CR du 19/11/2021

- Ordre du jour:

- Elaboration de plusieurs scénarios d'attaques,
- Validation de ces scénarios.

- Participants:

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

- Date de la prochaine réunion:

Mardi 30/11/2022 à 16h00.

Points abordés:

- Présentation des objectifs:
  - Scénariser 4 attaques en tout (XSS, CSP [utilisation de wildcard], CSP [autorisation d'origine détournée] et ClickJacking),
  - Lancer les scénarios d'attaque à partir d'un fichier json contenant les paramètres à utiliser,
  - Description détaillée des attaques envisagées.

Commentaires / remarques:

Beaucoup de remarques ont été faites durant cette réunion:

- Il nous a été conseillé d'implémenter une attaque "ancienne" HTTP response smuggling,

- Concernant l'attaque CSP[autorisation d'origine détournée] il est préférable de patcher nous même une librairie ou utiliser une ancienne libraire en Vue.js et utiliser cette librairie lors du build de l'application, c'est un point de départ pour cette attaque,

- Il faut garder en tête qu'il est crucial d'avoir un vecteur d'attaque, faire quelque chose de malveillant sur l'application (récupérer ou injecter de l'information.

- Pour le contournement de CSP, il serait intéressant de réfléchir en deux étapes: réussir un premier contournement de CSP mais ce contournement est bloqué par une seconde règle, il faut donc contourner la seconde pour réussir à contourner la première.
    - Par exemple, si l'on a un fichier scr, qui acceptera seulement une exécution des scripts locaux, il est possible de faire un contournement en injectant un script externe dans une image src laquelle sera alors considéré comme un fichier local.

    - Ou bien rendre un fichier externe exécutable lorsqu'un événement précis apparaît (OnClick, OnHandler, …).

- Concernant le ClickJacking, on a besoin d'obtenir une action de la victime que l'on ne peut pas simuler par un seasurf.
    - On force la victime à cliquer sur un endroit précis de la page.
    - L'utilisateur clique et on collecte son "click",
    - Quelle conséquence du clique?

- Il ya 3 types d'objectifs pour un ClickJacking
    1. Obtenir des likes sur des réseaux sociaux,
    2. Contourner le token CSRF de la victime,
    3. Activer un plugin vulnérable sur un browser.

- Il faut commencer à rédiger la documentation.

Objectif pour la prochaine réunion:

- Mettre en place le premier scénario d'attaque XSS.
- Commencer à rédiger la documentation.