Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquementFaille N°1

Pour la première faille sévère, nous pouvons retrouver des informations sur Semgrep :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Nous nous intéressons particulièrement à la ligne 18 car le problème rencontré et issu de cette ligne.

Une vulnérabilité provoquée est l’attaque XXE (XML External Entity).

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

En modifiant la ligne 19 de :

settings.DtdProcessing = DtdProcessing.Ignore; à settings.DtdProcessing = DtdProcessing.Ignore;

Cela empêche le parseur de rechercher ou de résoudre des entités externes, bloquant ainsi les attaques XXE.

Comme ça nous empêchons l’inclusions de fichiers externes qui peuvent interagir avec des systèmes internes de manière malveillante.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquementFaille n°2

Ici nous modifions la ligne 7.

En désactivant le traitement des DTDs externes avec libxml\_disable\_entity\_loader(true); nous fermons la porte aux attaques **XXE** et éliminons cette faille.

Cette fonction désactive le mécanisme de chargement d'entités XML externes. Cela signifie que le parseur XML ne pourra pas charger de fichiers externes ou faire de requêtes réseau via des entités déclarées dans le XML.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Faille n°3

LIBXML\_NONET au lieu de LIBXML\_DTDLOAD.

LIBXML\_DTDLOAD permet de charger des DTDs externes, ce qui est une mauvaise pratique pour la sécurité, car cela peut être utilisé par un attaquant pour effectuer une attaque XXE.

LIBXML\_NONET, empêche toute connexion réseau et le chargement d'entités externes. Cette option est beaucoup plus sûre car elle garantit que le parseur XML ne fera pas de requêtes réseau

Code corrigé :

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement