



VDB-355521 · CVE-2026-5705 · GCVE-100-355521

CODE-PROJECTS ONLINE HOTEL BOOKING 1.0 BOOKING ENDPOINT /BOOKNOW.PHP ROOMNAME CROSS SITE SCRIPTING

CVSS Meta Temp Score ⓘ

3.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.77

Summary

A vulnerability was found in [code-projects Online Hotel Booking 1.0](#). It has been classified as **problematic**. Affected by this issue is some unknown functionality of the file `/booknow.php` of the component *Booking Endpoint*. Performing a manipulation of the argument `roomname` results in cross site scripting. This vulnerability is identified as [CVE-2026-5705](#). The attack can be initiated remotely. Additionally, an exploit exists.

Details

A vulnerability, which was classified as **problematic**, was found in [code-projects Online Hotel Booking 1.0](#). This affects an unknown code block of the file `/booknow.php` of the component *Booking Endpoint*. The manipulation of the argument `roomname` 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 [github.com](#). This vulnerability is uniquely identified as [CVE-2026-5705](#). 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 [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:booknow.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.

Product

Type

- Hospitality Software

Vendor

- code-projects

Name

- Online Hotel Booking

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

04/06/2026		Advisory disclosed
04/06/2026	+0 days	VulDB entry created
04/06/2026	+0 days	VulDB entry last update

Sources

Vendor: code-projects.org

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5705](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5705](#)

GCVE (VulDB): [GCVE-100-355521](#)

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

Entry

Created: 04/06/2026 04:22 PM

Changes: 04/06/2026 04:22 PM (57)

Complete: 🔍

Submitter: [AhmadMarzouk](#)

Cache ID: 20:EEF:179

Submit

Accepted

- [Submit #786325](#): code-projects Online Hotel Booking IN PHP 1.0 Cross Site Scripting (by AhmadMarzouk)

Discussion

No comments yet. Languages: en.

Please log in to comment.