2022 부트캠프 036

- 인증 Authentication / mongoose-encryption

!Tips & Links

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

※ 암호복호 https://cryptii.com/

※ mongoose-encryption https://www.npmjs.com/package/mongoose-encryption

※ localhost:3000는 nodemon / 127.0.0.1은 mongod => mongoose.connet()

※ **mongodb://127.0.0.1:127017/DB**

app setting	init, i	npm init –y, npm I express ejs body-parser mongoose

	use
	set
		app.use(express.static("public"));
		app.set('view engine', 'ejs');
		app.use(bodyParser.urlencoded({ extended: true }));

	db	mongoose.connet("mongodb://127.0.0.1:27017/DB") // 새 DB연결
		const userSchema = new mongoose.Schema{ ~~ } // 스키마설정
		const User = new mongoose.model("User", userSchema) // 새 모델(컬렉션, 스키마)

Authentication: 보안(인증 Authentication, 권한부여 Authorization, 계정관리 Accounting)
Create an account (ID card), Restrict access

mongoose-encryption: mongoose의 암호화 패키지(상단 doc참고) / AES 암호화 알고리즘 사용, 모던 (encryption Key/assigning Key 사용, 또는 secret=long string을 Key로 사용)

☞ plug-in 사용하므로 스키마는 new mongoose.Schema({}) 써야함(그냥 객체no)

☞ 모델을 save & find할 때 자동으로 encrypt it & decrypt it

Install	npm i mongoose-encryption
Require	const encrypt = require("mongoose-encryption");
Schema Secret Plug-in	const 스키마 = new mongoose.Schema({ ~~ }); const secret = "~~~~~~~~~~(길이 무관 long string)"; 스키마.**plugin** (encrypt, {secret: secret, **encryptedField**: ["password"]}); const 모델 = new mongoose.model("모델", 스키마); ※ encryptedField가 여러 개일 경우 배열 => ["~~", "~~"]

인증 레벨		
level 1	use Email & Password 유저를 register	secrets.ejs는 /주소로 들어갈 수 없음 register 또는 login 페이지에서 POST의 res.render로만 접속한다.
		☞ password가 plain text이므로 보안에 굉장히 취약하다. just storing the password as plain text in DB
level 2	Encryption DB 암호화	mongoose-encryption을 사용해 데이터를 암호화(long string KEY)
		☞ password가 DB에 binary string으로 저장됨. long string KEY(const secret)를 찾으면 쉽게 데이터를 해독할 수 있다.

/* -----<lang: en>---------- */
OAuth? // consistent with industry standards of security of website // specify the values **for** the fields.
Enigma machine / Bletchley Park: computer museum
Caesar Cipher=> Simplest form of encryption / shift x n alphabet