

# #Introduction

Authentication is one of the big parts of every application. Security is always something that is changing and evolving. In the past, we have gone over Node authentication (<https://scotch.io/courses/easy-node-authentication>) using the great Passport (<http://passportjs.org/>) npm package.

Those articles used the session based authentication however, which has problems when we talk about scaling web services and creating an API that can be consumed across many devices and services.

As a primer to this article, go ahead and get yourself familiar with token based authentication principles (<https://scotch.io/bar-talk/the-ins-and-outs-of-token-based-authentication>) and the standard used for token based authentication, JSON Web Tokens (<https://scotch.io/tutorials/the-anatomy-of-a-json-web-token>).

## Table of Contents

- 1 Introduction
- 2 What We'll Be Building
- 3 Getting Started
- 4 Set Up Our Node Application (package.json)
- 5 The Actual Node Application (server.js)
- 6 Creating a Sample User
- 7 Showing Our User
- 8 Authenticating and Creating a Token
- 9 Route Middleware to Protect API Routes
- 10 Testing Our Middleware
- 11 Conclusion

Now that we've got all the important information about token based authentication out of the way, let's build a very simple Node API and use tokens to authenticate users that request access.

*Note:* Updated to fix a security vulnerability. Only passing in a set payload when creating our JWT as pointed out by Mydayyy (<https://github.com/Mydayyy>) on GitHub (<https://github.com/scotch-io/node-token-authentication/pull/9>).

# #What We'll Be Building

We'll build a quick API using Node and Express and we'll be using POSTman (<https://www.getpostman.com/>) to test it.

The main workflow of this is that we will:

1. Have unprotected and protected routes
2. A user will authenticate by passing in a name and a password and get back a token
3. The user will store this token on their client-side and send it for every request
4. We will validate this token, and if all is good, pass back information in JSON format

Our API will be built with:

- normal routes (not authenticated)
- route middleware to authenticate the token
- route to authenticate a user and password and get a token
- authenticated routes to get all users

**Further Reading:** For some information on Express routing and middleware, check out our article on Express 4.0 routing (<https://scotch.io/tutorials/javascript/learn-to-use-the-new-router-in-expressjs-4>).

## Tools Needed

- node and npm
- POSTman (<https://www.getpostman.com/>)

We know what we're going to build, now let's get to it!

Related Course: [Getting Started with JavaScript for Web Development \(https://bit.ly/2rVqDcs\)](https://bit.ly/2rVqDcs).

# #Getting Started

Let's take a look at our file structure for our Node application. This will be simplified and we'll be putting a lot of stuff into the `server.js` file.

## File Structure

```
- app/  
  ----- models/  
    ----- user.js  
- config.js  
- package.json  
- server.js
```

JAVASCRIPT

For a fully fledged application, you'd want to move some of this out of the main file and into separate files (particularly the routes).

# #Set Up Our Node Application (package.json)

First, we need to set up our `package.json` file. This is our beginning file for our Node application.

## JAVASCRIPT

```
{
  "name": "node-token-jwt",
  "main": "server.js"
}
```

Now that we have our `package.json` set, let's install our packages.

## JAVASCRIPT

```
$ npm install express body-parser morgan mongoose jsonwebtoken --save
```

- **express** is the popular Node framework
- **mongoose** is how we interact with our MongoDB database
- **morgan** will log requests to the console so we can see what is happening
- **body-parser** will let us get parameters from our POST requests
- **jsonwebtoken** is how we create and verify our JSON Web Tokens

The `--save` modifier will also save these packages to our `package.json` file. How convenient!

Next let's take care of a few files that we'll need for our project.

## User Model (app/models/user.js)

The user model that we define will be used when creating and getting users. To create a Mongoose model, let's create the file `app/models/user.js`

## JAVASCRIPT

```
// get an instance of mongoose and mongoose.Schema
var mongoose = require('mongoose');
var Schema = mongoose.Schema;

// set up a mongoose model and pass it using module.exports
module.exports = mongoose.model('User', new Schema({
  name: String,
  password: String,
  admin: Boolean
}));
```

The other file we'll need to create is our `config.js` file. This is where we can store different variables and configuration for our application.

## Config File (config.js)

For this file, **you will need to create MongoDB database**. You can either create one locally or easily use one online at [modulus.io](http://modulus.io) (<http://modulus.io>) for free. Either way, you will be able to get a URI string to use as your database configuration.

