BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions logicielles et applications métiers

U6 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2022

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 20 pages, numérotées de 1/20 à 20/20
(sans compter la page de garde).

Cas Easy2Drive

Ce sujet comporte 20 pages dont un dossier documentaire de 13 pages.
La candidate ou le candidat est invité(e) à vérifier qu'il est en possession d'un sujet complet.

Barème

DOSSIER A	Sécurisation de l'application de formation en ligne (*e-learning*)	30 points
DOSSIER B	Prise en compte des conclusions de l'audit de sécurité	25 points
DOSSIER C	Mise en œuvre de contre-mesures dans la gestion des avis	25 points
	TOTAL	80 points

Dossier documentaire

Présentation du contexte

Easy2Drive est une entreprise de 70 salariés spécialisée dans la conception, le développement et la commercialisation de supports pédagogiques imprimés et digitaux pour la formation aux différentes catégories de permis de conduire (scooter ou voiturette, voiture, moto, remorque, bateau). Elle propose une plateforme *Easy2Drive.fr* à laquelle sont abonnées environ 6 000 auto-écoles réparties sur le territoire français et utilisée par plus de 500 000 élèves.

Techniquement, cette plateforme a été développée dans l'environnement *PHP* et s'appuie sur le système de gestion de base de données (*SGBD*) *MySQL*. C'est une application *Web* composée de deux espaces :

- un espace "Pro" dans lequel les auto-écoles peuvent inscrire leurs élèves et leur affecter un formateur qui suivra leur formation ;
- un espace "*E-learning*" qui permet aux élèves de suivre des cours de code en ligne, de faire des séries de tests d'entraînement et de passer des examens blancs. Pour les élèves rattachés à une auto-école, cet espace leur permet également d'envoyer des messages aux formateurs et d'évaluer leur auto-école.

Ces deux espaces utilisent une même base de données BD_EASY.

Associé à cette plateforme, un site de marché (*marketplace*) référence toutes les auto-écoles partenaires de l'entreprise Easy2Drive, auto-écoles qui peuvent être notées par les élèves.

Le nombre d'auto-écoles utilisant les applications de l'entreprise Easy2Drive augmente chaque année et par la même occasion le nombre d'élèves. De plus, les circonstances sanitaires actuelles ont imposé de nouvelles pratiques qui intensifient encore la transition numérique. Les problématiques de sécurité n'ont jamais été laissées de côté, mais face à cette montée en puissance, Easy2Drive a fait réaliser un audit auprès d'une société externe spécialisée dans la sécurité informatique afin de renforcer la cybersécurité de ses applications informatiques.

La direction des systèmes d'information (DSI) de la société Easy2Drive couvre l'ensemble des services informatiques « métiers » et gère les infrastructures qui les supportent. Elle repose sur une équipe de dix personnes.

Vous accompagnez Mme Clémence Auroux, déléguée à la protection des données (*data protection officer DPO*) pour laquelle vous allez traiter certaines non-conformités révélées par l'audit et mettre en œuvre de nouvelles recommandations en matière de cybersécurité dans le développement de solutions applicatives.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

Dossier A – Sécurisation de l'application de formation en ligne (*e-learning*)

Mission A1 – Évaluation des risques à partir des récits utilisateurs

Le tableau « Besoins de sécurité pour les récits utilisateurs (*user stories*) », établi par la société d'audit, propose pour chaque récit, une évaluation du besoin de disponibilité, d'intégrité et de confidentialité des données manipulées et la nécessité d'éléments de traçabilité faisant office de preuve. Clémence Auroux vous demande d'analyser les niveaux d'importance indiqués par les auditeurs en termes de disponibilité, d'intégrité, de confidentialité et de preuve.

Question A.1.1

a) Justifier la différence de niveau du critère de disponibilité entre les récits utilisateurs 1 et 2.

b) Justifier les niveaux des critères d'intégrité et de confidentialité du récit utilisateur 2.

c) Justifier la différence de niveau en termes de preuve entre les récits utilisateurs 1 et 3.

Mission A2 – Prise en compte du règlement général sur la protection des données (RGPD)

Clémence Auroux vous demande de l'assister dans la vérification des obligations légales en cas de contentieux avec une famille ou un élève.

Question A.2.1

Expliquer en quoi la gestion des témoins de connexion (*cookies*) sur le site ne respecte pas la nouvelle réglementation de septembre 2020.

La famille Lefranc désire s'informer sur les services proposés par la société Easy2Drive et consulte l'espace public de la plateforme pour connaître le fonctionnement de l'espace de formation en ligne (*e-learning*).

Question A.2.2

Indiquer, parmi les données qui seront collectées dans le cadre du récit utilisateur n°1, celle(s) à caractère personnel en justifiant votre réponse.

Mission A3 – Vérification de la sécurité du mot de passe

Actuellement l'auto-école procède à l'inscription d'un nouvel élève qui reçoit alors par courriel son identifiant ainsi que son mot de passe initial. L'élève peut conserver ce mot de passe tout au long de sa formation qui dure en moyenne une année.

L'élève peut également modifier son mot de passe à tout moment. Le nouveau mot de passe est alors validé grâce à une fonction écrite en langage *PHP* appelée *verifPassword*.

L'audit a révélé des failles dans la gestion actuelle des mots de passe et Clémence Auroux vous demande d'y remédier.

Question A.3.1

a) Expliquer en quoi la communication et l'utilisation du mot de passe initial ne sont pas satisfaisantes d'un point de vue sécurité.

b) Proposer une meilleure solution pour communiquer le mot de passe initial.

La fonction *verifPassword* consiste à attribuer des points en fonction de la longueur et de la complexité du mot de passe et vérifie que ce nombre de points correspond à un nombre attendu.

Actuellement un mot de passe est validé si le nombre de points est égal à 6. Clémence Auroux vous demande de faire évoluer cette fonction afin que la validation du mot de passe se fasse à partir d'un nombre de points supérieur ou égal à 10.

Question A.3.2

a) Donner la politique de mot de passe actuellement utilisée en termes de longueur et de complexité en examinant le code de la fonction *verifPassword*.

b) Modifier la fonction *verifPassword* afin que les recommandations de la CNIL soient toutes respectées (écrire uniquement les parties à modifier ou à ajouter).

c) Modifier et compléter la fonction de tests unitaire *testVerifPassword* pour valider cette modification.

