



VDB-354189 · CVE-2026-5157 · GCVE-100-354189

CODE-PROJECTS ONLINE FOOD ORDERING SYSTEM 1.0 ORDER /FORM/ORDER.PHP CUST_ID CROSS SITE SCRIPTING

CVSS Meta Temp Score 

3.9

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

2.85

Summary

A vulnerability has been found in [code-projects Online Food Ordering System 1.0](#) and classified as **problematic**. Affected by this vulnerability is an unknown functionality of the file `/form/order.php` of the component *Order Module*. Performing a manipulation of the argument `cust_id` results in cross site scripting. This vulnerability is cataloged as [CVE-2026-5157](#). It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability, which was classified as **problematic**, was found in [code-projects Online Food Ordering System 1.0](#). This affects an unknown part of the file `/form/order.php` of the component *Order Module*. The manipulation of the argument `cust_id` with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as [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. This is going to have an impact on integrity.

The advisory is shared at [gist.github.com](#). This vulnerability is uniquely identified as [CVE-2026-5157](#). The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. It demands that the victim is doing some kind of user interaction. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique [T1059.007](#) for this issue.

The exploit is shared for download at [gist.github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:form/order.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-209440](#), [VDB-209441](#), [VDB-209442](#) and [VDB-209444](#) are related to this item.

Product

Type

- [Project Management Software](#)

Vendor

- [code-projects](#)

Name

- [Online Food Ordering System](#)

Version

- [1.0](#)

License

- [free](#)

Website

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

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 4.3

VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3

VulDB Temp Score: 3.9

VulDB Vector: 

VulDB 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

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

Sources

Vendor: code-projects.org

Advisory: gist.github.com

Status: Not defined

CVE: [CVE-2026-5157](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5157](#)

GCVE (VulDB): [GCVE-100-354189](#)

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

See also: 🗝️

Entry

Created: 03/30/2026 03:41 PM

Changes: 03/30/2026 03:41 PM (57)

Complete: 🔍

Submitter: [Abhiram T](#)

Cache ID: 20:975:179

Submit

Accepted

- [Submit #776186](#): code-projects Online Food Ordering System 1.0 Cross Site Scripting (by Abhiram T)

Discussion

No comments yet. Languages: en.

Please log in to comment.