Estácio - Mundo 5 - Missão Nível 5

Faculdade Estácio - Polo Itaipava - Petrópolis/RJ.
Curso: Desenvolvimento Full Stack.
Disciplina: Nível 5: Software sem segurança não serve
Semestre Letivo: 5.

Integrante: Jeferson Jones Smith da Rocha.
Repositório: https://github.com/JefersonSmith/estacio-mundo5-nivel5

Missão Prática / Software sem segurança não serve

Através dessa atividade o aluno analisará uma falha de segurança, em uma aplicação web, e aplicará as medidas corretivas necessárias para garantir o seu correto e seguro funcionamento

Roteiro de prática

- Material necessário para a prática

- Editor ou IDE para escrita de códigos-fonte.

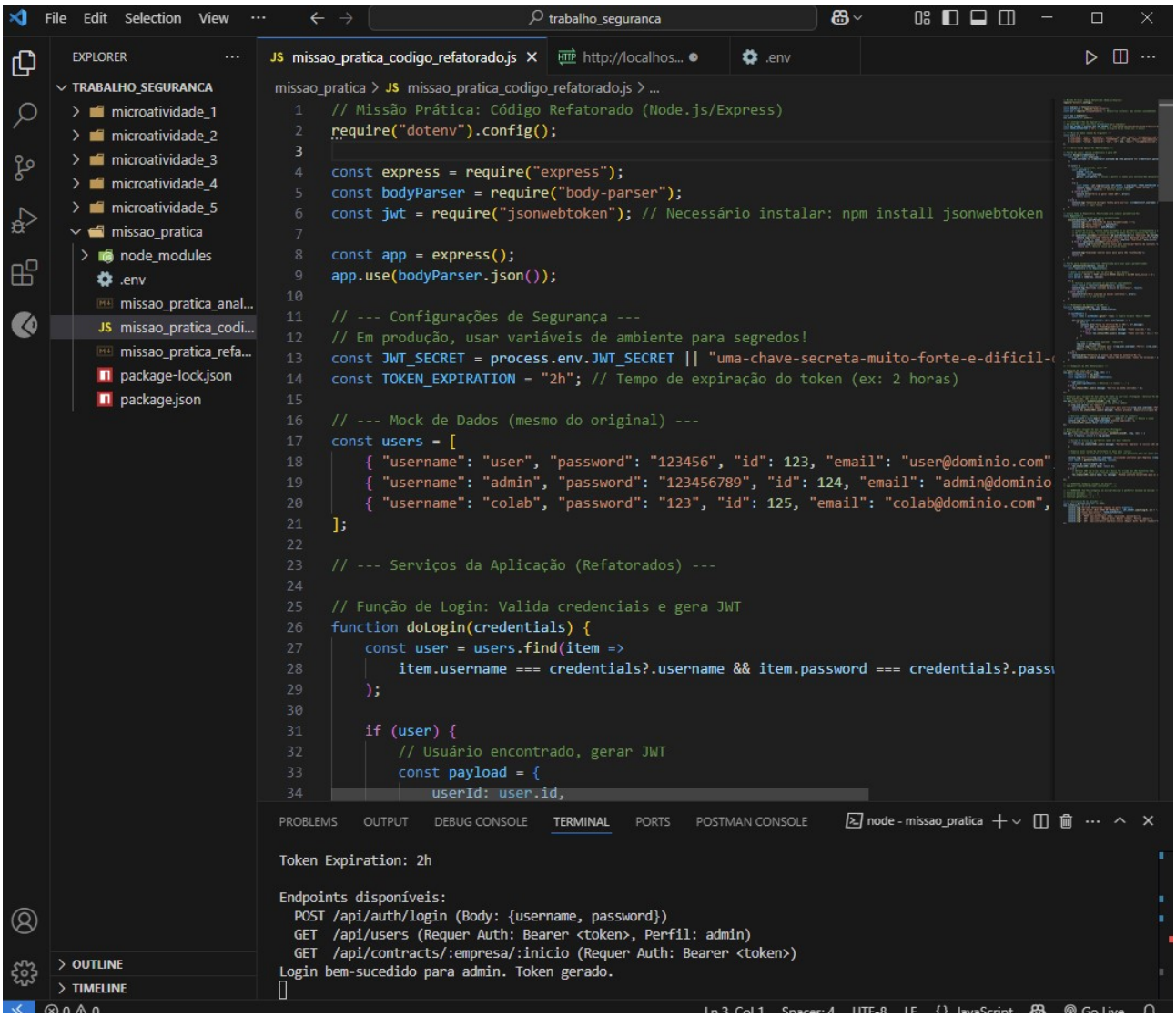
- Procedimentos

1. Abra o código-fonte fornecido acima na IDE ou editor;
3. “session-id” por um outro mecanismo de segurança, como tokens JWT;
5. “session-id”) não seja trafegado via URI, mas através do header da requisição;
7. identidade do usuário, data/hora de expiração do mesmo, etc.;
10. acessados apenas por usuários com perfil ‘admin’;
13. de acesso limitado ao perfil ‘admin’;
17. que garanta o sucesso do processo em questão;
18. Salve o código e coloque a API para ser executada;
20. testes na API, garantindo que todos os pontos acima foram tratados.

