Exercice 3

Mathieu Da Vinha

Dans un premier temps, on crée un faux site web avec une vulnérabilité facile mais indétectable par Semgrep, ici on développe une page de connexion où une faille de type BROKEN ACCESS CONTROL est accessible.

*Une vulnérabilité Broken Access Control survient lorsqu’une application utilise un identifiant utilisateur dans une requête GET (ex: GET /index.html?id=1), permettant à un attaquant de modifier cet ID (ex: id=2) pour accéder aux données d’autres utilisateurs sans contrôle adéquat.*

On effectue un scan Semgrep

A black background with white text

Description automatically generated  
^ Résultat du scan pour notre index.html

Aucune vulnérabilité détectée

Puis on lance une détection DAST dans Zap :

A screenshot of a computer

Description automatically generated

Zap a détecté 9 vulnérabilités là où Semgrep n’en a pas détecté.

SAST (Semgrep) analyse le code statiquement, sans exécution, idéal pour détecter des vulnérabilités en amont (code mal écrit). DAST (ZAP) teste l'application en fonctionnement, détectant des risques runtime (configurations, entrées non sécurisées). Semgrep a manqué la vulnérabilité dans la requête GET car elle dépendait du contexte d'exécution ou d'un flux de données non traçable dans le code, tandis que ZAP l'a repérée en simulant une attaque réelle.