Clémence Auroux décide qu'un élève doit renouveler obligatoirement son mot de passe au bout de 3 mois, soit 90 jours. Elle vous charge de mettre en place ce nouveau besoin au niveau de la base de données afin de vérifier, à chaque connexion d'un élève, l'ancienneté de son mot de passe.

Le cahier des charges technique qu'elle vous a fourni indique qu'il faut ajouter dans la table Utilisateur un champ obligatoire *dateMajMDP* initialisé lors de la création d'un compte. Il faudra également écrire une fonction *MySQL renouvelleMDP* qui prendra comme paramètre d'entrée l'identifiant d'un élève et retournera vrai si cet élève n'a pas changé son mot de passe depuis plus de 3 mois ou 90 jours.

Question A.3.3

a) Écrire la requête qui permet d'ajouter le nouveau champ.

b) Écrire la fonction stockée *renouvelleMDP*.

Dossier B – Prise en compte des conclusions de l'audit de sécurité

L'audit externe a révélé un certain nombre de scénarios de risques concernant la base de données. Clémence Auroux vous demande de prendre en charge les deux scénarios considérés comme les plus prioritaires : « attribution abusive de la Garantie Réussite » et « outil de traçage des événements inadaptés ».

Mission B1 - Attribution de la Garantie Réussite

Le premier scénario de risque est le suivant : « Le responsable d'une auto-école fait une fausse déclaration d'échec à l'examen du Code (ou ETG pour épreuve théorique générale) afin qu'un élève bénéficie de la Garantie Réussite ».

Question B.1.1

Identifier la principale conséquence pour Easy2Drive lorsqu'une auto-école fait une déclaration abusive d'échec d'un élève à l'ETG.

Lorsqu'une auto-école enregistre, sur la plateforme, l'échec d'un élève à l'ETG, un déclencheur nommé *check_garantie_reussite* est exécuté dans la base de données afin de contrôler que toutes les conditions sont remplies pour attribuer la Garantie Réussite.

Clémence Auroux vous demande de vérifier et de corriger ce déclencheur (*trigger*) afin de garantir que cette fonctionnalité ne puisse plus faire l'objet de déclarations malveillantes. Pour ce faire, elle vous fournit la liste des conditions de la Garantie Réussite ainsi que le code source du déclencheur correspondant.

Question B.1.2

a) Analyser le corps du déclencheur et repérer les conditions qui ne sont pas ou mal implémentées.

b) Écrire le code source corrigé du déclencheur (uniquement les parties à modifier ou à ajouter).

Mission B2 – Traçage des événements sur les données personnelles

L'audit a mis en lumière que Clémence Auroux, en tant que déléguée à la protection des données (*DPD*), ne disposait pas d'un outil efficace, conforme aux recommandations de la CNIL, pour répondre précisément à des questions d'utilisateurs sur l'usage de leurs données personnelles ou pour détecter d'éventuels comportements ou accès inhabituels.

Elle a travaillé sur une maquette de l'écran principal de la future application « *Logs RGPD* » et, lors d'un entretien, elle vous charge de travailler à l'élaboration d'une nouvelle base de données BD_RGPD_LOGS qui sera interrogée en lecture seule par cette application. Cette base de données sera alimentée en écriture par l'application *Easy2Drive* à chaque événement sur les données personnelles.

Par exemple :

- Samira Ghalam poste un nouveau message depuis l'application *Easy2Drive*. Le message est enregistré dans la base BD_EASY. L'action de création de l'enregistrement n°485685 dans la table Message par cette utilisatrice est journalisée dans la base BD_RGPD_LOGS.
- Fabien Leroux consulte les fiches de ses élèves de la matinée depuis l'application *Easy2Drive*. L'action de consultation des enregistrements n°2348 et n°1685 de la table Eleve par cet utilisateur est journalisée dans la base BD_RGPD_LOGS.

Question B.2.1

Compléter l'ébauche de schéma de la base BD_RGPD_LOGS pour répondre au besoin de la déléguée. Vous pourrez choisir le formalisme de votre choix : diagramme de classes ou schéma entité-association.

Pour garantir une sécurité optimale et ne pas surcharger la plateforme principale, Clémence Auroux souhaite que les événements sur les données personnelles soient enregistrés dans une base de données spécifique (BD_RGPD_LOGS) localisée sur un serveur physique différent. Le nom DNS du serveur *Web* hébergeant le site de l'application est *Easy2Drive.fr*.

Question B.2.2

Rédiger la requête permettant de créer, dans le SGBD *MySQL*, un utilisateur (nommé APPLI_RGPD_LOGS) qui permettra à l'application *Easy2Drive* de se connecter à la base de données BD_RGPD_LOGS.

L'application *Easy2Drive* devra avoir les droits d'écriture sur cette nouvelle base de données.

Pour satisfaire aux recommandations de la CNIL, il a été décidé que cette connexion d'application disposera uniquement de la permission d'ajouter des données dans BD_RGPD_LOGS.

Question B.2.3

Rédiger la requête permettant d'attribuer dans le SGBD *MySQL* la permission nécessaire.

Clémence Auroux insiste sur le fait que ces données devront être impérativement conservées pour une durée limitée. Elle souhaite donc que la purge se fasse automatiquement lorsque le délai est dépassé.

Question B.2.4

a) Proposer une durée de conservation des événements sur les données personnelles conforme aux recommandations de la CNIL.

b) Indiquer dans quel document exigé par le RGPD cette durée devra être consignée.

c) Proposer une solution technique (sans la réaliser) pour purger automatiquement les données de la base de données lorsque le délai de conservation est dépassé.

Dossier C – Mise en œuvre de contre-mesures dans la gestion des avis

Après l'obtention du permis, chaque élève est invité à laisser un avis général sur sa formation via un formulaire disponible dans l'espace d'évaluation de son auto-école, après s'être authentifié.

Cet avis est modéré a posteriori. Cette modération a pour but de s'assurer de la conformité du contenu collecté au droit français pour décider de publier ou non ce contenu.

L'analyse de risque effectuée pendant l'audit externe a mis en évidence des scénarios de risques (*abuser stories*) et des mesures à prévoir. Clémence Auroux vous charge de travailler sur le développement de ces contre-mesures.