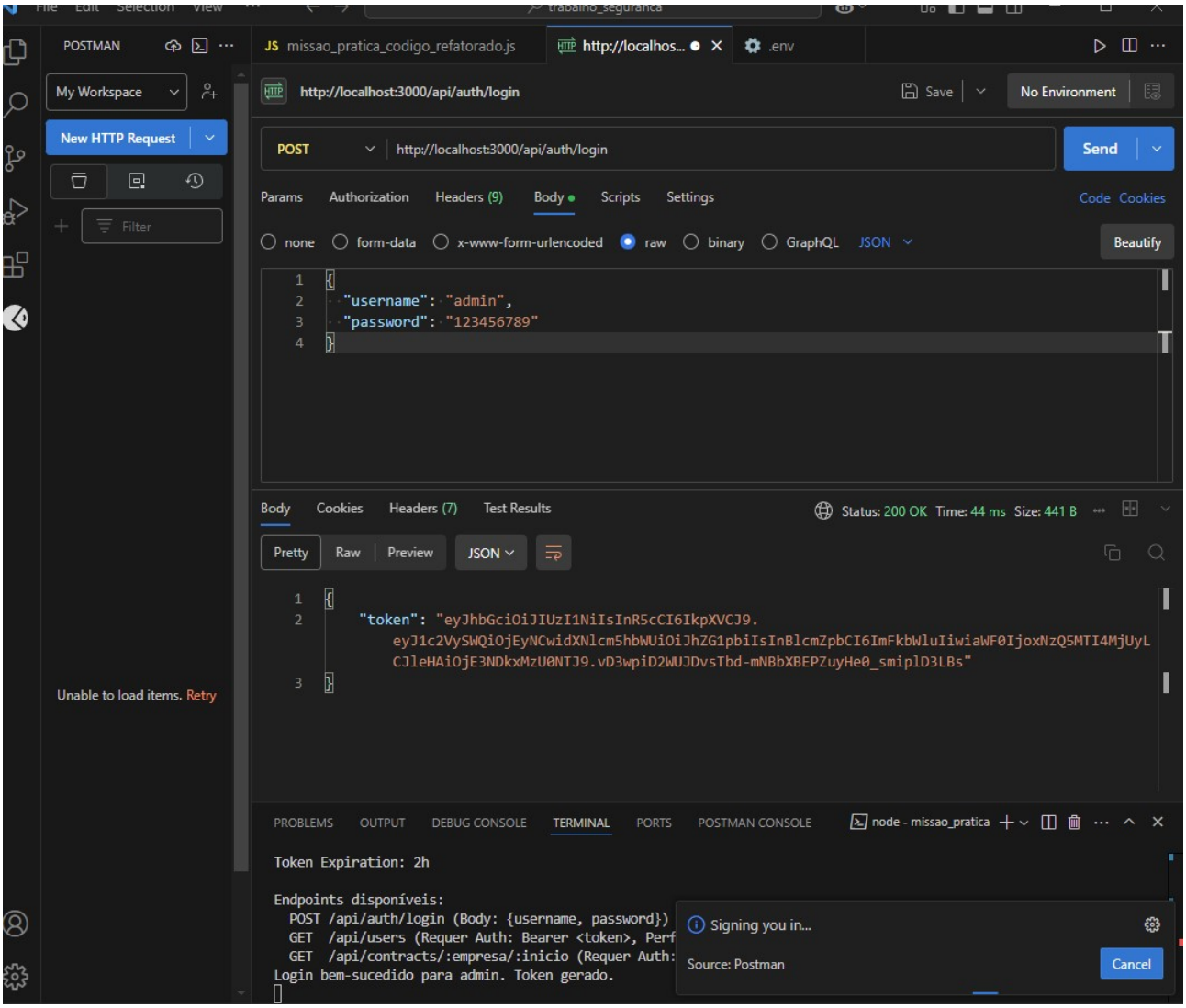
- Resultados esperados ✨

fornecida, aplicando medidas e boas práticas recomendadas na literatura relacionada.

