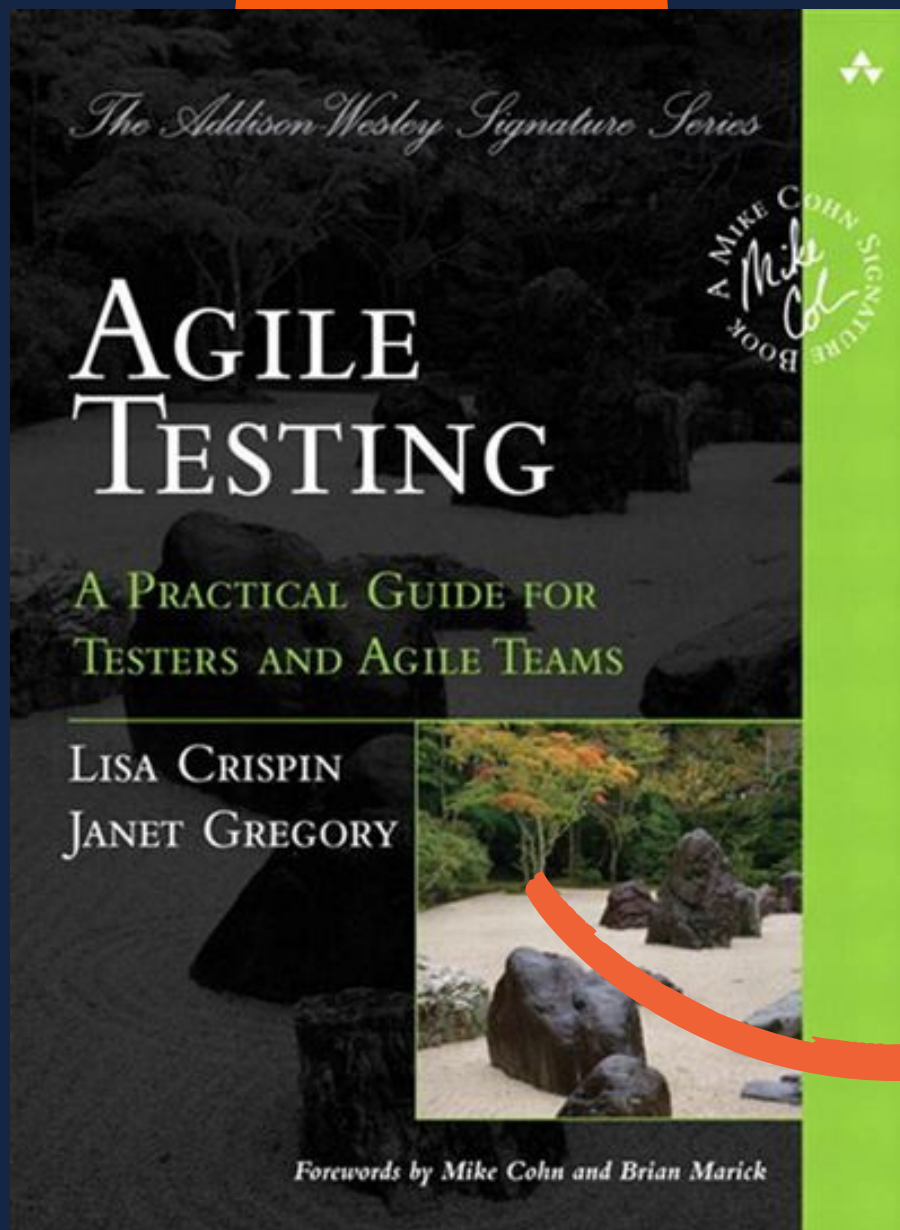
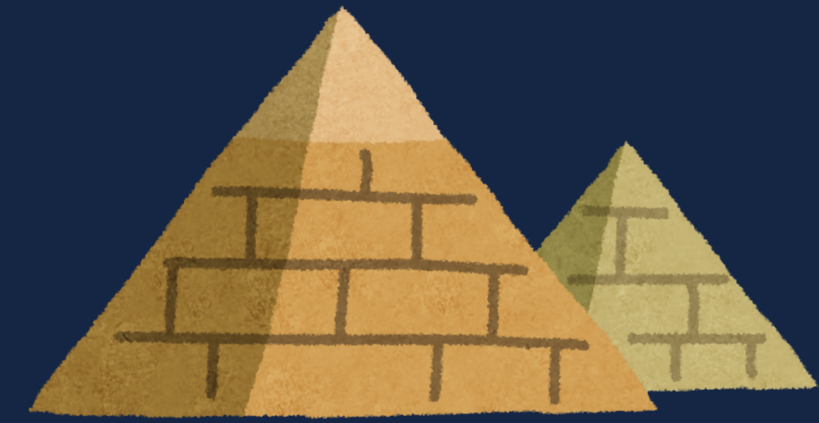
**On teste déjà
l'interface
graphique**



“Dans une approche agile, il est recommandé
de ne pas attendre d’avoir l’intégralité du
processus disponible et de tester ce que l’on a
[...] en particulier au niveau d’un microservice”



**On teste déjà
l'interface
graphique**

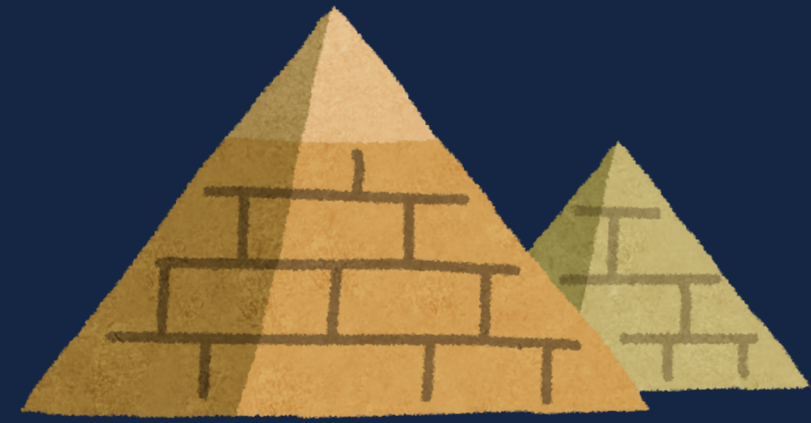


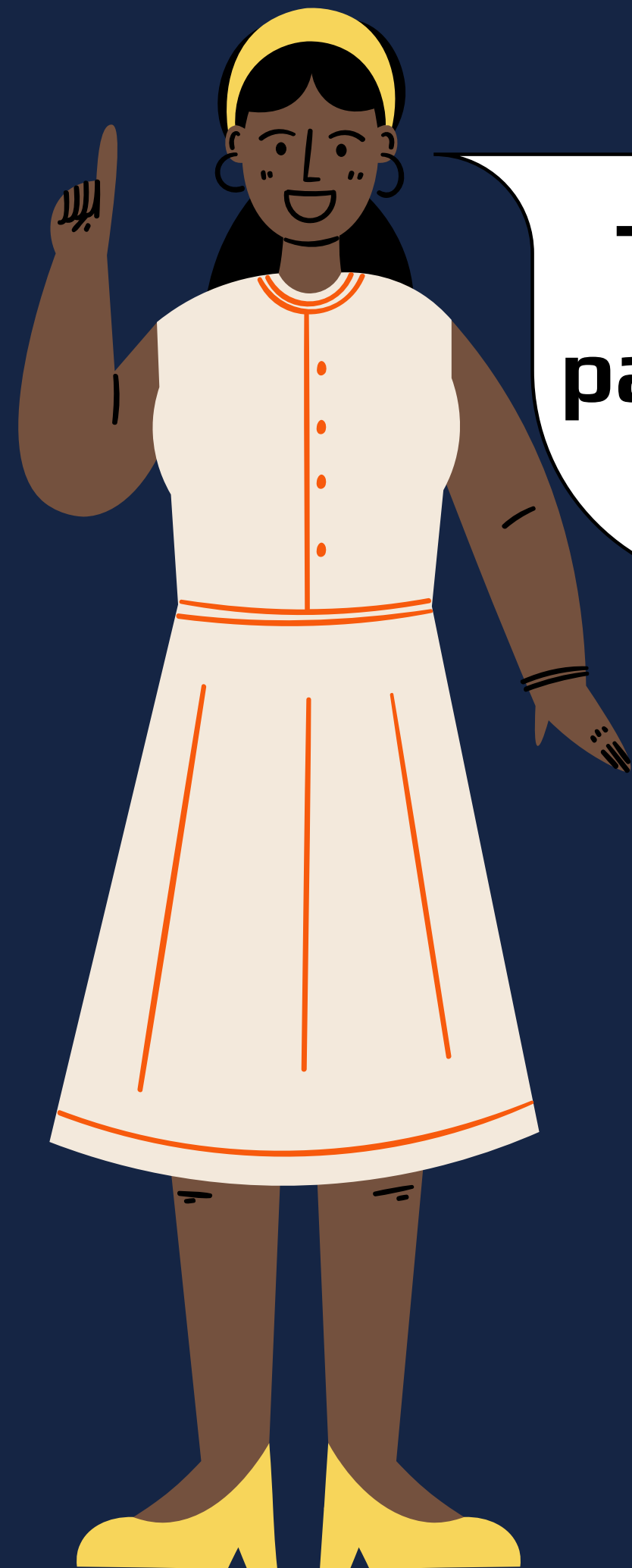
**EXTRA
BONUS**

“[API testing] might produce unexpected results and reveal bugs that would never be found through UI testing. You can control the tests much more easily than when using UI”

