XEFI NATIS

Culture

Etude de cas

XMCO NATIS

Compétence demandée :

Comprendre les enjeux des vulnérabilités

XWIKI NATIS

ATELIERS !

XMNATIS

Que s'est-il passé avec Ashley Madison en 2015 ?

XWIKI NATIS

Alors ? =)

XMNATIS

Que s‘est-il passé avec Apple et Ibrahim Balic en 2013 ?

XWIKI NATIS

Alors ? =)

XWIKI NATIS

Que s'est-il passé avec Wordpress en 2018 ?

XWIKI NATIS

Alors ? =)

XDNATIS

Que s‘est-il passé avec Windows 10 en 2021 ?

XWIKI NATIS

Alors ? =)

XDNATIS

Que s'est-il passé avec Drupal en 2013 ?

XWIKI NATIS

Alors ? =)

XWIKI NATIS

Que s'est-il passé avec Tiktok en 2020 ?

XWIKI NATIS

Alors ? =)

XONATIS

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

La société derrière Ashley Madison, le site de rencontres extra-conjugales a subi une cyber-attaque en 2015, et a payé une amende de 1,6 million de dollars pour ne pas avoir protégé les informations de compte des utilisateurs, soit l'un des plus importants règlements à ce jour pour violation de données

XONATIS

Le 15 juillet 2015, le site se fait pirater par un groupe de hackers se nommant « The Impact Team ». Celui-ci affirme avoir volé des données personnelles sur la base de données d'utilisateurs du site, et menace de publier beaucoup de noms d'utilisateurs inscrits ainsi que d'autres données personnelles si le site n'était pas fermé immédiatement.

XNATIS

À cause de la politique du site qui est de ne pas supprimer les données sur ses utilisateurs, dont leur état civil, leur adresse, leur historique de recherche et leurs numéros de carte de crédits, beaucoup d'inscrits ont eu peur d'être humiliés.

XMNATIS

Le 18 août, le groupe de pirates envoie toutes les données sur un site du Dark Web avec un message et un lien vers un fichier torrent contenant presque 10 Go de données. Décompressé, le tout atteint au moins 60 Go. Des experts confirment la validité des informations divulguées

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Protégez les DCP de vos clients et ayez une attention particulière sur la sécurité des DCP

XONATIS

XMNATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XMNATIS

Le 26 mars 2013, Ibrahim Balic envoyait un courriel à un responsable d'Apple et a soumis un rapport de bug, écrivant avoir réussi à franchir la sécurité du nuage de la Pomme par la force brute : Balic a pu tester 20 000 combinaisons de mots de passe afin de forcer le passage d'un compte iCloud

XWIKI NATIS

Les essais en force brute ont porté leur fruit sur les comptes de célébrités et a pu révéler des photos dénudés, en particulier pour des célébrités féminines comme Jennifer Lawrence, des photos téléchargées puis transférées sur les réseaux sociaux.

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Fixez un nombre limité d‘essais d‘identification par compte pour éviter les attaques par force brute !

XWIKI SAS

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

Des milliers de sites WordPress ont été piratés et compromis avec du code malveillant.
Les chercheurs pensent que les intrus accèdent à ces sites non pas en exploitant des failles dans le CMS WordPress lui-même, mais des vulnérabilités dans des thèmes et des plugins obsolètes.

XWIKI NATIS

Lorsqu'ils accèdent à un site, ils plantent une porte dérobée pour un accès futur et apportent des modifications au code du site.

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Faites les mises à jour régulièrement

XONATIS

XMNATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XMNATIS

La vulnérabilité permet aux utilisateurs non administrateurs de lire des fichiers sensibles qui sont normalement réservés aux administrateurs. Microsoft, de son côté, précise que si un individu malveillant parvient à exploiter cette faille, il pourrait exécuter du code arbitraire avec les privilèges SYSTEM.

XMNATIS

L'attaquant aurait ainsi toute la liberté d'installer des programmes, d'afficher, de modifier, de prélever ou de supprimer des données sur et de votre ordinateur. Sans oublier qu'il pourrait créer un nouveau compte, en s'octroyant tous les droits d'utilisateur.
Cette faille a été mise en évidence le jour de la sortie du système d’exploitation (zero-day).

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Soyez prêt le jour du lancement de votre site internet ! (zéro day)

XONATIS

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

Une violation de données Drupal a été annoncée par l'association officielle Drupal, selon laquelle les mots de passe de près d’1 million de comptes sur le site Web Drupal.org sont réinitialisés après que des pirates aient obtenu un accès non autorisé à des données utilisateur sensibles.

XWIKI NATIS

La sécurité du système de gestion de contenu open source a été compromise via un logiciel tiers installé sur l'infrastructure du serveur Drupal.org, et n'était pas le résultat d'une vulnérabilité au sein de Drupal lui-même.

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Faites attention avec qui vous collaborez (techniquement). Est-ce que leurs composants sont sécurisés ?

XONATIS

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

Au moins 235 millions d'utilisateurs d'Instagram appartenant à Facebook, de TikTok et de YouTube ont été touchés par une fuite massive de données et leurs profils personnels.
Selon les chercheurs en sécurité du site Web pro-consommateur Comparitech, une base de données non sécurisée était à l'origine de cette violation de données.

XWIKI NATIS

Les données étaient réparties sur plusieurs ensembles de données avec le plus important étant deux atteignant un peu moins de 100 millions chacun. La sécurité n'était pas uniforme sur l'ensemble des bases de données et une partie a pu être hackée.

XEBIA NATIS

Leçon retenue ?

XONATIS

XWIKI NATIS

Appliquez les mêmes règles de sécurité et ne faites pas d‘exceptions !

XWIKI SAS

XWIKI NATIS

Conclusion ?

XWIKI NATIS

1. Ashley Madison
2. Apple et Ibrahim Balic
3. Wordpress
4. Windows
5. Drupal
6. Tiktok

XWIKI NATIS

1. Protéger vos DCP
2. Protéger les inputs
3. Faites les mises à jour
4. Soyez prêt au zero-day
5. Faites attention aux third-parties
6. Ne faites pas d‘oubli !

XWIKI SAS