# CVE Detail – CVE-2021-25926

In SiCKRAGE, versions 9.3.54.dev1 to 10.0.11.dev1 are vulnerable to Reflected Cross-Site-Scripting (XSS) due to user input not being validated properly in the `quicksearch` feature. Therefore, an attacker can steal a user's sessionID to masquerade as a victim user, to carry out any actions in the context of the user.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.55325

## CVSS Scoring

CVSS v3.1 Score: 6.1

Severity: MEDIUM

## Mapped CWE(s)

* CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

## CAPEC(s)

* CAPEC-209: XSS Using MIME Type Mismatch
* CAPEC-588: DOM-Based XSS
* CAPEC-591: Reflected XSS
* CAPEC-592: Stored XSS
* CAPEC-63: Cross-Site Scripting (XSS)
* CAPEC-85: AJAX Footprinting

## Affected Products

* cpe:2.3:a:sickrage:sickrage:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:sickrage:sickrage:10.0.11:dev1:\*:\*:\*:\*:\*:\*