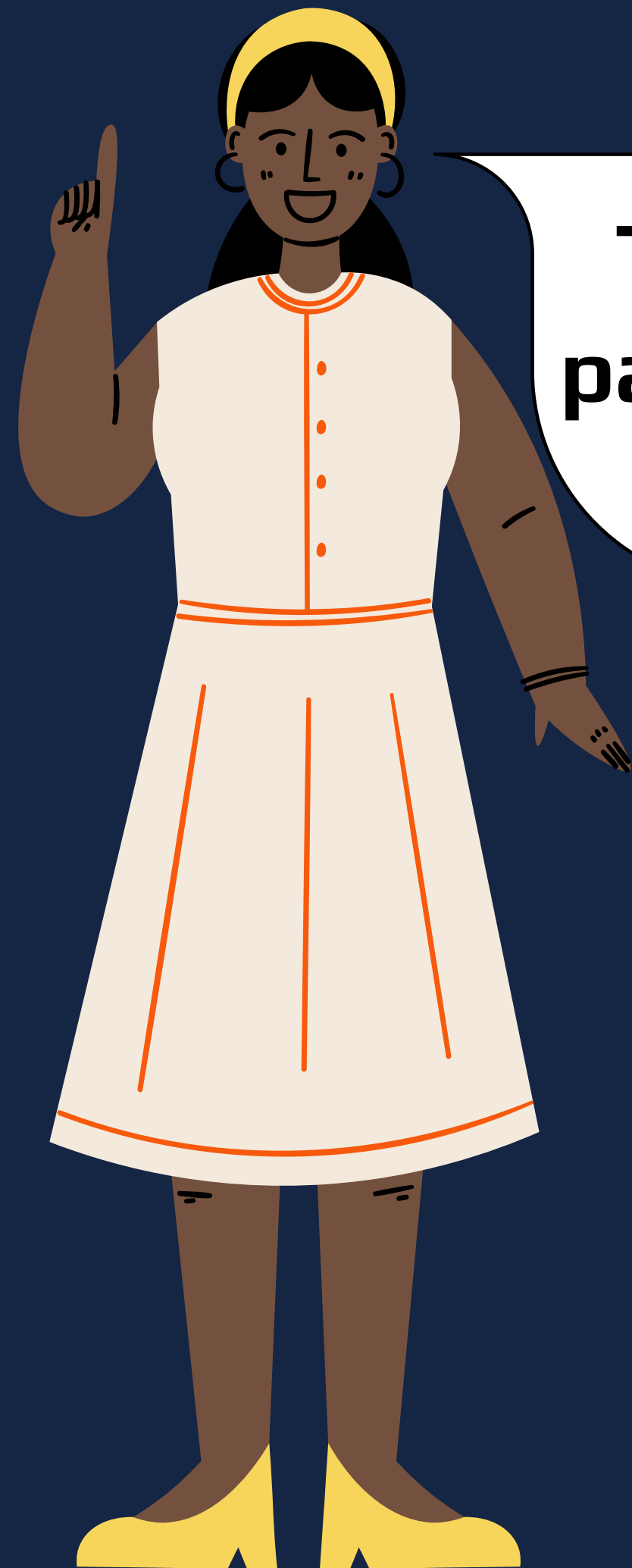


**On teste déjà
l'interface
graphique**

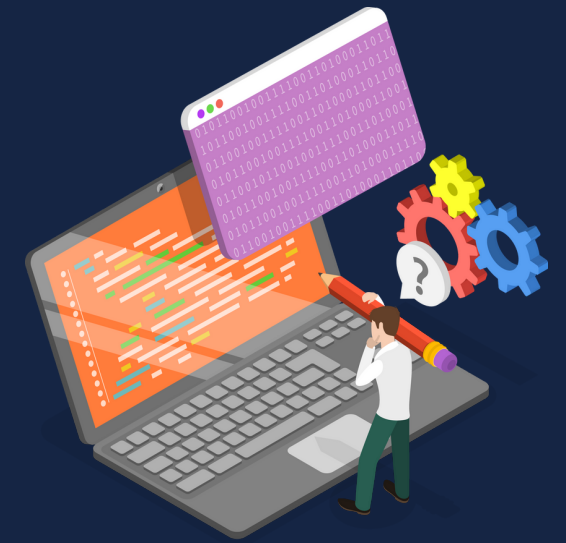


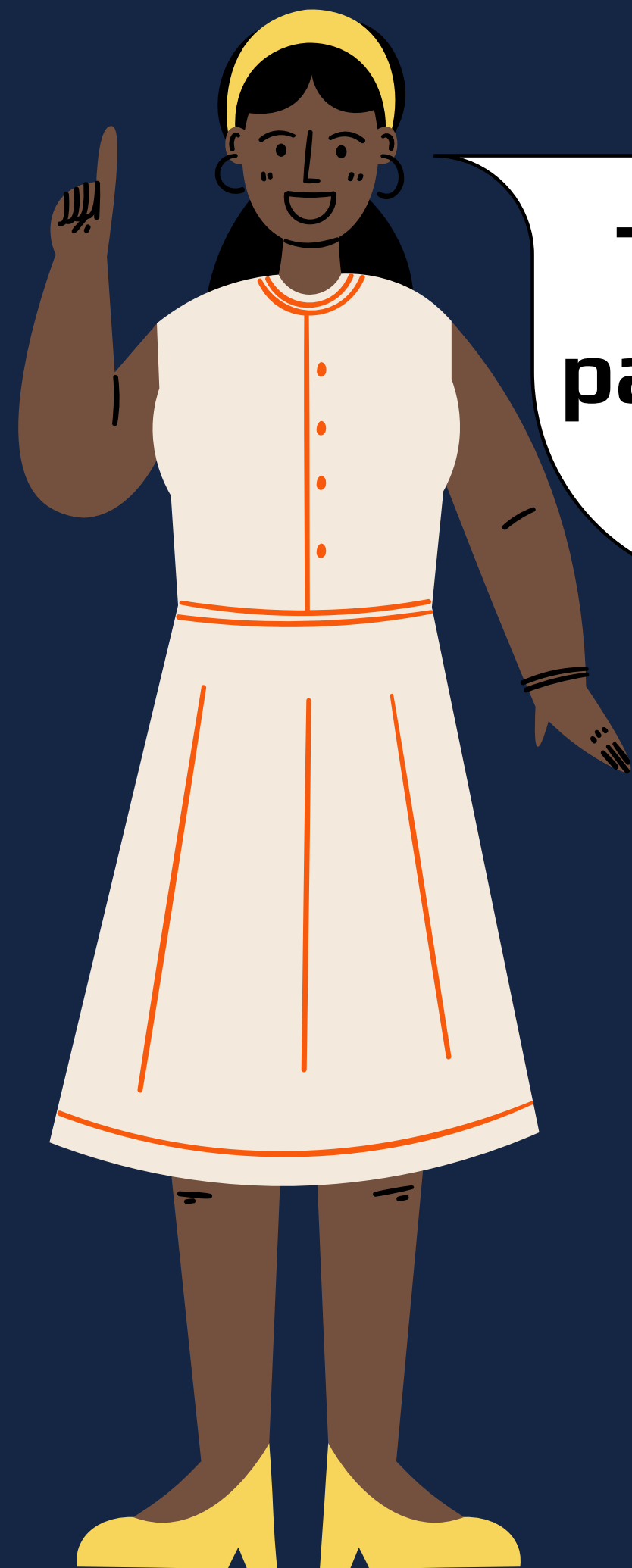


**Tester l'API, c'est ne
pas tester l'expérience
utilisateur.**

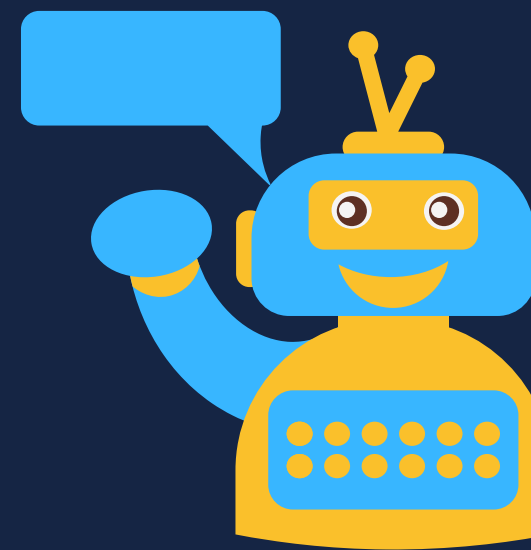


**Tester l'API, c'est ne
pas tester l'expérience
utilisateur.**



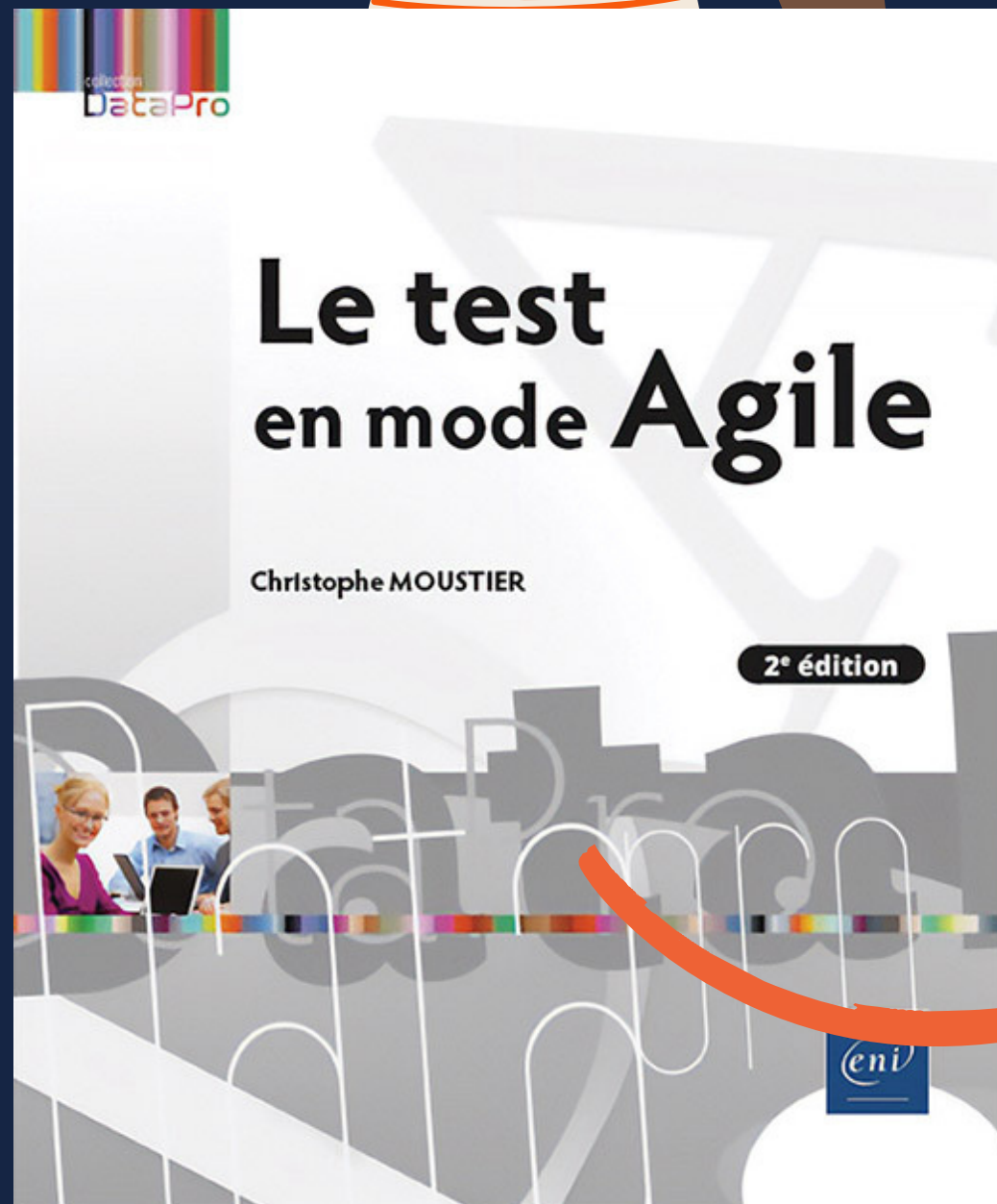


**Tester l'API, c'est ne
pas tester l'expérience
utilisateur.**



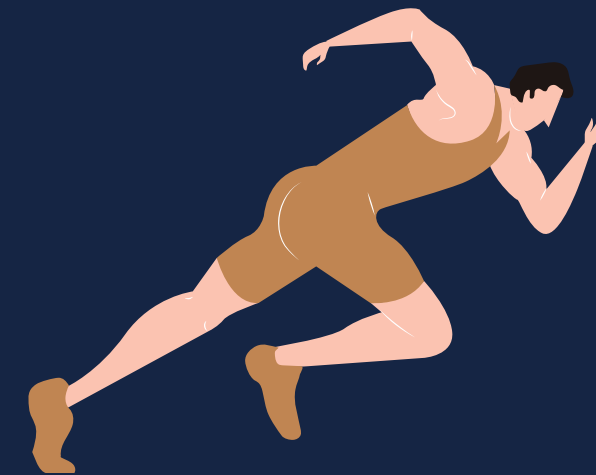
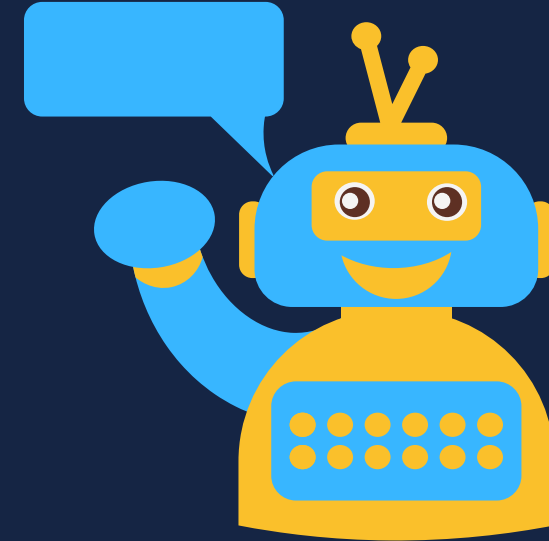


