

# M2 EPITA- Test d'intrusion



**Creative tech for Better Change**

TP 2 : Résolution de challenges - Plateforme RootMe

## Table des matières

<b>1. Objectifs et attentes</b>	<b>3</b>
1.1. Introduction	3
<b>1.2. Les challenges</b>	<b>4</b>
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

# 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 [url](#)

## 1.2. Les challenges

### 1.3. Challenge PHP - Injection de commande

Votre première mission sur site de RootMe est de résoudre le challenge [PHP - Injection de commande](#) dans la **catégorie web-serveur**.

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

## PHP - Injection de commande

10 Points 

Service de ping v1

**Auteur**  
sambecks, 20 septembre 2017

**Niveau**   


**Validations**  
36388 Challengeurs 

**Énoncé**  
Déterminez l'usage premier de ce service.  
  
Note : le mot de passe de validation est dans index.php.

Démarrer le challenge


**Validation**  
Entrer le mot de passe  
  
  
envoyer

## 1.4. Challenge - XSS - Stockée 1

Le but de ce deuxième challenge est de voler le cookie de l'administrateur afin de valider l'épreuve

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

### XSS - Stockée 1


30 Points 

Du gâteau !


Auteur

g0uZ, 3 mars 2012

Niveau ?



Validations

21537 Challengeurs 

Énoncé

Volez le cookie de session de l'administrateur et utilisez le pour valider l'épreuve.

## 1.5. Challenge - XSS - Stockée 2

Ce challenge est la suite du challenge ci-dessus, 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**.

### XSS - Stockée 2

50 Points 

Auteur

g0uZ, 4 mars 2012

Niveau ?



Validations

5107 Challengeurs 

Énoncé

Volez le cookie de session de l'administrateur et rendez-vous dans la section d'administration.


Démarrer le challenge

## 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.

### CSRF - 0 protection


35 Points 

Cross-Site Request Forgery


Auteur

sambecks, 16 février 2016

Niveau ?



Validations

12401 Challengeurs 

Énoncé

- Activez votre compte pour accéder à l'espace privé de l'intranet.

Démarrer le challenge

## 1.7. Challenge -The h@ckers l4b

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**