DOCUMENT DE CADRAGE DE LA SAÉ 36

Découvrir le pentesting :

Audit de sécurité d'une application Web

VERSION 1.0 DU 11 JANVIER 2023

1. Contexte professionnel de la SAÉ 36

Vous êtes un pentester et vous êtes en charge de la sécurité des applications Web. Vous devez auditer l'application Web d'un client.

2. Objectifs de la SAÉ

Vous êtes maintenant à la fin du semestre 3 et les SAÉ vont être de moins en moins guidées pour vraiment travailler l'autonomie. Le sujet de la SAÉ sera donc assez court et vous n'aurez pas de planning prévisionnel. Cette fois-ci c'est à vous de vous organiser !

L'objectif de la SAE est de faire un rapport d'audit d'une application Web. Vous travaillerez sur les applications Web fournies sur la machine virtuelle OWASP broken Web apps que vous avez installé lors des TP du module R317 introduction au pentest.

Vous tirerez au sort une machine et devrez faire un rapport de test sur cette machine. Le rapport de test devra expliquer en détail la faille de sécurité : principe général de la faille, cas particulier sur l'application et remédiation.

Vous êtes 15 étudiants et vous ferez 3 groupes de 5 pour travailler sur les 3 machines suivantes :

- Damn Vulnerable Web application DVWA
- bWAP
- OWASP Mutilidae II

Votre rapport de tests devra traiter :

- DVWA : injections SQL, injections SQL aveugles, Upload, CSRF pour les 3 niveaux de difficulté
- bWAP : l'ensemble des injections SQL et XSS
- OWASP Multidae II (OWASP 2013) : injections SQL et broken authentication and session management

Quand vous aurez fini ces tests vous devrez écrire un programme Python pour récupérer automatiquement un élément de la base de la base de données dans le cas d'une injections SQL aveugle.

A vous de vous organiser pour vous répartir les tâches et vous aider.

3. Organisation

- Durée de la SAÉ : 8 jours du 16 au 19 janvier et du 23 au 26 janvier, soutenance le 27 janvier après-midi.
- Nombre d'étudiants par groupe : 5

4. Livrables et présentation

Vous devrez fournir comme livrables :

- Votre rapport de test au format pdf
- Une présentation orale avec des slides

La soutenance se déroulera dans la salle de TP avec vos slides et la démonstration des failles sur la machine qui vous a été assignée. Vous aurez 50 minutes de présentation par groupe et 10 minutes de questions.