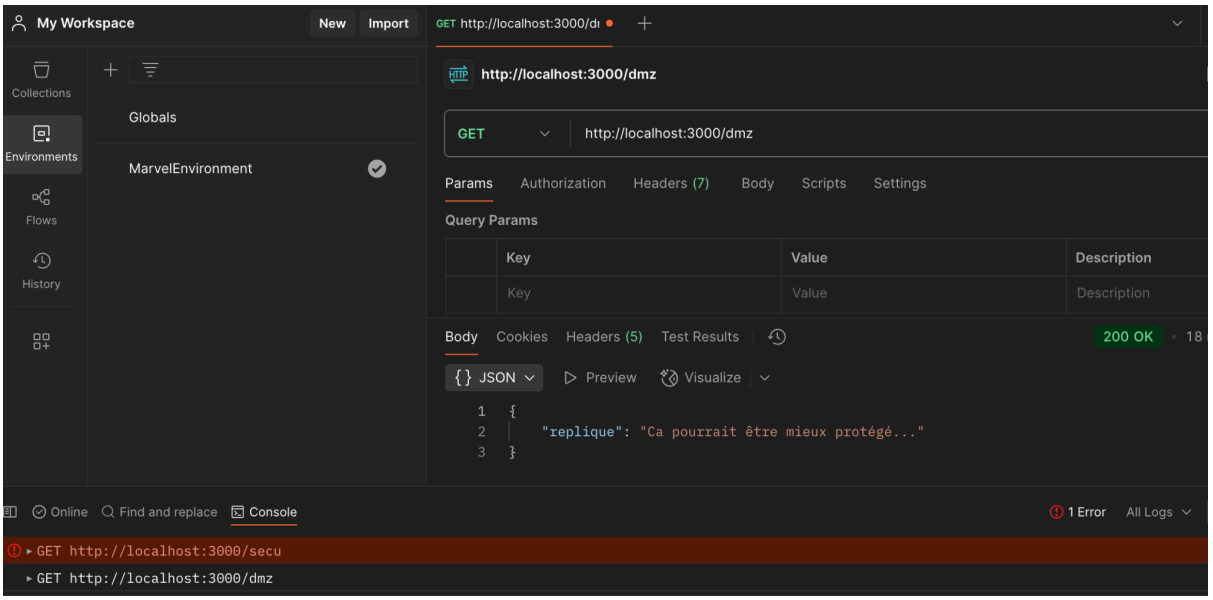
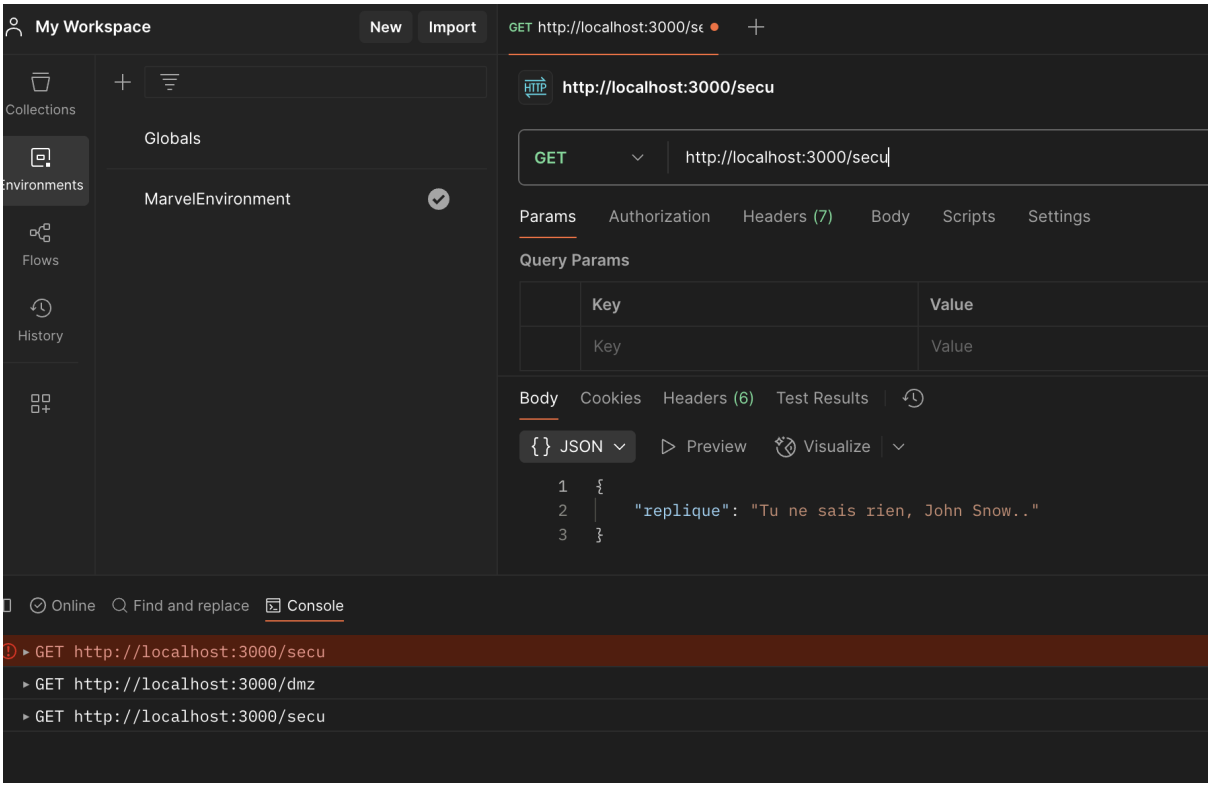
Rapport TP4 - Développement avancé