### MongoDB Atlas - Official Site - Cloud DBaaS for MongoDB

The Easiest Way to Deploy, Operate, and Scale MongoDB in the Cloud. Start Free! [mongodb.com/Atlas](https://mongodb.com/Atlas)



#### JAVASCRIPT

```
module.exports = {  
  
  'secret': 'ilovescotchyscotch',  
  'database': 'mongodb://noder:noderauth&54;proximus.modulusmongo.net:27017/so9pojyN'  
  
};
```

- **secret:** used when we create and verify JSON Web Tokens
- **database:** the URI with username and password to your MongoDB installation

With all that out of the way, we can get to the big parts of our tutorial. We still haven't defined our main file ( `server.js` ), so let's get to that.

# #The Actual Node Application (server.js)

In this file, we will:

**Grab All the Packages** This will include the packages we installed earlier (express, body-parser, morgan, mongoose, and jsonwebtoken) and also we'll be grabbing the model and config that we created.

**Configure Our Application** We will set our important variables, configure our packages, and connect to our database here.

**Create Basic Routes** These are the unprotected routes like the home page ( `http://localhost:8080` ). We'll also create a `/setup` route here so that we can create a sample user in our new database.

**Create API Routes** This includes the following routes:

- `POST http://localhost:8080/api/authenticate` Check name and password against the database and provide a token if authentication successful. This route will not require a token because this is where we get the token.
- `GET http://localhost:8080/api` Show a random message. This route is protected and will require a token.
- `GET http://localhost:8080/api/users` List all users. This route is protected and will require a token.

With those things in our mind, let's start our `server.js` file:

## JAVASCRIPT

```
// =====  
// get the packages we need =====  
// =====  
  
var express    = require('express');  
var app        = express();  
var bodyParser = require('body-parser');  
var morgan     = require('morgan');  
var mongoose   = require('mongoose');  
  
var jwt        = require('jsonwebtoken'); // used to create, sign, and verify tokens  
var config     = require('./config'); // get our config file  
var User       = require('./app/models/user'); // get our mongoose model  
  
// =====  
// configuration =====  
// =====  
  
var port = process.env.PORT || 8080; // used to create, sign, and verify tokens  
mongoose.connect(config.database); // connect to database  
app.set('superSecret', config.secret); // secret variable  
  
// use body parser so we can get info from POST and/or URL parameters  
app.use(bodyParser.urlencoded({ extended: false }));  
app.use(bodyParser.json());  
  
// use morgan to log requests to the console  
app.use(morgan('dev'));  
  
// =====  
// routes =====  
// =====  
// basic route  
app.get('/', function(req, res) {  
    res.send('Hello! The API is at http://localhost:' + port + '/api');  
});  
  
// API ROUTES -----  
// we'll get to these in a second  
  
// =====  
// start the server =====  
// =====  
  
app.listen(port);  
console.log('Magic happens at http://localhost:' + port);
```


With that, we should be able to start up our Node server (make sure you have a valid database configured in `config.js`). Now if we start the server with:

JAVASCRIPT

```
$ node server.js
```


**Tip:** Use nodemon to have your server restart on file changes. Install nodemon using `npm install -g nodemon`. Then start your server with `nodemon server.js`.

We should be able to go to our browser and see the message from the route we created. Go to `http://localhost:8080` (`http://localhost:8080`) and you'll see:

 2014-11-13 (2)

(<https://cask.scotch.io/2014/11/2014-11-13-2.png>)

As a bonus, since we used morgan, we are able to see the request logged to our console, which helps with development.

 2014-11-13 (4)

(<https://cask.scotch.io/2014/11/2014-11-13-4.png>)

## #Creating a Sample User



Now we know our application is up and running! Let's create a sample user using the model that we created earlier.

This is a very simple process, we'll just create a quick route that will create a user of our choosing.

