



Curso de Back-End con Node.js (Inicial)

Clase 10



Temario



Temario

- Autenticación.
- Autorización.
- ¿Cómo guardar contraseñas?
- Cookies y Sesiones.
- Passport.js.



Autenticación



Autenticación (1/2)

Es el **proceso** que determina si **alguien** (o algo) **es efectivamente quien dice ser quien es**. En el ámbito web, esto se traduce a un sistema de login de usuarios.

Para implementar un sistema de autenticación en una aplicación se necesita:

- a. Rutas y vistas que muestran los formularios de **registro** y **login** de usuarios.
- b. Método encargado de procesar el registro de usuarios (*handler* de las rutas anteriores).
- c. Método encargado de validar un email y password (*handler* de las rutas anteriores).
- d. Método encargado de “**proteger**” una **ruta**, es decir, inhabilitarla para usuarios que no han hecho login. Por ejemplo, las rutas que empiecen con `/admin` sólo deberían estar disponibles para usuarios logueados.
- e. Además se debe: **hashear** (**≈encriptar**) **contraseñas**, gestionar sesiones, crear migraciones para la base de datos...

En fin, no es una tarea sencilla y además se debe repetir para cada proyecto que requiera autenticación. Por suerte hay herramientas que simplifican la tarea.



Autenticación (2/2)

Recordemos que la **seguridad** es uno de los atributos de calidad que solemos buscar en todo sitio web o aplicación, pero según el tipo de aplicación podemos darle más o menos prioridad a la seguridad. Por ejemplo, un banco no requiere el mismo tipo de seguridad que un juego como “El Solitario”.

En caso de ser necesario, se pueden agregar mecanismos adicionales de seguridad como:

- Two-factor Authentication ([link](#)) usando, por ejemplo:
 - Token físico (digital).
 - Token físico (analógico). Ej: “Tarjeta de coordenadas” de Banco Santander.
 - SMS de verificación.
- Cambios periódicos de contraseña (algo muy debatible).
- Control de direcciones IP.

En cualquier caso, siempre usen **HTTPS**.



Autorización



Autorización

Es el proceso que determina **a qué recursos puede acceder** determinado usuario.

Este proceso ocurre luego de que el sistema haya podido autenticar al usuario.


Un típico ejemplo de autorización es definir distintos tipos de **roles** que pueden tener los usuarios de una aplicación como, por ejemplo: lector, editor, administrador, etc. Luego, según el rol del usuario, el sistema determina a qué datos puede acceder y cuáles puede modificar.



¿Cómo guardar contraseñas?



¿Cómo guardar contraseñas? (1/2)

-  Las contraseñas en una base de datos jamás se deben guardar como “texto plano”. ¡Sería un problema de seguridad enorme!
- Las contraseñas se deben encriptar o, mejor aún, *hashear*.
- La encriptación tienen un método inverso llamado desenscriptación. Para esto existe una “llave” o “clave” de encriptación y desenscriptación. Si bien guardar una contraseña encriptada es mejor que guardarla como texto plano, el hecho de que se pueda desenscriptar es peligroso.
- Las *funciones de hash* no requieren de una clave y no tienen una función inversa. Una vez que una contraseña es *hasheada*, no se puede volver para atrás.
- Cuando un usuario quiera loguearse a una aplicación, deberá ingresar su contraseña (texto plano). El sistema la *hashear*á y la comparará con el *hash* guardado en la BD.



¿Cómo guardar contraseñas? (2/2)

Existen varias funciones de hash disponibles, algunas son:

- MD5.
- SHA (SHA-1, SHA-256, SHA-512).
- BCrypt.

MD5 es una función de *hash* muy rápida. Es decir, una PC común y corriente puede calcular millones de hashes por segundo. Por lo tanto, no es recomendable su uso para contraseñas. En cambio, **BCrypt** es mucho más complejo y una PC demora mucho más en generar los hashes. Además, si la tecnología avanza y las PC se hacen más rápidas, BCrypt se puede configurar (de una forma muy sencilla) para complejizarse mucho más.

👉 La recomendación es usar **BCrypt** ([link](#)) y hay un [paquete en npm](#) para ello. ⚠ Si ese paquete no les anda (muy probablemente en Windows), prueben con [este otro](#).