Louis Prigneaux

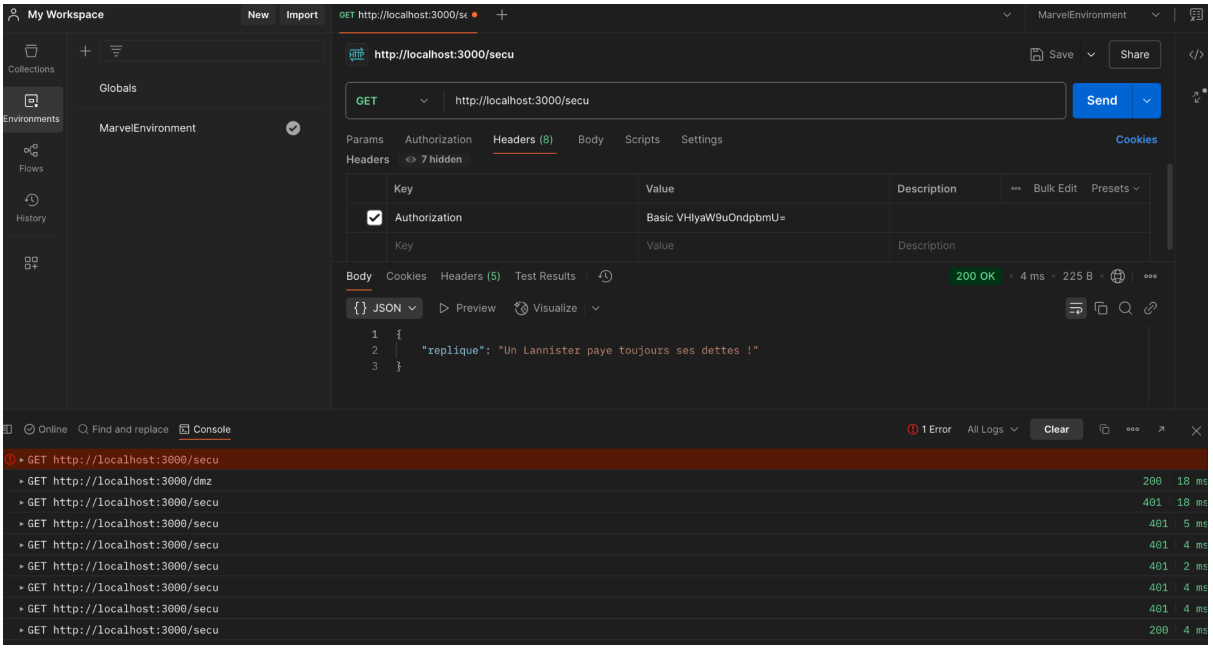
Etape 1 :

- Clone du projet
- Tests avec Postman :





- Clé en Base64 de “Tyrion:wine” = “VHlyaW9uOndpbmU=”
- Test avec la clé Authorization dans le header