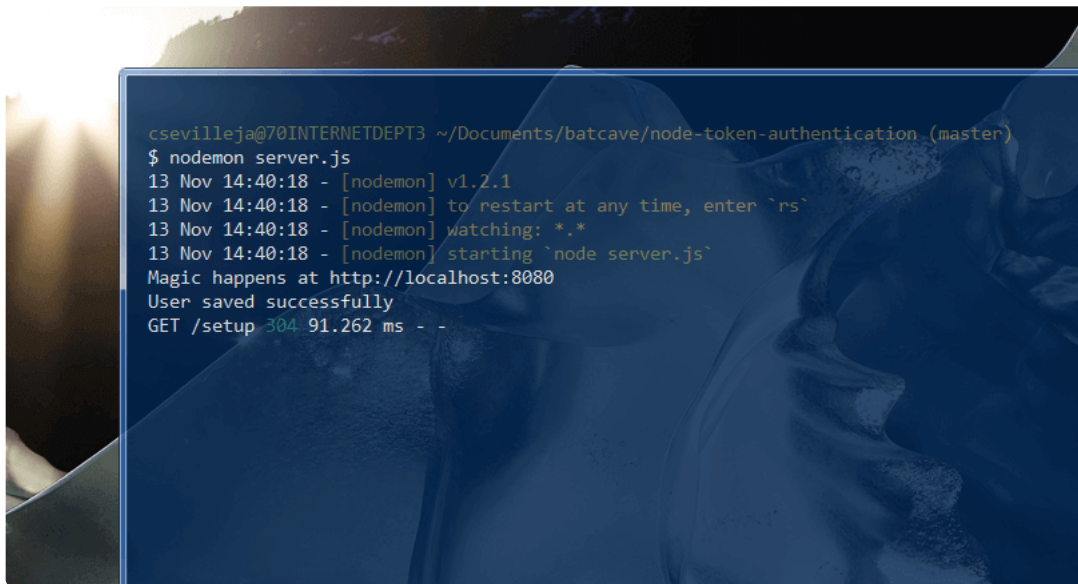
Here's that route. Just add it to the routes section of our `server.js` :

#### JAVASCRIPT

```
app.get('/setup', function(req, res) {  
  
  // create a sample user  
  var nick = new User({  
    name: 'Nick Cerminara',  
    password: 'password',  
    admin: true  
  });  
  
  // save the sample user  
  nick.save(function(err) {  
    if (err) throw err;  
  
    console.log('User saved successfully');  
    res.json({ success: true });  
  });  
});
```

It's important to note that we would **never** save a password to the database plain text like this. You would protect your passwords by hashing it.

Go ahead and visit your application at `http://localhost:8080/setup` . You should see the message 'User saved successfully' logged to your console and the JSON object with `{ success: true }` in your browser.



```
csevilleja@70INTERNETDEPT3 ~/Documents/batcave/node-token-authentication (master)
$ nodemon server.js
13 Nov 14:40:18 - [nodemon] v1.2.1
13 Nov 14:40:18 - [nodemon] to restart at any time, enter `rs`
13 Nov 14:40:18 - [nodemon] watching: *.*
13 Nov 14:40:18 - [nodemon] starting `node server.js`
Magic happens at http://localhost:8080
User saved successfully
GET /setup 304 91.262 ms - -
```

(<https://cask.scotch.io/2014/11/2014-11-13-3.png>)

We'll now create a route to get the users in our database and return them as JSON.

## #Showing Our User

Now let's create our API routes and create one to return all our users in JSON format. We'll use an instance of the Express router for this. We'll place a few placeholders so we can see where things will go. Here is the code for that:

## JAVASCRIPT

```
// API ROUTES -----

// get an instance of the router for api routes
var apiRoutes = express.Router();

// TODO: route to authenticate a user (POST http://localhost:8080/api/authenticate)

// TODO: route middleware to verify a token


// route to show a random message (GET http://localhost:8080/api/)
apiRoutes.get('/', function(req, res) {
  res.json({ message: 'Welcome to the coolest API on earth!' });
});

// route to return all users (GET http://localhost:8080/api/users)
apiRoutes.get('/users', function(req, res) {
  User.find({}, function(err, users) {
    res.json(users);
  });
});

// apply the routes to our application with the prefix /api
app.use('/api', apiRoutes);
```


We now have two routes that we can use. We can see these in our browser again, but at this point, let's switch over to POSTman.

For the URL, use: `http://localhost:8080/api/` and we will be able to see the message.

 2014-11-13 (6)

(<https://cask.scotch.io/2014/11/2014-11-13-6.png>)

Then we can go to: `http://localhost:8080/api/users` and see the list of users.

 2014-11-13 (5)

(<https://cask.scotch.io/2014/11/2014-11-13-5.png>)

This is great that we have been able to create a user and show them. We probably don't want any random person to see our list of users however.

Next, let's make sure that we can **authenticate a user** and then **protect those routes** using Express route middleware and requiring a token.

## #Authenticating and Creating a Token

Let's make our `POST http://localhost:8080/api/authenticate` route where we will accept a name and a password (probably from a form). If the name and password validate, then we will create a token and pass that back.

