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

Mission A1 – Évaluation des risques à partir des récits utilisateurs

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.

a) L'impossibilité de consulter le site au moment voulu pour une famille peut l'amener à souscrire un service chez un concurrent. L'impossibilité de modifier son mot de passe à un instant donné n'est pas bloquante car elle peut être réalisée plus tard et n'empêche pas l'accès aux autres fonctionnalités.

b) Lors d'un changement de mot de passe, il est primordial de s'assurer que celui-ci ne puisse pas être intercepté (confidentialité) et que l'utilisateur qui réalise l'opération soit le propriétaire du compte (intégrité).

c) Il n'y a pas besoin de tracer les accès anonymes en consultation. Au contraire, on doit pouvoir identifier les publications d'avis par les élèves. (Notion de preuve juridique non exigé)

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

Question A.2.1

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

La nouvelle réglementation des cookies n'est pas respectée puisque l'utilisateur n'a pas d'autre choix que d'accepter les cookies. Or l'utilisateur doit pouvoir soit accepter, soit refuser (continuer sans accepter), soit personnaliser les cookies.

Depuis le 1er avril 2021, une amende est même possible.

Source : Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »

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.

Donnée personnelle : Adresse IP qui permet d'identifier indirectement une personne physique par son fournisseur d'accès.

Mission A3 – Vérification de la sécurité du mot de passe

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.

a) On peut relever :

- que le mot de passe est communiqué en clair dans un courriel (brèche confidentialité)
- le mot de passe est communiqué avec le login (brèche confidentialité et intégrité)
- l'utilisateur n'est pas obligé de modifier le mot de passe.

b) Le courriel comprendra **une URL temporaire** dont la validité ne doit **pas excéder 24 heures et** qui permettra à l'élève de saisir un mot de passe personnel.

Ou le courriel peut contenir un mot de passe temporaire qui permettra à l'élève à la première connexion de saisir un mot de passe personnel.

Ou 2 médias de transmission.

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.

a) En examinant les tests, on peut en déduire que la politique actuelle impose une longueur minimum de 8 caractères, composé d'au moins une minuscule, une majuscule et un chiffre.

Le caractère spécial n'est pour l'instant pas exigé.

b) Modifier le nombre de points total : `$points_total = 10;`

Modifier le test sur la longueur : `if ($longueur >=12) { $points_long=1; }`

Et rajouter le code pour tester la présence d'un caractère spécial qui sera valorisé à 4 points CNIL :

```
if(preg_match("/\W/",$mdp)) { $points_comp=$points_comp+4; }
```

Autre expressions régulières possibles : [^A-Za-z0-9], ou liste de caractères spéciaux…

c) Le test qui passait avant est devenu de longueur insuffisante et la condition de caractère spécial n'est pas respectée.

```
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(false, verifPassword("qamQdVD3")); // 0 -> refusé (longueur insuffisante)
    $this->assertSame(false, verifPassword("qamQdVD3@")); // 0 -> refusé (4 critères mais longueur insuffisante)
    $this->assertSame(false, verifPassword("qamQdVD3vbn1")); // 6 -> refusé (longueur suffisante mais pas de caractère spécial)
    $this->assertSame(true, verifPassword("qamQdVD3@bn1")); // 10 ->accepté (longueur correcte et 4 critères présents)
}
```

Question A.3.3

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

b) Écrire la fonction *renouvelleMDP*.

a) ALTER TABLE utilisateur ADD dateMajMDP DATE NOT NULL DEFAULT CURRENT_DATE() ;

On acceptera également le format DATETIME

b) CREATE FUNCTION renouvelleMDP(num INT)

RETURNS boolean

BEGIN

```
DECLARE v_date1 DATE;
select dateMajMDP into v_date1 from Utilisateur  where id=num;
RETURN CURRENT_DATE()>DATE_ADD(v_date1,INTERVAL 3 MONTH);
```

END

On ne demande pas le délimiteur pour exécuter cette instruction.

On acceptera

solution avec un IF

select dateInscription into v_date1 from Eleve where id=num;

si le candidat n'a pas vu qu'il fallait ajouter un champ date pour le renouvellement.

(*Coquille dans l'exemple de fonction : on ne pénalise pas les candidats sur une condition inversée pour la date. On trouvera également id=num à la place de idUtilisateur=num sans conséquence.)*