Projet Final : Audit de Sécurité et Pentest Web (DVWA)

Module : Cybersécurité & Réseaux

Enseignant : Prof. Azeddine KHIAT

Cible de test : testphp.vulnweb.com(Reconnaissance) & Lab Local (Exploitation)

Date limite : 07 janvier 2026 avant 23:59

Introduction

Ce projet constitue l'aboutissement de vos travaux pratiques. Il s'agit de la suite directe de l'atelier **"Atelier DVWA sur Kali avec Docker Compose_2LIA"**. L'objectif est de passer d'une simple installation à une véritable démarche d'auditeur sécurité (**Pentester**).

---

1. Rappel Technique : Démarrage du Lab

Le projet doit impérativement se situer dans le répertoire **`dvwa-compose-lab`**. Assurez-vous que votre environnement est opérationnel avant de commencer les tests.

Procédure de démarrage (Terminal Kali) :

1. **Accédez au répertoire** : `cddvwa-compose-lab`
2. **Lancez les conteneurs** : `docker-compose up -d`
3. **Vérifiez le service** : `docker ps`
4. **Accès Web** : http://localhost(oul'IP de votre machine Docker).

Consigne : Si vousn'avez pasencoreinstallé DVWA via Docker, ce projet est l'occasion de le faire.C'est un prérequis indispensable.

---

2. Phase 1 : Reconnaissance et Analyse (Nmap & Wireshark)

Cette phase s'effectue sur la cible : `testphp.vulnweb.com.`

- **Nmap (Options d'apprentissage) :**
  - `nmap -sV` : Identification desversions des services.
  - `nmap -A` : Scan agressif (OS,scripts, traceroute).

- `nmap --script http-vuln-cve2017-10010` : Scan de vulnérabilités spécifiques.

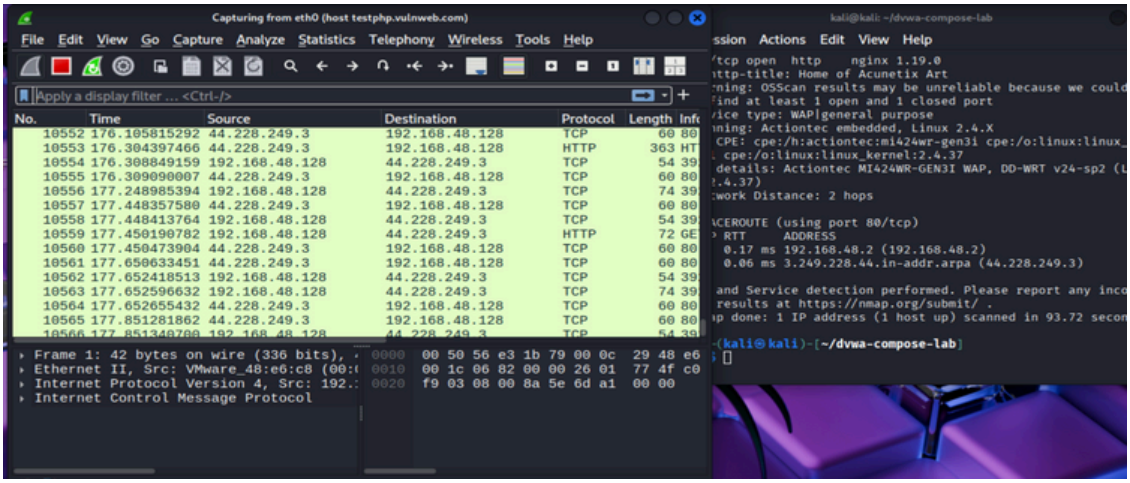
• **Wireshark:** Analysez le trafic pendant le scan Nmap pour identifier les paquets TCP (SYN/ACK).