Mission C1 – Saisie d'un avis par un élève

Scénario de risque : En tant qu'élève, je peux réécrire mon avis autant de fois que je le veux jusqu'à ce qu'un modérateur le publie.

Mesures à prévoir : Lorsqu'un élève a écrit un avis, il n'a plus accès au formulaire tant que l'avis n'a pas été modéré. Si le contenu de l'avis n'est pas conforme, le modérateur le rejette. L'élève peut alors en écrire un nouveau à partir du formulaire. Si cet avis n'est toujours pas conforme au bout de la troisième réécriture, il recevra un courriel lui indiquant le motif de rejet et n'aura plus la possibilité d'accéder au formulaire. Lorsqu'un avis est conforme, il est publié par un modérateur et sera alors automatiquement affiché sur le site de marché (*marketplace)*.

Question C1.1

Écrire le code de la méthode *getNbMaxAvisAtteint* de la classe Eleve.

Question C1.2

Compléter le code de la méthode *monAvis* du contrôleur AvisEleveController afin que le formulaire ne soit affiché que si l'élève est autorisé à saisir un avis.

L'audit de sécurité a mis en évidence que le champ texte du contenu de l'avis dans le formulaire était vulnérable aux injections en langage SQL :

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	https://eleve.easy2drive.fr/vues/acces_eleve/index.php#!avis
Method	POST
Parameter	txtContenu
Attack	foo-bar@example.com OR 1=1 --

Clémence Auroux vous demande de tester l'injection suivante depuis le compte de l'élève 12 :

```
Quelle incompétence!',now(),true,true,5),('A fuir absolument',now(),true,true,5),
('Accueil froid, moniteurs désagréables',now(),true,true,5), ('Aucun point
positif',now(),true,true,5), ('Choisissez une autre auto-école',now(),true,true,5) ,
('formation OK
```

Question C1.3

a) Indiquer le résultat obtenu dans la base de données après la réussite de cette injection.

b) Expliquer en quoi cette injection contourne les mesures précédemment mises en place.

c) Proposer une solution pour corriger la vulnérabilité détectée (sans la réaliser).

Mission C2 – La modération des avis

Une application *Web* composée d'un tableau de bord est utilisée par les modérateurs. Ce tableau de bord présente les derniers avis émis par les élèves qui n'ont pas encore été modérés.

ID Avis	Elève	Avis élève	nb avis refusés	Neph	Mail	Publier /Rejeter
2	Arkadi Pavel	Rien à dire, formateurs investis	0	✓	✓	✉ STOP
10	Leloup Clara	Rien à dire	0	✓	✓	✉ STOP
17	Naouri Lounis	Nul nul on dirait que les moniteurs n'ont pas le permis !	0	✓	✓	✉ STOP
19	Moreau Leo	Je recommande cette auto-école. Tout est parfait !	0	⚠	✓	✉ STOP
20	Costa Ombeline	Auto-école sérieuse. Equipe au top. Merci!	0	✓	📍	✉ STOP

Scénario de risque : En tant qu'auto-école, je peux créer un nouvel élève qui n'existe pas réellement et utiliser son compte pour émettre de faux avis positifs.

Mesures à prévoir : Les modérateurs doivent pouvoir détecter les avis émis par un élève qui n'existe pas réellement. Pour cela, le tableau de bord des modérateurs doit présenter des critères qui leur permettent de déceler un éventuel faux élève et de procéder dans ce cas à certaines vérifications :

- la présence d'un doublon, 📍, au niveau de l'adresse électronique : dans ce cas, les modérateurs pourront consulter la fiche d'identité des élèves afin de procéder à certaines vérifications (personne unique qui s'est inscrite dans deux auto-écoles différentes pour deux permis différents, adresse électronique des parents donnée pour deux enfants, etc.) ;
- l'absence de numéro NEPH, ⚠ : dans ce cas, les modérateurs pourront vérifier s'il s'agit d'un simple oubli de saisie ou non.

NEPH : numéro d'enregistrement à la préfecture

Question C2.1

Écrire le code de la méthode *getDoublonMail* de la classe PdoEasy2Drive.

Question C2.2

Compléter le code de la méthode *listeAvis* du contrôleur AvisModerateurController afin de transmettre à la vue la variable *$doublonMail* permettant de savoir si l'adresse électronique est en double.

Documents communs à plusieurs dossiers

Document commun 1 : Représentations partielles des traitements de l'application et données de BD_EASY

Remarques : Les parties « test » et « examen blanc » ont été simplifiées, la gestion des messages n'apparait pas.
NEPH : numéro d'enregistrement préfectural harmonisé (nécessaire pour passer le permis de conduire)
ETG : épreuve théorique générale du permis de conduire

Diagramme de classes

Pour simplifier le schéma, toutes les méthodes ne sont pas présentées sur ce diagramme de classes.

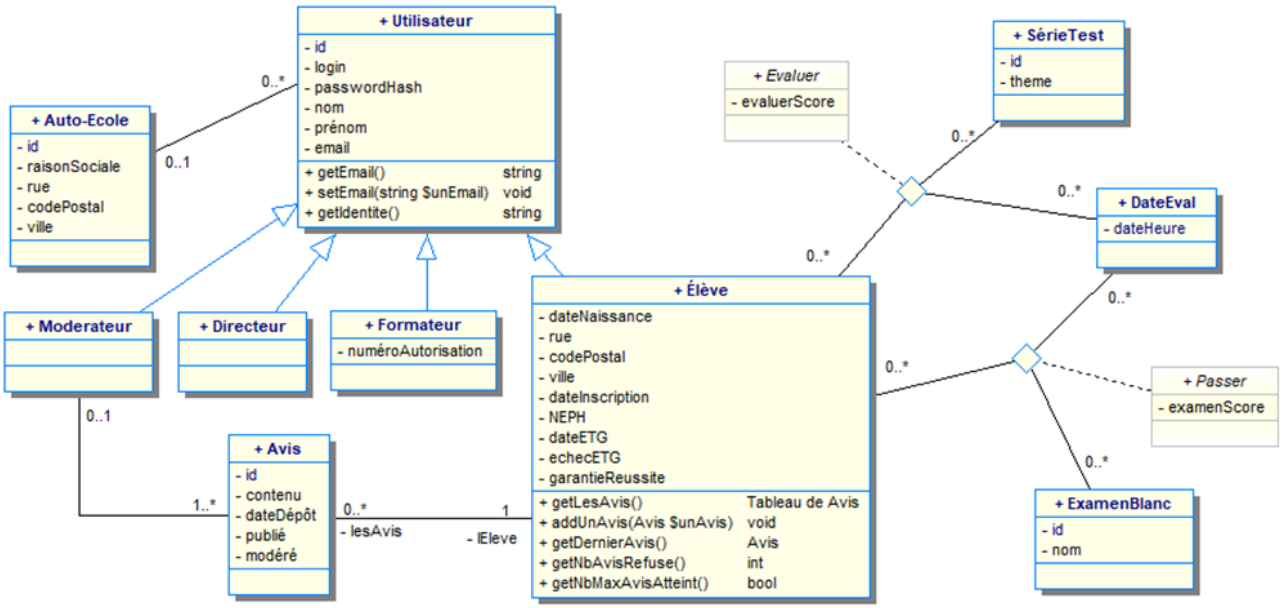


Schéma entité-association

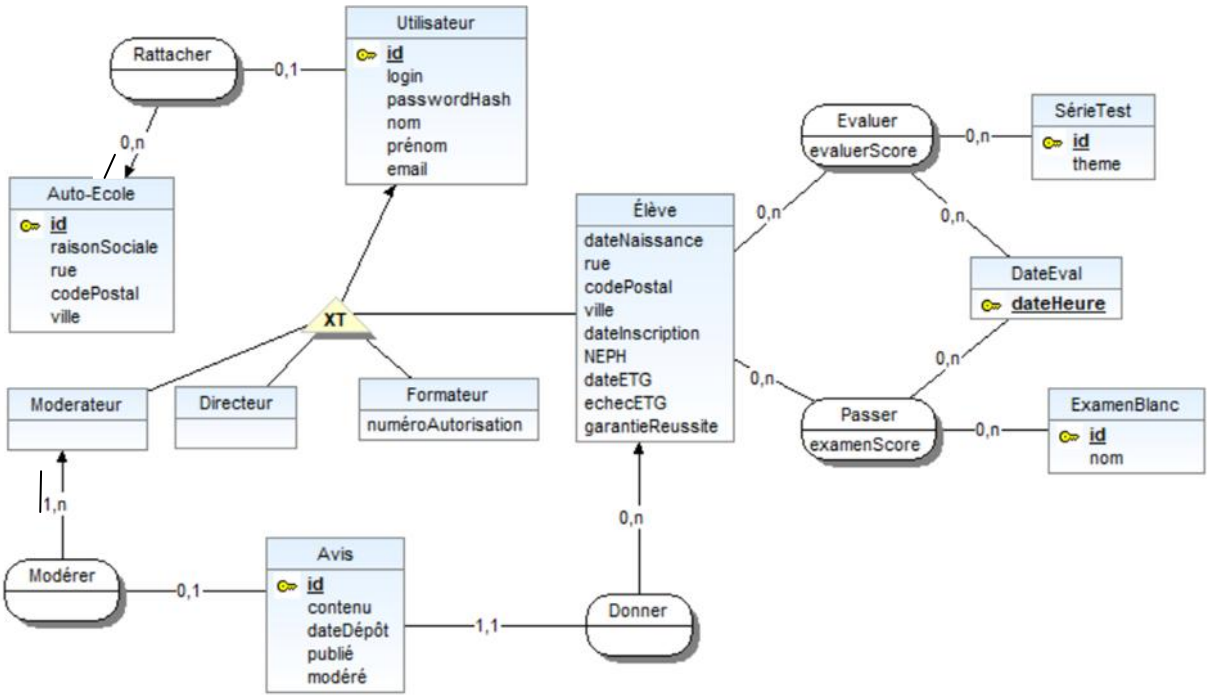


Schéma relationnel

Auto-Ecole (id, raisonSociale, rue, codePostal, ville)
Clé primaire : id

Utilisateur (id, login, passwordHash, nom, prenom, email, idAutoEcole)
Clé primaire : id
Clé étrangère : idAutoEcole en référence à id de AutoEcole

Eleve (idUtilisateur, dateNaissance, rue, codePostal, ville, dateInscription, NEPH, dateETG, echecETG, garantieReussite)
Clé primaire : idUtilisateur
Clé étrangère : idUtilisateur en référence à id de Utilisateur

Moderateur (idUtilisateur)
Clé primaire : idUtilisateur
Clé étrangère : idUtilisateur en référence à id de Utilisateur

Directeur (idUtilisateur)
Clé primaire : idUtilisateur
Clé étrangère : idUtilisateur en référence à id de Utilisateur

Formateur (idUtilisateur, numeroAutorisation)
Clé primaire : idUtilisateur
Clé étrangère : idUtilisateur en référence à id de Utilisateur

Avis (id, contenu, dateDepot, publie, modere, idEleve, idModerateur)
Clé primaire : id
Clé étrangère : idEleve en référence à idUtilisateur de Eleve
Clé étrangère : idModerateur en référence à idUtilisateur de Moderateur

SerieTest (id, theme)
Clé primaire : id

ExamenBlanc (id, nom)
Clé primaire : id

Evaluer (idEleve, idSerieTest, dateHeure, evaluerScore)
Clé primaire : idEleve, idSerieTest, dateHeure
Clés étrangères : idEleve en référence à idUtilisateur de Eleve
idSerieTest en référence à id de SerieTest

Passer (idEleve, idExamenBlanc, dateHeure, examenScore)
Clé primaire : idEleve, idExamenBlanc, dateHeure
Clés étrangères : idEleve en référence à idUtilisateur de Eleve
idExamenBlanc en référence à id de ExamenBlanc

Document commun 2 : extraits de la documentation de MySQL

CURRENT_DATE()

Cette fonction retourne la date courante du système sous le format «*année-mois-jour*».

```
CURRENT_DATE(); -- retourne : 2021-09-10 si nous sommes le 10 septembre 2021
```

DATE_ADD(*date*, INTERVAL *value addunit*)

```
DATE_ADD('2021-09-15', INTERVAL 10 DAY);  -- ajoute 10 jours et retourne  2021-09-25

DATE_ADD('2021-09-15', INTERVAL 1 MONTH); -- ajoute 1 mois et retourne 2021-10-15
```

