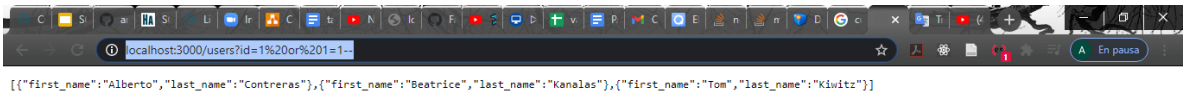
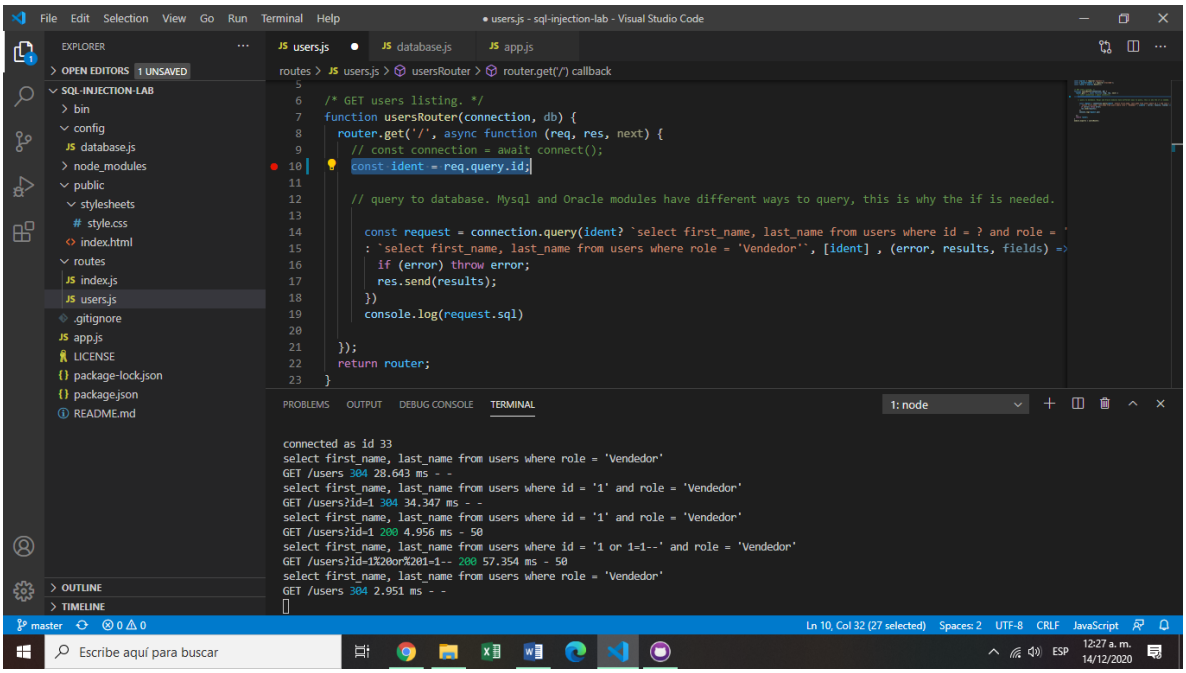
Laboratorio de inyeccion SQL

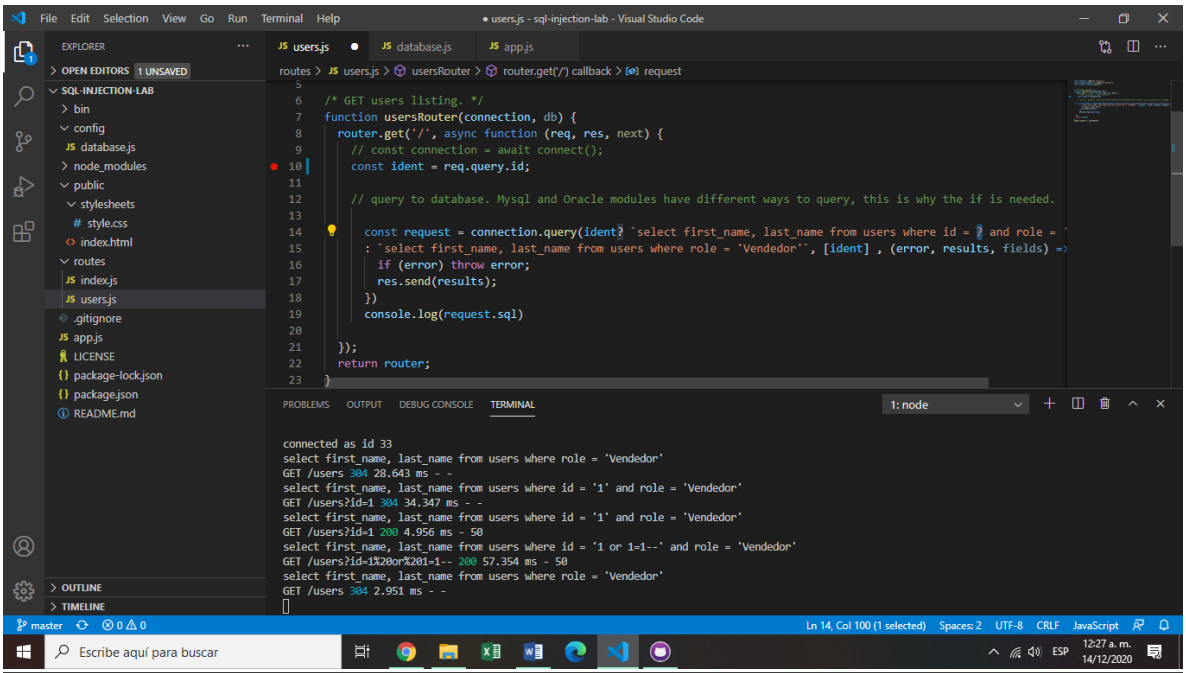
Por ANDRES DARIO HIGUITA PEREZ CC:1022099411