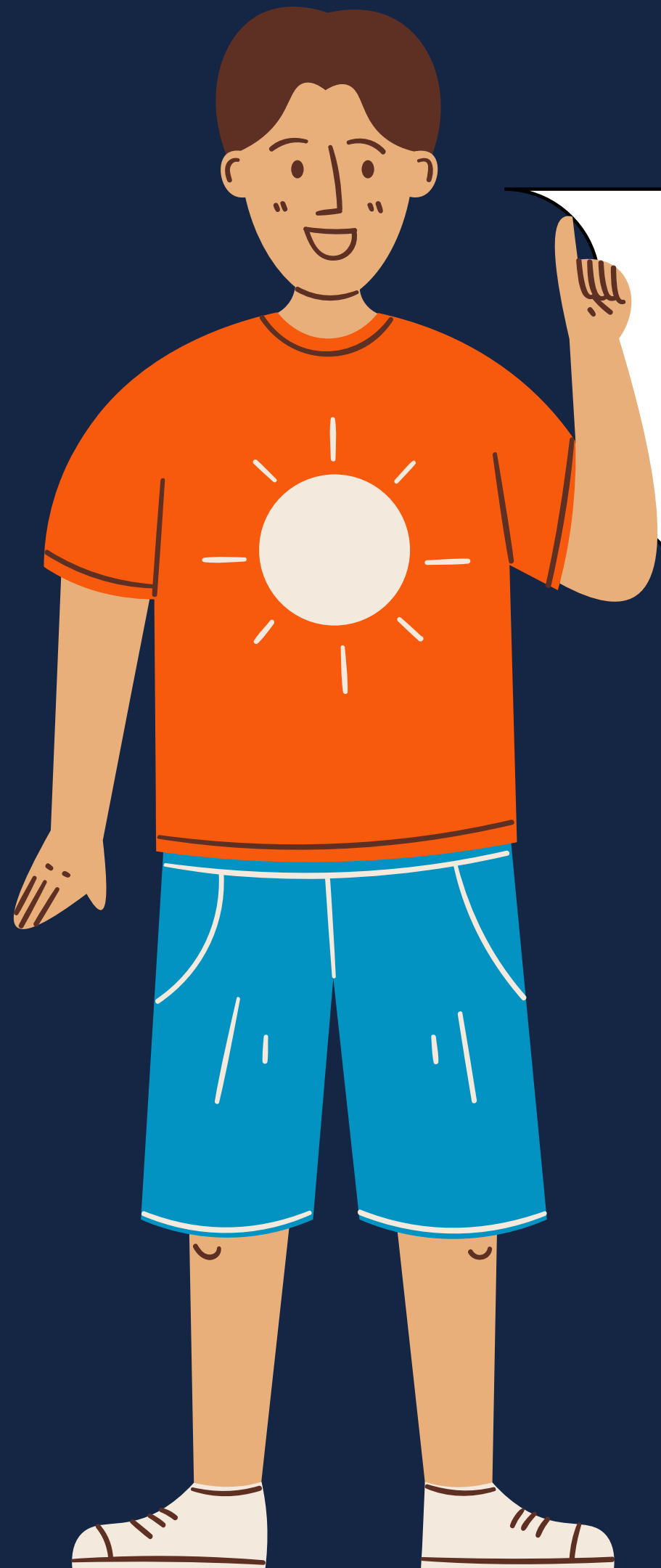
**Tester l'API, c'est ne
pas tester l'expérience
utilisateur.**



“Dans une approche agile, il est recommandé de ne pas attendre d'avoir l'intégralité du processus disponible et de tester ce que l'on a [...] en particulier au niveau d'un microservice”

**Titre : Tests de charge d'un
processus métier et
disponibilités des
microservices**

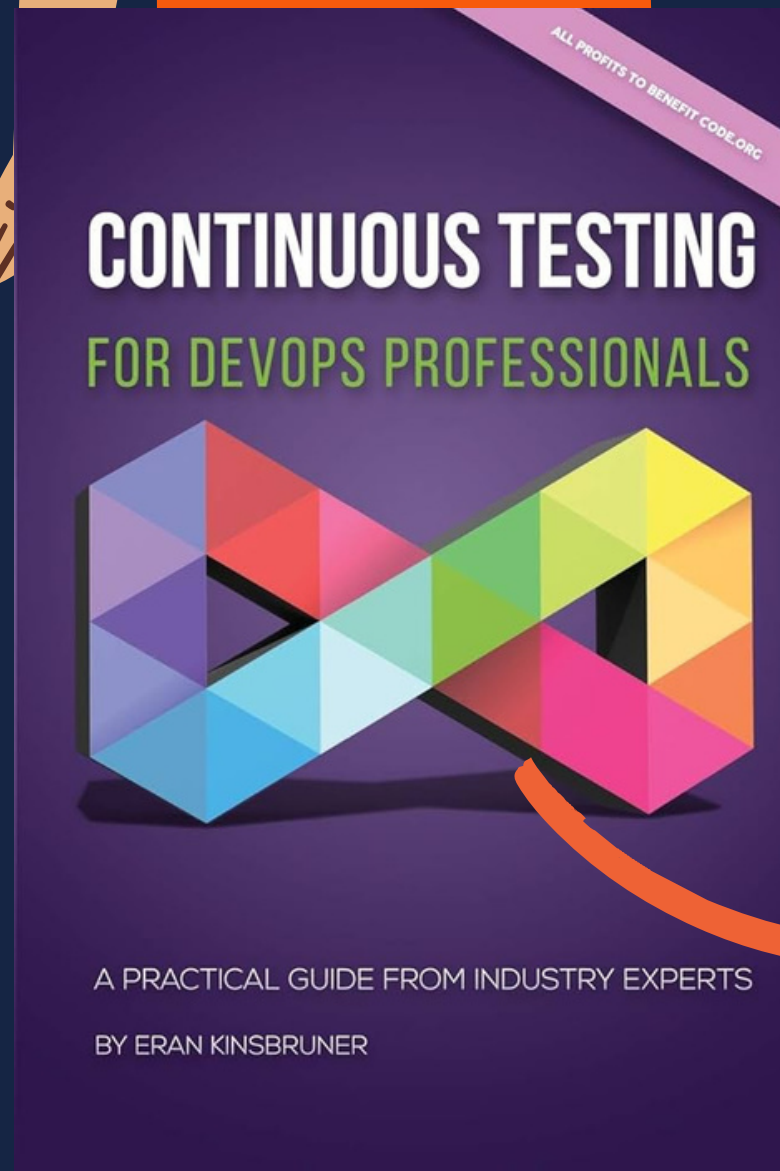




**Tester les APIs,
c'est technique.**



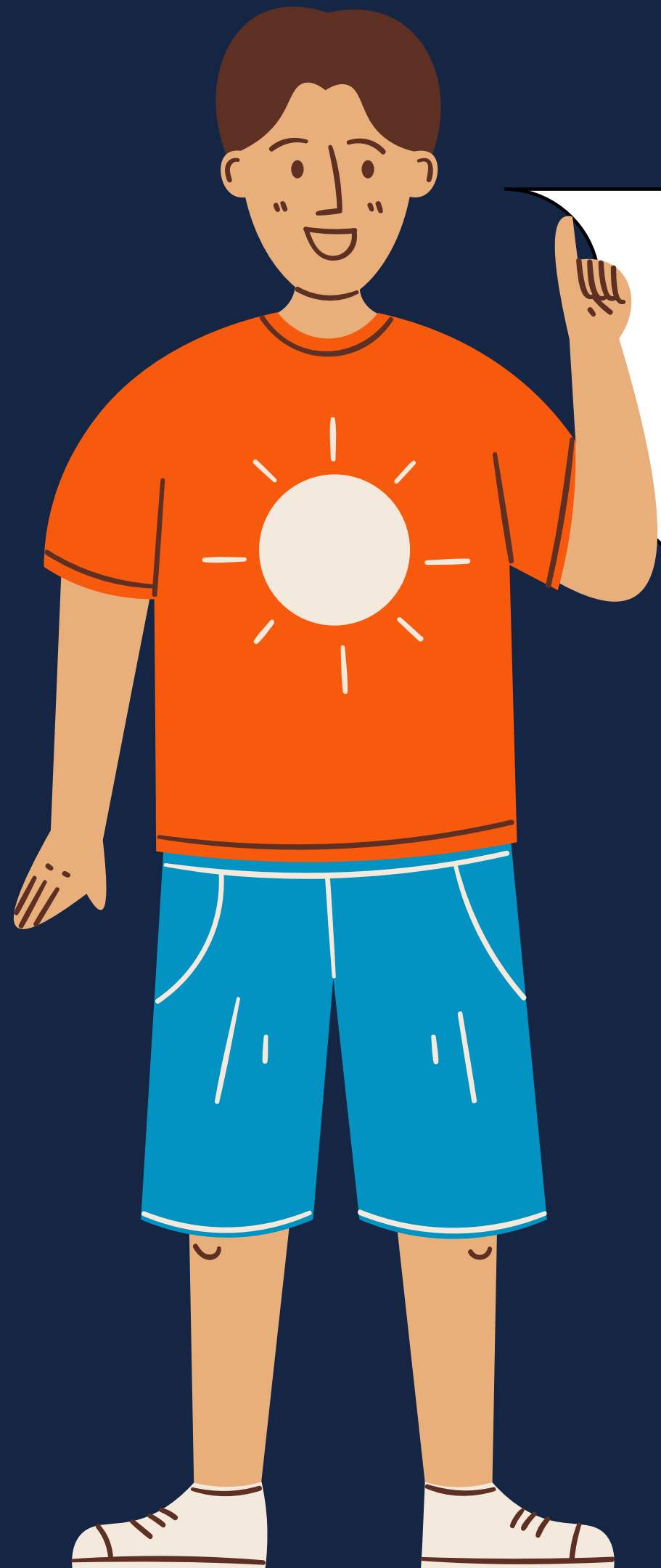
**Tester les APIs,
c'est technique.**



Automatisation des tests d'API :