Once the user has that token, they will store it client side and pass it with every request for information after that and we will validate the token on every request using route middleware.

Here's the code for our POST route:

## JAVASCRIPT

```
// API ROUTES -----

// get an instance of the router for api routes
var apiRoutes = express.Router();

// route to authenticate a user (POST http://localhost:8080/api/authenticate)
apiRoutes.post('/authenticate', function(req, res) {

  // find the user
  User.findOne({
    name: req.body.name
  }, function(err, user) {

    if (err) throw err;

    if (!user) {
      res.json({ success: false, message: 'Authentication failed. User not found.' });
    } else if (user) {

      // check if password matches
      if (user.password !== req.body.password) {
        res.json({ success: false, message: 'Authentication failed. Wrong password.' });
      } else {

        // if user is found and password is right
        // create a token with only our given payload
        // we don't want to pass in the entire user since that has the password
        const payload = {
          admin: user.admin
        };

        var token = jwt.sign(payload, app.get('superSecret'), {
          expiresInMinutes: 1440 // expires in 24 hours
        });

        // return the information including token as JSON
        res.json({
          success: true,
          message: 'Enjoy your token!',
          token: token
        });
      }
    }

  });
});
```

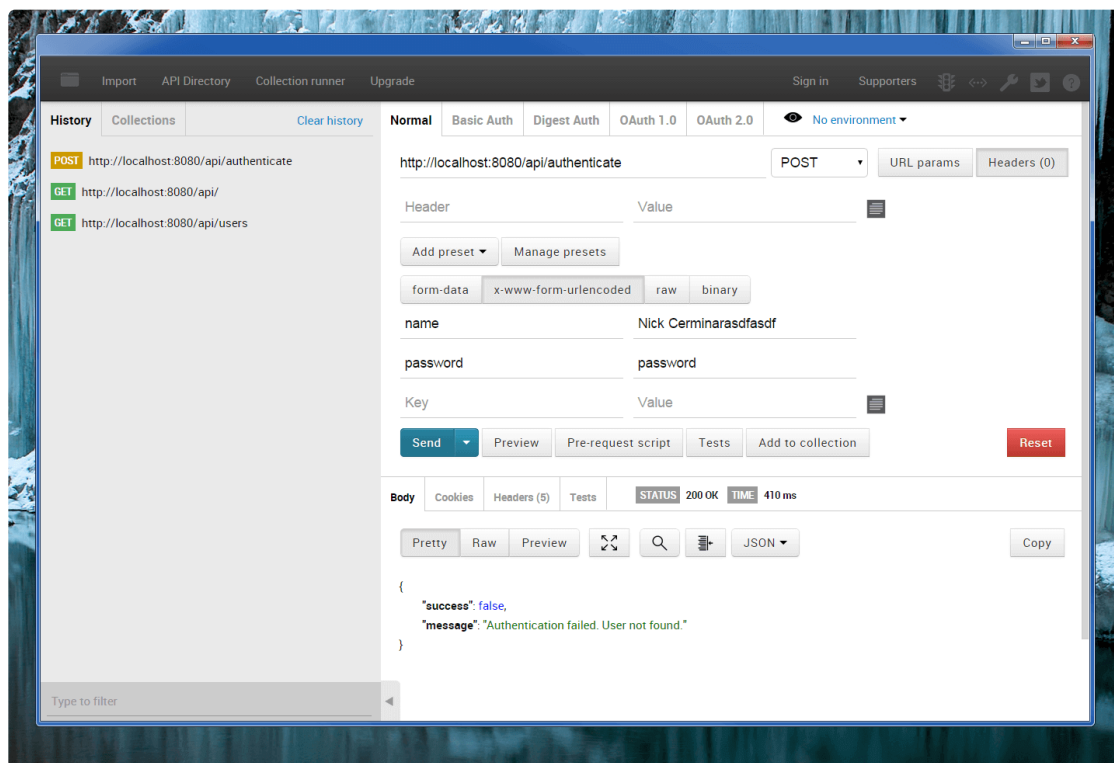
...

With this code, we can check our user and password and pass back a token in a JSON response. We are using **mongoose to find the user** and **jsonwebtoken to create the token**.

Let's test this out using POSTman. Change your HTTP request to POST and add the name and password parameters to `x-www-form-urlencoded`. This is how we simulate information coming through a form POST.

