



CVE-2020-24026

Published on: 05/18/2021 12:00:00 AM UTC

Last Modified on: 05/24/2021 07:59:00 PM UTC

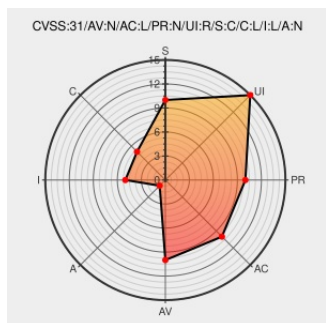
CVE-2020-24026

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Tinyshop](#) from [Tinyshop Project](#) contain the following vulnerability:

TinyShop, a free and open source mall based on RageFrame2, has a stored XSS vulnerability that affects version 1.2.0. TinyShop allows XSS via the explain_first and again_explain parameters of the /evaluate/index.php page. The vulnerability may be exploited remotely, resulting in cross-site scripting (XSS) or information disclosure.

CVE-2020-24026 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
GitHub - jianyan74/TinyShop: 一款基于 RageFrame2 的免费开源的基础销售功能的商城	github.com text/html	MISC github.com/jianyan74/TinyShop
GitHub - stavvan/TinyShop-1 IniApp: 基于 RageFrame2 的一款免费开源的基础商	github.com	MISC github.com/stavvan/TinyShop-

© jianyan74/TinyShop 小程序: 基于 RAGEFRAME2 的 免费及开源的轻量级商城销售功能的开源微商城。

[github.com](#)
text/html

[github.com/jianyan74/TinyShop](#)
UniApp

XSS vulnerability in reply to product reviews · Issue #14 · jianyan74/TinyShop · GitHub

[github.com](#)
text/html

[github.com/jianyan74/TinyShop/issues/14](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tinyshop Project	Tinyshop	1.2.0	All	All	All

cpe:2.3:a:tinyshop_project:tinyshop:1.2.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-24026 : TinyShop, a free and open source mall based on RageFrame2, has a stored #XSS vulnerability that af... twitter.com/i/web/status/1...	2021-05-18 15:05:05
/r/netcve	CVE-2020-24026	2021-05-18 15:41:23

← Previous ID

Next ID→