



VDB-355294 · CVE-2026-5541 · GCVE-100-355294

# CODE-PROJECTS SIMPLE LAUNDRY SYSTEM 1.0 PARAMETER /MODMEMBERINFO.PHP USERID CROSS SITE SCRIPTING

CVSS Meta Temp Score

3.9

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

3.54-

## Summary

A vulnerability, which was classified as [problematic](#), was found in [code-projects Simple Laundry System 1.0](#). Impacted is an unknown function of the file `/modmemberinfo.php` of the component *Parameter Handler*. Executing a manipulation of the argument `userid` can lead to cross site scripting. The identification of this vulnerability is [CVE-2026-5541](#). The attack may be launched remotely. Furthermore, there is an exploit available.

## Details

A vulnerability classified as problematic was found in [code-projects Simple Laundry System 1.0](#). This vulnerability affects some unknown functionality of the file `/modmemberinfo.php` of the component *Parameter Handler*. The manipulation of the argument `userid` with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is [CWE-79](#). The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. As an impact it is known to affect integrity.

The advisory is available at [github.com](#). This vulnerability was named [CVE-2026-5541](#). The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Successful exploitation requires user interaction by the victim. Technical details and also a public exploit are known. This vulnerability is assigned to [T1059.007](#) by the MITRE ATT&CK project.

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:modmemberinfo.php` it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entries [VDB-355328](#), [VDB-355330](#), [VDB-355334](#) and [VDB-355335](#) are related to this item.

## Product

### Type

- [Project Management Software](#)

### Vendor

- [code-projects](#)

### Name

- [Simple Laundry System](#)

### Version

- [1.0](#)

### License

- [free](#)

### Website

- Vendor: <https://code-projects.org/>

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

## CVSSv3

VuIDB Meta Base Score: 4.3

VuIDB Meta Temp Score: 3.9

VuIDB Base Score: 4.3

VuIDB Temp Score: 3.9

VuIDB Vector: 

VuIDB Reliability: 

# CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

## Exploiting

Class: Cross site scripting

CWE: [CWE-79](#) / [CWE-94](#) / [CWE-74](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

Google Hack: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

## Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

## Countermeasures

**Recommended:** no mitigation known

**Status:** 🔍

**0-Day Time:** 🔒

## Timeline

<b>04/04/2026</b>		Advisory disclosed
<b>04/04/2026</b>	+0 days	VulDB entry created
<b>04/04/2026</b>	+0 days	VulDB entry last update

## Sources

**Vendor:** [code-projects.org](https://code-projects.org)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-5541](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-5541](#)

**GCVE (VulDB):** [GCVE-100-355294](#)

**scip Labs:** <https://www.scip.ch/en/?labs.20161013>

**See also:** 🔒

## Entry

**Created:** 04/04/2026 08:52 AM

**Changes:** 04/04/2026 08:52 AM (57)

**Complete:** 🔍

**Submitter:** [Weining Xiao](#)

**Cache ID:** 20:E6C:179

## Submit

### Accepted

- [Submit #782223](#): code-projects Simple Laundry System V1.0 cross site scripting (by Weining Xiao)

## Discussion

No comments yet. Languages: en.

Please log in to comment.