Cookies y Sesiones



Cookies 🍪 (1/3)

- Son pequeñas cantidades de **datos** que un sitio web guarda (y luego lee) en el **navegador** de un usuario (generalmente sin que éste lo sepa).
- Fueron diseñadas para que un sitio pueda guardar información relativa al “estado” de una aplicación. Por ejemplo, para guardar:
 - Items en un carrito de compras (mientras el usuario navega).
 - Datos del navegante como nombre, email, dirección, etc. (aunque no muy común).
 - Preferencias del navegante como colores o *layout* de una página. Ej: dark/light themes.
 - Páginas visitadas por un navegante (*tracking cookies*).
- Están asociadas a un dominio. Por lo tanto, un sitio web “A” no puede acceder a las cookies guardadas por un sitio web “B”.
- En cada *request*, el navegador adjunta las cookies existentes en los *headers*.



Cookies 🍪 (2/3)

Otro de los usos más comunes para cookies es para guardar algún dato que permita **determinar si el navegante es un usuario logueado** en el sitio. De lo contrario, sería necesario pedirle al navegante que ingrese sus credenciales cada vez que quiera acceder a una página privada.

A este tipo de cookies generalmente se las conoce como ***authentication cookies***.



Cookies 🍪 (3/3)

¿Qué dato podríamos guardar en una *authentication cookie*? 🤔 Deberíamos guardar algún dato que permita identificar al usuario.

Claramente no podemos guardar las credenciales sin encriptar, pero aunque lo hiciésemos, se daría el siguiente problema: si para cada *request* se debe enviar el username y password (encriptados), del lado del servidor habría que desencriptarlos y validarlos contra la BD... es decir, habría que acceder a la BD para cada *request*, lo cual es poco eficiente 🐢 (aunque es común hacerlo).

Lo mejor suele ser guardar un *token* 🎉 (en una cookie), que no es más que un string con ciertos datos, que le permita al servidor identificar al usuario, idealmente sin necesidad de hacer consultas a la BD.



Sesiones (1/2)

Generalmente le decimos sesión al **intervalo de tiempo** mientras que un usuario permanece **logueado** en un sitio web.

La sesión comienza cuando el usuario se loguea en la aplicación. Aquí es cuando se crea la **authentication cookie**. La sesión se identifica con un **Session Id** y esto es lo que se suele guardar en la cookie. No se utiliza el User Id porque el usuario podría estar logueado en más de un equipo y, por lo tanto, tener **más de una sesión abierta**.

La sesión termina cuando el usuario se desloguea o cuando haya pasado determinada cantidad de tiempo. Para este último caso decimos que la sesión expiró. Aquí es cuando la cookie se destruye.



Sesiones (2/2)

- Notar que HTTP es un protocolo *stateless* (sin estado). No hay realmente una “sesión” o “conexión permanente” entre el cliente y el servidor. Es más que nada una “ilusión” que se logra guardando datos de la sesión en el cliente y/o en el servidor.
- En el servidor, los datos de la sesión se pueden guardar en memoria RAM, en un archivo o en una base de datos.
- Notar que cuando se trabaja con Web APIs no hay *cookies* ya que no necesariamente hay un navegador en el proceso. Para cada llamado a la API es necesario adjuntar las credenciales de autenticación (contraseña o *token*).



Repaso de Middlewares

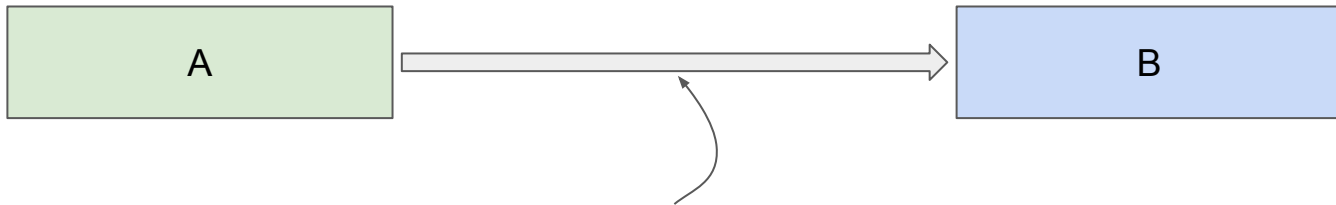


Repaso de Middlewares (1/4)

En el ambiente de Express se habla mucho de *middlewares*, aunque no es un concepto exclusivo de Express y probablemente hayan oído hablar de *middlewares* en otros ámbitos.

