



RPG0035 - SOFTWARE SEM SEGURANÇA NÃO SERVE
LUIS FERNANDO ELY – 202303157185

Missão Prática | Nível 5 | Mundo 5

Objetivos da prática

- Descrever o controle básico de acesso a uma API Rest;
- Descrever o tratamento de dados sensíveis e log de erros com foco em segurança;
- Descrever a prevenção de ataques de acesso não autorizado com base em tokens desprotegidos/desatualizados;
- Descrever o tratamento de SQL Injection em códigos-fonte; Descrever o tratamento de CRLF Injection em códigos-fonte;
- Descrever a prevenção a ataques do tipo CSRF em sistemas web;

Resultados:

REFATORAÇÃO DA APLICAÇÃO

- O uso de session-id foi removido e substituído por autenticação baseada em tokens JWT.
- Implementada a verificação do cabeçalho Authorization com o esquema Bearer para autenticação.
- Todos os endpoints agora verificam o token JWT para garantir a segurança das requisições.
- Endpoints que exigem privilégios de administrador realizam checagem específica de permissão.
- Criado o endpoint `/me`, que retorna os dados do usuário autenticado.
- Melhorias de segurança foram aplicadas utilizando ferramentas como Zod (validação de dados) e Bcrypt (criptografia de senhas), garantindo a integridade e segurança das informações enviadas às APIs.



ENDPOINTS:

The screenshot shows the Estácio API client interface. The left sidebar lists endpoints: POST Autenticação (200), POST Create Contract (201), POST Criar Usuario (201), GET Busca Empresa (404), and GET Usuarios (200). The main panel is titled 'Autenticação' and shows a POST request to `http://localhost:3000/api/auth/login`. The request body is a JSON object: `{ "username": "admin", "password": "admin" }`. The response is a 200 OK status with a 281 ms response time and 169 B of data. The response body is a JSON object: `{ "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZi6MSWicm9sZSI6ImFkbWluIiwiaWQiOiJ0eXNzQ5NTA0NjkiLCJleHAiOjE3NDkxMDQyOTV9.zKe8SmUN3mApeTZ3LI8yk1m8E4y0nXWoin7EurIaHg4" }`.

The screenshot shows the Estácio API client interface. The left sidebar lists endpoints: POST Autenticação (200), POST Create Contract (201), POST Criar Usuario (201), GET Busca Empresa (200), and GET Usuarios (200). The main panel is titled 'Create Contract' and shows a POST request to `http://localhost:3000/api/contracts`. The request body is a JSON object: `{ "empresa": "gremio", "data_inicio": "1903-08-09" }`. The response is a 201 Created status with a 20 ms response time and 99 B of data. The response body is a JSON object: `{ "message": "Criado com sucesso!", "contract": { "id": 3, "empresa": "gremio", "data_inicio": "1903-08-09" } }`.

estacio > No Environment Criar Usuario Personal Use

POST Autenticação 200
POST Create Contract 201
POST Criar Usuario 201
GET Busca Empresa 200
GET Usuarios 200

POST http://localhost:3000/api/auth/register

JSON Params Headers Auth Info

```
1 {  
2   "username": "user3",  
3   "password": "user3"  
4 }
```

201 Created • 288 ms • 152 B

Pretty Headers Info

```
1 {  
2   "message": "User registered",  
3   "user": {  
4     "id": 3,  
5     "username": "user3",  
6     "password":  
7       "$2b$12$Xf0X2P7LML77SSqM6noXi0P.3yt5R.vUiv8fc2IGNSfdSwtPkzoVW",  
8     "role": "user"  
9   }  
}
```

Setup FS Sync or Git

estacio > No Environment Busca Empresa Personal Use

POST Autenticação 200
POST Create Contract 201
POST Criar Usuario 201
GET Busca Empresa 200
GET Usuarios 200

