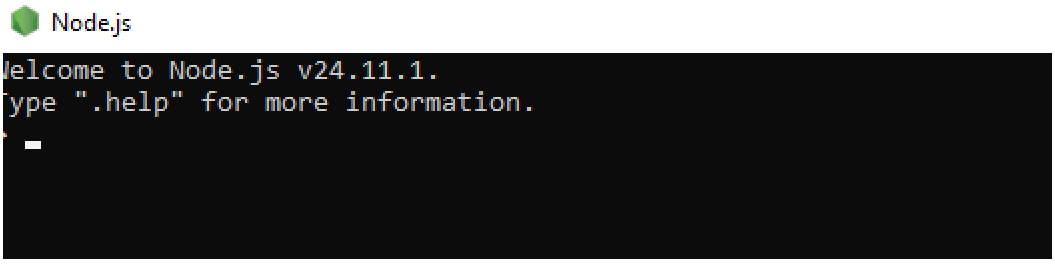
# INJECTION SQL

1- Téléchargement de Node.js



```
Welcome to Node.js v24.11.1.
Type ".help" for more information.
>
```

2- Activation de WAMP parce que mon Docker ne marche pas

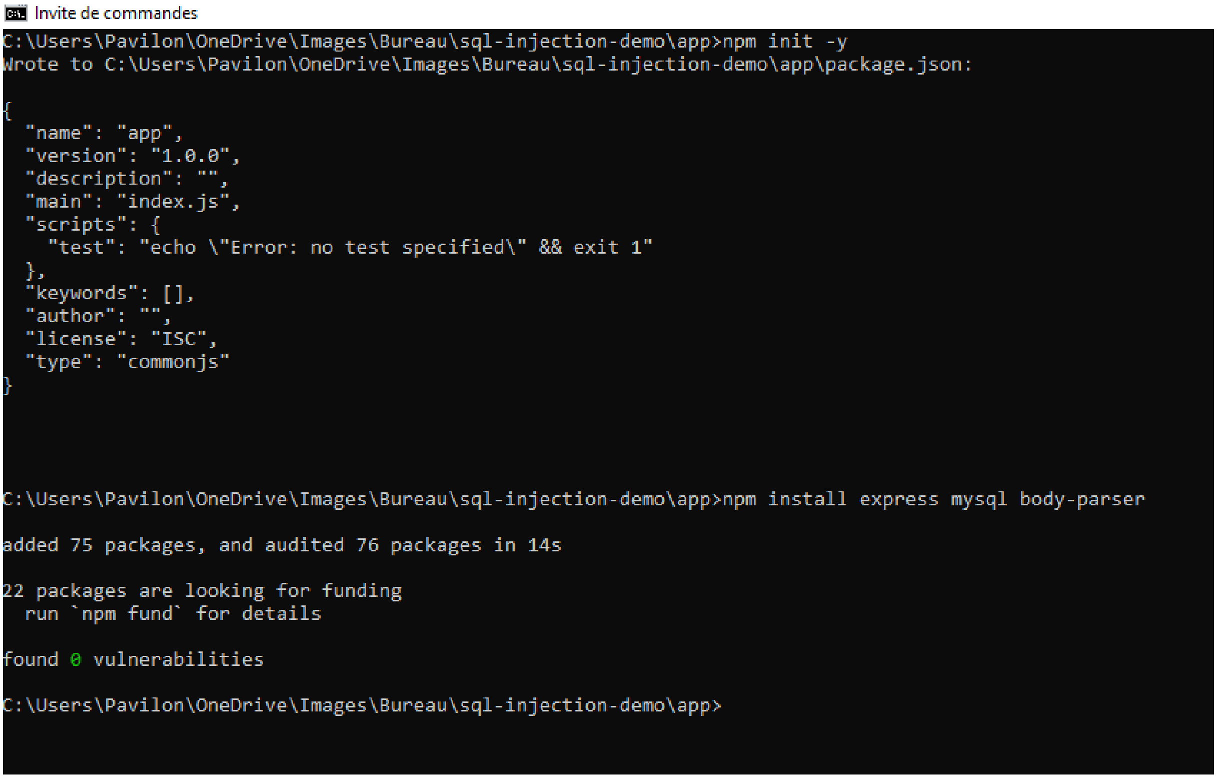
## Étape 1 : Créer la base de données (via WAMP)

3- Création de la base `login_db`, la table `users` et ajoute l'utilisateur `testuser`.

```
CREATE DATABASE login_db;
USE login_db;

CREATE TABLE users (
  id INT AUTO_INCREMENT PRIMARY KEY,
  username VARCHAR(255) NOT NULL,
  password VARCHAR(255) NOT NULL
);

INSERT INTO users (username, password) VALUES ('testuser', 'password123');
```

