Attaque par Force Brute sur DVWA

1. Présentation

Ce TP consiste à exploiter une vulnérabilité de type **Brute Force** sur l'application DVWA installée sur Kali Linux

Contexte

- Cours / Formation : U7 Cybersécurité
- Date : 03/03/2026
- Type : Individuel
- Durée : 2h

---

2. Objectif

- Comprendre le concept de force brute
- Observer le comportement d'un formulaire d'authentification
- Exploiter la vulnérabilité en difficulté *Low*
- Utiliser Burp Suite pour automatiser l'attaque
- Analyser les réponses serveur

---

3. Environnement technique

- VM Kali Linux
- DVWA installé en local
- Apache démarré
- MariaDB démarré
- Outil : Burp Suite

Identifiants :

- Kali : `kali / kali`
- DVWA : `admin / password`

---

4. Mise en place de l'environnement

Démarrage des services :

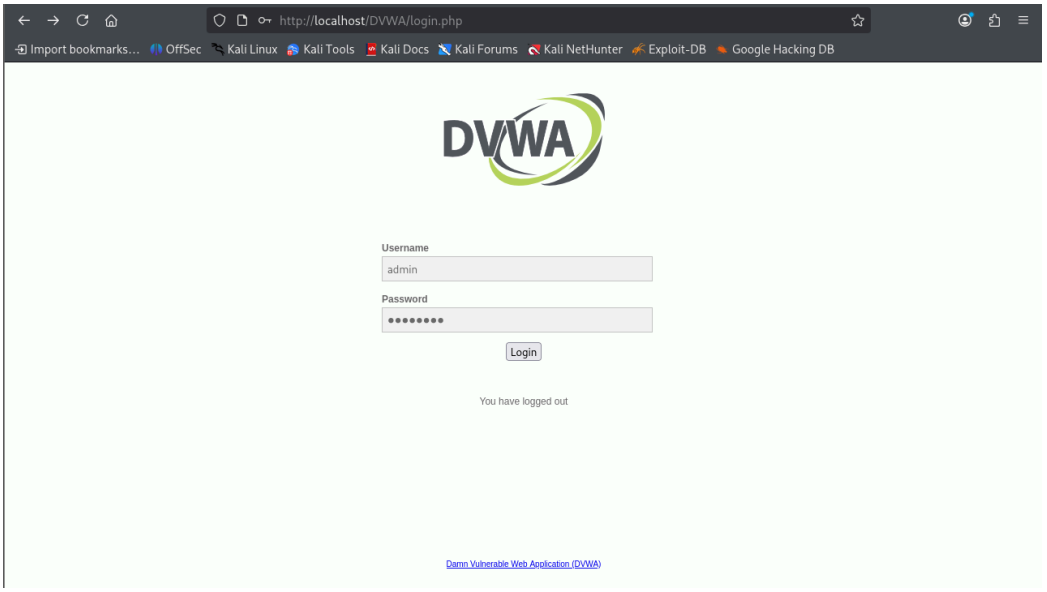
```
sudo systemctl start apache2
sudo systemctl status apache2
sudo service mysql start
sudo service mysql status
```

Accès à DVWA :

```
http://localhost/setup.php
```

Initialisation de la base si nécessaire.