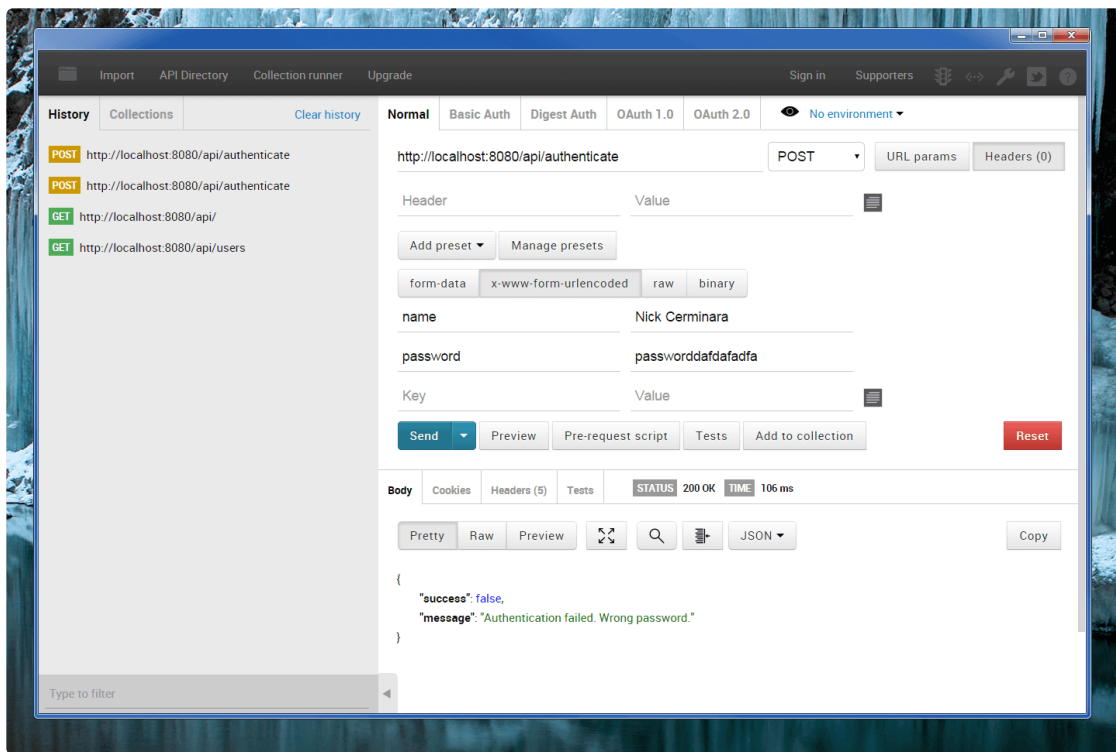
Remember the user we created earlier had a name of **Nick Cerminara** and a password of **password**. (super safe, I know)

Here's the route using the wrong name:



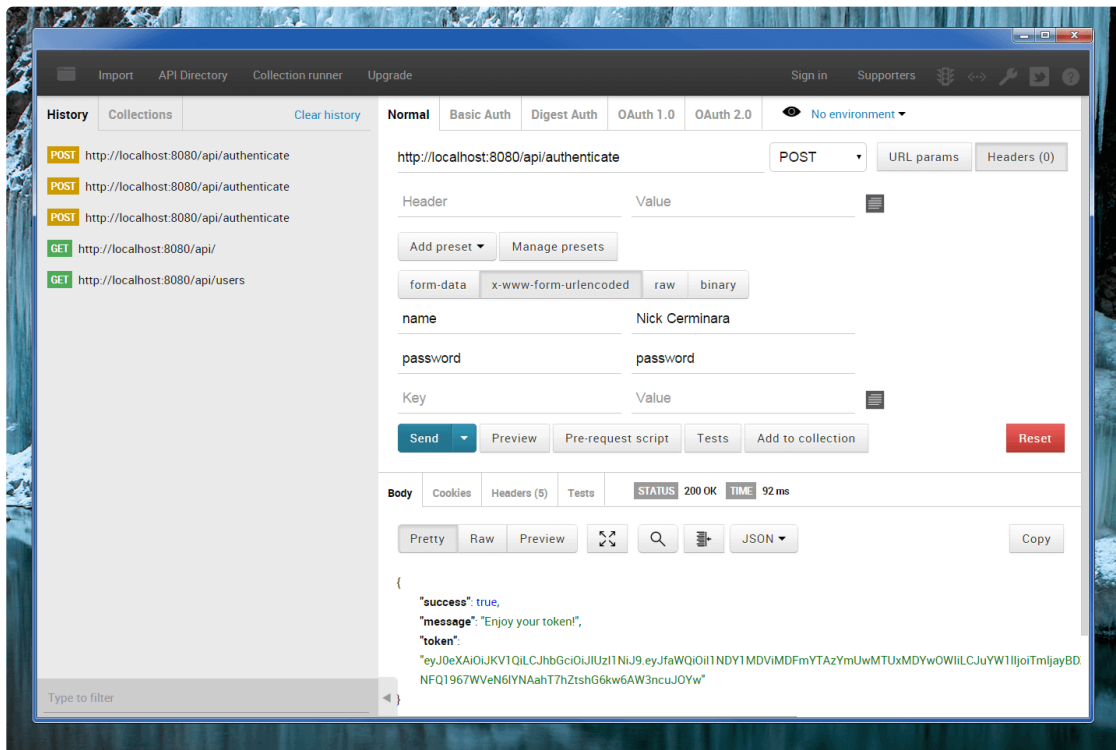
(<https://cask.scotch.io/2014/11/2014-11-13-7.png>)

