# Relatório de Segurança – Tópico 5.2

## Objetivo

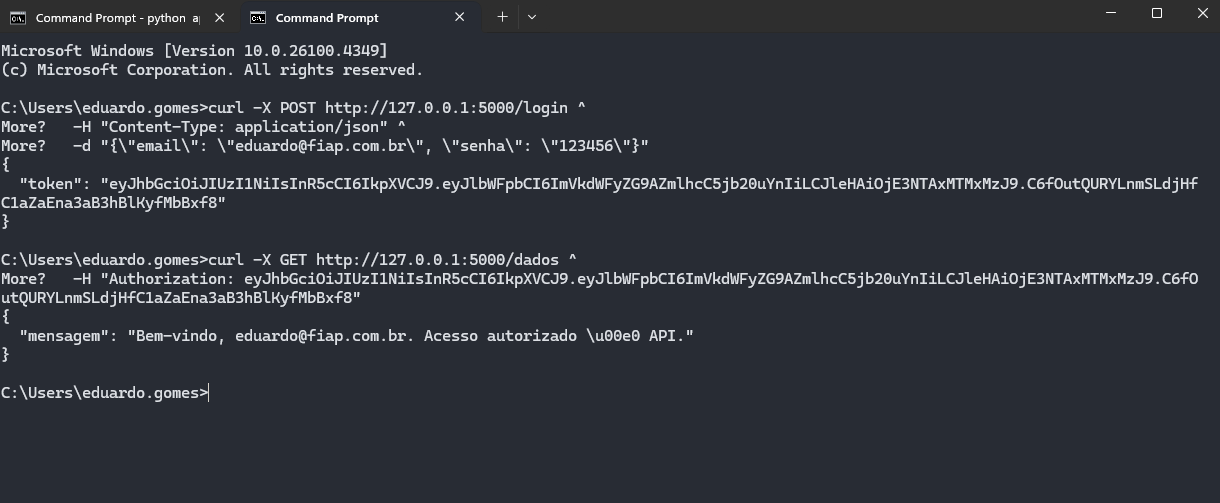
Proteger endpoints de API utilizando tokens seguros (JWT), garantindo que apenas usuários autenticados tenham acesso, com validações de expiração, assinatura e permissões básicas conforme as boas práticas de segurança.

## Ações Realizadas

- Criado endpoint `/login` que gera um JWT com validade de 5 minutos.  
- Token inclui dados do usuário e é assinado com chave secreta.  
- Implementado endpoint `/dados` protegido, acessível apenas com token válido via cabeçalho Authorization.  
- Realizada validação de:  
 - Presença do token  
 - Assinatura válida (chave secreta)  
 - Expiração do token

## Evidência

Terminal mostrando a geração do token via `/login` e o acesso autorizado à API via `/dados` com JWT.



## Conclusão

A autenticação por tokens JWT garante segurança e escalabilidade para APIs modernas, evitando acessos indevidos por meio da validação de identidade e tempo de expiração. Isso reforça a integridade e a confidencialidade dos dados trafegados via API.