Exemple d'une fonction stockée

```
CREATE FUNCTION verifieAge(num INT)-- retourne vrai si l'élève dont le numéro est passé en paramètre a plus de 15 ans et peut donc s'inscrire à l'auto-école.
RETURNS Boolean
BEGIN
   DECLARE v_dn DATE;
   DECLARE v_retour BOOLEAN DEFAULT true ;
   select dateNaissance into v_dn from Eleve where idUtilisateur=num;
   IF (DATE_ADD(v_dn, INTERVAL 15 YEAR) > CURRENT_DATE()) THEN
      SET v_retour = false;
   END IF
   RETURN v_retour;
END
```

Création d'un utilisateur

```
CREATE USER 'jeffrey'@'localhost' IDENTIFIED BY 'password'; -- crée un utilisateur 'jeffrey' qui se connecte avec le mot de passe 'password' depuis la machine locale.
```

Attribution de droits à un utilisateur

```
GRANT ALL ON base.table TO 'jeffrey'@'localhost'; -- donne à l'utilisateur 'jeffrey' tous les droits sur la table « table » de la base « base ».
```

Modification de la définition d'une table

```
ALTER TABLE base.table ADD nombre INT NOT NULL DEFAULT 0; -- ajoute un champ nommé « nombre » de type entier à la table « table » dont la valeur par défaut est 0.
```

Documents de la CNIL

Document CNIL 1 : Recommandations de la CNIL pour « L'authentification par mot de passe : les mesures de sécurité élémentaires »

Le mot de passe doit avoir une longueur minimum de 12 caractères et doit satisfaire aux 4 critères suivants pondérés en nombre de points :

- comporter au moins une minuscule (1 point) ;
- comporter au moins une majuscule (2 points) ;
- comporter au moins un chiffre (3 points) ;
- comporter au moins un caractère spécial (4 points).

Document CNIL 2 : Réglementation concernant les témoins de connexion (cookies)

Délibération du 17 septembre 2020 : L'utilisateur doit être clairement informé des objectifs des *cookies*. Le consentement implicite n'est plus accepté et le choix doit être affiché clairement (accepter, refuser ou gérer les *cookies*).

A compter du 1er Avril 2021, les entreprises seront sanctionnées par une amende.

Document CNIL 3 : Sécurité - Tracer les accès et gérer les incidents

Tracer les accès et prévoir des procédures pour gérer les incidents afin de pouvoir réagir en cas de violation de données (atteinte à la confidentialité, l'intégrité ou la disponibilité).

Afin de pouvoir identifier un accès frauduleux ou une utilisation abusive de données personnelles, ou de déterminer l'origine d'un incident, il convient d'enregistrer certaines des actions effectuées sur les systèmes informatiques. Pour ce faire, un dispositif de gestion des traces et des incidents doit être mis en place. Celui-ci doit enregistrer les évènements pertinents et garantir que ces enregistrements ne peuvent être altérés. Dans tous les cas, il ne faut pas conserver ces éléments pendant une durée excessive.

Les précautions élémentaires

- Prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « *logs* ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité.
    - Ces journaux doivent conserver les évènements sur une période glissante ne pouvant excéder six mois (sauf obligation légale, ou risque particulièrement important).
    - La journalisation doit concerner, au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion.
    - Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, les types de données consultées et la référence de l'enregistrement concerné.
- Informer les utilisateurs de la mise en place d'un tel système, après information et consultation des représentants du personnel.
- Protéger les équipements de journalisation et les informations journalisées contre les accès non autorisés, notamment en les rendant inaccessibles aux personnes dont l'activité est journalisée.
- Établir des procédures détaillant la surveillance de l'utilisation du traitement et examiner périodiquement les journaux d'événements pour y détecter d'éventuelles anomalies.
- Assurer que les gestionnaires du dispositif de gestion des traces notifient, dans les plus brefs délais, toute anomalie ou tout incident de sécurité au responsable de traitement.
- Notifier toute violation de données à caractère personnel à la CNIL et, sauf exception prévue par le RGPD, aux personnes concernées pour qu'elles puissent en limiter les conséquences.

Ce qu'il ne faut pas faire

Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique (par exemple, utiliser les traces pour compter les heures travaillées est un détournement de finalité, puni par la Loi).

Documents associés au dossier A

Document A1 : Besoins de sécurité pour les récits utilisateurs (user stories) (extraits)

	Intitulé du récit utilisateur (*user story)*	Disponibilité	Intégrité	Confidentialité	Preuve
1	En tant que famille, je veux consulter le site de *e-learning* à titre d'information mais sans créer un compte.	**	-	-	-
2	En tant qu'élève, je veux modifier mon mot de passe afin de sécuriser mon compte.	*	**	**	*
3	En tant qu'élève, je veux poster un commentaire afin de donner mon avis sur l'auto-école qui m'a accompagné.	*	**	-	**

- : sans objet ** : modéré* *** : important*

Disponibilité : la fonctionnalité doit être utilisée au moment voulu.
Intégrité : les données doivent être exactes et complètes.
Confidentialité : les informations ne doivent pas être divulguées.
Preuve : les traces de l'activité du système sont opposables en cas de contestation.

Document A2 : Bandeau actuel des témoins de connexion (cookies) de la plateforme

Nous utilisons des cookies pour nous assurer du bon fonctionnement de notre site. ✓ Accepter les cookies

Document A3 : Extrait de la politique de confidentialité

- **Utilisation du site internet à des fins d'information**

Lorsque vous consultez notre site internet à des fins d'information, c'est-à-dire sans souscrire l'un de nos services énumérés, nous sommes susceptibles de collecter automatiquement des informations supplémentaires telles que :

- votre adresse IP ;
- votre type d'appareil ;
- la teneur de vos requêtes ;
- des informations concernant la version de votre navigateur ;
- la résolution de votre écran ;
- des informations concernant votre système d'exploitation, notamment les paramètres de langue.

Nous n'utilisons ces informations que pour vous fournir un service efficace, par exemple adapter notre site aux caractéristiques de votre appareil ou pour vous permettre de vous connecter.

Les données à caractère personnel collectées automatiquement sont conservées pendant 12 mois avant d'être effacées.