Capture – Page login DVWA



---

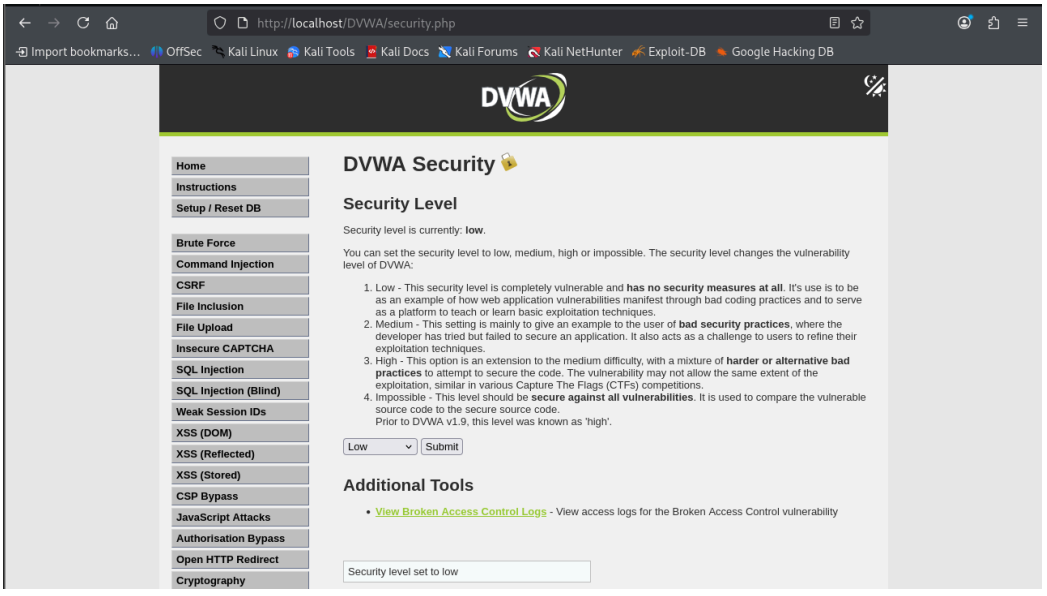
5. Configuration du niveau de sécurité

Connexion avec :

```
admin
password
```

Navigation :
DVWA Security → Sélectionner **Low** → Submit

Capture – Niveau Security Low



6. Observation du comportement (phase reconnaissance)

Aller dans :

Vulnerability → Brute Force

Tester manuellement :

- admin / password
- admin / mauvaispassword

Observer :

- Messages d’erreur
- Différences de comportement
- Réponses serveur

Cette étape permet de comprendre le fonctionnement du système avant automatisation.

---

7. Analyse du code et découverte d’informations

Utiliser :

Clic droit → Inspecter (Inspect Element)

Repérer :

```
src=/hackable/users/admin.jpg
```

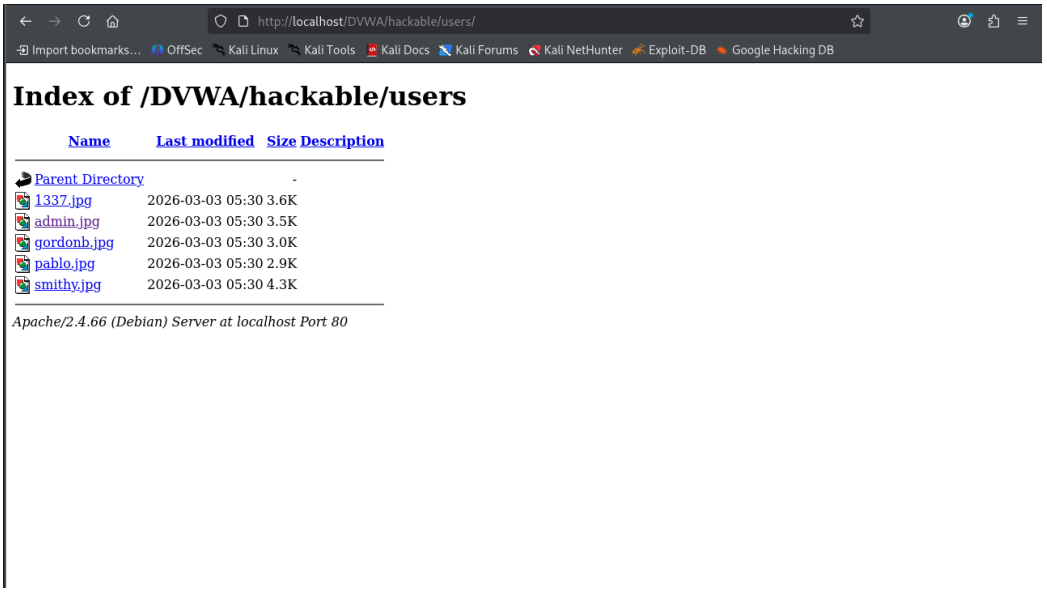
En accédant à :

```
http://localhost/hackable/users/
```

On découvre plusieurs utilisateurs

- admin
- gordonb
- pablo
- smithy
- 1337

Capture – Index of /hackable/users



8. Introduction à Burp Suite

Ouvrir Burp Suite.

