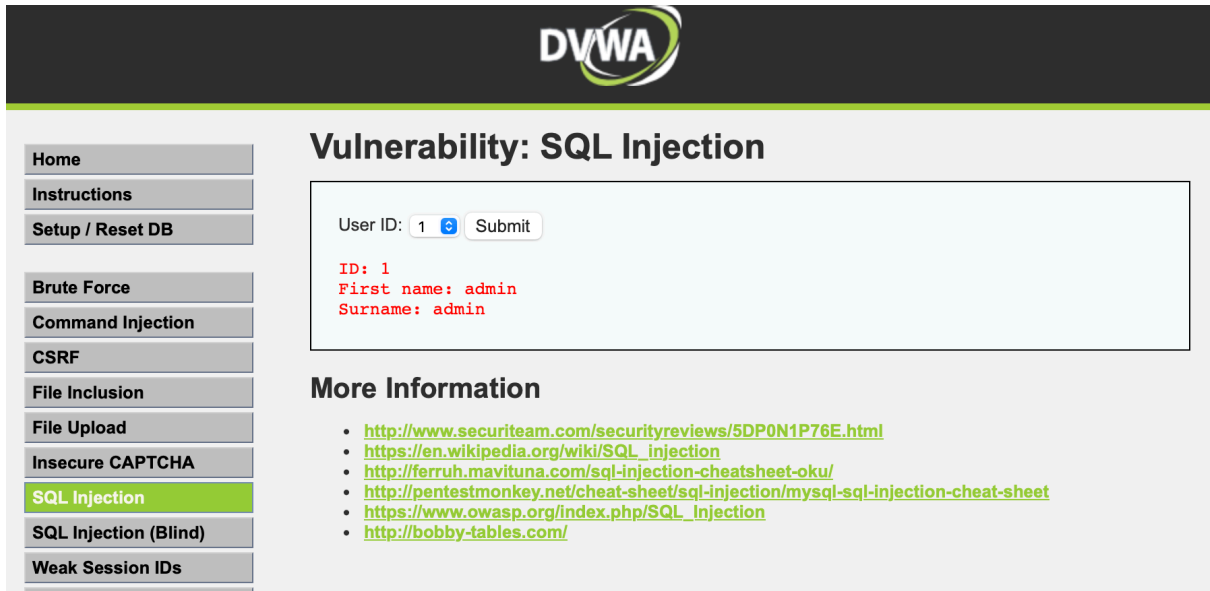


TP INJECTION SQL

SECURITY : MEDIUM



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

Vulnerability: SQL Injection

User ID:

ID: 1
First name: admin
Surname: admin

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Pour injecter des commandes sql dans ce type d'entrée, nous allons utiliser Burpsuite. Référez-vous au document permettant de répéter une requête avec Burpsuite.

Pour le 3 premières questions, il est demandé d'utiliser des injections SQL manuelles :

1. Récupérer le nom de la table utilisateur.
2. Récupérer le nom des colonnes de la table utilisateur pour obtenir le username et le password.
3. Récupérer le nom des colonnes de la table utilisateur.
4. Retrouver les résultats précédents en utilisant sqlmap.