XMNATIS

1. Les attaques MITM
2. Le phishing
3. Les attaques CSRF
4. Les modifications du DOM
5. Les injections
6. Le brute force

XMNATIS

LE BRUTE FORCE

XMNATIS

Avez-vous déjà entendu parler de brute forcing ?

XMNATIS

Le brute force n’est pas une stratégie de hacking en soi, bien que cela peut porter ses fruits.

Le brute forcing est simplement le fait d’essayer toutes les combinaisons possibles pour trouver un mot de passe

XWIKI NATIS

A LA PLACE D‘UN HACKER …

XMNATIS

Objectifs :

1. Trouver un mot de passe (d‘un email, d‘un wifi etc.)

XMNATIS

Mise en place :

1. Essayer d‘abord tous les mots communs

2. Essayer toutes les combinaisons de lettres et de chiffres pour toutes longueurs possibles de mot de passe

XWIKI NATIS

Quel est l‘inconvénient ?

XWIKI NATIS

Cela prend des années et des années !

XWIKI NATIS

Pour un mot de passe à 6 caractères (et supposons que ce sont des caractères parmis les 26 lettres de l'alphabet) :

26 x 26 .. x 26 = 308 915 776 combinaisons possibles

Si le hacker prend 5 secondes pour tester 1 combinaison, alors il prendra :

5 x 308 915 776 = 1 544 578 880 secondes

Soit 48,97 ans

XWIKI SAS

XMNATIS

CONCLUSION SUR LES VULNERABILITES

XMNATIS

1. Les attaques MITM
2. Le phishing
3. Les attaques CSRF
4. Les modifications du DOM
5. Les injections
6. Le brute force

XMNATIS

Qu‘a-t-on appris des attaques MITM ?

XMNATIS

Qu‘a-t-on appris du phishing ?

XWIKI NATIS

Qu‘a-t-on appris des attaques CSRF ?

XWIKI NATIS

Qu‘a-t-on appris des modifications du DOM ?

XWIKI NATIS

Qu‘a-t-on appris des injections ?

XWIKI NATIS

Qu‘a-t-on appris du bruteforce ?

XDNATIS

1. En HTTP, un hacker peu surveiller notre trafic
2. Un visiteur peut se faire avoir par un email
3. En cliquant sur un lien, un visiteur peut se faire leurrer et faire une action à son insu
4. Les vérifications ne doivent pas se faire au front
5. On ne peut pas faire confiance aux visiteurs pour les valeurs qu‘il va saisir dans les inputs
6. Un hacker peut trouver un mot de passe faible

XWIKI SAS

De manière générale …

Protéger vos visiteurs, mais méfiez-vous d'eux. Derrière un visiteur peut se cacher un hacker !