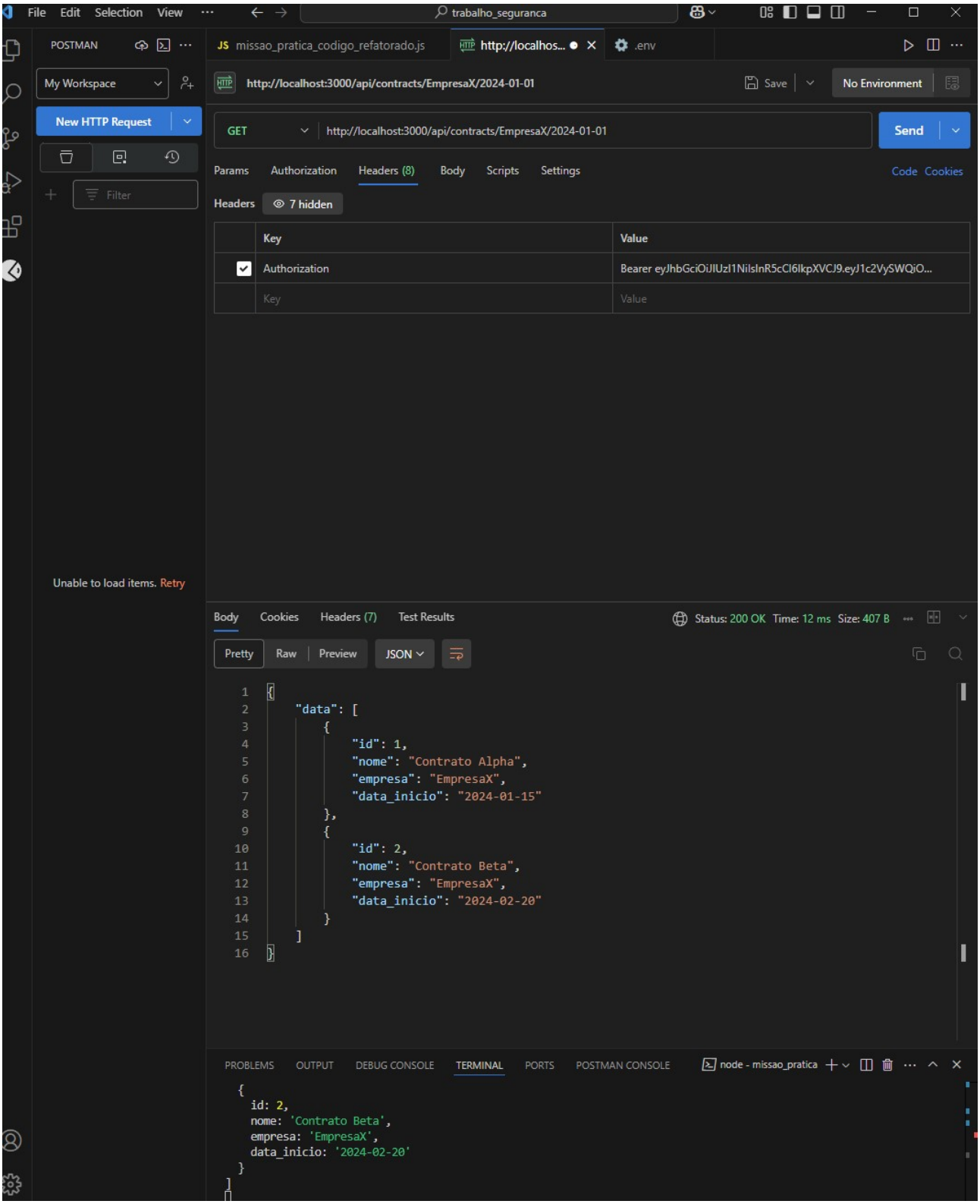
Código


File Edit Selection View
trabalho_seguranca
EXPLORER
TRABALHO_SEGURANCA
microatividade_1
microatividade_2
microatividade_3
microatividade_4
microatividade_5
missao_pratica
node_modules
.env
missao_pratica_anal...
missao_pratica_codi...
missao_pratica_refa...
package-lock.json
package.json
OUTLINE
TIMELINE
missao_pratica_codigo_refatorado.js
http://localhos...
.env
missao_pratica > missao_pratica_codigo_refatorado.js > ...
1 // Missão Prática: Código Refatorado (Node.js/Express)
2 require("dotenv").config();
3
4 const express = require("express");
5 const bodyParser = require("body-parser");
6 const jwt = require("jsonwebtoken"); // Necessário instalar: npm install jsonwebtoken
7
8 const app = express();
9 app.use(bodyParser.json());
10
11 // --- Configurações de Segurança ---
12 // Em produção, usar variáveis de ambiente para segredos!
13 const JWT_SECRET = process.env.JWT_SECRET || "uma-chave-secreta-muito-forte-e-dificil-
14 const TOKEN_EXPIRATION = "2h"; // Tempo de expiração do token (ex: 2 horas)
15
16 // --- Mock de Dados (mesmo do original) ---
17 const users = [
18 { "username": "user", "password": "123456", "id": 123, "email": "user@dominio.com"
19 { "username": "admin", "password": "123456789", "id": 124, "email": "admin@dominio
20 { "username": "colab", "password": "123", "id": 125, "email": "colab@dominio.com",
21];
22
23 // --- Serviços da Aplicação (Refatorados) ---
24
25 // Função de Login: Valida credenciais e gera JWT
26 function doLogin(credentials) {
27 const user = users.find(item =>
28 item.username === credentials?.username && item.password === credentials?.pass