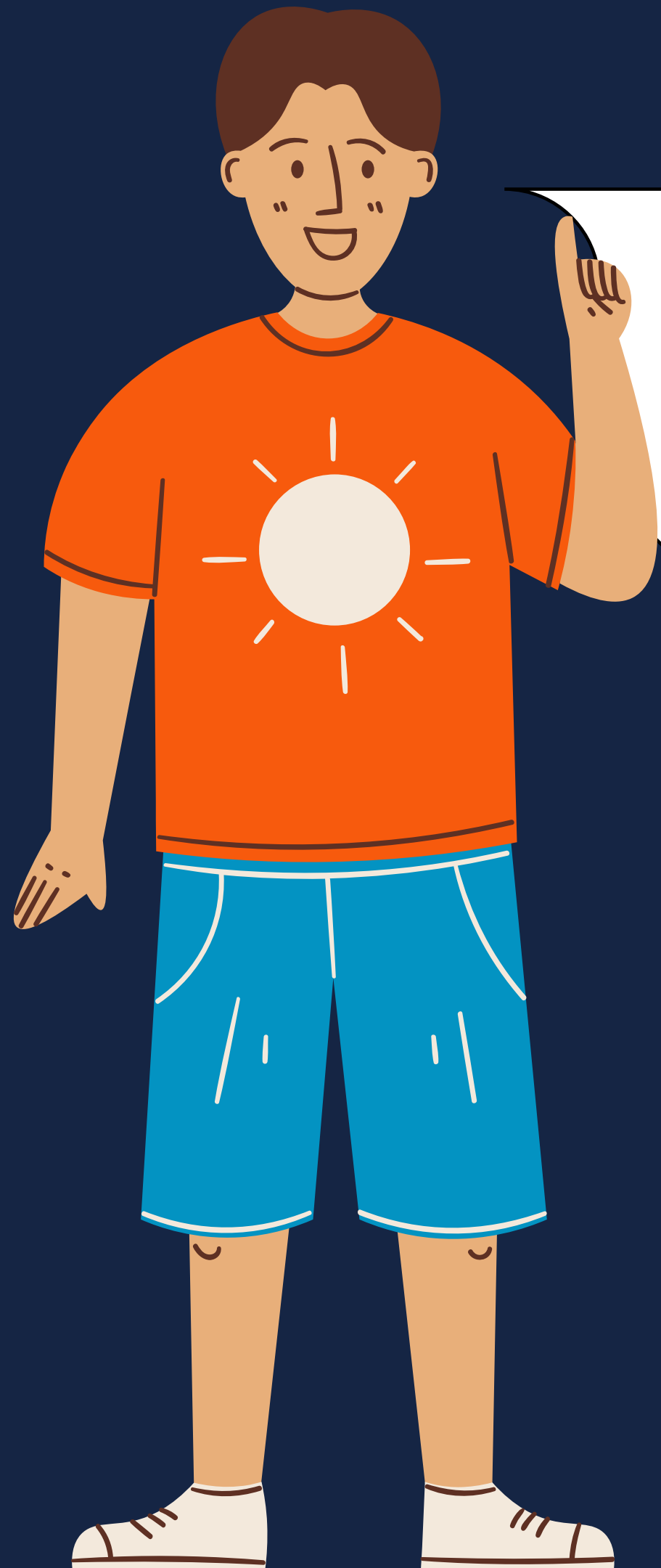
49% QA

28% Dev



**Tester les APIs,
c'est technique.**

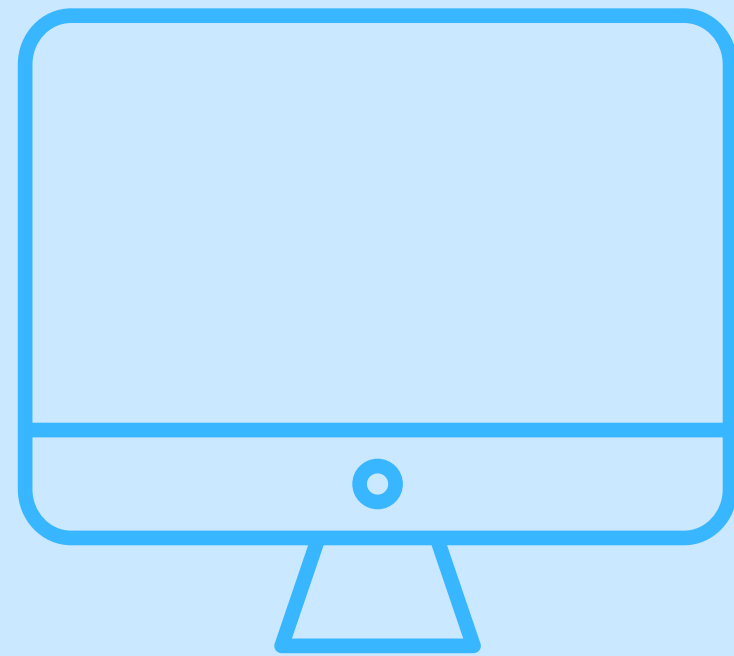




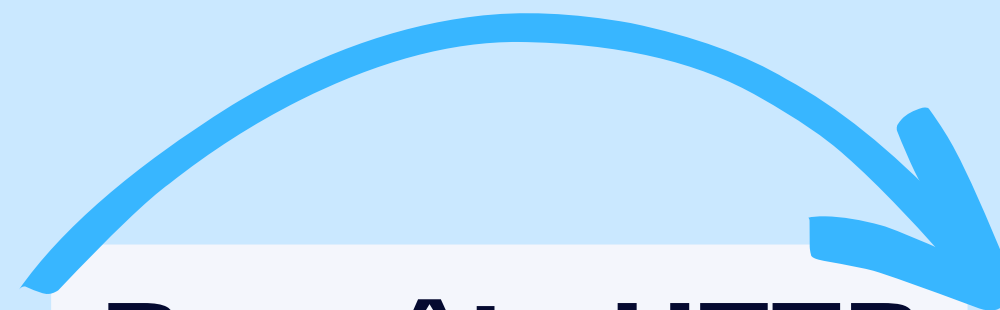
**Tester les APIs,
c'est technique.**



API REST



Client



Requête HTTP



Serveur



Réponse

Verbe

GET	Récupère
POST	Crée
PATCH/PUT	Modifie
DELETE	Supprime

Endpoint/URL

The screenshot shows a REST client interface with a dark theme. At the top, there's a dropdown menu set to 'POST' and a text input field containing the URL 'https://postman-echo.com/post'. To the right of the URL is a blue 'Send' button. Below these are tabs for 'Overview', 'Params', 'Authorization', 'Headers (11)', 'Body', 'Scripts', and 'Settings'. The 'Body' tab is selected and underlined. Under the 'Body' tab, there are radio buttons for 'none', 'form-data', 'x-www-form-urlencoded', 'raw' (which is selected), 'binary', and 'GraphQL'. To the right of these is a 'JSON' label with a dropdown arrow. Further right are links for 'Cookies' and 'Beautify'. The main area shows a JSON body with the following content:

```
1  {
2  |    "payload": "Bdx Testing"
3  }
```

Param

Query

Path

Request Body

Request Headers

...



Day 01: API client / API client / echo



Save



Share

POST



https://postman-echo.com/post

Send

Status code

Overview

Params

Authorization

Headers (11)

Body

Scripts

Settings

Cookies

☐ none ☐ form-data ☐ x-www-form-urlencoded ☒ raw ☐ binary ☐ GraphQL JSON

```
1 {
2   "payload": "Bdx Testing"
3 }
```

Body Cookies (1) Headers (7) Test Results

200 OK

• 1.12 s • 1.01 KB • | Save Response ...

{ } JSON

Preview

Visualization

```
1 {
2   "args": {},
3   "data": {
4     "payload": "Bdx Testing"
5   },
6   "files": {},
7   "form": {},
8   "headers": {
9     "host": "postman-echo.com",
10    "x-request-start": "t1742990195.496",
11    "connection": "close",
```

1XX

Information

2XX

Succès

3XX

Redirection

4XX

Erreur client

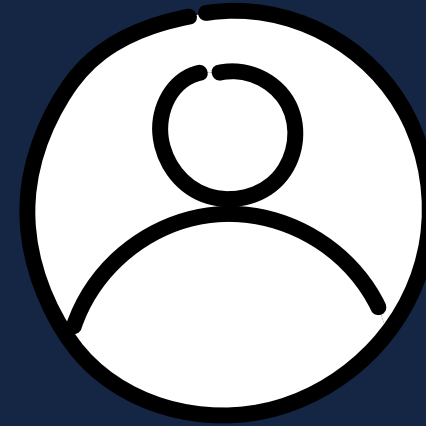
5XX

Erreur serveur

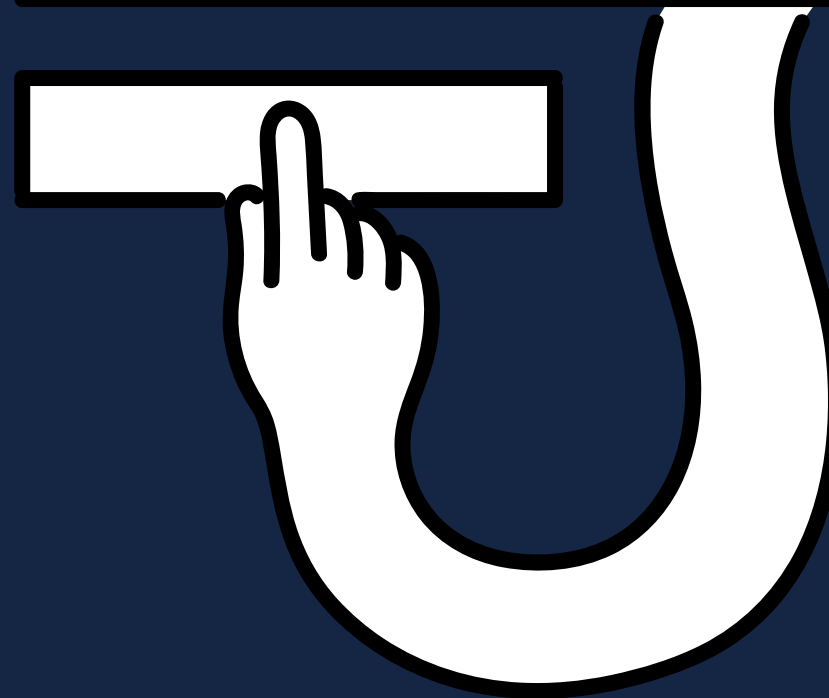
Réponse JSON



Débuter...

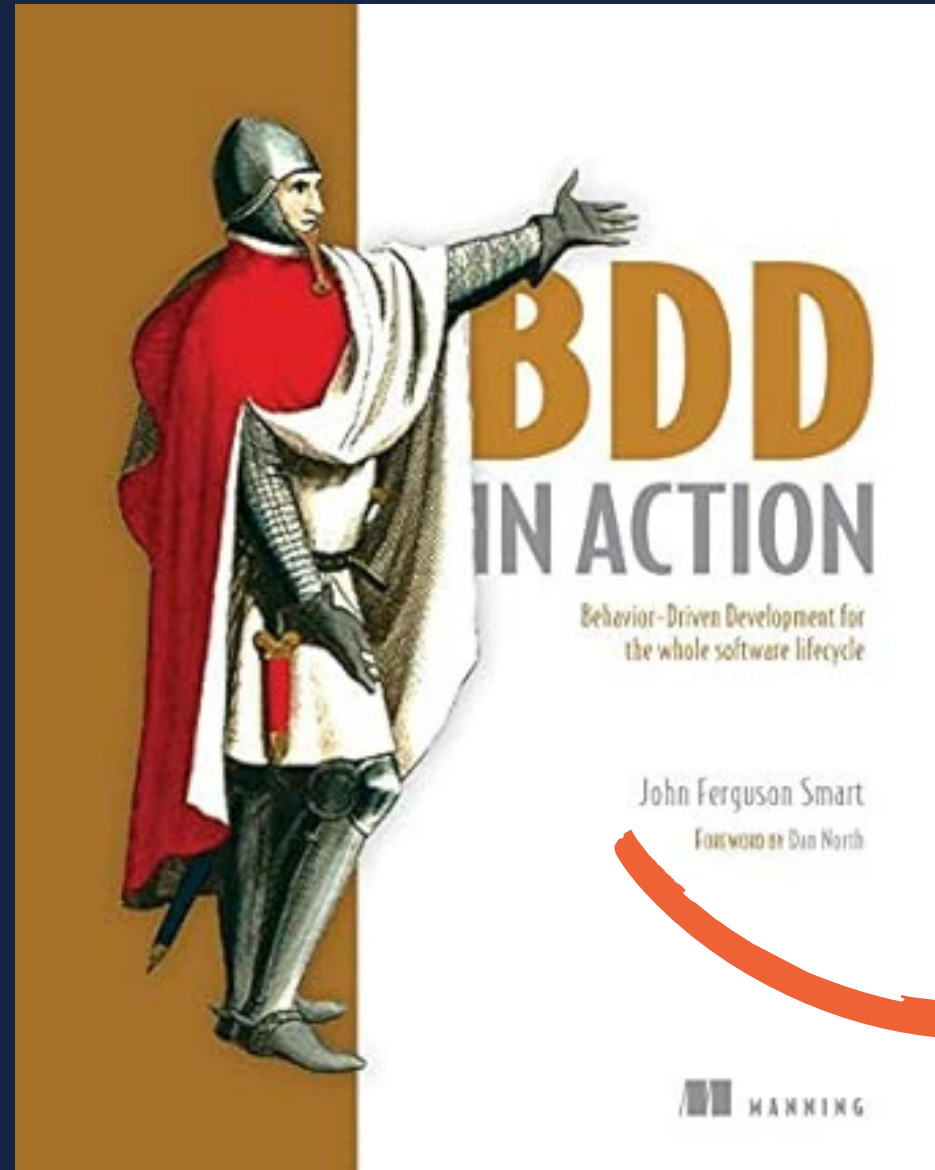


user





Shift left



“A service-based architecture works well
with BDD.”

