DAKSH

SOURCE CODE REVIEW ASSIST (SCRA)

ABC Online Bookstore Application

Daksh SCRA – Source Code Analysis Report

May 05, 2023

Scan Summary

Note: At the moment, the summary section is still being developed and only includes sample information. While not restricted to these, the section will feature the following details.

```
Inputs received:
    [*] Rule Selected        = 'php'
    [*] File Types Selected  = 'php'
    [*] Target Directory     = '../../Code/Platform/PHP/online-book-store/'
    [*] Filetypes Selected: ['*.php', '*.ini', '*.txt', '*.config', '*.xml', '*.lock',
'.htaccess']

Detection Summary:
    [*] Total files scanned: 44
    [*] File Extentions Identified: ['.php', '.txt']
    [*] Areas of interests identified: 200

Scan Duration:
    [*] Scan Start Time: 2023-04-30 12:44:53
    [*] Scan End Time: 2023-04-30 12:44:53
    [*] Total Time Taken: 2023-04-30 12:44:53
```

Security - Areas of Interest

This section lists the key areas within the source code that need to be examined for identifying potential security weaknesses.

The code reviewer should carefully examine the identified areas and review any reported code snippets and file paths to validate the presence of any potential vulnerabilities. The validation process should involve a thorough analysis of the code and its associated components to determine the extent of the potential security risk. Any issues identified during the validation process should be documented.

[+] Keyword Searched : Tainted Inputs: $_GET

- Source File : online-book-store/secure/admin_delete.php

```
[2]        $book_isbn = $_GET['bookisbn'];
```

- Source File : online-book-store/secure/admin_edit.php

```
[9]        if(isset($_GET['bookisbn'])){
[10]                $book_isbn = $_GET['bookisbn'];
```

- Source File : online-book-store/secure/book.php

```
[3]  $book_isbn = $_GET['bookisbn'];
```

- Source File : online-book-store/secure/bookPerPub.php

```
[5]        if(isset($_GET['pubid'])){
[6]                $pubid = $_GET['pubid'];
```

- Source File : online-book-store/secure/checkout.php

```
[6]                                book_isbn (get from $_GET['book_isbn']) => number of books
```

[+] Keyword Searched : PHP_SELF XSS

- Source File : online-book-store/secure/admin_add.php

```
[31]                        $directory_self = str_replace(basename($_SERVER['PHP_SELF']), '',
$_SERVER['PHP_SELF']);
```

- Source File : online-book-store/secure/edit_book.php

```
[17]                $directory_self = str_replace(basename($_SERVER['PHP_SELF']), '',
$_SERVER['PHP_SELF']);
```

[+] Keyword Searched : SELECT [*] FROM [anytable] WHERE

- Source File : online-book-store/secure/admin_add.php

```
[39]                $findPub = "SELECT * FROM publisher WHERE publisher_name = '$publisher'";
```

- Source File : online-book-store/secure/admin_edit.php

```
[22]        $query = "SELECT * FROM books WHERE book_isbn = '$book_isbn'";
```

- Source File : online-book-store/secure/book.php

```
[8]  $query = "SELECT * FROM books WHERE book_isbn = '$book_isbn'";
```

- Source File : online-book-store/secure/edit_book.php

```
[27]        $findPub = "SELECT * FROM publisher WHERE publisher_name = '$publisher'";
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Take.php

```
[202]            $this->stat=$this->conn->prepare("SELECT image FROM book WHERE book_id=?");
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

```
[514]            SELECT * FROM admin WHERE user_name=?;
[562]            SELECT * FROM author  WHERE name=?;
[577]            SELECT * FROM genre  WHERE genre_desc=?;
```

- Source File : online-book-store/secure/functions/database_functions.php

```
[36]                $query = "SELECT orderid FROM orders WHERE customerid = '$customerid'";
[58]                $query = "SELECT book_price FROM books WHERE book_isbn = '$isbn'";
[101]                $query = "SELECT publisher_name FROM publisher WHERE publisherid = '$pubid'";
```

[+] Keyword Searched : SELECT ORDERBY

- Source File : online-book-store/secure/publisher_list.php

```
[6]        $query = "SELECT * FROM publisher ORDER BY publisherid";
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

```
[467]            SELECT publisher_id,name FROM publisher ORDER BY  2 ");
[535]            SELECT * FROM admin ORDER BY admin_id;
[549]            SELECT * FROM author  ORDER BY name;
[593]            SELECT * FROM genre  ORDER BY genre_desc;
```

- Source File : online-book-store/secure/functions/database_functions.php

