2022 부트캠프 037

- Authentication / Environment Variable(환경변수): dotenv / Hash(해시): MD5

!Tips & Links

※ 강의 https://www.udemy.com/course/the-complete-web-development-bootcamp/

※ plain text offenders https://plaintextoffenders.com/ ※ THE CODE BOOK by Simon Singh

※ SplashData https://en.wikipedia.org/wiki/List_of_the_most_common_passwords#SplashData ※ https://haveibeenpwned.com/

※ gitignore 템플릿 파일 ☞ https://github.com/github/gitignore (Node.gitignore 사용)

git GUI => CLI 익숙해지기	git add . / git commit –m "메시지" / git push –u ~~

---

dotenv: 환경변수 패키지 / https://www.npmjs.com/package/dotenv

(process.env.~~) zero-dependency module, loads environment variables / .env의 process.env.~

install init	npm i dotenv (recommend to install locally) 최상단 **require("dotenv").config();** // 환경변수를 설정		
touch .env	SECRET=~~~~ API_KEY=e0e0e0~	규칙 rules	CAPITALIZE, snake_case no const, no space between equal sign no "quotation mark", no semicolon;
사용법	process.env.SECRET process.env.API_KEY	=> .env에 있는 환경변수를 가져옴 선 require("dontenv").config() 必	

Environment Variables: API Key, encryption Key등 유출되어 악용될 수 있음 ☞ .env에 담아서 ignore함

(환경변수) (heroku 등에 업로드 할 때 Config Var는 비공개로 관리한다.)

인증 레벨		
level 3	Hashing Password 해시로 변환	데이터 자체를 해시로 만들어 DB에 저장한다. 해시는 Decode 어려움(시간이 많이 걸림)
		☞ 클라이언트가 입력한 정보를 알아볼 수 없는 형태로 저장한다. 자주 사용하거나, 단순한 값 등은 해시테이블을 사용해 쉽게 해킹된다.

암호화 Encryption	유저데이터 + 키key =(암호화 알고리즘cipher method)=> 암호화 된 텍스트
해시 Hash Function	유저데이터 =(해시 함수Hash Function)=> 해시값 Hash

md5: 해시 패키지 / https://www.npmjs.com/package/md5

(md5(~~)) MD5로 메시지를 해싱해주는 자바스크립트 함수

install init	npm i md5 const md5=require("md5");

사용법:
function
	md5(~~~);로 사용한다. // 같은 값은 MD5 해시가 같음
	ex) 1111은 항상 ==b59c67bf196a4758191e42f76670ceba이다.

※ Hash Table이란?: dictionary, common password등 유추 가능한 해시값을 모은 테이블

(지금 GPU로 1s에 200억개 MD5 해시 생성가능 ~> 점차 취약해지고 있다.)

/* -----<lang: en>---------- */

keep your secrets off of the Internet! // a pane 창 // decided to plot

hash functions are mathematical equations // (someone) digress means => out of subject, rambling