Résultats du challenge

Olivier Levillain, Grégory Blanc, Christophe Kiennert

RESSI 2019

16 mai – Erquy

Retour sur le challenge

- **4 groupes constitués**
  - 2 hardcores qui sont restés jusqu'au bout
- **Beaucoup de vulnérabilités trouvées dans l'ensemble**
- **Quelques fails**
  - Site Web avec quelques bugs
  - Voiture un peu capricieuse
  - Vulnérabilité XSS auto-patché
  - Accès Internet…
- **Quelques moment intenses**
  - Retard de 30 minutes au début qui a accentué l'état de zombification à la fin du challenge à 1h30 du matin
  - Contorsions pour garder la voiture en vie lors du lancement d'attaques pour l'envoyer dans le mur
  - La voiture qui se met à faire des virages

Retour sur les vulnérabilités et contremesures : voiture

- **Fragilités du fonctionnement de la voiture**
  - communication ModBus non sécurisée
  - application naïve de la consigne par la voiture

- **Attaques envisagées**
  - déni de service
  - crash (en avant toute !)

- **Contremesures**
  - ajouter un mécanisme de type « fail safe »
  - garantir l'intégrité des communications

Retour sur les vulnérabilités et contremesures : infrastructure

- **Fragilités de l'infrastructure**
  - réseau à plat sans filtrage !
  - comptes système avec mot de passe faible (+sudo)
  - clé SSH non protégée présente sur une machine

- **Mesures de sécurité possibles**
  - ajouter un firewall (quels flux ?)
  - nettoyer les comptes et les accès sudoers
  - superviser les connexions

Retour sur les vulnérabilités et contremesures : Web

- **Nombreuses failles dans le code**
  - Injection SQL pour se logger comme admin
  - Interface de chat vulnérable à des attaques XSS
  - Base de données en clair librement accessible
  - RFI possible via l'avatar utilisateur lors de la création du compte

- **Contremesures possibles**
  - Filtrer les entrées
  - Protéger l'accès à la BDD + stocker un hachage des mots de passe

Remerciements

- Au comité de pilotage
- Au département RST
- À Florian, Waël et Gabriel : pour nous avoir largement mâché le travail et pour nous avoir supportés en tant qu'encadrants
- Aux participants : pour leur investissement, leur bonne humeur et le partage des bières
- Aux non-participants qui sont passés faire coucou (voire faire la fermeture)
- À Lolo pour le cidre
- Pas au Wifi

Remise des prix

4. DROP TABLES;--

A /ragequit prématurément mais beaucoup de bonnes idées

Remise des prix

4. DROP TABLES;--

A /ragequit prématurément mais beaucoup de bonnes idées

3. Galettes Saucisses

Bonne vision des vulnérabilités mais ont fini par céder à l'attrait de la voiture en mouvement

Remise des prix

4. DROP TABLES;--

A /ragequit prématurément mais beaucoup de bonnes idées

3. Galettes Saucisses

Bonne vision des vulnérabilités mais ont fini par céder à l'attrait de la voiture en mouvement

2. Les Poneys Fringants

Très bonne analyse des vulnérabilités et plusieurs propositions de patchs

Remise des prix

4. DROP TABLES;--

A /ragequit prématurément mais beaucoup de bonnes idées

3. Galettes Saucisses

Bonne vision des vulnérabilités mais ont fini par céder à l'attrait de la voiture en mouvement

2. Les Poneys Fringants

Très bonne analyse des vulnérabilités et plusieurs propositions de patchs

Les gagnants : Les bouffeurs de foin

Exploits de vulnérabilités délicates et nombreuses propositions de patchs

Le mot de la fin

À l'année prochaine !