UQAC

Département d'informatique et de mathématique
Université du Québec à Chicoutimi

Travail pratique #3

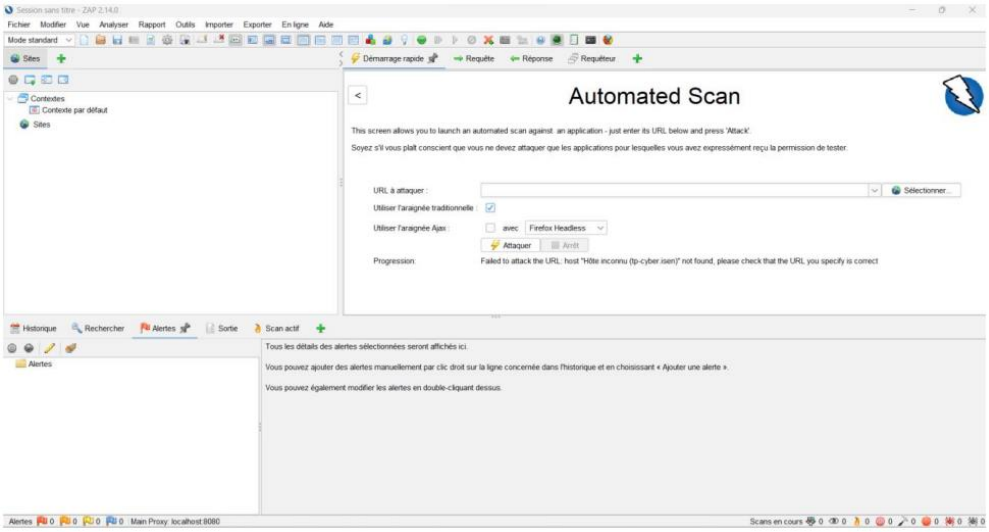
Objectifs du travail pratique

- Se familiariser avec un autre scanner de vulnérabilités
- Se familiariser avec les vulnérabilités d'applications Web
- Réaliser un audit de sécurité
- Comprendre et élaborer les étapes d'un audit de sécurité
- Réaliser un audit de sécurité de la plateforme web https://juice-shop.herokuapp.com de OWASP à l'aide de l'outil ZAP OWASP.

Exigences

1. Installation et configuration:

- Téléchargez et installez ZAP OWASP sur votre ordinateur : https://www.zaproxy.org/download/
- ZAP nécessite d'avoir une JDK d'installé sur votre machine. Si ce n'est pas le cas, télécherger la jdk qui correspond à votre machine : https://www.oracle.com/java/technologies/downloads
- Si vous avez correctement installé les deux éléments ci-dessus, vous devriez pouvoir exécuter ZAP :



- Configurez ZAP OWASP pour scanner la plateforme Juice Shop; c'est simple, on spécifie l'adresse dans le champ **URL à attaquer**.

2. **Analyse des Vulnérabilités:**
   - Lancez un scan complet de Juice Shop avec ZAP OWASP.
   - Identifiez et documentez les vulnérabilités OWASP découvertes.
   - Pour chaque vulnérabilité, indiquez :
     - La catégorie OWASP à laquelle elle appartient.
     - La description de la faille.
     - Le niveau de gravité.
     - Les preuves d'exploitation (si possible).

3. **Exploitation d'une vulnérabilité**
   - Choisissez une vulnérabilité à exploiter.
   - Utilisez des techniques appropriées pour exploiter la vulnérabilité choisie.
   - Documentez les résultats de l'exploitation.

4. **Réaliser un audit de sécurité**

   - Rédaction d'un rapport;
   - Rédigez un rapport d'audit clair et concis qui présente au minimum :
     - Les objectifs de l'audit.
     - La méthodologie utilisée.
     - Les résultats de l'analyse des vulnérabilités.
     - Les conclusions et recommandations.

Vous êtes encouragés à faire preuve d'initiative et d'originalité et pouvez vous aider avec des gabarits ou des normes pré-établies.

Évaluation

L'évaluation sera basée sur les éléments suivants :

- (60%) La qualité du rapport d'audit.
- (15%) La précision et la complétude de l'analyse des vulnérabilités.
- (25%) La capacité à exploiter une vulnérabilité.

Document à remettre

- Rédiger un document PDF contenant les étapes 2-3-4 ci-dessus. N’hésitez pas à y inclure des captures d’écrans.

Date de remise

Le vendredi 26 avril 2024 via le Moodle du cours.