Hacking et Pentesting

Mai 2021 | **Serie 7**

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

1.1 Clarification

Dans vos rapports d'exercices, faites attention à bien inclure:

- Captures d'écran de réussite
- Payload utilisés
- Tout code source utilisé pour l'exploitation (ou en annexe)
- Nom des outils utilisé

1.2 Root-Me

Les exercices suivants sont à faire sur la **plateforme Root-Me**. Cette plateforme propose des challenges de tout types. Libre a vous de vous exercer ou tester d'autres challenges. Des ressources et documentations sont disponibles pour chaque exercices.

Ces documentations peuvent être utilisées dans le cadre de l'examen final.

1.3 Simples

Les exercices suivants sont simples et rapides

- Web Server > HTML - Source code
- Web Server > HTTP - Open redirect
- Web Server > HTTP - Headers
- Web Server > Directory traversal

1.4 Injections

Cours sur les Injections

- Web Server > PHP - Command Injection
- Web Server > SQL injection - Authentication
- Web Server > SQL injection - String
- Web Server > LDAP injection - Authentication 8

1.5 File Upload

Partie sur les upload de fichiers

- Web Server > File upload - Double extensions
- Web Server > File upload - MIME type

1.6 XSS

- Web Client > XSS - Stored 1

1.7 CSRF

- Web Client > CSRF - 0 protection