



NodeJS

SECURITY CONFIGURATION

This lesson is a small one, but it is *incredibly important*. Now that we are dealing with Authentication, sessions, cookies and user passwords, it is crucial that we do everything we can so that our authentication system or databases are not compromised.

Learning Outcomes

By the end of this lesson, you should be able to do the following:

- Access environment variables using the `process` object in node.
- Use dotenv to store and make environment variables available to your application globally.
- Describe how environment variables are handled in version control.
- Have familiarity with `nconf`'s hierarchical configuration.

Essentially, in addition to using encryption to secure user passwords we need to make sure that important sensitive information such as our `express.sessions` secret, our `mongoDB` url (especially if it includes your username and password!) and any API keys that you might be using stay hidden. Details such as these should never get committed to a git repo or otherwise published.

Hiding secrets is easily accomplished and there are a handful of ways to do it. One of the most common is using an npm package called `dotenv`. It's usage is simple. Simply create a file called `.env` in your project directory and fill it with variables that represent things you need to keep secret. **Important note:** you need to add this file to your `gitignore` so that it does not get committed to git!

A more robust option is the package `nconf`. It can be used in place of, or alongside `dotenv`. Basically, it allows you to define configuration files in multiple ways for ultimate flexibility. For example you could have a `config.js` file that kept all of your secrets, but also add the ability to override one of those secrets with a command-line argument.

Digging into this package can be useful when creating bigger projects where app configuration needs to be a little more involved. This package makes it easy to configure things such as separate production and development databases, logging and debugging options or anything else.

Assignment



1. The main important takeaway here is to KEEP YOUR SECRETS SECRET by never accidentally publishing them.
2. Read through the documentation for [dotenv](#) and [nconf](#). There are other ways to go about hiding your secrets, but these two projects are popular and widely used.
3. Go back to your earlier projects and SECURE THEM!

[View Course](#)

[Login to track progress](#)

[Next Lesson](#)

 [Improve this lesson on GitHub](#)

Have a question?

Chat with our friendly Odin community in our Discord chatrooms!

[Open Discord](#)

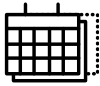
Are you interested in accelerating your web
development learning experience?

[Get started](#)





Thinkful



5-6 months



Job Guarantee



1-on-1 Mentorship



THE ODIN PROJECT



About
FAQ
Blog

Success Stories
Contribute
Terms of Use