Captures d'écran attendues :

- **Capture 1** : Résultat du scan nmap -A détaillé.
- **Capture 2** : Interface Wireshark montrant les flux générés par le scan.

```
┌──(kali㉿kali)-[~/dvwa-compose-lab]
└─$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-08 18:38 E
ST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.017s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9
b::2ce4:f903
rDNS record for 44.228.249.3: 3.249.228.44.in-addr.arpa
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect resu
lts at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.03 seconds
```



---

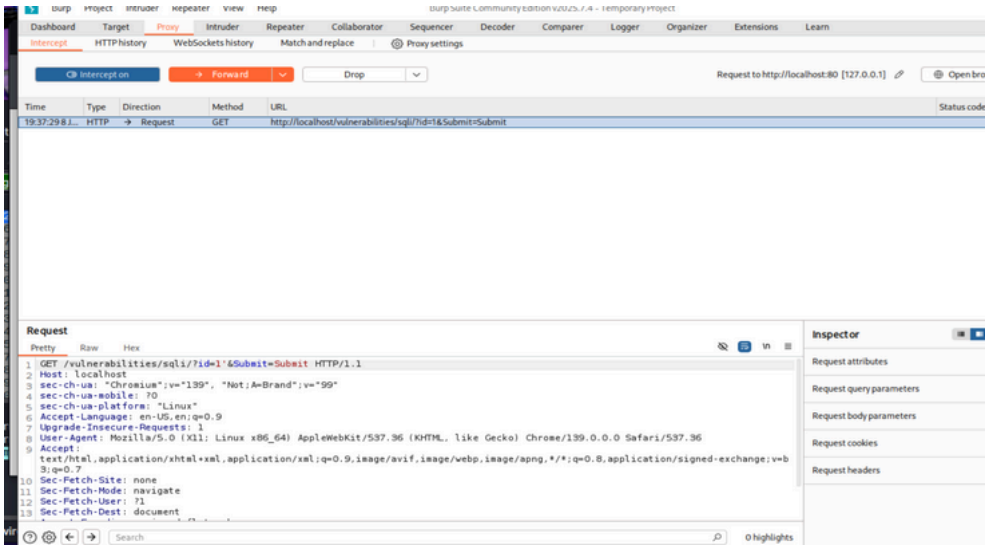
3. Phase 2 : Pentest Applicatif (OWASP Top 10)

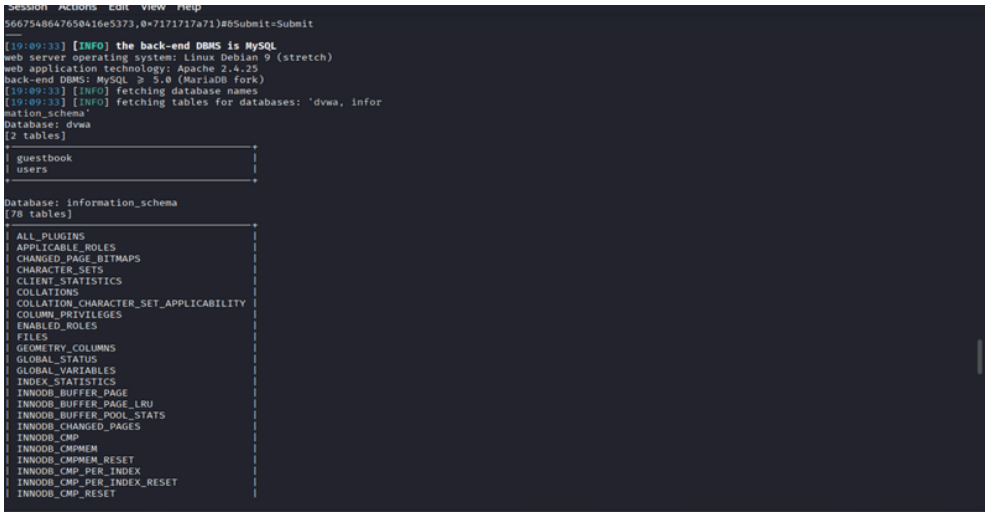
L'exploitation se fait sur votre lab local dans `dvwa-compose-lab`.