- **Souscription à nos services**

Notre site internet propose pour les professionnels un accès à un espace de gestion (*back-office*) et pour les particuliers un accès individuel à un espace de formation en ligne (*e-learning*), un espace de consultation/réservation de rendez-vous, un espace d'évaluation de votre auto-école.

Afin d'utiliser ces services, vous devez posséder un compte. Dans le cadre de la création de ce compte puis de son utilisation, nous traitons :

- les informations qui sont fournies lors de l'inscription : nom, prénom, mél (*mail*), date de naissance, numéro de téléphone, lieu de naissance, adresse postale, genre, photo, profession, niveau scolaire, NEPH, représentant légal ;
- les informations d'accès au compte (identifiant et mot de passe) ;
- les communications envoyées par vos soins (par courrier électronique ou via la messagerie intégrée ou formulaire de contact intégré au site).

L'auto-école se chargera de demander à la préfecture le NEPH (numéro d'enregistrement préfectoral harmonisé) qui sera nécessaire pour passer l'examen du code de la route, puis le permis de conduire. Ce numéro s'obtient en ligne sur le site de l'ANTS (agence nationale des titres sécurisés) https://permisdeconduire.ants.gouv.fr/

Document A4 : Courriel de confirmation d'inscription

Bonjour Mathieu Lefranc,

Votre auto-école **AutoSuper** vient de vous inscrire sur la plateforme *Easy2Drive.fr*. Depuis cette plateforme, vous pourrez, au fur et à mesure de l'avancée de votre formation, donner votre avis sur votre auto-école. Vous l'aiderez ainsi à améliorer la qualité de son enseignement.

Pour vous connecter, cliquez sur : https://eleve.easy2drive.fr
Puis renseignez vos identifiants :

Votre identifiant : **MATHIEU.LEFRANC**

Votre mot de passe : **qamQdVD3**

Merci de votre participation !

Cordialement,
Easy2Drive

Document A5 : fonction verifPassword

```
    function verifPassword($mdp): bool
    {
1       $points_total = 6;
2       $longueur = strlen($mdp); // nombre de caractères de $mdp
3       $points_long=0;     // points pour la longueur, soit 0, soit 1
4       $points_comp=0;     // points pour la complexité
5       if ($longueur >=8) { $points_long=1; }

6       if(preg_match("/[a-z]/", $mdp)) { $points_comp=$points_comp+1; }

7       if(preg_match("/[A-Z]/", $mdp)) { $points_comp=$points_comp+2; }

8       if(preg_match("/[0-9]/", $mdp)) { $points_comp=$points_comp+3; }

9       $resultat = $points_long * $points_comp;
10       return ($points_total == $resultat);
    }
```

Document A6 : Documentation de la fonction preg_match

La fonction *PHP preg_match($modele, $chaine): boolean* permet de rechercher un modèle bien précis au sein d'une chaîne de caractères.

Exemples de modèle recherché noté entre les délimiteurs /…/.

[abc] un simple caractère : a, b ou c
[a-z] un caractère appartenant à l'ensemble a-z
[A-Z] un caractère appartenant à l'ensemble A-Z
[0-9] un chiffre appartenant à l'ensemble 0-9
\W n'importe quel caractère spécial

Document A7 : Fonction de tests unitaires testVerifPassword

```
public function testVerifPassword()
{
    $this->assertSame(false, verifPassword("Qam3"));
    $this->assertSame(false, verifPassword("qamQdVDbdAbc"));
    $this->assertSame(false, verifPassword("qamqdvdbabc3"));
    $this->assertSame(false, verifPassword("QAMQDVDBABC3"));
    $this->assertSame(true, verifPassword("qamQdVD3"));
}
```

La fonction assertSame est une fonction de l'environnement (*framework*) de test phpUnit qui compare les 2 paramètres en termes de type et de valeur.

Documents associés au dossier B

Document B1 : Conditions d'attributions de la « Garantie Réussite »

Pour se démarquer de la concurrence, la société Easy2Drive propose aux élèves la « Garantie Réussite » qui leur permet en cas d'échec à l'examen du code d'être remboursé des frais de présentation à un nouvel examen sous certaines conditions.

Pour bénéficier de la garantie réussite et obtenir le remboursement de l'examen du code de la route, l'élève doit :

- avoir passé au moins 25 séries de quiz ;
- avoir passé au moins 4 examens blancs ;
- avoir obtenu au moins 34/40 de moyenne sur les 4 meilleurs examens blancs ;
- l'échec doit dater de moins de 6 mois ;
- la *Garantie Réussite* n'est accordée qu'une seule fois après le premier échec.

Document B2 : Déclencheur check_garantie_reussite

```
1  CREATE TRIGGER check_garantie_reussite
2  BEFORE UPDATE ON Eleve
3  FOR EACH ROW
4  BEGIN
5     DECLARE v_nbSerie INT;
6     DECLARE v_scoreMoyen DOUBLE;

7     IF OLD.echecEtg = TRUE AND NEW.echecEtg = TRUE THEN
8         -- Sortie du déclencheur avec un message d'erreur
9         SIGNAL SQLSTATE '10001'
10           SET MESSAGE_TEXT = 'Garantie réussite : deuxième échec';
11    END IF;

12    IF DATE_ADD(NEW.dateEtg, INTERVAL 6 MONTH) >= NOW() THEN
13        SIGNAL SQLSTATE '10002'
14           SET MESSAGE_TEXT = 'Garantie réussite : échec trop ancien';
15    END IF;

16    SELECT COUNT(*) INTO v_nbSerie FROM Evaluer WHERE idEleve = NEW.id;
17    IF v_nbSerie < 25 THEN
18        SIGNAL SQLSTATE '10003'
19           SET MESSAGE_TEXT = 'Garantie réussite : nombre de séries insuffisant';
20    END IF;

21    SELECT AVG(examenScore) INTO v_scoreMoyen FROM (SELECT examenScore FROM Passer
WHERE idEleve = NEW.id ORDER BY examenScore DESC LIMIT 4) AS MeilleureNotes;
22    IF v_scoreMoyen < 34 THEN
23       SIGNAL SQLSTATE '10005'
24           SET MESSAGE_TEXT = 'Garantie réussite : score examens blancs insuffisant';
25    END IF;

-- Garantie Réussite attribuée
END
```

Document B3 : Entretien avec Mme Clémence Auroux, DPD de l'entreprise Easy2Drive

« Vous : Quelles sont précisément les missions du DPD ?

