SQL Injection vulnerability was found in "login.php" in SourceCodester Prison Mangement System V1.0 allows allows ATTACKER to execute arbitrary SQL commands via the "txtmail" parameter of Employee Login page.

Affected Vendor: GitHub (https://github.com/)

Product Official Website URL: PHP-Bookstore-Website-Example 1.0 (https://github.com/ywxbear/PHP-Bookstore-Website-Example)

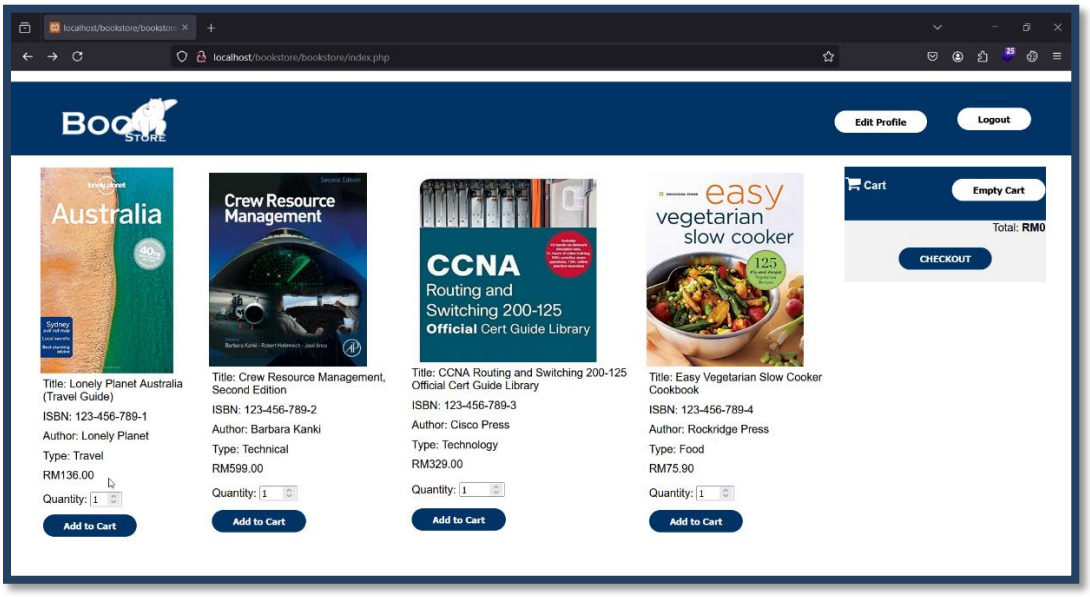
Version: 1.0

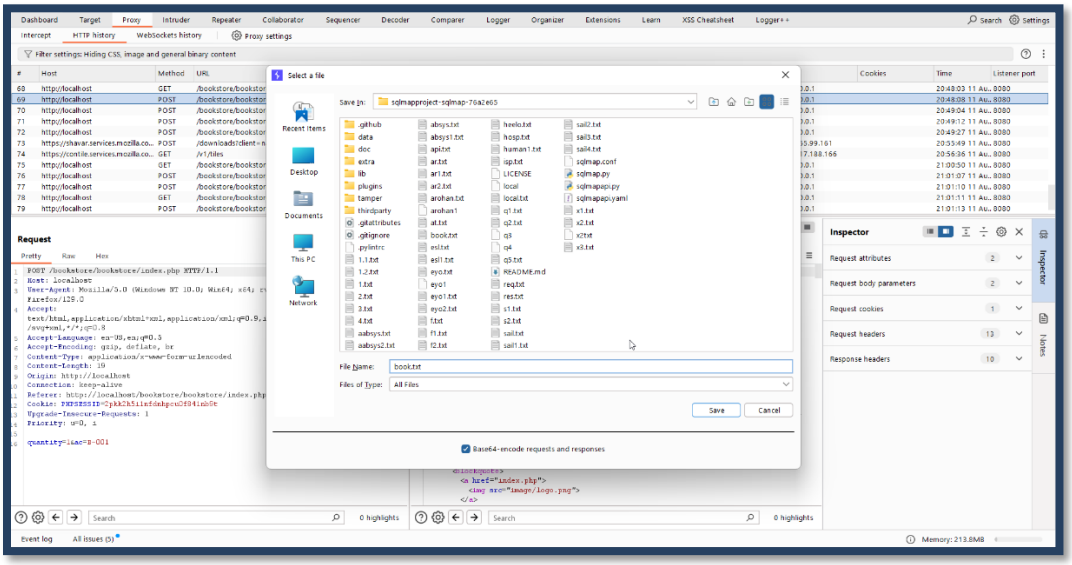
Affected Components:

- **Affected Endpoint:** `index.php` [checkout (parameter)]