Using the right name and wrong password:



(<https://cask.scotch.io/2014/11/2014-11-13-8.png>)

When everything goes well:



(<https://cask.scotch.io/2014/11/2014-11-13-9.png>)

You can see that in our response, we are given our token! Now let's copy and paste that token somewhere safe until we are able to use it after we create our route middleware next.

# #Route Middleware to Protect API Routes

At this point, we have 3 routes defined on our API routes ( `/api/authenticate` , `/api` , and `/api/users` ). Let's create route middleware to protect the last 2 routes. We won't want to protect the `/api/authenticate` route so what we'll do is place our middleware beneath that route. Order is important here.

Let's take a look at the code:



## JAVASCRIPT

```
// API ROUTES -----

// get an instance of the router for api routes
var apiRoutes = express.Router();

// route to authenticate a user (POST http://localhost:8080/api/authenticate)
...

// route middleware to verify a token
apiRoutes.use(function(req, res, next) {

  // check header or url parameters or post parameters for token
  var token = req.body.token || req.query.token || req.headers['x-access-token'];

  // decode token
  if (token) {

    // verifies secret and checks exp
    jwt.verify(token, app.get('superSecret'), function(err, decoded) {
      if (err) {
        return res.json({ success: false, message: 'Failed to authenticate token.' });
      } else {
        // if everything is good, save to request for use in other routes
        req.decoded = decoded;
        next();
      }
    });
  } else {

    // if there is no token
    // return an error
    return res.status(403).send({
      success: false,
      message: 'No token provided.'
    });
  }
});

// route to show a random message (GET http://localhost:8080/api/)
...

// route to return all users (GET http://localhost:8080/api/users)
...

```

```
// apply the routes to our application with the prefix /api  
app.use('/api', apiRoutes);
```

We are using the `jsonwebtoken` package again, but this time we are going to verify the token that was passed in. It is important that our secret used here matches the secret that was used to create the token. We are also making sure to send the right HTTP response code as 403 forbidden and our user was not authenticated to view any data.

If everything looks good the token was able to be verified, we'll take the information that came out of the token and pass it to the other routes in the `req` object.

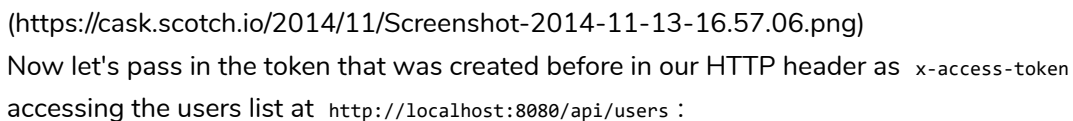
## #Testing Our Middleware

We have built our middleware that our Node application will run through before it gets to the routes that we want authenticated.