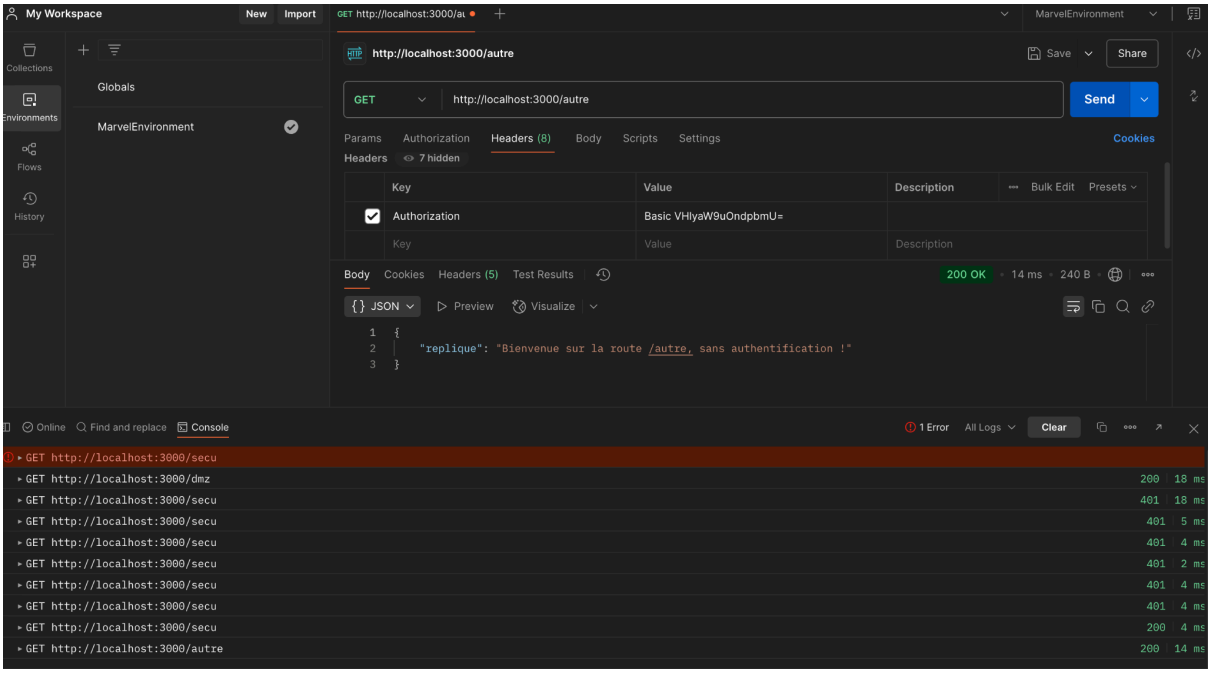


- *Rôle de after() :*
  S'assurer que le plugin @fastify/basic-auth est bien enregistré avant de déclarer la route /secu.
  Cela garantit que la méthode fastify.basicAuth est disponible pour sécuriser la route /secu.

  Eviter les erreurs liées à l’ordre d’enregistrement des plugins et des routes.
  Si la route /secu était déclarée avant l'enregistrement du plugin @fastify/basic-auth, cela provoquerait une erreur.

  Organiser le code :
  after() est utile pour regrouper les déclarations de routes qui dépendent des plugins précédemment enregistrés.

- Développement de la fonction pour accéder à /autre :



Etape 2 :

- Générer une clé privée de 2048 bits

openssl genrsa -out server.key 2048

- Créer une requête de signature de certificat (CSR)

openssl req -new -key server.key -out server.csr

- Générer le certificat autosigné

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

```
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu1 % openssl genrsa -out server.key 2048
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu1 % openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu1 % openssl x509 -req -days 365 -in server.csr -signkey server.key -out s
erver.crt
Certificate request self-signature ok
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
```

- Utilisez la commande suivante pour tester le certificat généré :

