Examen de Web sécurisé

Durée : 2h. Une copie double de notes manuscrites autorisée. Le barème est donné à titre indicatif et est susceptible de changer.

Toutes les réponses données doivent être justifiées. Les réponses non justifiées ne rapporteront pas de points. Il vous est conseillé de lire le sujet une fois en entier avant de commencer... Dans tous les exercices, il n'est pas demandé de produire du code, il suffit de préciser les propriétés importantes des fonctions utilisées.

Exercice 1 ([4 pt]) Vous vous connectez avec votre navigateur sur différents sites internet, et obtenez les résultats suivants. Pour chacun des cas :

- Donnez le niveau de sécurité du site en justifiant ;
- Donnez un exemple de contexte dans lequel vous pouvez tomber sur ce résultat ;
- Si la sécurité vous semble faible, donnez un exemple d'attaque ;
- Expliquez ce que vous devriez faire ensuite (poursuivre ou non la navigation sur ce site ? autre chose ?). Justifiez.

1. Votre navigateur vous affiche le message :

```
Votre connexion n'est pas privée

Il se peut que des pirates soient en train d'essayer de dérober vos
informations sur le site cerbere.gemtech.fr (mots de passe, messages
ou numéros de carte de crédit, par exemple).

NET:: ERR_CERT_WEAK_SIGNATURE_ALGORITHM
```

2. Le bandeau du navigateur affiche un cadenas vert avec les détails suivants :

```
Connexion chiffrée
(TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS1.2)
```

3. Votre navigateur vous affiche le message :

```
Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos
informations personnelles sur le site ***.***.com (mots de passe,
messages ou numéros de carte de crédit, par exemple).

NET::ERR_CERT_AUTHORITY_INVALID
```

4. Le bandeau du navigateur est gris et contient les informations suivantes :

```
Non Sécurisé | www.webmail.agora.net
```

5. Votre navigateur vous affiche le message :

```
Les propriétaires de www.google.fr ont mal configuré leur site
web. Pour éviter que vos données ne soient dérobées, Firefox ne
```

```
s'est pas connecté à ce site.
Le certificat est uniquement valide pour controleur.wifipass.org,
www.controleur.wifipass.org

Error code: SSL_ERROR_BAD_CERT_DOMAIN
```

6.
```
Secure Connection Failed

An error occurred during a connection to duckduckgo.com. The OCSP
response is not yet valid (contains a date in the future).

Error code: SEC_ERROR_OCSP_FUTURE_RESPONSE
```

Exercice 2 [16 pt] Suite à l'introduction de l'informatique dans les nouveaux programmes du lycée, on vous demande de réaliser un site web à destination de classes de lycées. Le site web devra présenter du contenu en lien avec le programme, en particulier autour de la sécurité informatique.

Chaque enseignant.e pourra inscrire sa classe, les lycéen.ne.s auront tou.te.s un compte sur le site lié à leur adresse email académique (`prenom.nom@eleve.ac-rouen.fr`), avec leur photo officielle du lycée. Les élèves pourront modifier leurs informations (mot de passe, photo mais pas email) dans la partie "gestion du compte".

Le site comportera une partie évaluation (des QCM et un espace "devoir" où les élèves pourront déposer des devoirs faits à la maison). Chaque enseignant.e aura accès aux résultats de sa classe via son compte "enseignant". L'enseignant.e pourra déposer les sujets des devoirs, les sujets corrigés, paramétrer les dates de visibilité des différents devoirs et corrigés, et il pourra aussi noter les devoirs (un peu comme le site `universitice.univ-rouen.fr`).

Le site comportera aussi un forum où les lycéen.ne.s pourront échanger entre eux et avec les enseignant.e.s.

Proposez une analyse des risques sécurité du projet, en détaillant pour chaque problème de sécurité identifié :

- le modèle de l'attaquant,
- la description de la vulnérabilité potentielle (expliquez clairement d'où vient le problème),
- des exemples de scénarios d'attaques,
- des impacts possibles en cas d'attaque,
- votre statégie de traitement du risque (= les mesures à mettre en oeuvre pour éviter l'attaque).

Vous coterez, sur la feuille jointe, chaque risque selon la vraissemblance (= facilité d'exploitation et d'apparition du risque) et les impacts en cas de survenue du risque, avant et après mise en oeuvre de votre stratégie de traitement du risque. La feuille sera à rendre avec votre copie, pensez bien à mettre votre nom ou numéro d'anonymat dessus !