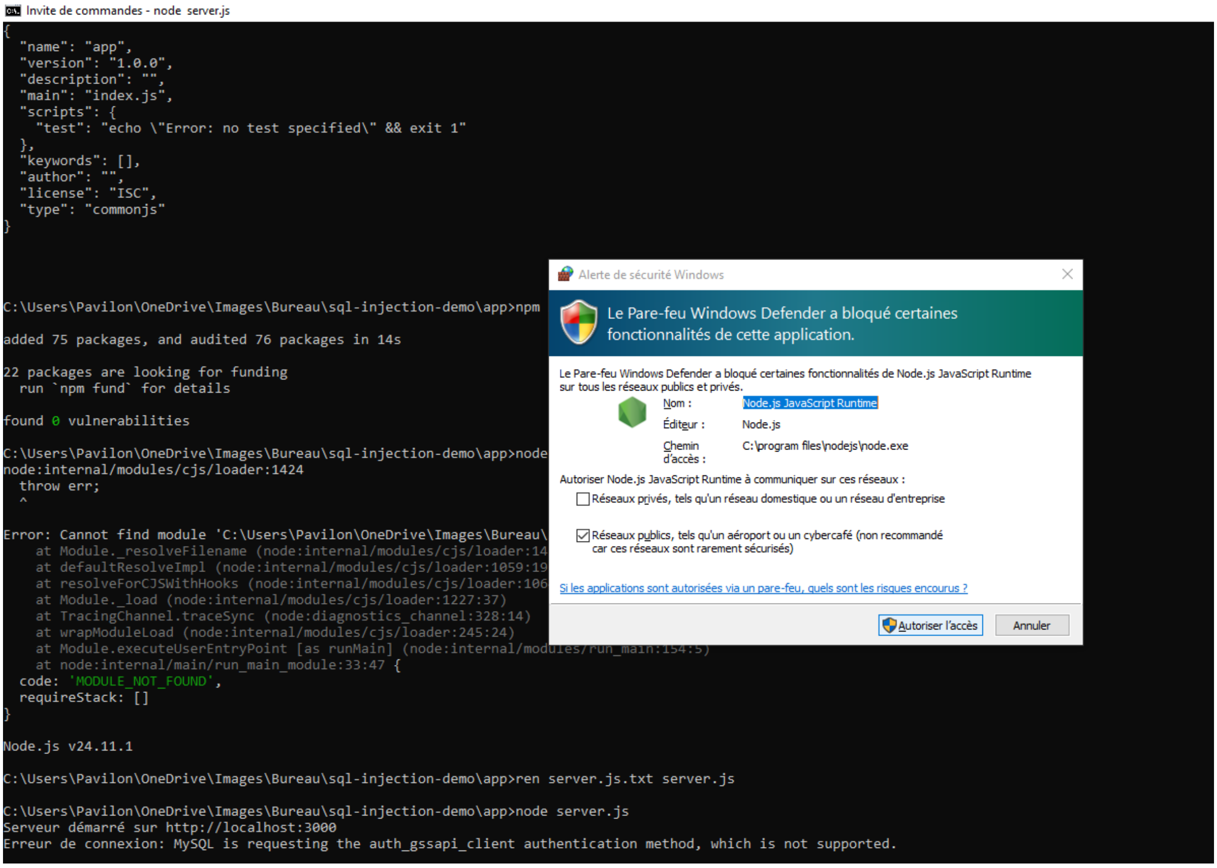
## Étape 2 : Créer le dossier du projet

Création de mon dossier sql-injection-demo sur le bureau et du sous-dossier app.



Invite de commandes

```
C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>npm init -y
Wrote to C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app\package.json:

{
  "name": "app",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "type": "commonjs"
}



C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>npm install express mysql body-parser

added 75 packages, and audited 76 packages in 14s

22 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>
```



Invite de commandes - node  server.js

```
{
  "name": "app",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "type": "commonjs"
}



C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>npm

added 75 packages, and audited 76 packages in 14s

22 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>node
node:internal/modules/cjs/loader:1424
  throw err;
  ^

Error: Cannot find module 'C:\Users\Pavilon\OneDrive\Images\Bureau\
    at Module._resolveFilename (node:internal/modules/cjs/loader:14
    at defaultResolveImpl (node:internal/modules/cjs/loader:1059:19
    at resolveForCJSWithHooks (node:internal/modules/cjs/loader:106
    at Module._load (node:internal/modules/cjs/loader:1227:37)
    at TracingChannel.traceSync (node:diagnostics_channel:328:14)
    at wrapModuleLoad (node:internal/modules/cjs/loader:245:24)
    at Module.executeUserEntryPoint [as runMain] (node:internal/modules/run_main:154:5)
    at node:internal/main/run_main_module:33:47 {
  code: 'MODULE_NOT_FOUND',
  requireStack: []
}

Node.js v24.11.1

C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>ren server.js.txt server.js

C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>node server.js
Serveur démarré sur http://localhost:3000
Erreur de connexion: MySQL is requesting the auth_gssapi_client authentication method, which is not supported.
```

Alerte de sécurité Windows

Le Pare-feu Windows Defender a bloqué certaines fonctionnalités de cette application.

Le Pare-feu Windows Defender a bloqué certaines fonctionnalités de Node.js JavaScript Runtime sur tous les réseaux publics et privés.