Como dice el nombre, el *middleware* es un “pedazo de código” que se ejecuta en medio de una comunicación, con el fin de agregar cierta funcionalidad en el proceso.

Ejemplo, un sistema A le quiere enviar datos a un sistema B:



Podríamos crear un *middleware* que se “meta” en medio de esa comunicación con el fin de, por ejemplo, manipular los datos que están siendo enviados. Por ejemplo, podríamos hacer una corrección ortográfica de los datos. Y podríamos “encadenar” otros *middlewares*.



Repaso de Middlewares (2/4)

En Express, un *middleware* es una **función** que recibe **tres parámetros**:

1. Objeto Request: `req`.
2. Objeto Response: `res`.
3. Función `next`.

La función *middleware* puede hacer una o varias de las siguientes acciones:

- Ejecutar cierto código (en principio, cualquier código).
- Hacer modificaciones sobre los objetos *Request* y *Response*.
- Finalizar el ciclo de *request-response*.
- Llamar al próximo *middleware* que hay para ejecutar.



Repaso de Middlewares (3/4)

Express ya viene con una serie de [middlewares integrados](#) que podemos usar.

Por ejemplo:

- [express.static](#) para servir archivos estáticos como imágenes, CSS, etc.
- [express.json](#) para *parsear requests* que vienen con contenido de tipo JSON.
- [express.urlencoded](#) para *parsear requests* que vienen con contenido de tipo URL-Encoded (como cuando nos están enviando datos que vienen desde un formulario).

👉 Definición: “Parsear” significa analizar un texto sintácticamente y convertirlo en otra estructura como, por ejemplo, un objeto. Un servidor, cuando recibe un *request* con contenido, recibe simplemente un texto, una cadena de caracteres. Por lo tanto hay que indicarle a Express cómo queremos *parsear* dicho texto.



Repaso de Middlewares (4/4)

Ejemplo de uso:

```
const express = require("express");  
const app = express();  
  
app.use(express.urlencoded({ extended: true }));
```

Con este código le estamos diciendo a Express que cuando lleguen datos de tipo “URL-Encoded” se debe crear un atributo `body` dentro del objeto *request*:

```
req.body
```



Passport.js

⚠ Passport.js es una librería cuya documentación requiere una lectura en detalle. Las siguientes diapositivas son sólo un pequeño resumen.



Passport.js (1/12)

Es un *middleware de autenticación* para Node.js. Su único objetivo es autenticar *requests*.

Es flexible, modular (fácil de agregar a nuestra aplicación) y soportar varias “*estrategias*” de autenticación como username/password (“local”), Facebook, Twitter y más.

Documentación: <http://www.passportjs.org>.

Instalación:

```
npm i passport
```




Passport.js (2/12)

Para usar Passport con **username/password**, es necesario instalar este otro [paquete](#):

```
npm i passport-local
```

Además, será necesario instalar un [paquete](#) para gestionar sesiones:

```
npm i express-session
```

Notar que este paquete es totalmente independiente de Passport.
Será el encargado de crear la cookie de autenticación.



Passport.js (3/12)

Luego, requerimos los módulos antes instalados:

```
const session = require("express-session");  
  
const passport = require("passport");  
  
const LocalStrategy = require("passport-local").Strategy;
```



Passport.js (4/12)

Hay que decirle a Express que utilice el *middleware* `session`:

```
app.use(  
  session({  
    secret: "AlgúnTextoSuperSecreto",  
    resave: false, // Docs: "The default value is true, but using the default has been deprecated".  
    saveUninitialized: false, // Docs: "The default value is true, but using the default has been deprecated".  
  })  
);
```

Por detalles sobre las opciones de configuración, consultar la documentación de [express-session](#). Por ejemplo, se puede definir una **fecha de expiración** para la sesión. También se puede definir una **store** (donde se guardará la sesión en el servidor). Por defecto, se usa la `MemoryStore` (la memoria RAM del servidor).