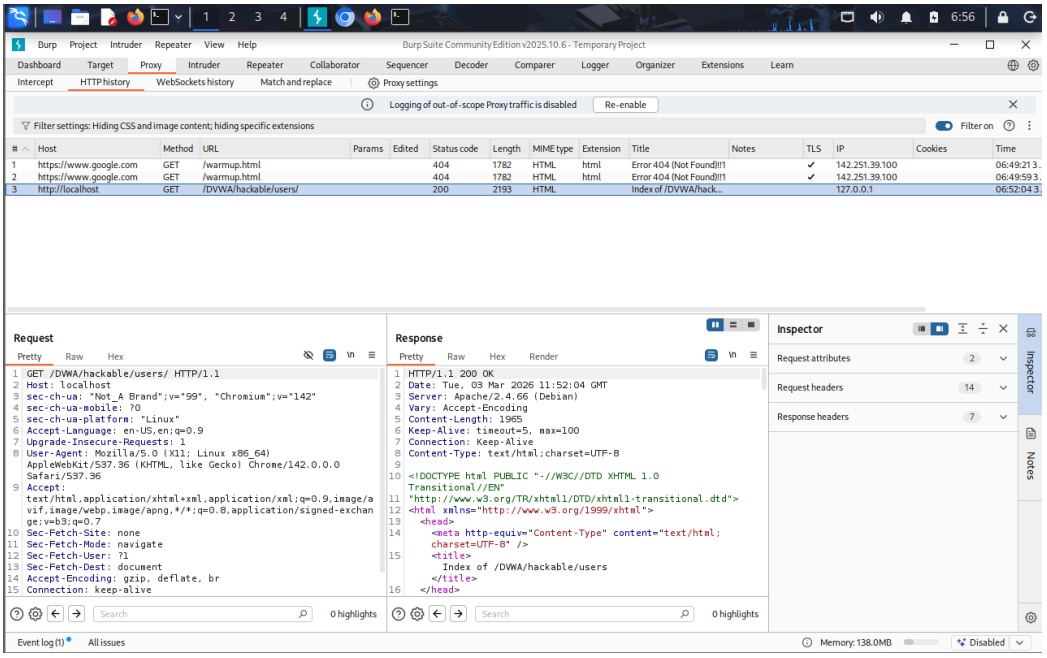
Dans l'onglet **Proxy** :

- Vérifier que "Intercept is off"
- Cliquer sur "Open Browser"

Ajouter la cible au scope :

Target → click droit → Add to scope

Capture – Burp Proxy ouvert



9. Capture du paquet Login

Dans le navigateur Burp :

Faire un login normal.

Dans Burp :