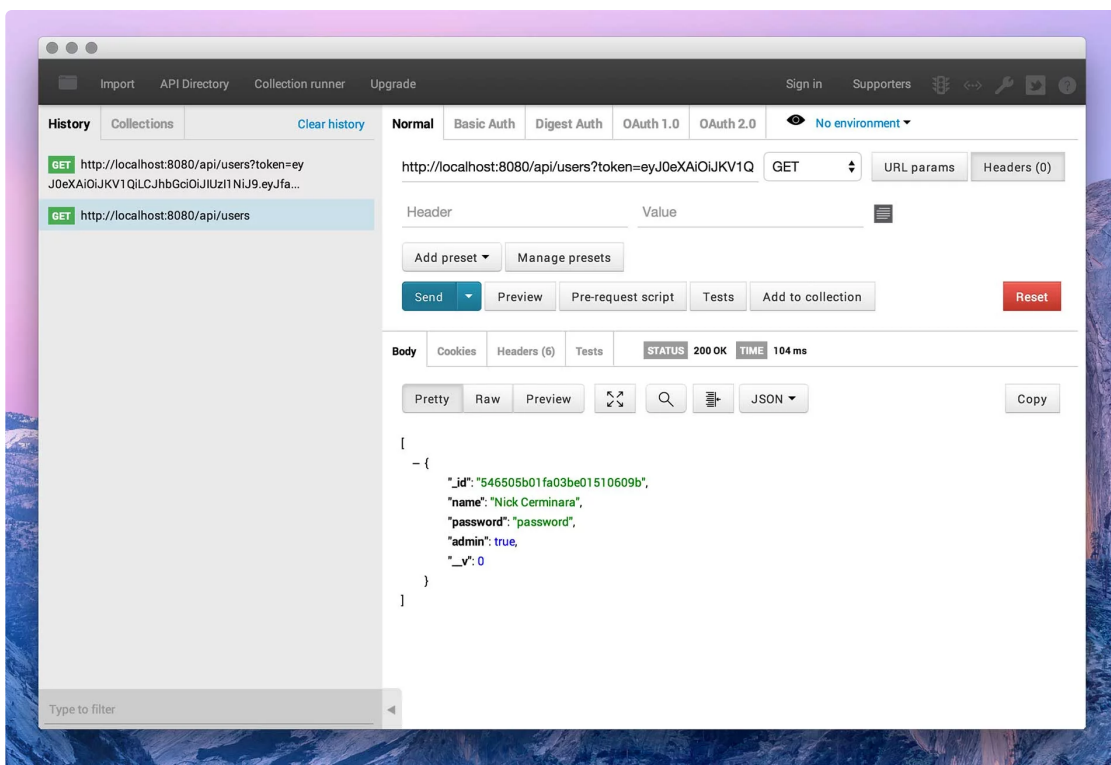
Let's go into POSTman again and try to access both routes without passing a token.

This is our route without the token just accessing the base api route of

`http://localhost:8080/api :`



We can also pass it in as a URL parameter by going to: `http://localhost:8080/api/users?token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJfaWQiOiI1NDY1MDViMDFmYTAzYmUwMTUxMDYwOWNFQ1967WVeN6YNAahT7hZtshG6kw6AW3ncuJOYw`



(<https://cask.scotch.io/2014/11/Screenshot-2014-11-13-17.57.40.jpg>)

## #Conclusion

This is a good look at how we can protect routes and our Node API using JSON Web Tokens. This can be expanded into a much larger scoped project like providing permission specific tokens and creating a more robust and feature filled API.

Hopefully this look has given you a good understanding of how the routes are used (especially middleware), tokens are created, and requests to the API all come together.







CODE([HTTPS://GITHUB.COM/SCOTCH-IO/NODE-TOKEN-AUTHENTICATION](https://github.com/Scotch-io/node-token-authentication))

Chris Sevilleja (/@chris)

Founder of Scotch.io. Google Developer Expert in Web Technologies. Slapping the keyboard until something good happens.



isoncode) (<https://facebook.com/sevilayha>) (<https://github.com/sevilayha>) (<https://instagram.com/chriscode.chrislift>) (<https://twitter.com/sevilayha>)

<p><b>A SIMPLE TIP TO IMPROVE YOUR...</b></p> <p> <b>CyanCorn</b> 4d</p> <p>What an obvious ad</p>	<p><b>CREATE A TYPING SPEED EFFECT WITH VUEJS</b></p> <p> <b>BlueBone</b> 4d</p> <p>Great tutorial! I wanted to learn mor...</p>	<p><b>BUILD AND UNDERSTAND A SIMPLE NODEJS...</b></p> <p> <b>GreenBullhorn</b> 6 Aug</p> <p>Hello, When I try npm start after enable my...</p>	<p><b>HANDLING AUTHENTICATION IN V...</b></p> <p> <b>PurplePizza</b> 7h</p> <p>How can i access the error messages to...</p>	<p><b>DOCKER AND VISUAL STUDIO CODE</b></p> <p><b>Дмитрий Ище...</b> 7 Aug</p> <p>Thank you for a great article! One question...</p>	<p><b>VUE AUTHENTICATION AND ROUTE HANDLING...</b></p> <p> <b>bayuangkasa</b> 7 Jul</p> <p>There is an error on table creation (db.js)...</p>	<p><b>UNDERSTANDING UNDERLYING PRO...</b></p> <p> <b>OrangeFa</b> 5 Jul</p> <p>Dude, I just pur... your book :)</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



(<https://dynamic-cdn.spot.im/yad/optout.html>)

### Conversation (247)

Sort by **Best** ▼

Have a Disqus Account?  [Log In](#)



Add a comment...