29);
30
31 if (user) {
32 // Usuário encontrado, gerar JWT
33 const payload = {
34 userId: user.id,
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS POSTMAN CONSOLE
node - missao_pratica
Token Expiration: 2h
Endpoints disponíveis:
POST /api/auth/login (Body: {username, password})
GET /api/users (Requer Auth: Bearer <token>, Perfil: admin)
GET /api/contracts/:empresa/:inicio (Requer Auth: Bearer <token>)
Login bem-sucedido para admin. Token gerado.

Login


POSTMAN
My Workspace
New HTTP Request
Filter
Unable to load items. Retry
missao_pratica_codigo_refatorado.js
http://localhos...
.env
http://localhost:3000/api/auth/login
Save
No Environment
POST
http://localhost:3000/api/auth/login
Send
Params
Authorization
Headers (9)
Body
Scripts
Settings
Code
Cookies
none
form-data
x-www-form-urlencoded
raw
binary
GraphQL
JSON
Beautify
{
"username": "admin",
"password": "123456789"
}
Body
Cookies
Headers (7)
Test Results
Status: 200 OK
Time: 44 ms
Size: 441 B
Pretty
Raw
Preview
JSON
{
"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJ1c2VySWQiOjEyNCwidXNlcm5hbWUiOiJhZG1pbiIsInBlcmZpbCI6ImFkbWluIiwiaWF0IjoxNzQ5MTI4MjUyL
CJleHAiOjE3NDkxMzU0NTJ9.vD3wpiD2WUJDvsTbd-mNBbXBEPZuyHe0_smiplD3LBs"
}
PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
POSTMAN CONSOLE
node - missao_pratica
Token Expiration: 2h
Endpoints disponíveis:
POST /api/auth/login (Body: {username, password})
GET /api/users (Requer Auth: Bearer <token>, Perf
GET /api/contracts/:empresa/:inicio (Requer Auth:
Login bem-sucedido para admin. Token gerado.
Signing you in...
Source: Postman
Cancel

Buscar contratos simulados



Consultar Usuários