Clémence Auroux (C.A.) : Je suis chargée, au sein de l'entreprise Easy2Drive, d'informer et de conseiller le responsable du traitement ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent, de contrôler le respect du règlement européen sur la protection des données (RGPD) pour l'ensemble des traitements que nous mettons en œuvre et de coopérer avec l'autorité de contrôle.

Vous : Vous souhaitez la mise en place d'un traçage des événements sur les données personnelles. Pourquoi ?

C.A. : Afin de pouvoir vérifier concrètement l'utilisation des données personnelles mais surtout de pouvoir mieux répondre aux demandes des utilisateurs. En effet, au titre de l'alinéa 4 de l'article 38 du RGPD, « *les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement.* ». En cas d'usage abusif (vol ou suppression par exemple) de ces données, nous ne disposons pas des informations nécessaires pour répondre précisément.

Vous : D'accord. Pouvez-vous préciser de quelles informations vous avez besoin exactement ?

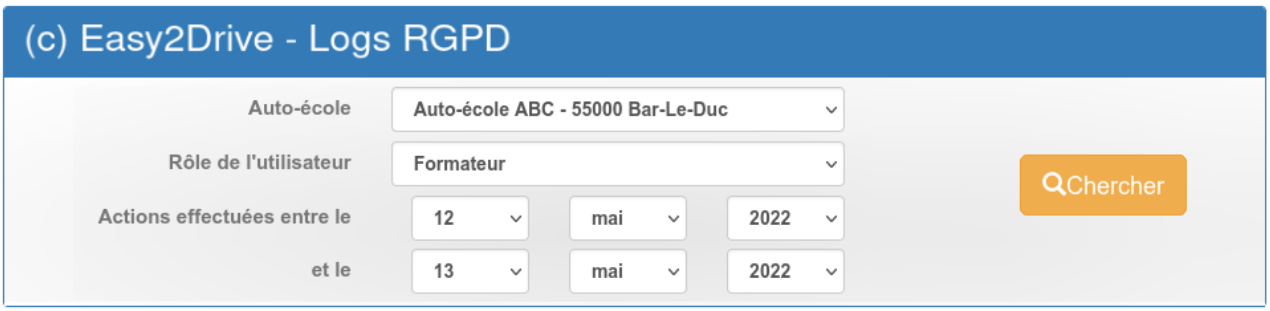
C.A. : Je souhaiterais disposer d'un outil, accessible en lecture et par moi seule, me permettant de répondre, pour une auto-école donnée, à des questions comme :

- Quel(s) utilisateur(s) (nom, prénom, rôle) a(ont) consulté l'enregistrement d'ID 1025 dans la table « Formateur » ?
- Quel utilisateur a modifié l'enregistrement d'ID 578 dans la table « Eleve » le 15/01/2022 ?
- Combien de messages (table « Message ») ont été envoyés par l'utilisateur d'ID 928 le 25/12/2021 ?

Vous : Si je résume, on doit pouvoir lister pour chaque table de la base de données, contenant des données personnelles, quel utilisateur, sous quel rôle (directeur, formateur, élève, modérateur) a réalisé quelle action (consultation, insertion, modification, suppression) et quand ?

C.A. : Bravo bel esprit de synthèse, c'est tout à fait ça ! J'ajoute que vous n'êtes pas sans savoir qu'il y a une réglementation concernant la durée et la conservation de ces journaux (*log*) que nous devons bien sûr respecter ! ».

Document B4 : Maquette d'écran de la future application de traçage « Logs RGPD »



Date	Utilisateur	Action	Table	Enregistrement
12 mai 2022 - 8:45:39	6292 - Fabien Leroux	Consultation	Eleve	n°1685
12 mai 2022 - 8:45:39	6292 - Fabien Leroux	Consultation	Eleve	n°2348
12 mai 2022 - 8:47:09	6292 - Fabien Leroux	Suppression	Eleve	n°7845
12 mai 2022 - 9:05:25	32678 - Samira Ghalam	Création	Message	n°485685

Document B5 : Schémas de la base de données BD_RGPD_LOGS à compléter

Diagramme de classes

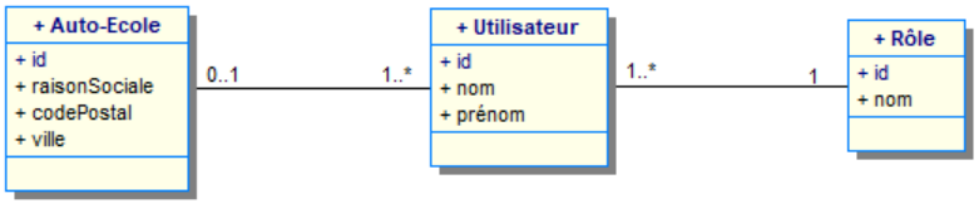
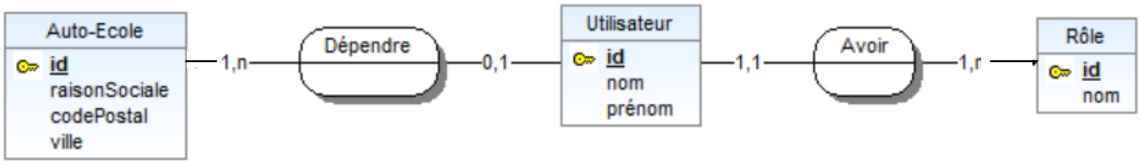


Schéma entité-association



Documents associés au dossier C

Document C1 : Extrait du code des classes métier (vue partielle)

```php
class Utilisateur
{
    private int $id;
    private string $email;
    private string $nom;
    private string $prenom;
    public function getEmail(): string {return $this->email;}
    public function setEmail(string $email) {$this->email = $email;}
    public function getIdentite(): string {return $this->nom. " " . $this->prenom;}
}

class Avis
{
    private int $id;
    private string $contenu;
    private string $dateDepot;
    private bool $publie; /* false tant que l'avis n'a pas été publié, true sinon */
    private bool $modere; /* false tant que l'avis n'a pas été modéré, true sinon */
    private Eleve $lEleve;
    public function getLEleve(): Eleve {return $this->lEleve;}
    public function setLEleve(Eleve $unEleve): void {$this->lEleve = $unEleve;}
    public function getModere(): bool {return $this->modere;}
}

class Eleve extends Utilisateur
{
    private int $id;
    private string $NEPH;
    private Array $lesAvis; // tableau de 0 à 3 Avis
    public function getLesAvis(): Array {return $this->lesAvis;}

    /* renvoie le dernier avis déposé par l'élève */
    public function getDernierAvis(): Avis {return $this->lesAvis->last();}

    /* renvoie vrai si l'élève a déjà déposé 3 avis, faux sinon */
    public function getNbMaxAvisAtteint(): bool
    {
          /* À compléter sur votre copie */
    }

    public function addUnAvis(Avis $unAvis): void
    {
        $this->lesAvis[] = $unAvis;
        $unAvis->setLEleve($this);
    }
}
```