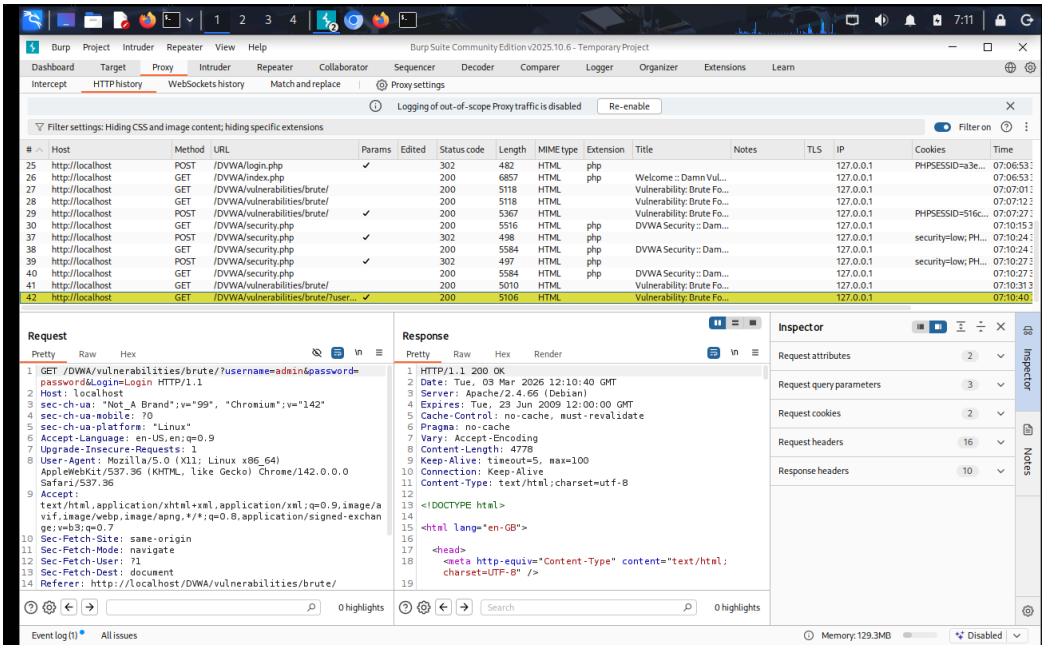
Proxy → HTTP History

Identifier le paquet responsable du login

Click droit → Highlight

Click droit → Send to Intruder

Capture – Paquet responsable du login



10. Configuration de l'attaque (Intruder)

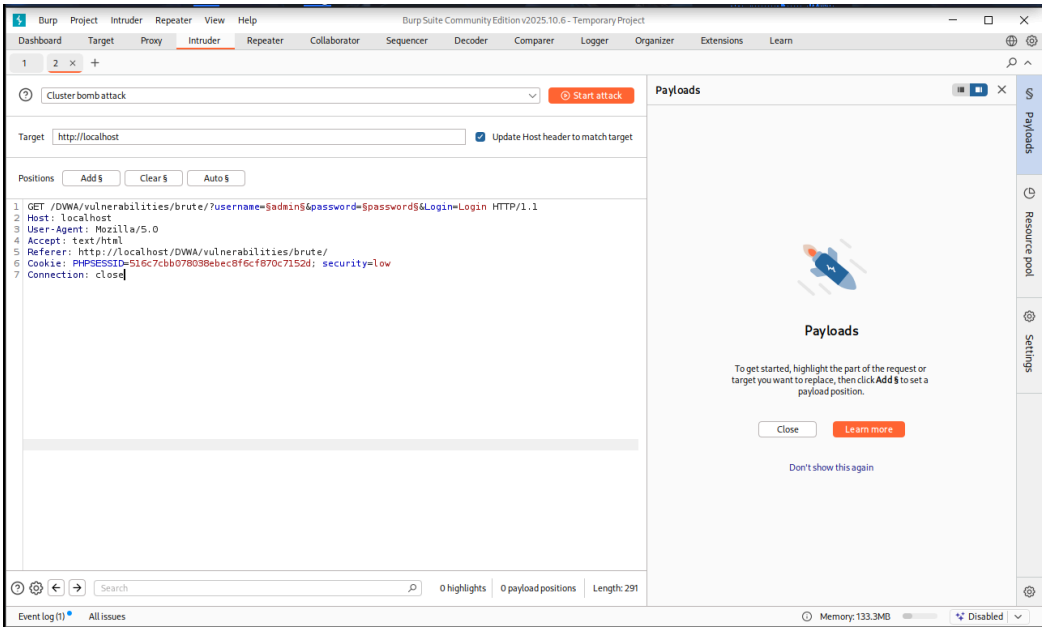
Dans l'onglet **Intruder** :
Attack type → **Cluster Bomb**

Définir les variables :

```
username=§admin§
password=§password§
```

Supprimer les autres §.