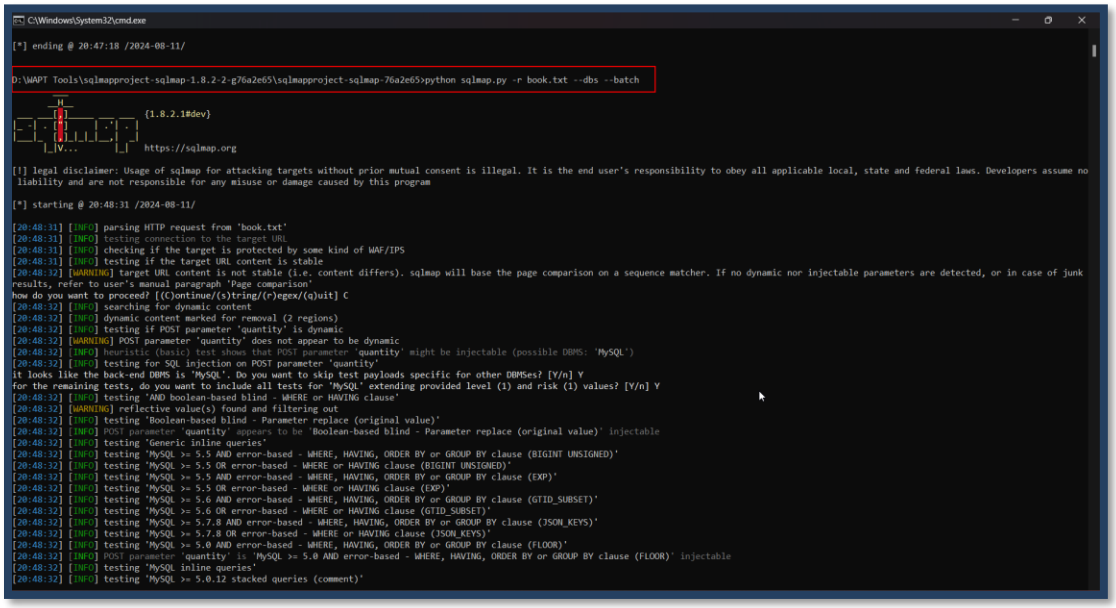
Steps:

1. After login into the application trying to buy a book (URL: http://localhost/bookstore/bookstore/index.php).
2. Capture the Request with Burpsuite and Save it.

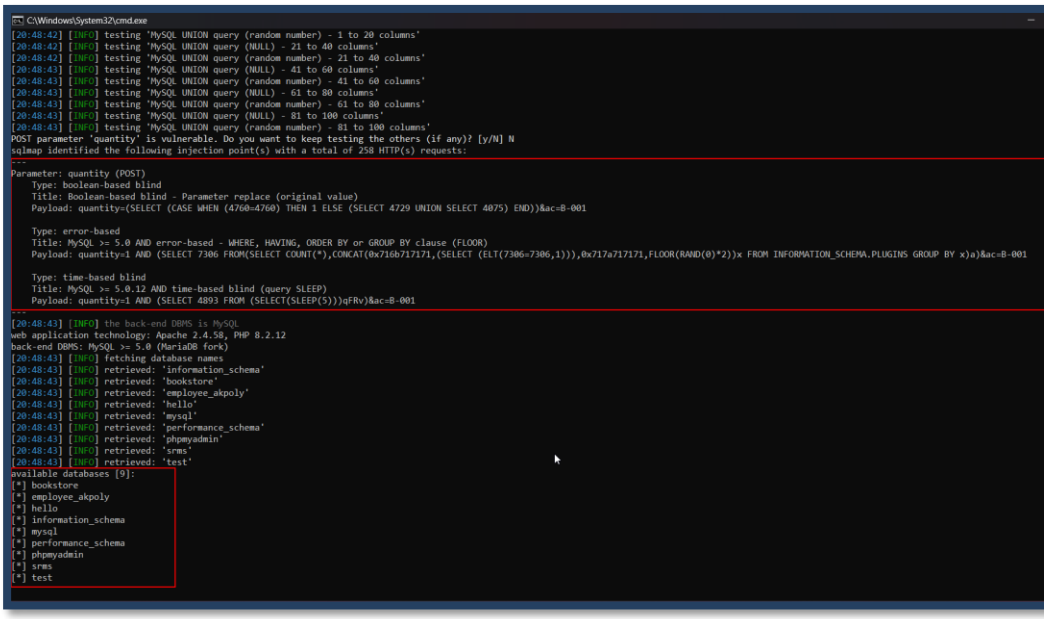




3. Run SQLmap with the saved request.



4. We can see all the database.
5. We can dump the data with SQLmap.



Impact: An attacker can retrieve sensitive information like usernames, passwords, credit card numbers, or personal details from the database, leading to data breaches. The attacker can modify or delete existing data. For example, they might change financial records, alter product prices, or delete critical information. SQL injection can allow an attacker to bypass authentication mechanisms, leading to unauthorized access to accounts, enabling them to impersonate other users, including administrators.

Solution/Good Reads:

1. Parameterized Queries
2. Input Validation and Sanitization

Links:

1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
2. https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection

References:

- https://owasp.org/www-community/attacks/SQL_Injection
- https://cwe.mitre.org/data/definitions/89.html