Además, recordar que este middleware es independiente de Passport.



Passport.js (5/12)

Es necesario especificarle a Express que utilice **Passport** con el siguiente *middleware*. Esto se utiliza para “inicializar” a Passport.

```
app.use(passport.initialize());
```

Además, dado que usaremos sesiones, también es necesario usar el siguiente *middleware*. Es importante que esto se ejecute luego del *middleware* `session` de la diapositiva anterior.

```
app.use(passport.session());
```



Passport.js (6/12)

Es necesario especificarle a Passport la **estrategia** que usaremos. Por ejemplo, para usar login con username/password usamos la “**Estrategia Local**” que habíamos importado previamente:

```
passport.use(new LocalStrategy(  
  // Hay varias opciones de configuración  
  // que se pueden consultar aquí.  
  // Ver la documentación de Passport por detalles.  
));
```

Se tiene que especificar por lo menos una estrategia, pero se podrían haber especificado adicionales.



Passport.js (7/12)

⚠ Nota importante: El código de ejemplo de la documentación respecto a la Estrategia Local es sólo eso, un ejemplo. No se debe copiar de forma literal.

```
passport.use(new LocalStrategy(function (username, password, done) {
  User.findOne({ username: username }, function (err, user) {
    if (err) {
      return done(err);
    }
    if (!user) {
      return done(null, false, { message: "Incorrect username." });
    }
    if (!user.validPassword(password)) {
      return done(null, false, { message: "Incorrect password." });
    }
    return done(null, user);
  });
}));
```

Ejemplos:

- La sintaxis del método `findOne` no es válida en Sequelize (falta el atributo `where`).
- El atributo `username` podría no existir en el modelo `User`. Podría ser `email` u otro dato.
- El método `validPassword` no existe en Sequelize (aunque se puede crear “a mano”).
- No obligatorio dar mensajes de error diferenciados para la contraseña y el nombre de usuario. Podría ser un único mensaje con el texto: “*Credenciales incorrectas*”.



Passport.js (8/12)

Luego, es necesario especificarle a Passport **qué** es lo que debe **guardar en la sesión** de autenticación. Lo más común en estos casos es guardar el `id` del usuario.

A su vez, hay que especificarle a Passport **qué** debe **hacer cuando recibe la cookie**.

```
passport.serializeUser(function (user, done) {
  done(null, user.id);
});

passport.deserializeUser(function (id, done) {
  User.findById(id)
    .then((user) => {
      done(null, user); // Usuario queda disponible en req.user.
    })
    .catch((error) => {
      done(error, user);
    });
});
```

Los métodos `serializeUser` y `deserializeUser` son propios de Passport. También la función `done`.

En este ejemplo se está usando Sequelize (y su método `findById`) para determinar si el `id` que contiene la *cookie* corresponde a un usuario válido. Pero también se podría haber usado otro método, o ni siquiera haber usado Sequelize. Notar que en la documentación oficial, el ejemplo se realiza con un método llamado `findById` (que no existe en Sequelize pero sí en otros ORM).

⚠ El usuario obtenido de la base de datos, queda disponible dentro del objeto `req.user`.



Passport.js (9/12)

Una vez que Passport esté configurado, quedan dos puntos por definir:

- Proceso de login/registro.
 - Rutas de login y registro. Ej: `/login` y `/register`. Son dos GET y dos POST.
 - Vistas de login y registro (los formularios).
 - Controlador de login y registro. Ej: `authController.js`. Esto es opcional, aunque recomendable.
- Rutas que debe quedar protegidas (privadas).

Ej: todas las rutas relativas al Admin deben estar privadas. El resto, públicas.



Passport.js (10/12)

Gracias a Passport, el *handler* de la ruta [POST] `/login` queda muy sencillo:

```
app.post("/login",  
  passport.authenticate("local", {  
    successRedirect: "/admin",  
    failureRedirect: "/login",  
  })  
);
```

No es necesario crear un *handler* “a mano”.