“When you design a new service using BDD,
you begin by describing the requirements in
the form of practical examples of how the
service will be used”



Doc review



Points de terminaison d'API REST pour les emojis

Utilisez l'API REST pour répertorier et afficher tous les emojis disponibles à utiliser sur GitHub.

Get emojis [↗](#)

Lists all the emojis available to use on GitHub.

Jetons d'accès affinés pour « Get emojis »

Ce point de terminaison fonctionne avec les types de jetons précis suivants:

- [Jetons d'accès utilisateur d'application GitHub](#)
- [Jetons d'accès d'installation d'application GitHub](#)
- [Jetons d'accès personnel affiné](#)

Le jeton précis ne nécessite aucune autorisation.

Ce point de terminaison peut être utilisé sans authentification ou si seules les ressources publiques sont demandées.

Codes d'état de la réponse HTTP pour « Get emojis »

Code d'état	Description
200	OK
304	Not modified

Exemples de code pour « Get emojis »

Exemple de requête

GET /emojis

cURL

JavaScript

Interface CLI de GitHub



```
curl -L \  
-H "Accept: application/vnd.github+json" \  
-H "Authorization: Bearer <YOUR-TOKEN>" \  
-H "X-GitHub-API-Version: 2022-11-28" \  
https://api.github.com/emojis
```

Response

Exemple de réponse

Schéma de réponse

Status: 200

```
{  
  "100":  
    "https://github.githubassets.com/images/icons/emoji/unicode/1f4af.png?v8",  
  "1234":  
    "https://github.githubassets.com/images/icons/emoji/unicode/1f522.png?v8",  
  "+1":  
    "https://github.githubassets.com/images/icons/emoji/unicode/1f44d.png?v8"
```

Requête



[HTTP](#) Day 01: API client / API client / **echo** Save Share

POST

https://postman-echo.com/post

Send

Overview

Params

Authorization

Headers (11)

Body

Scripts

Settings

Cookies

☐ none

☐ form-data

☐ x-www-form-urlencoded

☒ raw

☐ binary

☐ GraphQL

JSON

Beautify

```
1 {
2   "payload": "Bdx Testing"
3 }
```

Body

Cookies (1)

Headers (7)

Test Results

200 OK

1.12 s

1.01 KB

Save Response

{{}} JSON

Preview

Visualization

```
1 {
2   "args": {},
3   "data": {
4     "payload": "Bdx Testing"
5   },
6   "files": {},
7   "form": {},
8   "headers": {
9     "host": "postman-echo.com",
```

Requête



GET planets + No environment

HTTP Day 13: Newman / Newman / planets Save Share

GET https://swapi.dev/api/planets Send

Overview Params Auth Headers (7) Body Scripts Settings Cookies

Pre-req

Post-res •

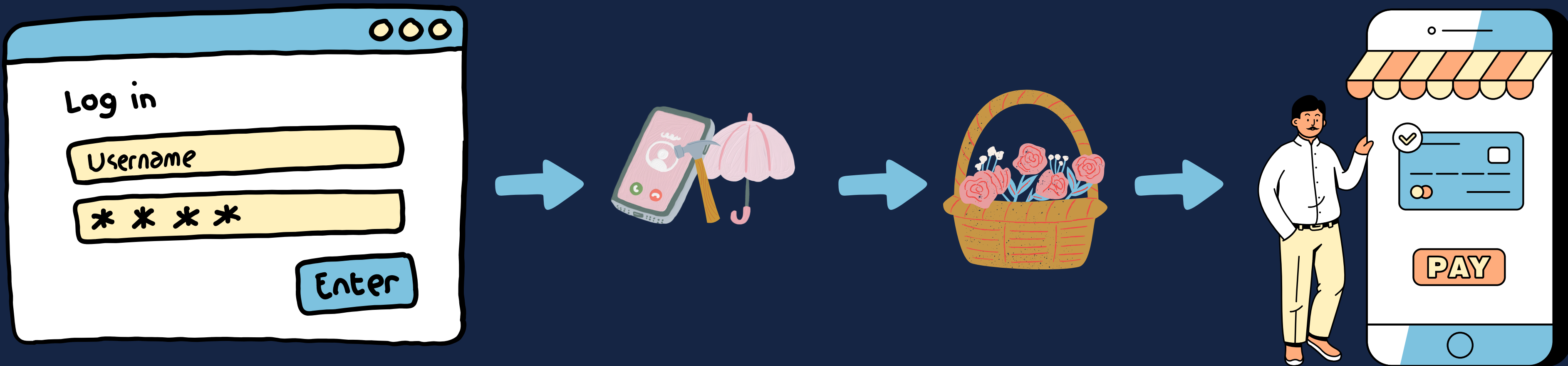
```
1 pm.test("Status code is 200", function () {
2   pm.response.to.have.status(200);
3 });
4 pm.test("Body matches string", function () {
5   pm.expect(pm.response.text()).to.include("Tatooine");
6 });
```

</> ↕ i

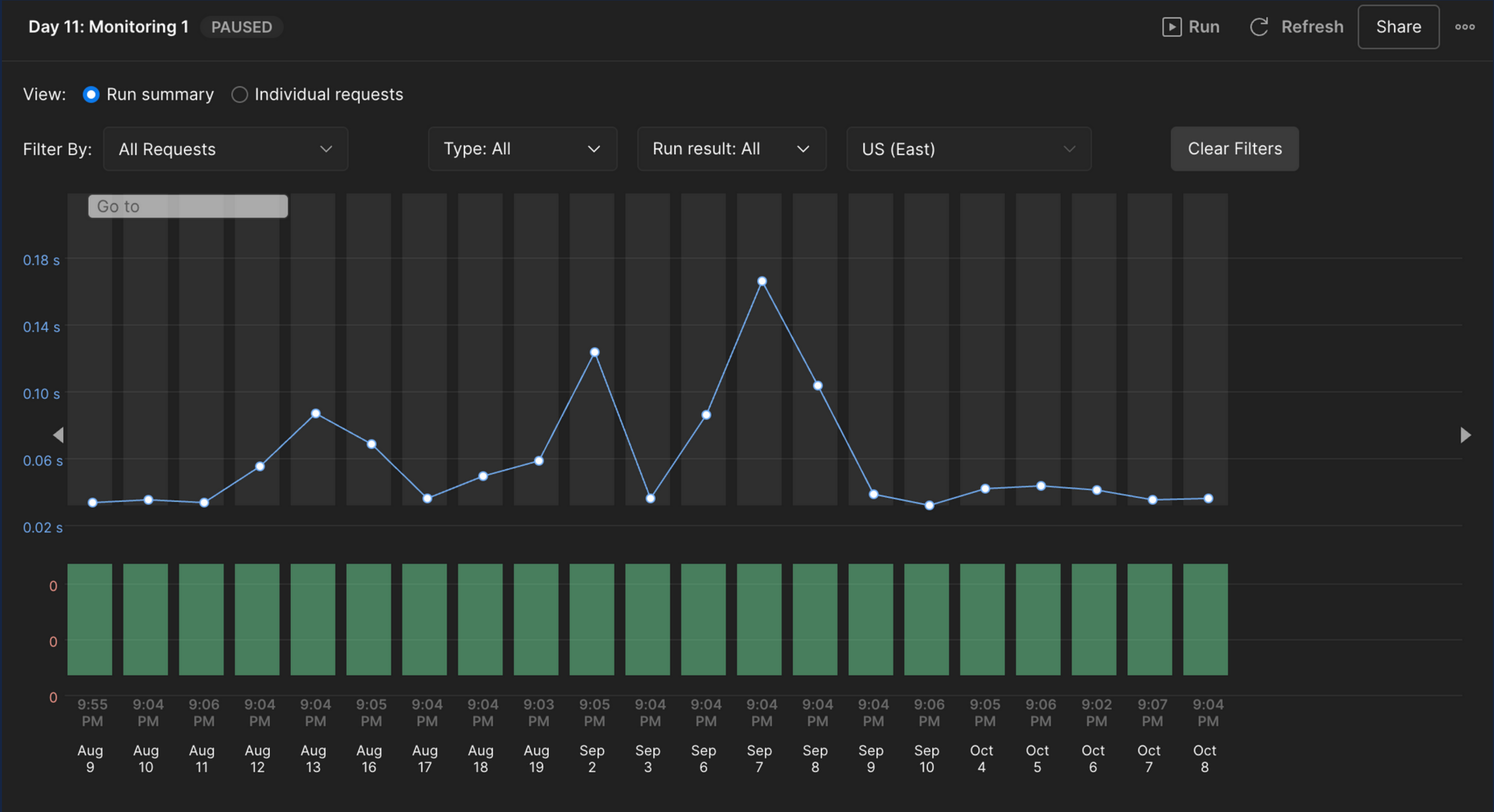


Aller plus loin...

Flow



Automatiser



Automatiser

Comment commencer ?



LE CHAÎNON MANQUANT



VALENTIN GUERLESQUIN
HENRI BIGOT

“Bien que les compétences techniques existantes soient des atouts pour envisager un virage vers l’automatisation des tests, la motivation des membres de l’équipe est une

des clés importantes du succès”

“Faites-vous accompagner”

Automatiser

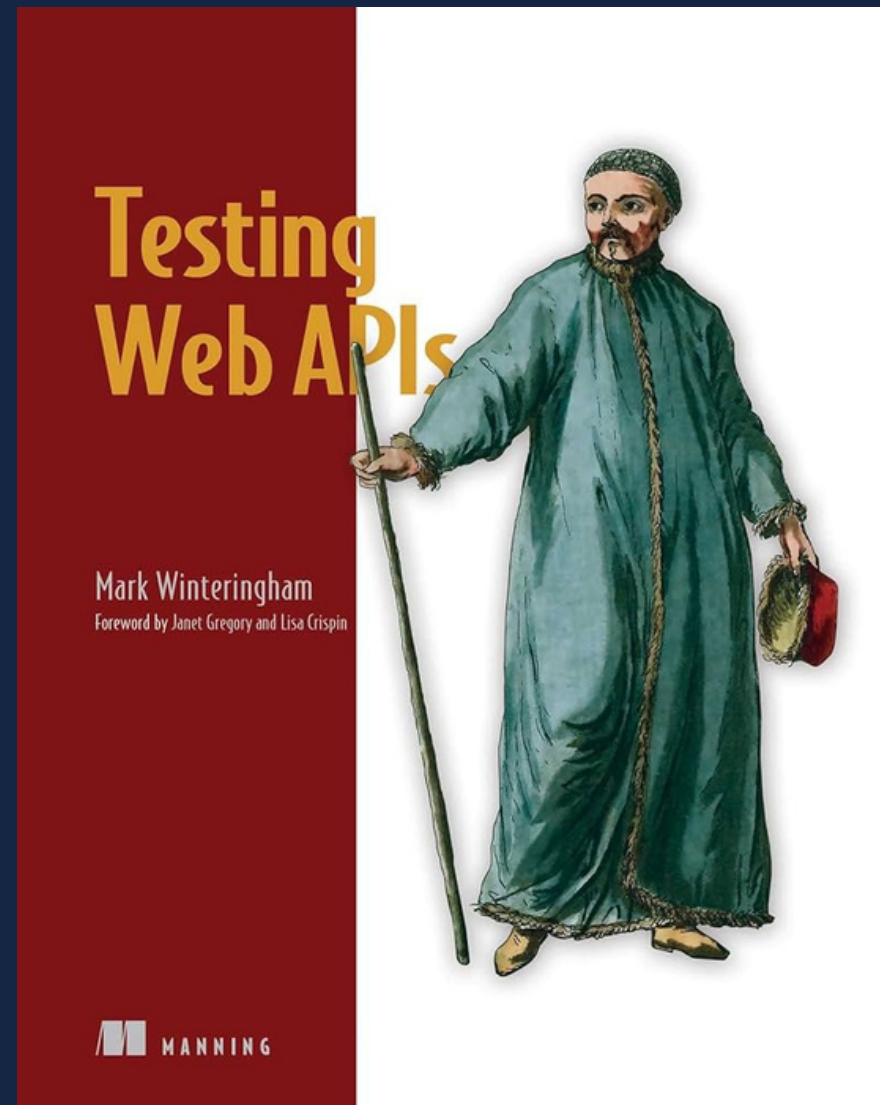
Sur le CI dev, QA, fréquence ?



