Projet de Sécurité des Applications

Bachelor Dev – 3éme Année

Nom : Brut

Prénom : Adam

Failles de Sécurité potentielles :

1 – Mot de passe non sécurisé

Lors de la création du compte (page Register) il est possible de créer un mot de passe avec deux caractères seulement (exemple : ‘de’) . Avec un mot de passe ‘faible’ comme cela, il peut y avoir des attaques par **Bruteforce** permettant de rapidement trouver le mot de passe d’un utilisateur. C’est pour cela que ça représente un danger et une faille de sécurité

2 . Double compte

Lors ce que l’on recrée un compte avec une adresse email , il nous est indiqué que l’email existe déjà , or cela peut induire l’attaquant a savoir les emails déjà présent sur le site et dans la base de données

3 – Reset de compte

Il y a aussi le fait que l’email et le token sont directement en paramètres GET dans l'URL générée étant donnée que l’email est une donnée personnelle selon les normes RGPD

Une des fonction prend un tableau $emails en argument et boucle dessus, et si un attaquant parvient à envoyer une liste de 10 000 emails à cette fonction, le serveur va tenter d'envoyer 10 000 mails d'un coup. Ce qui constitue une attaque par ddos.