CR du 05/10/2021

Ordre du jour:
Description du plan de travail au cours des 15 prochaines semaines de projet.

Participants:
Grégory Blanc, Christophe Kiennert, Lorenzo Nadal Santa, Samson Mazeau.

Date de la prochaine réunion:
Mardi 12/10/2021 à 14h30, même salle de réunion BBB.

Points abordés:

- Proposition d'un plan de travail au cours de 15 semaines à venir (du 04/10/2021 au 25/10/2021)
    - *Semaine 1 (04/10/2021)* : entraînement / documentation sur les différentes attaques XSS.
    - *Semaine 2 à semaine 5 (du 11/10/2021 au 08/11/2021)*: Développement de la plateforme de test, comprenant le développement du front, du back, de la base de données et de la/les APIs.
    - *Semaine 6 à semaine 9 (du 15/11/2021 au 06/12/2021)*: Implémentation des scénarios et attaques modernes sur la plateforme de test.
    - *Semaine 10 à semaine 12 (13/12/2021 *vacances de Noël* au 10/01/2022):* Implémentation des détections des vulnérabilités.
    - *Semaine 13 à semaine 14 (10/02/2022 au 25/01/2022)*: rédaction du rapport, phase de correction de code (si nécessaire) et préparation de la soutenance.

Commentaires / remarques:

- Le plan de travail est validé par Mr Blanc et Mr Kiennert, bonne découpe et bien équilibré. Bonne marge de manœuvre en cas d'imprévu.
- Ne pas oublier la semaine Procci qui est habituellement chargée.
- Essayer de finir les majeures points essentiels/importants du projet avant les vacances de Noël.
- Essayer d'avancer le projet et le rapport écrit en parallèle.

- Il n’est pas nécessaire de dépenser deux semaines sur la réalisation d’attaques / challenges orientés XSS.
- Privilégié la plateforme WebAcademy pendant la *semaine 1*:
  https://portswigger.net/web-security
- Possibilité de choisir certains challenges sur des plateformes de CTF (RootMe / HackTheBox, etc).
- **VIGILANCE: il ne faut absolument pas négliger les notions de défense, détection et filtrage des attaques qui est une pratique très professionnalisante.** Cela constitue une vraie valeur ajoutée pour le PFE et pour notre CV.
- Bien distinguer les attaques XSS stockées / réfléchies et DOM based qui s'exécutent côté client ou côté serveur.

Objectif pour la prochaine réunion:

Faire une restitution sur “qu’est ce qu’une attaque XSS?”, “comment s’implémente t-elle?”.