```
[13]                $query = "SELECT book_isbn, book_image FROM books ORDER BY book_isbn DESC";
[117]                $query = "SELECT * from books ORDER BY book_isbn DESC";
```

[+] Keyword Searched : Password

- Source File : online-book-store/secure/verify.php

```
[11]        $query = "SELECT username, password FROM admin";
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Take.php

```
[48]          $this->stat=$this->conn->prepare('INSERT INTO customer (customer_id, name, address_id, email, phone, password) VALUES (?,?,?,?,?,?)');
```

- Source File : online-book-store/secure/database/readme.txt.txt

```
[6]To change the localhost, username, password for connecting to database, change it only one time in
```

[+] Keyword Searched : Misc Modules (Admin|Administrator|CAPTCHA|Login|Authentication|Authenticated|Oauth|JWT)

- Source File : online-book-store/secure/admin_add.php

```
[62]                        header("Location: admin_book.php");
```

- Source File : online-book-store/secure/admin_delete.php

```
[13]        header("Location: admin_book.php");
```

- Source File : online-book-store/secure/admin_verify.php

```
[23]        $query = "SELECT name, pass from admin";
[39]        header("Location: admin_book.php");
```

- Source File : online-book-store/secure/edit_book.php

```
[56]                header("Location: admin_edit.php?bookisbn=$isbn");
```

- Source File : online-book-store/secure/verify.php

```
[11]        $query = "SELECT username, password FROM admin";
[20]                        echo "Welcome admin! Long time no see";
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

```
[507]     * @param $name : the name of admin
[508]     * @return Admin or null if any exception happened or user not found
[510]    public function getadmin ($name): Admin
[514]            SELECT * FROM admin WHERE user_name=?;
[520]            return new Admin($row['admin_id'], $row['user_name'], $row['pass']);
[535]            SELECT * FROM admin ORDER BY admin_id;
```

- Source File : online-book-store/secure/database/readme.txt.txt

```
[10]to connect the admin section, click the name Nghi Le Thanh at the bottom.
[11]the name and pass for log in is admin , admin. Just to make it simple.
```

- Source File : online-book-store/secure/models/admin/Admin.php

```
[10]class Admin
[18]     * Admin constructor.
[28]        Admin::$admins;
```

- Source File : online-book-store/secure/template/footer.php

```
[8]                         <a href="admin.php">Admin Login</a> 2017
```

[+] Keyword Searched : SELECT ORDERBY

- Source File : online-book-store/secure/publisher_list.php

```
[6]        $query = "SELECT * FROM publisher ORDER BY publisherid";
```

- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

```
[467]            SELECT publisher_id,name FROM publisher ORDER BY  2 ");
[535]            SELECT * FROM admin ORDER BY admin_id;
[549]            SELECT * FROM author  ORDER BY name;
[593]            SELECT * FROM genre  ORDER BY genre_desc;
```

- Source File : online-book-store/secure/functions/database_functions.php

```
[13]                $query = "SELECT book_isbn, book_image FROM books ORDER BY book_isbn DESC";
[117]                $query = "SELECT * from books ORDER BY book_isbn DESC";
```

[+] Keyword Searched : URLs

- Source File : online-book-store/secure/template/footer.php

