

UNIVERSITÉ CHEIKH ANTA DIOP
ESP - DAKAR



GROUPE 2

A07:2021 - IDENTIFICATION ET AUTHENTIFICATION DE MAUVAISE QUALITÉ



A07:2021 – Identification et authentification de mauvaise qualité



Haby DIOP



Mariama KA



Marième AIDARA



Papa Cheikh GUINGUE



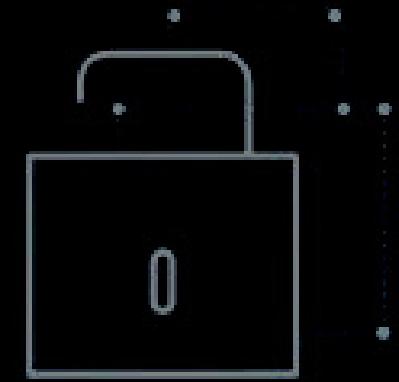
Taamba Brice Bedel THIOMBIANO

Matching des concepts avec les parties du cours

La confirmation de l'identité, de l'authentification et de la session de l'utilisateur sont essentielles pour se protéger des attaques liées à l'authentification. Cependant, il peut y avoir des faiblesses d'authentification si l'application autorise :



BRUTE FORCE ATTACK



Des attaques par
force brute

Chapitre1 _ page 52

D'utiliser des mot de passe en texte brute ou faiblement hachés

Chapitre1 _ page 23



D'autoriser l'authentification par défaut: confidentialité, intégrité, authentification, non répudiation



Maintenant pour s'en prémunir, il faut
absolument :



Implémenter l'authentification multifacteur et services de sécurité

Chapitre1 _ page 17



L'authentification multifacteur (MFA) est une méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN.

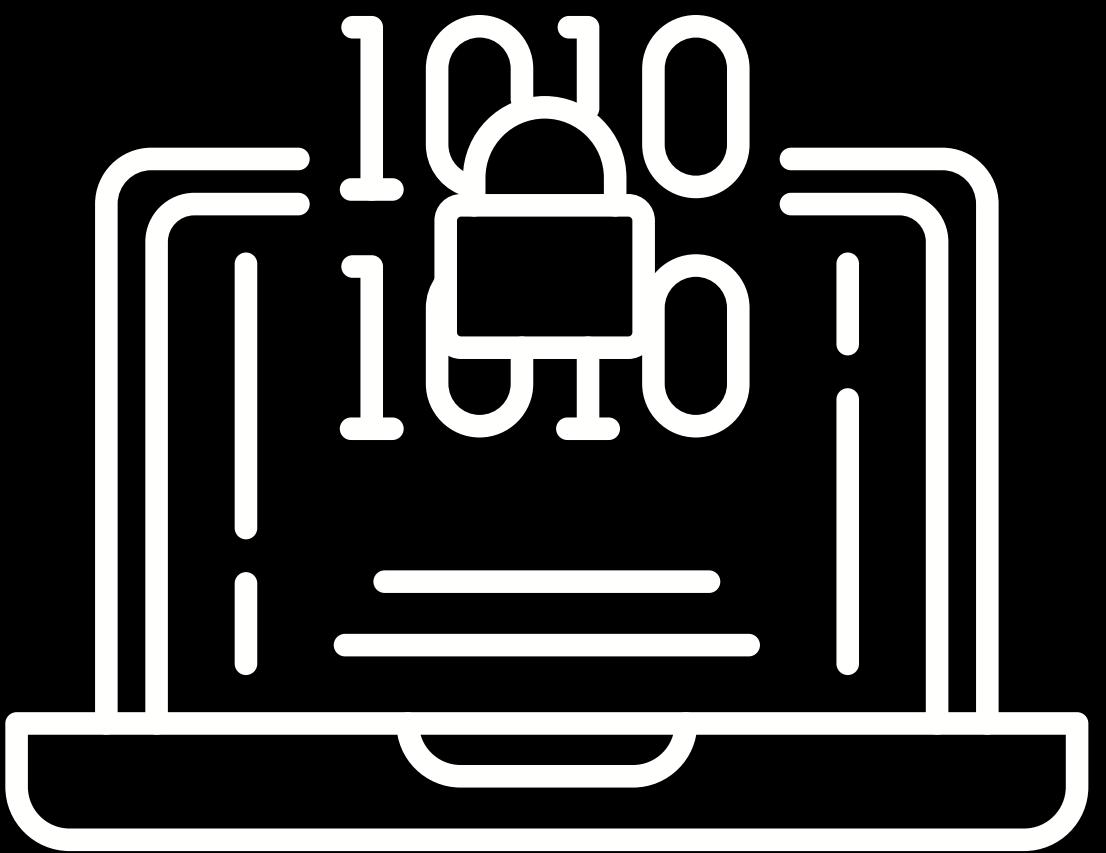
Intégrer des tests de mots de passes faibles, à la création ou utiliser des mots de passe cryptés ou hachés

Chapitre1 _ page 23



Utiliser des fonctions de hachages

Chapitre6 _ page 14



Merci pour votre
attention !