# M2 EPITA- Test d'intrusion







Version: 1.0 Date: Novembre 2022



## Table des matières

1. Objectifs et attentes	3
1.1. Introduction	3
1.2. Les challenges	4
1.3. Challenge PHP - Injection de commande	4
1.4. Challenge - XSS - Stockée 1	5
1.5. Challenge - XSS - Stockée 2	5
1.6. Challenge - CSRF - 0 Protection	6
1.7. Challenge -The h@ckers l4b	6

Copyright® Devoteam Page 2/6



# 1. Objectifs et attentes

#### 1.1. Introduction

Chaque challenge présente des technologies différentes dans le but de simuler une machine réelle avec des vulnérabilités pour améliorer les compétences et la méthodologie de travail.

L'objectif final pour chaque est d'obtenir le flag pour valider le challenge.

L'ensemble des challenges sont disponibles sur la plateforme RootMe accessible via cette <u>url</u>

Copyright® Devoteam Page 3/6



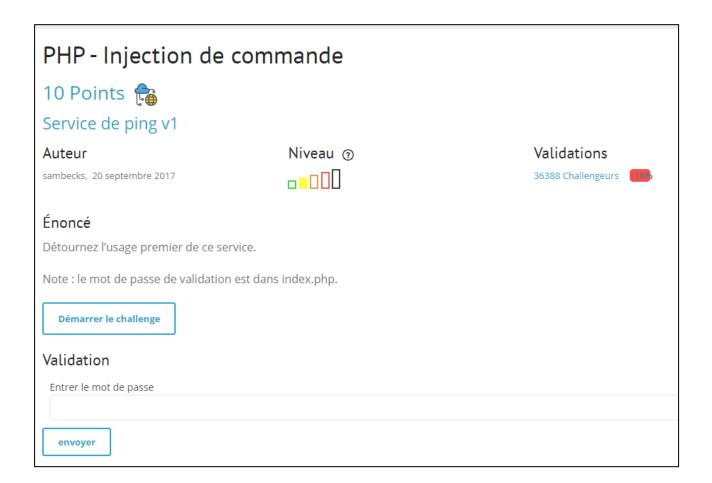
# 1.2. Les challenges

## 1.3. Challenge PHP - Injection de commande

Votre première mission sur site de RootMe est de résoudre le challenge <u>PHP - Injection de commande dans la catégorie web-serveur</u>.

L'objectif de ce challenge est de détourner l'usage du service de ping afin d'afficher le fichier index.php.

Le mot de passe de validation se trouve dans le fichier index. php



Copyright® Devoteam Page 4/6



#### 1.4. Challenge - XSS - Stockée 1

Le but de ce deuxième challenge est est volez le cookies de l'administrateur afin de valider l'épreuve

Merci de réaliser le challenge XSS - Stockée 1 dans la catégorie WEB-Client.



#### 1.5. Challenge - XSS - Stockée 2

Ce challenge est la suite du challenge ci-dessous, vous devez voler le cookie de session de l'administrateur et rendez-vous dans la section d'administration

Merci de réaliser le challenge XSS - Stockée 2 dans la catégorie WEB-Client.



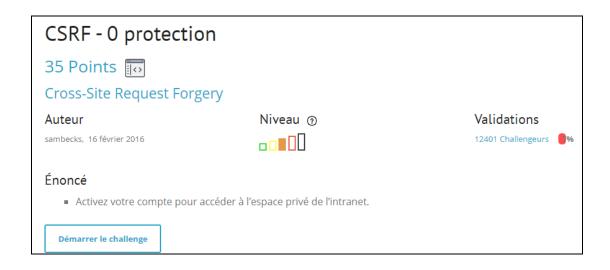
Copyright® Devoteam Page 5/6



#### 1.6. Challenge - CSRF - 0 Protection

Après avoir exploité les XSS, vous devez maintenant exploiter une CSFR sur le challenge CSRF - 0 protection disponible dans la **catégorie WEB-Client**.

Votre objectif est d'activer votre compte afin d'accéder à l'espace privé de l'intranet.



## 1.7. Challenge -The h@ckers I4b

Une agence de renseignements vient de prendre contact avec vous par email ; il semblerait qu'un groupe de hackers héberge ses outils, exploits en ligne. Il semblerait qu'il y ait quelques sploits intéressants, à vous de les dérober.

Merci de réaliser le The h@ckers l4b dans la catégorie réaliste

Copyright® Devoteam Page 6/6