```
[5]                <a href="http://projectworlds.in" target="_blank"> projectworlds </a>
```

Parsed Paths – Areas of Interest

This section contains a list of file paths that have been identified by matching them with a predefined set of keywords. These files are typically of interest to a code reviewer, and should be examined for possible security vulnerabilities or insecure implementations.

[+] Keyword Searched : Admin Section/Areas

- Source File : online-book-store/secure/admin.php
- Source File : online-book-store/secure/admin_add.php
- Source File : online-book-store/secure/admin_book.php
- Source File : online-book-store/secure/admin_delete.php
- Source File : online-book-store/secure/admin_edit.php
- Source File : online-book-store/secure/admin_signout.php
- Source File : online-book-store/secure/admin_verify.php
- Source File : online-book-store/secure/functions/admin.php
- Source File : online-book-store/secure/models/admin/Admin.php

[+] Keyword Searched : Purchases | Ordering

- Source File : online-book-store/secure/cart.php
- Source File : online-book-store/secure/purchase.php
- Source File : online-book-store/secure/functions/cart_functions.php
- Source File : online-book-store/secure/models/orders/OrderDetails.php
- Source File : online-book-store/secure/models/orders/Orders.php
- Source File : online-book-store/secure/models/orders/OrdersTest.php
- Source File : online-book-store/secure/models/orders/UnAvailableOrderDetails.php

[+] Keyword Searched : Models

- Source File : online-book-store/secure/models/admin/Admin.php
- Source File : online-book-store/secure/models/customer/Customers.php
- Source File : online-book-store/secure/models/goods/Address.php
- Source File : online-book-store/secure/models/goods/Author.php
- Source File : online-book-store/secure/models/goods/Book.php
- Source File : online-book-store/secure/models/goods/BookTest.php
- Source File : online-book-store/secure/models/goods/Genre.php
- Source File : online-book-store/secure/models/goods/Publishers.php
- Source File : online-book-store/secure/models/interfaces/Damage.php
- Source File : online-book-store/secure/models/orders/OrderDetails.php
- Source File : online-book-store/secure/models/orders/Orders.php
- Source File : online-book-store/secure/models/orders/OrdersTest.php
- Source File : online-book-store/secure/models/orders/UnAvailableOrderDetails.php
- Source File : online-book-store/secure/models/reviews/Review.php
- Source File : online-book-store/secure/models/serve/FileInterface.php
- Source File : online-book-store/secure/models/serve/Image.php

[+] Keyword Searched : Controllers

- Source File : online-book-store/secure/controllers/DatabaseTalking/Take.php
- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

Identified Files Path

In this section, you'll find a comprehensive list of project file paths that were parsed during the analysis. This list was generated based on the selected file types during the scanning process and was used to identify the areas of interest listed in the previous sections. It's important to note that this list includes all the files, making it a superset of the list provided in the "Parsed Paths - Areas of Interest" section.

It is still recommended for code reviewers to review this list for any potentially interesting files that may have been overlooked in the "Parsed Paths - Areas of Interest" section.

- Source File : online-book-store/secure/admin.php

- Source File : online-book-store/secure/admin_add.php

- Source File : online-book-store/secure/admin_book.php

- Source File : online-book-store/secure/admin_delete.php

- Source File : online-book-store/secure/admin_edit.php

- Source File : online-book-store/secure/admin_signout.php

- Source File : online-book-store/secure/admin_verify.php

- Source File : online-book-store/secure/book.php

- Source File : online-book-store/secure/bookPerPub.php

- Source File : online-book-store/secure/books.php

- Source File : online-book-store/secure/cart.php

- Source File : online-book-store/secure/checkout.php

- Source File : online-book-store/secure/contact.php

- Source File : online-book-store/secure/edit_book.php

- Source File : online-book-store/secure/empty_session.php

- Source File : online-book-store/secure/index.php

- Source File : online-book-store/secure/process.php

- Source File : online-book-store/secure/publisher_list.php

- Source File : online-book-store/secure/purchase.php

- Source File : online-book-store/secure/verify.php

- Source File : online-book-store/secure/controllers/DatabaseTalking/Take.php

- Source File : online-book-store/secure/controllers/DatabaseTalking/Talking.php

- Source File : online-book-store/secure/database/readme.txt.txt

- Source File : online-book-store/secure/functions/admin.php

- Source File : online-book-store/secure/functions/cart_functions.php

- Source File : online-book-store/secure/functions/database_functions.php

- Source File : online-book-store/secure/models/admin/Admin.php

- Source File : online-book-store/secure/models/customer/Customers.php

- Source File : online-book-store/secure/models/goods/Address.php

- Source File : online-book-store/secure/models/goods/Author.php

- Source File : online-book-store/secure/models/goods/Book.php

- Source File : online-book-store/secure/models/goods/BookTest.php

- Source File : online-book-store/secure/models/goods/Genre.php

- Source File : online-book-store/secure/models/goods/Publishers.php

- Source File : online-book-store/secure/models/interfaces/Damage.php

- Source File : online-book-store/secure/models/orders/OrderDetails.php
- Source File : online-book-store/secure/models/orders/Orders.php
- Source File : online-book-store/secure/models/orders/OrdersTest.php
- Source File : online-book-store/secure/models/orders/UnAvailableOrderDetails.php
- Source File : online-book-store/secure/models/reviews/Review.php
- Source File : online-book-store/secure/models/serve/FileInterface.php
- Source File : online-book-store/secure/models/serve/Image.php
- Source File : online-book-store/secure/template/footer.php
- Source File : online-book-store/secure/template/header.php