The Dude · 22 Apr, 2015

Nice write-up! Can't wait to give it a whirl. I like the TODO-add security article.

Reply · Share · 2 Likes ·  

**Chris Sevilleja** ➔ The Dude · 22 Apr, 2015

Whoops. Fixed! Thanks for pointing that out.

Reply · Share ·  

Filipe Sguarizi Panceri · 22 Apr, 2015

Sometimes i get throw new Error('Can\'t set headers after they are sent.');" on list all users.

Reply · Share ·  

**Chris Sevilleja** → Filipe Sguarizi Panceri · 23 Apr, 2015 

Sounds like the middleware is the problem. It's probably already returning data and not ending the app correctly.

I'll double check to make sure this tutorial does it right. Try using:

return res.send() and return res.json() instead of res.send()

Reply · Share ·  

**Filipe Sguarizi Panceri** → Chris Sevilleja · 23 Apr, 2015 

This error occurs when i put the invalid token and try to access /api or /api/users

Reply · Share ·  

**Shahar** → Filipe Sguarizi Panceri · 23 Apr, 2015 

+1

I tried to debug it, and it seems to send two json responses in a row:

- return res.json({ success: false, message: 'Failed to authenticate token.' });
- res.json(users);


although it shouldn't send the second one at all due to the authorization. I thought of checking the "req.decoded" inside the route using an if statement, but then an "opposite" problem occurs: it shows an error normally when the token is incorrect, but it gets stuck when the token is authenticated.


Reply · Share ·  

Show 2 more replies ▾



**pathsofdesign** · 23 Apr, 2015 

That's awesome. I just implemented this on a personal site running ReactJS.

Reply · Share ·  



**Chris Sevilleja** → pathsofdesign · 23 Apr, 2015 

That's really cool. How are you liking React?

Reply · Share ·  

**pathsofdesign** → Chris Sevilleja · 23 Apr, 2015 

I've really been digging it. I feel that it's helped me become more efficient with Javascript. Still a lot to learn to do what I can in Angular though.



Reply · Share · 2 Likes ·  

 **GoldMustache** → pathsofdesign · 28 Aug 

Hey there,

Could you help me linking this with ReactJS? Do you have your code on Git?



Abi

Reply · Share ·  

**kyllo** · 23 Apr, 2015 

Great article, i've been building something similar.

Would love to see how you handle permission specific tokens & refresh tokens.

Reply · Share · 3 Likes ·  

**seaniscreative** → kyllo · 24 Jul, 2015 



Wondering about this too. Haven't seen examples using refresh workflows...

Reply · Share ·  

**Philippe Leefsma** → seaniscreative · 25 Mar, 2016 

Refreshing the token is the duty of the client. The token provider can add a field

'expiresIn' to the token response. On the client/consumer app of the token, this value is then used to request a new token when the current one is about to expire.

Reply · Share · 2 Likes ·  

SHOW MORE COMMENTS...

💖 A side project brought to you from Las Vegas and DC by... (/about)

(<https://scotch.io/@chris>)

Chris Sevilleja (<https://scotch.io/@chris>)

Follow @chrisoncode

8,580 followers

(<https://bit.ly/2tDcLEK>)

(<https://scotch.io/courses/getting-started-with-vue>)

(<https://scotch.io/@nick>)

Nick Cerninara (<https://scotch.io/@nick>)

Follow @whatnicktweets

2,501 followers

Easiest Local Dev Environment

Get Started with Vue.js



# scotch

Top shelf learning. Informative tutorials explaining the code **and the choices behind it all.**



(<https://github.com/scotch->

(<https://twitter.com/scotchdevelopment>)

FAQ  
(/faq)

Privacy  
(/privacy)

Terms  
(/terms)

Rules  
(/rules)

Hosted by Digital Ocean  
(<https://m.do.co/c/7a59e9361ab7>)

1853-2018 © Scotch.io, LLC. All Rights Super Duper Reserved.