openssl s_server -accept 4567 -cert server.crt -key server.key -www -state

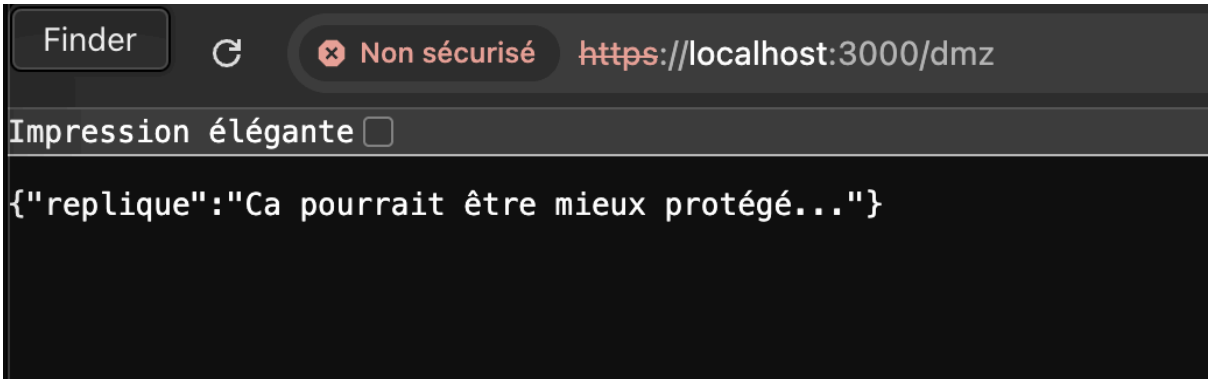
```
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu1 % openssl s_server -accept 4567 -cert server.crt -key server.key -www -
state
Using default temp DH parameters
ACCEPT
```

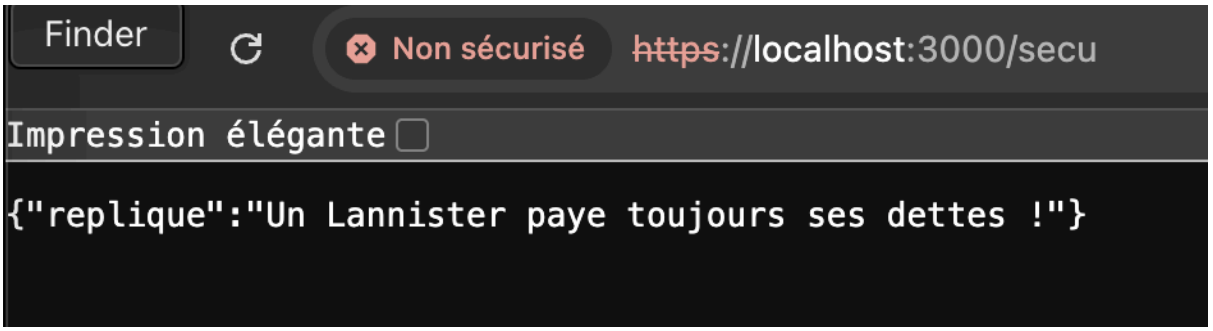
- Amélioration du server.js pour prendre en compte les certificat :

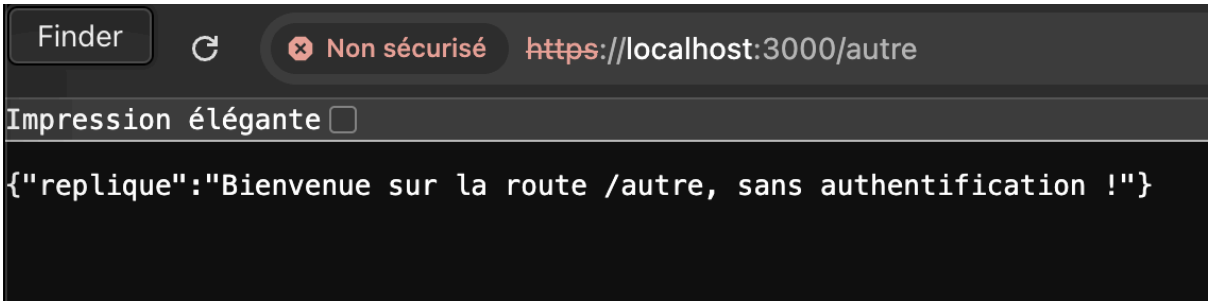
```
// Lecture des clés et du certificat
const httpsOptions = {
 key: readFileSync('./server.key'),
 cert: readFileSync('./server.crt')
};

// Création de l'instance Fastify en HTTPS
const fastify = Fastify({
 logger: true,
 https: httpsOptions
});
```

- Tests des https :







ETAPE 3 :

1.

- générer une clé privée et une clé publique compatibles avec **ES256**.

```
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu-ETAPE3_1 % openssl ecparam -genkey -name prime256v1 -noout -out .ssl/private.key
(base) louis@MacBook-Pro-de-Louis R6.A.05-TP-Secu-ETAPE3_1 % openssl ec -in .ssl/private.key -pubout -out .ssl/public.key
read EC key
writing EC key
```

- Création de login.js, data.js pour gérer l’accès au site.