GET http://localhost:3000/api/contracts/gremio/1903-08-09

JSON Params Headers Bearer Info

✓ Enabled

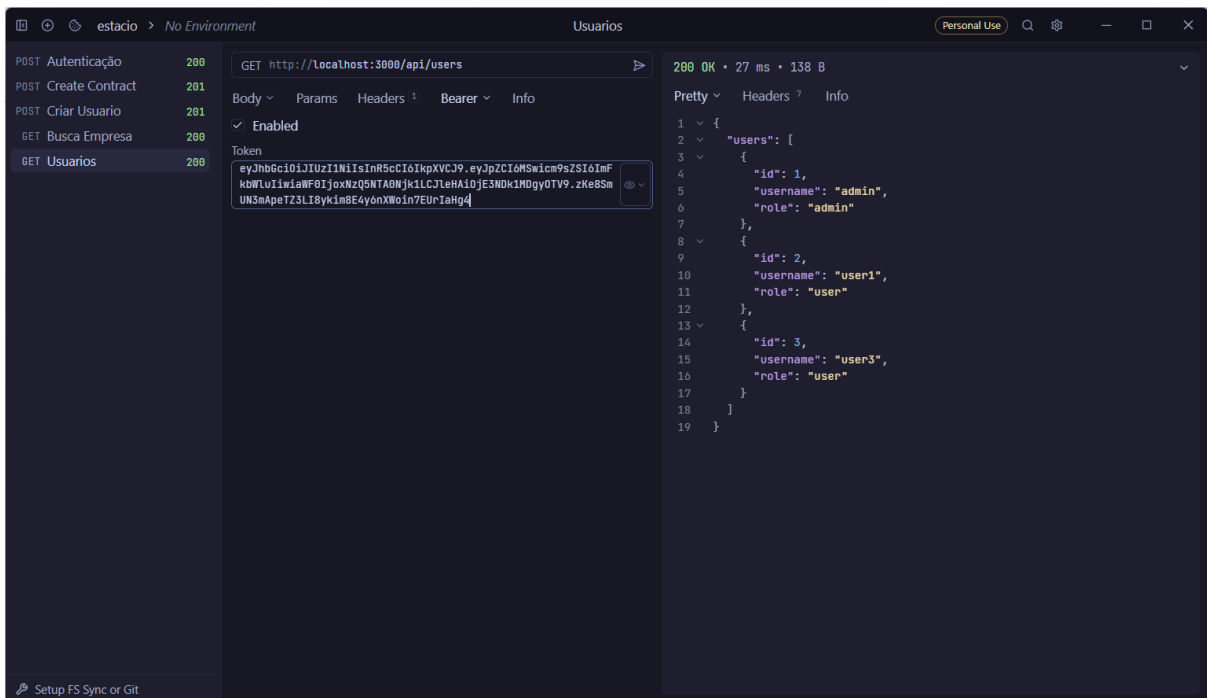
Token

200 OK • 19 ms • 70 B

Pretty Headers Info

```
1 {  
2   "contracts": [  
3     {  
4       "id": 3,  
5       "empresa": "gremio",  
6       "data_inicio": "1903-08-09"  
7     }  
8   ]  
9 }
```

Setup FS Sync or Git



estacio > No Environment Usuarios Personal Use

GET http://localhost:3000/api/users

200 OK • 27 ms • 138 B

Body Params Headers Bearer Info

✓ Enabled

Token

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSw1cm9sZSI6ImFkbWwluIiwiaWF0IjoxNzQ5NTA0Njk1LCJleHAiOjE3NDk1MDgyOTV9.zKe8SmUN3mApeT73L18yk1m8E4y6nXWoin7EurIahg4
```

1 {

2 "users": [

3 {

4 "id": 1,

5 "username": "admin",

6 "role": "admin"

7 },

8 {

9 "id": 2,

10 "username": "user1",

11 "role": "user"

12 },

13 {

14 "id": 3,

15 "username": "user3",

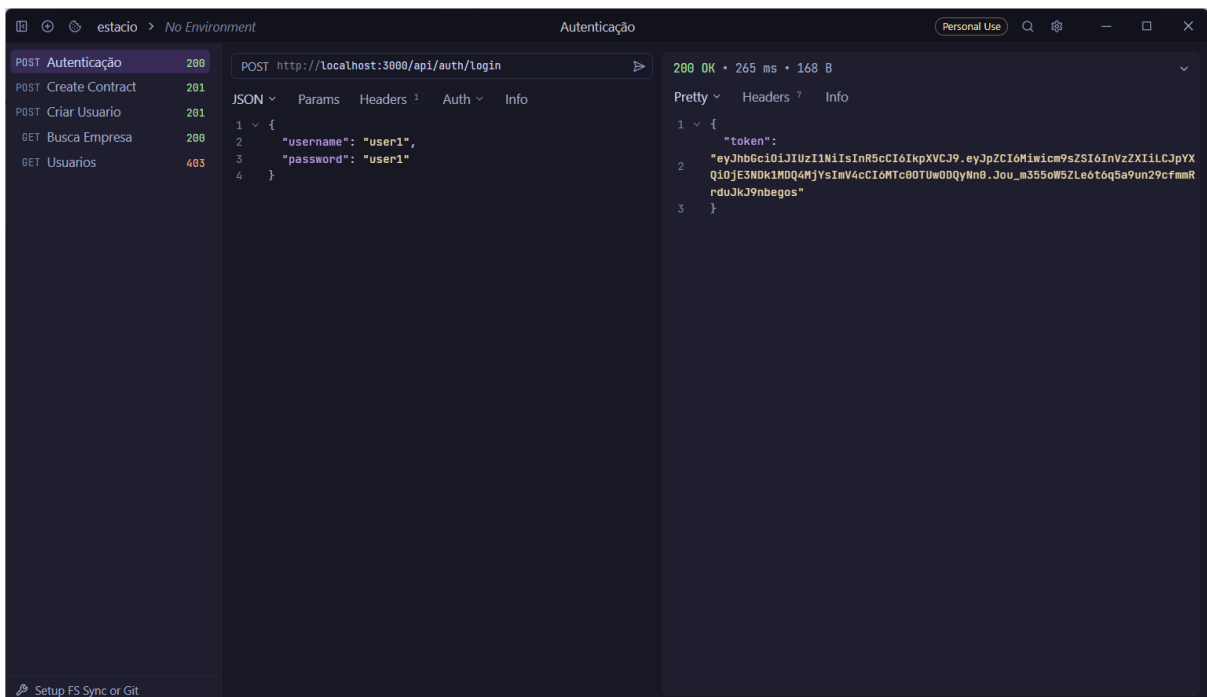
16 "role": "user"

17 }

18]

19 }

Acessando com perfil de Usuário



estacio > No Environment Autenticação Personal Use

POST http://localhost:3000/api/auth/login

200 OK • 265 ms • 168 B

JSON Params Headers Auth Info

1 {

2 "username": "user1",

3 "password": "user1"

4 }

1 {

2 "token":

3 "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSw1cm9sZSI6ImFkbWwluIiwiaWF0IjoxNzQ5NTA0Njk1LCJleHAiOjE3NDk1MDgyOTV9.zKe8SmUN3mApeT73L18yk1m8E4y6nXWoin7EurIahg4"

4 }