“Personne n’accepte qu’une simple fusion de branche prenne plus de 15 minutes”

“Des tests automatisés qui n’ont pas trouvé de bug depuis deux sprints peuvent passer d’un rythme quotidien à un rythme hebdomadaire afin de garder un build dans les 10 minutes”

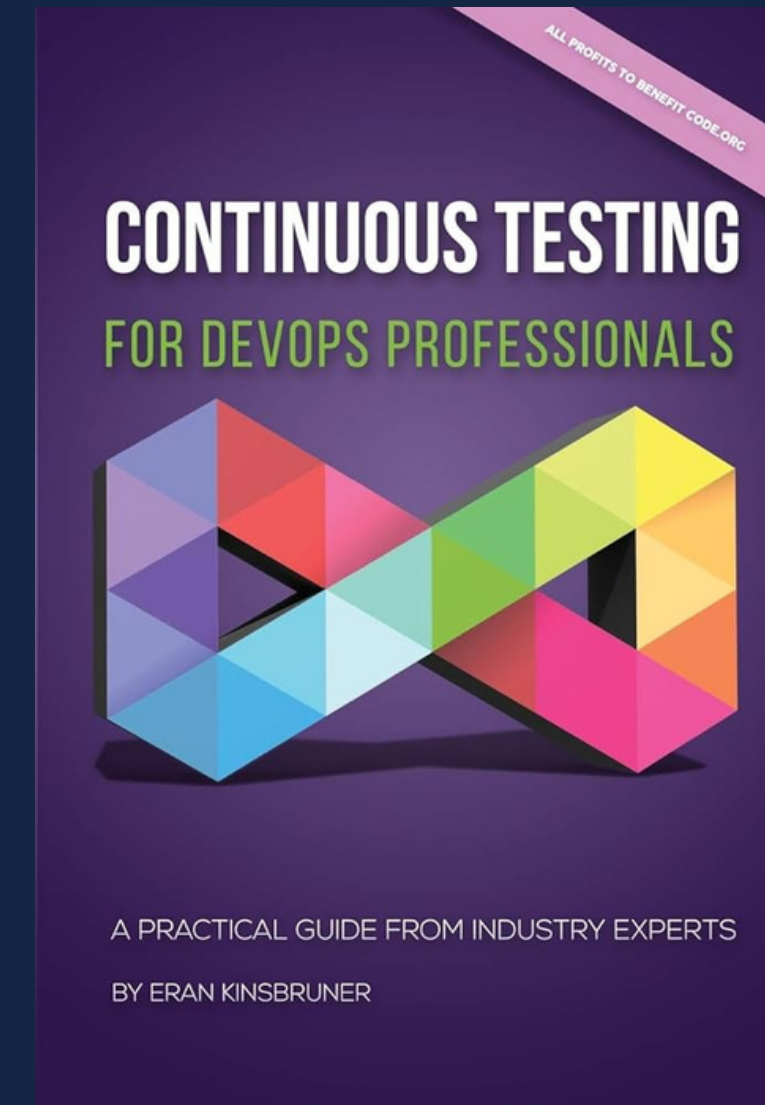
Exploratoire



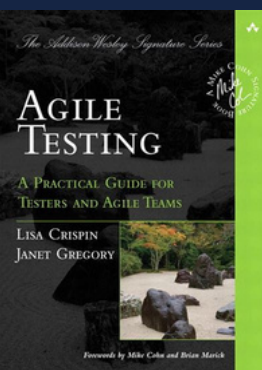
Un chapitre



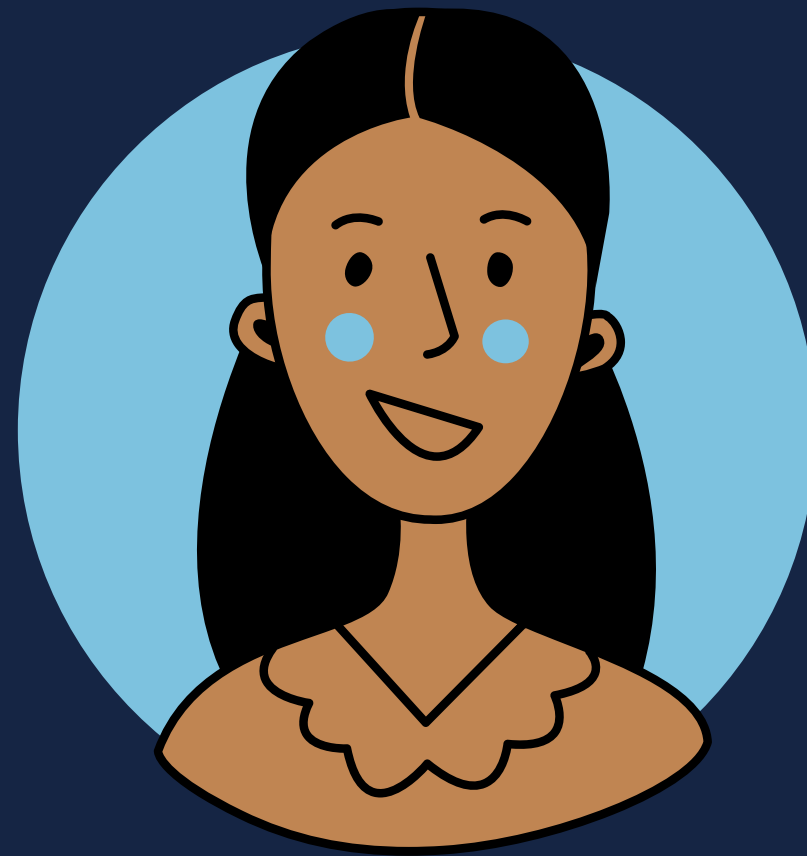
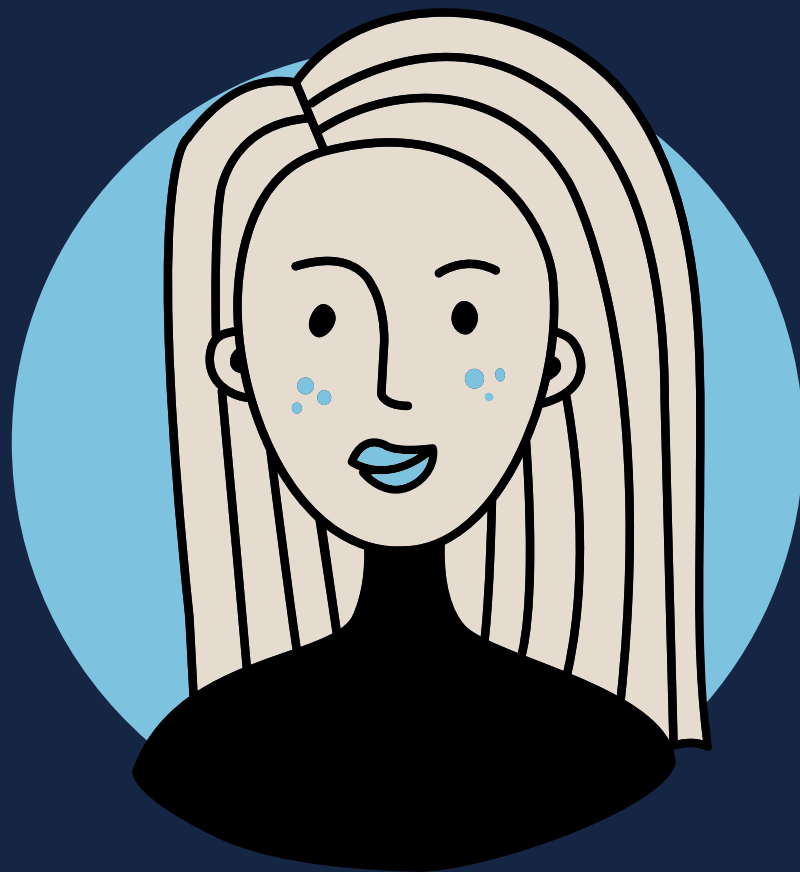
“I don’t think we
need to. You
convinced me”



“Pair ET with
other testers.”
“Think about the
end-user.”



