Surfaces d'attaque	Securisations possible	Mécanismes de sécurité	Principes de sécurité
Docker	dotenv	Gestion des erreurs	Défense en profondeur
	Maj des Images docker	Gestion des erreurs	Minimiser la surface d'attaque, Défense en profondeur, Corriger pb de sécu de manière pérenne
Web	limiter la taille des requetes	Gestion des erreurs	Minimiser la surface d'attaque, KISS
	cacher les urls des requetes (ex : paramètres, ...)	Chiffrement	Minimiser la surface d'attaque, KISS
	mettre le projet à jour avec les dernières sécurités des navigateurs	Gestion des erreurs	Minimiser la surface d'attaque, Corriger pb de sécu de manière pérenne
Spring-boot	obfusquer le code pour decourager les kiddos	Chiffrement	Défense en profondeur
	bloquer les connections inconnus	Authentification, Permission	Principe de moindre confiance
	proteger les champs d'entrées (email, mot de passe, etc..)	Validation de données	Minimiser la surface d'attaque, Défense en profondeur, Gestion sûre des erreurs
BDD	chiffrer les mots de passe	Chiffrement	Défense en profondeur
Get	enlever l'affichage des Id dans la réponse de la requête	Chiffrement	Principe de moindre privilège, sécurité par l'obscurité
	afficher seulement ce qui est utile en fonction de qui utilise	Authentification, Permission	Principe de moindre privilège, sécurité par l'obscurité
Post	pas de sécurité sur la personne qui fait la requête	Authentification, Permission	Principe de moindre confiance
	pas de vérification des paramètres	Validation de données	Minimiser la surface d'attaque, Gestion sûre des erreurs
Put	pas de sécurité sur la personne qui fait la requête	Authentification, Permission	Principe de moindre confiance
	pas de vérification des paramètres	Validation de données	Minimiser la surface d'attaque, Gestion sûre des erreurs
Delete	pas de sécurité sur la personne qui fait la requête	Authentification, Permission	Principe de moindre confiance