const express = require('express');

const bodyParser = require('body-parser');

const app = express();

const port = 3000;

app.use(bodyParser.urlencoded({ extended: true }));

// Route to handle form submission

app.post('/login', (req, res) => {

const username = req.body.username;

const password = req.body.password;

// Simulated vulnerable database query with SQL injection vulnerability

const query = `SELECT \* FROM users WHERE username='${username}' AND password='${password}'`;

db.query(query, (err, result) => {

if (err) {

console.error(err);

return res.status(500).send('Internal Server Error');

}

// Assuming 'result' contains the user data if found

if (result.length > 0) {

// Redirect to profile page upon successful login

res.redirect('/profile');

} else {

// Handle invalid credentials

res.send('Invalid username or password');

}

});

});

// Route to display profile page

app.get('/profile', (req, res) => {

res.send('Welcome to your profile page!');

});

app.listen(port, () => {

console.log(`Server is listening at http://localhost:${port}`);

});