



# CVE-2017-9609

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-9609
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-07-17 21:29:00 UTC
<b>Updated</b>	2017-07-21 14:31:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in Blackcat CMS 1.2 allows remote authenticated users to inject arbitrary web script

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Blackcat-cms</a>	<a href="#">Blackcat Cms</a>	1.2	All	All	All
Application	<a href="#">Blackcat-cms</a>	<a href="#">Blackcat Cms</a>	1.2	All	All	All

## References

### Reference

- GitHub - faizzaidi/Blackcat-cms-v1.2-xss-POC-by-Provensec-Ilc: BlackCat-CMS-Bundle-v1.2 Cross Site Scripting(XSS) Assigned CVE Number
- XSS in Blackcat cms v1.2 · Issue #373 · BlackCatDevelopment/BlackCatCMS · GitHub
- Blackcat CMS 1.2 Cross Site Scripting ≈ Packet Storm
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)