Université de Rouen - M2 GIL 2018-2019

Examen de Web sécurisé

Durée : 2h. Tout document est interdit. 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 [12 pt] Suite à la loi RGPD, votre directeur technique souhaite vérifier la sécurité existante sur les mots de passe des utilisateurs du site web de votre entreprise, que vous gérez.

1) [4 pt] Il vous dit qu'il a vu quatre méthodes différentes pour stocker un mot de passe `mdp` (la notation `::` indique une concaténation) :

1. stocker `mdp`
2. stocker `SHA256(mdp)`
3. tirer uniformément au hasard une valeur `sel` de 32 caractères hexadécimaux, stocker `sel::SHA1(sel::mdp)`
4. tirer uniformément au hasard une valeur `sel` de 32 caractères hexadécimaux, stocker `sel::MD5^2048(sel::mdp)` (où `MD5^2048` représente la fonction `MD5` itérée 2048 fois, par exemple `MD5^4(mdp) = MD5(MD5(MD5(MD5(mdp))))`.)

Expliquez-lui pour chaque méthode les problèmes possibles ou les intérêts de la méthode. Conseillez-le sur la bonne méthode à choisir.

2) [2 pt] Votre directeur vous demande quelles sont les précautions à prendre pour sécuriser les mots de passe des utilisateurs pendant leur transport. Expliquez-lui. Il a aussi entendu parler de "confidentialité persistante". Expliquez-lui ce que c'est et le risque associé s'il n'y en a pas. Comment sait-on si un serveur web sécurisant le transport des mots de passe propose de la confidentialité persistante ?

3) [2 pt] Suite à une authentification réussie, votre application attribue un cookie d'authentification au client. Décrivez deux attributs particuliers que vous pouvez donner à ce cookie, expliquez pour chacun de quelle(s) attaque(s) il protège et qui est protégé.

4) [1 pt] On vous fait remarquer que l'authentification par mot de passe n'est pas très « sûre » cryptographiquement parlant. Expliquez pourquoi, proposez une autre solution plus « sûre » (en expliquant).

5) [3 pt] Votre directeur a entendu parler de HSTS et HPKP. Expliquez-lui de quoi il s'agit, quelles sont les contraintes de mise en oeuvre, et si c'est intéressant ou non pour votre site.

Exercice 2 [8 pt]

1) [3 pt] Vous naviguez sur internet, et en cliquant sur un lien 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`

Qu'est-ce que cela signifie ? Est-ce un gros problème de sécurité (dans ce cas vous n'allez pas sur le site) ou pouvez-vous quand même ajouter une exception ?

2) [1 pt] Expliquez ce qu'est le principe de défense en profondeur.

3) [4 pt] Le TOP10 de l'OWASP comporte les risques suivants :

- une injection SQL.
- une faille XSS (persistante et non persistante).

Pour chacun d'eux, expliquez en quelques mots le principe de l'attaque (en donnant un exemple de mise en oeuvre), quels sont les risques et impacts en cas d'exploitation par un attaquant, et comment l'on s'en protège.