projectworldsofficial / **online-book-store-project-in-php** Public

Code · Issues 14 · Pull requests 2 · Actions · Projects · Security · ...

New issue

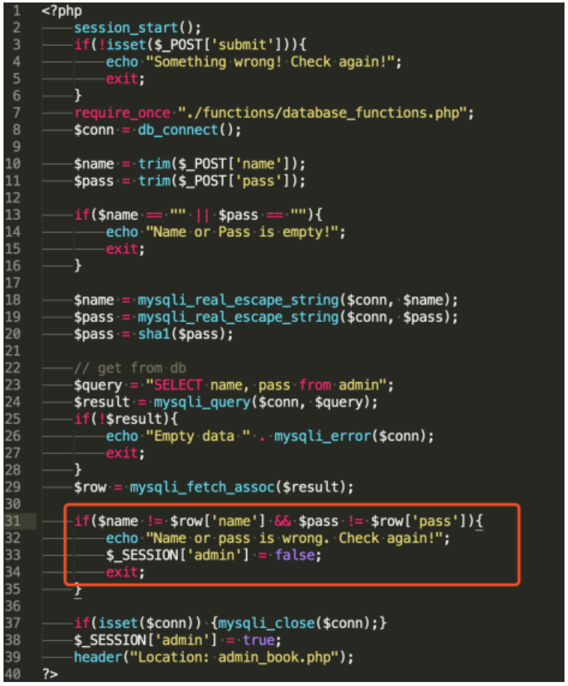
Jump to bottom

there is a login bypass vulnerability in admin_verify.php #14

○ Open **liao10086** opened this issue on Jan 17, 2020 · 0 comments

liao10086 commented on Jan 17, 2020

version:1.0
No login required.
View source code admin_verify.php

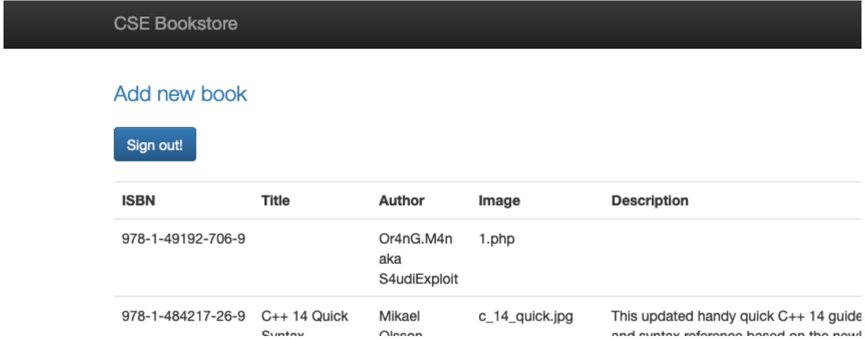


```
<?php
    session_start();
    if(!isset($_POST['submit'])){
        echo "Something wrong! Check again!";
        exit;
    }
    require_once "./functions/database_functions.php";
    $conn = db_connect();

    $name = trim($_POST['name']);
    $pass = trim($_POST['pass']);

    if($name == "" || $pass == ""){
        echo "Name or Pass is empty!";
        exit;
    }

    $name = mysqli_real_escape_string($conn, $name);
    $pass = mysqli_real_escape_string($conn, $pass);
    $pass = sha1($pass);

    // get from db
    $query = "SELECT name, pass from admin";
    $result = mysqli_query($conn, $query);
    if(!$result){
        echo "Empty data " . mysqli_error($conn);
        exit;
    }
    $row = mysqli_fetch_assoc($result);

    if($name != $row['name'] && $pass != $row['pass']){
        echo "Name or pass is wrong. Check again!";
        $_SESSION['admin'] = false;
        exit;
    }

    if(isset($conn)) {mysqli_close($conn);}
    $_SESSION['admin'] = true;
    header("Location: admin_book.php");
?>
```

he judgment is that if the query results of login name and password are not the same, the judgment is that the password or user name is wrong

This is obviously wrong. According to this meaning, you can log in successfully as long as the user name and password are matched

We test that the login name is admin password arbitrary



Add new book

ISBN	Title	Author	Image	Description
978-1-49192-706-9		Or4nG.M4n aka S4udiExploit	1.php	
978-1-484217-26-9	C++ 14 Quick	Mikael	c_14_quick.jpg	This updated handy quick C++ 14 guide

Login succuss!
suggest:Change this code to
if($name != $row['name'] || $pass != $row['pass']){
author:zionlab@dbappsecurity.com.cn

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

1 participant