freeloader9527 / **repro.md** Secret

Created last week

Code Revisions 1

Unauthenticated SQL Injection in Hotel Management System

repro.md

Vulnerability Report: Unauthenticated SQL Injection in Hotel-Management-System

0x01 Summary

- **Target**: Hotel-Management-System
- **Vulnerability**: Unauthenticated Time-based Blind SQL Injection
- **Vulnerable Parameter**: `id` in `/admin/roomdelete.php` (and others)
- **CVSS Score**: **9.8 (Critical)**

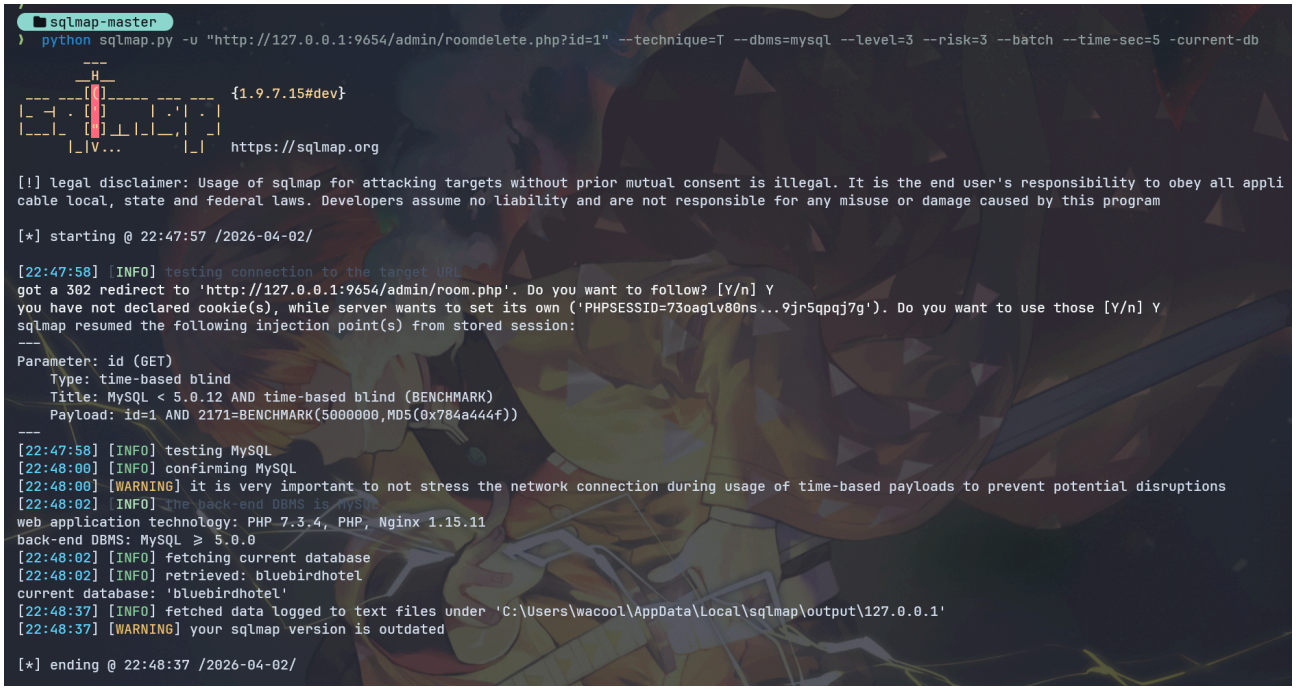
0x02 Description

The administrative endpoint `/admin/roomdelete.php` does not implement session authentication. Furthermore, the `id` parameter is directly concatenated into the SQL query without any sanitization or parameterization, allowing remote attackers to execute arbitrary SQL commands.

0x03 Proof of Concept (PoC)

Using **sqlmap**, the vulnerability can be verified with the following command:

```
python sqlmap.py -u "http://[TARGET_IP]:[PORT]/admin/roomdelete.php?id=1" \
--technique=T --dbms=mysql --level=3 --risk=3 --batch --time-sec=5 --current-
```



Analysis

The injection is a **Time-based Blind SQLi**. An attacker can exfiltrate the entire database, including administrator credentials and sensitive guest information, or perform destructive operations (e.g., deleting all rooms/records).

0x04 Mitigation

1. **Authentication**: Enforce session/role checks at the top of every PHP file in the `admin/` directory.
2. **Prepared Statements**: Use parameterized queries (e.g., PDO or MySQLi prepared statements) to handle user input securely.