XWIKI NATIS

1. Les attaques MITM : HTTPS
2. Le phishing : Eduquer les visiteurs
3. Les attaques CSRF : Token CSRF
4. Les modifications du DOM : Faire les vérifications au backend
5. Les injections : Figer la forme de la requete SQL et désactiver les balises HTML
6. Le brute force : Mettre une limite sur le nombre d‘essais

XWIKI SAS

XWIKI NATIS

Qu‘est-ce qu‘une attaque par brute force ?

XWIKI NATIS

A votre avis, comment empêcher les attaques par brute force ?

XMNATIS

PREVENTION

1. Limiter le nombre de tentatives de connexion
2. Création de mot de passe le plus complexe possible
3. Activation de la vérification à 2 facteurs

XONATIS

XWIKI NATIS

1. Limiter le nombre de tentatives de connexion

La solution la plus simple à ce problème consiste à limiter le nombre de tentatives de connexion. Si vous limitez le nombre à 3, vous avez alors trois occasions de saisir le mot de passe correct. Ainsi, si vous vous trompez en vous connectant, vous avez encore deux chances.

XWNATIS

1. Limiter le nombre de tentatives de connexion

Après la troisième tentative de connexion, le système verrouille le compte jusqu'à ce qu'il soit vérifié par courriel ou qu'une limite de temps soit atteinte. Cela signifie qu'un pirate informatique n'a que trois chances d'essayer de s'introduire avant que l'alarme ne se déclenche et que le compte ne soit verrouillé.

XONATIS

XWIKI NATIS

Selon vous, qu’est-ce qu’un mot de passe complexe ?

XWIKI NATIS

2. Création de mot de passe le plus complexe possible

Rien ne garantit que cela vous donnera une sécurité totale, mais cela va aider. Si un mot de passe est trop complexe, les pirates peuvent passer à une cible plus facile.

Un mot de passe de 12 à 16 caractères est encore plus sécurisé. Il doit s'agir d'un mélange aléatoire de lettres minuscules, de lettres majuscules, de chiffres et de caractères spéciaux.

XWIKI NATIS

2. Création de mot de passe le plus complexe possible

Par ailleurs, plus le mot de passe est complexe, plus il sera difficile pour un hacker de le retrouver en bruteforce, car plus le mot de passe est long et compliqué, plus le nombre de combinaisons possibles est important.

XWIKI SAS

XWIKI NATIS

Qu’est-ce que l’authentification à 2 facteurs ?

XWIKI NATIS

Est-ce que l’authentification à 2 facteurs existe seulement pour embêter les gens ?

XMNATIS

3. Activation de la vérification à 2 facteurs

Dans ce cas, les hackers peuvent être en mesure d'utiliser le brute force pour obtenir votre mot de passe, mais après l'avoir saisi, ils doivent également entrer un code qui est envoyé à votre téléphone portable ou créé par une application tierce.

Pour pirater votre compte, ils devraient voler votre mot de passe ET votre téléphone portable.

XWIKI NATIS

3. Activation de la vérification à 2 facteurs

Le nom technique de l’authentification à 2 facteurs est le MFA (Multi-factor authentication). Il existe pour empêcher ces cas dans lesquels un hacker découvre votre mot de passe afin de l’empêcher de se connecter.

XONATIS