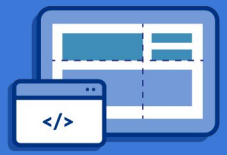
Clase 08. Seguridad II

JavaScript y Node.js



coderhouse

Objetivos de la clase

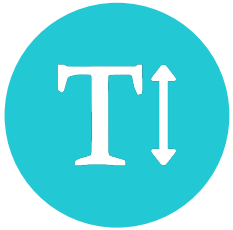
REPASO

Diferentes tipos de ataque

OAuth

Files + submit a package

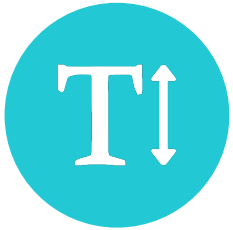
OAUTH



Environment Variables

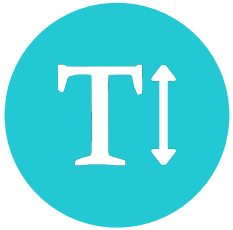
- process.env.PORT
- https://www.npmjs.com/package/dotenv

Seguridad



Conoce la aplicación

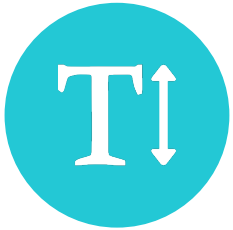
- ¿Como se deberia comportar?
- ¿Cual es el input?
- ¿Cual es el output?



Cross-site scripting XSS

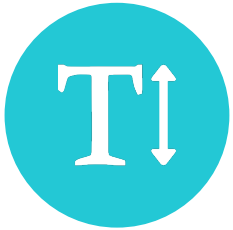
- Validar y Sanitiza todo (express-validator)
- Encripta el output (helmet)

Cross-site request forgery fuerza al usuario a ejecutar acciones indeseadas



CSRF

- Agregar token randoms e impredecibles en los request
- csurf

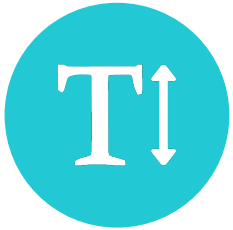


Session Managment

- Token TIENEN que expirar
- Recrear tokens despues de login
- Usar HTTPS
- Usar permisos (node_acl, passport)

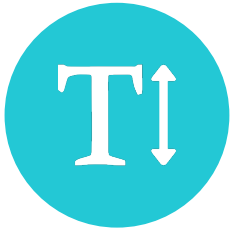
En el año 2012 Linkedin fue hackeado y mas de 6.5 millones de contraseñas fueron comprometidas

https://www.linkedin.com/pulse/linkedin-hack-understanding-why-so-easy-crack-tyler-cohen-wood/



Password

- Usar BCRYPT
- 2FT Speakeasy,Authy,Yubico o sms



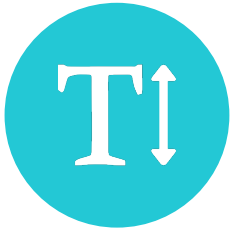
Cookies

- Tienen que expirar
- Packages: Cookies-session, cookies, keygrip

“Use strict” elimina errores silenciosos (Object.freeze)

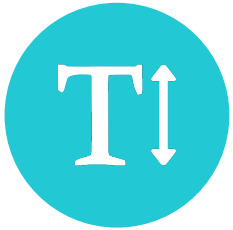
Valida tus packages de Typosquatting

https://www.theregister.co.uk/2017/08/02/typosquatting_npm/



Package validation

- retire.js
- https://github.com/nodesecurity/nsp



Documentation

- swagger
- apidoc.js

Limita tus archivos con MULTER

Subir archivos a npm con un index.js

https://docs.npmjs.com/getting-started/publishing-npm-packages

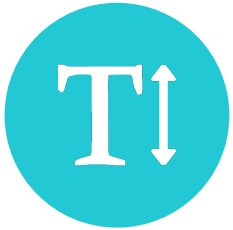
OAUTH

Crear y testear una API segura

Ejercicio

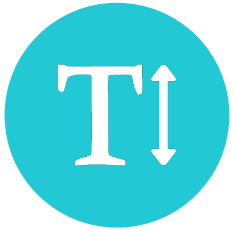
1. Login con Normal y con FB usando FB-TOKEN
2. Usar todos los metodos de seguridad vistos
3. Subir imagen si es el usuario creador
4. Todos los usuarios logueados pueden ver la imagen
5. Usar todos los metodos de seguridad vistos

REPASO



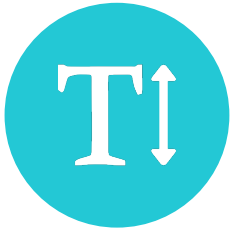
Clase 1

- Eventos
- Programacion funcional
- Linters y manejo de archivos



Clase 2

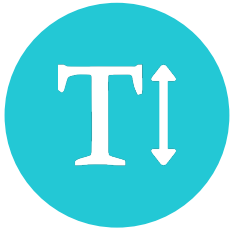
- Async
- Streams
- Http y express



Clase 3

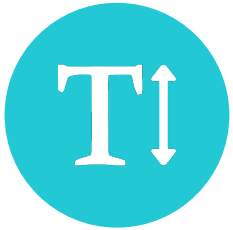
Routes como hacer

- Middleware
- Error handler
- APIS buenas practicas



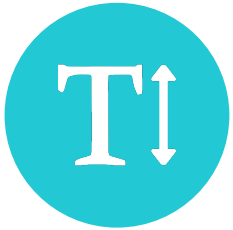
Clase 4

- Como crear una API de 0 con express (TODO)



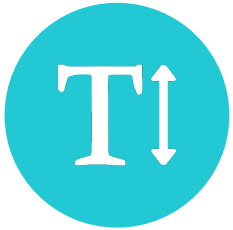
Clase 5

- Mongo vs SQL
- Mongoose
- Modelos



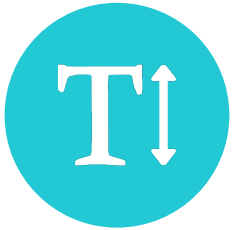
Clase 6

- Workshop de mongoose. Pinterest



Clase 7

- Authentication
- Passport y validation
- Modelos

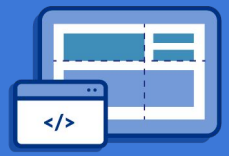


Clase 8

- OAUTH, 2fA
- Seguridad
- Ultimo ejercicio

¿Preguntas?

¡GRACIAS POR ESTUDIAR CON NOSOTROS!



coderhouse