Document C2 : Implémentation partielle de la vue formAvis.html.twig

```
<form method='post'>
  <div class="form-group">
    <label for="txtContenu">Votre Avis</label>
    <textarea id="txtContenu" name="txtContenu" class="form-control"></textarea>
  </div>
  <button class="btn btn-primary" type="submit" name='btnSubmit > enregistrer</button>
</form>
```

Document C3 : Implémentation partielle de la classe AvisEleveController

L'application est développée selon l'architecture *MVC* (Modèle Vue Contrôleur) en *PHP*.

```
class AvisEleveController
{
/* La méthode monAvis est exécutée lorsque l'élève, à partir de l'espace d'évaluation
de son auto-école, clique sur "Mon avis sur l'auto-école" pour saisir son avis et
lorsqu'il clique sur le bouton "enregistrer" après avoir saisi son avis */
    public function monAvis(PdoEasy2Drive $PdoEasy2Drive, Security $security):Response
    {
        //$user est un objet Eleve correspondant à l'élève authentifié
        $user = $security->getUser();

        if ( /* À compléter sur votre copie */ ) {
            // l'utilisateur est redirigé vers l'accueil
            return $this->redirectToRoute('home');
        } else  {
             //  le formulaire est accessible
            if (isset($_POST['btnSubmit'])) {
                // les données saisies sont enregistrées
                // puis l'utilisateur est redirigé vers l'accueil
                $unNouvelAvis = new Avis();
                $unNouvelAvis->setDateDepot(new \DateTime("Now"));
                $unNouvelAvis->setContenu($_POST['txtContenu']);
                $unNouvelAvis->setModere(false);
                $unNouvelAvis->setPublie(false);
                $user->addUnAvis($unNouvelAvis);
                $PdoEasy2Drive ->insertUnAvis($unNouvelAvis);
                return $this->redirectToRoute('home');
            } else {
                //  le formulaire est affiché
                return $this->render('avis/formAvis.html.twig');
            }
        }
    }
}
```

Document C4 : Implémentation partielle de la classe AvisModerateurController

```
class AvisModerateurController {
/* La méthode listeAvis est exécutée lorsque les modérateurs accèdent à leur tableau de
bord pour visualiser la liste des avis à modérer. Elle renvoie à la vue les données du
tableau tabDernierAvisParEleve[] qui contient pour chaque avis à modérer les
informations sur l'élève, son dernier avis ainsi que les critères permettant de
détecter un éventuel faux élève.*/
    public function listeAvis(PdoEasy2Drive $PdoEasy2Drive): Response
    {
        $lesEleves = $PdoEasy2Drive->getLesElevesNonModeres();
        $doublonNeph = true;
        $tabDernierAvisParEleve = [];

        foreach($lesEleves as $unEleve) {
            if ($unEleve->getNeph() == null) {
                $pasDeNeph = true;
            } else {
                $pasDeNeph = false;
            }

            // À compléter et modifier sur votre copie

            $tabDernierAvisParEleve[] = [
                    'leEleve' => $unEleve->getIdentite(),
                    'avis' => $unEleve->getDernierAvis(),
                    'nbRefus' => $unEleve->getNbAvisRefuse(),
                    'pasDeNeph' => $pasDeNeph
                     ];
        }
        return $this->render(
                    'avis/tbbModerateur.html.twig',
                    ['lesAvisAModerer' => $tabDernierAvisParEleve]
                     );
    }
}
```

Document C5 : Implémentation partielle de la classe d'accès aux données PdoEasy2Drive

```
class PdoEasy2Drive
{
    private static $monPdo;  //variable de connexion à la base de données

    /* renvoie une collection d'objets Eleve contenant les élèves ayant déposé un avis
en attente de modération */
    public function getLesElevesNonModeres(): Array
    {
        $req = "select eleve.id, nom, prenom, email, neph
                from eleve join utilisateur on eleve.id=utilisateur.id" ;
        $res = PdoEasy2Drive::$monPdo->prepare($req);
        $res->execute();
        $lesEleves = $res->fetchAll();
        $tabEleve=[];
        foreach($lesEleves as $unEleve) {
            $req = "select * from avis where idEleve=:id and modere=0" ;
            $res = PdoEasy2Drive::$monPdo->prepare($req);
            $res->bindParam(':id', $unEleve['id']);
            $res->execute();
            $lesAvis = $res->fetchAll();
            $tabAvis = [];
            foreach($lesAvis as $unAvis) {
                $objAvis = new Avis($unAvis['id'], $unAvis['contenu'],
                            $unAvis['dateDepot'], $unAvis['publie'],
                            $unAvis['modere']);
                $tabAvis[]=$objAvis;
            }
            if (!empty(tabAvis)) {
                $tabEleve[] = new Eleve($unEleve['nom'], $unEleve['prenom'],
                               $unEleve['email'], $unEleve['neph'], $tabAvis);
            }
        return $tabEleve;
    }

    public function insertUnAvis(Avis $unAvis)
    {
        $req = "insert into avis(contenu,dateDepot,publie, modere, idEleve) values('" .
        $unAvis->getContenu() . "',now()," . $unAvis->getPublie() . "," .
        $unAvis->getModere() . "," . $unAvis->getLEleve()->getId() . ")" ;
        PdoEasy2Drive::$monPdo->exec($req);
    }

    /* renvoie vrai si $unEmail est l'adresse électronique de plusieurs élèves */
    public function getDoublonMail($unEmail): bool
        {
            /* À compléter sur votre copie  */
        }
}
```