



PUC Minas

# Plataforma Node.js

## JSON Web Token (JWT)

# JSON Web Token (JWT)

Padrão que define uma forma compacta e segura de transferência de informações baseada em tokens no formato JSON ([RFC-7519](https://tools.ietf.org/html/rfc7519)) utilizadas em mecanismos de autenticação e autorização.

## Estrutura básica da token JWT

### [header]

Informações sobre o tipo da token e o algoritmo de criptografia utilizado

```
base64enc ({  
  "alg": "HS256",  
  "typ": "JWT"  
})
```

### [payload]

- Dados da token, denominados Claims que podem ser reservados, públicos ou privados

```
base64enc ({  
  "id": "HS256",  
  "roles": "ADMIN"  
})
```

### [signature]

- assinatura da token que garante a confiabilidade da token evitando alterações

```
HMACSHA256 (  
  base64enc(header) + "." +  
  base64enc(payload),  
  secretKey  
)
```

Fonte: [JWT – Auth0](#)

# JSON Web Token (JWT)

## Campos reservados (claims)

- Iss (Issuer) – Emissor da token JWT
- Sub (Subject) – Assunto da token
- Aud (Audience) – Identifica o público para o qual a token foi emitida
- Exp (Expiration Time) – Horário de expiração da token, a partir do qual não é mais aceita
- iat (Issued At) – Horário em que a token foi emitida

Fonte: [Wikipedia JSON Web Token](#)

