Titre du CTF : PHP Bruteforce Challenge

Description : Ce CTF met au défi les participants de trouver un login et un mot de passe valides en utilisant une attaque par force brute sur une page de connexion implémentée en PHP.

Objectif : Découvrir le bon login et mot de passe pour accéder au système.

Déroulement :

Analyse initiale : Les participants reçoivent un lien vers une page de connexion qui simule un système sécurisé.

Identification de la vulnérabilité : En examinant le code source de la page de connexion, les participants découvrent que le formulaire de connexion envoie les informations soumises à un script PHP qui traite les données.

Choix de l'approche : Les participants décident d'utiliser une attaque par force brute pour tester différentes combinaisons de logins et de mots de passe.

Lancement de l'attaque : Les participants utilisent des outils ou écrivent des scripts en PHP ou dans d'autres langages pour effectuer l'attaque par force brute en envoyant des requêtes HTTP avec différentes combinaisons de logins et de mots de passe.

Identification du succès : Après plusieurs tentatives, les participants reçoivent une réponse positive du serveur, indiquant qu'ils ont trouvé le bon login et mot de passe.

Accès au système : Avec les informations d'identification correctes, les participants se connectent avec succès au système et trouvent le flag, confirmant leur succès.

Conclusion : Ce CTF met en lumière l'importance de sécuriser les formulaires de connexion contre les attaques par force brute en mettant en place des mécanismes tels que des limites de tentatives de connexion, des captcha, ou des fonctions de hachage sécurisées pour stocker les mots de passe.

Login: mr_robot

Password: football