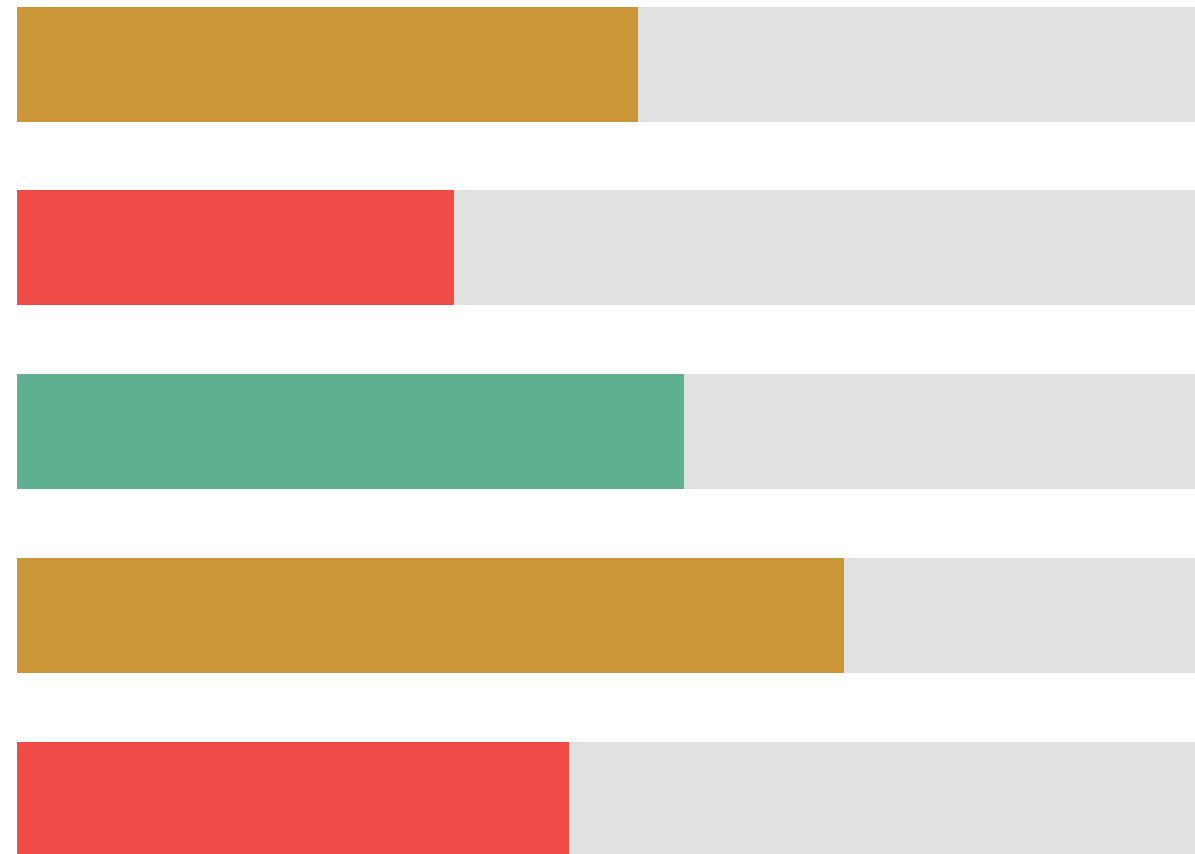
Exploratoire



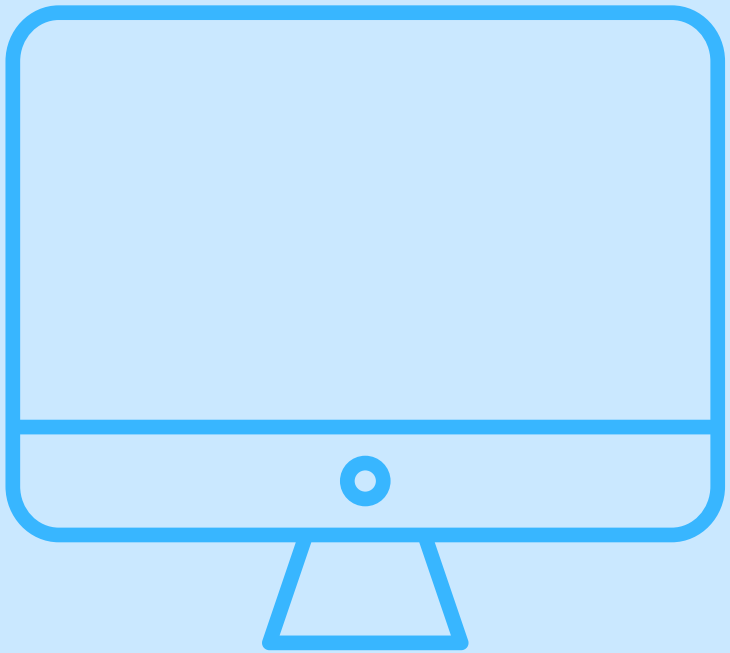


Aller encore
plus loin...

Monitoring



API REST



Client



Serveur

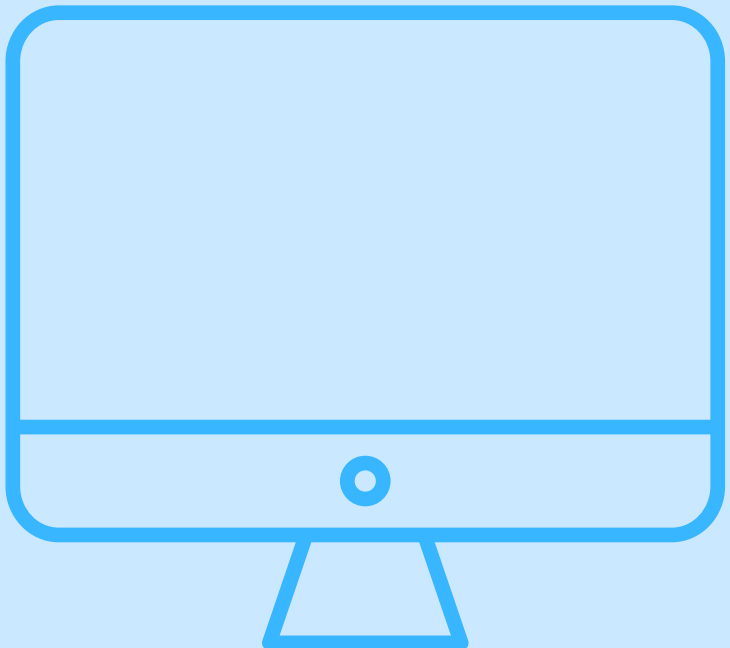


4XX

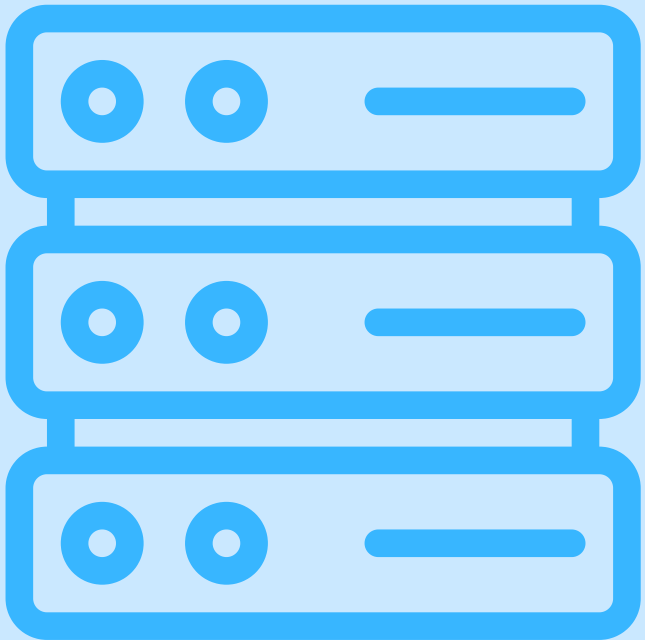
Erreur client

Status code

API REST



Client



Serveur



Status code



5XX
Erreur serveur

Monitoring



Alerting

+ Quid des environnements de tests

Sécurité

OWASP API Security - Top 10



Broken Level Authorization :

1
3
5

Object

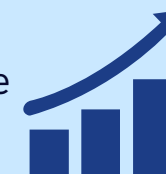
Object property

Function



4

Unrestricted Resource Consumption



7

Server Side Request Forgery



9

Improper Inventory Management



10

Unsafe Consumption of APIs



2

Broken Authentication



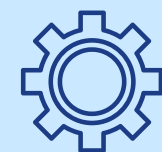
6

Unrestricted Access to Sensitive Business Flows



8

Security Misconfiguration



Plus d'info sur GitHub



Sécurité



Zoom - Broken Level Authorization :



Facteurs de menace / Vecteurs d'attaque	Faible de sécurité	Impact
Spécifique à l'API : Exploitabilité Facile	Prévalence Répondue : Détection Facile	Technique Modérée : Spécifique à l'organisation

Scénario #1

Une plateforme de e-commerce pour des magasins en ligne fournit une page avec les graphiques des revenus que le magasin a généré. En inspectant les requêtes du navigateur, un attaquant peut identifier les points d'accès de l'API utilisés comme source de données pour ces graphiques et leur modèle :

`/shops/{shopName}/revenue_data.json` . En utilisant un autre point d'accès de l'API, l'attaquant peut obtenir la liste de tous les noms de magasins hébergés. Avec un simple script pour manipuler les noms de la liste, en remplaçant `{shopName}` dans l'URL, l'attaquant obtient accès aux données de vente de milliers de magasins de e-commerce.

Sécurité



```
✗ Unit tests (in 4 s 802 ms)

  ✓ 9 passed ✗ 1 failed

===== FAILURES =====
----- POST /improper-input-type-handling -----
1. Test Case ID: gsi2Jl

- Server error

[500] Internal Server Error:

  `{"success":false,"error":"invalid literal for int() with base 10: 'á'"}`

Reproduce with:

  curl -X POST -H 'Content-Type: application/json' -d '{"number": "\u00e1"}' https://example.schem
  atesis.io/improper-input-type-handling

===== SUMMARY =====

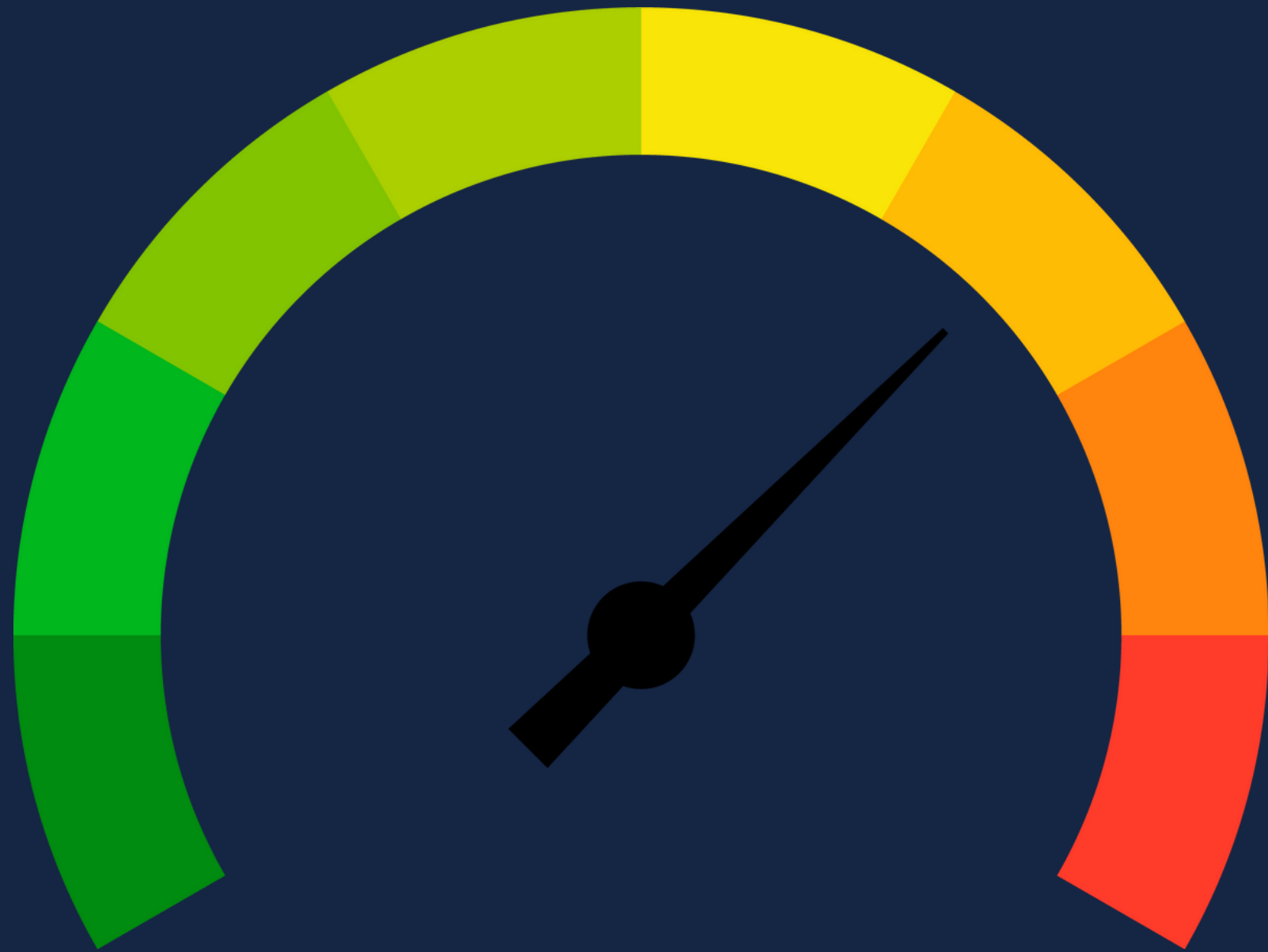
API Operations:
  Selected: 10/10
  Tested: 10

Failures:
  ✗ Server error: 1

Test cases:
  33 generated, 1 found 1 unique failure
  Unsafe Consumption of APIs

===== 1 failure in 4.93s =====
```