Capture – Cluster Bomb Attack



11. Configuration des Payloads

Payload 1 – Username

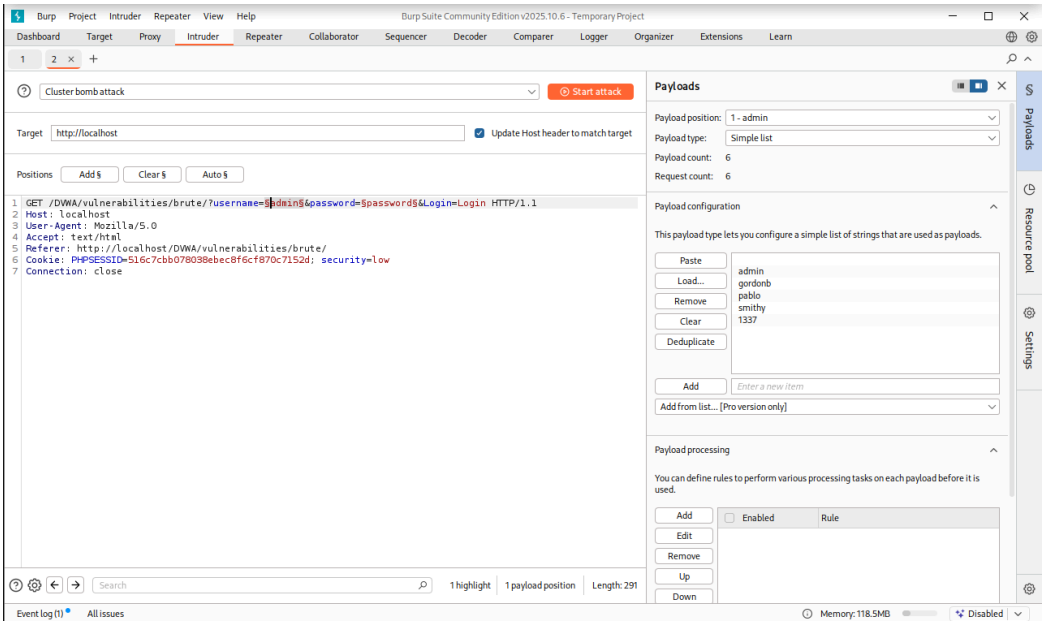
Payload set : 1

Payload type : Simple list

Ajouter :