Passport.js (11/12)

Ejemplo de *handler* para la ruta [POST] `/register`

```
app.post("/register", async (req, res) => {  
  const [user, created] = await User.findOrCreate({  
    // Ver opciones en Sequelize.  
  });  
  if (created) {  
    req.login(user, () => res.redirect("/admin"));  
  } else {  
    res.redirect("back");  
  }  
});
```

Este código es simplemente un ejemplo o guía para implementar el *handler*. En caso de no haber usado Sequelize, el código naturalmente sería diferente. Del mismo modo, las páginas a donde se quiera redirigir al usuario pueden ser distintas.



Passport.js (12/12)

Para proteger un *handler*, es necesario usar el método `isAuthenticated`.

```
app.get("/admin", (req, res) => {  
  if (req.isAuthenticated()) {  
    res.render("admin");  
  } else {  
    res.redirect("/login");  
  }  
});
```

Curiosamente, este método no está en la documentación oficial, 🤖 al menos a octubre de 2021. Ver [issue](#) en GitHub.

👉 Dado que sería engorroso hacer esta validación dentro de cada *handler*, se recomienda crear un [middleware](#) que se encargue de la misma. Luego asignar dicho *middleware* a las rutas correspondientes.



Ejercicio 1

Ejercicio 1

1. Crear una página de **registro** de usuarios. El formulario debe contener:
 - a. Nombre.
 - b. Apellido.
 - c. Email.
 - d. Contraseña.
2. Crear una página de **login** (con **email** y **contraseña**).
3. Crear una página **privada** (a la cual sólo podrán acceder usuarios autenticados). Si un usuario no *logueado* intenta entrar a esta página, se lo deberá redirigir a la página de *login*.

Usar las siguientes diapositivas como referencia.

Ejercicio 1 (cont)

A screenshot of a web browser window. The browser's address bar shows the URL 'http://localhost:3000/register'. The page title is 'Hack Academy'. The main content is a registration form titled 'Registro'. The form contains four input fields: 'Nombre' (Name), 'Apellido' (Last name), 'E-mail', and 'Contraseña' (Password). Each field has a placeholder text: 'Ingresar nombre...', 'Ingresar apellido...', 'Ingresar correo electrónico...', and 'Ingresar contraseña...' respectively. Below the input fields is a green button labeled 'Iniciar sesión' (Log in).

Registro

Nombre

Ingresar nombre...

Apellido

Ingresar apellido...

E-mail

Ingresar correo electrónico...

Contraseña

Ingresar contraseña...

Iniciar sesión

Ejercicio 1 (cont)

A screenshot of a web browser window. The browser's address bar shows the URL 'http://localhost:3000/login'. The page title is 'Hack Academy'. The main content is a login form titled 'Iniciar sesión'. It contains two input fields: 'E-mail' with the placeholder text 'Ingresar correo electrónico...' and 'Contraseña' with the placeholder text 'Ingresar contraseña...'. Below these fields is a green button labeled 'Iniciar sesión'. At the bottom of the form, there is a link that says '¿Aún no tienes una cuenta? [Regístrate aquí.](#)'.

Iniciar sesión

E-mail

Ingresar correo electrónico...

Contraseña

Ingresar contraseña...

Iniciar sesión

¿Aún no tienes una cuenta? [Regístrate aquí.](#)

Ejercicio 1 (cont)

A screenshot of a web browser window. The browser's address bar shows 'http://localhost:3000/login'. The page title is 'Hack Academy'. The main content is a login form titled 'Iniciar sesión'. At the top of the form, there is a red error message: 'Credenciales incorrectas'. Below this, there are two input fields: 'E-mail' with the placeholder text 'Ingresar correo electrónico...' and 'Contraseña' with the placeholder text 'Ingresar contraseña...'. At the bottom of the form is a green button labeled 'Iniciar sesión'. Below the button, there is a link that says '¿Aún no tienes una cuenta? [Regístrate aquí.](#)'.

Hack Academy

← → ↻ http://localhost:3000/login

☆ 6 Incognito

Iniciar sesión

Credenciales incorrectas

E-mail

Contraseña

Iniciar sesión

¿Aún no tienes una cuenta? [Regístrate aquí.](#)

Ejercicio 1 (cont)

