Master INFO
RT0706

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

TP3: Server-side attacks

Un compte rendu de TP doit être rédigé, nommé sous la forme **TP3_NOM1_NOM2.pdf** et envoyé dans la section dédiée sur le Moodle.

Un retard de livraison de compte rendu entrainera une perte de points.

Chaque réponse doit-être accompagnée :

- Du flag
- D'une preuve sous forme d'une ou plusieurs captures d'écran
- D'un texte explicatif démontrant votre démarche et votre compréhension de l'exercice
- D'une proposition de patch de la vulnérabilité

La démarche est bien plus importante que le flag. Une réponse avec le flag mais sans démonstration ne vaut que très peu de points. A l'inverse, une bonne démarche sans le flag peut valoir la quasi-totalité des points de l'exercice.

1. Root-me.org (20 points)

Facile (5 points)

a. Faire le challenge :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/Injection-de-commande-Contournement-de-filtre
     (2.5 points)

b. Faire le challenge :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/Local-File-Inclusion
     (2.5 points)

Moyen (8 points)

a. Faire le challenge :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/File-upload-null-byte (4 points)

b. Faire le challenge :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/SQL-injection-string (4 points)

Difficile (7 points)

a. Faire le challenge :
   - https://www.root-me.org/fr/Challenges/Web-Serveur/XML-External-Entity (7 points)