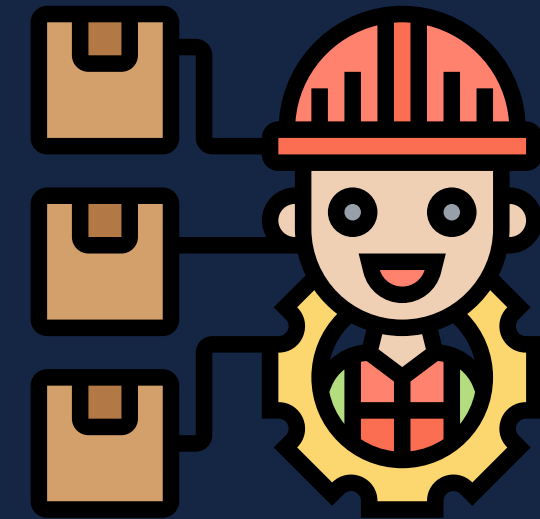
Performance



Contract



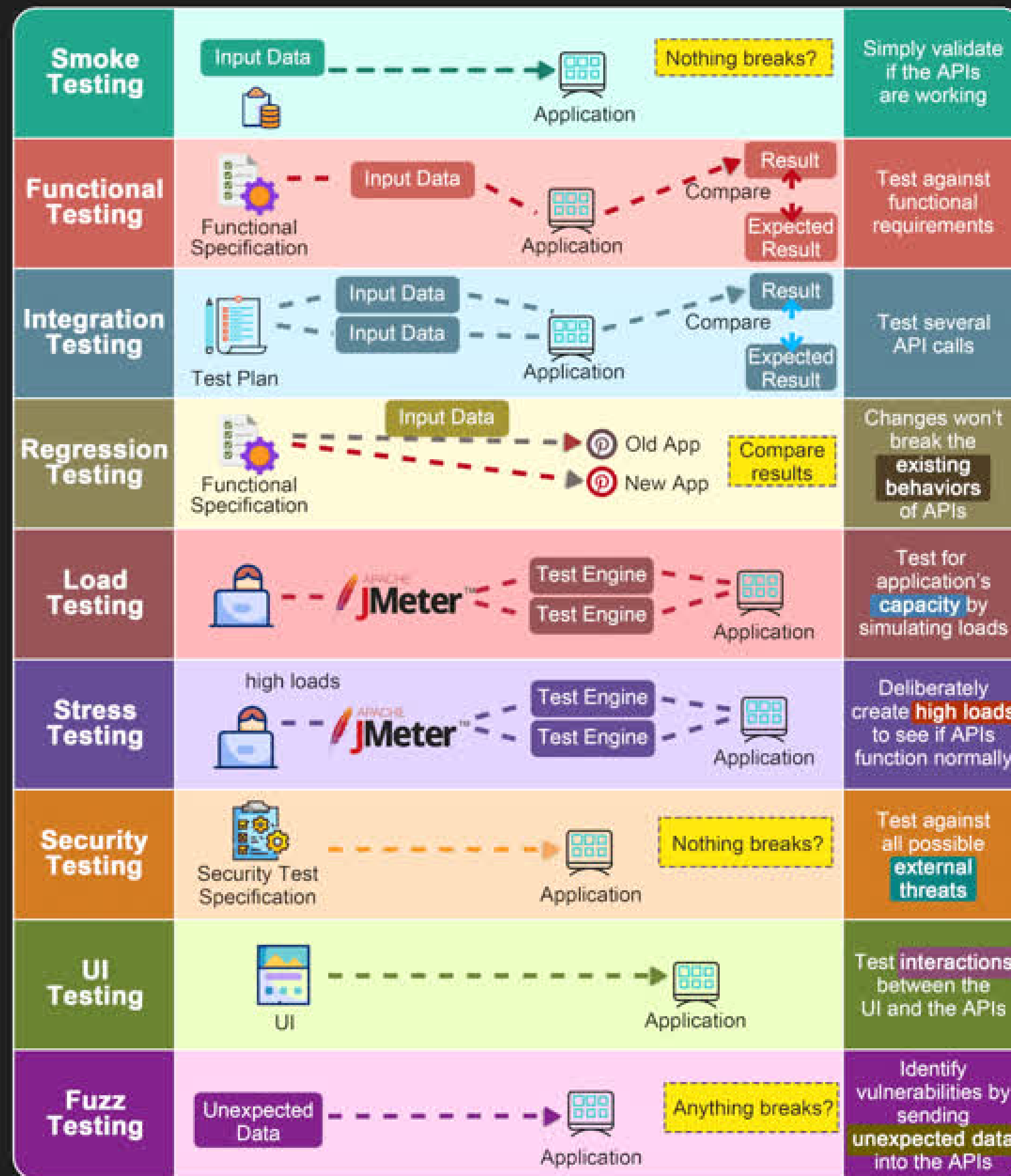
Consommateur
Consumer



Fournisseur
Provider

9 Types API Testing

blog.bytebytego.com



9 catégories de tests pour les API

Démystifier les 9 catégories de tests API : Un guide complet

Medium / Oct 30, 2023

Tester une API

Participer à la conception

Lire la documentation

Tester les requêtes



Pour aller plus loin :

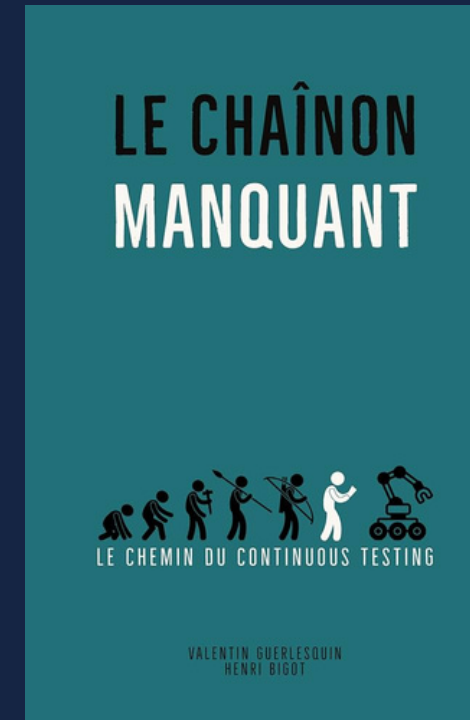
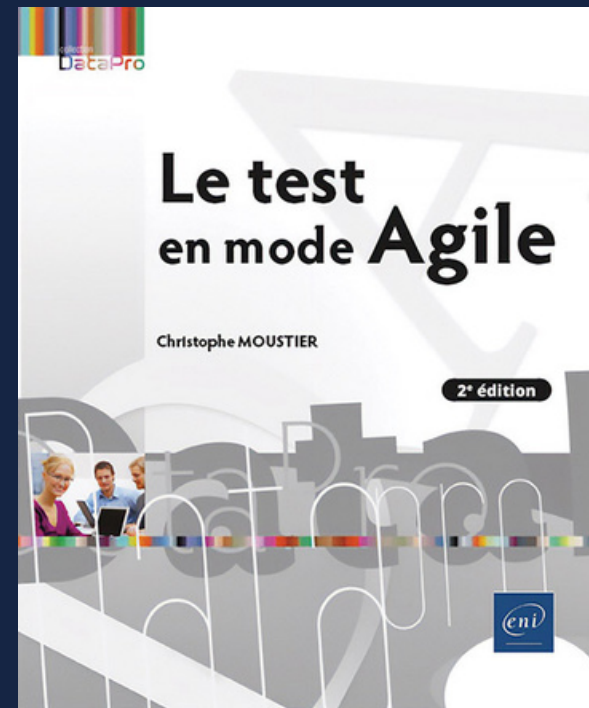
- Monitoring & alerting
- Attaquer l'API
- Contrôler les performances
- Tester les contrats

Les APIs sont partout !

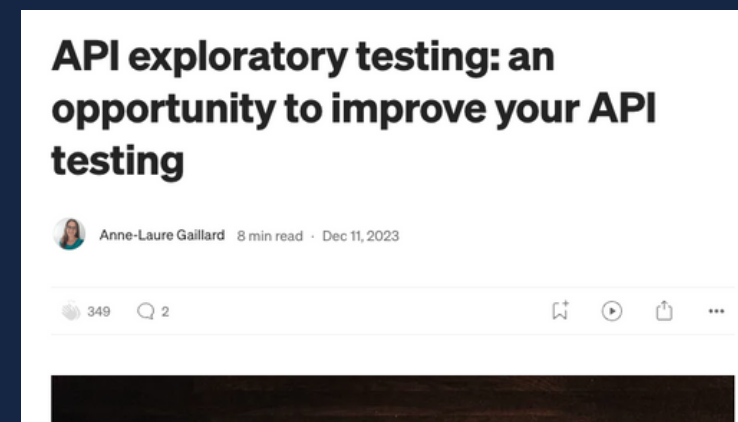
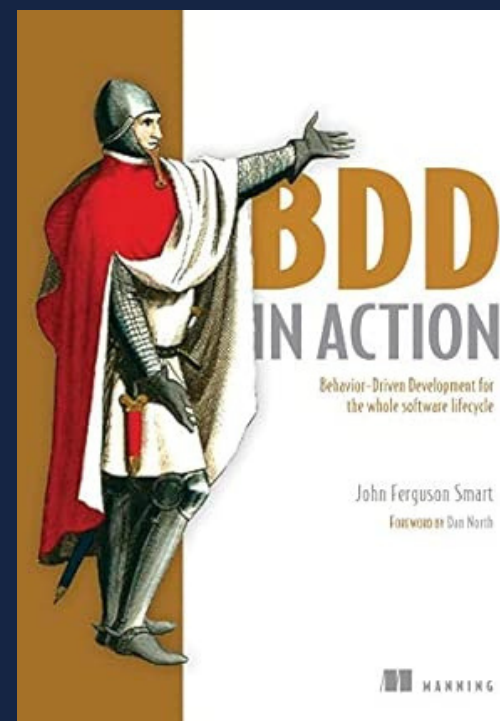
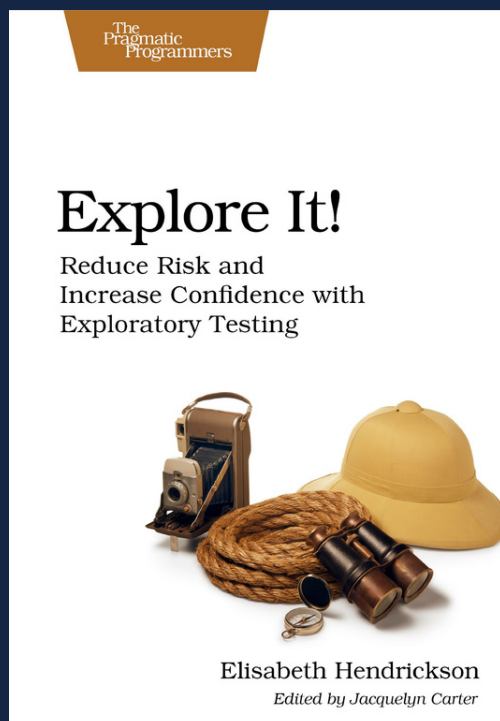
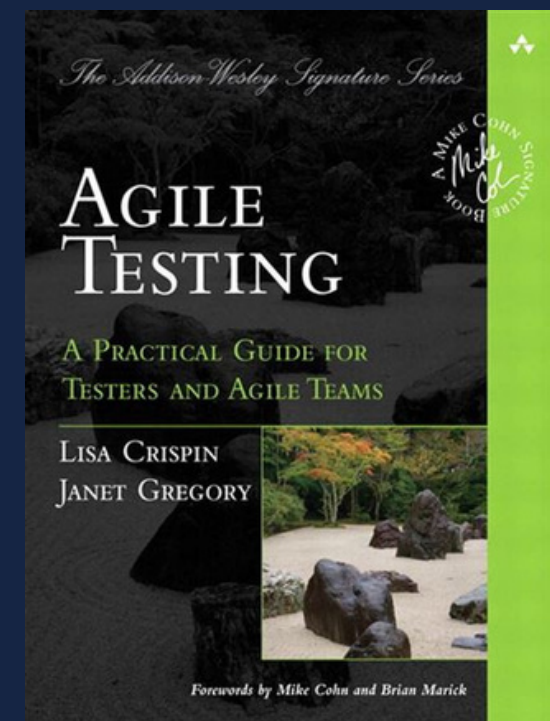
Vous êtes capables de les tester

Merci

Quelques références



<https://www.youtube.com/watch?v=FPrMPOlqZN4>



<https://medium.com/manomano-tech/api-exploratory-testing-an-opportunity-to-improve-your-api-testing-d18e125f244d>