# JSON Web Token (JWT)

Exemplo da criação de uma token para informações do usuário via Node.js

Instalação JSONWebToken  
`npm install jsonwebtoken`

```
require ('dotenv').config()
const JWT = require('jsonwebtoken')
const express = require("express")
const app = express()

app.get("/", function(req, res){
  JWT.sign({ userID: 'abc123' },
    process.env.SECRET_KEY,
    { algorithm: 'HS256' },
    (err, token) => {
      if (err) console.error('Erro: ' + err);
      else console.log (token)
    })

  res.send ('Hello JWT')
});

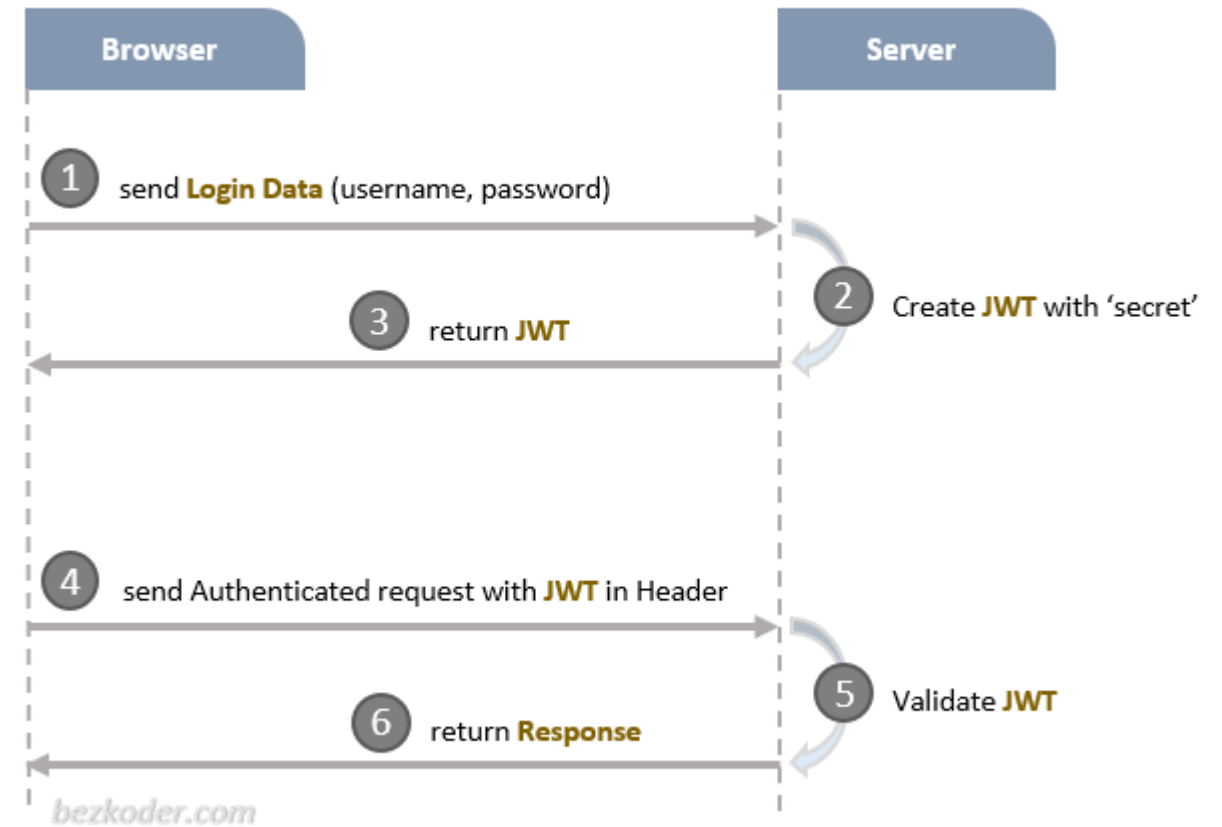
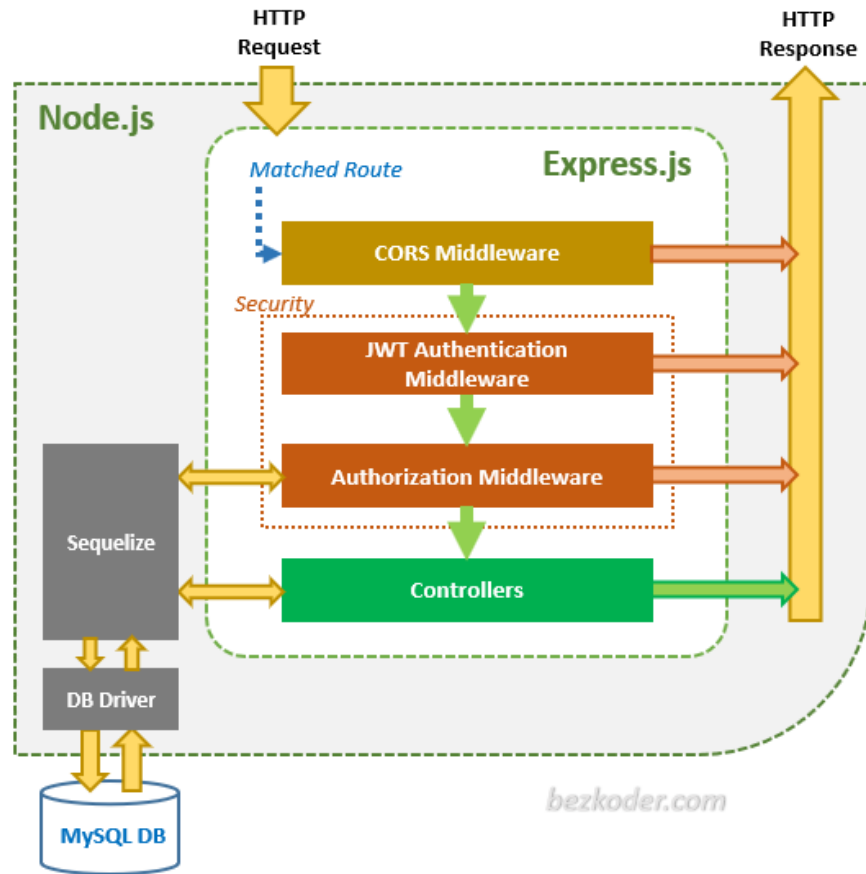
app.listen(3000);
```

# JSON Web Token (JWT)

Gerando uma chave forte em JavaScript com Node.js

```
>> node -e "console.log(require('crypto').randomBytes(256).toString('base64'));"  
  
//Exemplo de chave secreta gerada  
GdLOU8owaDRw3kF23gicjzWHLsICP5pP365G/8Jd1Vm90qaphvQFRJAtZOFU2BuAj+yObat3ImenitbJp  
ZF+9toj9+4L7A9XZW98kxLo+oGJhXJwlwc78bvJaHH7zzx1VFBZ9ipGoIz57xqlhqZE7buH1nPjRGOSH  
MQuqZ7XxZ1/Odk7Veib182SboX3G8gCI38FIBmiJM4quWDv3MZOIP1ElQlWgVBjH/y6AxZkxSMA  
n8DyZ9xa94pKxwXFMQPZrbD0+rhneC0rfi5kvcxVLM/w3rB3EHWBHNNaQ941QKpIMjqAg8iI1LUegfZ4tJs49tGV  
fYgwtBKAKXwI6YuCIw==
```

# Autenticação e autorização com JWT



Fonte: [Node.js Express: JWT example | Token Based Authentication & Authorization](#)

# Obrigado!