

# Autenticação e Autorização com Flask (JWT + Bcrypt)

## Trabalho Bimestral – 4º Bimestre

Disciplina: Linguagem Técnica de Programação

Integrantes: Fernanda Nascimento de Paula e Bruna Camargo Galindo

Turma: A

Professor: Luiz Gustavo Vêras

Data de entrega: 30/10/2025

### 1. Introdução

Este trabalho tem como objetivo aplicar autenticação e autorização seguras à API Parla, utilizando os conceitos de JWT (JSON Web Token) e Flask-Bcrypt. A proposta consiste em aprimorar o sistema desenvolvido nos bimestres anteriores, garantindo que apenas usuários autenticados possam acessar as rotas da aplicação.

### 2. Explicação Técnica

JWT (JSON Web Token): é um token digital temporário gerado no login. Ele contém as informações do usuário e uma data de expiração. Sempre que o usuário acessa uma rota protegida, o token é enviado no cabeçalho da requisição e validado pelo sistema, permitindo o acesso apenas se for válido.

Bcrypt: é uma biblioteca de criptografia usada para proteger senhas. Ela transforma a senha original em um código irreversível antes de salvar no banco de dados. Durante o login, o sistema compara a senha digitada com a versão criptografada, garantindo segurança total.

### 3. Fluxo de Funcionamento

Etapa	Descrição
1. Registro	O usuário cria uma conta e a senha é criptografada com Bcrypt.
2. Login	As credenciais são verificadas e um token JWT é gerado.
3. Acesso	As rotas protegidas exigem o envio do token no cabeçalho Authorization.
4. Logout	O token é invalidado e o acesso é bloqueado até novo login.

### 4. Testes Realizados (Insomnia)

Os testes foram realizados utilizando o Insomnia, validando os seguintes cenários:

- Registro de usuário (rota /register)
- Login com senha correta e incorreta
- Acesso a rotas protegidas com e sem token
- Logout e tentativa de reuso de token invalidado

Durante os testes, foi possível observar que o banco de dados armazena a senha de forma criptografada, seguindo o formato padrão Bcrypt (exemplo: \$2b\$12\$...).

## 5. Conclusão

Com a implementação do JWT e do Bcrypt, a API Parla passou a oferecer um sistema de autenticação seguro e moderno. Agora, todas as rotas são protegidas e apenas usuários autenticados podem acessá-las. O uso de tokens temporários garante controle de sessão e o Bcrypt assegura que as senhas não possam ser reveladas.

## 6. Resumo para Apresentação

O JWT funciona como um crachá digital que o usuário precisa para acessar as rotas protegidas. O Bcrypt transforma a senha em um código indecifrável, protegendo os dados armazenados. Juntos, eles garantem segurança, privacidade e controle de acesso em toda a API Parla.