



CVE-2021-38699

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-38699
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-15 18:15:00 UTC
Updated	2021-10-18 12:23:00 UTC
Description	TastyIgniter 3.0.7 allows XSS via /account, /reservation, /admin/dashboard, and /admin/system_logs.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tastyigniter	Tastyigniter	3.0.7	All	All	All

References

Reference	Source	Link
TastyIgniter 3.0.7 Cross Site Scripting ≈ Packet Storm	MISC	packet
GitHub - HuskyHacks/CVE-2021-38699-Reflected-XSS: Multiple Reflected XSS in TastyIgniter v3.0.7 Restaurant CMS	MISC	github
Support Center - TastyIgniter	MISC	tastyig
GitHub - HuskyHacks/CVE-2021-38699-Stored-XSS: Stored XSS in TastyIgniter v3.0.7 Restaurant CMS	MISC	github
CVE-2021-38699 TastyIgniter 3.0.7 Stored Cross Site Scripting Vulnerability – PentesterNotes	MISC	pentest
GitHub - Justin-1993/CVE-2021-38699: TastyIgniter 3.0.7 allows XSS via the name field during user-account creation	MISC	github
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)