

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

LE BRUTE FORCE

Avez-vous déjà entendu parler
de brute forcing ?



Le brute force (attaque force brute) 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



A LA PLACE D'UN HACKER ...

Objectifs :

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

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

Quel est l'inconvénient ?



Cela prend des années et des
années !

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

$26 \times 26 \dots \times 26 = 308\,915\,776$ combinaisons possibles

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

$5 \times 308\,915\,776 = 1\,544\,578\,880$ secondes

Soit 48,97 ans

CONCLUSION SUR LES VULNERABILITES

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



Qu'a-t-on appris des attaques MITM ?





Qu'a-t-on appris du phishing ?





Qu'a-t-on appris des attaques CSRF ?





Qu'a-t-on appris des
modifications du DOM ?





Qu'a-t-on appris des injections ?





Qu'a-t-on appris du brute force ?



1. En HTTP, un hacker peut 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



De manière générale ...

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