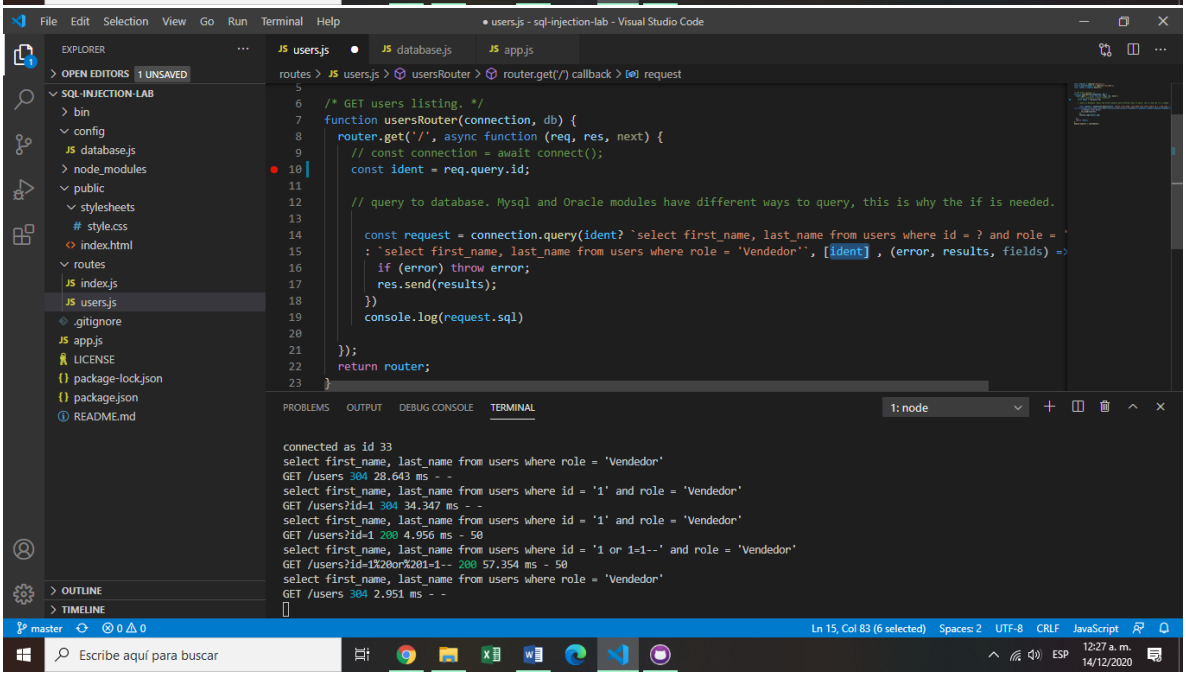
Para lograr que se vieran todos los usuarios del sistema incluyendo a todos aquellos que tengan un rol diferente a VENDEDOR solo coloque después de ‘ ? ’ id=1 or 1 =1- - con esto anule la condición de que solo aparecieran vendedores, dando lugar a que aparezcan los demás:



Para evitar esta inyección SQL realice una sencilla parametrización con la cual se puede evitar que un usuario pueda acceder a la concatenación de string.


File Edit Selection View Go Run Terminal Help
• users.js - sql-injection-lab - Visual Studio Code
EXPLORER
OPEN EDITORS 1 UNSAVED
SQL-INJECTION-LAB
bin
config
database.js
node_modules
public
stylesheets
style.css
index.html
routes
index.js
users.js
.gitignore
app.js
LICENSE
package-lock.json
package.json
README.md
OUTLINE
TIMELINE
users.js
database.js
app.js
routes > users.js > usersRouter > router.get('/') callback
/* GET users listing. */
function usersRouter(connection, db) {
router.get('/', async function (req, res, next) {
// const connection = await connect();
const ident = req.query.id;
// query to database. Mysql and Oracle modules have different ways to query, this is why the if is needed.
const request = connection.query(ident? `select first_name, last_name from users where id = ? and role =
: `select first_name, last_name from users where role = 'Vendedor'`, [ident] , (error, results, fields) =>
if (error) throw error;
res.send(results);
})
console.log(request.sql)
});
return router;
}
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: node
connected as id 33
select first_name, last_name from users where role = 'Vendedor'
GET /users 304 28.643 ms - -
select first_name, last_name from users where id = '1' and role = 'Vendedor'
GET /users?id=1 304 34.347 ms - -
select first_name, last_name from users where id = '1' and role = 'Vendedor'
GET /users?id=1 200 4.956 ms - 50
select first_name, last_name from users where id = '1 or 1=1--' and role = 'Vendedor'
GET /users?id=1%20or%201=1-- 200 57.354 ms - 50
select first_name, last_name from users where role = 'Vendedor'
GET /users 304 2.951 ms - -
master
0 0
Ln 10, Col 32 (27 selected) Spaces: 2 UTF-8 CRLF JavaScript
Escribe aquí para buscar
ESP
12:27 a. m.
14/12/2020





Al realizer la inyeccion ya no aparecen todos los datos

[{"first_name":"Alberto","last_name":"Contreras"}]