Nom : Node.js JavaScript Runtime

Éditeur : Node.js

Chemin d'accès : C:\program files\nodejs\node.exe

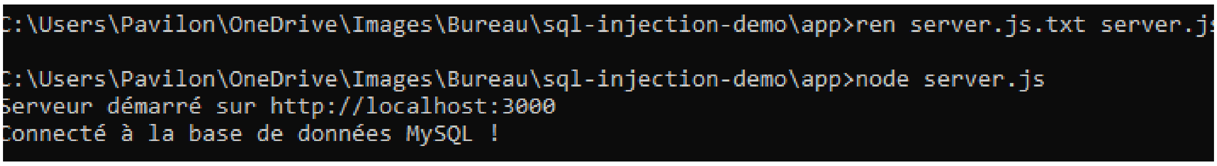
Autoriser Node.js JavaScript Runtime à communiquer sur ces réseaux :

☐ Réseaux privés, tels qu'un réseau domestique ou un réseau d'entreprise

☑ Réseaux publics, tels qu'un aéroport ou un cybercafé (non recommandé car ces réseaux sont rarement sécurisés)

Si les applications sont autorisées via un pare-feu, quels sont les risques encourus ?

**"Serveur démarré sur http://localhost:3000"  "Connecté à la base de données MySQL !"**

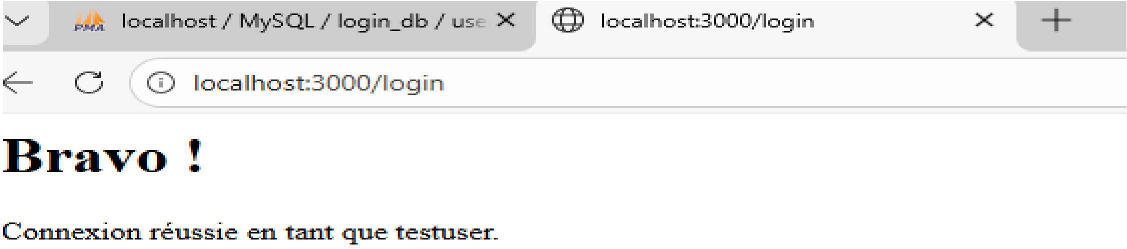


```
:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>ren server.js.txt server.j

:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>node server.js
erveur démarré sur http://localhost:3000
onnecté à la base de données MySQL !
```

## Étape 3: Pirater mon propre site (La démonstration)

### L'attaque :

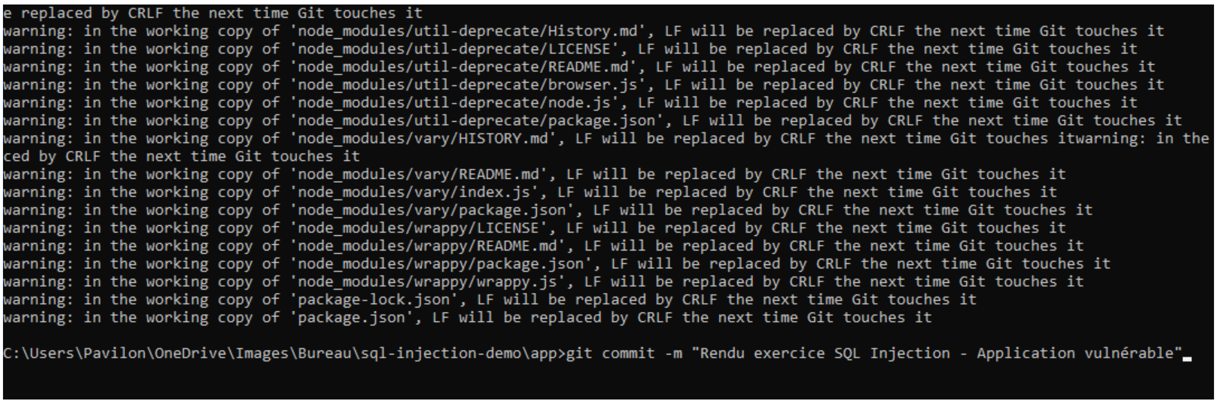
- **Nom d'utilisateur :** testuser' OR '1'='1
- **Mot de passe :** 253115 (j'entre n'importe quel mot de passe)



# Bravo !

Connexion réussie en tant que testuser.

## COMPTE RENDU DE A VULNÉRABILITÉ



```
e replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/History.md', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/LICENSE', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/README.md', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/browser.js', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/node.js', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/util-deprecate/package.json', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/vary/HISTORY.md', LF will be replaced by CRLF the next time Git touches itwarning: in the
ced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/vary/README.md', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/vary/index.js', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/vary/package.json', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/wrappy/LICENSE', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/wrappy/README.md', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/wrappy/package.json', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'node_modules/wrappy/wrappy.js', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'package-lock.json', LF will be replaced by CRLF the next time Git touches it
warning: in the working copy of 'package.json', LF will be replaced by CRLF the next time Git touches it

C:\Users\Pavilon\OneDrive\Images\Bureau\sql-injection-demo\app>git commit -m "Rendu exercice SQL Injection - Application vulnérable"
```