- admin
- gordonb
- pablo
- smithy
- 1337

Image



Payload 2 – Password

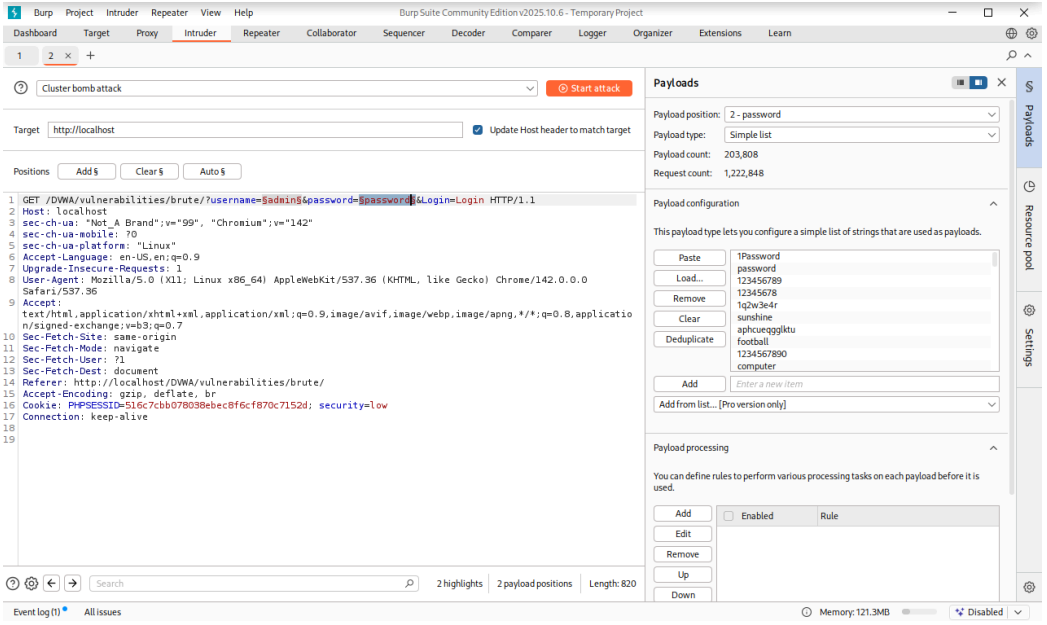
Payload set : 2

Payload type : Simple list

Charger le fichier :

```
/usr/share/dict/wordlist-probale.txt
```

Image



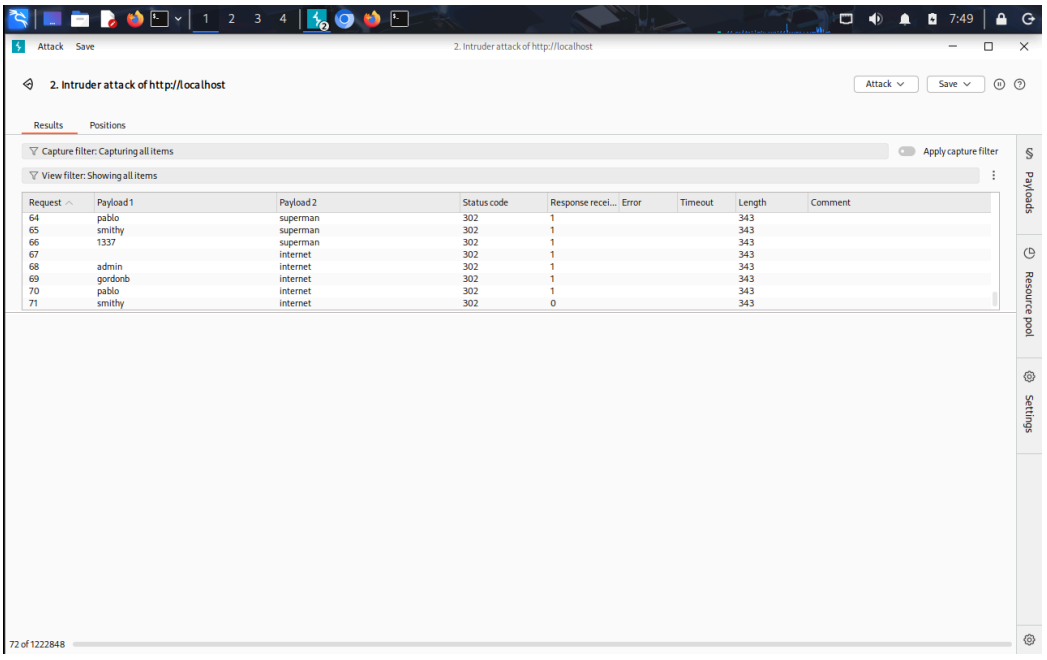
12. Lancement de l'attaque

Cliquer sur **Start Attack**

Analyser :

- Longueur des réponses
- Codes HTTP
- Différences dans les réponses réussies

Capture – Résultats Intruder



---

13. Test en difficulté Medium

Changer niveau :

DVWA Security → Medium

Reprendre l'exercice.

Lire la section "View Help" pour comprendre les changements

Comparer le comportement avec le niveau Low.

---

14. Outils alternatifs

Rechercher et tester :

- wfuzz
- hydra

Ces outils permettent une exécution plus rapide de l'attaque.

---

15. Conclusion

Ce TP a permis de comprendre le fonctionnement d'une attaque par force brute sur une application web vulnérable.

L'utilisation de Burp Suite a permis d'analyser le trafic HTTP, de manipuler les requêtes et d'automatiser les tentatives d'authentification.

La différence de comportement selon le niveau de sécurité (Low / Medium) montre l’importance des mécanismes de protection contre les attaques par force brute.

Alexis DE JESUS - BTS SIO SLAM