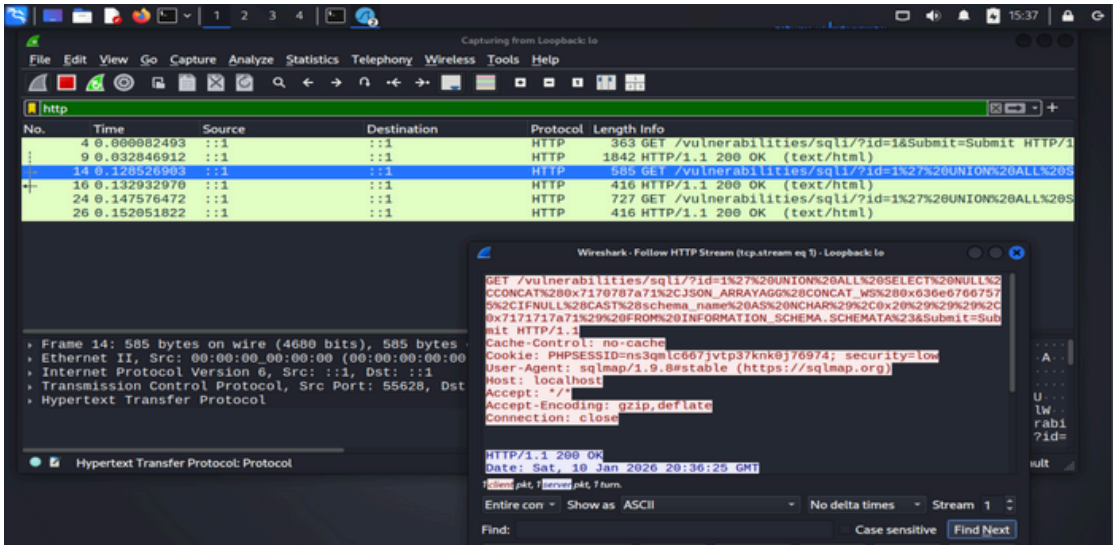
- **SQL Injection (SQLi):**Utilisez sqlmap pour extraire lesbases de données.
- **Interception (Burp Suite):** Modifiez les paramètres de requête en temps réel.
- **AnalyseRéseau (Wireshark):** Capturez le flux HTTP pendant l'attaque pour voir les données circuler en clair.

Captures d'écran attendues :

- **Capture 3** : Requête interceptée et modifiée dans **Burp Suite**.
- **Capture 4** : Succès de l'extraction des tables via **SQLmap**.
- **Capture 5** : Analyse Wireshark (Filtre http) montrant la charge utile de l'attaque.







---

4. Ce qui est attendu dans le Rapport (PDF)

Votre rapport doit être clair, bien structuré et contenir obligatoirement :

- **Page de garde** : Logo, Titre, Votre nom, Prof. Azeddine KHIAT, Année 2025/2026.
- **Analyses détaillées** : Expliquez *pourquoi* vous utilisez tel outil ou telle option.
- • **Contextualisation OWASP** : Reliez chaque faille trouvée à une catégorie du
- **OWASP Top 10**.
  Remédiation : Proposez une solution technique pour chaque faille découverte.
  Lien GitHub : Vers votre dépôt dvwa-compose-lab.

---

5. Présentation Vidéo (~7 minutes)

Chaque étudiant doit déposer le compte rendu et la séquence vidéo sur Classroom:

1. **Vue d'ensemble** : Présentation de la topologie et du lab Docker.
2. **Démonstration Nmap** : Explication des options et résultats.

3. **DémonstrationPentest** : Exploitation en direct d'une faille (SQLi ou XSS).
4. **Analyse Wireshark** : Preuve visuelle du trafic d'attaque.
5. **Conclusion** : Résumé des objectifs atteints.

À la fin de votre rapport, vous devez impérativement ajouter une **section d'explications** et une **conclusion générale**. Ce projet ne consiste pas uniquement à exécuter des commandes ou à insérer des captures : vous devez démontrer une véritable démarche d'audit. Pour chaque étape réalisée (reconnaissance sur **testphp.vulnweb.com** avec **Nmap** et **Wireshark**, puis exploitation sur votre lab local **DVWA** avec **Burp Suite**, **SQLmap** et **Wireshark**), expliquez clairement **l'objectif**, **l'outil utilisé**, **ce que vous observez**, et **ce que cela signifie en termes de sécurité**. La conclusion devra récapituler le travail effectué, mettre en évidence les vulnérabilités identifiées/exploitées (ex : **SQLi**, interception et modification de requêtes, extraction de données, trafic HTTP en clair), et proposer des **recommandations de correction** (au minimum 4) adaptées à un contexte réel. Un rapport sans explications ni conclusion sera considéré comme incomplet.